# Compaq PATHWORKS for OpenVMS (Advanced Server)

# Server Administrator's Guide

Order Number: AA–R6G6C–TE

**October 2001**

This guide presents step-by-step procedures for managing and maintaining the Advanced Server. It explains how to complete common tasks, such as managing files and directories, printing, and administering the network.

| | |
|---|---|
| **Revision/Update Information:** | This guide supersedes the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Administrator's Guide*, Version 6.0B. |
| **Operating System:** | OpenVMS Alpha Version 6.2, 7.2-1, 7.2-2, 7.3<br>OpenVMS VAX Version 6.2, 7.2, 7.3 |
| **Software Version:** | PATHWORKS V6.1 for OpenVMS (Advanced Server) |

**Compaq Computer Corporation**
**Houston, Texas**

ZK6556

The PATHWORKS for OpenVMS (Advanced Server) documentation set is available on CD-ROM.

This document was prepared using DECdocument, Version 3.3-1b.

# Contents

## 2 Managing Domains and Servers

## 3 Managing Users and Groups

## 4 Managing Directory and File Sharing

## 5 Managing Printers, Print Queues, and Print Shares

## 6 Monitoring Events and Troubleshooting

## 7 Managing Server Configuration Parameters

## A Network Protocols



## Index

## Examples



## Figures



## Tables

# Preface

## About This Guide

Welcome to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Administrator's Guide*. For the purpose of this text, the PATHWORKS for OpenVMS (Advanced Server) software is referred to as the PATHWORKS Advanced Server. The PATHWORKS Advanced Server and its associated OpenVMS system platform provide a powerful, reliable, and open operating environment that meets the demands of client/server computing.

The *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Administrator's Guide* presents step-by-step procedures for managing and maintaining the PATHWORKS Advanced Server. It explains how to complete common tasks, such as managing files and directories, printing, and administering the network. Unless otherwise noted, commands used in procedures and examples are PATHWORKS Advanced Server ADMINISTER commands.

## Intended Audience

This guide is for the OpenVMS network administrator. As the administrator, you must be familiar with the Compaq *OpenVMS* operating system to support the server, and with other operating systems to support clients. It is also expected that you have had experience managing an OpenVMS system and doing network administration, and that you are familiar with the specific network configuration being managed.

You are assumed to have read the following product manuals:

- *Compaq Advanced Server for OpenVMS Concepts and Planning Guide*
- *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide*
- *Compaq Advanced Server for OpenVMS Guide to Managing Advanced Server Licenses*

If you are upgrading your server from a previous version such as PATHWORKS for OpenVMS (LAN Manager), be sure to follow the procedures in the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Migration Guide*.

You are assumed to have access to the following documentation:

- *Compaq Advanced Server for OpenVMS Commands Reference Manual*
- Documentation for any clients running other operating systems

This guide addresses use of the PATHWORKS for OpenVMS (Advanced Server) only.

## Document Structure

The following table lists the chapters in this guide:

| Chapter | Description |
|---|---|
| Chapter 1 | Provides an overview of the responsibilities of a network administrator, the features of a PATHWORKS Advanced Server network, the principles of resource sharing, and the network administration interfaces for administering the PATHWORKS Advanced Server |
| Chapter 2 | Explains how to manage servers and domains with the PATHWORKS Advanced Server software |
| Chapter 3 | Explains how to manage users and groups in the PATHWORKS Advanced Server environment |
| Chapter 4 | Explains how to manage shared disk resources, including directory and file sharing |
| Chapter 5 | Explains how to share printer resources, including printers and print queues |
| Chapter 6 | Explains how to monitor events and troubleshoot your server |
| Chapter 7 | Describes the Configuration Manager tool and how to use it to configure and tune parameters that, for the most part, affect your server's system environment, and the LANMAN.INI file, which stores basic server-specific configuration parameters |
| Appendix A | Describes each of the supported network protocols |

## Related Documents

The following table lists PATHWORKS Advanced Server documents:

| Document | Description |
|---|---|
| *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Migration Guide* | Explains how to upgrade a PATHWORKS (LAN Manager) server to PATHWORKS V6 for OpenVMS (Advanced Server) |
| *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide* | Explains how to install and configure PATHWORKS for OpenVMS (Advanced Server) software |
| *Compaq Advanced Server for OpenVMS Concepts and Planning Guide* | Provides an overview of and introduction to the Advanced Server software and associated networking concepts for system administrators and operators |
| *Compaq Advanced Server for OpenVMS Commands Reference Manual* | Provides command syntax descriptions for all ADMINISTER commands and NET command equivalents |
| *Compaq Advanced Server for OpenVMS Guide to Managing Advanced Server Licenses* | Describes the LICENSE SERVER software and how to manage Advanced Server licenses |

The following table lists related OpenVMS documents:

| OpenVMS Document | Description |
|---|---|
| *OpenVMS Version 7.x New Features and Documentation Overview Manual* | Describes the new features of the OpenVMS software and provides an overview of the documentation that supports it |
| *OpenVMS Alpha Version 7.x Upgrade and Installation Manual* | Explains how to install the OpenVMS Alpha system software |
| *OpenVMS VAX Version 7.x Upgrade and Installation Manual* | Explains how to install the OpenVMS VAX system software |
| *OpenVMS System Manager's Manual* | A task-oriented guide (in two volumes) to managing an OpenVMS system; explains how to set up the required system services |
| *OpenVMS System Management Utilities Reference Manual* | A reference guide (in two volumes) to the utilities and tools used in managing an OpenVMS system |
| *OpenVMS License Management Utility Manual* | Explains how to load and manage license Product Authorization Keys (PAKs) |
| *Compaq C Run-Time Library Utilities Reference Manual* | Describes utilities that help you manage localization and time zone data for international software applications |

For additional information about the OpenVMS products and services, access the following World Wide Web address:

`http://www.openvms.compaq.com/`

## Reader's Comments

Compaq welcomes your comments on this manual. Please send comments to either of the following addresses:

| | |
|---|---|
| Internet | **openvmsdoc@compaq.com** |
| Mail | Compaq Computer Corporation<br>OSSG Documentation Group, ZKO3-4/U08<br>110 Spit Brook Rd.<br>Nashua, NH 03062-2698 |

## How To Order Additional Documentation

Visit the following World Wide Web address for information about how to order additional documentation:

`http://www.openvms.compaq.com/`

If you need help deciding which documentation best meets your needs, call 800-282-6672.

## Conventions

The terms PATHWORKS Advanced Server and Advanced Server are used in this guide to refer to the PATHWORKS for OpenVMS (Advanced Server) file and print server.

The following conventions are used in the PATHWORKS Advanced Server documentation:

| Convention | Meaning |
|---|---|
| *Italic* | Italic text indicates a placeholder for information or parameters that you must provide. For example, if the procedure asks you to type *file-name*, you must type the actual name of a file.<br>Italic text also indicates path names, new terms, and the titles of other documents. |
| **bold** | Bold text indicates a server configuration parameter name, a command button name, or a menu item. |
| `monospace` | Monospace text indicates the actual commands, words, or characters that you type in a dialog box or at a command prompt or system output. |
| UPPERCASE TEXT | Uppercase text indicates names of OpenVMS and Advanced Server commands and qualifiers. You can enter commands and qualifiers in any combination of uppercase and lowercase letters, unless otherwise noted. |
| / | A forward slash in command descriptions indicates that a command qualifier follows. |
| = | An equal sign (=) in command descriptions indicates you must provide information. |
| [ ] | In command format descriptions, brackets indicate optional elements. Multiple elements are separated by vertical bars ( \| ). You can enter as many as you want. |

| Convention | Meaning |
|---|---|
| { } | In command format descriptions, braces indicate you must enter at least one listed element. The elements are separated by bars ( \| ). |
| . . . | A horizontal ellipsis following an entry in a command line indicates that the entry or a similar entry can be repeated any number of times. An ellipsis following a file name indicates that additional parameters, values, or information can be entered. |
| .<br>.<br>. | A vertical ellipsis in an example indicates that not all the data is shown. |
| **Note** | The use of **Note** indicates information of special importance. |
| **Caution** | The use of **Caution** indicates information to avoid damaging hardware or software. |
| Ctrl/*x* | While you hold down the Ctrl key, press another key or a pointing device button. |
| Return or Enter | In text, Return or Enter indicates where you should press the Return or Enter key to execute a command or terminate a sequence. This key is labeled Return or Enter, depending on your keyboard. |
| Tab | In examples, a key name enclosed in a box indicates that you press a key on the keyboard. (In text, a key name is not enclosed in a box.)<br>In the HTML version of this document, this convention appears as brackets, rather than a box. |
| PF1 *x* | A sequence such as PF1 *x* indicates that you must first press and release the key labeled PF1 and then press and release another key or a pointing device button. |

# 1
# Overview

The Advanced Server is an OpenVMS-based network operating system (NOS) compatible with Microsoft networking technology. The Advanced Server software provides a flexible system for managing wide area networks (WANs) and local area networks (LANs). The software lets you use Compaq Computer Corporation computers as servers to share network resources with supported clients and is compatible with Windows NT and Windows 2000 servers running in the same network.

As a server for computers in a network, the Advanced Server provides file and print services that enable the efficient sharing of computing resources among a community of desktop users. It can function as a file and print server for a small, isolated community of users or as the foundation of a large network distributed over a wide geographical area.

You can perform Advanced Server management tasks from any client or server that is running Windows NT server administration tools, and from any Advanced Server using the Advanced Server ADMINISTER commands. This document shows you how to manage your servers using Advanced Server software.

This overview of Advanced Server describes the role of the network administrator, and the features available with Advanced Server, in the following sections:

- Section 1.1, The Role of the Administrator, describes what you do, as the server administrator, and what tasks you perform to administer the network.
- Section 1.2, The Advanced Server Network, describes the components of the network, its features, and services.
- Section 1.3, Resource Sharing, describes the resources you can share, such as directories and print queues, and how to share them.
- Section 1.4, Monitoring Events and Troubleshooting, describes the tools you use to track resource use and to modify your network configurations.

- Section 1.5, Network Administration Interfaces, describes the server and client software interfaces with which you manage your servers, including the Advanced Server ADMINISTER command-line interface.
- Section 1.6, The Advanced Server ADMINISTER Command-Line Interface, describes the Advanced Server ADMINISTER command-line interface.

## 1.1 The Role of the Administrator

When you administer any network, you plan, set up, and maintain that network. For information on planning and design, refer to the *Compaq Advanced Server for OpenVMS Concepts and Planning Guide*.

To plan a network, complete the following tasks:

- Organize the network into domains.
- Decide how to configure each server in a domain.
- Evaluate new applications and peripherals.

After planning your network and putting all hardware and connecting links in place, you install and configure Advanced Server software. You can then use the instructions in this document to customize and manage the server.

### 1.1.1 Setting Up the Advanced Server Environment

As part of the configuration procedure (PWRK$CONFIG.COM) described in the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide*, you can specify parameters to establish your network and server system.

Initial configuration of the server is performed when you install and configure the server software. The configuration procedure, PWRK$CONFIG.COM, allows you to modify the system environment in which the server operates and also to determine the initial server configuration that is stored in the LANMAN.INI file. The PWRK$CONFIG.COM configuration procedure is described in the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide*. If you choose to modify the system environment parameters (such as client capacity, OpenVMS process priority, and network transports), the PWRK$CONFIG.COM configuration procedure invokes the Configuration Manager (a character-cell interface). After you finish modifying those parameters and exit from the Configuration Manager, the PWRK$CONFIG.COM procedure then allows you to modify the basic server configuration parameters (such as the server role, cluster alias, and comment string) stored in the LANMAN.INI file.

After completing the configuration procedure, you can modify server parameters directly affecting the server by changing or adding keyword values to the LANMAN.INI file. For more information, see Section 7.3, Using the LANMAN.INI File. You can also invoke the Advanced Server Configuration Manager manually with the ADMINISTER/CONFIGURATION command to modify the server parameters affecting the server system's environment. For more information, see Section 7.2, Using the Configuration Manager.

### 1.1.2 Administering the Network

Once you have planned and set up your overall network configuration, you support it by performing the following tasks:

- Maintaining user accounts, shares, and other resources, such as printers
- Monitoring events and troubleshooting server problems

#### 1.1.2.1 Maintaining User Accounts, Shares, and Resources

Performing this maintenance includes:

- Keeping records of the network configuration
- Adding new users who need access to server resources
- Removing users who no longer need access to server resources
- Setting up and controlling shared directories
- Setting up and controlling shared print queues
- Controlling server disk storage space
- Backing up and restoring server files

#### 1.1.2.2 Monitoring Events and Troubleshooting Server Problems

You may need to perform certain infrequently used procedures to resolve network problems caused by unexpected conditions; for example, faulty wiring, faulty hardware, or overloaded servers or printers. Advanced Server provides commands and diagnostic tools to help you isolate and fix such problems.

Chapter 6, Monitoring Events and Troubleshooting, describes some ways to monitor and troubleshoot your network.

## 1.2 The Advanced Server Network

An Advanced Server network consists of computers, both servers and clients. Servers control resources that client systems on the network can use. Clients are typically PC-based systems that need access to resources on the server. Workstations and other computers running networking software that can access network resources can be clients.

Supported client operating systems include Windows 3.11, Windows 95, Windows 98, Windows 2000, Windows NT, Windows for Workgroups, and MS-DOS. Compaq PATHWORKS 32 client software is supported but not required.

Servers in the network can run the following software:

- Advanced Server for OpenVMS, V7.2 or higher
- PATHWORKS V6 for OpenVMS (Advanced Server)
- PATHWORKS V5 for OpenVMS (LAN Manager)
- Advanced Server for UNIX (*Tru64* UNIX)
- Windows NT Server V3.51 or V4
- Windows 2000

### 1.2.1 Domains

To help you manage a large and diverse network, Advanced Server software lets you divide the network into domains, or administrative groups of servers and clients. With domains, control of user access to the network and its resources is centralized and simplified, and you can establish exactly which servers a specific user can access.

A domain is a collection of computers that share a common security accounts database and security policy. You create a domain when you install and configure a primary domain controller. To enable users to access resources in domains where they have no user accounts, you can establish trust relationships between domains. This provides flexibility when configuring large networks with multiple domains. For more information about planning domains, refer to the *Compaq Advanced Server for OpenVMS Concepts and Planning Guide*. For more information on managing domains, see Chapter 2, Managing Domains and Servers.

### 1.2.2 Security

Advanced Server provides two security models:

- Advanced Server Only security model
- Advanced Server and OpenVMS security model

The Advanced Server Only security model provides access based on Advanced Server user account security policies and user access rights on shared resources. The Advanced Server and OpenVMS security model provides access based on both Advanced Server and OpenVMS security policies. The Advanced Server and OpenVMS security model is never necessary to control user access to resources, but is provided to allow administrators of systems with complex OpenVMS security controls already in place to use those same controls to restrict access by client users. Note that use of the Advanced Server and OpenVMS security model results in the extra overhead of validating both the Advanced Server and OpenVMS settings.

### 1.2.3 Users

A user who needs access to resources shared on a server must have access to one of the following:

- An Advanced Server user account established on that server. A user account contains all the information that the Advanced Server needs to define a user, including the user name, a description, and a password.
- A server that provides Guest access to resources.
- A server that provides access based on domain trust relationships.

The user account, with its associated password, identifies the user to the Advanced Server software. You can enable logon restrictions for each user account; for example, limiting the hours during which the user can access server resources.

By default, a shared resource is available to all users. You can assign access permissions to users for resources, specifying the type of access each user can have to a given resource. You can assign a different set of permissions for each user and for each shared resource. If you use the Advanced Server Only security model, access permissions grant access to OpenVMS files and directories on the server, regardless of the OpenVMS file protections. For more information on the interaction of these two access permissions, see Section 4.1.2, Advanced Server Security Models.

If a trust relationship has been established between two domains, you can grant access to resources for users from the trusted domain. To grant permissions to a user from a trusted domain, include the domain name when you specify the user name. For more information on trust relationships, see Section 2.1.8, Managing Trust Relationships.

### 1.2.4 Groups

To simplify administration of access permissions, you define groups of users. The members of a group are users and other groups. Groups provide an easy way to grant common capabilities to several users; group permissions are provided to all its members.

A group can be either global or local. A global group is a collection of user accounts allowed to access resources in one domain. It can also be assigned permissions to use resources in a trusting domain. A global group:

- Can be used to assign permissions and rights within the domain
- Cannot contain other groups as members
- Cannot contain users from another domain
- Cannot contain groups from another domain

A local group can include users and global groups from its own domain and from trusted domains. Thus, it provides access to resources in its domain to users in its domain and in trusted domains.

If a trust relationship has been established between two domains, you can grant access to resources for groups from the trusted domain. To grant permissions to the members of a group from another domain, include the domain name when you specify the group name.

For more information about groups, see Chapter 3, Managing Users and Groups.

### 1.2.5 Logon Validation

The Advanced Server can validate requests of users to log on to the network. Logon validation is provided by the NetLogon service and allows the following:

- A single, domainwide security accounts database
- Single domainwide logon, which lets a user access resources on any server in the domain and on servers that trust the domain

You create the master security accounts database for the domain when you configure the primary domain controller. This database is automatically copied to the backup domain controllers in the domain that are running the NetLogon service. You do not have to create user accounts separately on each server. All the servers in the domain that run the NetLogon service use identical copies of the same domainwide security accounts database.

Through external authentication, specified OpenVMS users are automatically validated on the network when they log in to the OpenVMS system running the Advanced Server. This pass-through style of authentication ensures password synchronization between OpenVMS user accounts and their corresponding Advanced Server network account. It eliminates the need for users to maintain a separate password for their OpenVMS and domain (network) user accounts. For more information about external authentication, see Section 3.1.17, External Authentication.

### 1.2.6 Logon Scripts

As the network administrator, you can use logon scripts to configure the working environments of your users by allowing them to automatically make network connections and start applications. The network administrator can create logon scripts and then assign a different logon script to each user, or create a logon script for multiple users. A logon script runs automatically whenever a user logs on at a workstation running Windows NT, Windows for Workgroups, Windows 95, Windows 98, or Windows 2000.

### 1.2.7 Home Directories

As the network administrator, you may want to assign a user a home directory on a server. Users can store private data in their home directories and have access control over these directories to restrict or grant access to other users. If users have home directories on computers other than their own, connections can be made automatically to home directories whenever users log on. Depending on the client operating system, you may need to specify the home directory in a logon script. For information about how to specify a logon script and home directory for a user account, see Section 3.1.3, User Account Attributes.

### 1.2.8 Advanced Server Licensing

To access the Advanced Server, clients must be properly licensed with a valid Client Access license. A client may obtain a client-based license to access an unlimited number of PATHWORKS servers, or an unlicensed client may be assigned a server-based license while accessing resources on a single PATHWORKS server. The Advanced Server includes the Advanced Server License Server, which distributes client-based licenses to clients during client startup. The Advanced Server License Registrar validates client-based licenses when the client establishes a session, and it allocates server-based licenses. The *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide* describes how to install the License Server. Refer to the *Compaq Advanced Server for OpenVMS Guide to Managing Advanced Server Licenses* for more information about Advanced Server licensing.

## 1.3 Resource Sharing

Sharing is the process of making resources (printers, directories, and files) available to users. As the network administrator, you make a resource available to clients who access the printer or directory by specifying a share name and permissions to control access to the share.

Users gain access to a shared resource by:

1. Logging on to the domain or a trusted domain
2. Connecting to the share

As the network administrator, you define which resources to share, which users and groups can access them, and the type of access each user and group can have.

### 1.3.1 Disk Directories

The Advanced Server automatically shares the root directory of all disk devices connected to the server that are mounted when you start the server process. This type of share is called an autoshare. It is accessible by Administrators only.

Advanced Server lets you audit user attempts to access shared files or directories. You specify the types of access attempts to be audited. When one of those events occurs, the Advanced Server records an entry in the Security event log.

For information about setting permissions and auditing for individual files and directories, see Chapter 4, Managing Directory and File Sharing.

The PATHWORKS for OpenVMS (Advanced Server) supports ODS-2 disk volumes. It treats ODS-5 disk volumes as ODS-2 disk volumes. (ODS-5 disk volumes, supported on OpenVMS Alpha systems V7.2 and higher, include support of Extended File Specifications, providing greater compatibility with Windows 2000, Windows 98, Windows 95, and Windows NT file systems. The PATHWORKS for OpenVMS (Advanced Server) product does not support the features provided by Extended File Specifications. The Advanced Server for OpenVMS product does support these features.)

### 1.3.2 Printers

The Advanced Server lets you share printers connected to the network. With Advanced Server, you can:

- Create Advanced Server print queues.
- Share print queues and set print queue permissions to restrict access to the queue. By default, a print share is available to all users.
- Manage print queues, print shares, and print jobs.

For information about managing print shares and queues, see Chapter 5, Managing Printers, Print Queues, and Print Shares.

## 1.4 Monitoring Events and Troubleshooting

The Advanced Server provides log files for monitoring server resource use and for recording client and server problems.

The event log records client and server events. It contains the following information about each event:

- Nature of the event
- Event type
- Date and time when the event occurred

You can establish an audit policy for event types on a server and set auditing for individual directories or files. The audit policy defines the types of events to be logged. Auditing also allows you to record server resource use. It can provide the following information about each access attempt:

- Name of the server resource accessed
- Operation performed or attempted
- Date and time of the operation
- User name of the user requesting access

For information about setting auditing for specific events and about troubleshooting server problems, see Chapter 6, Monitoring Events and Troubleshooting.

## 1.5 Network Administration Interfaces

You can administer the Advanced Server, another server, or a workstation in the network, from either a Compaq OpenVMS server or from another computer, using one of the interfaces listed in Table 1–1, Network Administration Interfaces.

**Table 1–1 Network Administration Interfaces**

| Computer Type | Interface |
|---|---|
| Advanced Server for OpenVMS and PATHWORKS V6 for OpenVMS (Advanced Server) | Includes the following:<br>• Advanced Server ADMINISTER commands (a command-line interface) – to administer servers, domains, and shares. The complete command set is described in the *Compaq Advanced Server for OpenVMS Commands Reference Manual*.<br>• Advanced Server Configuration Manager – to manage server-specific parameters that are not stored in the LANMAN.INI file on PATHWORKS for OpenVMS (Advanced Server) servers. These parameters are, directly or indirectly, related to the environment in which the Advanced Server operates, such as the server's usage of OpenVMS system resources and physical memory. This is described in Section 7.2, Using the Configuration Manager.<br>• On PATHWORKS for OpenVMS (Advanced Server) only, you can manage parameters that affect the behavior of the PATHWORKS for OpenVMS (Advanced Server) but not, for the most part, file server resource consumption, by editing the LANMAN.INI file, where these parameters are stored.<br>• Advanced Server License Manager (a character-cell interface) – to manage the Advanced Server licenses and License Server. For more information about the License Manager, refer to the *Compaq Advanced Server for OpenVMS Guide to Managing Advanced Server Licenses*. |
| Windows NT Server | Windows NT server administration tools (Windows-based interfaces, including Server Manager, Print Manager,[1] User Manager for Domains, and Event Viewer). |
| PATHWORKS (LAN Manager) | ADMIN/PATH utility (a character-cell user interface), or Net commands (a command-line interface). |

[1]Includes limited functionality, such as displaying, pausing, and deleting print jobs.

(continued on next page)

**Table 1–1 (Cont.) Network Administration Interfaces**

| Computer Type | Interface |
|---|---|
| Advanced Server for UNIX | `pwadmin` commands (a command-line interface), or `net` commands (limited functions). |
| DOS client | Net commands (a command-line interface). |
| Windows, Windows NT, Windows 2000, Windows 95, or Windows 98 client | MS-DOS Net interface (a command-line interface), Windows NT server administration tools (Windows-based user interfaces). |

## 1.6 The Advanced Server ADMINISTER Command-Line Interface

You can control most aspects of the Advanced Server using the Advanced Server ADMINISTER command-line interface. You invoke the Advanced Server ADMINISTER command-line interface by entering the ADMINISTER command at the OpenVMS system prompt. The Advanced Server command-line interface prompts you with the name of the domain and the name of the server you are currently administering. For example:

```
$ ADMINISTER
LANDOFOZ\\TINMAN>
```

In this example, you are managing a domain called LANDOFOZ and a server called TINMAN. You can enter ADMINISTER commands at the prompt.

You can also execute ADMINISTER commands on the DCL command line in the following way:

```
$ ADMINISTER SET PASSWORD SCARECROW "YellowRoad" "EmeraldCity"
%PWRK-S-PSWCHANGED, password changed for user "SCARECROW" in domain
"LANDOFOZ"

$
```

In this example, the command-line interface executes a single command and returns to the OpenVMS system prompt.

The ADMINISTER command-line interface prompts you for any required information that you did not supply on the command line. For example, you can log on to the network using the LOGON command, as follows. Note that the password is required, so the software prompts you for it. When you type the password, it is not displayed on the screen.

```
$ ADMINISTER
LANDOFOZ\\TINMAN> LOGON ADMINISTRATOR
Password:
The server \\TINMAN successfully logged you on as Administrator.
Your privilege level on domain LANDOFOZ is ADMIN.
The last time you logged on was 06/19/01 06:41 PM.

LANDOFOZ\\TINMAN>
```

### 1.6.1 Getting Help with ADMINISTER Commands

The Advanced Server ADMINISTER command-line interface has online help that describes command syntax, options, and qualifiers. It also explains each command and gives examples of command use. The Help facility for the ADMINISTER command-line interface has the same structure as OpenVMS DCL help.

To use online help, enter one of the following commands at the DCL prompt ($):

| Syntax | Information Provided |
|---|---|
| ADMINISTER HELP | A list of help topics |
| ADMINISTER HELP *command* | The description, syntax, qualifiers, and examples for the specified ADMINISTER command |
| ADMINISTER *domain*\ \ *server*> HELP | A list of help topics |

For complete information about ADMINISTER commands and their syntax, refer to the *Compaq Advanced Server for OpenVMS Commands Reference Manual* or to the ADMINISTER command-line interface help.

### 1.6.2 Administering Domains and Servers

There are two types of Advanced Server ADMINISTER commands:

- Commands that operate on a domain

  These commands allow you to administer users, groups, or account policies, audit policies, and trust relationships, and to add, delete, or display computers. All such ADMINISTER commands can include the /DOMAIN qualifier to specify a domain other than the one currently being administered. If you specify the /DOMAIN qualifier, you cannot use the /SERVER qualifier with these commands; the commands are executed on the primary domain controller of the specified domain.

A member server does not store or maintain the domainwide security accounts database; only domain controllers do. When you administer the member server's local security accounts database, certain ADMINISTER commands are disallowed or restricted. For information about managing a member server's local database, see Section 2.1.5, Member Servers and Domain Management.

- Commands that operate on a specific server

  These commands allow you to administer shared resources, services, and server operation; they operate directly on either the default server or on the server you specify using the /SERVER qualifier. You cannot use the /DOMAIN qualifier with server-specific commands.

By default, you are set up to administer the local server and the domain to which it belongs. The default domain remains in effect for the duration of the current OpenVMS login session, or until you log off the domain or change the default domain. Commands are executed on the domain and server indicated by the ADMINISTER command-line interface prompt. For example, the following prompt indicates that the domain currently being administered is LANDOFOZ, and the server is TINMAN:

```
LANDOFOZ\\TINMAN>
```

For administering other (remote) domains and servers with the ADMINISTER command-line interface, you have these options:

- SET ADMINISTRATION command — You specify the domain or server, or both, and all subsequent commands affect the specified domain or server.
- TELL command — You specify the server and a single command that is directed to that server. For example, you can use the TELL command to direct commands to a down-level server (a server such as the PATHWORKS LAN Manager server, which runs an earlier network operating system than that of the Advanced Server).
- LOGON command — You specify the domain, and all subsequent commands affect the specified domain. The server name is set to the local server if the local server is a member of that domain. It is set to the name of the primary domain controller of the specified domain if the local server is not a member of the specified domain.
- /SERVER or /DOMAIN qualifier — Commands that support these qualifier allow you to specify the server or domain to be affected by the specified command.

## 1.6 The Advanced Server ADMINISTER Command-Line Interface

You can use the SET ADMINISTRATION command to administer resources, services, and server operation in another domain or server, if you have been validated for a user account that is a member of the Administrators group. For more information, see Section 2.1.4, Administering Another Domain.

If you have OpenVMS system management privileges SYSLCK and OPER on the system, you can execute any server-related ADMINISTER commands on the local server without logging on to the network, except commands that require operations with other servers. If your local server is a primary domain controller, you can also execute any domain-related commands that do not require operations with other servers. When you have these OpenVMS privileges, you are treated as if you had logged on to the network as Administrator. If you do not have these OpenVMS privileges, or if you wish to manage a server other than your local server, you must log on to a network user account that is a member of the Administrators local group (for example, the Administrator user account).

To log on to the network, use the LOGON command. For example:

```
LANDOFOZ\\TINMAN> LOGON
Username: ADMINISTRATOR
Password:
The server \\TINMAN successfully logged you on as Administrator.
Your privilege level on domain LANDOFOZ is ADMIN.
The last time you logged on was 06/19/01 06:41 PM.

LANDOFOZ\\TINMAN>
```

You are prompted for your user name and password. The password is not displayed as you enter it. Once you log on to the domain, you remain logged on after you exit from the ADMINISTER command interface. To log off the domain, use the LOGOFF command before exiting.

You can administer another server using the TELL command. TELL sends the command to be executed to the specified server. In the following example, the server currently being administered is TINMAN, and the other server is WOODMAN. The command to be executed on server WOODMAN is SHOW COMPUTERS.

```
LANDOFOZ\\TINMAN> TELL WOODMAN SHOW COMPUTERS

%PWRK-I-SRVINFO, the server type is: Advanced Server for OpenVMS

Computers in domain "LANDOFOZ":

Computer             Type                       Description
-------------------  -------------------------  -------------------------
[PD] TINMAN          OpenVMS (NT 3.51) Primary  PATHWORKS V6.1 for OpenVMS
                                                (Advanced Server)
```

```
[BD] WOODMAN          OpenVMS (NT 3.51) Backup   PATHWORKS V6.1 for OpenVMS
                                                 (Advanced Server)

  Total of 2 computers

LANDOFOZ\\TINMAN>
```

Be sure to use the proper command syntax for the server you are administering. For example, to administer a server running PATHWORKS V5 for OpenVMS (LAN Manager), use LAN Manager NET commands. In the following example, the PATHWORKS V5 for OpenVMS (LAN Manager) server name is QUEEN.

```
LANDOFOZ\\TINMAN> TELL QUEEN NET SHARE
%PWRK-I-SRVINFO, the server type is: LAN Manager 2.2 for OpenVMS

Sharename       Resource                  Remark
------------------------------------------------------------------------------
ADMIN$                                    Remote Admin
C$              USERS:[PWRK$ROOT]         PATHWORKS share
IPC$                                      Remote IPC
USERS$          _QUEEN$DUA1:              ODS-2 volume USERS:
VAXVMSV0.55$    _QUEEN$DUA2               ODS-2 volume VAXVMSV0.55:
NETLOGON                                  Logon Users Directory
PWUTIL          C:[LANMAN.SHARES.WIN]     Adv. Srv. Client-based Utilities
RONNIE          USERS:[RONNIE]
RPL             C:[LANMAN.RPL]            Remoteboot server share
RPLFILES        C:[LANMAN.RPL.RPLFILES]   Remoteboot server share
USERS                                     Logon Users Directory
The command completed successfully

LANDOFOZ\\TINMAN>
```

## 1.6.3 Administrative Groups

Some of your network users may be designated as members of administrative groups, such as account operators, print operators, server operators, or administrators. These users have administrative or operator privileges that enable them to perform specific tasks, as described in Table 1–2, Administrative Groups.

**Table 1–2 Administrative Groups**

| Group Name | Tasks |
|---|---|
| Account Operators | Create and manage user accounts and global and local groups. |

(continued on next page)

**Table 1–2 (Cont.) Administrative Groups**

| Group Name | Tasks |
|---|---|
| Administrators | Access servers and computers from the network; take ownership of files; manage auditing and security logs; perform all account operator tasks; assign user rights; create groups; keep a local profile; share and stop sharing directories, files, and printers. |
| Print Operators | Keep a local profile; share and stop sharing printers. |
| Server Operators | Access servers and computers from the network; take ownership of files; manage auditing and security logs; share and stop sharing directories, files, and printers. |

If you have different operators responsible for different parts of your network and you do not want to assign them full administrative privileges, make them members of the Server Operators group only at the server they can administer.

## 1.6.4 ADMINISTER Command Output Display Format

To change the way ADMINISTER commands handle C1 character codes (127 through 160 decimal), use the ADMINISTER SET MODE/OUTPUT=[NO]FILTER command. By default (/OUTPUT=FILTER), such characters are converted to spaces before output. To disable conversion of these characters, specify the SET MODE/OUTPUT=NOFILTER command; output on some terminals might be unpredictable.

### 1.6.4.1 How the Default Output Mode Is Determined

Settings made with the SET MODE command are preserved until you log off the system. These settings determine the default mode that takes effect each time you invoke the ADMINISTER command-line interface.

You can set permanent defaults by inserting the appropriate SET MODE command in your login command file. For example, to set output so that the C1 character codes are not converted to spaces, enter the following command in your LOGIN.COM file. The server does not have to be running for this command to execute.

```
$ ADMINISTER SET MODE/OUTPUT=NOFILTER
```

#### 1.6.4.2 Displaying the Current Output Mode

To determine the current mode in effect for ADMINISTER commands, use the ADMINISTER SHOW MODE command. In the following example, the SHOW MODE command indicates that output is filtered.

```
LANDOFOZ\\TINMAN> SHOW MODE

Current mode settings:

Output: FILTER
```

# 2

# Managing Domains and Servers

This chapter describes the way the Advanced Server participates in a domain and provides the concepts and procedures you use to manage servers and domains from Advanced Server.

- Section 2.1, Managing a Domain, describes the way Advanced Server participates in domains and describes the procedures for administering domain operations from an Advanced Server.
- Section 2.2, Managing Security Policies, describes how to manage the account policy and the audit policy.
- Section 2.3, Managing a Server, describes the Advanced Server and how to administer server-specific operations.
- Section 2.4, Advanced Server in OpenVMS Clusters, describes the way an OpenVMS Cluster acts as an Advanced Server.

## 2.1 Managing a Domain

A domain is a set of computers that share a common security accounts database (also referred to as the Security Account Manager [SAM] database) and security policy. The security accounts database contains security information such as user accounts and passwords, and groups, and the settings of the security policies. When you manage a domain and its services, you control its system entities and resources, and you can display information about its resources, such as its computers, connections, users and user sessions, shares, and services.

The Advanced Server may participate in any of the following three kinds of domains:

- Windows NT domains, which consist of primary domain controllers (PDCs), backup domain controllers (BDCs), and member servers; Advanced Servers can participate in any of these three roles. A Windows NT domain must include at least one PDC. The PDC maintains the domainwide security

accounts database. Copies are kept on each BDC. Changes made to the PDC are replicated to the BDCs in the domain.

- Windows 2000 mixed-mode domains, which include both Windows 2000 domain controllers and Windows NT or Compaq Advanced Server domain controllers; Advanced Servers can participate as BDCs and member servers. A Windows 2000 mixed-mode domain must include at least one Windows 2000 domain controller.
- Windows 2000 native-mode domains (also referred to as pure Windows 2000 domains), in which all domain controllers are Windows 2000 systems; Advanced Servers can participate as member servers only. A Windows 2000 native-mode domain must include at least one domain controller.

  The domain controllers participate in a **multimaster domain controller model,** in which changes to the SAM database can be made on any domain controller. Any domain controller can be the replicator, sending copies of the updated SAM database to the other domain controllers.

  This model contrasts with the PDC/BDC model used by Windows NT Servers and Advanced Server servers configured as PDCs and BDCs. In the PDC/BDC model, changes to the SAM database are made on the PDC first, which then propagates the database changes to the BDCs.

Section 2.1.1, Server Roles in the Domain, describes the roles that the Advanced Server can take in a domain.

### 2.1.1 Server Roles in the Domain

The Advanced Server can have one of three roles in a domain:

- Primary domain controller (PDC)

  Each domain running logon validation must have one server that functions as the primary domain controller. This server has the domain's master copy of the security accounts database. The PDC can validate logon requests in the domain. You can change the security accounts database from any computer in the domain, and the change is made to the security accounts database on the PDC.

  When you configure the server software into a new domain, the server establishes the domain's security accounts database (SAM database) and becomes the PDC. The default domain name is LANGROUP. You can specify a name that reflects your company or group.

- Backup domain controller (BDC)

  In addition to the primary domain controller, the domain can have backup domain controllers (BDCs). A BDC keeps a copy of the domain's master security accounts database. The copy of the security accounts database stored on BDCs is synchronized with the PDC's database, as explained in Section 2.1.2.1, Synchronizing SAM Databases on Domain Controllers. Like the PDC, a BDC can validate logon requests. This improves performance and reliability because the load of logon validation can be spread among several servers. Furthermore, logon validation in the domain can continue even if the PDC is unavailable. A BDC can be promoted to PDC.

  When you configure the server software and specify an existing domain name, you can have the server join the existing domain as a BDC. The domain must include one active PDC. Note that as a BDC, the Advanced Server can participate in Windows 2000 mixed-mode domains. To participate in a native-mode Windows 2000 domain, the Advanced Server must be configured as a member server.

- Member server

  A member server is a member of a domain but does not store a copy of the domain's security accounts database and does not validate logon requests. Member servers rely on domain controllers to validate credentials of users requesting access to member server shares. Member servers maintain their own local security accounts database. For more information about managing a member server's local database, see Section 2.1.5, Member Servers and Domain Management.

  Configuring the Advanced Server as a member server allows it to participate in a native-mode Windows 2000 domain without interruption to the Windows 2000 domain. A native-mode Windows 2000 domain must include at least one domain controller. Windows NT member servers can also participate along with Advanced Server member servers in native-mode Windows 2000 environments.

When you configure the Advanced Server for the first time, you select the role your server will perform in the domain. At times, you may need to change the role of your server. The method you use to change the server depends on the current role of the server and the role to which you want to change it. For more information about changing a server's role, see Section 2.1.1.1, Changing a Server's Role in a Domain.

In an OpenVMS Cluster, all nodes on the cluster running the Advanced Server must have the same role.

#### 2.1.1.1 Changing a Server's Role in a Domain

The first server to be configured in a domain is always the primary domain controller (PDC). The PDC role is established during initial installation and configuration of the server. When you install a new server in an existing domain, you can configure it as a backup domain controller (BDC) or member server. You can change the role of the server from a BDC to a PDC, or from a PDC to a BDC. using the ADMINISTER SET COMPUTER/ROLE command. To change the role of a BDC to a member server, or vice versa, you must use the PWRK$CONFIG.COM procedure. To change a PDC to a member server, you must first promote a BDC to a PDC in that domain. The original PDC is automatically demoted to a BDC, and then you can use the PWRK$CONFIG.COM procedure to reconfigure it as a member server. Likewise, to change a member server to a PDC, you must first change the member server to a BDC (using PWRK$CONFIG.COM) and then change the BDC to a PDC.

Table 2–1, Role Changes, lists the role changes you can make and indicates the methods you can use to make the changes (PWRK$CONFIG or the ADMINISTER SET COMPUTER/ROLE command). Section 2.1.1.1.1, Changing a BDC to a PDC, or a PDC to a BDC, explains in detail how to change the role of a BDC to a PCD, or vice versa. Section 2.1.1.1.2, Changing a BDC to a Member Server, or Vice Versa, explains how to change a BDC to a member server, or a member server to a BDC.

**Table 2–1 Role Changes**

| Role Change | Method | Comments |
|---|---|---|
| BDC to PDC | ADMINISTER | Promoting the BDC automatically demotes the current PDC of the domain to a BDC. |
| BDC to member server | PWRK$CONFIG | |
| Member server to PDC | PWRK$CONFIG, then ADMINISTER | First use PWRK$CONFIG to change the member server to a BDC; then use ADMINISTER to promote the BDC to a PDC. |
| Member server to BDC | PWRK$CONFIG | |

(continued on next page)

**Table 2–1 (Cont.) Role Changes**

| Role Change | Method | Comments |
|---|---|---|
| PDC to BDC | ADMINISTER | Use the ADMINISTER command to promote a BDC to PDC; this demotes the PDC to a BDC. |
| PDC to member server | ADMINISTER, then PWRK$CONFIG | First use ADMINISTER to promote a BDC in the domain to a PDC. This demotes the original PDC to a BDC. Then use PWRK$CONFIG to change the BDC to a member server. |

When you change the server role on one node in an OpenVMS Cluster, the role on all cluster members running the Advanced Server is also changed automatically. For information about running the Advanced Server in a cluster environment, see Section 2.4, Advanced Server in OpenVMS Clusters.

**2.1.1.1.1 Changing a BDC to a PDC, or a PDC to a BDC** You change the role of the PDC by promoting a BDC. For example, if the PDC needs to be taken off line for maintenance, you can promote a BDC to PDC. When you promote a BDC, the role of the original PDC is automatically changed to BDC, at which point you can take it off line. In this case, when the original PDC comes back on line, it has the role of BDC. You can then promote it to PDC, if necessary.

If the PDC fails unexpectedly, the domain continues to provide logon validation as long as the NetLogon service is running on a BDC. However, to make changes to the security accounts database, a PDC is required. Therefore, if you think the PDC will be unavailable for more than a short time, you should promote a BDC. When the original PDC comes back on line after an unscheduled interruption, it continues in its role of PDC. If the PDC is restarted and you have promoted a BDC in its absence, the NetLogon service is not started on the server, and the following Alert message is generated and recorded in the system event log:

```
A primary domain controller is running in the domain
```

In this case, you must explicitly change the server's role to BDC using the SET COMPUTER/ROLE command. It may take a few minutes to complete a server role change in a domain.

While server roles are changing, you cannot make changes to the security accounts database; logon validation remains available during the role change if there is another BDC running the NetLogon service. For more information about the NetLogon service, see Section 2.3.4, Managing Services.

To change the server role in a domain from BDC to PDC, or from PDC to BDC, follow these steps:

1. Log on as the domain administrator.
2. Use the SHOW COMPUTERS command to check the server's current role.
3. Use the SET COMPUTER/ROLE command to change a server's role.
4. Use the SHOW COMPUTERS command to verify the new server role.

For example:

```
$ ADMINISTER
LANDOFOZ\\TINMAN> LOGON ADMINISTRATOR
Password:
The server \\TINMAN successfully logged you on as Administrator.
Your privilege level on domain LANDOFOZ is ADMIN.
The last time you logged on was 4/11/01 2:57 PM.

LANDOFOZ\\TINMAN> SHOW COMPUTERS

Computers in domain "LANDOFOZ":
Computer       Type                         Description
------------   ------------------------     ----------------------------
[PD] TINMAN    OpenVMS (NT 3.51) Primary    PATHWORKS V6.1 for OpenVMS
                                            (Advanced Server)
[BD] WOODMAN   OpenVMS (NT 3.51) Backup     PATHWORKS V6.1 for OpenVMS
                                            (Advanced Server)
[SV] LIONHEART OpenVMS (NT 3.51) Server     PATHWORKS V6.1 for OpenVMS
                                            (Advanced Server)
  Total of 3 computers

LANDOFOZ\\TINMAN> SET COMPUTER WOODMAN/ROLE=PRIMARY_DOMAIN_CONTROLLER

Promoting "WOODMAN" to a Primary Domain Controller may take a few minutes.

Do you want to continue with the promotion [YES or NO] (YES) : YES
%PWRK-I-ROLESYNC, synchronizing "WOODMAN" with its primary
%PWRK-I-ROLENLSTOP, stopping the Net Logon service on "WOODMAN"
%PWRK-I-ROLENLSTOP, stopping the Net Logon service on "TINMAN"
%PWRK-I-ROLECHANGE, changing "TINMAN"'s role to Backup Domain Controller
%PWRK-I-ROLECHANGE, changing "WOODMAN"'s role to Primary Domain Controller
%PWRK-I-ROLENLSTART, starting the Net Logon service on "WOODMAN"
%PWRK-I-ROLENLSTART, starting the Net Logon service on "TINMAN"
%PWRK-I-ROLECHANGED, the computers role was successfully changed

LANDOFOZ\\TINMAN> SHOW COMPUTERS

Computers in domain "LANDOFOZ":
```

```
Computer      Type                          Description
------------  ----------------------------  -------------------------
[BD] TINMAN   OpenVMS (NT 3.51) Backup      PATHWORKS V6.1 for OpenVMS
                                            (Advanced Server)
[PD] WOODMAN  OpenVMS (NT 3.51) Primary     PATHWORKS V6.1 for OpenVMS
                                            (Advanced Server)
[SV] LIONHEART OpenVMS (NT 3.51) Server     PATHWORKS V6.1 for OpenVMS
                                            (Advanced Server)

  Total of 3 computers

LANDOFOZ\\TINMAN>
```

Note that a member server (in this example, LIONHEART) is represented with the display symbol [SV], and the server type is Server.

**2.1.1.1.2 Changing a BDC to a Member Server, or Vice Versa** To change the role of a BDC to a member server, you must use the PWRK$CONFIG procedure. You cannot use the SET COMPUTER/ROLE command. The same is true of changing the role of a member server to a BDC. These restrictions are similar to (but less restrictive than) those of Windows NT, which requires the operating system software to be reinstalled to change a domain controller to a member server or vice versa. For a list of advantages gained by configuring your server as a member server, and for details about configuring a server as a member server, refer to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide.*

**Caution**

If you reconfigure a backup domain controller as a member server, PWRK$CONFIG automatically removes the domain controller's domain user account database. If you reconfigure a member server to a BDC, PWRK$CONFIG automatically removes the member server's local user account database. The removed database is stored in the PWRK$LMDOMAINS: and PWRK$LMDATAFILES: directories in case you decide to restore them later. For more information, refer to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide.*

In either case, because of loss of local group information, access to some resources might be affected. If resource permissions were set using local groups, those permissions will have to be reset. If resource permissions were set using global groups or global user accounts, those permissions remain in effect after the role change.

## 2.1.2 Domain Controllers and the SAM Database

The NetLogon service ensures that each BDC's copy of the domainwide security accounts (SAM) database is identical to the master copy kept on the PDC. At regular intervals, any changes made to the master copy of the security accounts database on the PDC are replicated to all BDCs, as described in Section 2.1.2.1, Synchronizing SAM Databases on Domain Controllers. However, the Advanced Server does not replicate user files and directories.
If the PDC fails or is stopped, you cannot make changes that affect the domain's security accounts database, but logon validation continues as long as one or more BDCs are running the NetLogon service. Because PDCs and BDCs keep their own copies of the database, and because the PDC and all BDCs can validate logon requests, there is no single point of failure in the domain. However, if the PDC is unavailable for an extended period, you should promote a BDC to the PDC role so that changes can be made to user accounts.

Each domain in a network is identified internally by a security identifier (SID), a unique number associated with the domain. When a PDC is installed and started, a unique SID is assigned. Therefore, if you have an existing domain, and you want to add a new server to the domain as the PDC, you must install the new server as a BDC first, then change the server's role. For information about changing the server's role, see Section 2.1.1.1, Changing a Server's Role in a Domain.

### 2.1.2.1 Synchronizing SAM Databases on Domain Controllers

Normally, the domain security databases are synchronized automatically at regular intervals: the PDC replicates its databases to the BDCs. In rare cases, you may need to synchronize them manually. For example, you may have just added some new users or groups and you want the BDCs to be able to validate the new user logons now rather than after the next synchronization. To do this, use the SET COMPUTER/ACCOUNT_SYNCHRONIZE command. You can synchronize all BDCs at once, or synchronize an individual BDC with the PDC.

**2.1.2.1.1 How to Synchronize All Controllers in a Domain** To ensure that all BDCs are synchronized with the PDC, enter the SET COMPUTER /ACCOUNT_SYNCHRONIZE command, specifying the PDC on the command line.

For example, if the PDC is called TINMAN, the following command ensures that all BDCs in the domain are synchronized with TINMAN. This command results in each BDC receiving a synchronize status message from the PDC. The information in this message determines whether the BDC's databases are synchronized with the PDC's databases. If the status message indicates to a BDC that the PDC's databases contain changes that are not represented in the

BDC's databases, the BDC will request a partial synchronization. The PDC sends the BDC only those database elements that were changed since the last time the BDC received a status message.

```
LANDOFOZ\\TINMAN> SET COMPUTER TINMAN/ACCOUNT_SYNCHRONIZE

Resynchronizing "LANDOFOZ" domain may take a few minutes.

Do you want to continue with the synchronization [YES or NO] (YES) : YES
%PWRK-S-ACCSYNCHED, account synchronization was successfully initiated
LANDOFOZ\\TINMAN>
```

Although the command has completed successfully, the synchronization process takes a few minutes to complete. You can monitor its progress by reviewing the System event log file using the SHOW EVENTS command. If the BDCs are already uptodate, no event log message is recorded.

**2.1.2.1.2 How to Synchronize a Specific Backup Domain Controller with the Primary Domain Controller** To synchronize a specific backup domain controller (BDC) with the primary domain controller (PDC), enter the SET COMPUTER/ACCOUNT_SYNCHRONIZE command, specifying the BDC name on the command line.

For example, if the BDC is called WOODMAN, the following command synchronizes only the server WOODMAN with the domain's PDC, TINMAN. The BDC requests a full synchronization, meaning that the entire databases are replicated to the BDC.

```
LANDOFOZ\\TINMAN> SET COMPUTER WOODMAN/ACCOUNT_SYNCHRONIZE

Resynchronizing "WOODMAN" with its Primary Domain Controller "TINMAN"
may take a few minutes.
After the synchronization has completed, you should check the Event Logs on
"WOODMAN" and "TINMAN" to determine whether synchronization was
successful.

Do you want to continue with the synchronization [YES or NO] (YES) : YES
%PWRK-S-ACCSYNCHED, account synchronization was successful

LANDOFOZ\\TINMAN>
```

Although the command has completed successfully, the synchronization process takes a few minutes to complete, and it may take longer if the database contains thousands of accounts. You can monitor its progress by reviewing the System event log of the PDC, using the command SHOW EVENTS/SERVER=*pdc_name* (where *pdc_name* is the name of the PDC). (Note that the PDC periodically posts an update to its System event log during a full synchronization; the BDCs post a single update when the synchronization has completed.)

### 2.1.3 Displaying the Current Domain

When you use the ADMINISTER command-line interface, the command prompt provides the name of your domain, along with the name of the server. By default, you are set up to administer the local server and the domain to which it belongs. The default domain remains in effect for the duration of the current OpenVMS login session, or until you log off the domain or change the default domain. (You can change the default server, too.)

To display the current domain and server, use the ADMINISTER command. For example:

```
$ ADMINISTER
LANDOFOZ\\TINMAN>
```

The domain name and server name are in the command prompt. In this example, the domain name is LANDOFOZ and the server name is TINMAN.

Any domain name prefixed with double backslashes indicates that a member server (or workstation) local security accounts database will be the target of ADMINISTER commands. For more information about managing member servers, see Section 2.1.5, Member Servers and Domain Management.

Use the SHOW ADMINISTRATION command to display information about the current domain and your logged-on user account. For example:

```
LANDOFOZ\\TINMAN> SHOW ADMINISTRATION

Administration information:

The domain being administered is: LANDOFOZ
The domain controller for the domain is: TINMAN
The domain controller type is: Advanced Server for OpenVMS

The server being administered is TINMAN
The server type is: Advanced Server for OpenVMS

The user name is: ADMINISTRATOR
The user is logged on to domain LANDOFOZ and has been authenticated.
The user's privilege level on this domain is: ADMIN
The user's workstation is TINMAN and is in domain LANDOFOZ.
LANDOFOZ\\TINMAN>
```

### 2.1.4 Administering Another Domain

You can administer another domain in either of the following ways:

- Use the SET ADMINISTRATION /DOMAIN command. You can perform only administrative functions that do not require you to be logged on to the domain you are administering, such as the SHOW TRUSTS command. For example:

```
LANDOFOZ\\TINMAN> SET ADMINISTRATION/DOMAIN=RUBYPALACE
%PWRK-S-ADMSET, now administering domain "RUBYPALACE", server "QUEEN"
RUBYPALACE\\QUEEN> SHOW TRUSTS

There are currently no domains trusted by domain RUBYPALACE.

Domains permitted to trust domain RUBYPALACE:
    LANDOFOZ
```

  In this example, because a server was not specified with the SET ADMINISTRATION command (that is, using the /SERVER qualifier), and the local server (TINMAN) is not a member of the specified domain (RUBYPLACE), the default server is the primary domain controller of the specified domain. The primary domain controller in domain RUBYPLACE is QUEEN.

- Use the LOGON command to log on to the domain. You must log on to the domain to perform some administrative functions, such as the ADD TRUST command. If you do not supply the password on the LOGON command line, you will be prompted for it. For example:

```
$ ADMINISTER
LANDOFOZ\\TINMAN> LOGON ADMINISTRATOR/DOMAIN=RUBYPALACE
Password:
The server \\QUEEN successfully logged you on as Administrator.
Your privilege level on domain RUBYPALACE is ADMIN.
The last time you logged on was 04/09/01 07:44 AM.
RUBYPALACE\\QUEEN>
```

  To administer LANDOFOZ again, log off the network by using the LOGOFF command. After you log off the server QUEEN, you must log on to the server TINMAN to administer domain LANDOFOZ. For example:

```
RUBYPALACE\\QUEEN>LOGOFF
ADMINISTRATOR was logged off successfully.
LANDOFOZ\\TINMAN>LOGON ADMINISTRATOR
Password:
The server \\TINMAN successfully logged you on as Administrator.
Your privilege level on domain LANDOFOZ is ADMIN.
The last time you logged on was 04/09/01 07:16 AM.
```

For information about the requirements for administrative functions, refer to the *Compaq Advanced Server for OpenVMS Commands Reference Manual*.

Section 2.1.5, Member Servers and Domain Management, explains how to administer a member server's local database.

## 2.1.5 Member Servers and Domain Management

Using ADMINISTER commands on a member server (or directing them to a member server), you can manage the domainwide security accounts database as you would from any domain controller. Although a member server does not store or maintain the domainwide database, it still has access to the benefits of the centralized, domainwide database.

As with Windows NT, in some situations you might want to allow users to manage a server without giving them the ability to manage the entire domain. For this reason, the Advanced Server member server has a local security accounts database. This database initially has the users Administrator and Guest as local to the server.

Both the domain's Administrator and the local Administrator can manage the member server. Certain users can set the default to the member server's local database, as explained in Section 2.1.5.1, Administering the Member Server's Local Database. In any case, certain objects, such as global groups and trusts, are manageable only when logged into a domain controller's domain. Certain ADMINISTER commands will be restricted. Section 2.1.5.2, ADMINISTER Command Variances on Member Servers, lists the ADMINISTER commands that are not allowed or that provide restricted capabilities. The information in both of these sections applies to workstations as well as member servers.

### 2.1.5.1 Administering the Member Server's Local Database

Unless you have changed the default to the member server's local database, ADMINISTER commands normally operate domainwide — that is, on the domain to which the member server belongs. For example, if you enter the ADMINISTER command on member server WIZARD in domain LANDOFOZ, the ADMINISTER prompt displays domain LANDOFOZ and server WIZARD:

```
$ ADMINISTER
LANDOFOZ\\WIZARD>
```

To manage a member server's local database, you must either log on, or change the default domain to the local database. To change the default domain, specify for the domain name the member server's name preceded by two backslashes (\ \). The following example shows how to use the SET ADMINISTRATION command to administer member server WIZARD's local domain database:

```
LANDOFOZ\\TINMAN> SET ADMINISTRATION/DOMAIN=\\WIZARD
%PWRK-S-ADMSET, now administering domain "\\WIZARD", server "WIZARD"
\\WIZARD\\WIZARD>
```

Note that when you administer the member server's local domain database, the ADMINISTER prompt displays the domain name preceded by two backslashes, and the domain name is the same as the name of the member server (in this case, \ \ WIZARD \ \ WIZARD).

In an OpenVMS Cluster in which the Advanced Servers are member servers, you can optionally specify for the domain name the Advanced Server cluster alias name preceded by two backslashes. When administering a clustered member server's local database, the ADMINISTER prompt displays the Advanced Server cluster alias as the domain (preceded by two backslashes). For the server name, unless you specified a server name, the prompt displays the name of the cluster member that responded first to the ADMINISTER interface.

#### 2.1.5.2 ADMINISTER Command Variances on Member Servers

As mentioned previously, member servers do not maintain or manage the domainwide security accounts database and cannot manage or display certain objects, such as global groups, primary groups, and trusts. Table 2–2, Disallowed or Restricted Commands When Administering a Member Server's Local Database, lists the commands that are not allowed or that are restricted, when administering the member server's local domain and database. If you attempt to use these commands in such circumstances, the following error message will be displayed:

```
%PWRK-E-DCONLY, operation is only valid to a Domain Controller
```

The affected commands are categorized by each of the following management objects: COMPUTER, GROUP, TRUST, and USER.

**Table 2–2 Disallowed or Restricted Commands When Administering a Member Server's Local Database**

| Object | Command | Restriction |
|---|---|---|
| COMPUTER | ADD | Not allowed. |
| | REMOVE | Not allowed. |
| | SET | Not allowed with the /ACCOUNT_ SYNCHRONIZE or /ROLE= qualifiers. |
| | SHOW | When you do not specify a computer name with the command, it displays information about the member server only (the computer you are managing) rather than about all the computers in the domain. Note that the display symbol for a member server is [SV]. |
| GROUP | ADD, COPY, MODIFY, REMOVE, SHOW | Do not use with global groups, and do not use the /GLOBAL or /PRIMARY_GROUP qualifier; GROUP commands manage local groups only. |
| TRUST | ADD, REMOVE, SHOW | Not allowed. |
| USER | ADD, COPY, MODIFY | Do not use with the /PRIMARY_GROUP qualifier; the ADD USER command adds the user to the Users local group; these commands manage memberships in local groups only. |
| | REMOVE, SHOW | These commands manage memberships in local groups only; the SHOW USERS command does not display the primary group or memberships in global groups. |

### 2.1.6 Adding a Computer Account to a Domain

For an Advanced Server or a Windows NT computer to become a domain member, it must be added to the domain's security accounts database.

When a computer is configured to join an existing domain (for example, when you install a Windows NT Server or workstation, or when you run the PWRK$CONFIG.COM command procedure on an Advanced Server), the computer account can be added to the domain's security database automatically. This procedure requires that the user name and password of a user account with membership in the Administrators group be supplied.

Alternatively, use the ADD COMPUTER command to add the computer account to the domain's security database. After you add the computer account, the computer joins the domain automatically when it is started. No password is required when a computer joins the domain in this case.

The ADD COMPUTER command is useful only if you do not want to give out the user name and password of an Administrator account in your domain to the administrator of the computer that will join your domain. You can use the ADD COMPUTER command to add the computer account to your domain before the computer's administrator joins the domain. If you supply password information to the administrator of the other computer, the administrator can use the password when joining, and the computer account will be added to the domain automatically. Note that until the intended computer account actually joins the domain, a malicious user could give a different computer that computer name, and then have it join the domain using the computer account you have just created.

If the intended computer does not join the domain immediately, you can remove the computer account from the domain's security database by using the REMOVE COMPUTER command, as described in Section 2.1.7, Removing a Computer Account from a Domain's Security Database.

#### 2.1.6.1 Procedure for Adding a Computer to a Domain

To add a computer to a domain, follow these steps:

1. Identify the name of the domain to which you will add the computer.
2. Obtain or establish the name of the computer you will add; be sure it is unique in the network and no more than 15 characters long.
3. Determine whether the computer you are adding is to be a workstation, server, or backup domain controller.
4. Use the ADD COMPUTER command. Optionally, include the /DESCRIPTION qualifier to provide a description of the computer. If you enter a description that contains nonalphanumeric characters, spaces, or lowercase letters, enclose the description string in quotation marks.

For example, the following command adds the computer GREENGIRL as a Windows NT workstation to the domain LANDOFOZ:

```
LANDOFOZ\\TINMAN> ADD COMPUTER GREENGIRL
%PWRK-S-COMPADD, computer "GREENGIRL" added to domain "LANDOFOZ"
LANDOFOZ\\TINMAN>
```

The computer is added to the domain's security database. The SHOW COMPUTERS command shows GREENGIRL as a Windows NT workstation. For example:

```
LANDOFOZ\\TINMAN> SHOW COMPUTERS
Computers in domain "LANDOFOZ":
Computer        Type                      Description
-----------     --------------------      -------------------------------
[PD] TINMAN     OpenVMS (NT 3.51) Primary  PATHWORKS V6.1 for OpenVMS
                                           (Advanced Server)

[ws] GREENGIRL  Windows NT Workstation
```

Note that when the computer type display symbol is in lowercase, such as [ws] in this example, it indicates that the computer is unavailable to the network. The computer might be unavailable because it has not yet been configured and started.

To determine whether a specific computer is available, use the SHOW COMPUTER command and specify the name of the computer.

## 2.1.7 Removing a Computer Account from a Domain's Security Database

When you remove a computer account from the domain's security database, the computer can no longer participate in domain security. It might be useful to remove a computer account from the domain's security database if the computer did not join the domain after its account was added to the domain's security database. You cannot remove a primary domain controller.

### 2.1.7.1 Procedure for Removing a Computer from a Domain

To remove a computer from a domain, follow these steps:

1. Identify the name of the computer you will remove.
2. Enter the REMOVE COMPUTER command. When you use this command, you receive a prompt to confirm the requested action.

For example, the following command removes the computer GREENGIRL from the domain LANDOFOZ:

```
LANDOFOZ\\TINMAN> REMOVE COMPUTER GREENGIRL
Removing computer "GREENGIRL" from domain "LANDOFOZ" will render it
incapable of authenticating domain logons until it is added to another
domain.
Do you want to continue with the removal [YES or NO] (YES) : YES
%PWRK-S-COMPREM, computer "GREENGIRL" removed from domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

## 2.1.8 Managing Trust Relationships

A trust relationship is a link between two domains, in which one domain honors the users of another domain, trusting the other domain to authenticate the logons of its users. When trust relationships are properly established among domains and resource permissions are set properly, a user with an account in one domain is allowed to access resources on another domain. The domain that has the user accounts is the trusted domain; the domain with the required resources is the trusting domain.

The administrators of both domains must supply the same password when establishing the trust relationship. After the trust relationship is established, the password is changed periodically by the domain software.

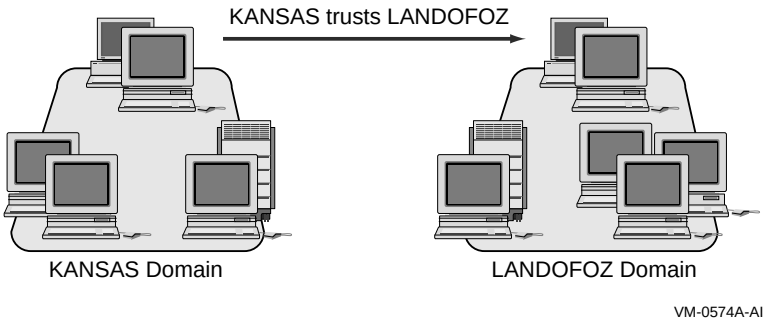
### 2.1.8.1 Establishing Trust Relationships

Both domains participating in a trust relationship must take an action to establish the trust. First, the domain that will be trusted (that is, the domain in which the user accounts are defined) must indicate that it is willing to be trusted by permitting the other domain to trust it. Then the domain that will be trusting (that is, the domain in which the shared resources are defined) can indicate that it is willing to trust the other domain.

### 2.1.8.2 Setting Up a One-Way Trust Relationship

As an example, domain KANSAS has resources required by users who have user accounts in domain LANDOFOZ. You need to set up a trust relationship so that KANSAS trusts LANDOFOZ, as shown in Figure 2–1, One-Way Trust Relationship: KANSAS Domain Trusting LANDOFOZ Domain. This is called a **one-way trust relationship**.

**Figure 2–1 One-Way Trust Relationship: KANSAS Domain Trusting LANDOFOZ Domain**




To set up the one-way trust relationship between domains LANDOFOZ and KANSAS, use the following procedure:

1. When logged on in domain LANDOFOZ, enter the following command:

```
LANDOFOZ\\TINMAN> ADD TRUST KANSAS/PERMITTED
Password:
Password verification:
%PWRK-S-TRUSTADD, trust between domains "LANDOFOZ" and "KANSAS" added

LANDOFOZ\\TINMAN>
```

   This adds domain KANSAS to the list of domains permitted to trust LANDOFOZ.

2. Log on to domain KANSAS, and enter the following command. Use the same password in this command that was used in the previous command.

```
KANSAS\\TOPEKA> ADD TRUST LANDOFOZ/TRUSTED
Password:
Password verification:
%PWRK-S-TRUSTADD, trust between domains "KANSAS" and "LANDOFOZ" added

KANSAS\\TOPEKA>
```

   This command adds domain LANDOFOZ to the list of domains trusted by domain KANSAS.

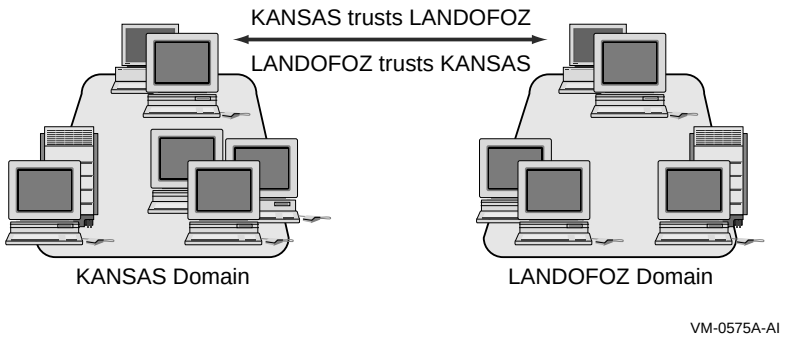
If the steps to establishing a trust are done in the opposite order (that is, one domain trusts the other before the other has permitted the first domain to trust it), the trust will eventually work. However, this can take up to 15 minutes.

### 2.1.8.3 Setting Up a Two-Way Trust Relationship

When a **two-way trust relationship** has been established, each domain trusts the other, and users in both domains can access resources in the other domain, assuming resource permissions have been set up properly.

To set up a two-way trust relationship between domains LANDOFOZ and KANSAS, as shown in Figure 2–2, Two-Way Trust Relationship Between Domains KANSAS and LANDOFOZ, use the following procedure:

**Figure 2–2 Two-Way Trust Relationship Between Domains KANSAS and LANDOFOZ**




1. When logged on in domain LANDOFOZ, add the domain KANSAS to the list of domains permitted to trust LANDOFOZ, as follows:

   ```
   LANDOFOZ\\TINMAN> ADD TRUST KANSAS/PERMITTED
   ```

2. On domain KANSAS, add the domain LANDOFOZ to the list of domains trusted by KANSAS, as follows:

   ```
   KANSAS\\TOPEKA> ADD TRUST LANDOFOZ/TRUSTED
   ```

3. On domain KANSAS, add LANDOFOZ to the list of domains that are permitted to trust KANSAS, as follows:

   ```
   KANSAS\\TOPEKA> ADD TRUST LANDOFOZ/PERMITTED
   ```

4. On domain LANDOFOZ, add KANSAS to the list of domains that are trusted by LANDOFOZ, as follows:

   ```
   LANDOFOZ\\TINMAN> ADD TRUST KANSAS/TRUSTED
   ```

#### 2.1.8.4 Displaying the Trust Relationships

To display trust relationships, use the SHOW TRUSTS command. In the following example, a trust relationship has been established to enable domain KANSAS to trust domain LANDOFOZ. Use the SHOW TRUSTS command on domain LANDOFOZ to display its trust:

```
LANDOFOZ\\TINMAN> SHOW TRUSTS
There are currently no domains trusted by domain LANDOFOZ
Domains permitted to trust domain LANDOFOZ:
    KANSAS
LANDOFOZ\\TINMAN>
```

Use the SHOW TRUSTS command on domain KANSAS to display its trust:

```
LANDOFOZ\\TINMAN> SHOW TRUSTS/DOMAIN=KANSAS
Domains trusted by KANSAS:
    LANDOFOZ
There are currently no domains permitted to trust domain KANSAS
LANDOFOZ\\TINMAN>
```

#### 2.1.8.5 Removing Trust Relationships

If you no longer want a trust relationship to be in effect, you must remove it. When you remove a trust, the trusting domain must cease to trust the trusted domain, and the trusted domain must cease to permit the trusting domain to trust it.

To remove a trust relationship, use the REMOVE TRUST/TRUSTED command and the REMOVE TRUST/PERMITTED command. For example:

```
LANDOFOZ\\TINMAN> REMOVE TRUST KANSAS/PERMITTED
Removing domain "KANSAS" from the Permitted Domains List will
prevent users in domain "LANDOFOZ" from accessing resources in
domain "KANSAS". If you choose to continue, you must also
administer domain "KANSAS" and remove "LANDOFOZ" from its list of
Trusted Domains.

Do you want to continue with the removal [YES or NO] (YES) : YES
%PWRK-S-TRUSTREM, trust between domains "LANDOFOZ" and "KANSAS"
removed

LANDOFOZ\\TINMAN>
```

To reestablish the trust relationship, you again must supply matching passwords for the trusting and trusted domains. If only one side of the trust relationship is broken and reestablished, the trust will appear to work in some ways and fail in others. For example, you can grant resource access to a user from the trusted domain, but the user is not actually granted the indicated access. To eliminate such problems, remove the old trust relationships and establish new trust relationships.

## 2.2 Managing Security Policies

You can manage the following security policies:

- Account Policy — controls how passwords and logon hours are managed for user accounts.
- Audit Policy — defines which security events are logged by the server in a domain.

### 2.2.1 Managing the Account Policy

You manage the account policy for your domain using the SET ACCOUNT POLICY command. You can view the account policy with the SHOW ACCOUNT POLICY command. Changes to the account policy affect every user at the next logon.

The account policy characteristics that you can specify include:

- Whether a user connection is forcibly disconnected when the logon hours specified for that user account are exceeded — specify the SET ACCOUNT POLICY/FORCE_DISCONNECT command. You specify logon hours for each user account with the ADD USER, COPY USER, or MODIFY USER command, using the /HOURS qualifier, as explained in Section 3.1.7, Specifying Logon Hours.

  If you specify /NOFORCE_DISCONNECT for the account policy, the user is not disconnected when the logon hours are exceeded, but the user cannot make a new connection until the times (days and hours) specified as the logon hours for the account.

- The policy for usage of passwords — use the SET ACCOUNT POLICY/PASSWORD_POLICY=*keyword* command. You can specify the following keywords and values with the /PASSWORD_POLICY qualifier:
  - [NO]MINAGE=*n* — the minimum number of days a user's password must be used before the user can change it.
  - [NO]MAXAGE=*n* — the maximum number of days a user's password can be used before the server requires the user to change it.
  - MINLENGTH=*n* — the minimum length of a password.
  - [NO]HISTORY=*n* — the number of new passwords that must be used before an old password can be reused.

- Whether a user account is locked out after a specified number of failed attempts to logon — use the SET ACCOUNT POLICY/LOCKOUT=*keyword* command. To enable account lockout, you must specify the following three keywords and their values with the /LOCKOUT qualifier:
  - ATTEMPTS=*n*, where *n* specifies the number of failed attempts to allow before locking the user account.
  - DURATION=*n*, where *n* specifies the number of minutes before a locked account is automatically unlocked. The value of this parameter must be greater than, or equal to, the value set for the WINDOW parameter.
  - WINDOW=*n*, where *n* specifies the number of minutes to wait after a user account has been locked out, before resetting the logon count.

  Specify these three parameters with the /LOCKOUT qualifier as shown in the example in Section 2.2.1.1, Example: Setting a User Account Policy.

  By default, user account lockout is disabled, meaning that the user accounts are never locked out, no matter how many failed logon attempts are made on a user account. The /NOLOCKOUT qualifier specifies that user accounts are never locked out.

  To unlock a user account that has been locked, use the MODIFY USER command with the /UNLOCK qualifier.

#### 2.2.1.1 Example: Setting a User Account Policy

The following example shows how to set the account policy for the domain so that users are disconnected when they exceed their logon hours (/FORCE_ DISCONNECT), and they are locked out after three failed logon attemps. The failed logon count resets 20 minutes after the last failed login attempt, and locked-out accounts are unlocked after 25 minutes.

```
LANDOFOZ\\TINMAN> SET ACCOUNT POLICY/FORCE_DISCONNECT -
_LANDOFOZ\\TINMAN> /LOCKOUT=(ATTEMPTS=3,WINDOW=20,DURATION=25)
%PWRK-S-ACCPOLSET, account policy set for domain "LANDOFOZ"
```

#### 2.2.1.2 Example: Displaying the Account Policy for a Domain

The following example shows how to use the SHOW ACCOUNT POLICY command to display the account policy for a domain:

```
LANDOFOZ\\TINMAN> SHOW ACCOUNT POLICY

Account Policy for domain "LANDOFOZ":
```

```
Minimum password age (days) : 1
Maximum password age (days) : 42
Minimum password length : 0
Length of password history maintained : None
Force user logoff after logon hours expire: YES
Lock out account after how many bad password attempts : 3
Number of minutes account remains locked : 20
Number of minutes to wait before resetting lockout count : 25
Role of server TINMAN : Primary Domain Controller
```

### 2.2.2 Managing the Audit Policy

You specify the audit policy using the SET AUDIT POLICY command. When auditing is enabled, the server records selected security-related activities in the Security event log. The server can record systemwide events, such as a user logging on, and file-specific events, such as a user attempting to access a specific file. You display the audit policy using the SHOW AUDIT POLICY command.

The audit policy affects Security event logging for all servers in the domain, because they share the same audit policy. You can specify whether to log failed events and successful events. See Table 2–3 for a list of the events that you can audit. Note that to audit events pertaining to files or directories (ACCESS events), you must also set auditing on the files or directories. For more information, see Section 6.1.3.6, Setting and Displaying Security Event Auditing for Files and Directories.

**Table 2–3 Events You Can Audit**

| Audit Event Name | Events Audited |
|---|---|
| ACCESS | - A user accessing a directory or file that is set for auditing (SET FILE/AUDIT=)<br>- A user sending a print job to a printer that is set for auditing |
| ACCOUNT_MANAGEMENT | - Creating, changing, or deleting a user account or group<br>- Renaming, disabling, or enabling a user account<br>- Setting or changing a password |
| LOGONOFF | - A user logging on or logging off<br>- A user making a network connection |
| POLICY_CHANGE | - Changing the audit policy<br>- Changing a trust relationship<br>- Changing user rights policies |
| PROCESS | - Program activation<br>- Handling duplication<br>- Indirect object access<br>- Process exit |
| SYSTEM | - A user starting or restarting a server<br>- A system security event<br>- An event that affects the security log |
| USER_RIGHTS | - A user exercised a user right such as accessing a file, except for logon/logoff rights |

#### 2.2.2.1 Example: Displaying the Audit Policy for a Domain

The following example shows how to display the audit policy for a domain:

```
LANDOFOZ\\TINMAN> SHOW AUDIT POLICY

Audit Policy for domain "LANDOFOZ":

Auditing is currently Disabled.

Audit Event states:

Audit Event         Success   Failure
------------------- --------  --------
ACCESS              Disabled  Disabled
ACCOUNT_MANAGEMENT  Disabled  Disabled
LOGONOFF            Disabled  Disabled
POLICY_CHANGE       Disabled  Disabled
PROCESS             Disabled  Disabled
SYSTEM              Disabled  Disabled
USER_RIGHTS         Disabled  Disabled

LANDOFOZ\\TINMAN>
```

#### 2.2.2.2 Example: Enabling Auditing and Setting the Audit Policy for a Domain

The following example shows how to enable auditing and set the audit policy for a domain, using the SET AUDIT POLICY/AUDIT command. In this example, the /SUCCESS=LOGONOFF qualifier enables auditing of successful logon and logoff operations.

```
LANDOFOZ\\TINMAN> SET AUDIT POLICY/AUDIT/SUCCESS=LOGONOFF
%PWRK-S-AUDPOLSET, audit policy set for domain "LANDOFOZ"
LANDOFOZ\\TINMAN> SHOW AUDIT POLICY

Audit Policy for domain "LANDOFOZ":

Auditing is currently Enabled.

Audit Event states:

Audit Event         Success   Failure
------------------  --------  --------
ACCESS              Disabled  Disabled
ACCOUNT_MANAGEMENT  Disabled  Disabled
LOGONOFF            Enabled   Disabled
POLICY_CHANGE       Disabled  Disabled
PROCESS             Disabled  Disabled
SYSTEM              Disabled  Disabled
USER_RIGHTS         Disabled  Disabled

LANDOFOZ\\TINMAN>
```

To enable auditing of all events, use the following command:

SET AUDIT POLICY/AUDIT/SUCCESS=ALL/FAILURE=ALL

## 2.3 Managing a Server

When you manage a server, you can display server information, send messages to users, and start and stop services.

### 2.3.1 Displaying Server Information

You can display information about the server including connections, user sessions, shared resources, and the software version number.

#### 2.3.1.1 Displaying Connections

As you manage your server, you may need to know which connections are active. A connection is a virtual link between a workstation or a server process and a shared resource on a server.

To display existing connections, use the SHOW CONNECTIONS command. The SHOW CONNECTIONS command displays information about active connections to the server, including connections from the Advanced Server. The information about each connection includes:

- Connected user's name
- User's computer name (including connections from the Advanced Server)
- Name of the shared resource connected to
- Number of opens to each share
- Total connect time to the share (in days, hours, minutes)

The following example displays information about all the connections to the server currently being administered (TINMAN).

```
LANDOFOZ\\TINMAN> SHOW CONNECTIONS

 Connections on server "TINMAN":

 User name             Computer name    Share name  Opens  Time
 --------------------  ---------------  -----------------  --------
 ADMINISTRATOR         TINMAN_176       IPC$            3   0 11:30
 SCARECROW             TINMAN_149       ADMIN$          0   0 00:00
 SCARECROW             TINMAN_149       IPC$            0   0 00:00
 SCARECROW             TINMAN_149       IPC$            1   0 00:00
 SCARECROW             TINMAN_149       RAINBOW         0   0 06:14

   Total of 5 connections
```

#### 2.3.1.2 Displaying User Sessions

As you manage your server, you may need to know which sessions are active. A session is a link between a workstation and a server. Multiple share connections can be established over a single session.

To display user sessions, use the SHOW SESSIONS command. You can include the /SERVER qualifier to display sessions on a specific server. The display includes:

- Name of the user that established the session
- Name of the computer that established the session
- Number of resources opened on the server by user
- Elapsed time since the session was established
- Elapsed time since the user last initiated an action
- Whether a session is using Guest access

For example:

```
LANDOFOZ\\TINMAN> SHOW SESSIONS/SERVER=WOODMAN

User sessions on server "WOODMAN":

Connected Users     Computer      Opens   Time       Idle       Guest
------------------  ---------     -----   -------    -------    -----
ADMINISTRATOR       TINMAN            1   1 22:54    0 00:00    No
SCARECROW           DOROTHY           3   0 03:48    0 00:03    No

  Total of 2 connected users

LANDOFOZ\\TINMAN>
```

#### 2.3.1.3 Displaying Shared Resources

The Advanced Server allows you to display information about shared resources. You can display information about the share permissions and the OpenVMS protections on them, as well as the maximum number of connections to the share allowed at one time. You can specify the display of only the active shares (those currently connected to) or by the type of share (printers or directories).

To see shared resources from the current server, use the SHOW SHARES command. This command displays:

- Name of the share
- Share type (Directory or Print)
- Share description

Specify the share name to display information about only one share. Use the /FULL qualifier to display detailed information about each share.

For example, the following command displays the shares on the server currently being administered (TINMAN):

```
LANDOFOZ\\TINMAN> SHOW SHARES

Shared resources on Server "TINMAN":

Name              Type         Description
---------       ---------      --------------------------------
NETLOGON        Directory      Logon Scripts Directory
RAINBOW         Directory      Local Oz Share
PWLIC           Directory      PATHWORKS Client License Sftwr
PWLICENSE       Directory      PATHWORKS Client License Sftwr
PWUTIL          Directory      Adv. Srv. Client-based Utilities
USERS           Directory      Users Directory

   Total of 6 shares

LANDOFOZ\\TINMAN>
```

To display hidden shares (shares whose name ends in a dollar sign ($), such as administrative resources and local device shares (such as C$)), you must include the /HIDDEN qualifier or specify the share name. For example, the following command displays the local device share C$:

```
LANDOFOZ\\TINMAN> SHOW SHARES C$

Shared resources on Server "TINMAN":

Name          Type       Description
------------  ---------  ----------------------------------------
C$            Directory  PATHWORKS share

  Total of 1 share
```

#### 2.3.1.4 Displaying the Advanced Server Version Number

You can verify the version number of Advanced Server software. To display the version number of server software on your system, use the SHOW VERSION command. For example:

```
LANDOFOZ\TINMAN> SHOW VERSION

PATHWORKS V6.1 for OpenVMS (Advanced Server)

LANDOFOZ\\TINMAN>
```

This command is valid for PATHWORKS for OpenVMS (Advanced Server) and Advanced Server for OpenVMS servers only.

### 2.3.2 Stopping the Advanced Server

You can stop the Advanced Server at any time for any reason, which can include the following:

- When you want to change server configuration parameters
- As part of an orderly system shutdown

To stop the Advanced Server, enter the following command:

```
$ @SYS$STARTUP:PWRK$SHUTDOWN
Shutting down the currently running server(s)...
```

For a cluster server, enter:

```
$ @SYS$STARTUP:PWRK$SHUTDOWN CLUSTER
```

To stop the Advanced Server as part of an orderly system shutdown, add the shutdown command to the site-specific system shutdown procedure. In addition, prior to shutting down the server, announce the planned shutdown to connected users by using the ADMINISTER SEND/USERS command, as described in Section 2.3.3, Sending Messages to Users.

## 2.3.3 Sending Messages to Users

You should send messages to users before you change the operating characteristics of a server. For example, you might send a message before disconnecting users or if you need to stop sharing a resource on a computer. For a message to be sent and received, the Alerter service must be running on the computer sending the message, and the Messenger service must be running on the computer receiving the message.

**Note**

The Messenger service is not supported on the Advanced Server. Therefore, OpenVMS users on Advanced Servers will not receive messages sent this way.

### 2.3.3.1 Sending a Message to the User of a Specific Computer

To send a message to the user of a specific computer, follow these steps:

1. Identify the computer to which you will send your message.
2. Enter the ADMINISTER SEND command, including the computer name and the message. Enclose the message in quotation marks.

For example, the following command sends the message "Shutdown at 1 pm today!!!" to the computer called WORTHY.

```
LANDOFOZ\\TINMAN> SEND WORTHY "Shutdown at 1pm today!!!"
LANDOFOZ\\TINMAN>
```

The message is displayed in a Messenger Service pop-up window on computer WORTHY in the following form:

```
Message from TINMAN to WORTHY on 4/30/01 11:20 AM
"Shutdown at 1pm today!!!"
```

With the /SERVER=servername qualifier, you can send a message from another specified server in your domain to a specific group of users in your domain. With the /USER qualifier, you can send a message to all or specific users on a server.

#### 2.3.3.2 Sending a Message to Users on a Specific Server

To send a message to users connected to a specific server, use the /SERVER qualifier. For example, the following command sends the message "Shutdown at 1pm today!!!" to all users connected to server WOODMAN.

```
LANDOFOZ\\TINMAN> SEND/USERS/SERVER=WOODMAN "Shutdown at 1pm today!!!"
LANDOFOZ\\TINMAN>
```

This command may take a few minutes to complete.

## 2.3.4 Managing Services

To manage Advanced Server services, you need to know how to start and stop services and how to configure service startup. Services are set up during server installation and configuration.

You can start and stop some of the services available on the computer and determine whether a service will start up automatically when the system starts. You must be logged on to a user account that has membership in the Administrators group or the Server Operators group to perform these operations. Table 2–4, Network Services on the Advanced Server, shows the default services provided with Advanced Server.

**Table 2–4 Network Services on the Advanced Server**

| Service | Description | Supported on Advanced Servers | Starts by Default | Can Be Paused | Can Be Stopped |
|---|---|---|---|---|---|
| Alerter | Notifies selected users and computers of administrative alerts that occur on this server. Used by the server and other services. | Yes | Yes | No | Yes |
| Browser | Lists network entities, such as domains, computers, and shared resources. | Yes | Yes | No | Yes |
| EventLog | Records system, security, and application events in the event logs, and enables remote access to those logs. Cannot be stopped separately; stops together with the Server service. | Yes | Yes | No | No |

(continued on next page)

**Table 2–4 (Cont.) Network Services on the Advanced Server**

| Service | Description | Supported on Advanced Servers | Starts by Default | Can Be Paused | Can Be Stopped |
|---|---|---|---|---|---|
| NetLogon | Verifies the user name and password of each user who attempts to log on to the network or gain access to the server. Synchronizes security databases. | Yes | Yes | Yes | Yes |
| Server | Provides file and print sharing. | Yes | Yes | Yes | No[1] |
| TimeSource | Identifies a server as the time server for a domain. Other computers synchronize their clocks with the time server. | Yes | No | No | Yes |
| Replicator | Replicates user directories and files. | No | No | No | No |
| Messenger | Allows receipt of server management messages | No | No | No | No |

[1]Only by using the PWRK$SHUTDOWN command procedure.

The Replicator and Messenger services are supported on Windows NT and can be stopped and started, but not paused, from the Advanced Server.

The Alerter, NetLogon, and TimeSource services can be enabled and disabled by adding them to the list of services associated with the **SrvServices** server configuration parameter stored in the LANMAN.INI file, as described in Section 7.3, Using the LANMAN.INI File. When a service is enabled, it is started automatically when the Advanced Server starts.

**Note**

For smooth operation of the domain, Compaq recommends that the NetLogon service always be enabled, even on member servers.

#### 2.3.4.1 Displaying Services

As you manage your server, you may need to know the state of network services.

To display available services, use the SHOW SERVICES command. For example:

```
LANDOFOZ\\TINMAN> SHOW SERVICES

Services on server "TINMAN":

Service           Current State
--------------    ---------------
ALERTER           Started
BROWSER           Started
EVENTLOG          Started
NETLOGON          Started
SERVER            Started
TIMESOURCE        Started

   Total of 6 services

LANDOFOZ\\TINMAN>
```

#### 2.3.4.2 Starting Services

By default, the Server, Alerter, Browser, and NetLogon services are started automatically when the server is started.

To start a service, use the START SERVICE command, specifying the full service name. For example:

```
LANDOFOZ\\TINMAN> START SERVICE TIMESOURCE
%PWRK-S-SVCSTART, service "TIMESOURCE" started on server "TINMAN"

LANDOFOZ\\TINMAN>
```

#### 2.3.4.3 Pausing Services

You can suspend execution of the Server and NetLogon services. Unlike stopping a service, pausing does not cancel resource sharing, terminate connections or change any settings associated with the service.

Pausing the Server service prevents users from making new connections to the server's shared resources; however, users who have already connected to shared resources can continue to use the resources. Pausing the Server service does not prevent users who are members of the Administrators group from connecting to the service.

Pausing the NetLogon service prevents the server from synchronizing the domain's security accounts database. The server will not validate logons.

To pause a service, use the PAUSE SERVICE command. For example:

```
LANDOFOZ\\TINMAN> PAUSE SERVICE SERVER
Do you really want to pause service "SERVER" [YES or NO](YES): YES
%PWRK-S-SVCPAUSE, service "SERVER" paused on server "TINMAN"

LANDOFOZ\\TINMAN>
```

#### 2.3.4.4 Continuing Services

You can use the CONTINUE SERVICE command to continue a paused service. When you continue a service, you restore access to the service.

To continue a service, use the CONTINUE SERVICE command. For example:

```
LANDOFOZ\\TINMAN> CONTINUE SERVICE SERVER
%PWRK-S-SVCCONT, service "SERVER" continued on server "TINMAN"

LANDOFOZ\\TINMAN>
```

#### 2.3.4.5 Stopping Services

Stopping a service disables all operations provided by that service. You can use ADMINISTER commands to stop the following services:

- Alerter
- Browser
- NetLogon
- TimeSource

To stop the Server service, use the PWRK$SHUTDOWN.COM command procedure, as described in Section 2.3.2, Stopping the Advanced Server. Before you stop the Server service, you should follow these steps:

1. Pause the service.
2. Send a message to users connected to the server's shared resources, warning them that Advanced Server will be shut down. Your message should ask all users to stop their current activities and close all files. Give users adequate time to close their files before you proceed. If you shut down the server while users are accessing shared resources, they may lose data.

To stop a service, use the STOP SERVICE command. For example:

```
LANDOFOZ\\TINMAN> STOP SERVICE TIMESOURCE
Do you really want to stop service "TIMESOURCE" [YES or NO] (YES): YES
%PWRK-S-SVCSTOP, service "TIMESOURCE" stopped on server "TINMAN"

LANDOFOZ\\TINMAN>
```

#### 2.3.4.6 Synchronizing Clocks on All Network Computers

You can designate an Advanced Server as the network time server in a domain by having it run the TimeSource service. Client computers on the network can synchronize their time with the time server, which makes it possible to synchronize network events. For Compaq OpenVMS servers, the operating system maintains the clock, which cannot be set with Advanced Server commands. (For information about changing the time or time zone for a system, see Section 2.3.5, Changing Time Zones or Daylight Saving Time Settings.

To run the TimeSource service automatically, do one of the following:

- Edit the LANMAN.INI file to include TIMESOURCE in the SERVER section as a value for the SRVSERVICES keyword. For example, the LANMAN.INI file could contain an entry of the following form:

  ```
  [SERVER]
        .
        .
        .
  SRVSERVICES=ALERTER,NETLOGON,TIMESOURCE
  ```

  With this entry in place, the TimeSource service starts automatically whenever you start the server. To activate the TimeSource service after the server is running, you can use the START SERVICE TIMESOURCE command.

- Run the configuration procedure PWRK$CONFIG.COM, and answer YES to the option "Enable Timesource service."

Then the TimeSource service will start automatically whenever you start the server.

To activate the TimeSource service after the server is running, use the START SERVICE TIMESOURCE command.

### 2.3.5 Changing Time Zones or Daylight Saving Time Settings

To properly represent the time in your local environment, you must set up the OpenVMS time zone information before the server is started, as explained in the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide.* If your server is moved to a location in a different time zone, you must set the new time zone information accordingly. If your server system resides in an area that observes daylight saving time, the time zone information must be modified appropriately when daylight saving starts and ends.

### 2.3.6 Setting Up the Time Zone Information on OpenVMS Version 6.2

For OpenVMS Version 6.2, you can set up the time zone as an optional feature using SYS$MANAGER:UTC$CONFIGURE_TDF.COM, as explained in the *OpenVMS System Manager's Manual*. However, PATHWORKS Advanced Servers running on OpenVMS Version 6.2 do not use the values defined by UTC$CONFIGURE_TDF.COM. Instead, you must define the logicals PWRK$$TDF and PWRK$$DST before starting the server.

PWRK$$TDF defines the time differential factor (TDF). The default is -5, which works for Eastern Standard Time. The value for PWRK$$TDF must be a whole number in the range -13 to 13 hours. Seconds are not significant.

PWRK$$DST sets daylight saving time status. The default is 1, signifying that daylight saving time currently applies. Set a value of 0 when daylight saving time does not currently apply. In regions where daylight saving time is not observed, this setting can be set permanently to 0. If daylight saving time is observed in your system's time zone, you must change this logical twice a year, accordingly, and restart the server. For systems located in time zones that observe daylight saving time, the SYS$EXAMPLES:DAYLIGHT_SAVINGS.COM file can be used to adjust the system time and TDF automatically twice a year.

You define these logicals in either SYS$MANAGER:SYSTARTUP_VMS.COM or SYS$MANAGER:SYLOGICALS.COM, using the DEFINE/SYSTEM command. The following example shows the definitions for the PWRK$$TDF and PWRK$$DST logicals on a system located in San Diego, California. The TDF for this part of the United States is -8. The PWRK$$DST definition indicates that daylight saving time is currently in effect.

```
$ DEFINE/SYSTEM PWRK$$TDF -8
$ DEFINE/SYSTEM PWRK$$DST 1
```

In those states of the United States that observe daylight saving time, daylight saving time applies from the first Sunday in April to the last Sunday in October. Thus, on the last Sunday in October, the PWRK$$DST logical for the PATHWORKS Advanced Server system in San Diego must be changed to 0 (and the server restarted).

### 2.3.7 Setting Up the Time Zone Information on OpenVMS Version 7.*x* Systems

Advanced Servers running on OpenVMS Version 7.*x* systems implement default date/time support using the UTC standard.

You can use the OpenVMS SYS$EXAMPLES:DAYLIGHT_SAVINGS.COM procedure to adjust the system time and TDF automatically twice a year. You check and set the time zone and time differential factor (TDF) settings on your system by running the OpenVMS command procedure UTC$TIME_SETUP.COM. (This command procedure defines the logicals needed by the Advanced Server. You do not define logicals manually for time services support, as you must on PATHWORKS Advanced Servers running on OpenVMS Version 6.2.) From the SYSTEM account, enter the following command to begin the procedure:

```
$ @SYS$MANAGER:UTC$TIME_SETUP.COM
```

When you elect to change the time zone or TDF setting, or both, the changes are also made clusterwide if your server participates in an OpenVMS Cluster.

If you change any time zone information, you must restart the server for the time to be properly represented.

For more information about running the command procedure and resetting the time zone and TDF, refer to the *OpenVMS System Manager's Manual*.

## 2.4 Advanced Server in OpenVMS Clusters

Some servers in your network may be configured in an OpenVMS Cluster environment. Advanced Servers running in an OpenVMS Cluster share the same copy of the user accounts and shares databases and assume a single role, either a primary domain controller, a backup domain controller, or a member server. They operate as a single entity identified by the Advanced Server cluster alias name.

When you change the server role on one member of an OpenVMS Cluster, the role on all cluster members running the Advanced Server is also changed accordingly.

Use the SHOW COMPUTERS command to display a list of all the nodes in the cluster with the server role. Because of the way a Windows NT Server detects the cluster, the information displayed by the Windows NT Server Manager may not reflect the cluster role information accurately when the cluster is a primary domain controller.

The following sections discuss the Advanced Server cluster alias and cluster load balancing in LANs and WANs:

- Section 2.4.1, About the Advanced Server Cluster Alias, describes the Advanced Server cluster alias.
- Section 2.4.2, Defining the Advanced Server Cluster Alias, explains how to define the Advanced Server cluster alias.
- Section 2.4.3, Cluster Load Balancing in LANs, describes how the Advanced Server cluster alias provides cluster load balancing for clients that are on the same LAN as the server.
- Section 2.4.4, Dynamic Cluster Load Balancing in WANs, describes how the Advanced Server cluster alias provides cluster load balancing for clients that are not on the same LAN as the server.

### 2.4.1 About the Advanced Server Cluster Alias

In an OpenVMS Cluster, an Advanced Server cluster alias name allows all the members of the OpenVMS Cluster that are running the Advanced Server to be addressable as a single entity.

Unlike the DECnet and TCP/IP cluster aliases, the Advanced Server cluster alias is transport independent. (The TCP/IP cluster alias is also referred to as the TCP/IP cluster impersonator name.)

Clients can access resources on the OpenVMS Cluster by connecting to the cluster using the Advanced Server cluster alias or the name of a specific Advanced Server cluster member. Make sure a static entry for the Advanced Server cluster alias is defined in each client's LMHOSTS file, or a static multihomed entry is defined in the WINS (Windows Internet Name Service) database; however, if load balancing and failover are desired for LAN or WAN environments, remove any static entries for the cluster alias from the LMHOSTS file, the local hosts file, and the WINS database to ensure that the cluster alias is resolved appropriately. *Failover* occurs when the node to which the client is connected becomes unavailable; the client is reconnected (using the Advanced Server alias) to the cluster member that is least loaded. For more information about load balancing, see Section 2.4.3, Cluster Load Balancing in LANs, and Section 2.4.4, Dynamic Cluster Load Balancing in WANs.

**Note**

If LMHOSTS is the only method you are using for resolving NetBIOS names, other domain controllers (including the PDC) that are not in the same subnet as the Advanced Server cluster must add an entry for the Advanced Server cluster alias to their LMHOSTS file. The LMHOSTS

file does not offer any means for mapping multiple IP addresses to a single NetBIOS name. Therefore, the entry for the Advanced Server cluster alias must be mapped to the IP address of one specific server cluster member. If the Advanced Server is stopped on that cluster member, you must modify the LMHOSTS file on all clients and servers to map the cluster alias name to the IP address of a cluster member on which the Advanced Server is still running. On systems running a Microsoft Windows operating system, the NetBIOS name cache must also be reloaded using the command NBTSTAT -R (capital R required).

Due to the LMHOSTS limitations noted above, it is difficult (and perhaps unmanageable) to gain the benefits of load balancing and failover using an LMHOSTS file.

---

### 2.4.2 Defining the Advanced Server Cluster Alias

You define the Advanced Server cluster alias name when you run the PWRK$CONFIG configuration procedure. The Advanced Server cluster alias name is a NetBIOS name that is unique among domain names and server names. OpenVMS Clusters running DECnet may have a DECnet cluster alias name defined as well. The DECnet cluster alias name is used by the DECnet transport only. OpenVMS Clusters running TCP/IP may have a cluster alias defined for the purpose of providing failover for Network File System (NFS) clients. The Advanced Server cluster alias can be the same as the TCP/IP cluster alias and/or the DECnet cluster alias; however, Compaq strongly recommends that the Advanced Server cluster alias not be the same as the TCP/IP cluster alias.

**Note**

Do not use the name of the domain as the Advanced Server cluster alias; if they are the same, the NetLogon service will fail to start.

---

During the initial configuration process (when you run PWRK$CONFIG.COM), you can accept the default Advanced Server cluster alias name (*nodename*_ALIAS), or you can specify a different name. For more information about the PWRK$CONFIG.COM command procedure and configuring the Advanced Server alias, refer to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide*.

When an Advanced Server running on an OpenVMS Cluster joins a domain, a computer account by the name of the cluster alias is created in the domain security database; a separate account is not created for each cluster member running the Advanced Server.

Clients using the Advanced Server cluster alias to obtain Advanced Server services can gain the benefit of load balancing, in which the alias is resolved to the Advanced Server cluster member that has the least load. For more information about cluster load balancing, see Section 2.4.3, Cluster Load Balancing in LANs, and Section 2.4.4, Dynamic Cluster Load Balancing in WANs.

Note that when a client connects to a server using the Advanced Server cluster alias, the connection is associated with the network address of the cluster member to which the client is actually connected. Additional connections made from the same client to the Advanced Server alias are made directly to the same cluster member. Once a client is connected, no further load balancing for that client is done. When the node to which the client is connected becomes unavailable, failover is possible: the client is reconnected (using the Advanced Server alias) to the cluster member that is least loaded.

**Note**

To perform administrative functions on a particular cluster member, you must connect to that member by using its specific node name, rather than the cluster alias.

The Advanced Server cluster alias is stored in the LANMAN.INI file as keyword **pwrkalias** in the VMSSERVER section. For more information, see Section 7.3, Using the LANMAN.INI File.

### 2.4.3 Cluster Load Balancing in LANs

The Advanced Server cluster alias makes load balancing possible for clients that are on the same LAN as the server. To gain the benefits of load balancing and failover, clients must connect to the Advanced Server on the OpenVMS Cluster by using the Advanced Server cluster alias. The clients use the NetBIOS broadcast facility to request resolution of the Advanced Server cluster alias. Only one Advanced Server node in the cluster is designated to respond to the request: the Advanced Server node that is the least loaded of the servers in the cluster. The relative loads of the servers in the cluster are checked periodically, and so the node designated to respond will change from time to time.

Cluster load balancing is not available if clients using Windows Internet Name Service (WINS) to resolve the Advanced Server cluster alias have a static entry for this alias in the WINS database.

### 2.4.4 Dynamic Cluster Load Balancing in WANs

Dynamic cluster load balancing is available for service requests from WAN clients that are outside the server cluster's LAN. Dynamic cluster load balancing for WAN environments is provided by Compaq TCP/IP Services for OpenVMS Version 5.0A or later, and uses a Domain Name System (DNS) server to resolve the Advanced Server cluster alias name, instead of WINS or LMHOSTS.

**Note**

You can set up dynamic cluster load balancing using TCP/IP Services for OpenVMS Version 4.2 (supported on OpenVMS Version 6.2 systems); however, Compaq recommends using TCP/IP Services for OpenVMS, Version 5.0A or later, which means you would need to upgrade any OpenVMS Version 6.2 systems.

The Advanced Server cluster alias name should be registered as a cluster name (that is, as having multiple A resource records for a single host name) at the authoritative DNS server for the TCP/IP domain to which the cluster belongs. This DNS name server must support dynamic updates (Berkeley Internet Name Domain (BIND) server, Version 8.1.1 or later).

The DNS server associates the Advanced Server cluster alias name with an ordered list of the IP addresses of all, or more typically, a subset of, associated cluster nodes that are running the Advanced Server. The order of the list is based on the relative loads of the servers in the cluster. The DNS name server returns this ordered list to any client querying for the server cluster alias name. Periodically, the cluster load balancing software dynamically updates this cluster alias entry at the DNS server, providing a new ordered list of associated IP addresses, based on the latest relative loads on the servers running in the cluster.

**Note**

To have DNS resolve NetBIOS names, you must enable NetBIOS name resolution using DNS, as described in Section 7.2.6.2, Selecting NetBIOS Name Resolution. To correctly resolve the Advanced Server

cluster alias and gain the benefits of cluster load balancing, all clients and servers should enable NetBIOS name resolution using DNS.

---

#### 2.4.4.1 Background and Overview: Advanced Server Clusters and Load Balancing

The Advanced Server encompasses many of the features of the OpenVMS operating system, including OpenVMS Clusters and symmetric multiprocessing. Advanced Servers in your network that are configured in an OpenVMS Cluster environment share the same copy of the domain security accounts and shares databases and assume a single role, either a PDC, BDC, or member server.

For Advanced Servers in an OpenVMS Cluster, you must define a server cluster alias so that client workstations and network nodes can address the Advanced Servers in the OpenVMS Cluster as a single entity.

Clients should connect to the Advanced Server using the Advanced Server cluster alias; the client is connected to the least-loaded server in the OpenVMS Cluster. To gain the benefits of load balancing and failover using DNS, remove any entries for the cluster alias from the LMHOSTS file and local hosts file on clients, and you might need to remove any static entries for the cluster alias from the WINS database on WINS servers that are used by clients. (If Windows 95, Windows 98, or Windows NT clients are configured to use both WINS and DNS for NetBIOS name resolution, they first query the WINS server to resolve the name.)

#### 2.4.4.2 The Software for Dynamic Cluster Load Balancing in WANs

The Advanced Server in conjunction with TCP/IP Services for OpenVMS provides dynamic load balancing through use of the *load broker*. The load broker is a configurable software component that calculates the relative loads of Advanced Server cluster members so that client requests for services can be distributed appropriately among these members. For information about configuring the load broker, refer to the latest TCP/IP Services for OpenVMS documentation of cluster load balancing with BIND servers.

The load broker periodically polls the Metric Server running on the cluster members to determine the current load on each member and then compiles a list of all cluster members associated with the Advanced Server cluster alias, dropping any systems that are not responding, and ordering the list based on the relative loads. The load broker provides this list when it sends a dynamic update request to a specified DNS server. The DNS server then updates the Advanced Server cluster alias name entry in the DNS name server database.

The DNS name server uses this ordered list to answer client requests for the Advanced Server cluster alias name. In addition, to further balance the load among the server members of the cluster, the name server uses round-robin scheduling. For every consecutive request for resolving the Advanced Server cluster alias, the name server returns a new list, rotated by one (the second server in the preceding list now being the first server in the new list, and so on).

#### 2.4.4.3 Enabling Dynamic Load Balancing Using TCP/IP Services for OpenVMS

To enable dynamic cluster load balancing for service requests from WAN clients, complete the following tasks:

- If you are using WINS to resolve NetBIOS names, you might need to remove all static entries for the cluster alias from the WINS database of all WINS servers that might be used by clients. (If Windows 95, Windows 98, or Windows NT clients are configured to use both WINS and DNS for NetBIOS name resolution, they first query the WINS server to resolve the name). WINS should still be the primary resource for resolving names.)
- If you are using LMHOSTS to resolve NetBIOS names, remove all entries for the cluster alias from the LMHOSTS file and local hosts file of all clients and servers.
- On all clients and servers, to correctly resolve the Advanced Server cluster alias and gain the benefits of cluster load balancing, enable NetBIOS name resolution using DNS.
- Ensure that all hosts in the cluster are running Compaq TCP/IP Services for OpenVMS (Compaq recommends Version 5.0A or later). On each member of the cluster that is running the Advanced Server, enable the *Metric Server*. The Metric Server calculates the load on the cluster member that it is running on.
- Configure the TCP/IP Services for OpenVMS load broker. When configuring the load broker, the following load broker parameters are important regarding load balancing:
  - **max-members**

    The **max-members** parameter specifies the maximum number of IP addresses to be returned to the DNS name server in each dynamic update. Be sure to set this parameter to a value that is anywhere from one-third to one-half of the number of cluster members running the Advanced Server. The load broker will then send the DNS server a list of that number of servers on the cluster that have the least loads of all the server cluster members. The DNS server uses the list to answer clients' queries in round-robin fashion. Do NOT set the parameter to

the actual number of cluster members running the Advanced Server; otherwise, the load broker will send the DNS server a list of all the server cluster members — even the most heavily loaded members — and load balancing will not be accomplished.

– **polling-interval**

The **polling-interval** parameter specifies the time interval between polls to the cluster members. The default is 30 seconds.

– **dns-refresh**

The **dns-refresh** parameter specifies how often the DNS information for a given DNS cluster name is refreshed. The default is 30 seconds. If you want to quickly pick up changes in the system load (reported by metric servers), set **dns-refresh** to a smaller number. This parameter should be set in conjunction with the **polling-interval** parameter — when you change one, you should most likely change the other. Though both parameters default to the same value, the value of the **dns-refresh** parameter should be greater than or equal to that of the **polling-interval** parameter. It is unproductive to refresh more often than you poll.

For more information about configuring the load broker, refer to the *TCP/IP Services for OpenVMS Management* guide.

- Ensure TCP/IP connectivity between the cluster members and the load broker.
- At the authoritative DNS (BIND) name server for the cluster, ensure that the Advanced Server cluster alias name is NOT already registered as a cluster alias name (that is, as having multiple A resource records for a single host name). The cluster name is associated with the IP addresses of all cluster members that are running the Advanced Server. If the addresses of the cluster members are added to the DNS database, round-robin load balancing will be in effect instead of dynamic load balancing.
- Configure the authoritative DNS name server to allow dynamic updates from the host on which the load broker is running, as explained in the *TCP/IP Services for OpenVMS Management* guide.
- Optionally, as appropriate, configure the parameters and logical names described in the latest *TCP/IP Services for OpenVMS Management* guide.

Review the following guidelines:

- The server cluster alias and the TCP/IP cluster alias should be different (in many environments, this will facilitate troubleshooting problems that involve name resolution).

- Cluster hosts and clients are not required to be on the same bridged LAN.
- The number of cluster member hosts is limited to 32.
- The load broker can also be a cluster member.
- A DNS (BIND) name server can also be a cluster member host.
- The authoritative name server can be any name server that supports BIND Version 8.1.1 or later, or that supports dynamic updates.

Note the following regarding an Advanced Server BDC that needs to resolve a PDC cluster alias for dynamic DNS load balancing:

- If the BDC and the PDC are in the same DNS domain (for example, BUDGET.ACME.COM and SALES.ACME.COM), then WAN DNS dynamic load balancing will work.
- If the BDC and the PDC are not in the same DNS domain (for example, STANS_WS.BUILDING1 and SYSMGR_WS.BUILDING2), in order for WAN DNS load balancing to work, you must add entries for the domain names in the TCP/IP BIND resolver's domain search list. This assumes TCP/IP Services for OpenVMS V5.0A or later is running. If an earlier version of TCP/IP Services for OpenVMS is running, you must insert an entry for the cluster alias in the LMHOSTS file or a static entry for the cluster alias in the WINS database.

# 3

# Managing Users and Groups

On OpenVMS, you use Advanced Server ADMINISTER commands to manage network user accounts and groups for domains and computers. You can also use the Windows NT server administration tool, User Manager for Domains, to perform these tasks.

The Upgrade utility lets you upgrade users, groups, shares, and security from a PATHWORKS V5 for OpenVMS (LAN Manager) server. Refer to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Migration Guide* for information about upgrading your server.

The following topics are discussed in this chapter:

- Section 3.1, Managing Network User Accounts, describes how to add, modify, disable, enable, delete, rename, and display network user accounts and how to specify passwords, logon hours, scripts, workstations, and other user account information.
- Section 3.2, Managing Advanced Server Groups, describes how to create, copy, modify, delete, and display network groups.

Network user accounts and groups are separate and distinct from OpenVMS user accounts and groups. This guide discusses management of network user accounts and groups using Advanced Server.

## 3.1 Managing Network User Accounts

A network user account contains all the information that defines an Advanced Server user. This includes user name, password, and group memberships. It can also include information such as the user's full name, the user account description, user profile information, a list of logon workstations, and a schedule of authorized logon hours.

### 3.1.1 Built-In User Accounts

Two predefined, built-in user accounts are provided when an Advanced Server is installed:

- The Administrator user account is used to manage the server's users, groups, and resources. The Administrator account belongs to the Administrators, Domain Admins, and Domain Users built-in groups.

  You can use the Administrator account to administer a new server or workstation before you have had the opportunity to create an account for yourself. You cannot delete or disable the Administrator account. This ensures that you will never lock yourself out of the computer. When you initially configure the Advanced Server, you are prompted to choose a password for the Administrator account. Always assign a password to the Administrator account to help ensure security.

- The Guest user account belongs to the Domain Guests group and allows logons for users who do not have accounts in the computer's domain, or in a domain trusted by the domain where the Guest account has been enabled. By default, the Guest account is disabled at installation. You can enable it if Guest access is desired.

**Note**

Guest users should not create files in their default directory that they do not want other users to access, because all users logged on as Guest access the same default directory.

### 3.1.2 Types of User Accounts

Every network user account is either a global account or a local account:

- Global user accounts provide access to resources in the domain where the user account is created, and can also provide access to resources in domains that trust the domain where the user account is created.
- Local user accounts are restricted to the local domain. A local account can be used only to access server resources over the network. It cannot be used to log on to a Windows NT Server or workstation computer from the console.

### 3.1.3 User Account Attributes

The user account identifies the user to Advanced Server. The user account is used to authenticate the user both when the user logs on to the domain and when the user requests access to shared resources.

Each user account must have a unique user name in the domain. When you create a user account, you can specify the user account attributes shown in Table 3–1, User Account Attributes.

**Table 3–1 User Account Attributes**

| Attribute | Contains |
|---|---|
| User name | The user's account name (up to 20 alphanumeric characters). |
| Password | The password the user enters to log on to the account (up to 14 uppercase and lowercase alphanumeric characters). Passwords entered on ADMINISTER command lines are converted to uppercase unless enclosed within quotation marks. |
| Full name | User's full name, typically more complete than the account name (up to 256 characters). |
| Description | A brief text string describing the account. |
| Expiration date | Date when the account expires. |
| Type | Global or local. |
| Group names | The names of groups of which the user is a member. Determines privileges and access. |
| Logon restrictions | Logon hours and valid workstations. |
| Logon script | A script that is executed when the user logs on. |
| Home directory | A specified location containing files and programs for the user. |
| User profile | Setup information for the user's specific environment. |

Advanced Server allows you to integrate OpenVMS user accounts with network user accounts. Network user accounts can be linked (*host mapped*) to OpenVMS user accounts, simplifying user account management, ensuring password synchronization, and providing automatic access to network administration functions for OpenVMS system manager and operators. See Section 3.1.16.2, Establishing User Account Host Mapping, for more information.

To set account characteristics across all network user accounts, set the account policy, as described in Section 2.2.1, Managing the Account Policy.

User accounts are stored in the domain's Security Account Manager (SAM) database. The SAM database is maintained by the primary domain controller and periodically updated on the backup domain controllers. One of the computers in the domain must be running as a primary domain controller in order for user accounts to be created or modified.

## 3.1.4 Creating User Accounts

You create network user accounts on the Advanced Server with the ADD USER or COPY USER command.

### 3.1.4.1 Creating a Network User Account

When you create a user account, you must provide all the information relevant to that user. You can use the ADD USER command to create a user account, or the COPY USER command to copy another account and modify it to suit the specific user.

When you display user information, the users are listed alphabetically by user name; you can optionally sort the display based on the full name. Therefore, follow the same conventions for all users when you enter full names; for example, Cowardly Lion or Lion, Cowardly.

Passwords for network user accounts are case sensitive. Passwords entered on the ADMINISTER command line default to all uppercase characters, unless you enclose them in quotation marks. To preserve lowercase letters, spaces, and other nonalphanumeric characters in passwords when you enter ADMINISTER commands, enclose the password in quotation marks, or enter the password in response to the prompt instead of on the command line. The following example shows how to enter a mixed-case password on the command line:

```
LANDOFOZ\\TINMAN> ADD USER SCARECROW/PASSWORD="OverTheRainbow"
%PWRK-S-USERADD, user "SCARECROW" added to domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

You can specify an optional description for the user by including the /DESCRIPTION qualifier. If the description contains nonalphanumeric characters, spaces, or lowercase letters, enclose the description in quotation marks.

**3.1.4.1.1 Creating a Global User Account** Use the ADD USER command to create a global user account, as in the following example:

```
LANDOFOZ\\TINMAN> ADD USER SCARECROW/PASSWORD -
_LANDOFOZ\\TINMAN> /DESCRIPTION= "The Straw Man" -
_LANDOFOZ\\TINMAN> /FULLNAME="Man, Straw"
Password:
Password verification:
%PWRK-S-USERADD, user "SCARECROW" added to domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

You can let Advanced Server prompt you for the user name and the password. The password is not displayed as you enter it. You should always supply a password when you add a user account, or explicitly specify that the user account has no password (using the /NOPASSWORD qualifier); otherwise the password value is unknown. By default, a user account is created with an expired password. The user must enter a new password at first logon. To remove the need for users to reset their passwords at first logon, use the /FLAGS=(NOPWDEXPIRED) qualifier with the ADD USER command.

You can specify additional details about the user account, including an account description, expiration date, a full name, type of account (global or local), a home directory, logon hours, group membership, user profile, logon script, and workstation names, if any. For details on the ADD USER command, refer to the *Compaq Advanced Server for OpenVMS Commands Reference Manual*.

The ADD USER command does not create an OpenVMS user account. However, if the user also has an OpenVMS account, you can associate the two user accounts. For more information, see Section 3.1.16, User Account Host Mapping.

Users with both a network account and an OpenVMS account have two passwords: one for each user account. You can enable external authentication for these users, providing automatic password synchronization between the OpenVMS password and the network password. For information about external authentication, see Section 3.1.17, External Authentication.

**3.1.4.1.2 Verifying That the User Has Been Added** To verify that the user you created an account for has been added, use the SHOW USERS command. You can display details about a user account with the SHOW USERS/FULL command. For example:

```
LANDOFOZ\\TINMAN> SHOW USERS SCARECROW/FULL

User accounts in domain "LANDOFOZ":

User Name             Full Name             Type    Description
-------------------   -------------------   ------  ---------------
SCARECROW             Man, Straw            Global  The Straw Man
    User Profile:
    Logon Script:
    Primary Group: Domain Users
    Member of groups: Domain Users
    Workstations: No workstation restrictions
    Logon Flags: Login script is executed, Password is expired
    Account Type: Global
    Account Expires: Never
    Logon hours: (All hours)
    Last Log On: 07/23/01 05:07 PM
    Password Last Set: 06/30/01 11:03 AM
    Password Changeable: 06/30/01 11:03 AM
    Password Expires: 09/11/01 11:03 AM

  Total of 1 user account

LANDOFOZ\\TINMAN>
```

A primary group is used when a user logs on using Windows NT Services for Macintosh, or runs POSIX applications.

**3.1.4.1.3 Creating a Local User Account** To create a local user account, use the ADD USER command as shown previously, and include the /LOCAL qualifier.

### 3.1.4.2 Creating User Account Templates

You can create a template for user accounts, specifying user account information common to the new user accounts you need to create. Most user account information can be copied from the template to the new user accounts, except for user name and password. For example, you could create a template user account as follows:

```
LANDOFOZ\\TINMAN> ADD USER TEMPLATE/LOCAL/HOURS=(8-5) -
_LANDOFOZ\\TINMAN> /MEMBER_OF_GROUPS=MUNCHKINS
%PWRK-S-USERADD, user "TEMPLATE" added to domain "LANDOFOZ"
```

You can then use the COPY USER command to create many new user accounts that have these same characteristics. Once you have completed adding all your new user accounts, you can then delete or disable the TEMPLATE user account, as described in Section 3.1.15, Disabling and Removing User Accounts.

#### 3.1.4.3 Copying User Accounts

You can use the COPY USER command to create a new user account from an existing account or a template account. Some of the original user account information is copied to the new user account, such as group memberships and logon restrictions. A template account makes it easier to create many similar user accounts with fewer errors than to create them one by one. Some user account information, such as user name and password, is not copied to the new user account. You should always supply a password when you create a new user account, or explicitly specify that the user account has no password (using the /NOPASSWORD qualifier); otherwise the password value is unknown.

Use the /PASSWORD qualifier with the COPY USER command to specify the password for the new user account. For example, to create a new user LION based on a user account template (TEMPLATE), enter the following command:

```
LANDOFOZ\\TINMAN> COPY USER TEMPLATE LION/PASSWORD="Roaring1" -
_LANDOFOZ\\TINMAN> /FULL_NAME="Cowardly Lion"
%PWRK-S-USERCOPY, user "TEMPLATE" copied to "LION" in domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

This example copies the TEMPLATE user account information to a new account for user LION and uses the /FULL_NAME qualifier to provide the full name for the new user. The /PASSWORD qualifier specifies the password for the account LION. You can verify that the user is correctly added, by using the SHOW USERS command.

### 3.1.5 Specifying Passwords

Users must specify their password when they log on to the domain. The user name and password are validated against the security accounts database.

Advanced Server password characteristics are controlled by the following:

- The /FLAGS qualifier with the ADD USER, COPY USER, and MODIFY USER commands.

  For example, use ADD USER/FLAGS=(*keyword*) to specify password characteristics when you create a user account. The keywords that control the password characteristics are:

  - [NO]DISPWDEXPIRATION, which prevents the password from expiring.
  - [NO]PWDEXPIRED, which specifies whether the password is initially expired. This forces the user to specify a new password when they log on the first time.

  - [NO]PWDLOCKED, which specifies whether the user is allowed to change the password.

  For more information about these commands and qualifiers, refer to the *Compaq Advanced Server for OpenVMS Commands Reference Manual*.

- The SET ACCOUNT POLICY/PASSWORD_POLICY command.

  This command sets domainwide account policy characteristics that pertain to all passwords, including the:

  - Maximum password age
  - Minimum password age
  - Minimum length of the password
  - Whether password history is maintained

  For more information about how to use this command to establish a policy for password usage, see Section 2.2.1, Managing the Account Policy.

- The SET ACCOUNT POLICY/LOCKOUT command.

  This command establishes how failed attempts to log on to the network are handled. You can use this command to specify the number of failed logon attempts before the account is locked, as explained in detail in Section 2.2.1, Managing the Account Policy.

  By default, user account lockout is disabled, meaning that the user accounts are never locked out, no matter how many failed logon attempts are made on a user account.

  For more information about setting the account policy, see Section 2.2, Managing Security Policies and refer to the *Compaq Advanced Server for OpenVMS Commands Reference Manual*.

Network users who also have OpenVMS user accounts have two passwords, one for each account. If password synchronization is important, as with external authentication, be careful to observe limitations in password length and characters required by OpenVMS as well as Advanced Server. Network passwords can be up to 14 characters long; OpenVMS passwords can be longer. To help ensure security, select secure passwords using words not found in the dictionary, including numbers or nonalphabetic characters.

When you add a new user or modify the password for an existing user, you specify the password for that user. For example:

```
LANDOFOZ\\TINMAN> ADD USER SCARECROW/PASSWORD="YellowRoad"
%PWRK-S-USERADD, user "SCARECROW" added on domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

To preserve case in a password, enclose it in quotation marks. By default, a password entered on the command line that is not enclosed in quotation marks is stored in uppercase letters. However, case is preserved for a password entered in response to a prompt.

#### 3.1.5.1 Changing a User Password

To change a user's password, you can use the SET PASSWORD command or the MODIFY USER/PASSWORD command. For example:

```
LANDOFOZ\\TINMAN> SET PASSWORD SCARECROW "YellowRoad" "EmeraldCity"
%PWRK-S-PSWCHANGED, password changed for user "SCARECROW" in domain
"LANDOFOZ"

LANDOFOZ\\TINMAN>
```

In this example, the user name is SCARECROW, the existing password is "YellowRoad" and the password is changed to "EmeraldCity."

### 3.1.6 Specifying Group Membership

Group membership allows you to control multiple user accounts and to grant permissions to use resources to a group of users rather than specifying individual users for resource permissions. By default, all user accounts are included in the special group Everyone. For the purposes of network administration, the user account is also included in the groups Domain Users and Users.

When you create a user account, you can specify membership in additional groups using the ADD GROUP or COPY GROUP command. For example, to include the user SCARECROW in the group MUNCHKINS, add the user account including the /MEMBER_OF_GROUPS qualifier, as follows:

```
LANDOFOZ\\TINMAN>ADD USER SCARECROW/PASSWORD/MEMBER_OF_GROUPS=(MUNCHKINS)
Password:
Password verification:
%PWRK-S-USERADD, user "SCARECROW" added to domain LANDOFOZ"

LANDOFOZ\\TINMAN>
```

### 3.1.7 Specifying Logon Hours

You can restrict the days and hours during which a user can connect to a server. The default is to allow a user to connect at all times. To specify logon hours, use the ADD USER, COPY USER, or MODIFY USER command with the /HOURS qualifier. Specify the hours to be administered as shown in Table 3–2, Specifying Logon Hours. The /NOHOURS qualifier specifies that the user cannot log on to the server.

Hours are inclusive: if you grant access during a given hour, access extends to the end of that hour; if no hours are specified for a given day, all hours are allowed.

**Table 3–2 Specifying Logon Hours**

| Hours to Specify | Example Specification |
|---|---|
| A specific hour | /HOURS=(MONDAY=(8)) |
| A block of hours | /HOURS=(FRIDAY=(8-12)) |
| One entire day | /HOURS=(SUNDAY) |
| A specific hour across all seven days | /HOURS=(SUNDAY=(1),MONDAY=(1), TUESDAY=(1), WEDNESDAY=(1), THURSDAY=(1),FRIDAY=(1), SATURDAY=(1)) |
| All weekdays | /HOURS=(WEEKDAYS) |
| The entire week | /HOURS=(EVERYDAY) |

In the following example, a user called MOUSEQUEEN is added to the domain LANDOFOZ with logon capability on Fridays from 8 a.m. to 12 noon.

```
LANDOFOZ\\TINMAN> ADD USER MOUSEQUEEN/HOURS=(FRIDAY=(8-12))
%PWRK-S-USERADD, user "MOUSEQUEEN" added to domain "LANDOFOZ"
```

The following example adds user BLACKCROW to domain LANDOFOZ, with logon capability from Monday through Friday, all hours.

```
LANDOFOZ\\TINMAN> ADD USER BLACKCROW/HOURS=(WEEKDAYS)
%PWRK-S-USERADD, user "BLACKCROW" added to domain "LANDOFOZ"
```

For more details on the /HOURS qualifier, see Section 3.1.14, Modifying User Accounts.

## 3.1.8 Specifying Logon Scripts

You can specify the execution of a logon script when a user logs on. A logon script is an executable or batch file of commands that runs on the client. It is typically used to configure the client for a particular user, performing such tasks as making network connections and starting applications. Logon scripts can be tailored to the requirements of individual users. A logon script typically has a .BAT, .CMD, or .EXE file extension, depending on its function.

#### 3.1.8.1 Setting Up a Logon Script

When a user logs on, Advanced Server checks the user's account on the logon server for the name of a script. Scripts are kept on the primary and backup domain controllers. By default, user scripts on an Advanced Server are stored in the following location:

PWRK$LMROOT:[LANMAN.REPL.IMPORT.SCRIPTS]

#### 3.1.8.2 Providing User Access to Logon Scripts

For a user to have access to a logon script, the following conditions must be true:

- The SCRIPTS directory must be shared.
- The user must have R (read) permission for the script. By default, all users in group Everyone have R (read) permission to access the scripts directory.

Ensure that permissions on the directory or share where the scripts reside permit access to all users who will be using the scripts. Advanced Server automatically provides Read access to members of the special group Everyone.

When the NetLogon service starts, the Advanced Server shares the scripts directory identified with the share name NETLOGON. For logon scripts to run, do not remove the NETLOGON share. You can display information about the NETLOGON share using the SHOW SHARE NETLOGON/FULL command. For example:

```
LANDOFOZ\\TINMAN> SHOW SHARE NETLOGON/FULL

Shared resources on server "TINMAN":
Name         Type       Description
-----------  ---------  ----------------------------------------
NETLOGON     Directory  Logon Scripts Directory
    Path: PWRK$LMROOT:[LANMAN.REPL.IMPORT.SCRIPTS]
    Connections:  Current: 0, Maximum: No limit
    RMS file format: Stream
    Directory Permissions: System: RWED, Owner: RWED, Group: RWED, World: RE
    File Permissions: System: RWD, Owner: RWD, Group: RWD, World: R
    Share Permissions:
        Everyone                      Read

  Total of 1 share

LANDOFOZ\\TINMAN>
```

### 3.1.9 Specifying Workstations

Use the /WORKSTATIONS qualifier to restrict the workstations from which users can log on to domain accounts. The default is to allow a user to log on from any workstation, but you can optionally restrict a user's logons to certain workstations. You can specify up to eight workstations for the user account.

To manage logon workstations, use the ADD USER, COPY USER, or MODIFY USER command, with the /WORKSTATION qualifier. For example:

```
LANDOFOZ\\TINMAN> ADD USER LION /WORKSTATION=(LIONS_DEN)
%PWRK-S-USERADD, user "LION" added to domain "LANDOFOZ"
```

This command creates the new user account LION and specifies that the user can log on from the LIONS_DEN workstation.

### 3.1.10 Specifying Home Directories

A user's home directory is accessible to the user and contains files and programs for that user. When a user logs on at a workstation, a connection can be made to that user's home directory automatically. Depending on the client computer, you may need to specify the home directory in a logon script. The home directory becomes the user's default directory for file access and for all applications that do not have a defined working directory. Home directories can make it easier for an administrator to back up user files because they keep many or all of a user's files in one location.

On a server running Advanced Server software, the default parent directory for user account home directories is:

PWRK$LMROOT:[LANMAN.ACCOUNTS.USERDIRS]

You can specify a home directory as an absolute path name or as a UNC (Universal Naming Convention) path name, which is domain wide. To specify the default parent directory for user account home directories, enter:

*server*\LANMAN\ACCOUNTS\USERDIRS

If you omit the /HOME qualifier when you create a user account, no home directory is defined for a user.

**Note**

The Advanced Server home directory is not associated with the OpenVMS SYS$LOGIN directory.

A home directory can be assigned to a single user or it can be shared by several users. It can be a local directory on a user's workstation or a shared network directory. If you specify a network path for the home directory, an attempt is made to create that home directory. If the directory cannot be created, a message instructs you to create the directory manually.

To specify a home directory, use the ADD USER, COPY USER, or MODIFY USER command, with the /HOME=(PATH=*pathname*) qualifier. The home directory *pathname* must be specified in one of the following forms:

- The absolute path of a directory local to the user's workstation
- The UNC path for a shared network directory, as follows:

  *servername**sharename**directoryname*

  If you specify a UNC path, you must also specify a drive letter that is not currently being used on the user's workstation, to be assigned to the path when the user logs on.

For example, to modify user account LION, specifying a home directory on server TINMAN to be associated with drive D, enter the following command:

```
LANDOFOZ\\TINMAN> MODIFY USER LION/HOME=(PATH=\\TINMAN\USERS\LION,DRIVE=D:)
%PWRK-S-USERMOD, user "LION" modified on domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

### 3.1.11 Specifying User Account Expiration Dates

You can assign an expiration date for a user account, at which time the account is automatically expired but not removed from the accounts database. You can reactivate an expired account by removing the expiration date or by assigning a new date.

By default, there is no expiration date for a user account. Use the ADD USER, COPY USER, or MODIFY USER command with the /EXPIRATION qualifier to define the account expiration date for a user account.

When an account has an expiration date, the account is disabled at the end of the previous day. When an account expires, a user who is logged on remains logged on, but cannot establish new network connections or log on again after logging off.

For example, to add a user named FRIENDLY to the domain LANDOFOZ and set the account to expire on November 9, 2001, enter the following command:

```
LANDOFOZ\\TINMAN> ADD USER FRIENDLY/PASSWORD="PotOfGold"-
_LANDOFOZ\\TINMAN>/EXPIRATION_DATE=09-NOV-2001
%PWRK-S-USERADD, user "FRIENDLY" added to domain "LANDOFOZ"
```

### 3.1.12 Specifying User Profiles

User profiles allow you to set up the user's environment so that it can be downloaded to the user's workstation when the user logs on to the network. The user profile contains configuration information such as:

- Desktop arrangement
- Personal program groups and program items
- Screen colors and screen savers
- Network connections
- Mouse settings
- Window size and positions

When the user logs on, the user profile is downloaded and the user's workstation is configured accordingly.

You create user profiles using the Windows NT Server tool User Profile Editor. Refer to your Windows NT Server documentation for more information.

When you add a user, you can specify a profile and its path.

To specify a profile, use the ADD USER or MODIFY USER command with the /PROFILE qualifier. For example, to add user SCARECROW with a profile that is stored on the server TINMAN, enter the following command:

```
LANDOFOZ\\TINMAN> ADD USER SCARECROW/PROFILE="\\TINMAN\PROFILES\SCARECROW.USR"
%PWRK-S-USERADD, user "SCARECROW" added to domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

Note that the network path to the profile is enclosed in quotation marks.

### 3.1.13 Displaying User Accounts

To display information about user accounts, use the SHOW USERS command. For example:

```
LANDOFOZ\\TINMAN> SHOW USERS

User accounts in domain "LANDOFOZ":

User Name          Full Name      Type    Description
--------------     -----------    ------  -----------------------
Administrator                     Global   Built-in account for
                                           administering the domain
Guest                             Global   Built-in account for
                                           guest access to the domain
LION               Lion,Cowardly  Global   Cowardly Lion
SCARECROW          Man, Straw     Global   The Straw Man
```

```
   Total of 4 user accounts

LANDOFOZ\\TINMAN>
```

### 3.1.13.1 Example: Sorting the Display by User Full Name

To sort the display by user full name, use the SHOW USERS/SORT=FULLNAME command, as in the following example:

```
LANDOFOZ\\TINMAN> SHOW USERS/SORT=FULLNAME

User accounts in domain "LANDOFOZ:"

Full Name      User Name        Type    Description
-------------- -------------    ------  --------------------------
               Administrator    Global  Built-in account for
                                        administering the domain
               Guest            Global  Built-in account for guest
                                        access to the domain
Lion, Cowardly  LION            Global  Cowardly Lion
Man, Straw      SCARECROW       Global  The Straw Man

   Total of 4 user accounts

LANDOFOZ\\TINMAN>
```

### 3.1.13.2 Example: Reviewing User Account Settings for a Specific User

To display user account settings for a specific user, use the SHOW USERS/FULL command. For example, the following display shows the settings for user LION.

```
LANDOFOZ\\TINMAN> SHOW USERS LION/FULL

User accounts in domain "LANDOFOZ":

User Name       Full Name       Type    Description
--------------- --------------- ------- -------------
LION            Lion, Cowardly  Global  Cowardly Lion
   User profile:
   Logon script:
   Home Path: D: Path: \\TINMAN\USERS\LION
   Primary Group: Domain Users
   Member of groups: Domain Users, MUNCHKINS
   Workstations: No workstation restrictions
   Logon Flags: Logon script is executed, Password is expired
   Account Type: Global
   Account Expires: Never
   Logon hours (All hours)
   Last Log On: 07/23/01 05:07 PM
   Password Last Set: 06/30/01 11:03 AM
   Password Changeable: 06/30/01 11:03 AM
   Password Expires: 09/11/01 11:03 AM

  Total of 1 user account

LANDOFOZ\\TINMAN>
```

## 3.1.14 Modifying User Accounts

Use the MODIFY USER command to change the attributes of an existing user account. You can:

- Change group membership
- Add, change, or delete a description
- Specify a full name
- Specify whether the user is a global or local user
- Change the user's account settings
- Remove a user from a group
- Specify workstations that the user can access

### 3.1.14.1 Example: Adding an Existing User to a Group

To add an existing user to a group, use the MODIFY USER/ADD_TO_GROUPS command, as in the following example:

```
LANDOFOZ\\TINMAN> MODIFY USER SCARECROW/ADD_TO_GROUPS=MUNCHKINS
%PWRK-S-USERMOD, user "SCARECROW" modified on domain "LANDOFOZ"
```

You can then enter the SHOW GROUPS/FULL command to see that the group MUNCHKINS now includes the user SCARECROW:

```
LANDOFOZ\\TINMAN> SHOW GROUPS MUNCHKINS/FULL

Groups in domain "LANDOFOZ":
Group Name            Type    Description
--------------------  ------  ----------------------------------
MUNCHKINS             Global  Users in the Land of Oz
    Members: [US]LION, [US]SCARECROW)

  Total of 1 group)

LANDOFOZ\\TINMAN>
```

### 3.1.14.2 Example: Changing a User's Logon Hours

To change the hours when a user can log on, use the MODIFY USER/HOURS command. For example, to restrict a user to logging on only on Monday from 8 a.m. to 9 a.m. and from 3 p.m. to 8 p.m., specify /HOURS=(MON=(8-9,15-20)).

For example, to modify LION's logon hours, use the MODIFY USER command, as follows.

```
LANDOFOZ\\TINMAN> MODIFY USER LION/HOURS=(MON=(8-9,15-20))
%PWRK-S-USERMOD, user "LION" modified on domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

You can verify that the change was made correctly using the SHOW USERS/FULL command. For example:

```
LANDOFOZ\\TINMAN> SHOW USERS LION/FULL

User accounts in domain "LANDOFOZ":

User Name       Full Name       Type     Description
--------------- --------------- ------- -------------
LION            Lion, Cowardly  Global  Cowardly Lion
   User profile:
   Logon script:
   Home Path: D: Path: \\TINMAN\USERS\LION
   Primary Group: Domain Users
   Member of groups: Domain Users, MUNCHKINS
   Workstations: No workstation restrictions
   Logon Flags: Logon script is executed, Password is expired
   Account Type: Global
   Account Expires: Never
   Logon hours: 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 2 2 2 2
                0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
        Sunday: - - - - - - - - - - - - - - - - - - - - - - - -
        Monday: - - - - - - - - X X - - - - - X X X X X X - - -
       Tuesday: - - - - - - - - - - - - - - - - - - - - - - - -
     Wednesday: - - - - - - - - - - - - - - - - - - - - - - - -
      Thursday: - - - - - - - - - - - - - - - - - - - - - - - -
        Friday: - - - - - - - - - - - - - - - - - - - - - - - -
      Saturday: - - - - - - - - - - - - - - - - - - - - - - - -
   Last Log On: 07/23/01 05:07 PM
   Password Last Set: 06/30/01 11:03 AM
   Password Changeable: 06/30/01 11:03 AM
   Password Expires: 09/11/01 11:03 AM

  Total of 1 user account

LANDOFOZ\\TINMAN>
```

### 3.1.15 Disabling and Removing User Accounts

A user's ability to log on can be rescinded by either disabling or removing the user account. A disabled user account still exists, but the user is not permitted to log on. It continues to appear in the user accounts list. It can be restored to enabled status at any time. A removed account is permanently removed and cannot be recreated with the same security settings.

Each user in a domain is identified by a unique security identifier (SID). The SID is created when a user account is created and is used when assigning permissions to a resource. Because a SID is unique to an account, a new account, even with the same user name, is assigned a new SID. Therefore, if you delete a user account and then need to create another user account for the same user with the same user name, the new user account will not have the rights or permissions that previously were granted to the old user account, because the user account will have a different SID. To avoid problems,

first disable a user account you want to remove and then remove it after a reasonable time.

#### 3.1.15.1 Disabling a User Account

Set the account to Disabled, using the MODIFY USER/FLAGS=(DISUSER) command.

#### 3.1.15.2 Deleting a User Account

To delete a user account, use the REMOVE USER command. You are prompted for confirmation before the command executes.

A deleted user account is removed from the user accounts list and cannot be restored or recreated. Make sure that you want to delete a user account before doing so. For example:

```
LANDOFOZ\\TINMAN> REMOVE USER LION
Each user account is represented by a unique identifier which is
independent of the user name.  Once the user account is deleted,
even creating an identically named user account in the future will
not restore access to resources which currently name this user
account in the access control list.
Remove user "LION" [YES or NO] (YES) : YES
%PWRK-S-USERREM, user "LION" removed from domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

### 3.1.16 User Account Host Mapping

Advanced Server provides user account host mapping, which associates a network user account with an OpenVMS user account, simplifying the management of both user accounts. Host mapping is required for users who are externally authenticated, as described in Section 3.1.17, External Authentication.

Every file on an OpenVMS system must have an owner. Host mapping establishes which OpenVMS account is assigned as the owner when an Advanced Server user creates files or directories. Host mapping is also used to determine the OpenVMS user name when logging on to OpenVMS using external authentication. Additionally, when the Advanced Server and OpenVMS security model is enabled, host mappings are used to determine the OpenVMS access rights permitted to the user. The security models are selected using the Configuration Manager, as described in Section 7.2, Using the Configuration Manager.

### 3.1.16.1 Implicit and Explicit Host Mapping

The Advanced Server supports both explicit and implicit host mapping between OpenVMS and Advanced Server user accounts. You can explicitly map a network user name to an OpenVMS user name using the ADMINISTER command ADD HOSTMAP.

Implicit host mapping is established when:

- An OpenVMS user name matches a network user name exactly.
- The network user name is one of the following:
  - Administrator (implicitly mapped to the SYSTEM account)
  - Guest (implicitly mapped to PWRK$GUEST)
  - PWRK$DEFAULT (used when no match is found)

Host mapping is used to determine the OpenVMS user name when logging on to OpenVMS using external authentication. The user account Administrator is implicitly mapped to the OpenVMS user account SYSTEM. Therefore, if you enable the OpenVMS user account SYSTEM for external authentication, you can log in to the SYSTEM account using the Administrator user name and password, without explicitly defining any host map information. See Section 3.1.17, External Authentication, for more information.

Implicit host mapping is based on the user account names. Therefore, if you copy the Administrator account or the Guest account, you must specifically set up host mapping for the new user accounts. If you rename the Administrator or Guest account, the implicit mapping is not preserved. You must explicitly map the newly renamed account name to the OpenVMS SYSTEM account using the ADMINISTER command ADD HOSTMAP.

### 3.1.16.2 Establishing User Account Host Mapping

By default, if a user name for a network user account is identical to the user name for an OpenVMS user account, the user accounts are host mapped. Files created by the network user are automatically designated with the OpenVMS owner setting. This feature is controlled by a set of server configuration parameters, described in Section 7.3, Using the LANMAN.INI File. including:

- **HostMapUseVMSNames**, which specifies whether host mapping is enabled or not. By default, host mapping is enabled.
- **HostMapDomains**, which specifies domain names for user accounts in trusted domains.
- **HostMapDefault**, which specifies the default OpenVMS user name to associate with user accounts that have no default or specified mapping.

When a user creates a file or directory using the Advanced Server, the resource is assigned the OpenVMS ownership associated with the user's mapped account. The mapped account is used for OpenVMS resource ownership. (For more information about enabling this security model, see Section 7.2, Using the Configuration Manager.)

**3.1.16.2.1 Setting Up Explicit Host Mapping** To set up explicit host mapping, use the ADD HOSTMAP command in the following form:

ADD HOSTMAP *network-user-name OpenVMS-user-name*

In the following example, the network user account for SCARECROW is host mapped to the user's OpenVMS user account STRAWMAN. If SCARECROW creates a file, the file is assigned the RMS ownership attributes associated with the OpenVMS account STRAWMAN.

```
LANDOFOZ\\TINMAN> ADD HOSTMAP SCARECROW STRAWMAN
%PWRK-S-HOSTMAPADD, user "SCARECROW" mapped to host user "STRAWMAN"

LANDOFOZ\\TINMAN>
```

**3.1.16.2.2 Displaying Host Mapping** To display host mapping, use the SHOW HOSTMAP command. For example:

```
LANDOFOZ\\TINMAN> SHOW HOSTMAP
Host Mappings for server "TINMAN":

User Name                       Host Name
----------------------------    -----------
Guest                           PWRK$GUEST
SCARECROW                       STRAWMAN
LION                            CLION

  Total of 3 host mappings

LANDOFOZ\\TINMAN>
```

## 3.1.17 External Authentication

External authentication is supported on OpenVMS systems Version 7.1 and higher. External authentication allows the OpenVMS system manager to set up an OpenVMS user account for which login authentication is verified by the Advanced Server domain security. External authentication allows the Advanced Server to perform the user authentication for both Advanced Server domain user and OpenVMS user accounts.

External authentication is an option for users who have both OpenVMS and Advanced Server domain user accounts. It is not required. User host mapping provides the link between these two accounts, as described in Section 3.1.16, User Account Host Mapping.

With external authentication, users get automatic password synchronization between their OpenVMS accounts and their corresponding Advanced Server domain accounts. If the domain account password is changed, the OpenVMS LOGINOUT program sets the OpenVMS account password to the domain account password the next time the user logs in to the OpenVMS account. If the user changes the OpenVMS password with the DCL SET PASSWORD command, the the SET PASSWORD command sends the password change to the Advanced Server external authenticator. For synchronization to succeed, an Advanced Server domain controller must be available and the domain account password must meet OpenVMS syntax requirements. Externally authenticated users are considered to have a single password and are not subject to OpenVMS password policies, such as password expiration, password history, and minimum and maximum password length restrictions. Users are, however, subject to the Advanced Server domain user account policy that is defined. All other OpenVMS account restrictions remain in effect, such as disabled accounts, time restrictions, and quotas. For information about enabling external authentication, as well as information about setting up external authentication in OpenVMS Clusters, refer to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide*. For information about setting up the system and enabling OpenVMS user accounts for external authentication, refer to the *OpenVMS Guide to System Security*.

#### 3.1.17.1 Configuring the Server Capacity for External Authentication

By default, the Advanced Server can support up to 10 simultaneous external authentication logon requests (signons). You can modify this maximum to suit the server requirements, using the Configuration Manager. For more details, see Section 7.2.4.4, Specifying the Maximum Number of Concurrent Signons.

#### 3.1.17.2 Synchronizing Passwords

The password of an externally authenticated OpenVMS user is automatically synchronized with the host mapped Advanced Server domain user, regardless of the role of the Advanced Server in the domain.

When a user changes the OpenVMS password using the OpenVMS command SET PASSWORD, and external authentication is set for the user, OpenVMS forwards the password change request to the Advanced Server. When the password change request is successfully processed, OpenVMS updates the OpenVMS user password. If Advanced Server is not running when the OpenVMS command SET PASSWORD is executed, the domain password is not changed.

When users change their passwords from their client workstations, or the server administrator changes a password with the ADMINISTER command SET PASSWORD, the Advanced Server processes the password change as usual. The OpenVMS password is synchronized when the user next logs in to OpenVMS. All password changes are synchronized. When an OpenVMS user no longer has the external authentication flag set, the password for the OpenVMS user account is the same as the one that was last set by Advanced Server.

When users change their password on the OpenVMS system or on their client computer, they should use the new password to log in to OpenVMS. If, for some reason, the Advanced Server software is down at the time of the OpenVMS login, users can use their old OpenVMS password to log in, but only if you have enabled overriding of external authentication. In this case, privileged users can enter the /LOCAL_PASSWORD qualifier after their OpenVMS user name at the login prompt, as explained in Section 3.1.17.4, Bypassing External Authentication When the Network Is Down. This causes OpenVMS to perform local authentication.

**Note**

Password synchronization may fail due to the different sets of valid characters allowed by OpenVMS and Advanced Server. Keep this in mind when changing the password of an externally authenticated user.

#### 3.1.17.3 Disabling External Authentication

If you want to disable external authentication, then before starting the Advanced Server, define the SYS$SINGLE_SIGNON logical in SYSTARTUP_VMS.COM to a value of 0, as in the following example:

```
$ DEFINE/SYSTEM/EXECUTIVE SYS$SINGLE_SIGNON 0
```

For more information, refer to the *OpenVMS Guide to System Security*.

#### 3.1.17.4 Bypassing External Authentication When the Network Is Down

External authentication cannot occur if a network connection is required and the network is down. However, as a temporary solution, privileged users can enter the /LOCAL_PASSWORD qualifier after the OpenVMS user name at the login prompt, to specify local authentication. Be sure to specify the OpenVMS user name and password when using the /LOCAL_PASSWORD qualifier.

Because using the /LOCAL_PASSWORD qualifier effectively overrides the security policy established by the system manager, it is allowed only when the user's account has SYSPRV as an authorized privilege. This allows the system manager to gain access to the system when the network is down.

When Bit 1 is set in the SYS$SINGLE_SIGNON logical name, nonprivileged users who are normally externally authenticated can log in locally (the /LOCAL_PASSWORD qualifier need not be specified).

For more information about the /LOCAL_PASSWORD qualifier for the login command line, refer to the *OpenVMS Guide to System Security*.

#### 3.1.17.5 Logging On to Externally Authenticated Accounts

OpenVMS accepts the user name in one of the following formats for user accounts set for external authentication:

- *ASusername* (network user name)
- *Domainname\ASusername*
- *ASusername@Domainname*

The form of the user name string determines the order in which OpenVMS verifies the logon:

- If *ASusername* is used, this name is first interpreted as an OpenVMS user name. If the user name exists (in the OpenVMS System User Authorization File (SYSUAF)), and that user is not set for external authentication, the authentication is done as a standard OpenVMS login. Advanced Server authentication does not take place.

  If the user name does not exist in SYSUAF, the Advanced Server checks the domain accounts database (SAM) for the name and looks for an explicit host mapping to find the *ASusername* user's OpenVMS account. The server then verifies that the OpenVMS account is set for external authentication.
- If the domain name is included in the user name, OpenVMS activates external authentication of the user, using the name of the domain supplied:
  - If the domain name is the same as that of the local server, the local server will proceed to authenticate this request.
  - If the domain name is different from that of the local server, the software first checks whether the user name is mapped to the domain name explicitly. If so, the authentication request is forwarded to the specified domain for authentication. (For more information about host mapping, see Section 3.1.16.1, Implicit and Explicit Host Mapping.)

If the user name is not mapped to the domain name explicitly, the local server software checks the server configuration parameter **HostMapDomains** in LANMAN.INI to verify whether the specified domain is in the list of those trusted domains that the server allows to externally authenticate Advanced Server users. If the domain is listed there, the authentication request is forwarded to the specified domain for authentication. If the domain is not listed there, the logon request is denied.

#### 3.1.17.6 Avoiding User Name Conflicts

Because external authentication depends on host mapping information, it is important to set up user accounts and host mapping carefully. For example, if the same user name exists in the Advanced Server and OpenVMS, but they are not the same user, external authentication may not work as you expect.

In the following examples, you have Advanced Server running on OpenVMS node VMS1 in the domain SaleOffice, with network users Smith and J_Smith and OpenVMS users Smith and V_Smith:

- You enable external authentication for both of the OpenVMS users and then specify the user host mapping as follows:

  ```
  $ ADMINISTER ADD HOSTMAP SMITH V_SMITH
  $ ADMINISTER ADD HOSTMAP J_SMITH SMITH
  ```

  When OpenVMS user Smith uses his network user name J_Smith and password to log on to VMS1, this logon will be successful, providing the password is correct.

  However, when OpenVMS user V_Smith uses her network user name Smith and password to log on to VMS1, this logon will fail because of the name space conflict between Advanced Server and OpenVMS.

  To log on, OpenVMS user V_Smith must specify her network user name, specifying the domain name (either Smith@SaleOffice or SaleOffice\Smith).

- You enable external authentication only for OpenVMS user V_Smith, specifying the following command:

  ```
  $ ADMINISTER ADD HOSTMAP SMITH V_SMITH
  ```

  When OpenVMS user V_Smith uses her network user name Smith to log on to VMS1, the logon will fail, because Smith will first be interpreted as an OpenVMS user name. Because the OpenVMS user name exists, and it is not enabled for external authentication, the OpenVMS authentication mechanism is used to verify the password.

To log on, the OpenVMS user V_Smith must specify the domain name with her network user name (either Smith@SaleOffice or SaleOffice\Smith).

#### 3.1.17.7 Setting Up External Authentication by a Trusted Domain

You can set up an OpenVMS account to be externally authenticated by a trusted domain in your network. To enable this feature, you must include the trusted domain name in the data field for the server configuration parameter **HostMapDomains** in LANMAN.INI. See Section 7.3, Using the LANMAN.INI File.

For example, if your OpenVMS system is in the SaleOffice domain, and this domain trusts the Marketing domain, set up OpenVMS user Jones to be externally authenticated by the Marketing domain as follows:

1. Set the data field for the server configuration parameter **HostMapDomains** in the LANMAN.INI file (in the VMSSERVER section) to include the trusted domain name, as follows:

   ```
   HOSTMAPDOMAINS=Marketing
   ```

2. Ensure that a network user account with user name Jones exists in the Marketing Domain.
3. Enable external authentication for OpenVMS user account Jones.
4. To log on, the user must specify the user name in one of the following forms:

   ```
   Jones@Marketing
   Marketing\Jones
   ```

#### 3.1.17.8 Changing the Default Domain for External Authentication

The local server's domain is the default domain for users when external authentication is established. If you want to change the default domain for users using external authentication, define the Advanced Server logical PWRK$ACME_DEFAULT_DOMAIN on the system as follows:

```
$ DEFINE/SYS/EXE PWRK$ACME_DEFAULT_DOMAIN domain_name
```

where *domain_name* is the name of the new default domain. After defining this logical, if a user does not specify a domain name at login, the system will use the specified default domain for external authentication.

#### 3.1.17.9 Requirement for External Authentication Over DECnet-Plus

To allow users to be externally authenticated over DECnet-Plus for OpenVMS, set the system parameter NET_CALLOUTS to 255. This enables Advanced Server user ID mapping and authentication for network logins.

## 3.2 Managing Advanced Server Groups

Groups are collections of user accounts and other groups. When you add a user to a group, the user has all the rights and permissions granted to the group. This provides an easy way to grant common capabilities to sets of users. (For additional information about planning Advanced Server groups, refer to the *Compaq Advanced Server for OpenVMS Concepts and Planning Guide*.)

**Note**

OpenVMS system groups are unrelated to Advanced Server domain groups.

You use groups to manage access to resources like directories, files, and printers. To do this, assign permissions to the resource, specifying the group names, and add the user accounts to the groups. To change the permissions for a group, add or remove the permissions on the resource for the group, rather than for each user. Or, if you need to give a user access to specific resources (for example, certain directories and files), add the user's account to the appropriate group rather than changing permissions on each individual resource. Maintaining permissions for a group is simpler than maintaining permissions for individual user accounts.

Every group is either a global group or a local group.

- Global groups can be used both in their own domain and in trusting domains. You can use global groups to grant rights and permissions to global users. By default, new groups are global groups. Global groups can be members of a local group.
- Local groups can be granted permissions and rights only for the servers in their domain. However, they can contain user accounts and global groups both from their domain and from trusted domains. Local groups let you create sets of users from both inside and outside the domain, to access resources in the domain where the local group is created. The use of local groups in permissions lists for files and shares can also help reduce disk space consumption, as noted in Section 4.1.3.6, Streamlining Security Information Storage and Lookups.

Table 3–3 summarizes how to organize local and global groups.

**Table 3–3 Uses of Local and Global Groups**

| Users and Needs | Appropriate Group To Use |
|---|---|
| User accounts from this domain requiring access to the servers and workstations of this domain or of trusting domains | Global group |
| User accounts from trusting domains requiring access to the servers of this domain | Local group |
| Global groups from this domain requiring access to the servers of this domain | Local group |
| Global groups from trusting domains requiring access to the servers of this domain | Local group |

### 3.2.1 Built-In Groups

The Advanced Server creates several built-in groups automatically during installation. Each built-in group has a unique set of access rights. To give one such set of access rights to a user account, add the user to the appropriate group. By default, all users belong to the built-in group Domain Users.

Table 3–4 lists the built-in groups, with their group type (global or local), and their default members.

**Table 3–4 Built-In Groups**

| Group Name | Group Type | Description | Default Members |
|---|---|---|---|
| Account Operators | Local | Members can administer domain user and group accounts. | None |
| Administrators | Local | Members can fully administer the domain. | Administrator, Domain Admins |
| Backup Operators | Local | Members can bypass file security to back up files. | None |

(continued on next page)

**Table 3–4 (Cont.) Built-In Groups**

| Group Name | Group Type | Description | Default Members |
|---|---|---|---|
| Domain Admins | Global | Designated administrators of the domain. | Administrator |
| Domain Guests | Global | All domain guests. | Guests |
| Domain Users | Global | All domain users. | Administrator, user accounts |
| Guests | Local | Users granted guest access to the domain. | Domain Guests |
| Print Operators | Local | Members can administer domain printers. | None |
| Server Operators | Local | Members can administer domain servers. | None |
| Users | Local | Ordinary users. | Domain Users |

### 3.2.2 Setting Up User Groups

To set up a new user group, use the ADD GROUP command. To create a local group, include the /LOCAL qualifier on the command line. For example, to add the local group MUNCHKINS, enter the following command. Note that the description of the group is enclosed in quotation marks. If you do not specify the group type, the default is to add the group as a global group.

```
LANDOFOZ\\TINMAN> ADD GROUP MUNCHKINS/DESCRIPTION="Oz local group"/LOCAL
%PWRK-S-GROUPADD, group "MUNCHKINS" added to domain "LANDOFOZ"

LANDOFOZ\\TINMAN> SHOW GROUPS
Groups in domain "LANDOFOZ":
Group Name              Type          Description
--------------------    -----------   -----------------------------------
Account Operators       Local         Members can administer domain user and
                                      group accounts
Administrators          Local         Members can fully administer the domain
Backup Operators        Local         Members can bypass file security to back
                                      up files
DEVAS                   Global
DEVIS                   Global
Domain Admins           Global        Designated administrators of the domain
Domain Guests           Global        All domain guests
Domain Users            Global        All domain users
Guests                  Local         Users granted guest access to the domain
MONKEYS                 Global        Users in the Land of Oz
MUNCHKINS               Local         Oz local group
Print Operators         Local         Members can administer domain printers
Replicator              Local         Supports file replication in a domain
Server Operators        Local         Members can administer domain servers
Users                   Local         Ordinary users

   Total of 15 groups

LANDOFOZ\\TINMAN>
```

### 3.2.3 Adding Users to Groups

You can add users to groups in any of the following ways:

- When you use the ADD GROUP command, include the /MEMBERS qualifier.
- When you add a new user (using the ADD USER command), include the /MEMBER_OF_GROUPS qualifier. (See Section 3.1.6, Specifying Group Membership, for more information.)

Local groups can include users from domains other than the one currently being administered. To specify a user account from another domain, a trust relationship must be established that allows the domain being administered to trust the domain where the user account is defined.

To specify a user account or global group in a trusted domain, enter a domain-qualified name (*domain-name*\ *member-name*), such as KANSAS\ DOLE, where KANSAS is the name of the trusted domain, and DOLE is the user or group name defined in the trusted domain. If you omit a domain name, the user or group is assumed to be defined in the domain being administered.

#### 3.2.3.1 Adding Members to a New Group

To add members to a new group, include the /MEMBERS qualifier on the ADD GROUP command. For example, to add a new group MUNCHKINS and specify the group members SCARECROW and STRAWMAN, enter the following command:

```
LANDOFOZ\\TINMAN> ADD GROUP MUNCHKINS/MEMBERS=(SCARECROW,STRAWMAN)
%PWRK-S-GROUPADD, group "MUNCHKINS" added to domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

### 3.2.4 Copying Groups

To simplify creating a new group, you can use the COPY GROUP command to copy an existing group to the new group, with a new name, keeping the members and description from the previous group. For example, to form a new group called QUADLINGS from an existing group called MUNCHKINS, use the following command:

```
LANDOFOZ\\TINMAN> COPY GROUP MUNCHKINS QUADLINGS
%PWRK-S-GROUPCOPY, group "MUNCHKINS" copied to "QUADLINGS" in domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

This command copies the description and group members from MUNCHKINS to the new group named QUADLINGS. You can display information about the new group using the SHOW GROUPS/FULL command. For example, the following command displays the type, description, and members of the QUADLINGS group:

```
LANDOFOZ\\TINMAN> SHOW GROUPS QUADLINGS/FULL

Groups in domain "LANDOFOZ":

Group Name      Type             Description
----------      ------           ------------------------------
QUADLINGS        Local            Oz local group
    Members: [US]LION,[US]SCARECROW

  Total of 1 group

LANDOFOZ\\TINMAN>
```

### 3.2.5 Modifying a Group

You can change the membership or description of an existing group.

#### 3.2.5.1 Adding a Member to an Existing Group

To add a member to an existing group, use the MODIFY GROUP command with the /ADD_MEMBERS qualifier. For example, to add the user LION to the group MONKEYS, enter the following command:

```
LANDOFOZ\\TINMAN> MODIFY GROUP MONKEYS/ADD_MEMBERS=LION
%PWRK-S-GROUPMOD, group "MONKEYS" modified on domain "LANDOFOZ"

LANDOFOZ\\TINMAN> SHOW GROUP MONKEYS

Groups in domain "LANDOFOZ":

Group Name      Full Name       Type     Description
----------      ---------       -------  -----------------------
MONKEYS                         Global   Winged monkeys
    Members: [US]LION

 Total of 1 group)

LANDOFOZ\\TINMAN>
```

#### 3.2.5.2 Removing a Member From a Group

To remove a member from a group, use the MODIFY GROUP command with the /REMOVE_MEMBERS qualifier. For example, to remove SCARECROW from the group MUNCHKINS, enter the following command:

```
LANDOFOZ\\TINMAN> MODIFY GROUP MUNCHKINS/REMOVE_MEMBERS=SCARECROW
%PWRK-S-GROUPMOD, group "MUNCHKINS" modified on domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

#### 3.2.5.3 Changing the Description of a Group

To change the group description, use the MODIFY GROUP/DESCRIPTION command, as in the following example:

```
LANDOFOZ\\TINMAN> MODIFY GROUP MUNCHKINS/DESCRIPTION="First Floor"
%PWRK-S-GROUPMOD, group "MUNCHKINS" modified on domain "LANDOFOZ"
```

### 3.2.6 Deleting a Group

Deleting a group removes only that group; it does not delete user accounts or global groups that are members of the deleted group. You cannot recover a deleted group.

Internally, the Advanced Server recognizes every group by its security identifier (SID), which is used when assigning permissions to a resource. If you delete a group and then create another group with the same group name, the new group does not inherit access to any resources available to the old group because the groups have different SIDs. To delete a group, use the REMOVE GROUP command, as in the following example:

```
LANDOFOZ\\TINMAN> REMOVE GROUP QUADLINGS

Each group is represented by a unique identifier which is independent
of the group name.  Once this group is deleted, even creating an
identically named group in the future will not restore access to
resources which currently name this group in the access control list.
Remove "QUADLINGS" [YES or NO] (YES) : YES
%PWRK-S-GROUPREM, group "QUADLINGS" removed from domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

The command deletes the group QUADLINGS from the LANDOFOZ domain.

# 4

# Managing Directory and File Sharing

You use the ADMINISTER command-line interface to set up files and directories for sharing. To do this, you need to become familiar with the concepts and procedures described in this chapter:

- Section 4.1, Planning Directory and File Sharing, describes how to plan the sharing of directories and files for your users and the access permissions you can set.
- Section 4.2, Administrative Shares, describes the disk administrative resources.
- Section 4.3, Managing Shared Directories and Files, describes how to secure directories and files, share a directory on the OpenVMS system, audit directory and file access, and take ownership of directories and files. It also describes how to manage Advanced Server shares from Windows NT Server computers.
- Section 4.3.11.3, File-Naming Conventions, describes the conventions for Advanced Server file names and how they are stored on the server.

## 4.1 Planning Directory and File Sharing

To serve your users most effectively, you should plan carefully for sharing files and directories. Some projects will require directory sharing, and some groups may need to share only certain files. Use the Shares Worksheet in the *Compaq Advanced Server for OpenVMS Concepts and Planning Guide* to help you set up your shares.

Sharing a directory makes the directory and the files located in it available to other network users. The Advanced Server integrates two levels of permissions for shared files and directories: share permissions, and file and directory access permissions.

- Share permissions specify the maximum access possible for a user or group on all files and directories residing on that share. For example, setting share permissions to Read for the group Everyone would allow all users

to read a file, and prevent any user from altering the contents of the file. You set share permissions using the ADD SHARE and MODIFY SHARE commands. If you do not specify share permissions when you add the share, the default is to allow all users to access the share.

- File and directory access permissions specify the access that a group or user is granted to a particular directory or file in a shared directory. You set file and directory access permissions with the SET FILE/PERMISSIONS command, as described in Section 4.3.6, Specifying File and Directory Access Permissions.

**Note**

When you copy files or directories, security permissions set on them are discarded in addition to ownership and auditing information. The files inherit a new set of permissions from the directory into which they have been copied. If the new directory does not specify permissions for files, only the file's owner (the person who copied the file) will have permission to use the file.

In addition to the two levels of permissions supported by the Advanced Server, the OpenVMS file system imposes a set of protections, which are used if the Advanced Server and OpenVMS security model is enabled. These must be considered when managing shared directories. (For more information, see Section 4.1.2, Advanced Server Security Models.) Shared directories must have the appropriate OpenVMS system protections applied to them if interactive OpenVMS users and other OpenVMS processes need access to them.

### 4.1.1 Disk Resources

The Advanced Server supports the traditional OpenVMS file system, which includes RMS (Record Management Services) and is based on the Files-11, ODS-2 (On-Disk Structure) disk structure. ODS-5 disk volumes are treated as ODS-2 disk volumes. PATHWORKS for OpenVMS (Advanced Server) does not support the extended file system provided by OpenVMS Version 7.2 and higher for ODS-5 disk volumes. The extended file system, which provides Extended File Specifications and deep directories for greater compatibility with the file systems of Windows 95, Windows 98, Windows 2000, and Windows NT file systems, is supported by the Advanced Server for OpenVMS.

Disk resources include the disk devices on a server, the directories on those devices, and the files in the directories. With Advanced Server you can create a share for a directory, including the root directory for a disk, and specify access permissions for the share. Access permissions define the network users or

groups permitted to access the share, and the kinds of operations that each may perform.

You cannot create a share for a file. Users access files through the directory share where the files reside. However, you can set access permissions on shares, directories, and files.

By configuring the server security model, you can enhance access permissions using OpenVMS file protection mechanisms.

### 4.1.2 Advanced Server Security Models

All Advanced Server users have either a network user account or access to the Guest account. The type of access allowed to each user account is determined by the access permissions set on the resource. Each network user account may be mapped to an OpenVMS user account. This mapping enables the Advanced Server to integrate network security with OpenVMS file access security.

You can define the level of integration by setting the server configuration parameter that specifies one of the following security models:

- Advanced Server Only (default)

  Only network security is enforced; OpenVMS access checks are bypassed. Advanced Server Only is the default security model when you install the server software. Unless you change the default parameter setting for the security model, Advanced Server Only security is established on your server. Advanced Server Only security is sufficient for most network environments.

- Advanced Server and OpenVMS

  Both network security and OpenVMS security are enforced. If the user's access request passes the Advanced Server security check, Advanced Server checks the OpenVMS security set on the requested resource, determined by the OpenVMS user account to which the network user account is mapped. Access is granted when the user passes both security checks. For information about how network user accounts are mapped to OpenVMS user accounts, see Section 3.1.16.2, Establishing User Account Host Mapping.

  The Advanced Server and OpenVMS security model is best suited for environments that require the additional control provided by the OpenVMS operating system. For example, this model would benefit systems with legacy OpenVMS data already protected by the elaborate OpenVMS security settings. Rather than having to establish the same security settings at the server level, you could simply give Everyone full control and let OpenVMS security settings determine access. Note that use of

the Advanced Server and OpenVMS security model results in the extra overhead of validating both the Advanced Server and OpenVMS settings.

You can change the security model configuration parameter setting, using the Configuration Manager as described in Chapter 7, Managing Server Configuration Parameters. You can also enable the server to perform dynamic upgrading of network security on files it accesses. Files whose security is specified entirely according to PATHWORKS V5 for OpenVMS (LAN Manager) security are upgraded to PATHWORKS V6 for OpenVMS (Advanced Server) security. For more information, see Section 7.2.5.5, Enabling Dynamic Security Upgrade.

The following sections describe the security models in more detail. Each security model provides the security checks shown in Table 4–1, Security Checks.

**Table 4–1 Security Checks**

| Security Model | Checks Advanced Server Permissions? | Checks OpenVMS Protections? |
|---|---|---|
| Advanced Server Only | Yes | No |
| Advanced Server and OpenVMS | Yes | Yes |

#### 4.1.2.1 Advanced Server Only Security Model

Whether the Advanced Server grants or denies a file access request depends on three factors:

- The security model in effect on the server
- Permissions established for the group of which the user is a member
- Permissions established for the user

To effectively implement the Advanced Server Only security model, keep the following in mind:

- Network users cannot use a directory or file unless they have been granted permission to do so or belong to a group that has permission to do so.
- Share permissions are cumulative, except that the No Access permission overrides all other permissions. For example, the MUNCHKINS group has Write permission for a file and the WINKIES group has only Read permission. User SCARECROW is a member of both groups; therefore, SCARECROW is granted Read and Write permission.

If you change the WINKIES group's permission for the file to No Access, SCARECROW cannot use the file even though he is a member of the MUNCHKINS group, which still has access to it.

- The user who creates a file or directory is the owner of that file or directory. The owner can always control access to the file or directory by changing the permissions set on it. Network administrators can always take ownership of a file or directory.

  For files and directories that existed on an OpenVMS device before the share was created, the owner of the file or directory is set to be the user who created the share.

- The easiest way to administer security is by setting permissions for groups, not individual users. Typically, a user needs access to many files. If the user is a member of a group that has access to the files, you can end the user's access by removing the user from the group rather than changing the permissions on each of the files.

**4.1.2.1.1 Windows NT Security Descriptors** As enforced by the Advanced Server Only security model, network security uses Windows NT security descriptors for each shared directory and file.

A Windows NT security descriptor contains information such as the Windows NT owner of the file and a list of Windows NT users and groups with their respective access levels for that file.

These descriptors are stored in OpenVMS application access control entries (ACEs) that are included in the OpenVMS access control lists (ACLs) associated with the file.

#### 4.1.2.2 Advanced Server and OpenVMS Security Model

In this security model, OpenVMS security is enforced in addition to the Advanced Server security model. The OpenVMS security is based on the OpenVMS user account to which the network user is mapped.

An OpenVMS account identifies a user to the OpenVMS operating system. The account includes the user's name, a password, privileges, and access to directories and files associated with the account. Network user accounts are associated with OpenVMS user accounts by means of host mapping. For more information about host mapping, see Section 3.1.16, User Account Host Mapping.

OpenVMS stores a security profile for each directory or file. The security profile contains the following types of information:

- User identification code (UIC) of the owner of the object (file, directory, or device). The system uses this element to help interpret the RMS protection code.
- Protection code defining access to objects (files, directories, or devices) based on categories of system, owner, group, and world. This protection code controls broad categories of users.
- The access control list (ACL) identifying the users and groups allowed or denied access to the file or directory. The ACL contains an entry for each user and group. These entries are called access control entries (ACEs).

In short, the OpenVMS operating system provides two methods of assigning protection to files and directories:

- RMS protections (see Section 4.1.2.2.1, RMS Protections)
- Access control lists (ACLs) (see Section 4.1.2.2.2, Access Control Lists (ACLs))

**4.1.2.2.1 RMS Protections** RMS sets protection on files and directories based on user identification codes (UICs). A UIC consists of a group code and a user code assigned to every OpenVMS user by the system administrator. The user's UIC determines which categories a user belongs to. Table 4–2, OpenVMS Group Codes, lists and describes the group codes.

**Table 4–2 OpenVMS Group Codes**

| UIC Category | Includes |
|---|---|
| System (S) | Users with SYSTEM privileges (the OpenVMS privilege SYSPRV) or users with low group numbers in their UICs, as determined by the system administrator. |
| Owner (O) | The user who is the owner of a file or directory. The user code of the UIC associated with the file or directory matches the user code of the UIC of a user. |
| Group (G) | All users who have the same group code in their UICs. |
| World (W) | All users regardless of UIC. |

RMS assigns file protections for each of these categories according to the following format:

- R for read-only access
- W for write access

- E for execute access
- D for delete access

The default protections for directories and files are listed in Table 4–3.

**Table 4–3 Default Values for RMS File and Directory Protections**

| Protections | RMS Protection Codes |
|---|---|
| Directory | S: RWED, O: RWED, G: RWED, W: RE |
| File | S: RWD, O: RWD, G: RWD, W:R |

For directories, this RMS protection allows read, write, execute, and delete access to the system, owner, and group; and read and execute access to the world. For files, the RMS protection allows read, write, and delete access to the system, owner, and group; and read access to world.

The administrator can change the RMS protection on a specific share by using the ADMINISTER MODIFY SHARE command with the /HOST_ATTRIBUTES qualifier to set the file and directory protections. For example,

```
$ ADMINISTER MODIFY SHARE share-name -
_$ /HOST_ATTRIBUTES=(DIRECTORY_PROTECTION=(O:WRE,G:WR,W:R), -
_$ FILE_PROTECTION=(O:WRED, G:WR, W: R))
```

**Note**

Because share data (such as host attributes) is cached when the first client accesses the share, the changes made to share protections are not reflected until either all users are disconnected from the share or the Advanced Server is restarted.

**4.1.2.2.2 Access Control Lists (ACLs)** An access control entry (ACE) is an entry in an access control list (ACL) that controls access to files and directories by resource identifiers. ACLs give you more control than RMS protections. For example, with RMS, the only way to grant READ access to users in different UIC groups is to grant World Read (W:R) access. In contrast, with ACLs, you can provide users from several UIC groups with access to a file or directory without granting World access, and you can deny specific users access to specific files.

If you use both RMS protections and ACLs, OpenVMS checks ACEs in the ACLs before it checks the RMS protections. For more information about RMS protections and ACLs, refer to the *OpenVMS System Manager's Manual*.

## 4.1.3 The Advanced Server and Windows NT Security Information

The Advanced Server supports both OpenVMS and network security, and ownership information. It achieves this by storing Windows NT security descriptors for directories and files on OpenVMS disk devices. (For more information on Windows NT security descriptors, see Section 4.1.2.1.1, Windows NT Security Descriptors.

The following sections explain how the Advanced Server handles file security information and describes utilities you can use to manipulate this information.

### 4.1.3.1 Inheritance of Directory Permissions

Each Windows NT directory has two sets of permissions: (A) directory-specific security permissions that provide access control to the directory itself and (B) inheritable permissions that will be inherited automatically by any file created in that directory, becoming the default access permissions for that new file.

The Advanced Server is designed to conform with Windows NT security behavior. When you create a file in a shared directory, the parent directory's inheritable permissions (B) are propagated to that file to become the file's access permissions. When you create a subdirectory, both the parent directory's access control permissions (A) and inheritable permissions (B) propagate to the subdirectory becoming the subdirectory's access control (A) and inheritable permissions (B), respectively.

### 4.1.3.2 Inheritance of Ownership

In conformance with Windows NT security behavior, Advanced Server security is designed to assign ownership of a file or directory to the user who creates the file or directory. The owner can always control access to the file or directory by changing the permissions set on it.

### 4.1.3.3 ACEs and OpenVMS Volume Index Files

Every OpenVMS file has a file header block stored in the volume index file, INDEXF.SYS. Each file header is limited to 512 bytes. The ACL for a file is stored in the file's header. When a file contains several ACEs, it may exceed the 512-byte limit, and a secondary file header (known as an extension file header) is allocated.

When a file has a large number of "PATHWORKS" ACEs (displayed as PATHWORKS ACES, these are ACEs created by Advanced Server or PATHWORKS servers; see Section 4.1.3.8, Displaying Advanced Server for OpenVMS and PATHWORKS ACEs), the secondary headers required to store the ACEs will consume additional space in the index file. As the index file extends to provide more headers, the space available for other files is reduced, and the index file itself becomes fragmented. In addition, there is a limit to

the number of times the index file can be extended. Its header can become full from mapping its own multiple extensions.

You can reduce the number of ACEs by using local groups in permissions lists for files and directories, rather than by adding individual users or global groups. Ideally, each file and directory permissions list should reflect only local groups, and no two entries in a permissions list should duplicate the same permissions. The Advanced Server can help reduce the number and size of the ACEs created, and thereby reduce the consumption of index header blocks used for secondary headers.

For example, the file server parameter **Store_Security_Aces** allows you to control the amount of Windows NT security information stored with the file at file creation. By default (parameter value equals YES), the file server writes a complete set of Windows NT security information to a new file. By changing the value of the **Store_Security_Aces** parameter to NO, only the ownership information is represented in the file's ACL, excluding all the file access permission ACEs. For more information about this parameter, see Section 4.1.3.6, Streamlining Security Information Storage and Lookups. This can make more efficient use of disk space.

Note that there are tradeoffs for using the **Store_Security_Aces**=NO setting. For example, while conserving disk space, additional run-time is required to determine access permissions for files that do not have explicit access permissions associated with them. Section 4.1.3.6, Streamlining Security Information Storage and Lookups, discusses the tradeoffs in more detail, and explains how to recover from over consumption of disk space caused by oversized file security descriptors (excessive ACEs on a file) or inappropriate propagation of ACEs to files.

#### 4.1.3.4 How the File Server Reads Windows NT Security Information on Files

When a client accesses a shared file whose ACL contains the complete Windows NT security descriptor information (that is, owner, group, discretionary access control lists (DACLs) and system access control lists (SACLs)), then the Advanced Server uses that information to determine the access rights to the file.

If the file lacks any or all of the required Windows NT security descriptor information, the file server builds a complete security descriptor for the file, getting the required security descriptor information from the directory hierarchy above the file. (A file lacks all Windows NT security information if it was not created by an Advanced Server for OpenVMS or by a PATHWORKS Advanced Server; an example is a file that was created on an OpenVMS system before the directory became shared.)

If, for example, a file has owner information but no group, DACL, and SACL information, the server looks up the directory structure, level by level, as far as the device root, but a maximum of up to 15 levels, until it finds enough information to build a complete Windows NT security descriptor for that file. If nothing is found in the search all the way to the root, the server creates a default descriptor for the file in which Everyone has full access control.

The file server might not find all the required file security information at the same directory level. In some cases, it might extract the information from several different directory levels.

For example, given a file with no security information available, the server might find the owner information in the file's parent directory, but then have to search up one or more additional directory levels to find the other information. When the file server finds a directory that has the Windows NT security descriptor information it is seeking, it inserts the needed information in the file's security descriptor. The owner of the file was already determined from the file's parent directory: the file server does not use the higher directory's ownership for the file's security descriptor.

In summary, the file server must determine the access rights for a file in these circumstances:

- If the complete Windows NT security descriptor is explicitly stored in a file's ACL, the file server uses this information to determine a user's access rights (without needing to look up the directory structure to determine additional Information).
- If the file has no security information, the file server looks up the directory structure for the information required to build the file's Windows NT security descriptor. If no security information is found in the directory hierarchy (from that file's parent directory up to the device root), the server creates a default security descriptor for the file, giving Everyone access to the file.
- If the file has some but not all of the security information in its security descriptor, the file server looks up the directory structure for the missing information.
- When searching up the directory structure for the needed information, the file server might either:
  - Find all the information at the parent directory level, or if none is available there, all at a higher directory level
  - Find part of the information at one level, and pull the rest of the missing information from one or more levels above that level

– Not find the information at all (searching in vain up to the device root level)

#### 4.1.3.5 How the Advanced Server File Server Builds File Security Descriptor Information

One subtle difference exists in how and when the Advanced Server and Windows NT build security information for a file. By default, both the Advanced Server and Windows NT are designed to write complete security information for a file when the file is created, propagating it from the parent directory as necessary. However, the Advanced Server file server allows you to change this default behavior to make more efficient use of security information and disk space. For more information, see the discussion of the **Store_Security_Aces** parameter in Section 4.1.3.6, Streamlining Security Information Storage and Lookups.

As a result of making this change, when a file is created in a shared directory, only the owner information is stored with the new file. When a user attempts to access the file, the server uses security information from the parent directory structure to dynamically build a Windows NT security descriptor for the file. The file server does not modify the file or the security information stored with the file in any way.

After the file server has used the dynamically built Windows NT security descriptor to determine whether the user has permission to access the file, the dynamically built Windows NT security descriptor is discarded. The next time a client attempts to access the file, the file server again dynamically builds a Windows NT security descriptor to determine the access permission for the file.

A significant consequence of this behavior, which is unique to the Advanced Server file server, is that the file security information for a file (whose security descriptor is built dynamically) can change when the security information in the directory structure above it changes. For example, assume a directory named ACCOUNT is owned by user JOHNSON and has full access for Everyone. User CARTER creates file CABINET in that directory. On a Windows NT system, the new file's security descriptor will include:

- CARTER as owner (creator gets ownership)
- Full access for Everyone (permissions inherited from the parent directory, ACCOUNT)

By default, the same would be true on an Advanced Server share. But, if the **Store_Security_Aces** parameter is changed from the default YES to NO, the security descriptor for file CABINET sets CARTER as the owner but does not store any access rights information. Nevertheless, when a client attempts to access the file CABINET, the file server dynamically determines that access to

file CABINET is full access for Everyone (determining the access permissions from the parent directory, ACCOUNT).

If the access permissions for the ACCOUNT directory are changed to read access for Everyone, then on a Windows NT system, and by default, on an Advanced Server share, the access for file CABINET remains full access for Everyone (as originally inherited from the parent directory when CABINET was created). But, if the value of the Advanced Server **Store_Security_Aces** parameter is NO, the access for the shared file CABINET would be READ access for Everyone: the access permissions were not stored with CABINET at file creation, so the server builds the file's security descriptor dynamically, determining the file's access permissions from the parent directory, ACCOUNT.

#### 4.1.3.6 Streamlining Security Information Storage and Lookups

As noted previously, the default propagation of security information to new files in shared directories can require that secondary headers be allocated for these files to store the security ACEs. Over time, this excessive consumption of file headers can cause excessive growth of the volume's index file, reducing the disk space available for creating new files. Techniques for minimizing file header usage are described later on in this section.

If disk space is not a problem, multiple extensions of the index file can still fragment the file across the volume, making access to the file headers less efficient, and eventually making further extension of the index file impossible. The solution is to make the index file contiguous, and make it large enough to help eliminate the need for further extensions in the future. However, be sure not to make the index file too large, or else space will be wasted.

You can make the volume and all of its files (including the index file) contiguous by performing a simple backup and restore of the volume. In addition, before doing the restore, you can initialize the volume with a larger index file, if appropriate. However, there is currently no easy way to determine how much the index file has grown, how many times it has grown (how fragmented it has become), or how many free headers it currently contains. For details on making the index file contiguous and estimating an appropriate size for the index file, see Section 4.1.3.6.1, Managing the Index File on a Volume with Shared Files.

If consumption of disk space is a problem, you can change the LANMAN.INI **Store_Security_Aces** keyword's value to NO. The default value (YES) causes the file server to write a complete set of Windows NT security information to a new file's ACL. By changing the keyword value to NO, you limit the amount of security information stored with the new file: only the ownership information is represented in the file's ACL, and all the file access permission

ACEs are excluded. This keyword is stored in the VMSSERVER section of the LANMAN.INI file.

Note the tradeoffs between using the default (YES) or changing the parameter to NO, described in Table 4–4. In short, setting the parameter to NO saves file header usage but might result in increased file access times. Because the security information is not propagated to the files in a directory, the file server must look up the directory tree to determine missing information.

**Table 4–4 Tradeoffs Regarding the STORE_SECURITY_ACES Parameter Settings**

| | If using the default (store all security information) | If setting to NO (store owner information only) |
|---|---|---|
| Server Behaves as Windows NT does? | Yes | No |
| Performance | Faster | Slower |
| File Header Usage | Higher | Lower |
| How Security Settings Are Determined | Direct from files | Dynamically, using the file's directory tree |

If security problems arise because of inappropriate ACEs on files, or if you want to minimize consumption of disk space by index blocks required for storage of ACEs, use the Advanced Server utility SYS$SYSTEM:PWRK$FIXACE.EXE. This utility optimizes disk storage by compressing ACEs, removing unnecessary ACEs, and preventing ACEs from being propagated to files created in shares.

Invoke this utility as follows:

```
$ MCR PWRK$FIXACE
```

In addition, you can clean up unwanted ACEs by using the PWRK$DELETEACE utility, as documented in Section 4.1.3.7, Removing PATHWORKS ACEs. This utility will help you reclaim disk space.

#### 4.1.3.6.1 Managing the Index File on a Volume with Shared Files

This section provides examples of the image backup and restore operations that make the index file (and all other files) on a volume contiguous.

To make the index file on a volume contiguous, follow these steps. For details, refer to the *OpenVMS System Manager's Manual*.

1. Perform an image backup of the volume, using the OpenVMS DCL BACKUP/IMAGE command.
2. If a larger index file is indicated, manually reinitialize the volume, using the /HEADERS qualifier to specify an appropriate value for the number of headers to allocate. For more information about how to determine the appropriate value, see Section 4.1.3.6.2, Determining the Number of Index File Headers to Allocate.

   ```
   $ INITIALIZE/HEADERS=n disk_volume:
   ```

3. Restore the backup using the OpenVMS DCL BACKUP/IMAGE command. If the disk was manually initialized in step 2, then the /NOINITIALIZE qualifier is also necessary to preserve the new index file size.

#### 4.1.3.6.2 Determining the Number of Index File Headers to Allocate

This section explains how to determine whether a larger index file is indicated, and if so, how many file headers to specify with the INITIALIZE/HEADERS command. As stated previously, there is no easy way to determine how much the index file has grown, how fragmented it has become, or how many free headers it currently contains.

You can estimate whether the index file should be made larger by monitoring the size of the index file and the total count of all shared files on the volume. Suppose you observe that an index file is growing rapidly, most likely because of an increase in the number of shared files on the volume. If you can estimate how much the number of shared files might grow in the future, you can calculate how much larger the index file might become as well. From this value, you can approximate the total number of headers to specify.

If you suspect that the index file is fragmented, but have no data to support any estimates, you may still perform the image backup and restore without changing the index file size, and then start monitoring the volume as described above.

For example, assume earlier monitoring revealed these results:

```
$ DIRECTORY/SIZE DKB0:[000000]INDEXF.SYS

Directory DKB0:[000000]

INDEXF.SYS;1           24426

Total of 1 file, 24426 blocks.

$ DIRECTORY/GRAND_TOTAL DKB0:[SHARE_DIRECTORIES...]

Grand total of 56 directories, 13512 files.
```

Assume current monitoring reveals the following results:

```
$ DIRECTORY/SIZE DKB0:[000000]INDEXF.SYS

Directory DKB0:[000000]

INDEXF.SYS;1           90704

Total of 1 file, 90704 blocks.

$ DIRECTORY/GRAND_TOTAL DKB0:[SHARE_DIRECTORIES...]

Grand total of 73 directories, 37182 files.
```

Then you can calculate the increase in file count and the associated increase in the size of the index file. In this example, these calculations are as follows:

```
Shared file count increase = 37,182 - 13,512 = 23,670 files
Index file size increase   = 90,704 - 24,426 = 66,278 blocks.
```

If you estimate that the number of shared files will grow to 120,000 in the lifetime of the current configuration, then the number of files will have increased by 82,818 files (subtract 37,182 from 120,000).

From that calculation, you can estimate the index file growth by use of simple proportions, where the ratio of the projected file count increase to the projected index file header increase (*n*) is equal to the ratio of the observed file count increase (23,670 files) to the observed index file header increase (66,278 blocks):

```
82,818    23,670
------  = ------
  n       66,278
```

Thus, the projected index file header increase (*n*) is calculated as follows:

```
      82,818 * 66,278
n  =  ---------------  =  231,897 blocks
          23,670
```

The total size of the future index file will then be its current size plus the projected increase, or:

$$24,426 + 231,897 = 256,323\ blocks$$

Given that each file header occupies one disk block, and assuming for simplicity that the entire index file consists of file headers (this is an overestimation), the total number of headers needed in the future is 256,323. Thus, to initialize the volume, you would specify this value for the /HEADERS qualifier in the INITIALIZE command mentioned in step 2 in the preceding section.

You can also apply this same reasoning independently to any other product that maintains a large number of files on the volume, such as MAIL or ALL-IN-1, or products such as POLYCENTER HSM (Hierarchical Storage Management) for OpenVMS that maintain file headers in INDEXF.SYS when shelving specified files.

#### 4.1.3.7 Removing PATHWORKS ACEs

To remove some or all ACEs associated with Advanced Server for OpenVMS and PATHWORKS products, use the SYS$SYSTEM:PWRK$DELETEACE.EXE utility provided with the Advanced Server software.

The PWRK$DELETEACE utility allows you to selectively remove:

- PATHWORKS and Advanced Server for OpenVMS file attribute ACEs (the utility refers to these ACEs as "PW ACEs"). When you display file ACEs (see Section 4.1.3.8, Displaying Advanced Server for OpenVMS and PATHWORKS ACEs), these begin with "UNKNOWN=%X80" and are used by Advanced Server for OpenVMS, PATHWORKS V6 for OpenVMS (Advanced Server), and PATHWORKS V5 for OpenVMS (LAN Manager) to store file attributes and dates. These ACEs should be removed only on files that are no longer accessed by the server.
- Advanced Server for OpenVMS and PATHWORKS V6 for OpenVMS (Advanced Server) security ACEs. These ACEs begin with "UNKNOWN=%X86" and are used to store Windows NT-style security information, such as owner, DACL, and SACL.
- PATHWORKS V5 for OpenVMS (LAN Manager) security ACEs. These begin with "UNKNOWN=%X82".
- PATHWORKS V4 ACEs. V4 ACEs begin with "IDENTIFIER =PCFS$READ", "IDENTIFIER=PCFS$UPDATE", or "APPLICATION".
- PATHWORKS for OpenVMS (Macintosh) comment ACEs (the utility refers to these as "AFP Comment ACEs").

The following example shows how the PWRK$DELETEACE utility works:

```
$ MCR PWRK$DELETEACE
Exit=x File Spec: DKA200:[LMSHARES.CSCSEC]*.*
Cancel=x Delete V4 ACEs Y/N: Y
Cancel=x Delete PW ACEs Y/N: Y
Cancel=x Delete V5 security ACEs Y/N: Y
Cancel=x Delete V6 security ACEs Y/N: Y
Cancel=x Delete AFP Comment ACEs Y/N: Y
DKA200:[LMSHARES.C CSCSEC]DEFAULT_SECURITY.EXAMPLE;1  ACEs removed
DKA200:[LMSHARES.CSCSEC]NEW__20FOLDER.DIR;1           ACEs removed
DKA200:[LMSHARES.CSCSEC]WYSIWYG.EXAMPLE;1             ACEs removed
Exit=x FileSpec: x
$
```

#### 4.1.3.8 Displaying Advanced Server for OpenVMS and PATHWORKS ACEs

On OpenVMS Version 6.2 systems, you can display information about PATHWORKS ACEs by using the DCL SHOW SECURITY, DIRECTORY/SECURITY, or DIRECTORY/FULL command for files that contain ACEs. On OpenVMS Version 7.1 and later systems, if you use any of these commands for files containing PATHWORKS ACEs, the hexadecimal representation for each ACE is not displayed. Instead, the commands summarize the total number of ACEs encountered for each file in this message:

"Suppressed *n* PATHWORKS ACES."

To display the suppressed ACEs, use the DCL DIRECTORY command with the /NOSUPPRESS qualifier along with either the /FULL, /SECURITY, or /ACL qualifier.

### 4.1.4 Controlling User Access to Disk Resources

By default, when a directory is shared, all users have full access to the share. To control user access to disk resources, you can assign users to the groups that have the appropriate access permissions, or you can assign permissions directly to shares. Administratively, it is easier to use group permissions than user permissions to grant access.

You can set or modify the permissions at the share level (using the ADD SHARE/PERMISSIONS= or MODIFY SHARE/PERMISSIONS= command). You can also assign permissions to specific files or directories within a shared directory (using the SET FILE/PERMISSIONS= command).

Share permissions determine which users can access the shared directory or file, and the type of access those users are allowed. These permissions control network access to the directory or file.

In general, the simplest method to control access to disk resources is to assign FULL access for Everyone to the share (the default), and then restrict access at the directory or file level with the SET FILE command. For more information, see Section 4.3.5, Planning File and Directory Access Permissions, and Section 4.3.6, Specifying File and Directory Access Permissions.

#### 4.1.4.1 Administrator Access

Server administrators can access all resources shared on a server, but only if they have the appropriate access permissions set for those resources. Access permissions apply to administrators as well as ordinary users. However, network administrators can always take ownership of a file or directory.

#### 4.1.4.2 Group Access

If a user belongs to two groups, both of which are assigned access permissions for a resource, then that user has all access permissions assigned to both groups. For example, if the MUNCHKINS group has RW (Read and Write) access permission and the WINKIES group has E (Execute) access permission for the resource REPORTS, then a user who is a member of both groups has RWE access permissions for that resource. A user account that is a member of a group that has been denied access gets no access. (See Section 3.2, Managing Advanced Server Groups, for more information about network groups.)

#### 4.1.4.3 User Access

If you assign access permission explicitly to a specific user, that user has only that access permission, regardless of the permissions assigned to any groups that include that user. For example, a user who is a member of the groups MUNCHKINS and WINKIES, but who has been assigned only R (Read) access permission for the share GREATOZ has only Read permission for GREATOZ. If the user is also in a group denied access, the user has no access.

#### 4.1.4.4 Access Checks

In general, the ability to connect to a resource does not guarantee the ability to perform operations with that resource. If the user name and password match an account in the security accounts database, the user is granted access based on the permissions set on the resource. If the user name is invalid, the user may be able to access the resource as a Guest.

If the resource is a file or directory, the server performs the following checks:

1. For a file, the server checks access permission on the file and the share. Both the file and the share must grant the requested access. If access is permitted, the server continues to step 2. If the check fails at any level, the server denies access.

2. If the Advanced Server and OpenVMS security model is enabled, the server verifies OpenVMS access to the resource based on the host mapped OpenVMS user name.

## 4.2 Administrative Shares

The Advanced Server automatically creates special shares for administrative and system use. Only network administrators can change their properties. Table 4–5, Network Administrative Shares, lists some of the default shares created when the software is installed.

**Table 4–5 Network Administrative Shares**

| Share Name | Type | Description |
|---|---|---|
| ADMIN$ | Directory | The Admin share, a special administrative resource for remote administration. |
| C$ | Directory | The root share, an administrative resource that provides a connection to the root of the directory tree containing the Advanced Server's data files. On an Advanced Server, C$ is equivalent to PWRK$LMROOT:[000000]. |
| IPC$ | IPC | The IPC share, an administrative resource that supports interprocess communication. |

A server's administrative shares allow network administrators to perform certain tasks on the server, including examining the shares, administering the server remotely, and running distributed applications.

Administrative shares include ADMIN$, IPC$, and disk administrative shares. They are hidden from most network users; only administrators can see information about them using the ADMINISTER command-line interface. To display information about hidden shares, including administrative shares, include the /HIDDEN qualifier on the ADMINISTER command SHOW SHARES. For example:

```
LANDOFOZ\\TINMAN> SHOW SHARES/HIDDEN

Shared resources on server "TINMAN":
```

```
Name           Type       Description
------------   ---------  ----------------------------------------
ADMIN$         Directory  Admin Share
ALP072$        Directory
C$             Directory  PATHWORKS share
IPC$           IPC        IPC Share
NETLOGON       Directory  Logon Scripts Directory
PAGE_TINMAN$   Directory
PWLIC          Directory  PATHWORKS Client License Sftwr
PWLICENSE      Directory  PATHWORKS Client License Sftwr
PWODS5$        Directory
PWROOT$        Directory
PWTEST         Directory
PWUTIL         Directory  Adv. Srv. Client-based Utilities
USERS          Directory  Users Directory

  Total of 13 shares
```

The following sections explain the function of each administrative share and compare how these shares are shared.

### 4.2.1 The ADMIN$ Share

The ADMIN$ share controls access to server administration functions. A server's ADMIN$ share must be shared if that server is to be administered remotely. When a server starts, Advanced Server automatically shares ADMIN$. You cannot stop sharing the ADMIN$ share.

When you begin an administration session, Advanced Server makes a connection to the ADMIN$ share.

### 4.2.2 The IPC$ Share

The IPC$ share controls interprocess communication, such as communication between different components of a program, different computers running parts of a single program, or two programs working together. In the Advanced Server environment, interprocess communication occurs when a user or administrator:

- Views a list of a server's available resources
- Administers the server remotely
- Runs a distributed application

Servers share the IPC$ share automatically. You cannot stop sharing the IPC$ share. When the IPC$ share is needed, Advanced Server makes a connection to it automatically.

### 4.2.3 Disk Administrative Shares

The Advanced Server automatically defines disk devices as shares by offering all mounted disk devices as autoshares (automatic shares) at server startup time. An autoshare points to the top-level (root) directory on the disk. For example, if you connect to the autoshare USER1_DISK$, a volume label, you access the directory USER1_DISK:[000000].

Only administrators can connect to disk administrative resources. Such connections allow access to all directories and files on the disk. Administrators working at remote servers or clients cannot make these connections if the ADMIN$ and IPC$ resource are not shared.

#### 4.2.3.1 Autoshare Names

The Advanced Server creates an autoshare name using the OpenVMS volume label of the associated OpenVMS disk device. Autoshare names must conform to network resource naming restrictions (no more than 11 characters), with the last character a dollar sign ($), which identifies the share name as a hidden share.

**Note**

The autoshare name C$ is reserved. By default, Advanced Server defines C$ as an autoshare alias for PWRK$LMROOT:[000000]. If you define another volume as C$, the share name will be rejected.

When you create shares for directories using the ADMINISTER ADD SHARE command, you can specify any of the following for the device name in the share path:

- The autoshare name
- The physical device name
- An OpenVMS device logical name (search lists are not supported)

For more information, see Section 4.3.2, Creating a Share.

Note that when a logical name is specified for the device in the share path, if you need to move the share later to another device, you simply assign the same logical name to the new device when you mount the device. Then users can continue to access the same share in the new location, as if nothing had changed.

#### 4.2.3.2 Defining Autoshares

Sometimes the autoshare name created by the Advanced Server is not ideal for the situation. The Advanced Server lets you define your own autoshare names. This is useful when:

- You have a disk device whose volume label exceeds the 11-character limit.
- You want to map a server device to a single letter to accommodate the DOS disk device-naming convention.
- You do not want to autoshare some devices.

The server cannot define devices with volume labels that exceed the 11-character limit as autoshares. When the server starts, disk devices with volume labels that exceed the limit are not shared, and an event is recorded in the Advanced Server log file, which is viewable with the ADMIN/ANALYZE command. (For information about using the ADMIN/ANALYZE command, see Section 6.1.4.2, The Advanced Server Common Event Log.)

You use the **Autoshare** keyword in the LANMAN.INI file to define autoshare names for the server to create in addition to the autoshares that the server creates automatically. Use the **NoAutoshare** value to specify the names of devices that you do not want to autoshare.

The **Autoshare** and **NoAutoshare** parameters function as follows:

- If a device is listed in the **NoAutoshare** parameter, that device is not shared and cannot be accessed by the Advanced Server. Existing shares on the device are no longer accessible.
- If a device is listed in the **Autoshare** parameter, that device is shared and mapped to the specified autoshare name. If the length of the device volume label is 11 characters or less, the device will also be shared using the label name.
- If a device is not specified in either the **NoAutoshare** or **Autoshare** parameter, the Advanced Server creates a default autoshare using the volume label (as long as the volume label does not exceed the 11-character name limit). For a disk with a volume label longer than 11 characters, the Advanced Server does not create a disk administrative share, and the device is not accessible to the Advanced Server.

If you are running Advanced Server in an OpenVMS Cluster environment, see Section 4.2.3.6, Autosharing in an OpenVMS Cluster Environment, for information about defining autoshares and preventing autoshare creation on specific nodes in the cluster.

#### 4.2.3.3 The Autoshare Parameter

The **Autoshare** keyword in the LANMAN.INI file specifies an alias for the autoshare name created by default for an OpenVMS disk device. Advanced Server creates an autoshare for each mounted OpenVMS disk device when the server starts. To create a more meaningful share name or to map the device name to a DOS format, use the **Autoshare** keyword in the LANMAN.INI file.

The format of the data associated with the **Autoshare** value is as follows, where *devname_n* is the device name (such as DUA2:), and *sharename_n* is the name of the autoshare:

*devname_1=sharename_1, . . . , devname_n=sharename_n*

For example, the following line specified in the LANMAN.INI VMSSERVER section creates an autoshare named M$ for device DOT$DUA2:, and an autoshare named WORK5$ for device DOT$DUA3:.

```
AUTOSHARE = DOT$DUA2=M,DOT$DUA3=WORK5
```

As shown in this command example, when adding multiple entries, delimit each entry in the list with a comma. Note that the share name cannot exceed 11 characters. In addition, do not append a dollar sign ($) to the device name; the Advanced Server does this automatically.

Table 4–6, Sample Default Autoshare Names, shows physical device names and volume labels for disk devices mounted on node DOT and the autoshare names that the Advanced Server creates by default.

**Table 4–6 Sample Default Autoshare Names**

| Device | Volume Label | Autoshare Name |
|---|---|---|
| DOT$DUA0: | AXPVMS072 | AXPVMS072$ |
| DOT$DUA1: | USERS_1 | USERS_1$ |
| DOT$DUA2: | USERS_2 | USERS_2$ |
| DOT$DUA3: | WORK_DISK055 | None: the volume label exceeds the 11-character limit. |

For example, the values associated with the **AutoShare** keyword in the LANMAN.INI file appear as follows:

```
DOT$DUA2=M
DOT$DUA3=WORK5
```

The **Autoshare** parameter directs the Advanced Server to create an autoshare named M$ for device DOT$DUA2: and an autoshare named WORK5$ for device DOT$DUA3:. If an administrator maps a network drive to the hidden share name M$, administrators connecting to M$ are accessing DOT$DUA2:[000000]. When you display the list of hidden shares, these autoshare names will also be listed. These autoshare names may also be used in share paths when creating directory shares.

As shown in Table 4–6, Sample Default Autoshare Names, the Advanced Server did not create an implicit autoshare for the device DOT$DUA3:, because the volume label WORK_DISK055 exceeds the 11-character limit. But Advanced Server allows you to include the device name (DOT$DUA3) in the autoshare list in the LANMAN.INI file and creates the explicit autoshare WORK5$ for DOT$DUA3:.

#### 4.2.3.4 The NoAutoshare Parameter

The **NoAutoshare** parameter specifies the OpenVMS device names that should not be automatically shared or available to the Advanced Server. If a device is listed in both the **Autoshare** list and the **NoAutoshare** list, the **NoAutoshare** definition takes precedence.

If the server configuration includes many disk devices, you may want to specify which devices are not shared automatically. By sharing some devices and not sharing others, you can separate OpenVMS disk resources from Advanced Server resources and reduce unnecessary resource consumption by the server.

The **NoAutoshare** parameter value is a comma-delimited list of implicit wildcard device references. For example, the following data associated with the **NoAutoshare** keyword in the LANMAN.INI file specifies search strings DFS*, DAD*, and PWRK$DKB1*:

```
DFS,DAD,PWRK$DKB1
```

With this data, any OpenVMS device names that begin with the strings DFS, DAD, or PWRK$DKB1 are not autoshared. If you want to exclude a specific device and negate the use of the wildcard, include the colon in the device specification. For example, the **NoAutoshare** value PWRK$DKB1: will always apply to a single device, while the value PWRK$DKB1 can apply to many devices, such as PWRK$DKB100:.

#### 4.2.3.5 Sharing DECdfs Devices

DECdfs is a DECnet-based layered product that provides OpenVMS users with the ability to use remote disks as if they were directly attached to the local system. By default, Advanced Server does not automatically share devices managed by DECdfs. The LANMAN.INI file contains the following default values associated with the **NoAutoshare** keyword:

```
DAD,_DFS
```

You cannot assign permissions to DECdfs devices; therefore, if you override the default and allow the Advanced Server to create an autoshare for a DECdfs device, users with user or operator privileges cannot access that device. Access to a shared DECdfs device is restricted to users in the Administrators group.

#### 4.2.3.6 Autosharing in an OpenVMS Cluster Environment

OpenVMS disk devices mounted clusterwide are offered to users as shared devices (autoshares) by all server nodes in an OpenVMS Cluster system. Devices mounted on a specific server (not clusterwide) are accessible to users connected to that server only.

The LANMAN.INI file contains two types of keywords to define autoshares:

- **Autoshare** and **NoAutoshare**
- **Autoshare**_*nodename* and **NoAutoshare**_*nodename*

In an OpenVMS Cluster system, you can make a device available clusterwide by using the **AutoShare** value. You can restrict device availability using the **NoAutoshare** value.

In addition, you can control the devices to be automatically shared on a single node in the cluster, using the **Autoshare**_*nodename* and **NoAutoshare**_*nodename* values.

The following examples show how you can share disk devices in an OpenVMS Cluster. For this example, the cluster contains two members: DOT and TINMAN.

- On both DOT and TINMAN, the following value is defined:

  ```
  Autoshare = PCS524$DKA100=J,PCS524$DKA200=K
  ```

- On the cluster member named DOT, the following value is defined:

  ```
  Autoshare_DOT = DUA1001=H,DUA1002=G,DUA1006=I
  ```

- On the cluster member named TINMAN, the following value is defined:

```
Autoshare_TINMAN = DUA1001=H,DUA1002=G

NoAutoshare_TINMAN = DUA1006
```

In this example:

- PCS524$DKA100 and PCS524$DKA200 are available as shared devices on autoshares J: and K: on all OpenVMS Cluster server nodes.
- DUA1001 and DUA1002 are available as shared devices on autoshares H: and G: on server nodes DOT and TINMAN, respectively.
- DUA1006 is available as a shared device on autoshare I: on node DOT only.

The Advanced Server compares the clusterwide definitions with the node-specific definitions. If the same device is listed in both the clusterwide and node-specific **Autoshare** parameters, the clusterwide definition prevails. The **NoAutoshare** parameter uses the union of the clusterwide and node-specific autoshare lists.

#### 4.2.3.7 Synchronizing Autoshares

By default, each disk device available to the Advanced Server when it starts is assigned an autoshare name. If you mount a disk device after the server has started, you must synchronize the available devices using the SET COMPUTER command, to make the disk device available to the Advanced Server. For example:

```
LANDOFOZ\\TINMAN> SET COMPUTER TINMAN/AUTOSHARE_SYNCHRONIZE
%PWRK-S-AUTOSHRSYNCHED, autoshare synchronization was successful

LANDOFOZ\\TINMAN>
```

In the OpenVMS Cluster environment, you must enter this command on every node in the cluster.

## 4.3 Managing Shared Directories and Files

Advanced Server allows you to create shared and personal shared directories. Some shares are provided by default.

### 4.3.1 Default Shares

When you install Advanced Server software, it creates the default shares shown in Table 4–7, Default Shares.

**Table 4–7 Default Shares**

| Share Name | Description |
|---|---|
| USERS | Contains user home directories. This shared directory is created only when logon validation is enabled. |
| NETLOGON | Default location for logon scripts. This directory is shared if the Netlogon service is running. |
| PWLIC | Client Licensing Software |
| PWLICENSE | Client Licensing Software |
| PWUTIL | Default location for Advanced Server utilities. |

### 4.3.2 Creating a Share

A share is a shared directory. By sharing a directory, you allow users on the network to access the directory.

Any directory on the server can be shared, including the root directory of a disk device. Users specify the share name when accessing and displaying shares. No two resources on the same server can have the same share name.

When you create a shared directory, you assign access permissions to users and groups. These permissions define the access to the share for the specified users and groups. If you do not specify permissions when you add a share, all users are allowed to access the share.

You can define an OpenVMS system logical name that refers to an OpenVMS physical device. Then you can specify the logical name when you create the share using the ADD SHARE command. This allows you to move the physical structure to another device, redefine the logical name, and continue to provide access to the structure by the same share name. Users connected to the share will have to reconnect after this change.

#### 4.3.2.1 Preparing to Share a Directory

When you share directories on a server, it is important to be well organized. If many users access the same directory for different purposes and activities, the directory can become a clutter of unrelated files. If you take the time to create separate directories organized by group and function, it will be easier to keep files organized and to ensure security.

Before setting up a shared directory, prepare a list of directories you will need to share on the server. Also prepare a list of the users and groups that will require access to each shared directory and the kinds of permissions they will need. Use the worksheets in the *Compaq Advanced Server for OpenVMS Concepts and Planning Guide* to help you prepare these lists.

When sharing a directory on a server, you specify the names of the users and groups who can access the shared directory by setting share permissions, and who can access the subdirectories and files in the share by setting file and directory access permissions as described in Section 4.3.6, Specifying File and Directory Access Permissions. This allows you to set different permissions for each subdirectory and file in the shared directory.

You can also set up auditing of each type of access and of specific files and directories, as described in Section 4.3.9, Auditing Directory and File Access. This provides event log messages when the files and directories are accessed.

To create a share, you must be a member of the Administrators or Server Operators group, and the associated OpenVMS directory must already exist. If a directory to be shared does not exist, you must create it either on OpenVMS or remotely. To create a directory on the OpenVMS system, use the OpenVMS command CREATE/DIRECTORY. For example, to create the directory [SHARED] on disk device USER1, enter the following OpenVMS command:

```
$ CREATE/DIRECTORY USER1:[SHARED]
```

#### 4.3.2.2 Planning Share Permissions

To secure shared directories effectively, keep the following in mind:

- Share permissions apply to network users, not OpenVMS users. However, network user accounts can be host mapped to OpenVMS user accounts, providing access to OpenVMS resources for network users based on their OpenVMS user accounts.
- Share permissions apply to all files and subdirectories created in the shared directory. You can set access permissions for specific files and subdirectories in the share. For more information, see Section 4.3.5.3, Inheriting Permissions. Note that you can restrict user access to specific

files and subdirectories in a share (using the SET FILE command), or you can restrict user access at the share level (using the ADD SHARE/PERMISSIONS= or MODIFY SHARE/PERMISSIONS= command). For example, you can restrict a user to READ access to the contents of a share by modifying the permissions for that share. This would override any other access previously granted the user to the contents of that share.

Table 4–8, Share Permissions, shows permissions available for shares and the actions available to users for each permission.

**Table 4–8 Share Permissions**

| Actions | No Access | Read Access | Change Access | Full Control |
|---|---|---|---|---|
| Display subdirectory names and file names | | X | X | X |
| Display file data and attributes | | X | X | X |
| Run program files | | X | X | X |
| Go to subdirectories of the directory | | X | X | X |
| Create subdirectories and add files | | | X | X |
| Change data in and append data to files | | | X | X |
| Change file attributes | | | X | X |
| Delete subdirectories and files | | | X | X |
| Change permissions (Windows NT files and directories only) | | | | X |
| Take ownership (Windows NT files and directories only) | | | | X |

#### 4.3.2.3 Creating a Share

You can share an existing OpenVMS directory. When you share a directory, you specify its location on the server, including the disk device, the directory name, and the name for the share. The following example shows how to share a directory on the server:

Use the ADD SHARE/DIRECTORY command. For example:

```
LANDOFOZ\\TINMAN> ADD SHARE/DIRECTORY RAINBOW USER1:[SHARED] -
_LANDOFOZ\\TINMAN> /HOST_ATTRIBUTES=(RMS_FORMAT=STREAM)
%PWRK-S-SHAREADD, share "RAINBOW" added on server "TINMAN"
```

This command adds a directory share named RAINBOW for the directory USER1:[SHARED]. Files created in this directory will be RMS stream-format files. Because the /PERMISSIONS qualifier is not included on the command line, the new share is available to all network users.

#### 4.3.2.4 Creating a Personal Share

When a server is upgraded from PATHWORKS (LAN Manager) to PATHWORKS for OpenVMS (Advanced Server), any V5 personal shares are upgraded and preserved as personal shares. The Advanced Server allows you to create personal shares, which are typically used for sharing a user's OpenVMS login directory. Personal shares are unique in that they are hidden (they will not appear in the list of shares users can display, such as in Network Neighborhood), but the names of personal shares do not end with a dollar sign ($). Thus, when users want to map a drive to their OpenVMS login directory, they specify a personal share name (typically the same as their user name) without having to include a dollar sign in the share name.

**Note**

Users cannot specify personal shares in the UNC path when connecting to or listing resources. To access such a file or run an application from the personal share, users must specify the device associated with the share.

A personal share typically points to the root directory of a user's OpenVMS account. For example, network user SCARECROW has a personal share that is mapped to the OpenVMS directory [STRAWMAN] on server TINMAN. If you display the personal shares on TINMAN, the following information appears:

```
LANDOFOZ\\TINMAN> SHOW SHARES/TYPE=PERSONAL

Shared resources on server "TINMAN":

Name          Type       Description
------------  ---------  -----------------------------------
STRAWMAN      Personal

  Total of 1 share
```

STRAWMAN, the host mapped OpenVMS account, has a login directory defined in the UAF record; for example: DUA1:[000000]STRAWMAN.DIR, or DUA1:[STRAWMAN]. You can use the AUTHORIZE utility to display a system's UAF records. For example:

```
$ MCR AUTHORIZE
UAF> SHOW STRAWMAN
```

```
Username:     STRAWMAN          Owner: SYSTEM MANAGER
Account:      SYSTEM                   UIC: [360,44] ([PCSA,STRAWMAN])
CLI:          DCL                      Table: DCLTABLES
Default:      DUA1:[STRAWMAN]
LGICMD: LOGIN
   .
   .
   .
```

Only users in the Administrators group can display and access all the personal shares on a server.

**Note**

A user with OpenVMS user accounts on multiple servers in a domain may have a personal share associated with an account on each server.

**4.3.2.4.1 Procedure for Creating a Personal Share** Follow these steps to create a personal share:

1. Add a share using the ADD SHARE/PERSONAL command.
2. Use the SHOW SHARES/TYPE=PERSONAL command to display the share. Include the /FULL qualifier to display the path and permissions. For example:

```
LANDOFOZ\\TINMAN> ADD SHARE GREATOZ USER1:[USERS] -
_LANDOFOZ\\TINMAN> /PERSONAL/NOPERMISSIONS/PERMISSIONS=(LION=FULL)
%PWRK-S-SHAREADD, share "GREATOZ" added on server "TINMAN"

LANDOFOZ\\TINMAN> SHOW SHARES/TYPE=PERSONAL/FULL

Shared resources on server "TINMAN":

Name          Type       Description
------------  ---------  ----------------------------------------
GREATOZ       Personal
    Path: USER1:[USERS]
    Connections:  Current: 0, Maximum: No limit
    RMS file format: Stream
    Directory Permissions: System: RWED, Owner: RWED, Group: RWED, World: RE
    File Permissions: System: RWD, Owner: RWD, Group: RWD, World: R
    Share Permissions:
        LION                          Full Control
     Total of 1 share

LANDOFOZ\\TINMAN>
```

After the personal share is created, you can set up the associated directory as the user's home directory. The home directory contains files and programs for the user, and is automatically accessible when the user logs on to the network. For information about setting up home directories, see Section 3.1.10, Specifying Home Directories.

#### 4.3.2.5 Stopping Directory Sharing

You may need to stop sharing a directory when the directory is no longer being used and you want to delete it; for example, when a project requiring the use of shared files is completed. Advise users when you are planning to stop sharing a directory.

For example, to stop sharing the directory GREATOZ, use the ADMINISTER command REMOVE SHARE, as follows:

```
LANDOFOZ\\TINMAN> REMOVE SHARE GREATOZ/NOCONFIRM
%PWRK-S-SHAREREM, share "GREATOZ" removed from server "TINMAN"

LANDOFOZ\\TINMAN>
```

This example removes the share named GREATOZ from the server named TINMAN; no confirmation is required. When you stop sharing a directory, the share name is removed from the share database and no longer appears on the list of available shares. However, the directory and its files are not deleted.

### 4.3.3 Displaying Information About Shares

You can use the SHOW SHARES command to display the shares provided by a server and to see which shares are available to the network. Before sharing a new directory from the server, first check which shares are currently available.

The following example shows how to display the shared directories for your server:

```
LANDOFOZ\\TINMAN> SHOW SHARES

Shared resources on server "TINMAN":

Name          Type       Description
------------  ---------  ---------------------------------------
NETLOGON      Directory  Logon Scripts Directory
PWLIC         Directory  PATHWORKS Client License Sftwr
PWLICENSE     Directory  PATHWORKS Client License Sftwr
PWUTIL        Directory  Adv. Srv. Client-based Utilities
USERS         Directory  Users Directory

  Total of 5 shares

LANDOFOZ\\TINMAN>
```

The default display does not show administrative shares and personal shares.

You can display information about administrative shares (those that end with $) using the SHOW SHARES/HIDDEN command, as described in Section 4.2, Administrative Shares.

You can display information about personal shares using the SHOW SHARES/TYPE=PERSONAL command.

You can display information about all shares using the SHOW SHARE/TYPE=ALL command.

#### 4.3.3.1 Displaying Information About a Specific Share

You can display information about any share, regardless of the type of share, by specifying the share name, as in the following example:

```
LANDOFOZ\\TINMAN> SHOW SHARES RAINBOW

Shared resources on server "TINMAN":

Name          Type       Description
------------  ---------  --------------------
RAINBOW       Personal

  Total of 1 share
```

#### 4.3.3.2 Displaying Share Permissions

To display share permissions, use the SHOW SHARES command with the /PERMISSIONS qualifier. For example:

```
LANDOFOZ\\TINMAN> SHOW SHARES/PERMISSIONS
Shared resources on server "TINMAN":
Name          Type       Description
------------  ---------  -------------------------------------------------
DICK          Printer    Dick's print share
    Share Permissions:
        Everyone                      Full Control
NETLOGON      Directory  Logon Scripts Directory
    Share Permissions:
        Everyone                      Read
PATHWORKS     Directory
    Share Permissions:
        Everyone                      Full Control
PWLIC         Directory  PATHWORKS Client License Sftwr
    Share Permissions:
        Administrators                Full Control
        Everyone                      Read
PWLICENSE     Directory  PATHWORKS Client License Sftwr
    Share Permissions:
        Administrators                Full Control
        Everyone                      Read
PWUTIL        Directory  Adv. Srv. Client-based Utilities
    Share Permissions:
        Everyone                      Read
USERS         Directory  Users Directory
    Share Permissions:
        Everyone                      Full Control

  Total of 7 shares

LANDOFOZ\\TINMAN>
```

### 4.3.4 Changing Share Properties

You can change the properties of an existing share using the MODIFY SHARE command. You can change the following share properties:

- Number of users allowed to connect to a shared directory
- Shared directory's description
- Share permissions

To change the properties of a shared directory, you must be logged on as a member of the Administrators or Server Operators group.

The following example shows how to use the MODIFY SHARE command to add permissions on an existing directory share called GREATOZ and to grant READ access to the user SCARECROW:

```
LANDOFOZ\\TINMAN> MODIFY SHARE GREATOZ/PERMISSIONS=(SCARECROW=READ)
%PWRK-S-SHAREMOD, share "GREATOZ" modified on server "TINMAN"

LANDOFOZ\\TINMAN>
```

### 4.3.5 Planning File and Directory Access Permissions

Users and groups can be granted or denied access to specific files and subdirectories in a shared directory. A user denied access to a file or directory, either individually or as a member of a group, can connect to the share but cannot perform any operations with the files and directories in the share. You can grant specific unique access permissions for files and directories in shares that users can access. Once a user connects to the resource, the file and directory access permissions control the operations that the user can perform. For information about specifying share permissions, see Section 4.3.2.2, Planning Share Permissions.

You can enable users to set access permissions on their own files and directories. These users can then control whether other users can read, write, or modify files in that directory. To enable users to set access permissions, give them full control using the SET FILE command.

#### 4.3.5.1 File and Directory Access Permissions

Table 4–9, Directory Access Permissions and Actions on Directories, lists the types of access users can have and the permissions to set on directories.

**Table 4–9 Directory Access Permissions and Actions on Directories**

| User Actions | NONE | LIST | READ | ADD | ADD AND READ | CHANGE | FULL CONTROL |
|---|---|---|---|---|---|---|---|
| Display directory file names | | X | X | | X | X | X |
| Display directory attributes | | X | X | X | X | X | X |
| Go to directory subdirectories | | X | X | X | X | X | X |
| Change directory attributes | | | | X | X | X | X |
| Create subdirectories and add files | | | | X | X | X | X |
| Display directory owner and permissions | | X | X | X | X | X | X |
| Delete the directory | | | | | | X | X |
| Delete any file or empty subdirectory in a directory | | | | | | | X |
| Change directory permissions | | | | | | | X |
| Take ownership of the directory | | | | | | | X |

Table 4–10, Directory Access Permissions and Actions on Files, lists the types of access users can have to files and the permissions to set on them.

**Table 4–10 Directory Access Permissions and Actions on Files**

| User Actions | NONE | LIST | READ | ADD | ADD AND READ | CHANGE | FULL CONTROL |
|---|---|---|---|---|---|---|---|
| Display file owner and permissions | | | X | | X | X | X |
| Display file data | | | X | | X | X | X |
| Display file attributes | | | X | | X | X | X |
| Run a program file | | | X | | X | X | X |
| Change file attributes | | | | | | X | X |
| Change data in and append data to the file | | | | | | X | X |
| Delete the file | | | | | | X | X |
| Change the file permissions | | | | | | | X |
| Take ownership of the file | | | | | | | X |

### 4.3.5.2 Setting Permissions on a File or Directory

By default, anyone with a valid network user name and password can log on to a server and connect to a share on that server. However, a user must have the requisite permissions to access the directories and files in the share. You use the SET FILE/PERMISSIONS command to set permissions on a shared directory. You may need to change access permissions if users cannot access the directories or files they need, or if unauthorized users can access them. For information about how a file or directory that does not have explicit permissions inherits the permissions, see Section 4.1.3.1, Inheritance of Directory Permissions, and Section 4.3.5.3, Inheriting Permissions.

Permissions for disk resources are stored on the disk with each resource as an OpenVMS access control list (ACL). Thus, resource permissions are backed up by the OpenVMS Backup utility.

#### 4.3.5.3 Inheriting Permissions

As you create subdirectories and files in shared directories that have existing permissions, those permissions are automatically propagated to the new subdirectories and files. (This assumes the default for the **STORE_SECURITY_ACES** is in effect; see Section 4.1.3.6, Streamlining Security Information Storage and Lookups, for more information.) However, if you decide to share a directory that contains existing subdirectories and files, the permissions you assign to the new share are not propagated to its subdirectories and files. You can either explicitly set permissions for each subdirectory and file, or you allow their permissions to be inherited.

### 4.3.6 Specifying File and Directory Access Permissions

When sharing a directory on a server, you specify the name of the groups and users who can access the share, its subdirectories, and its files, and the permissions each group or user has for the share. After the share has been created, you can modify the permissions on the files and directories in the share. The following example shows how to use the SET FILE/PERMISSIONS command to modify permissions. In this example, the command specifies the access permissions for all files with the .C extension in the directory CURTAIN in share GREATOZ.

```
LANDOFOZ\\TINMAN> SET FILE GREATOZ\CURTAIN\*.C -
_LANDOFOZ\\TINMAN> MUNCHKINS/PERMISSIONS=READ -
_LANDOFOZ\\TINMAN> SCARECROW/PERMISSIONS=FULL_CONTROL
%PWRK-S-FILEMOD, "GREATOZ\CURTAIN\FILE1.C" modified on server "TINMAN"

%PWRK-S-FILESMODIFIED, total of 1 file modified
LANDOFOZ\\TINMAN>
```

As a result, the following permissions are set:

- Group MUNCHKINS has READ access
- User SCARECROW has FULL access

### 4.3.7 Displaying File and Directory Access Permissions

To display directory and file permissions, use the SHOW FILES/PERMISSIONS command, specifying a share name and its path. For example, with a share called RAINBOW and a file called LOGS.TXT, you can display permissions as follows:

```
LANDOFOZ\\TINMAN> SHOW FILES RAINBOW\LOG.TXT /PERMISSIONS

Files in: \\TINMAN\RAINBOW
     LOGS.TXT
          Permissions:
              Administrators           Full (All)
              Everyone                 Change (RWXD)
              Server Operators         Change (RWXD)
              SYSTEM                   Full (All)

     Total of 1 file

LANDOFOZ\\TINMAN>
```

## 4.3.8 Using Network Permissions and OpenVMS Protections

If the Advanced Server and OpenVMS security model is enabled, and a network user attempts to access a file or directory, the access must be allowed by two security checks: network permissions, and OpenVMS file and directory protections.

### 4.3.8.1 OpenVMS Protections

Every file on an OpenVMS system has four protection codes:

- The OpenVMS SYSTEM UIC group (System).
- The OpenVMS owner of a file (Owner).
- The OpenVMS group that can access a file (Group). (This is the OpenVMS group to which the owner belongs.)
- The world, which means everyone else (World).

To set OpenVMS system file protections, use the OpenVMS command SET PROTECTION.

When a network user attempts to access a file, the following rules determine the way that OpenVMS system protections control the access:

- If the network user account is mapped to the OpenVMS user account that is the owner of the file, then the Owner protections apply.
- If the network user account is mapped to an OpenVMS user that is in the same UIC group as the file owner, then Group protections apply.
- If the user's UIC group is in the range of SYSTEM UIC group numbers, then the System protections apply.
- Otherwise, World protections apply.

### 4.3.9 Auditing Directory and File Access

When you assign permissions for a resource, you can also audit use of the resource. The Advanced Server can write an entry to the Security event log whenever a user accesses the resource in a certain way. The audit entry shows the resource, action performed, user who performed it, and date and time of the event.

Events that Advanced Server can audit for directory and file access include:

- Successful and failed attempts to take ownership of a file or directory
- Successful and failed attempts to access a file or directory
- Successful or failed attempts to change access permissions on a file or directory

For more information about auditing and viewing events, see Chapter 6, Monitoring Events and Troubleshooting.

### 4.3.10 Taking Ownership of Files or Directories

When you create a file or directory, you become its owner. By granting permissions, the owner controls how the file or directory is used. The owner can grant permission to another user to take ownership of a file or directory. Otherwise, you must be logged on as a member of the Administrators group to take ownership. Although an administrator can take ownership, an administrator cannot transfer ownership to others. This preserves security. To make sure that your files are secure, you should check their ownership regularly using the SHOW FILES/OWNER command.

#### 4.3.10.1 Authorizing a User to Take Ownership of a File or Directory

You can specify permission to take ownership of a file or a directory using the following commands:

- SET FILE/PERMISSIONS=FILE_SPECIFIC=TAKE_OWNERSHIP
- SET FILE/PERMISSIONS=DIRECTORY_SPECIFIC=TAKE_OWNERSHIP

For example, to authorize the user SCARECROW to take ownership of a file called SIMIANS.DAT that is stored on domain LANDOFOZ in the directory \WITCH\MKEY, enter the following command:

```
LANDOFOZ\\TINMAN> SET FILE WITCH\MKEY\SIMIANS.DAT -
_LANDOFOZ\\TINMAN>SCARECROW/PERMISSIONS=FILE_SPECIFIC=TAKE_OWNERSHIP
%PWRK-S-FILEMOD, "\\TINMAN\WITCH\MKEY\SIMIANS.DAT" modified
```

#### 4.3.10.2 Taking Ownership of a File or Directory

To take ownership of a file or directory, use the TAKE FILE OWNERSHIP command as follows:

```
TAKE FILE OWNERSHIP UNCpath [/qualifiers])
```

For example, the following command takes ownership of the file called SIMIANS.DAT that is stored on domain LANDOFOZ in the directory \WITCH\MKEY:

```
LANDOFOZ\\TINMAN> TAKE FILE OWNERSHIP WITCH\MKEY\SIMIANS.DAT
%PWRK-S-FILEMOD, "\\TINMAN\WITCH\MKEY\SIMIANS.DAT" modified

LANDOFOZ\\TINMAN>
```

### 4.3.11 Managing Shares from a Windows NT Server

You can manage shares on the Advanced Server using a Windows NT Server. When the Windows NT Server performs server administration, the Windows NT server administration tool Server Manager attempts to verify the share path locally before passing the server operation request to the Advanced Server. Any share path that does not conform to the *device:\directory* convention, where *device:* is a single letter drive letter, fails the share path verification; therefore, you cannot manage an Advanced Server share from the Windows NT Server Manager if the share path does not conform to the *device:\directory* convention.

The following sections describe ways to manage an Advanced Server share from the Windows NT Server.

#### 4.3.11.1 Adding a Share from a Windows NT Server

To add an Advanced Server share using a Windows NT Server, use one of the following procedures:

- Define the OpenVMS device using the **Autoshare** server configuration parameter in the LANMAN.INI file. This server parameter allows you to map the OpenVMS device to a single letter DOS device. (See Section 4.2.3.2, Defining Autoshares, for more information.)

  When a device is defined as an autoshare this way, you can add the share using the Windows NT Server by specifying the share path as *device:\directory*, where *device* is the mapped device letter.

  For example, to share the directory DUA1:[SHARE1] using the device letter D, include the following in the LANMAN.INI file:

  ```
  Autoshare= DUA1=D
  ```

To add this share using the Windows NT Server Manager, specify the share path as follows:

```
d:\share1
```

- Convert the share path input string from the OpenVMS directory path by adding C:\ to the beginning of the path specification. Instead of specifying *device:[share]*, enter *device\share*. The Advanced Server is designed to interpret C: correctly.

  For example, if the OpenVMS directory that you want to share is DUA1:[SHARE1], specify the share path as follows:

  ```
  C:\DUA1\SHARE1
  ```

  By default, the C: device is defined as PWRK$LMROOT:[000000]. To add this share, use the following path name:

  ```
  C:\SHARE1
  ```

  In this case, the actual OpenVMS specification is PWRK$LMROOT:[SHARE1].

#### 4.3.11.2 Displaying and Modifying Shares from a Windows NT Server

To display and modify the OpenVMS share from a Windows NT Server, use the following share path:

```
C:\vmsdevicename\directorypath
```

For example, if you add a share using the ADMINISTER command ADD SHARE, and you specify $1$DUA2:[SHARE.LEVEL2] as the share path for share LEVEL2, when you display this share from the Windows NT Server Manager, the share path is displayed in the following format:

```
C:\$1$DUA2\SHARE\LEVEL2
```

#### 4.3.11.3 File-Naming Conventions

An operating system's file system determines the conventions that apply to file and directory names. When you use the PATHWORKS Advanced Server, you can use long file and directory names, much as with OpenVMS. Windows NT, Windows 95, Windows 98, and Windows 2000 provide long file names, but Windows V3.11 and MS-DOS do not. For example, on Windows NT, Windows 95, Windows 98, and Windows 2000 clients, file names may contain more than one period, and have file extensions of any length within the file name length limit. In contrast, MS-DOS clients limit file names to the "8.3" convention: file names can be no longer than eight characters, there must be one period to separate the file name from the file extension, and the file extension can be up to three characters.

All files stored on the PATHWORKS Advanced Server are subject to the PATHWORKS Advanced Server file naming conventions.

**4.3.11.3.1 PATHWORKS Advanced Server File Naming** The PATHWORKS Advanced Server uses the naming conventions shown in the following table.

**Note**

PATHWORKS Advanced Server stores file names as all uppercase characters.

**Table 4–11 Advanced Server File-Naming Conventions**

| Convention | What Is Supported | Notes |
|---|---|---|
| File name length | Up to 78 characters, including the extension (39.39 format). Separate the extension from the name by using a period. | When clients store files whose names include spaces or nonalphanumeric characters (characters not included in the standard character sets), the length of a file name on an ODS-2 volume is limited further: Each such character takes up four characters on the disk volume. |

(continued on next page)

**Table 4–11 (Cont.) Advanced Server File-Naming Conventions**

| Convention | What Is Supported | Notes |
|---|---|---|
| File name characters | Alphanumeric characters (a-z, A-Z, 0-9), dollar sign ($), underscore (_) and hyphen (-), plus any of the 8-bit nonalphanumeric characters of the ISO Latin-1 character set, with the exception of the following characters:<br>C0 control codes (0x00 to 0x1F inclusive)<br>Double quotation marks (")<br>Asterisk (*)<br>Backslash (\)<br>Colon (:)<br>Left angle bracket (<)<br>Right angle bracket (>)<br>Slash (/)<br>Question mark (?)<br>Vertical bar ( \| ) | Lowercase letters are stored as uppercase.<br>Supported 8-bit nonalphanumeric characters are encoded as _*XX*, where *XX* is the 8-bit code.<br>Any OpenVMS system file or directory name that contains excluded characters is neither visible nor accessible by the client. |

**4.3.11.3.2 MS-DOS and Windows File Naming** If you are using the Advanced Server in an environment where long file names are not always supported, users should continue using MS-DOS file naming conventions. For example, if your clients are running Windows 3.11, or older Windows applications that only recognize the 8.3 file format, file names should follow the 8.3 file-naming convention; if your clients are running Windows 95, Windows 98, or Windows 2000, they can use long file names.

On MS-DOS, Windows NT, Windows 95, Windows 98, and Windows 2000 clients, the following names are reserved and cannot be used for files or directories on OpenVMS disk volumes: AUX, COM1, COM2, COM3, COM4, CON, LPT1, LPT2, LPT3, NUL, and PRN.

On Windows NT, Windows 95, Windows 98, and Windows 2000 clients, file names preserve uppercase and lowercase characters, and are case sensitive. The Advanced Server stores these file names as uppercase and is not case sensitive.

For more details on file naming conventions supported by each type of client, refer to the appropriate documentation for that client operating system.

**4.3.11.3.3 Alias File Names Accommodate Client Applications Limited to the MS-DOS File Name Format** As noted previously, clients and client applications are more restrictive with file names than are the Advanced Server and Windows NT. For example, MS-DOS file names are limited to the "8.3" convention: file names can be no longer than eight characters, with a period separating the file name from the file extension, and the file extension can be up to three characters. Obviously, these applications do not take full advantage of longer file names supported on Windows NT, the Advanced Server, and other systems.

To maintain compatibility between MS-DOS clients and Windows NT, and between legacy applications and Windows NT, the Windows NT Server provides an alternate way of accessing files with names that are not compatible with MS-DOS conventions. Windows NT generates MS-DOS-compatible *alias names* for these files.

The PATHWORKS Advanced Server file server also creates MS-DOS-compatible *alias file names* for shared files whose names do not conform to the MS-DOS format. As a result, client applications that must use, or choose to use, the MS-DOS format for file names, can access these shared files on the server by using the file's associated alias name. Clients (depending on their file systems) can use either the real file name or the alias file name to access the file.

**Note**

Alias file names are usually used by client applications. Users will seldom need to use them.

The Advanced Server alias file names are functionally equivalent to the alias names generated by the Windows NT Server in that each alias file name:

- Is MS-DOS compatible
- Is unique among all file names, real or alias, within the parent directory
- Positively identifies the associated file
- Has a first character and an extension derived from the real file name

For generating its alias file names, the Advanced Server uses a different algorithm than does Windows NT; consequently, the alias file names generated by the Advanced Server do not resemble alias file names generated by the Windows NT Server. An Advanced Server alias file name always includes an eight-character base, and includes an extension of the same length as the original extension, if any, up to three characters. The first character and

extension of the alias file name are derived from the real file name and its extension, substituting an underscore (_) for any such character that is not MS-DOS-compatible.

The following example shows an MS-DOS directory listing that includes alias file names generated for MS-DOS compatibility. In this example:

- The first file name listed, 12345678.123, has a standard length (8.3 or less) with no invalid characters, and so no alias file name is generated.
- The name of the second file, 123456789.1234, is longer than the standard, so the alias file name 14AD1'HA.123 is created.
- The name of the third file (LONG FILENAME) exceeds the standard length and also includes an invalid character (the space) for an MS-DOS file name. The alias file name (L1JKGVAM) does not include an extension because the original file name does not have an extension.
- The fourth file name listed (X.1+345678) has an extension that exceeds the standard length and includes a character (+) that is not compatible with MS-DOS. Accordingly, the alias file name extension includes an underscore (_) for the incompatible character.
- The last file name (+.+) includes an incompatible character in the name and extension. The alias file name generated for this file has an underscore in its name and extension.

```
F:\DEMO>dir/x
 Volume in drive F is USER1
 Volume Serial Number is 0000-0001

 Directory of F:\DEMO

06/01/01  01:14p        <DIR>                          .
05/31/01  04:14p        <DIR>                          ..
05/21/01  04:30p                     16                12345678.123
05/21/01  04:30p                     16 14AD1'HA.123   123456789.1234
05/21/01  04:30p                     16 L1JKGVAM       LONG FILENAME
05/21/01  04:30p                     16 X2$'XC`R.1_3   X.1+345678
05/21/01  04:30p                     16 _0XY8I@H._     +.+
   .
   .
   .
```

# 5

# Managing Printers, Print Queues, and Print Shares

The Advanced Server software lets you share printers connected to the network (accessible from the OpenVMS system). You can create an Advanced Server print share for any OpenVMS print queue and assign access permissions to that share. Users can then send print jobs to the queue specified by the share as though they were using a local printer.

The procedures you use to manage shared printers are described in this chapter:

- Section 5.1, OpenVMS Print Queues, describes OpenVMS print queues and explains how to create and manage them.
- Section 5.2, Planning Printer Services, explains how to plan printer services to meet client needs.
- Section 5.3, Managing Printers, Print Shares, and Print Jobs, explains how to manage printers, print shares, and print jobs:
  - Section 5.3.1, Setting Up a New Printer, explains how to set up network printers on the server.
  - Section 5.3.2, Managing Printers Using the Advanced Server ADMINISTER Command-Line Interface, explains how to manage printers by using the ADMINISTER command interface.

The Advanced Server makes printers available to network users through shared print queues. A print queue stores print jobs as users submit them. When a printer associated with the queue becomes available, the Advanced Server routes a job to that printer.

To share a printer, you add the printer (print queue) to the server's share database. You use ADMINISTER commands to add a print queue and set it up for sharing. You assign the share name to a queue that points to the printer.

Because the Advanced Server is based on the OpenVMS operating system, the print queues and the printers that you share can be OpenVMS print queues and printers.

This chapter explains how to share printers that are connected to the network, accessible from the OpenVMS system.

## 5.1 OpenVMS Print Queues

OpenVMS systems use execution queues and generic queues to provide access to printers as follows:

- One or more execution queues can be created for each printer.
- One or more generic queues can point to multiple execution queues and, therefore, multiple printers.
- Print jobs can be submitted either to a generic queue or to an execution queue.

You can use any of the following methods to create and manage OpenVMS print queues:

- OpenVMS commands such as INITIALIZE/QUEUE, which can be used to create execution queues or generic queues, and SET QUEUE, which modifies the attributes of the created queue. Refer to the *OpenVMS System Manager's Manual* for information about setting up print queues on OpenVMS systems.
- Advanced Server ADMINISTER commands such as ADD PRINT QUEUE and SET PRINT QUEUE, which primarily do the same as the OpenVMS INITIALIZE/QUEUE and SET QUEUE commands.

### 5.1.1 Types of Advanced Server Print Queues

An Advanced Server print queue can be either of the following:

- A printer queue pointing directly to a physical printer. A printer queue is equivalent to an OpenVMS execution queue.
- A routing queue that points to one or more printer queues. A routing queue is equivalent to an OpenVMS generic queue.

## 5.2 Planning Printer Services

To support the printing needs of your users, plan print queues and print shares to meet their requirements. You can set up printers as shared devices, and you can establish constraints on print queues.

### 5.2.1 Sharing Printers and Print Queues

The way you make printers available to Advanced Server users depends on your server installation and whether you want to share existing OpenVMS print queues or create new ones.

- If you have installed Advanced Server software on a system for the first time and the printer you want to share has an existing OpenVMS queue, you can share that queue or create and share a new queue for that printer. You can display existing print queues using the ADMINISTER SHOW PRINT QUEUE command. You must define an Advanced Server print share for every OpenVMS print queue that you want Advanced Server users to access. Section 5.3.2.7.1, Creating an Advanced Server Print Share, explains how to set up and define a print share, using the Advanced Server ADMINISTER command interface.
- If the printer you want to share does not have an existing OpenVMS print queue, you can create one using the procedure in Section 5.3.1, Setting Up a New Printer.
- If you have installed PATHWORKS Advanced Server software on a server that ran PATHWORKS V5 for OpenVMS (LAN Manager) software, and the printer you want to share was previously shared, you can use the PATHWORKS Upgrade utility to automatically convert existing print shares to PATHWORKS Advanced Server print shares, as described in the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Migration Guide*.

Advanced Server users access the print queue by specifying a print share.

To make a print share operational, a print queue must be established first. To establish both a print queue and a print share, first set up the print queue, then set up the print share.

With the ADMINISTER interface, you create a print share so that users can send print requests to the print share rather than to individual print queues. For access from Windows NT, Windows 95, Windows 98, and Windows 2000 clients that will print to a Advanced Server shared print queue, the share name and the queue name must be the same; for other clients, like Windows 3.11, the share and queue name can be different. Multiple print shares can point to the same print queue.

The Advanced Server print queue name is limited to no more than 12 characters. If the OpenVMS print queue name has more than 12 characters, you can define an OpenVMS logical name for the print queue, to translate the queue name. You might use a logical name that is the same as the share name.

For example, the following OpenVMS command defines a logical name GLENDA for the OpenVMS print queue GLENDASPRINTER:

```
$ DEFINE/SYSTEM GLENDA GLENDASPRINTER
```

Then, when you use ADMINISTER commands, you can use the logical name to specify the print queue when you create a print share for it.

## 5.3 Managing Printers, Print Shares, and Print Jobs

You manage printers, print shares, and print jobs by using the ADMINISTER command-line interface. To set up shared printers, do the following:

1. Use the ADD PRINT QUEUE command to establish an OpenVMS print queue as a print queue on the server, defining it as either a printer queue (OpenVMS execution queue) or a routing queue (OpenVMS generic queue).
2. Create a share for that queue, using the ADD SHARE/PRINT command.

### 5.3.1 Setting Up a New Printer

The information in this section applies only to printers supported by the OpenVMS operating system. If you start with no OpenVMS queue and create an Advanced Server print queue, the Advanced Server creates the OpenVMS print queue.

To set up a new printer to make it available to Advanced Server clients:

1. Connect the printer to your server or network. Refer to your printer documentation for physical connection information. See Section 5.3.1.2, Connecting Your Printer, for information about specifying printer connections to OpenVMS systems.
2. Use the ADMINISTER command interface to:
   a. Create a printer queue for the printer, as described in Section 5.3.1.3, Creating an Advanced Server Print Queue.
   b. Create a routing print queue (optional), as described in Section 5.3.1.3, Creating an Advanced Server Print Queue.
   c. Create a print share for the queue, as described in Section 5.3.2.7.1, Creating an Advanced Server Print Share.

#### 5.3.1.1 Printer Types

To share a PostScript printer, selected PostScript printers might require use of the DECprint Supervisor for OpenVMS (DCPS) software for communication with the printers over DECnet or TCP/IP. In this case, use DCPS to create the queue. Then set up the queue as an Advanced Server print share, using the ADMINISTER ADD SHARE/PRINT command, as explained in Section 5.3.2.7.1, Creating an Advanced Server Print Share.

Printers supported by Advanced Server software include:

- All printers supported by OpenVMS
- PostScript printers supported by DECprint Supervisor for OpenVMS software

To use the Advanced Server ADMINISTER command interface to display the printers that are supported, enter the following command:

```
LANDOFOZ\\TINMAN>HELP ADD PRINT QUEUE /TYPE
```

#### 5.3.1.2 Connecting Your Printer

When you connect your printer, make a note of the printer type and the name of the physical device or port to which it is connected.

The list of physical device connectors or ports includes, but is not limited to:

- OP*xn*
- TT*xn*
- TX*xn*
- LT*xnnn*

For example, the type of printer may be a DL3200 (a DEClaser 3200), and the physical device or port to which it is connected may be LTA201.

#### 5.3.1.3 Creating an Advanced Server Print Queue

A print queue can be either a printer queue associated with a physical printing device, or a routing queue that routes print requests to one or more print queues. Typically, a routing queue points to a group of printers that have similar characteristics. You could also set up several print queues for the same printer. This might be useful if you want to set up different print queue characteristics for a printer.

To create queues for printers on your server, you must be logged on to a user account that is a member of one of the following groups:

- Administrators

- Server Operators
- Print Operators

To create a printer queue or routing queue, use the ADD PRINT QUEUE command. Use the SET PRINT QUEUE command to change the characteristics of an existing queue.

For each Advanced Server queue, you must specify whether it is a printer queue or a routing queue. For a printer queue, you can specify the printer device type and the port to which the printer is connected to the OpenVMS system. For a routing queue, you can specify one or more printer queues to which the print jobs in the routing queue will be sent.

For example, the following command creates a printer queue called GLENDA1 for the DEClaser 3200 printer that is connected to LTA201:

```
LANDOFOZ\\TINMAN> ADD PRINT QUEUE GLENDA1 /PRINTER=LTA201-
_LANDOFOZ\\TINMAN> /TYPE=DL3200
%PWRK-S-QUEADD, queue "GLENDA" added on server "TINMAN"
```

The following command sets up or establishes the routing queue called GLENDA. Print jobs sent to GLENDA go to either of the two printer queues, GLENDA1 or GLENDA2. The description of the routing queue is "Glenda's routing queue."

```
LANDOFOZ\\TINMAN> ADD PRINT QUEUE GLENDA /ROUTE_TO=(GLENDA1,GLENDA2) -
_LANDOFOZ\\TINMAN> /DESCRIPTION="GLENDA's routing queue"
%PWRK-S-QUEADD, queue "GLENDA" added on server "TINMAN"

LANDOFOZ\\TINMAN>
```

### 5.3.2 Managing Printers Using the Advanced Server ADMINISTER Command-Line Interface

This section provides information about displaying, modifying, and managing print queues from the Advanced Server, using the ADMINISTER command interface. To manage print queues, you must be logged on to a user account that is a member of one of the following groups:

- Administrators
- Server Operators
- Print Operators

There are no special requirements for displaying print queue information.

#### 5.3.2.1 Displaying Print Queue Information

Using the SHOW PRINT QUEUE command, you can display a list of the server's print queues, information about a specific queue, or information about the print jobs in each queue. To display information about the print queues on a server, use one of the following procedures.

**5.3.2.1.1 Displaying Information About All Print Queues on a Server** To display information about all print queues on a server, use the SHOW PRINT QUEUES command, as in the following example:

```
LANDOFOZ\\TINMAN> SHOW PRINT QUEUES
Name              Jobs   Status        Printer/Routing    Description
---------------   ------ ------        ---------------    --------------
User_PRNT          2     destination   LRA0:GENERIC
                          paused
GLENDA             0     PAUSED

LANDOFOZ\\TINMAN>
```

The Advanced Server displays, in tabular form:

- Queue name
- Number of jobs in the queue
- Queue status
- If a printer queue, "printer device:printer type"; if a routing queue, the list of printer queues to which print jobs are routed
- The queue description

If a job is currently printing from a given queue, an additional line is displayed that contains the job ID (job identification number), the user name that queued the print job, and the status of the print job.

**5.3.2.1.2 Displaying Information About a Single Print Queue** To display information about a single print queue, specify the queue name with the SHOW PRINT QUEUE command, as in the following example:

```
LANDOFOZ\\TINMAN> SHOW PRINT QUEUE TOTO
Name            Jobs    Status          Printer/Routing   Description
-----------     ----    ------------    ---------------   ----------------
TOTO             1      printing        LRA0:GENERIC

LANDOFOZ\\TINMAN>
```

The Advanced Server displays the queue name and status of the queue and the number of print jobs currently in the queue.

#### 5.3.2.2 Changing the Printer Type

Specify the type of printer supported by a shared print queue using the SET PRINT QUEUE command with the /TYPE qualifier. For example, the following command sets the print queue TOTO to support a DEClaser 3200 printer:

```
LANDOFOZ\\TINMAN> SET PRINT QUEUE TOTO/TYPE=DL3200
%PWRK-S-QUESET, characteristics set for queue "TOTO" on server "TINMAN"

LANDOFOZ\\TINMAN>
```

#### 5.3.2.3 Pausing a Print Queue

You can hold or pause a print queue; this prevents the queue from sending any jobs to printers. When you do this, printers associated with the queue finish printing their current jobs, but all further jobs stay in the queue until the queue is released.

To pause a print queue, use the PAUSE PRINT QUEUE command, as in the following example:

```
LANDOFOZ\\TINMAN> PAUSE PRINT QUEUE TOTO
Do you really want to pause print queue "TOTO" [YES or NO] (YES) : YES
%PWRK-S-QUESET, queue "TOTO" paused on server "TINMAN"

LANDOFOZ\\TINMAN> SHOW PRINT QUEUE
Name         Jobs  Status               Printer/Routing    Description
----------   ----- ------------------   ---------------    ----------------
BRUCE_PRNT       0 destination paused   LRA0:GENERIC
PARSIFAL         0 ACTIVE               BRUCE_PRNT
TOTO             0 PAUSED               BRUCE_PRNT         Printer in the
                                                           Land of Oz
LANDOFOZ\\TINMAN>
```

You can also pause a print queue with the SET PRINT QUEUE/PAUSE command. In the following example, the queue called BRUCE_PRNT is a printer queue that points to a physical device, LRA0:GENERIC, and the queues GLENDA and TOTO are routing queues that point to the printer queue BRUCE_PRNT.

```
LANDOFOZ\\TINMAN> SET PRINT QUEUE TOTO/PAUSE
%PWRK-S-QUESET, queue "TOTO" paused on server "TINMAN"

LANDOFOZ\\TINMAN> SHOW PRINT QUEUE
Name          Jobs  Status               Printer/Routing    Description
----------    ----- ------------------   ---------------    ------------
BRUCE_PRNT       0  destination paused   LRA0:GENERIC
GLENDA           0  ACTIVE               BRUCE_PRNT
TOTO             0  PAUSED               BRUCE_PRNT         Printer in the
                                                            Land of Oz
LANDOFOZ\\TINMAN>
```

#### 5.3.2.4 Continuing a Print Queue

After you have paused a print queue, you can continue printing on the queue, returning it to normal status. Continuing a queue that is in an error condition clears the error. Use the SET PRINT QUEUE /CONTINUE command, as in the following example:

```
LANDOFOZ\\TINMAN> SET PRINT QUEUE TOTO/CONTINUE
%PWRK-S-QUESET, queue "TOTO" continued on server "TINMAN"

LANDOFOZ\\TINMAN>
```

This example continues a paused print queue. Any jobs that were waiting in the paused print queue can now print.

#### 5.3.2.5 Purging Print Jobs from a Print Queue

You can purge a shared print queue; that is, you can delete all jobs in the queue except the one currently printing. Use the SET PRINT QUEUE /PURGE command, as in the following example:

```
LANDOFOZ\\TINMAN> SET PRINT QUEUE TOTO/PURGE
%PWRK-S-QUESET, queue "TOTO" purged on server "TINMAN"

LANDOFOZ\\TINMAN>
```

#### 5.3.2.6 Deleting a Print Queue

To remove an Advanced Server print queue from network access, use the REMOVE PRINT QUEUE command. Removing the queue deletes the OpenVMS queue, but does not remove any print shares assigned to the print queue; these must be removed manually.

The following rules and restrictions apply to deleting print queues:

- You can delete only queues created by the Advanced Server. You cannot use ADMINISTER commands to delete a queue created by DECprint Supervisor for OpenVMS or OpenVMS software.
- Before deleting a printer queue (one that points directly to an OpenVMS execution queue), you must use the following commands, in the order shown:

  1. PAUSE PRINT QUEUE — to pause the print queue. Pausing the queue is an OpenVMS restriction. You do not have to pause a routing queue before deleting it. (When you use the REMOVE PRINT QUEUE command to delete a print queue, the queue is not deleted until all jobs in that queue complete.)
  2. REMOVE PRINT QUEUE — to delete any routing queues that point to the printer queue.

Then, use the REMOVE PRINT QUEUE command to delete the printer queue. The following example shows the sequence of commands required to remove printer queue GLENDA1. Routing queue GLENDA points to GLENDA1.

```
LANDOFOZ\\TINMAN> PAUSE PRINT QUEUE GLENDA1/NOCONFIRM
%PWRK-S-QUESET, queue "GLENDA1" paused on server "TINMAN"

LANDOFOZ\\TINMAN> REMOVE PRINT QUEUE GLENDA
Do you really want to remove print queue "GLENDA" [YES or NO] (YES) : YES
%PWRK-S-QUEREM, queue "GLENDA" removed from server "TINMAN"

LANDOFOZ\\TINMAN> REMOVE PRINT QUEUE GLENDA1
Do you really want to remove print queue "GLENDA1" [YES or NO] (YES) : YES
%PWRK-S-QUEREM, queue "GLENDA1" removed from server "TINMAN"
```

- To delete a print queue and all pending jobs in that queue except the job currently printing, first use the SET PRINT QUEUE/PURGE command to delete the pending print jobs, then use the REMOVE PRINT QUEUE command.
- To remove a print queue and all jobs in its queue, including the one currently printing, use the following commands, in the order shown:
  1. SET PRINT QUEUE/PURGE — to delete all pending print jobs.
  2. SET PRINT JOB/DELETE — to delete the currently printing job.
  3. REMOVE PRINT QUEUE — to delete the queue.

To delete a print queue, use the REMOVE PRINT QUEUE command, as in the following example:

```
LANDOFOZ\\TINMAN> REMOVE PRINT QUEUE TOTO
Do you really want to remove print queue "TOTO" [YES or NO] (YES) : YES
%PWRK-S-QUEREM, queue "TOTO" removed from server "TINMAN"

LANDOFOZ\\TINMAN>
```

This command removes the print queue called TOTO from the list of print queues known to the server called TINMAN. All jobs in the queue complete before the queue is removed.

#### 5.3.2.7 Managing Print Shares

The following sections describe how to create print shares, set permissions on print shares to control access to the printers, how to change the characteristics of a print share, and how to stop sharing a print queue. To manage print shares, you must be logged on to a user account that is a member of one of the following groups:

- Administrators

- Account Operators
- Server Operators
- Print Operators

There are no special requirements for displaying print share information.

**5.3.2.7.1 Creating an Advanced Server Print Share** To give network users access to a print queue, you share that queue over the network by creating a print share. To access the print queue, network users specify the share name associated with that queue. If you do not specify permissions when you add the print share, it is available to all users. You control user access by specifying permissions for the print share. When multiple permissions apply to a print share, the minimum permission is used. To create a print share, use the ADD SHARE/PRINT command and set permissions for the share. You should add a print share based on a routing queue that points to the specific printer queue. For example:

1. Set up your routing queue.
2. Set up your print share with the same name as the routing queue.

For example, the following command sets up a print share called GLENDA. The share name is the same as the routing queue name, as required by Windows NT.

```
LANDOFOZ\\TINMAN> ADD SHARE/PRINT GLENDA/DESCRIPTION="GLENDA's print share"
%PWRK-S-SHAREADD, share "GLENDA" added on server "TINMAN"

LANDOFOZ\\TINMAN>
```

### 5.3.2.8 Controlling Access to Print Shares

To control user access to print shares, you can assign users to the groups that have the appropriate access permissions, or you can assign permissions directly to shares.

Permissions set on the share will apply to the queue as well. If you do not specify permissions on a print share, the default is to allow access by all users (that is, /PERMISSIONS=(EVERYONE=FULL)). The default setting sets permissions on the share, not on the queue. Any permissions that applied previously to a queue (that is, which previously were associated with another share) are retained and not explicitly visible. Therefore, when you add a print share that points to an existing queue, the queue may have permissions retained from a previous print share, which may conflict with the permissions on the print share. To ensure that permissions are set correctly, set permissions when you set up a new print share.

You can specify the following access permission levels for print shares:

- NONE—Users have no access to the share.
- PRINT—Users have print access to the share. Can pause and delete their own print jobs.
- MANAGE_DOCUMENTS—Users can manage print jobs; for example, pause and delete print jobs not their own.
- FULL—Users have full access to the share. Can modify and delete both shares and queues. This is the default if you do not specify permissions when creating the share.

As part of monitoring printer security, you can enable auditing and keep track of successful and failed attempts to access a print share. The server logs these events in the audit trail. To set auditing for printer access, use the SET AUDIT POLICY command. For example:

```
LANDOFOZ\\TINMAN> SET AUDIT POLICY/AUDIT/SUCCESS=ACCESS/FAILURE=ACCESS
%PWRK-S-AUDPOLSET, audit policy set for domain "LANDOFOZ"
```

See Section 6.1.3.3, Auditing Security Events Domainwide, for information about enabling auditing for printer events.

To set permissions for a shared print queue, use the ADD SHARE/PRINT command or the MODIFY SHARE command. The following example adds a share called WESTWITCH and sets the permissions for the print share so that user SCARECROW has full access to the share, but user LION has no access to the share. The share WESTWITCH is a print share for an existing print queue named WESTWITCH.

```
LANDOFOZ\\TINMAN> ADD SHARE/PRINT WESTWITCH -
_LANDOFOZ\\TINMAN>/PERMISSIONS=(SCARECROW=FULL,LION=NONE)
_LANDOFOZ\\TINMAN>/DESCRIPTION="Shared Print Queue in the Land of Oz"
%PWRK-S-SHAREADD, share "WESTWITCH" added on server "TINMAN"

LANDOFOZ\\TINMAN>
```

#### 5.3.2.9 Changing Print Share Options

The Advanced Server lets you change the options for an existing print share. For example, you may want to revise the share's description. Changes you make take effect immediately for new print jobs, but do not affect jobs already in the queue, except for changes in the routing list. Use the MODIFY SHARE command.

The options you can change include:

- Description

- Maximum number of users (limit)
- Permissions

**5.3.2.9.1 Example: Changing the Maximum Number of Connections for an Existing Print Share** To set the print share TOTO to have no limit on the number of client connections, enter the following command:

```
LANDOFOZ\\TINMAN> MODIFY SHARE TOTO/NOLIMIT
%PWRK-S-SHAREMOD, share "TOTO" modified on server "TINMAN"

LANDOFOZ\\TINMAN>
```

**5.3.2.9.2 Example: To Change the Permissions for an Existing Print Share** The following example modifies permissions for the print share WESTWITCH, so that user LION has PRINT access to the share, and user TINY has MANAGE_DOCUMENTS access to the share:

```
LANDOFOZ\\TINMAN> MODIFY SHARE WESTWITCH -
_LANDOFOZ\\TINMAN>/PERMISSIONS=(LION=PRINT,TINY=MANAGE_DOCUMENTS)
%PWRK-S-SHAREMOD, share "WESTWITCH" modified on server "TINMAN"
```

### 5.3.2.10 Displaying Information About Print Shares, Using ADMINISTER Commands

You can display the print share information, including the permissions on the share. Use the SHOW SHARES /FULL command. For example, to display the permissions for the print share WESTWITCH, enter the following command:

```
LANDOFOZ\\TINMAN> SHOW SHARES WESTWITCH/FULL

Shared resources on server "TINMAN":
Name          Type       Description
-----------   ---------  ---------------------------------------
WESTWITCH     Printer    Shared Print Queue in the Land of Oz
    Path: TOTO
    Connections:  Current: 0, Maximum: No limit
    Share Permissions:
        Everyone                        Full Control
        LION                            Print
        TINY                            Manage Documents
  Total of 1 share

LANDOFOZ\\TINMAN>
```

#### 5.3.2.11 Stopping a Print Share

You may need to stop sharing a print share for several reasons:

- To reorganize shared print queues
- To remove a printer, if this printer is the only printer servicing the queue
- To remove a shared print queue that is no longer needed

To stop sharing a print share, use the REMOVE SHARE command. The queue still exists and can be displayed using the SHOW PRINT QUEUE command, but it is unavailable to network users. Jobs in the print queue complete as usual. For example:

```
LANDOFOZ\\TINMAN> REMOVE SHARE TOTO
Do you really want to remove share "TOTO" [YES or NO] (YES) : YES
%PWRK-S-SHAREREM, share "TOTO" removed from server "TINMAN"

LANDOFOZ\\TINMAN>
```

#### 5.3.2.12 Managing Print Jobs

The Advanced Server lets you display and control print jobs in Advanced Server print queues.

This section provides information about the following topics:

- Displaying print jobs
- Pausing (holding) a print job
- Releasing a print job
- Restarting a print job
- Moving a print job in a print queue
- Deleting a print job

To manage print jobs, you must be logged on to a user account that is a member of one of the following groups:

- Administrators
- Server Operators
- Print Operators

There are no special requirements for displaying print job information.

**5.3.2.12.1 Displaying Print Jobs** To display print jobs, use the SHOW PRINT JOBS command. For example:

```
LANDOFOZ\\TINMAN> SHOW PRINT JOBS

Routing Queue TOTO : ACTIVE
        Job  User Name       Size         Status
        ---- --------------- -----------  ----------
          5  system                  512  QUEUED
          6  system                  512  QUEUED
          7  system                  512  PAUSED

LANDOFOZ\\TINMAN>
```

**5.3.2.12.2 Pausing a Print Job** If you have FULL or MANAGE_DOCUMENTS permission on the share, you can pause (or in OpenVMS terminology, hold) any print job that the queue has not yet sent to the printer. The paused job stays in the queue until you release it; other jobs in the queue are printed. Other users can pause and release their own print jobs.

To pause a print job, use the SET PRINT JOB /HOLD command. For example:

```
LANDOFOZ\\TINMAN> SET PRINT JOB 3330/HOLD
%PWRK-S-JOBSET, print job 3330 held on server "TINMAN"

LANDOFOZ\\TINMAN> SHOW PRINT JOB

Routing Queue TOTO : PENDING
        Job   User Name            Size         Status
        ----  ----------------     ------------ ---------------
        3330  system                        512 PAUSED

LANDOFOZ\\TINMAN>
```

This example pauses or holds print job number 3330.

**5.3.2.12.3 Releasing a Print Job** You can release a print job that has been held. The job prints when it reaches the top of the queue.

To release a print job, use the SET PRINT JOB /RELEASE command. For example:

```
LANDOFOZ\\TINMAN> SET PRINT JOB 3330/RELEASE
%PWRK-S-JOBSET, print job 3330 released on server "TINMAN"

LANDOFOZ\\TINMAN>
```

This example releases the specified print job that was on hold. The job then proceeds to print.

**5.3.2.12.4 Restarting a Print Job** You can restart a print job, printing it again from the beginning. This can be useful if a job is interrupted by an error or printer problem.

To restart a print job, use the SET PRINT QUEUE /RESTART command. For example:

```
LANDOFOZ\\TINMAN> SET PRINT QUEUE TOTO/RESTART
%PWRK-S-JOBACTION, print job 1 at server "TINMAN" has been restarted

LANDOFOZ\\TINMAN>
```

**5.3.2.12.5 Moving a Print Job in a Print Queue** You can use the SET PRINT JOB command to move a print job to the beginning or end of the queue.

To move a print job to the first position in its queue, use the SET PRINT JOB/FIRST command. For example:

```
LANDOFOZ\\TINMAN> SET PRINT JOB 3330/FIRST
%PWRK-S-JOBSET, job 3330 set to first position on server "TINMAN"

LANDOFOZ\\TINMAN>
```

This example moves job number 3330 in the print queue to the first position in the queue. It prints as soon as any currently printing job is done.

To move a print job to the last position in a queue, use the SET PRINT JOB /LAST command. For example:

```
LANDOFOZ\\TINMAN> SET PRINT JOB 3330/LAST
%PWRK-S-JOBSET, job 3330 set to last position on server "TINMAN"

LANDOFOZ\\TINMAN>
```

This example moves print job number 3330 to the last position in the print queue. The print job prints after all other print jobs currently in the queue are done.

**5.3.2.12.6 Deleting a Print Job** If you have FULL or MANAGE_DOCUMENTS permission on the share, you can delete any job that is waiting in a print queue. Other users can delete their own print jobs. Use the SET PRINT JOB /DELETE command to delete a print job. To abort a print job that is currently printing, use the SET PRINT JOB /ABORT command.

To delete a print job, use the SET PRINT JOB/DELETE command, as in the following example:

```
LANDOFOZ\\TINMAN> SET PRINT JOB 3330/DELETE
%PWRK-S-JOBSET, print job 3330 deleted on server "TINMAN"

LANDOFOZ\\TINMAN>
```

This example deletes job number 3330 from the print queue.

To cancel a print job that is currently printing, use the SET PRINT QUEUE/ABORT command.

When you need to shut down a printer immediately, you may need to cancel a print job that is printing. Or you may need to cancel a print job that is printing incorrectly, such as a PostScript file that is printing as an ASCII or text file. For example:

```
LANDOFOZ\\TINMAN> SET PRINT JOB 3330/ABORT
%PWRK-S-JOBSET, print job 3330 aborted on server "TINMAN"

LANDOFOZ\\TINMAN>
```

This example cancels print job number 3330 while it is printing. To restart a deleted job, you must resubmit the print job.

# 6

# Monitoring Events and Troubleshooting

The PATHWORKS Advanced Server provides several ways for you to determine the specific cause of a server problem and to implement a solution.

This chapter describes the procedures you can use to monitor events and troubleshoot problems:

- Section 6.1, Monitoring Server Events, describes commands and utilities that allow you to monitor current server activity and display information about server events in log files, including:
  - ADMINISTER commands
  - Alert messages
  - Event logs
  - Advanced Server log files
- Section 6.2, Troubleshooting Server Problems, describes how to troubleshoot Advanced Server problems.
- Section 6.3, Solving Server Upgrade Problems, describes the procedure for rolling back to the PATHWORKS (LAN Manager) server.

## 6.1 Monitoring Server Events

Advanced Server lets you monitor server events as they happen and capture events in log files. The following sections describe the tools you can use to monitor and evaluate server events.

### 6.1.1 ADMINISTER Commands

Advanced Server ADMINISTER commands let you display information about current server activity and status, as well as recorded events and error messages. In addition, you can use ADMINISTER commands to modify items in the server database to correct certain types of problems.

For example, the SHOW SESSIONS command displays current client sessions. To remove a session that is no longer being used, enter the CLOSE SESSION command.

Refer to the procedures described in Section 6.2.2, The Problem Analysis Process, for information about ADMINISTER commands you can use to help solve certain types of server problems.

### 6.1.2 Automatic Alerts

Advanced Server includes an Alerter service that sends automatic alert messages to specified clients and users when:

- The number of failed logon attempts exceeded the set alert level.
- Errors are encountered during server startup.
- Any event log file is 80% or more full.
- A printer is malfunctioning.
- A print request has been deleted.

The Alerter service can also tell you when certain events occur, as specified by the data associated with the Alerter server configuration parameters in the LANMAN.INI file. You control when the Alerter service sends messages for these events by modifying the appropriate value in the LANMAN.INI file, as described in Section 7.3, Using the LANMAN.INI File.

Table 6–1, Alerter Configuration Parameters, lists the server configuration parameters you can modify to control the way the Alerter service works. You can set the value of each parameter listed in the second column to any positive integer.

**Table 6–1 Alerter Configuration Parameters**

| Desired Action | Parameter to Use | Default Data |
|---|---|---|
| Define the total number of errors that can occur before the server sends an alert message. | **ErrorAlert** | 5 |
| Define the total number of incorrect password attempts that can occur before the server sends an alert message. | **LogonAlert** | 5 |
| Define the total number of resource access violations that can occur before the server sends an alert message. | **AccessAlert** | 5 |

The Alerter service runs automatically when the server starts, if the Alerter service is included in the values associated with the **SrvrServices** server parameter in the LANMAN.INI file. The Alerter service is included in the initial configuration by default. To disable the Alerter service, remove the Alerter name from the list defined for the **SrvrServices** keyword. For more information about services, see Section 2.3.4, Managing Services.

You can specify which Advanced Server users and clients are to receive alert messages. Include the names of these users and clients in the list of values for the **AlertNames** keyword in the SERVER section of the LANMAN.INI file. For more information about LANMAN.INI keywords, see Section 7.3, Using the LANMAN.INI File.

**Note**

Client workstations must be running the Messenger service to receive alert messages. The Messenger service does not run on the OpenVMS system; therefore, users logged on from OpenVMS processes will not receive alert messages.

### 6.1.3 Event Logging

In the Advanced Server, an event is any significant occurrence in the system or in an application that requires user notification. For events that do not require immediate attention, the Advanced Server adds data to an event log file. This event logging service starts automatically every time you start the Advanced Server.

Event logs can provide valuable information about server activities.

Event messages are stored in event files in PWRK$LMROOT:[LANMAN.LOGS]. Each event type is maintained in a separate event log file, as shown in Table 6–2, Event Log Files.

**Table 6–2 Event Log Files**

| Event Type | Event Log File Name | Description |
|---|---|---|
| Application events | APPEVENT.EVT | Application event messages are generated by applications. For example, user-written applications may store messages in the application event log. |
| Security events | SECEVENT.EVT | Event messages are generated based on the audit policy specified for the server, including files or directories. (For more information, see Section 6.1.3.3, Auditing Security Events Domainwide.) |
| System events | SYSEVENT.EVT | System event messages are generated by server components. |

Table 6–3, Information in Event Files, lists the information shown in each line of an event file.

**Table 6–3 Information in Event Files**

| Item | Meaning |
|---|---|
| Source | The server component that logged the message. |
| Class | The event class, either information, warning, error, success audit, or failure audit. |
| Time | The date and time of the event. |
| Category | Classification of the message. |
| Message ID | Unique number for the message. |
| User | The user account name for the user who was logged on and working when the message was logged. N/A indicates that the entry does not specify a user. |
| Computer | The name of the computer where the message was generated. |

### 6.1.3.1 Displaying Events

You can display events recorded in the event log file in either of the following ways:

- If the Advanced Server is running, use the ADMINISTER command SHOW EVENTS.
- If the Advanced Server is not running, use the ELFREAD utility.

These methods are described in the following sections.

**6.1.3.1.1 Displaying Events When the Advanced Server Is Running** The following example shows how use the SHOW EVENTS command to display events while the Advanced Server is running. Use the /TYPE qualifier to specify one of the types of events, as follows: SYSTEM (default), SECURITY, or APPLICATION. In this example, the SHOW EVENTS command displays the system events.

```
LANDOFOZ\\TINMAN> SHOW EVENTS
T Date     Time        Source    Category    Event  User    Computer
- -------- ----------- -------   ----------- -----  ----    -----------
I 08/26/98 11:49:56 AM SYSTEM    None        528    N/A     TINMAN
W 08/27/98 12:07:01 PM Eventlog  None        603    N/A     TINMAN
I 08/27/98 12:15:31 PM Print     None        604    N/A     TINMAN
W 08/27/98 12:46:31 PM BROWSER   None        605    N/A     TINMAN
Total of 4 events

LANDOFOZ\\TINMAN>
```

You can display detailed information for each event, as generated by the application that was the source of the event record, by specifying the SHOW EVENTS/FULL command. The information might include such additional information as the domain and system names. Not all sources or events generate event details. The following example shows a portion of the data that might be displayed with the SHOW EVENTS/FULL command:

```
E 06/05/01 04:13:50 PM NETLOGON  None            5513   N/A        TINMAN
NET5513:   The computer DOROTHY tried to connect to the server TINMAN using
 the trust relationship established by the LANDOFOZ domain. However, the
 computer lost the correct security identifier (SID)
 when the domain was reconfigured. Reestablish the trust
 relationship.

I 06/05/01 03:52:17 PM NETLOGON  None            5715   N/A        TINMAN
NET5715:   The partial synchronization replication of the LSA database
 from the domain controller \\WOODMAN completed successfully. 1 delta(s)
 is(are) applied to the database.
```

```
I 06/05/01 03:36:38 PM NETLOGON  None            5715   N/A        TINMAN
NET5715:   The partial synchronization replication of the SAM database
 from the domain controller \\WOODMAN completed successfully. 1 delta(s)
 is(are) applied to the database.
    .
    .
    .
```

**6.1.3.1.2 Displaying Events When the Advanced Server Is Not Running** To display events when the Advanced Server is not running, use the ELFREAD utility. The ELFREAD utility allows you to display records in the event file in the following ways:

- In reverse chronological order (default)
- In chronological order

You can view records in brief (default) or detailed format.

The ELFREAD command is defined as part of the Advanced Server command set in the SYS$MANAGER:PWRK$DEFINE_COMMANDS.COM command procedure.

The syntax for the ELFREAD command is:

ELFREAD [-o] [-d] *event-type*

Use the optional parameters to control the ELFREAD output as described in Table 6–4, ELFREAD Command Options.

**Table 6–4 ELFREAD Command Options**

| Desired Output | Parameters to Use |
|---|---|
| Records in chronological order | -o |
| Detail records | -d |
| *event-type* | The event log file specified:<br>• SYSTEM<br>• SECURITY<br>• APPLICATION |

#### 6.1.3.2 Saving and Clearing the Event Logs

You can display the event logs and, when necessary, clear the event logs. The Alerter service sends you a message advising you when an event log becomes 80% or more full. When an event file is full, no additional event logging will take place until the event file is cleared. Before clearing an event file, you should save it to a backup file for future reference. The maximum size of an event file is specified by server configuration parameters in the LANMAN.INI file. The server parameter controlling the event log file size is stored in the section associated with each event log and is called MaxSize. (See Section 7.3, Using the LANMAN.INI File, for more information.)

**Note**

Before changing the value of this parameter (or before restarting the server, once you have changed the parameter), you should rename or delete the current event log file to which the parameter applies. Table 6–2, Event Log Files, lists the event log file names.

When an event log becomes full, you can save and clear the event log:

- Saving an event log causes the current event log entries to be written to a specified archive file on the local computer.
- Clearing an event log causes the current event log entries to be deleted.

**6.1.3.2.1 Saving an Event Log** To save an event log, use the SAVE EVENTS command. The event log is stored, using the file name and location that you specify in the command line. For example, to save the Security event log to the file SEVENTS.BKP, enter the following command:

```
LANDOFOZ\\TINMAN> SAVE EVENTS SEVENTS.BKP/TYPE=SECURITY
%PWRK-S-ELFSAVE, Security Event Log from server "TINMAN" saved

LANDOFOZ\\TINMAN>
```

If you do not specify a path as part of the file name, the event file is created in the PWRK$LMLOGS: directory. You can save the event log file of a remote Compaq OpenVMS Advanced Server by specifying the server name with the /SERVER qualifier, as in the following example:

```
LANDOFOZ\\TINMAN> SAVE EVENTS SYSTEM.BKP/TYPE=SYSTEM/SERVER=DOROTHY
%PWRK-S-ELFSAVE, System Event Log from server "DOROTHY" saved
```

This saves the system event log file of server DOROTHY to the file PWRK$LMLOGS:SYSTEM.BKP on server DOROTHY.

You can display the saved event file by using the ADMINISTER SHOW EVENTS /TYPE command, specifying the event file name and location and the types of events to be viewed. See Section 6.1.3.1.1, Displaying Events When the Advanced Server Is Running.

**6.1.3.2.2 Clearing an Event Log** To clear an event log, enter the CLEAR EVENTS command. The specified event log entries are deleted. For example:

```
LANDOFOZ\\TINMAN> CLEAR EVENTS/TYPE=SECURITY
Clear the Security Event Log [YES or NO] (YES) : YES
%PWRK-S-ELFCLEARED, Security Event Log on server "TINMAN" cleared
```

If you do not specify the event log type, the default is to clear the system event log.

### 6.1.3.3 Auditing Security Events Domainwide

The Advanced Server can track selected activities of users by auditing security events and then placing entries in a server's security log. You must enable auditing in order for the server to record security events. By default, auditing is not enabled.

To enable auditing, you must use the SET AUDIT POLICY command, as documented in Section 6.1.3.3.1, Enabling Security Event Auditing. You can use the command to establish an audit policy for the entire domain. (The command affects the security logs of the domain controller and of all server domain controllers in the domain: they all share the same audit policy. Member servers maintain their own auditing policy.) You can select any of several types of security events to be logged in the domain. For example, you can log:

- A systemwide event such as a user logging on or off
- An attempt by a user to access a specific directory or file
- An attempt by a user to rename a user account or change a password

You can select whether successful or unsuccessful attempts at specific operations are to generate event messages.

For more information about setting an auditing policy, see Section 6.1.3.4, Establishing the Audit Policy.

**6.1.3.3.1 Enabling Security Event Auditing** To enable auditing on the server, use the SET AUDIT POLICY command with the /AUDIT qualifier. For example:

```
LANDOFOZ\\TINMAN> SET AUDIT POLICY/AUDIT
%PWRK-S-AUDPOLSET, audit policy set for domain "LANDOFOZ"
```

**6.1.3.3.2 Disabling Auditing** To disable auditing on the domain, use the SET AUDIT POLICY command with the /NOAUDIT qualifier.

### 6.1.3.4 Establishing the Audit Policy

The audit policy defines the types of events to be included in the Security event log. You can change the audit policy for the domain using the SET AUDIT POLICY command.

The SET AUDIT POLICY command lets you specify event results for which auditing is enabled, including both successful and failed attempts to perform certain functions. Include the /SUCCESS qualifier to specify successful completion of operations, and the /FAILURE qualifier to specify failed operations.

The following list shows the events you can specify:

- All events
- None of the events
- Attempts to access a directory or file set for auditing or to send a print job to a shared print queue set for auditing
- Attempts to create, change, and delete user accounts and groups; attempts to rename, disable, and enable a user account; attempts to set or change a password
- Attempts to log on to the domain, log off the domain, and make server connections
- Attempts to change user rights policies, auditing policies, or trust relationships
- Attempts to invoke a program, and handle duplication, indirect accesses, and process exits
- Attempts to restart or shut down the system, and events that affect system security or the security log
- Attempts to exercise a user right (except those associated with logging on and logging off)

For more information about using the SET AUDIT POLICY command, refer to the *Compaq Advanced Server for OpenVMS Commands Reference Manual* or the ADMINISTER command interface online help.

**6.1.3.4.1 Example: Setting the Audit Policy** The following example shows how to use the SET AUDIT POLICY command to log all failures of logon and logoff attempts:

```
LANDOFOZ\\TINMAN> SET AUDIT POLICY/AUDIT/FAILURE=(LOGONOFF)
%PWRK-S-AUDPOLSET, audit policy set for domain "LANDOFOZ"

LANDOFOZ\\TINMAN>
```

### 6.1.3.5 Displaying the Audit Policy

To display the audit policy, enter the SHOW AUDIT POLICY command. This displays the audit policy currently established for the server. For example:

```
LANDOFOZ\\TINMAN> SHOW AUDIT POLICY

Audit Policy for domain "LANDOFOZ":

Auditing is currently Enabled.

Audit Event states:

Audit Event         Success   Failure
------------------  --------  --------
ACCESS              Disabled  Disabled
ACCOUNT_MANAGEMENT  Disabled  Disabled
LOGONOFF            Disabled  Enabled
POLICY_CHANGE       Disabled  Disabled
PROCESS             Disabled  Disabled
SYSTEM              Disabled  Disabled
USER_RIGHTS         Disabled  Disabled

LANDOFOZ\\TINMAN>
```

### 6.1.3.6 Setting and Displaying Security Event Auditing for Files and Directories

You can set and display the audit trail for a specific file or directory using the SET FILE and SHOW FILE commands.

Use the SET FILE command with the /AUDIT qualifier to specify the events to audit.

The following list shows the types of operations you can audit for files and directories:

- All events
- Attempts to display file names, attributes, permissions, owner, or data
- Attempts to create subdirectories and files, change attributes, and display permissions and owner
- Attempts to display attributes, permissions, and owner; attempts to change subdirectories; and attempts to run program files

- Attempts to delete a directory or file
- Attempts to change directory or file permissions
- Attempts to change directory or file ownership

For more information about using the SET FILE command, refer to the *Compaq Advanced Server for OpenVMS Commands Reference Manual* or the ADMINISTER command interface online help.

For example, to set auditing of operations on the user file SIMIANS.DAT, enter the following command:

```
LANDOFOZ\\TINMAN> SET FILE \WITCH\MKEY\SIMIANS.DAT-
_LANDOFOZ\\TINMAN>/AUDIT=(SUCCESS=ALL,FAILURE=ALL)
%PWRK-S-FILEMOD, "\\TINMAN\WITCH\MKEY\SIMIANS.DAT" modified
%PWRK-S-FILESMODIFIED, total of 1 file modified

LANDOFOZ\\TINMAN>
```

**6.1.3.6.1 Example: Displaying the Audit Settings for a File** The following example shows how to display the audit settings for a file, using the SHOW FILES /AUDIT command:

```
LANDOFOZ\\TINMAN> SHOW FILES \WITCH\MKEY\SIMIANS.DAT/AUDIT
\\TINMAN \WITCH\MKEY\SIMIANS.DAT
    SIMIANS.DAT
        Audit Events:                Success         Failure
           LION                      RWXDPO          RWXDPO

Total of 1 file

LANDOFOZ\\TINMAN>
```

## 6.1.4 Advanced Server Log Files

The Advanced Server records several types of messages in log files in the following locations:

- PWRK$LOGS:, the logical name for the directory PWRK$COMMONROOT:[LOGS]
- PWRK$LMLOGS:, the logical name for the directory PWRK$LMROOT:[LANMAN.LOGS]

Table 6–5, Log File Names, lists the log files kept in the PWRK$LOGS and PWRK$LMLOGS areas. In each case, *nodename* refers to the name of the server node.

**Table 6–5 Log File Names**

| Log File Name | Message Type |
|---|---|
| **In PWRK$LOGS:** | |
| NETBIOS_*nodename*.LOG | NetBIOS protocol over DECnet |
| NETBIOS_ERROR.LOG | NetBIOS protocol over DECnet error |
| NETBIOS_OUTPUT.LOG | NetBIOS protocol over DECnet output |
| PWRK$CONFIG_INFO_*nodename*.LOG | Configuration information |
| PWRK$CONFIG_ERROR_*nodename*.LOG | Configuration errors |
| PWRK$KNBDAEMON_*nodename*.LOG | NetBIOS protocol over TCP/IP |
| PWRK$LICENSE_R_*nodename*.LOG | License Registrar |
| PWRK$LICENSE_REGISTRAR_*nodename*.LOG | License Registrar |
| PWRK$LICENSE_S_*nodename*.LOG | License Server |
| PWRK$LICENSE_SERVER_*nodename*.LOG | License Server |
| PWRK$MASTER_*nodename*.LOG | Master process (process start and shutdown) |
| PWRK$NBDAEMON_*nodename*.LOG | NetBIOS protocol over NetBEUI |
| **In PWRK$LMLOGS:** | |
| PWRK$ADMIN_*n _ nodename* .LOG | Remote task command |
| PWRK$LMMCP_*nodename.* LOG | Master control process |
| PWRK$LMSRV_*nodename*.LOG | File server process |
| PWRK$LMBROWSER_*nodename*.LOG | Browser |
| PWRK$UPGRADE.LOG | Upgrade utility |

#### 6.1.4.1 Displaying Log Files

You can use any ASCII text editor to look at log files, so long as the log files are not open (that is, in use by the Advanced Server). Even if open, most log files can be read using the TYPE command. A convenient way to view the end of most log files is to include the /TAIL and /PAGE qualifiers with the TYPE command, as in the following example, where *nodename* is the name of the server node:

```
$ TYPE/TAIL=50/PAGE PWRK$LMLOGS:PWRK$LMSRV_nodename.LOG
```

The log files record messages that have occurred during server operation. Not all the messages in the log need your attention. Many messages are caused by communication problems from which the server recovers automatically. If the server fails to recover from a problem, log files can provide you with information about the cause of the problem.

You can examine messages recorded in any log file. Each line in a log file provides information about logged entries, including a date and time stamp. For example, the PWRK$LMSRV_*nodename*.LOG file might contain information about cache exhaustion conditions.

To examine log files that are in use, use the OpenVMS DCL command BACKUP/IGNORE=INTERLOCK to back them up to a text file, as in the following example:

```
$ BACKUP/IGNORE=INTERLOCK PWRK$LOGS:NETBIOS_DOROTHY.LOG; -
_$ PWRK$LOGS:NETBIOS_DOROTHY.TXT
```

#### 6.1.4.2 The Advanced Server Common Event Log

The Advanced Server provides its own common event log for recording events that cannot be recorded in the System, Security, or Application event logs. These events include process startup and shutdown, autoshare errors, problems caused by underlying OpenVMS errors (such as disk quota exceeded), and failed attempts to connect because of licensing problems.

The Advanced Server provides the ADMIN/ANALYZE utility for viewing events in Advanced Server common event log files. The events are logged in the file PWRK$COMMON:EVTLOG.DAT on each server.

To view output or to purge the EVTLOG.DAT file, enter the following command:

```
$ ADMINISTER/ANALYZE
```

Table 6–6, Event Logger Command Qualifiers, lists the qualifiers you can use with the ADMINISTER/ANALYZE command.

**Table 6–6 Event Logger Command Qualifiers**

| Qualifier | Description |
|---|---|
| /AFTER=*dd-mmm-yy hh:mm:ss.cc* | Restricts the report or the purge operation to events after the specified time. |

(continued on next page)

**Table 6–6 (Cont.) Event Logger Command Qualifiers**

| Qualifier | Description |
|---|---|
| /BEFORE=*dd-mmm-yy hh:mm:ss.cc* | Restricts the report or the purge operation to events before the specified time. |
| /CLASS=*event_class* | Filters the logged events that are written to the report or purged from the EVTLOG.DAT file. The available classes are:<br>• ALL—all events; the default<br>• ERROR—events that affect server operation, but are not necessarily fatal<br>• WARNING—events that do not directly affect server operation; informational |
| /FULL or /BRIEF | The /FULL qualifier generates a report that includes all information logged for each event. The /BRIEF qualifier outputs only the event header and is the default. |
| /INPUT=*event_log_file* | Specifies the name of the event log file. The default file is: SYS$SYSDEVICE:[PWRK$ROOT]EVTLOG.DAT |
| /OUTPUT=*report_file* | Specifies the name of the output file you want the report written to. The default output is written to SYS$OUTPUT. |
| /PID=*pid* | Specifies the process ID whose events you want to display. |
| /PURGE | Purges entries from the EVTLOG.DAT file on the local server.<br>If you use the /PURGE qualifier without other qualifiers, all entries are purged and EVTLOG.DAT file is empty. You can use /PURGE with other qualifiers to specify which entries you want to purge. For example, to purge all events in the EVTLOG.DAT file on the server that are classed as ERROR and written to the file before June 1, 2001, enter the following command:<br>`$ ADMIN/ANALYZE/PURGE/CLASS=ERROR/BEFORE=01-JUN-2001` |

(continued on next page)

**Table 6–6 (Cont.) Event Logger Command Qualifiers**

| Qualifier | Description |
|---|---|
| /SOURCE=*event_source* | Filters the logged events that are written to the report or purged from the EVTLOG.DAT file. The available sources are:<br>• ALL—includes events from all sources; this is the default<br>• COMMON_SERVICES—events originating from common components, such as the PATHWORKS lock manager and PATHWORKS file system<br>• LAN_MANAGER—events originating from LAN Manager<br>• LICENSE_MANAGER—events originating from the license management utility<br>• MANAGEMENT—events originating from the Monitor process or Configurator<br>• MASTER_PROCESS—events originating from the master process, PWRK$MASTER<br>• TRANSPORT—events originating from any of the transports |

Example 6–1, ADMINISTER/ANALYZE Command and Display, shows a sample report from the Event logger generated by the following command executed on the server TINMAN.

**Example 6–1 ADMINISTER/ANALYZE Command and Display**

```
$ ADMINISTER/ANALYZE/INPUT=EVTLOG.DAT

  :::::::::: PATHWORKS Error Log Report ::::::::::
           DATE: 25-JUN-2001 15:52:06.88

   ================ EVENT #1 ==================

Event Time:   18-JUN-2001 17:14:09.04       Node:  TINMAN
Process Id:   000001DB
Event:        Master Process starting
Event Source: Master Process
Event Class:  Audit

      Process Id:   000001DB(X)


   ================ EVENT #2 ==================

Event Time:   18-JUN-2001 17:14:19.57       Node:  TINMAN
Process Id:   000001DB
Event:        NetBEUI Daemon process starting
Event Source: Master Process
Event Class:  Audit

      Process Id:   000002DE(X)


   ================ EVENT #3 ==================

Event Time:   18-JUN-2001 17:14:23.26       Node:  TINMAN
Process Id:   000001DB
Event:        NetBEUI Daemon process shutting down
Event Source: Master Process
Event Class:  Audit

      Process Id:   000002DE(X)
      Status:       SYSTEM-S-NORMAL, normal successful completion

   ================ EVENT #4 ==================

Event Time:   18-JUN-2001 17:14:29.04       Node:  TINMAN
Process Id:   000001DB
Event:        NetBIOS transport process starting
Event Source: Master Process
Event Class:  Audit

      Process Id:   00000262(X)
```

(continued on next page)

**Example 6–1 (Cont.) ADMINISTER/ANALYZE Command and Display**

```
   ================ EVENT #5 ================

Event Time:   18-JUN-2001 17:14:37.19       Node:  TINMAN
Process Id:   000001DB
Event:        LANman Controller process starting
Event Source: Master Process
Event Class:  Audit

      Process Id:   00000282(X)


   ================ EVENT #6 ================

Event Time:   18-JUN-2001 17:14:50.93       Node:  TINMAN
Process Id:   000001DB
Event:        License Registrar process starting
Event Source: Master Process
Event Class:  Audit

      Process Id:   000002D1(X)

                .
                .
                .

   ================ EVENT #19 ================

Event Time:   19-JUN-2001 09:23:34.63       Node:  TINMAN
Process Id:   000003DE
Event:        No license for client - access denied
Event Source: LAN Manager Server
Event Class:  Warning

      Client:   PCGURU

                .
                .
                .

============== EVENT #25 ==================

Event Time:  19-JUN-2001 10:38:11.85       Node:  TINMAN
Process Id:  555749340
Event:        Unexpected System Error Encountered
Event Source: PATHWORKS Printing Services
Event Class:  Error
```

Example 6–2, ADMINISTER/ANALYZE/FULL Command and Display, shows a portion of the more detailed report generated when you use the /FULL qualifier.

**Example 6–2 ADMINISTER/ANALYZE/FULL Command and Display**

```
$ ADMINISTER/ANALYZE/FULL/INPUT=EVTLOG.DAT

  :::::::::: PATHWORKS Error Log Report ::::::::::
           DATE: 25-JUN-2001 15:52:06.88

================ EVENT #1 =================

Event Time:   18-JUN-2001 17:14:09.04       Node:  TINMAN
Process Id:  555749340
Event:        PATHWORKS Lock Database is 90% full
Event Source: Common Services PLM
Event Class:  Warning

0x00000032     Total Database Resources:   50
0x0000002D     Current Resources in Use:   45
0x00000019       Currently open Streams:   25
0x00000017       Currently unique Opens:   23
0x00000004      Currently Locked Ranges:   4

Decode information unavailable (Hex. output):
0x62426141
0x64446343
0x66466545
0x68486747
0x00006949
   .
   .
   .
```

## 6.2 Troubleshooting Server Problems

To troubleshoot server problems, you should be familiar with the following topics:

- OpenVMS system administration and troubleshooting

  The OpenVMS log files, system administration procedures, and parameter settings are described in the OpenVMS operating system documentation.

- Advanced Server concepts

  The Advanced Server concepts are described in the *Compaq Advanced Server for OpenVMS Concepts and Planning Guide.*

- Site-specific network configuration

  Advanced Server provides data-gathering tools that are useful for describing the server and the network environment; in addition, each server system should have a log of the installation and configuration setup, including client requirements and shared resources, network administration accounts, and domain trust information.

- Client environment

  You should be familiar with the software running on the client computers that access the server, including their server requirements and their network capabilities. For clients running PATHWORKS client software, see the extensive PATHWORKS client documentation that describes client configuration, modification, and error messages.

## 6.2.1 Troubleshooting Overview

The following sections describe how to determine the cause of a server problem and solve it if possible. Problem resolution includes determining whether the problem is caused by the Advanced Server software. To solve client-based problems, hardware problems, and application-specific problems, see the documentation for the specific products involved.

Troubleshooting a server problem requires the following stages:

1. Collecting information about the problem
2. Analyzing the problem to determine its characteristics and to isolate the cause of the problem
3. Solving the problem

The following sections describe each stage in more detail.

### 6.2.1.1 Stage 1: Collecting Information About the Problem

When you first detect a server problem, or when the problem is reported, collect as much information as possible immediately. Record the following information:

- The time and date that the problem occurred
- The type of work that the user was performing when the problem occurred, including applications running, shares accessed, and resources used
- Specific information about the network transport the client uses to connect to the server, the server name that the client uses to connect, whether the user account is currently logged on, and the physical location of the client connection to the network

If you are investigating a recurring or ongoing problem, you should, if possible, implement an immediate solution that allows the client to continue working. Record server problems and save a dump file, if one was generated, and save associated log files and data files before restarting the server or changing the server configuration. You can use the information gathering command procedure SYS$STARTUP:PWRK$GATHER_INFO.COM to save these files.

#### 6.2.1.2 Stage 2: Analyzing the Problem

When you analyze the server problem, you should also look for the solution to the problem. Therefore, you must isolate the component that needs to be modified, replaced, removed, or enhanced.

Advanced Server software provides information in log files and tools to help you determine the cause of a server problem. These tools keep records of activities and errors. You can use them to isolate problem areas and to help solve problems. You may be able to solve the problem using the Advanced Server commands and utilities.

#### 6.2.1.3 Stage 3: Solving the Problem

The cause of a server problem may be within your ability to correct. At best, you may determine a configuration or definition change that will correct the problem. Or, you may be able to modify a server parameter or disable a service until the problem is solved more satisfactorily.

The procedure for solving a server problem depends on your ability to capture information about the problem and the state of the server at the time of the problem. If a problem is reported to be intermittent and is difficult to reproduce at will, the procedure for analysis and solution will take longer and be more difficult. Thus, it is particularly important to collect detailed information as soon as the problem is reported.

The following sections show how to use the Advanced Server tools in the problem-solving process. Using these tools, you can modify the server to report on network activity and events, providing more detailed investigation of problems that you have already determined to be caused by the server or its network resources.

If you cannot determine the cause of a server problem, or if you cannot solve the problem, report the problem to your software specialist and keep the Advanced Server data structure PWRK$LMROOT and the log files for future analysis.

To help you report the information required for analyzing a server problem, the Advanced Server software includes a procedure you can run to gather server information.

**6.2.1.3.1 Gathering Information About Server Status** To invoke the procedure provided by the server to gather server status information, enter the following commands:

```
$ SET DEFAULT SYS$STARTUP
$ @PWRK$GATHER_INFO.COM
```

The resulting file (PATHWORKS_AS_INFO.BCK) is a BACKUP saveset containing copies of the Advanced Server database, logs, and, if present, process dump files.

If the problem you are investigating causes a systemwide failure, create a dump file for the system. The system dump file captures system information. Be sure to verify that your system dump file size is sufficient to capture a full system dump.

## 6.2.2 The Problem Analysis Process

Problem analysis is a process of elimination. Given little information to start, you must begin at the general level and use the information-gathering tools described in this chapter to determine the area from which the problem originates. If you have sufficient information at the beginning to isolate the problem area or if the problem is ongoing or if you can reproduce the problem, you can proceed directly to the section in this chapter that addresses the type of problem you are investigating.

The problem-solving procedure differs depending on the type of problem reported. The following sections describe several types of problems, in analytical order, from the generic characteristics of server problems to the more specific.

Problem types are characterized by behavior or source as follows:

- Intermittent
- Domain and Computer
- Server operation
- Services
- Client connection
- Share access
- Printer
- User account
- Privileged user

- Advanced Server connection
- License acquisition

#### 6.2.2.1 Intermittent Problems

Intermittent problems are those that are not easily reproducible. They may not prevent server operation, like ongoing problems, and they may be difficult to analyze and solve. For these types of problems, your analysis depends heavily on the log files and messages reported before and during the time the problem occurred. To help locate such problems, you can use network traces, both on the condition where the problem can be reproduced, and when the problem is intermittent.

Table 6–7, Procedure for Solving Intermittent Problems, describes how to determine the cause of an intermittent problem and what to do about it.

**Table 6–7 Procedure for Solving Intermittent Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | Record the time and date when the problem occurred, the nature of the symptoms, the computer name of the client, if any. Related information can include applications that have connections to the server, server shares, and resources consumed by the client. | Check for alerts around the time the problem occurred. Attempt to reproduce the problem on the same client and on other clients in the domain. | You can enable and modify the Alerter service to provide more specific, immediate error notification, as described in Table 6–1, Alerter Configuration Parameters. If the problem circumstances can be reproduced, use the Alerter service to watch the messages during the occurrence of the problem. |

(continued on next page)

**Table 6–7 (Cont.) Procedure for Solving Intermittent Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 2 | If the problem is unique to a specific group or one client, see Analyze the Problem in the next column of this table.<br>If the problem is continuous, or if you can reproduce the problem at will, continue to the section Domain and Computer Problems. | Use the SHOW EVENTS command to see the event messages that were recorded for the time the problem occurred. Enable additional event/audit tracking to get more detailed information. See Section 6.1.3 in this guide for more information.<br>Check Advanced Server log files for additional messages, as described in Section 6.1.4, Advanced Server Log Files. | Review events and log files to isolate the cause of the problem and address it accordingly.<br>Intermittent problems that do not prevent use of the server may be due to faulty hardware. Check the connections to the client, the client configuration, and the network hardware. |

#### 6.2.2.2 Domain and Computer Problems

The domainwide functions of the server depend on its role in the domain and on the other servers in the domain. The Advanced Server command-line interface lets you display information about the domain and modify server activity in the domain.

Table 6–8, Procedure for Solving Domain and Computer Problems, describes how to determine the cause of domain and computer problems and what to do about it.

**Table 6–8 Procedure for Solving Domain and Computer Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | Determine whether users of other computers in the domain receive error messages when attempting to connect to a server, or whether server administrators receive error messages using ADMINISTER commands. | If so, the problem may be due to a server's relationship to the other servers in the domain. Use the SHOW COMPUTERS command to determine the status of other computers in the domain. | Use the REMOVE COMPUTER command to take the computer off the domain.<br>Use the SET COMPUTER /ACCOUNT_ SYNCH command to synchronize the security accounts database across the domain.<br>Use the SET COMPUTER/ROLE command to change the server role of a server in the domain, as described in Section 2.1.1.1, Changing a Server's Role in a Domain. |

(continued on next page)

**Table 6–8 (Cont.) Procedure for Solving Domain and Computer Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 2 | Determine whether domain problems require changes on multiple servers in the domain. | Use the SHOW ADMINISTRATION command to display the server and domain name of the server currently being administered. | Use the SET ADMINISTRATION command to set the server and domain name of the server to be managed, as described in Section 2.1.4, Administering Another Domain. |
| 3 | When setting up trusts between domains, you receive the error message "Could not find domain controller for this domain." | Check that each domain has a running domain controller.<br>Check that both domains are running the same transport protocol (TCP/IP, DECnet, or NetBEUI). | Start at least one server in each domain.<br>Use the Configuration Manager to enable the same transport on both domains, as described in Section 7.2, Using the Configuration Manager. |

#### 6.2.2.3 Server Operation Problems

If the server fails to complete routine operations, the log files and error messages from the software usually indicate the nature and source of the problem.

Table 6–9, Procedure for Solving Server Operation Problems, describes how to determine the cause of a problem in server operation and what to do about it.

**Table 6–9 Procedure for Solving Server Operation Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | Check the error messages seen during failing procedures and operations. | Use Advanced Server log files to display messages about problems during software startup and operation. | Use the Configuration Manager to modify server parameters that affect the way the server runs, as described in Section 7.2, Using the Configuration Manager, or modify server configuration parameters, as described in Section 7.3, Using the LANMAN.INI File. |
| 2 | Check service startup failures, which are logged in the system event log files. | Use the SHOW EVENTS command to display system events. | Use the START SERVICES and STOP SERVICES commands to manage services, as described in Section 2.3.4, Managing Services. |

**6.2.2.3.1 Monitoring Data Cache Use by the File Server** Advanced Server uses its data cache for caching the security databases, in addition to client file data. To ensure a balance of cache usage, the file server periodically monitors its use of the data cache, as follows:

- Total security databases utilization

  The file server monitors the total utilization of the data cache by the security databases. If the file server detects that the utilization of the data cache for these files exceeds thirty-five percent (35%), a warning message is posted to the file server log file indicating that the current

cache configuration may not be adequate for the current load imposed on the file server.

For example:

```
BlobCache Warning: Sum of Blob file control areas
                   is 950272 bytes (45% of data cache).
```

The condition reported by this warning message will not prevent the file server from being able to properly process requests associated with the security databases. The message (shown below) indicates that you should increase the size of the data cache.

- Individual security database utilization

  The file server monitors utilization of the data cache by individual security database files. When the database expands in size, more cache resources are required to continue operating. If the file server detects that an operation will cause a database file expansion, and that expanding the database file will cause it to utilize more than fifty percent (50%) of the data cache, error messages are recorded in the file server log, as in the following example:

  ```
  BlobCache Error: The largest single Blob file control area
                   is 1187840 bytes (57% of data cache).

  BlobCache Error: The largest single Blob file control area
                   is PWRK$LMROOT:[LANMAN.DOMAINS]DOMAIN1.
  ```

  In addition to recording the problem in the file server log, the software generates an operator message and raises a server alert.

  These messages indicate that the operation will prevent the file server from completing the current and future operations. In this case, you should use the Configuration Manager (ADMIN/CONFIG), as described in Section 7.2, Using the Configuration Manager, to increase the size of the data cache so that utilization of the data cache by a single database file remains under 50%. The change to the data cache size takes effect the next time you start the server.

You can use the ADMIN/ANALYZE command to monitor these warning messages and error messages, as described in Section 6.1.4.2, The Advanced Server Common Event Log.

#### 6.2.2.4 Problems with Services

Advanced Server software includes several optional services. For example, Auditing is a service useful for analyzing server problems. However, the services must be enabled.

Table 6–10, Procedure for Solving Service Problems, describes how to determine the cause of a network service problem and what do to about it.

**Table 6–10 Procedure for Solving Service Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | Check whether the services are running. | Use the SHOW SERVICES command to display the services that are running. | Use the following commands to control the operation of the services:<br>START SERVICE<br>STOP SERVICE<br>PAUSE SERVICE<br>CONTINUE SERVICE<br>(See Section 2.3.4, Managing Services, for more information.) |

#### 6.2.2.5 Client Connection Problems

Clients may be individually or collectively reporting a failure to connect to the server or reporting slow response time in connecting to the server or the share.

Table 6–11, Procedure for Solving Client Connection Problems, describes how to determine the causes behind many typical client connection problems and what to do about them. For information about problems connecting to shares or specific files, see Section 6.2.2.6, Share Access Problems.

**Table 6–11 Procedure for Solving Client Connection Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | If a client cannot end a session or there are too many sessions, you can control the user sessions. | Use the SHOW SESSIONS command to display current Advanced Server client sessions. | Use the CLOSE SESSION command to close unneeded sessions. |
| 2 | If more than one client reports a problem when connection to the server is lost or with slow response time, the problem may be caused by too many connections to the same server. | Use the SHOW CONNECTIONS command to display the connections that clients have established to Advanced Server shares. | Use the CLOSE CONNECTION command to end one or more connections. |
| 3 | When a client tries to log on over a WAN, the following message is received: "You were logged on, but have not been validated by a server." | Clients may use NetBIOS broadcasts to send logon requests, and these requests do not go over the router. | To locate domain controllers capable of authenticating logons, use a WINS Server or LMHOSTS entries that include the #DOM directive. |

#### 6.2.2.6 Share Access Problems

Clients may fail to connect to shares or lose existing connections. The shares must be set to permit client access. Share setup includes:

- Allowing access to users who are members of user groups that have access to the share
- Setting permissions to allow access to the share such as read access
- Setting OpenVMS file and directory protections, if the Advanced Server and OpenVMS security model is in use
- Setting the maximum connection limit to allow the required connects

Table 6–12, Procedure for Solving Share Access Problems, describes how to determine the causes behind some typical share access problems and what to do about them.

**Table 6–12 Procedure for Solving Share Access Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | Determine whether the client is connected but failing to access resources in the shares. For example, the client computer displays the connection to the server but is unable to list all the files and directories to which the client requires access. | Use the SHOW USER command to display the groups to which the user belongs.<br>Use the SHOW SHARE command to display the groups allowed to access the share. | To add the user to a group, use the MODIFY GROUP command to add the user name. To let the user's group access a share, use the MODIFY SHARE/PERMISSIONS command, as described in Section 4.3.4, Changing Share Properties. |

(continued on next page)

**Table 6–12 (Cont.) Procedure for Solving Share Access Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| | | Use the SHOW FILE command to display access permissions on the resources. If the OpenVMS and Advanced Server security model is enabled, use the OpenVMS command DIRECTORY/SECURITY to display the OpenVMS owner and protection information. | Use the server SET FILE/PERMISSIONS command, as described in Section 4.3.5.2, Setting Permissions on a File or Directory, to modify the permissions on the file to give the user or group access to the specific resource. Use the OpenVMS SET FILE/PROTECTION command to modify the RMS protections on a directory or file. |
| | | Use the Advanced Server SHOW HOSTMAP command to display host mapped user accounts. | Use the ADD HOSTMAP command, as described in Section 3.1.16.2, Establishing User Account Host Mapping, to associate a network user account with an OpenVMS user account. |
| 2 | If some clients report problems connecting to a share, the problem may be caused by too many connections. | Use the SHOW SHARES command to display information about the connection limit on the share. | Use the MODIFY SHARE command to change the connection limit on the share, as described in Section 4.3.4, Changing Share Properties. |

(continued on next page)

**Table 6–12 (Cont.) Procedure for Solving Share Access Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 3 | If clients report failure to access a specific file, the problem may be caused by incorrect permission settings on the file. | Use the SHOW FILE command to display files that are open, clients who have the files open, and the permissions granted to the clients. | Use the SET FILE /PERMISSIONS command, as described in Section 4.3.6, Specifying File and Directory Access Permissions, to set the file permissions correctly. |

#### 6.2.2.7 Printer Problems

Problems with the print software can occur after changes in hardware configuration or print queues. The Advanced Server provides commands to modify and remove print jobs and print queues.

Table 6–13, Procedure for Solving Printing Problems, describes how to determine the causes behind some typical printing problems and what to do about them.

**Table 6–13 Procedure for Solving Printing Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | Obtain the physical printer name, the print queue name, the print share name, and the specific print command used to submit the print job. | Use the SHOW PRINT JOBS command to display information about print jobs.<br>Set the audit policy to record printer-related events by using the following command: ADMINISTER SET AUDIT POLICY/SUCCESS=ACCESS. | Use the SET PRINT JOB command to change the status of a print job or delete a print job, as described in Section 5.3.2.12, Managing Print Jobs. |

(continued on next page)

**Table 6–13 (Cont.) Procedure for Solving Printing Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 2 | During printer maintenance and when printers are off line, you may need to prevent users from submitting print jobs. | Use the SHOW PRINT QUEUE command to display information about the print queue, the print jobs in the print queue, and the status of the print queue. | Use the following commands to control the print queue while you correct the problem:<br>• PAUSE PRINT QUEUE<br>• CONTINUE PRINT QUEUE<br>• REMOVE PRINT QUEUE<br>See Section 5.3.2, Managing Printers Using the Advanced Server ADMINISTER Command-Line Interface, for more information. |
| 2 | Windows NT, Windows 95, Windows 98, or Windows 2000 client cannot print to a shared print queue. | Use the ADMINISTER SHOW SHARES/TYPE=PRINT command to view the shared print queues. | The share name and the queue name must differ for printing from these Windows clients. |

#### 6.2.2.8 User Account Problems

When one user reports a problem connecting to the server or a share, establish whether the problem is caused by the Advanced Server user account definition. You can help users with password problems immediately, by changing their passwords.

Table 6–14, Procedure for Solving User Account Problems, describes how to determine the causes of typical problems in user account definition and what do to about them.

If a client reports a failure to log on to the network, use the procedure described in this table.

**Table 6–14 Procedure for Solving User Account Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | Determine whether the user account is set up properly. | Use the SHOW USER command to display user account information. Look for logon restrictions, such as logon hours, which might give the client access only during specific hours of the day and days of the week. Check also whether the account has expired or is locked out. | Use the MODIFY USER command to change user account information like restricted hours, or to unlock the user account, as described in Section 3.1.3, User Account Attributes. |
| 2 | Determine whether the user is entering the correct password. | | Use the SET PASSWORD command to change a user account password, as described in Section 3.1.5, Specifying Passwords. |

#### 6.2.2.9 Privileged User Problems

Users with responsibility for privileged operations, such as administrators, printer operators, and server operators, may receive error messages when attempting to use privileged commands and procedures. Make sure the user is a member of the appropriate group.

If users are unable to perform privileged operations, use the procedure described in Table 6–15, Procedure for Solving Problems of Privileged Users, to determine the cause of the problem and what to do about it.

**Table 6–15 Procedure for Solving Problems of Privileged Users**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | Determine whether users are unable to perform administrative operations on a file, such as deleting the file, modifying file protections, and displaying directory information about the file. | Check the user accounts and predefined groups for operators and administrators. | If an Advanced Server user does not have the required user rights, use the MODIFY USER/ADD_TO_ GROUP command to add the user to the appropriate groups, as described in Section 3.1.14, Modifying User Accounts. |
| 2 | Determine whether users are unable to perform administrative operations on a file, such as deleting the file, modifying file protections, and displaying directory information about the file. | Use the SHOW FILES command to display the permissions set on the file. Use this information to notify users of changes you plan to make to the file. | Use the TAKE FILE OWNERSHIP or SET FILE /PERMISSIONS command to obtain the desired control over a file and set permissions appropriately, as described in Section 4.3.10, Taking Ownership of Files or Directories, and Section 4.3.6, Specifying File and Directory Access Permissions. |

#### 6.2.2.10 Problems Connecting to the Advanced Server

Clients and servers in the network that communicate with the Advanced Server to perform various tasks might receive error messages when attempting to locate the Advanced Server. Table 6–16, Procedure for Solving Problems Connecting to the Advanced Server, describes how to determine the cause of host-to-host communication problems and what do about it.

**Table 6–16 Procedure for Solving Problems Connecting to the Advanced Server**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | The client computer receives the following error when attempting to map a network drive:<br>"Network path not found" | Can the client communicate with any other system on the network? Use PING or NCP LOOP commands against other systems on the same physical segment. | Check the physical cabling and network adapter of the client for loose connections. |
| | | Can the client communicate with the target server at the transport level? For example, can the client PING or TELNET to the server using the server's IP address? If a Wide Area Network path is used, verify communication along each segment of the network using a utility such as Tracert. | Check the transport configuration such as IP address, subnet mask, broadcast address, and default gateway/routes of systems involved. |

(continued on next page)

**Table 6–16 (Cont.) Procedure for Solving Problems Connecting to the Advanced Server**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| | | Can the source system resolve the NetBIOS name(s) of the target system, and can the target server resolve the NetBIOS name(s) of the source system? You can use tools such as NBTSTAT.EXE on Windows systems and NBSHOW[1] KNBSTATUS on Advanced Server and PATHWORKS systems to perform limited NetBIOS name resolution testing. In addition, you can use Windows NT Resource Kit utilities such as DOMMON, NLTEST, and BROWSTAT to test connectivity. | Ensure NetBIOS name registration is occurring on the correct WINS Server or that appropriate NetBIOS names are represented in LMHOSTS files. |
| | | Is the problem license related? | See Section 6.2.2.11, License Acquisition and Validation Problems. |
| | | Is the Advanced Server file server process running? Use the PWSHOW command and verify that the PWRK$LMSRV process is present. | If the PWRK$LMSRV process is not running, restart the Advanced Server with the command PWRESTART. |

[1]The NBSHOW command and other Advanced Server management commands are defined in the SYS$STARTUP:PWRK$DEFINE_COMMANDS.COM command file; for more information, refer to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide.*

(continued on next page)

**Table 6–16 (Cont.) Procedure for Solving Problems Connecting to the Advanced Server**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 2 | The client computer receives the error "Network name not found." | This error usually indicates that the share name cannot be found or the share path is not available. Use the ADMINISTER SHOW SHARE/PATH command to verify that the share exists and the share path is correct. Verify that the share path is available (that is, that the device reference is valid). Use the ADMINISTER/ANALYZE command to check for device and autoshare related errors. | If the share path is incorrect, the share must be removed and added again using the correct path.<br>If the device is not mounted, mount it.<br>For autoshare errors, change the volume label to 11 characters or less or establish a different autoshare name for the device as described in Section 4.2.3.2, Defining Autoshares.<br>If the device was mounted after the Advanced Server started, use the following ADMINISTER command to make it accessible to the Advanced Server: SET COMPUTER/ AUTOSHARE_ SYNCHRONIZE. |

#### 6.2.2.11 License Acquisition and Validation Problems

For a client to use the services of a PATHWORKS V6.1 for OpenVMS (Advanced Server) server, the minimum license required is the Client Access license PWLMXXXCA07.03, or an equivalent client virtual license. A client can acquire either one of the following:

- Client-based license from a License Server
- Server-based license from the Advanced Server system to which the client connects

A client-based license is acquired once, and thereafter it is verified during client startup. The License Server is responsible for assigning and verifying client-based licenses. Once acquired, the client-based license is presented for validation when establishing a session to any PATHWORKS server. The License Registrar on each PATHWORKS server is responsible for validating client-based licenses or assigning a server-based license, if available, when clients establish a session.

A server-based license is assigned to a client only for the duration of the client's session with the server.

Note that client-based licensing involves two distinct operations:

- Obtaining (or verifying, once initially acquired) the appropriate license from a License Server during startup
- Validating the appropriate license when establishing a session to an Advanced Server.

Clients using client-based licensing may report license acquisition (or verification) problems during startup. These problems typically result in a "LICnnnn error" being displayed on the client. Refer to the *Compaq Advanced Server for OpenVMS Guide to Managing Advanced Server Licenses* for more information about these messages.

All clients, whether using client-based licensing or not, may also report problems connecting to a server that could be the result of a license validation issue. Table 6–17, Procedure for Solving License Validation Problems describes how to determine the cause of license validation problems and what to do about it.

**Table 6–17 Procedure for Solving License Validation Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 1 | When mapping a network drive, the Windows NT or Windows 2000 client sees:<br>• The error message: "A connection to the server could not be made because the limit on the number of concurrent connections for this account has been reached."<br>• If the Alerter service is running on the server, a Messenger pop-up window indicating that the connection attempt was denied because the server failed to authenticate a license for the client. | If a license problem is preventing a client from connecting to a server, a warning message is written to the Advanced Server common event log ($ ADMIN/ANALYZE) indicating "No server license for client - access denied," along with the name of the client. | Add server-based licenses to the server, or check the License Server to ensure adequate client-based licenses are available to clients. For more information, refer to the *Compaq Advanced Server for OpenVMS Guide to Managing Advanced Server Licenses*. |
| | | Also check for applicable messages in the License Registrar log file on the server (PWRK$LICENSE_REGISTRAR_*nodename*.LOG). | Extend the logging performed by the License Registrar process, and then recheck the PWRK$LICENSE_REGISTRAR_*nodneame*.LOG file for errors. For details on logging capabilities, see the comments in the License Registrar process startup file, SYS$STARTUP:PWRK$LICENSE_R_START.COM. |

(continued on next page)

**Table 6–17 (Cont.) Procedure for Solving License Validation Problems**

| Step | Stage 1: Collect Information | Stage 2: Analyze the Problem | Stage 3: Solve the Problem |
|---|---|---|---|
| 2 | When mapping a network drive, the Windows 95 or Windows 98 client sees the following error message: "The local device type and the network resource type are not the same." | See analysis instructions above. | See problem-solving instructions above. |

## 6.3 Solving Server Upgrade Problems

If your server was previously running PATHWORKS (LAN Manager), and you encounter a problem that is completely unsolvable, you can remove the newly installed software using the Rollback command procedure provided with PATHWORKS Advanced Server. The Rollback procedure must have been enabled during the server installation procedure. Refer to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Migration Guide* for information about reverting to the previous version of the server.

**Caution**

Using the Rollback procedure restores your environment to PATHWORKS (LAN Manager) at the time of PATHWORKS Advanced Server installation. Therefore, information about changes made while PATHWORKS Advanced Server was running, like newly added users or changed permissions, will be lost.

# 7

# Managing Server Configuration Parameters

The Advanced Server allows you to make adjustments to the server software configuration after running the server configuration procedure, PWRK$CONFIG.COM. You can use the Configuration Manager (invoked by the ADMINISTER/CONFIGURATION command) to modify parameters affecting the system environment. You can edit the LANMAN.INI file to modify server-specific parameters that are not modifiable with PWRK$CONFIG.

This chapter explains how to use Configuration Manager and how to modify the parameters stored in the LANMAN.INI file. This chapter includes the following sections:

- Section 7.1, Overview of Server Configuration, describes the server configuration environment and distinguishes the server system-specific parameters that are modifiable using the Configuration Manager (ADMINISTER/CONFIGURATION) from the server-specific LANMAN.INI parameters.
- Section 7.2, Using the Configuration Manager, describes how to use the Configuration Manager to manage the server's system environment configuration.
- Section 7.3, Using the LANMAN.INI File, describes the structure of the LANMAN.INI file and how to modify its contents.

## 7.1 Overview of Server Configuration

The PWRK$CONFIG configuration procedure allows you to modify parameters that determine the server's system environment and parameters affecting the initial configuration of the server itself.

### 7.1.1 Server System Environment Parameters

When the PWRK$CONFIG.COM configuration procedure prompts you whether you want to "change server configuration parameters," it is giving you the option to modify the system environment parameters, using the Configuration Manager, a character-cell user interface. These are server-specific parameters that are not stored in the LANMAN.INI file. These parameters are, for the most part, directly or indirectly related to the environment in which the Advanced Server operates, such as the server's usage of OpenVMS system resources (physical memory, for example). Examples of these parameters include the server's client capacity, the size of its data cache, and which network transports it should use.

You can adjust these parameters after running PWRK$CONFIG by invoking the Configuration Manager with the ADMINISTER/CONFIGURATION command.

### 7.1.2 Server-Specific LANMAN.INI Configuration Parameters

The main function of the PWRK$CONFIG.COM configuration procedure is to let you set up or modify your initial Advanced Server configuration. For example, it allows you to specify:

- Whether to run the License Server
- Whether to enable specific services
- The domain name
- The server role in the domain
- The computer name
- The server cluster alias
- The server description

Your responses to the PWRK$CONFIG.COM configuration procedure prompts determine the values of parameters (keywords) stored in the LANMAN.INI file. The LANMAN.INI stores other server-specific parameters that are not modified by means of the PWRK$CONFIG.COM configuration procedure. The defaults for these parameters are appropriate for most typical environments. However, you can modify these by editing the LANMAN.INI file. These parameters affect the behavior of the Advanced Server but not, for the most part, file server resource consumption. These include parameters that affect Browser activity, network logon, and the function of other services; and values that define the shares created automatically by the Advanced Server.

When the PATHWORKS Advanced Server is installed, the LANMAN.INI file contains values for certain parameter keywords. Other keywords, and the titles of the sections to which they belong, are added when you run the Configuration Manager or edit the LANMAN.INI file. If a keyword does not appear in the file (or is commented out with a semicolon), it is set to its default value.

## 7.2 Using the Configuration Manager

The Configuration Manager has a character-cell user interface. If you are using DECterm or an equivalent terminal emulator, you can access all the functions of the Configuration Manager using a mouse input device. If you are using a keyboard to control the Configuration Manager, see Section 7.2.8, Navigating the Configuration Manager Using a Keyboard, for information about the keys you can use to control the Configuration Manager.

The server parameters you can modify using the Configuration Manager include:

- Basic configuration parameters, including:
  - The client capacity of the server
  - The percentage of free physical memory to be considered available to the server
  - The size of the server's data cache
  - The maximum number of concurrent user signons
  - The OpenVMS process priority for the server process
- Advanced configuration parameters, including:
  - Enabling and disabling open file caching, which delays the actual closing of user files
  - The time interval controlling open file caching
  - The average number of files allowed open per client
  - The average number of byte range locks held per client
  - Enabling and disabling dynamic security upgrading of PATHWORKS V5 for OpenVMS (LAN Manager) files
  - The security model that the server uses at the file access level
- Transport parameters, including:
  - The selection of transports enabled

- The wide-area networking (WAN) capabilities of the server, if any

Each type of parameter is presented on a separate screen by the Configuration Manager. Each parameter is described in more detail in a later section.

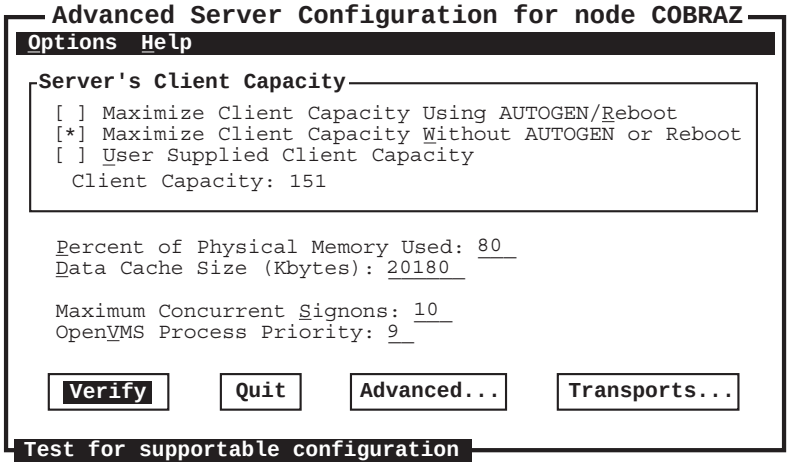
### 7.2.1 Starting the Configuration Manager

To start the Configuration Manager, log in to the OpenVMS SYSTEM account, or to an account with similar privileges, and enter the following command:

```
$ ADMINISTER/CONFIGURATION
```

The screen shown in Figure 7–1, Basic Configuration Parameters Screen, appears.

**Figure 7–1 Basic Configuration Parameters Screen**




VM-0215A-AI

The Basic Configuration Parameters screen allows you to modify the basic server configuration parameters and provides access to the Advanced Configuration Parameters screen and the Transport Configuration Parameters screen. It allows you to verify the current configuration settings or to quit the Configuration Manager without changing any configuration settings, and provides online help information through the Help menu.

### 7.2.2 Exiting the Configuration Manager

To exit the Configuration Manager, select one of the following buttons on the Basic Configuration Parameters screen, and press the Enter or Return key:

- The **Verify** button allows you to verify and save the configuration you have established. For more information about saving and verifying your parameter settings, see Section 7.2.7, Verifying and Saving the New Configuration.
- The **Quit** button allows you to exit the Configuration Manager without saving your changes to the server parameters. To quit the Configuration Manager, select the Quit command button and press the Enter or Return key, choose the Quit menu item in the Options menu, or press Ctrl/Z.

### 7.2.3 Getting Help on the Configuration Manager

To get help while running the Configuration Manager, select the Help menu at the top of the Basic Configuration Parameters screen.

From the Help menu, you can choose to display the following types of information:

- The **Overview** menu item describes the purpose and operation of the Configuration Manager.
- The **Basic configuration** menu item describes the server parameters you change on the Basic Configuration Parameters screen.
- The **Advanced configuration** menu item describes the server parameters you change on the Advanced Configuration Parameters screen.
- The **Transport configuration** menu item describes the server parameters you change on the Transport Configuration Parameters screen.

The following sections describe each screen and each parameter in detail.

### 7.2.4 Modifying Basic Configuration Parameters

The first screen that appears when you start the Configuration Manager is the Basic Configuration Parameters screen. It allows you to change the basic server configuration parameters, as described in the following sections.

#### 7.2.4.1 Specifying a Server's Client Capacity

Client capacity is the maximum number of client sessions the server can support at a time. You can enter a value, or you can let the Configuration Manager determine a value based on current resources.

To specify the client capacity, on the Basic Configuration Parameters screen:

1. Select User Supplied Client Capacity.
2. Enter the new value in the Client Capacity text box.

The Configuration Manager may need to run AUTOGEN or reboot your system to make additional resources available to support such a configuration.

To allow the Configuration Manager to determine the appropriate setting, select one of the following:

- Maximize Client Capacity Using AUTOGEN or Reboot

  Determines the maximum number of clients the server can accommodate simultaneously given the maximum resource capacity of your system. The Configuration Manager may need to run AUTOGEN, reboot your system, or do both, to make additional resources available to support such a configuration.

- Maximize Client Capacity Without Using AUTOGEN/Reboot

  Determines the maximum number of clients the server can accommodate simultaneously, using the system resources currently being accessed. You do not need to run AUTOGEN or reboot the system for such a configuration.

To determine the maximum number of clients, use the following procedure:

1. Make sure the values on the Advanced Configuration Parameters screen and the Transport Configuration Parameters screen are correct.
2. Choose one of the Client Capacity option buttons on the Basic Configuration Parameters screen to control the way the determination will be made.
3. Select the Verify command button to verify and save the server parameter settings, as described in Section 7.2.7, Verifying and Saving the New Configuration.

After you determine the maximum number of clients the server will accommodate, be sure that the network transports you want to use can accept at least this many links. If not, configure the transports to accept more links.

- For the DECnet family of products, the configuration change depends on the version of DECnet. For DECnet Phase IV, the default maximum number of transport links is 32. For this version of DECnet, you can

configure the transport to accept 100 links by entering the following commands:

```
$ MCR NCP DEFINE EXECUTOR MAXIMUM LINKS 100
$ MCR NCP SET EXECUTOR MAXIMUM LINKS 100
```

- For DECnet-Plus, the default maximum number of transport links is 200. To raise this maximum to 300, enter the following commands:

  ```
  $ MCR NCL SET NODE 0 NSP MAXIMUM RECEIVE BUFFERS 6000
  $ MCR NCL SET NODE 0 NSP MAXIMUM TRANSPORT CONNECTIONS 300
  ```

  Note that the number of receive buffers should be set to 20 * *n*, where *n* is the maximum number of transport connections. In addition, be sure to edit the NET$LOGICALS.COM file to increase the NET$ACP quotas appropriately.

For more information about configuring the DECnet transport, refer to the *Compaq DECnet for OpenVMS Network Management Utilities* manual.

#### 7.2.4.2 Specifying the Percent of Physical Memory Used

The Configuration Manager allows you to specify the maximum percentage of the system's physical memory that the configuration may use, primarily for the number of clients and the data cache size. For example, if you set the value to 50%, and your Advanced Server currently has 200 MB of free memory available (when the Configuration Manager verifies the configuration), the Configuration Manager allows a maximum of 100 MB of memory to be available to support the number of clients and data cache size currently configured for the server.

If, in the preceding example, the Configuration Manager determines that 100 MB is not enough to support the currently configured client capacity and data cache size, then you can do either of the following:

- Increase the percentage of physical memory used
- Reduce the number of supported clients and/or the data cache size to accommodate the percentage of physical memory available.

You can specify from 1% to 100% of physical memory. If you set the maximum percentage value too high, other OpenVMS applications might not have enough memory to operate. The default setting is 80%.

To modify the percentage of physical memory the server may use, on the Basic Configuration Parameters screen, enter the percent value in the Percent of Physical Memory Used field.

#### 7.2.4.3 Specifying Server Data Cache Size

The Configuration Manager allows you to specify the size of the data cache for the server's file data. A proper setting can decrease the amount of disk I/O, improving server response. You can set this value from 512 Kbytes to 131,072 Kbytes (128 Mbytes). The default setting is 2048 Kbytes (2 Mbtyes). Compaq recommends a minimum of 128 Kbytes of cache per concurrent client session. For example, if you expect 200 concurrent client sessions, set the data cache size to at least 25,600 Kbytes. When the Advanced Server starts, it allocates pages directly off the free page list to create the data cache. For more information about setting the data cache size, see Section 6.2.2.3.1, Monitoring Data Cache Use by the File Server.

To modify server data cache size, on the Basic Configuration Parameters screen, enter the number of Kbytes in the Data Cache Size field.

#### 7.2.4.4 Specifying the Maximum Number of Concurrent Signons

The Configuration Manager allows you to specify the maximum number of external authentication signon operations that can take place concurrently. External authentication allows the Advanced Server to do the logon validation for both network accounts and OpenVMS user accounts. For more information about external authentication, see Section 3.1.17, External Authentication.

You can enter any number from 2 through 999. The default value for this parameter is 10.

To modify the maximum number of concurrent signons, on the Basic Configuration Parameters screen, enter the new value in the Maximum Concurrent Signons field.

#### 7.2.4.5 Specifying OpenVMS Process Priority

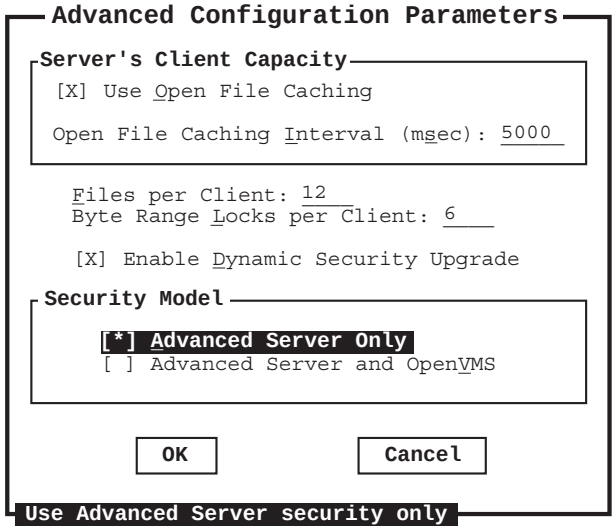
The Configuration Manager allows you to specify the base priority assigned to main server processes for scheduling purposes. Values from 9 to 12 are most appropriate. Server processes below base priority 9 can be preempted by interactive processes, and processes above base priority 12 will not receive their priority boosts.

To change the base process priority for the server, on the Basic Configuration Parameters screen, enter the value in the OpenVMS Process Priority field.

## 7.2.5 Modifying Advanced Configuration Parameters

The Advanced Configuration Parameters screen allows you to modify configuration parameters that are less frequently modified. To change advanced parameters, select the Advanced command button on the Basic Configuration Parameters screen. The screen shown in Figure 7–2, Advanced Configuration Parameters Screen, appears.

**Figure 7–2 Advanced Configuration Parameters Screen**




VM-0015A-AI

The following sections describe the advanced configuration parameters and how to set them.

### 7.2.5.1 Enabling and Disabling Open File Caching

When Open File Caching is enabled, the server delays the actual closing of files in case they are reopened shortly. Open File Caching is enabled by default. You can disable Open File Caching by deselecting the Use Open File Caching option on the Advanced Configuration Parameters screen.

To enable or disable Open File Caching, on the Advanced Configuration Parameters screen, select Use Open File Caching. The check box contains an X when open file caching is enabled.

#### 7.2.5.2 Setting the Open File Caching Interval

When Open File Caching is enabled, you can specify the amount of time to delay the actual closing of files. The default setting is 5000 msec (milliseconds), which is 5 seconds. You can specify from 0 to 65,535 milliseconds.

To modify the Open File Caching interval, on the Advanced Configuration Parameters screen:

1. Be sure that the Use Open File Caching option is checked.
2. Enter the number of milliseconds to delay in the Open File Caching Interval field.

#### 7.2.5.3 Specifying the Files per Client

The Configuration Manager allows you to specify the average number of files open per client. This value is used to compute values for a number of other parameters having to do with open files and file I/O. You can specify any nonzero value for this parameter; the default average is 12 open files per client.

To modify the Files per Client value, on the Advanced Configuration Parameters screen, enter the new value in the Files per Client field.

#### 7.2.5.4 Specifying the Byte Range Locks per Client

The Configuration Manager allows you to specify the average number of byte range locks held per client. Byte range locks are used by client applications for locking portions of open shared files. You can specify any nonzero value for this parameter; the default is 6 byte range locks per client.

To modify the value of Byte Range Locks per Client, on the Advanced Configuration Parameters screen, enter the new value in the Byte Range Locks per Client field.

#### 7.2.5.5 Enabling Dynamic Security Upgrade

The Configuration Manager allows you to specify whether the server performs dynamic upgrading of network security on files it accesses. When enabled, any file the server accesses whose security is specified entirely according to PATHWORKS V5 for OpenVMS (LAN Manager) security, is upgraded to PATHWORKS V6 for OpenVMS (Advanced Server) security. The mapping file created by the V6 Upgrade utility must be in place for dynamic security upgrade to be performed. Refer to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Migration Guide* for more information about the Upgrade utility. By default, dynamic security upgrade is not enabled.

To enable or disable Dynamic Security Upgrade, on the Advanced Configuration Parameters screen, select the Enable Dynamic Security Upgrade option. The check box contains an X when dynamic security upgrading is enabled.

#### 7.2.5.6 Specifying the Server Security Model

The Configuration Manager lets you specify the security model that the server uses when checking access to a file, as shown in Table 7–1, Security Model Configuration Parameter Settings.

**Table 7–1 Security Model Configuration Parameter Settings**

| Security Model Selected | What the Server Checks |
|---|---|
| Advanced Server Only | A security model in which only network permissions are checked. This is the default. |
| Advanced Server and OpenVMS | A security model in which both network permissions and OpenVMS protections are checked. |

For more information about the security models, see Section 4.1.2, Advanced Server Security Models.

To select the server security model, on the Advanced Configuration Parameters screen, select either Advanced Server Only or Advanced Server and OpenVMS.

#### 7.2.5.7 Saving Advanced Configuration Parameter Changes

You can save the Advanced Configuration Parameters you have modified, or you can quit without saving your changes.

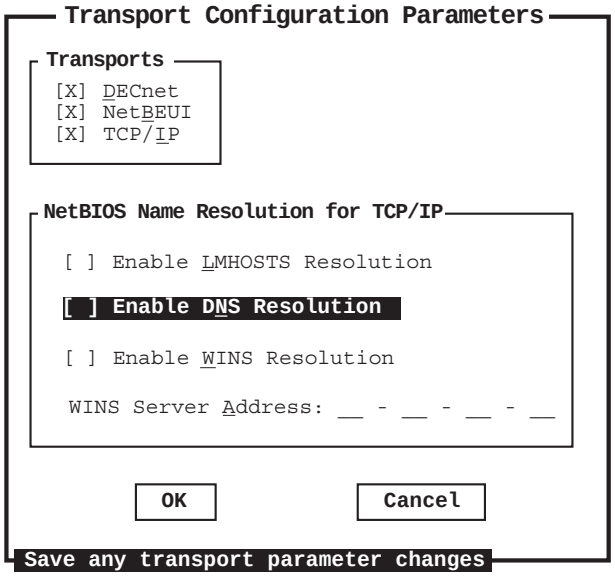
To save advanced configuration parameters changes, on the Advanced Configuration Parameters screen, select the **OK** button. If any setting is not appropriate, the Configuration Manager displays an Information screen (such as shown in Figure 7–5, Information Screen. If all the settings are appropriate, the Basic Configuration Parameters screen reappears.

To ignore advanced configuration parameters changes, on the Advanced Configuration Parameters screen, select the **Cancel** button or press Ctrl/C. The Basic Configuration Parameters screen reappears.

## 7.2.6 Configuring Transports

The Transport Configuration Parameters screen allows you to specify the types of transports that are enabled on the server, and the type of wide-area network capabilities, if any. To change the transport parameters, select the Tranports command button on the Basic Configuration Parameters screen. The Transport Configuration Parameters screen appears, such as the one shown in Figure 7–3, Transport Configuration Parameters Screen.

**Figure 7–3 Transport Configuration Parameters Screen**




VM-0016A-AI

The transport configuration parameters are described in the following sections.

### 7.2.6.1 Enabling and Disabling Transports

The Configuration Manager lets you enable or disable one or more of the following transports: DECnet, NetBEUI, TCP/IP. (Note that for wide area networking, the TCP/IP transport is required. DECnet also supports wide area networks but the functionality it provides is not as extensive as that provided by TCP/IP. NetBEUI is recommended only for use in small LAN-only environments (approximately 50 nodes or less).) For more information about transports and the protocols they support, see Appendix A, Network Protocols.

To enable and disable a transport, on the Transport Configuration Parameters screen, select the transport names. The transport is enabled if the check box contains an X.

#### 7.2.6.2 Selecting NetBIOS Name Resolution

The Configuration Manager lets you select name resolution for wide-area network support, using LMHOSTS, WINS, and DNS name resolution. (You can enable one, two, or all three of these name resolution methods.)

- The Enable LMHOSTS Resolution option allows the server to resolve NetBIOS names by looking them up in a local database that maps NetBIOS names to TCP/IP addresses.
- The Enable DNS Resolution option allows the server to use DNS services to resolve NetBIOS names as a last resort if all other methods fail to resolve a NetBIOS name.

**Note**

DNS is not configured as a replacement for WINS or LMHOSTS but rather as a supplement. DNS is used primarily for resolving node or computer names; it is not used for resolving domain names. With DNS, the Advanced Server still uses WINS, LMHOSTS, or both methods for resolving domain names and certain other names.

- The Enable WINS Resolution option allows the server to act as a WINS client, which will use a specified WINS Server for NetBIOS name registration and resolution.

  The WINS Server Address field allows you to specify the TCP/IP address for the WINS Server if WINS Resolution is enabled.

For additional procedures required to set up wide-area networking, refer to the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide.*

To enable or disable LMHOSTS, on the Transport Configuration Parameters screen, select Enable LMHOSTS Resolution. The checkbox contains an X when LMHOSTS Resolution is enabled.

To enable or disable DNS name resolution, on the Transport Configuration Parameters screen, select Enable DNS Resolution. The check box contains an X when DNS name resolution is enabled.

To enable or disable WINS name resolution, on the Transport Configuration Parameters screen, select Enable WINS Resolution. The check box contains an X when WINS name resolution is enabled.

When WINS name resolution is enabled, you must supply the TCP/IP address for the WINS Server.

To supply the TCP/IP address for the WINS Server, on the Transport Configuration Parameters screen:

1. Be sure Enable WINS Resolution is enabled.
2. Enter the TCP/IP address of the WINS Server in the WINS Server Address field.

**Note**

If your Advanced Server runs in an OpenVMS Cluster in the domain and you have it set up for dynamic cluster load balancing using DNS, then enable the use of DNS for NetBIOS name resolution on all servers and clients. Remove any entries for the cluster alias from the LMHOSTS file and from the WINS database on WINS servers that might be used by clients. For information about setting up dynamic load balancing, see Section 2.4.4, Dynamic Cluster Load Balancing in WANs.

#### 7.2.6.3 Saving Transport Configuration Parameter Changes

You can save the changes you have made to the transport configuration, or you can quit without saving your changes.

To save transport configuration parameter changes, on the Transport Configuration Parameters screen, choose the **OK** command button. If any setting is not appropriate, the Configuration Manager displays an Information screen, such as the one shown in Figure 7–5, Information Screen. If all the settings are appropriate, the Basic Configuration Parameter screen reappears.

To ignore transport configuration parameter changes, on the Transport Configuration Parameters screen, choose the **Cancel** command button, or press Ctrl/C. The Basic Configuration Parameters screen reappears.

### 7.2.7 Verifying and Saving the New Configuration

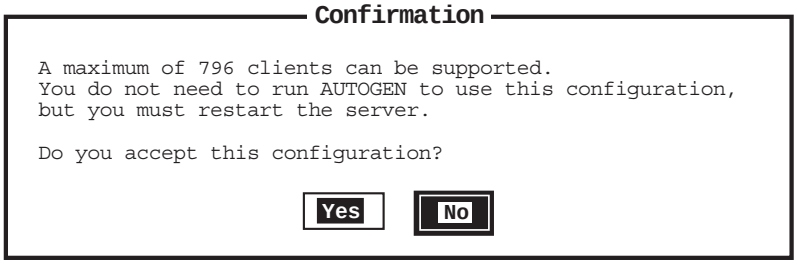
When you verify the configuration, the Configuration Manager determines whether the new configuration can be supported.

To verify the new configuration, on the Basic Configuration Parameters screen, select the **Verify** command button.

- If any basic configuration parameter settings are inappropriate, the Configuration Manager displays an Information screen, such as the one shown in Figure 7–5, Information Screen.
- If all the settings are appropriate, the Configuration Manager displays either a Confirmation screen, such as the one shown in Figure 7–4, Confirmation Screen, or an Information screen, depending on whether the configuration can be supported.

If the configuration can be supported, the Configuration Manager displays a Confirmation screen that allows you to accept or reject the new configuration. The Confirmation screen also tells you whether the server must be restarted for the new settings to take effect, or if AUTOGEN and/or reboot will be necessary to use the new configuration.

**Figure 7–4 Confirmation Screen**




VM-0017A-AI

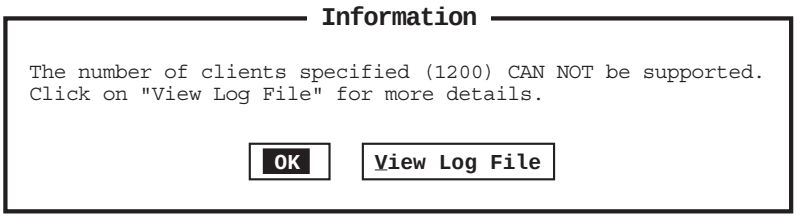
- Choose the **Yes** button to accept the configuration you have established.

  If you select **Yes**, the Configuration Manager saves the new configuration and allows you to choose whether the AUTOGEN, reboot, or both should be performed immediately, if required.
- Choose the **No** button to reject the configuration you have established.

  If you select **No** and reject the configuration, the Basic Configuration Parameters screen reappears.

If the configuration cannot be supported, or if it requires AUTOGEN, reboot, or both, the Configuration Manager displays an Information screen, such as the one shown in Figure 7–5, Information Screen, which allows you to view the configuration log file for details.

**Figure 7–5 Information Screen**




VM-0018A-AI

To view the log file, select the **View Log File** button. The log file shows the OpenVMS SYSGEN parameter changes required to support the new configuration, or why the configuration cannot be supported at all.

To dismiss the Information screen, select the **OK** button.

### 7.2.8 Navigating the Configuration Manager Using a Keyboard

You can control the Configuration Manager using a mouse or using keys on the keyboard. Using the mouse, you can navigate through the Configuration Manager screens by pointing and clicking on the desired item to select (highlight) items in the menus, scroll boxes, or dialog boxes. (You must have a DECterm window or equivalent emulator.) Table 7–2, Keys for Controlling the Configuration Manager, lists the keys you use to control the action of the Configuration Manager.

**Table 7–2 Keys for Controlling the Configuration Manager**

| Desired Action | Keys to Use |
|---|---|
| Access the menu bar | Press F10, or press PF1 twice. Use the Tab key to select the first item on the menu bar. |
| Move from one menu to another | Use the left and right arrow keys. |
| Point to a menu item | Use the up and down arrow keys. |

(continued on next page)

**Table 7–2 (Cont.) Keys for Controlling the Configuration Manager**

| Desired Action | Keys to Use |
|---|---|
| Select a menu item within a menu | Use the up and down arrow keys, then press the Enter or Return key. |
| Select a menu or an item within a menu | Move to the menu or menu item, then press the Enter or Return key. |
| Exit the menu bar | Press Ctrl/Z. |
| Point to buttons and items in a dialog box | Press the Tab key to advance, and PF1 Tab to back up. |
| Move within a set of buttons or check boxes | Use the arrow keys. |
| Choose among a set of options (radio buttons) | Advance to the currently selected option button using Tab or PF1 Tab. Then use the arrow keys to choose a new option within the set. |
| Change the state of a check box (on or off) | Advance to the check box, then press the space bar to toggle the state of the box. |
| Press a command button | Advance to the button and press the space bar or the Return key. This executes the button's command. |
| Enter new text in a text box | Advance to the text box using Tab or PF1 Tab, and enter the new text. Any previous text is erased. |
| Edit text or edit text in a text box | Advance to the text box using Tab or PF1 Tab. Use the arrow keys to move within existing text. |
| Refresh the display at any time | Press Ctrl/W. |
| Save any changes made in a dialog box, and return to the previous dialog box | At the **OK** command button, press the Enter or Return key. |
| Discard any changes made in a dialog box and return to the Basic Configuration parameters screen. | At the **Cancel** command button, press the Enter or Return key; or press Ctrl/C; or press the Enter or Return key at the **Quit** button on the Basic Configuration Parameters screen. |

## 7.3 Using the LANMAN.INI File

The LANMAN.INI file defines the basic configuration of the server. This file is located in the OpenVMS PWRK$LMROOT:[LANMAN] system directory and contains a collection of keywords with associated values. The values define the configuration of a server running PATHWORKS Advanced Server software. When the PATHWORKS Advanced Server is installed, default values are assigned to these keywords.

This section contains the following topics:

- Section 7.3.1, File Organization — describes the way the LANMAN.INI file is organized and provides an example of the default file.
- Section 7.3.2, File Contents — describes the syntax used in the LANMAN.INI file and the keywords you can use in each file section.
- Section 7.3.3, Defining Autoshares — describes the syntax for the **Autoshare** and **Noautoshare** keywords.

**Note**

The LANMAN.INI file must be world readable. To set the file as world readable from OpenVMS at the DCL prompt, enter the following command:

```
$ SET PROTECTION LANMAN.INI/PROTECTION=(WORLD:READ)
```

### 7.3.1 File Organization

This section describes the organization of the LANMAN.INI file and provides hints on how to adjust certain parameters that affect server performance.

The LANMAN.INI file contains several sections. Within each section, you can use keywords that define specific server functions. Sections can appear in any order in the LANMAN.INI file.

The LANMAN.INI section names are:

- BROWSER, which contains keywords that control browser activity on a server.
- NETLOGON, which contains keywords used to configure logon validation.
- NODE, where *servername* contains keywords that control parameters that apply only to the specified node (*servername*).

- SERVER, which contains keywords common to all PATHWORKS for OpenVMS Advanced Servers.
- VMSSERVER, which contains keywords that specify PATHWORKS for OpenVMS Advanced Server characteristics.
- WORKSTATION, which contains keywords that identify the server's domain.

#### 7.3.1.1 Default LANMAN.INI File

The following example shows the default PATHWORKS for OpenVMS (Advanced Server) LANMAN.INI file. The entry *nodename* is replaced with the actual node name of the node where the configuration is established.

```
; Advanced Server initialization file, for server configuration.
;
; Refer to the PATHWORKS V6 for OpenVMS (Advanced Server) Server
; Administrator's Guide for information on keywords and keyword values.
;
;                               W A R N I N G
;
; DO NOT modify DOMAIN, LISTENNAME, or PWRKALIAS. Doing so will have adverse
; effects on the server.  To change these parameters use PWRK$CONFIG.COM or
; PWRK$SETINI.COM.
;
[server]
  srvcomment = PATHWORKS V6.1 for OpenVMS (Advanced Server)
  srvservices = alerter,netlogon

[vmsserver]
  autoshare =
  noautoshare = dad, _dfs
  pwrkalias =

[workstation]
  domain = LANGROUP

[netlogon]
  scripts = PWRK$LMROOT:[LANMAN.REPL.IMPORT.SCRIPTS]
```

### 7.3.2 File Contents

When the PATHWORKS Advanced Server is installed, the LANMAN.INI file contains values for certain keywords. Other keywords, and the titles of the sections to which they belong, are added when you run the Configuration Manager or edit the LANMAN.INI file. If a keyword does not appear in the file (or is commented out with a semicolon), it is set to its default value.

#### 7.3.2.1 Syntax of the LANMAN.INI File

Within each section of the LANMAN.INI file, keywords are listed as follows:

- Each keyword begins a line, followed by an equal sign and the value assigned to it, for example, *keyword=value*.
- Comments start with a semicolon (;). If a semicolon precedes a keyword on the line, that keyword is ignored.
- When a list of values is assigned to a keyword, the values are separated by commas. For example:

  ```
  [NODE_DOT]
  AUTOSHARE = DUA1:=D,DUA2:=E
  ```

  For specific information, refer to the description of the appropriate keywords in tables in this section.
- When a value consists of a path, the path can be absolute, or it can be relative to the PWRK$LMROOT:[LANMAN] directory.
- When a keyword has no assigned value (nothing to the right of the equal sign), the default value is 0 for a keyword that requires a number and NULL for a keyword that requires a character string. A null value is not valid for all keywords.

#### 7.3.2.2 Changing Keyword Values

Before you change any keywords in the LANMAN.INI file, you should understand the relationship between the LANMAN.INI file entries and server parameter default settings. All server parameters have default settings.

With certain exceptions, you can edit the LANMAN.INI file to set keywords to values other than the server defaults. Server parameter defaults do not appear in the LANMAN.INI file. A value assigned to any keyword in the LANMAN.INI file always supersedes the default value for that keyword.

The keywords whose value you cannot change by editing the LANMAN.INI file are:

- domain
- listenname
- pwrkalias

To change these parameters, use the PWRK$CONFIG.COM configuration command procedure.

When you want to set the value of a keyword to something other than the default, you must edit the LANMAN.INI file, locate or add the appropriate section title in the file, and then add the desired *keyword=value* entry.

**To change a keyword in the LANMAN.INI file:**

Edit the LANMAN.INI file with an ASCII editor or use the PWRK$CONFIG.COM configuration procedure.

The following sections describe each LANMAN.INI keyword. The keywords are grouped according to the section of the LANMAN.INI file in which they reside. Sections are in alphabetical order.

#### 7.3.2.3 BROWSER Section

In the BROWSER section, you specify how the server deals with Browser activity. The Master Browser polls for domains, and builds and updates a master list of its domains. The backup Browser sends a request to the Master Browser to update its own list. The Browser service is always started at server startup.

**Table 7–3 Browser Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| masterupdate=*n* | Specifies the interval after which domain updates occur. | Minimum: 60<br>Maximum: unlimited | 720 seconds (12 minutes) |
| backupupdate=*n* | Specifies the interval after which a backup Browser updates its list by querying the Master Browser. | Minimum: 60<br>Maximum: unlimited | 900 seconds (15 minutes) |
| backuprecovery=*n* | Specifies that recovery is initiated if the backup Browser gets no response from the Master Browser after the specified interval. | Minimum: 60<br>Maximum: unlimited | 1800 seconds (30 minutes) |
| morelog=YES/NO | Specifies whether the Browser is to log more details. | YES or NO | NO |

#### 7.3.2.4 NETLOGON Section

In the NETLOGON section, you specify parameters related to network logon. The NetLogon service is started automatically at server startup.

**Table 7–4 NETLOGON Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| maxclisess=*n* | Specifies the number of links for internal communication that this server can initiate. This represents the maximum number of domains that this domain can trust, plus one (number of trusted domains plus 1). | Minimum: 5<br>Maximum: 128 | 32 |
| maxsrvsess=*n* | Specifies the number of links used for internal communication that this server can accept. This number must include the number of domains that trust this domain, the number of backup domain controllers in this domain, and the number of Windows NT workstations in this domain (trusting domains + BDCs + Windows NT workstations). | Minimum: 5<br>Maximum: unlimited | 200 |
| pulse=*n* | Specifies the number of seconds that the primary domain controller waits before sending update notices to each backup domain controller and member server. | 60-3600 seconds | 300 seconds<br>5 minutes |

(continued on next page)

**Table 7–4 (Cont.) NETLOGON Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| randomize=*n* | Specifies the number of seconds that a backup domain controller randomizes a request to get updates after receiving an update notice from the primary domain controller. This keyword decreases the odds of servers in the same domain requesting an update from the primary domain controller at the same time. | 5-120 seconds | 30 seconds |
| scripts=*path* | Specifies the location of logon scripts. | | If you do not specify this keyword, the login scripts are assumed to be stored at: PWRK$LMROOT:[LANMAN.REPL.IMPORT.SCRIPTS] |
| update=YES/NO | Controls synchronization of the user accounts database with the master database on the primary domain controller when the server starts. This keyword applies only to a backup domain controller and is ignored by the primary domain controller. | YES or NO | NO (do not synchronize on startup) |

#### 7.3.2.5 NODE_*servername* Section

In the NODE_*servername* section, s*ervername* specifies the name of a server node, and you use keywords to enable node-specific keyword values. For example, if you use the **Autoshare** keyword in a section called NODE_ TINMAN to create an autoshare name for a disk device, only users on node TINMAN can see and connect to that autoshare.

**Note**

If keywords appear in both the NODE_*servername* and VMSSERVER sections of your LANMAN.INI file, values in VMSSERVER take precedence.

**Table 7–5 NODE_*servername* Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| autoshare=*device=sharename* | | | |
| | Specifies a synonym for the autoshare name created by default for an OpenVMS disk device. The value for this keyword is a list of OpenVMS device names (or volume labels) and share name synonym to which each device maps. | All OpenVMS disk devices are automatically shared, and share names are based on the volume label of each disk device. (See Section 7.3.3, Defining Autoshares). | NULL |
| noautoshare=*(device[, . . . ])* | | | |
| | Specifies a disk device or list of devices that should not be automatically shared when the server starts. Autosharing DFS devices is not recommended. | Up to 512 characters, including commas | dad, _dfs |

(continued on next page)

**Table 7–5 (Cont.) NODE_*servername* Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| listenname=*servername* | | | |
| | Specifies the name of the server on the network; up to 15 characters. Using this keyword, you enable users to connect to a server using a different server name.<br>**Caution:** Do not change the listenname by editing the LANMAN.INI file directly. To change the listenname, use the PWRK$CONFIG.COM configuration procedure. | Up to 15 characters | The server node name |
| srvservices=*list* | Specifies the services that start automatically when the server is started. Because services are started in the order they appear in the srvservices entry, you must ensure that "NetLogon" appears before any services that require the NetLogon service.<br>The Browser service is not controlled by this keyword. It is started automatically when the Server service starts. | alerter, netlogon, browser | alerter, netlogon |

#### 7.3.2.6 SERVER Section

The SERVER section allows you to specify parameters related to your server, as shown in the following table.

**Table 7–6 Server Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| accessalert=*n* | Specifies the number of resource access violations that can occur before the server sends an alert to the alertnames list. | 0 to unlimited | 5 |
| alertnames=*list* | Specifies a list of the Advanced Server user accounts to receive administrative alerts. To receive alerts, a client workstation must be running the Messenger service. The Messenger service is not supported on OpenVMS servers. | | None |
| autodisconnect=*n* | Specifies the interval, in minutes, that the server waits before dropping the virtual circuit to an inactive client. | 0 to unlimited | 0 (no automatic disconnect) |
| erroralert=*n* | Specifies the number of errors that can occur before the server sends an alert to the alertnames list. | 0 to unlimited | 5 |
| logonalert=*n* | Specifies the number of logon violations that can occur before the server sends an alert to the alertnames list. | 0 to unlimited | 5 |
| maxapplog=*n* | Specifies the maximum size, in kilobytes, of the Application event log file. | 0 to unlimited | 100 Kbytes |
| maxauditlog=*n* | Specifies the maximum size, in kilobytes, of the Security event log file. | 0 to unlimited | 100 Kbytes |

(continued on next page)

**Table 7–6 (Cont.) Server Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| maxclients=*n* | Specifies the maximum number of clients. | 1 to unlimited | 50 |
| maxerrlog=*n* | Specifies the maximum size, in kilobytes, of the System event log file. | 0 to unlimited | 100 Kbytes |
| srvannounce=*n* | Specifies the number of seconds at which the server announces its presence to the network. This keyword has effect only if srvhidden=NO. | 1 to unlimited | 180 seconds |
| srvcomment=*text* | Specifies the descriptive comment that the server sends when it announces its presence to the network. | Up to 48 characters, including spaces | PATHWORKS V6.1 for OpenVMS (Advanced Server) |
| srvhidden=YES/NO | Specifies whether the server is hidden on the network. If the server is not hidden, it announces its presence at the interval set by srvannounce and can be viewed using the ADMINISTER SHOW COMPUTERS command. | YES or NO | NO (visible) |
| srvservices=*list* | Specifies the services that start automatically when the server is started. Because services are started in the order they appear in the srvservices entry, you must ensure that NetLogon appears before any services that require it.<br>The Browser service is not controlled by this keyword. It is started when the Server service is started. | alerter netlogon, browser | alerter, netlogon |

(continued on next page)

**Table 7–6 (Cont.) Server Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| userpath=*path* | Specifies the OpenVMS system directory on the server to be used as a default parent directory for home directories for new user accounts. | Up to 255 characters | If you do not specify this keyword, the path is assumed to be: PWRK$LMROOT:[LANMAN.ACCOUNTS.USERDIRS |

#### 7.3.2.7 VMSSERVER Section

The VMSSERVER section allows you to specify parameters related to your server setup.

**Table 7–7 VMSSERVER Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| autoshare=*devn=sharename* | | | |
| | Specifies a synonym for the autoshare name for an OpenVMS disk device. The value for this keyword is a list of OpenVMS device names (or volume labels) and the share name for each device. (See Section 7.3.3.) | All OpenVMS disk devices are automatically shared, and share names are based on the volume label of each disk device | |
| hostmapusevmsnames=YES/NO | | | |
| | Checks to see if the PATHWORKS Advanced Server user's name matches an OpenVMS user account name. Explicit host mapping is checked and used first. If host mapping has not been specified, the software searches for a matching OpenVMS user name. (See Section 3.1.16.) | YES or NO | YES |

(continued on next page)

**Table 7–7 (Cont.) VMSSERVER Keywords**

| Keyword | Description | Setting | Default Setting |
|---|---|---|---|
| hostmapdomains=*(domainname,...)* | | | |
| | Used for external authentication of a network user name located in a domain other than the one where the server is located. Checks that the user's domain name matches one of the domains listed, where the PATHWORKS Advanced Server user name matches an OpenVMS user account name. Affects hostmapusevmsnames translations. | List of domains used for OpenVMS host mapping | NULL. The server's domain name is assumed. |
| hostmapdefault=*text* | Used when no other host mapping definitions apply. | ADMINISTRATOR, PWRK$DEFAULT, GUEST, or REJECT | PWRK$DEFAULT |
| noautoshare=(*device[,...device]*) | | | |
| | Specifies a disk device or list of devices that should not be automatically shared when the server starts. DFS disk devices are not automatically shared. | Up to 512 characters | dad, _dfs |
| | Autosharing DFS devices is not recommended. | | |
| pwrkalias=*text* | Specifies the PATHWORKS cluster alias. | Cluster alias name | OpenVMS Cluster alias |
| | **Caution:** Do not change pwrkalias by editing the LANMAN.INI file directly. To change the PATHWORKS cluster alias, use the PWRK$CONFIG.COM configuration procedure. | | |

#### 7.3.2.8 WORKSTATION Section

The WORKSTATION section specifies how users connect from workstations.

**Table 7–8 WORKSTATION Keywords**

| Keyword | Meaning | Setting | Default Setting |
|---|---|---|---|
| domain=*domainname* | Specifies the name of the domain that includes this server.<br>**Caution:** Do not change the domain name by editing the LANMAN.INI file directly. To change the domain name, use the PWRK$CONFIG.COM configuration procedure. Changing the domain name reinitializes the server security database. | Up to 15 characters | LANGROUP |

### 7.3.3 Defining Autoshares

The PATHWORKS Advanced Server lets you map autoshare names through entries in the LANMAN.INI file. This feature is useful if:

- You have a disk device whose volume label exceeds the 11-character limit.
- You want to map a server device to a single letter to accommodate the DOS disk device-naming convention.
- You do not want to autoshare some devices.

You can use the **Autoshare** and **Noautoshare** keywords in the VMSSERVER section of the server's LANMAN.INI file to specify a list of autoshare names for the server to create, in addition to the autoshares that the server creates automatically, and to specify the names of devices that you do not want to autoshare. You must restart the server to activate these changes.

If you are running PATHWORKS Advanced Server in an OpenVMS Cluster environment, you can specify the **Autoshare** and **Noautoshare** keywords in the node-specific section of the LANMAN.INI file called NODE_*servername*. The devices you specify in the node-specific section remain local to that server node; they are not served to other OpenVMS Cluster members. Keywords specified in the VMSSERVER section override identical keywords in the NODE_*servername* section. See Section 4.2.3.6 for more information.

The **Autoshare** and **Noautoshare** keywords function as follows:

- If a volume label is specified with the **Noautoshare** keyword, that device is not shared, but it is still available by its logical name.
- If a volume label is specified with the **Autoshare** keyword, that device is shared and mapped to the specified autoshare name.
- If a volume is not specified, PATHWORKS Advanced Server creates an autoshare by default, so long as the volume label does not exceed the 11-character name limit.

#### 7.3.3.1 The Autoshare Keyword

The **Autoshare** keyword in the LANMAN.INI file specifies an alias for the autoshare name created by default for an OpenVMS disk device. PATHWORKS Advanced Server creates an autoshare for each mounted OpenVMS disk device when the server starts. To create a more meaningful share name or to map the device name to a DOS format, use the **Autoshare** keyword in the LANMAN.INI file.

The format is as follows:

AUTOSHARE=(*devname*_1=*sharename*_1,...,*devname* _n=*sharename*_n)

The share name cannot exceed 11 characters. Do not append a dollar sign ($) to the device name; the PATHWORKS Advanced Server does this automatically.

For example, Table 4-4, Sample Autoshare Names, shows physical device names and volume labels for disk devices mounted on node DOT and the autoshare names that PATHWORKS Advanced Server creates by default.

The following example shows an **Autoshare** keyword in the VMSSERVER section of the LANMAN.INI file:

```
AUTOSHARE = DOT$DUA1=USERS_1,DOT$DUA2=M,DOT$DUA3=WORK5
```

If you connect to an autoshare, you access the root directory of the disk device. For example, if you connect to the share USERS_1$, you access DOT$DUA1:[000000]. The **Autoshare** keyword directs PATHWORKS Advanced Server to create an autoshare named M$. When a user displays a list of available devices (for example, to create a shared directory), the device M: is listed.

**Note**

The autoshare name C$ is reserved. By default, PATHWORKS defines C$ as an autoshare alias for PWRK$LMROOT:[000000]. If you use the **Autoshare** keyword to define another volume as C$, the share name will be rejected.

As shown in Table 4–6, Sample Default Autoshare Names, PATHWORKS Advanced Server did not create an autoshare for the device DOT$DUA3:, because the volume label WORK_DISK055 exceeds the 11-character limit. But PATHWORKS Advanced Server allows you to include the device name (DOT$DUA3) in the autoshare list in the LANMAN.INI file and creates the autoshare WORK5$ for DOT$DUA3:.

#### 7.3.3.2 The Noautoshare Keyword

The **Noautoshare** keyword in the LANMAN.INI file specifies the OpenVMS device names that should not be automatically shared.

If the server configuration includes many disk devices, you may want to specify which devices are not shared automatically. By sharing some devices and not sharing others, you can separate OpenVMS disk resources from PATHWORKS Advanced Server resources and reduce unnecessary resource consumption by the server. Entries in the **Noautoshare** keyword list match OpenVMS device names that contain the search string. For example, the following line in the VMSSERVER section of the LANMAN.INI file specifies search strings DFS, DAD*, and PWRK$DKB300.

NOAUTOSHARE = DFS,DAD*,PWRK$DKB300

With this set of search strings, any OpenVMS device name containing the string DFS, any string containing DAD followed by any characters such as DAD1 and DAD2, and the explicit device PWRK$DKB300 are not shared. The total search string after the equal sign (=) cannot exceed 128 characters.

**Note**

By default, PATHWORKS Advanced Server does not automatically share devices managed by DECdfs (DFS) software. The default LANMAN.INI file contains the following line in the VMSSERVER section: NOAUTOSHARE = dad,_dfs. DFS is a DECnet VAX and Alpha layered product that provides OpenVMS users with the ability to use remote disks as if they were directly attached to the local system. You cannot assign permissions to DFS devices, so if you override the default and allow PATHWORKS Advanced Server to create an autoshare for a DFS device, users with user or operator privileges cannot access that device. Access to a shared DFS device is restricted to users in the Administrators group.

#### 7.3.3.3 Autosharing in an OpenVMS Cluster Environment

OpenVMS disk devices mounted clusterwide are offered to users as shared devices (autoshares) by all server nodes in an OpenVMS Cluster system. Devices mounted on a specific server (not clusterwide) are accessible to users connected to that server only.

The LANMAN.INI file contains two sections that govern autoshares: the VMSSERVER section and the NODE_*servername* section. In an OpenVMS Cluster system, you can make a device available clusterwide by using the **Autoshare** keyword in the VMSSERVER section. You can restrict device availability to a particular server by using the **Autoshare** keyword in the NODE_*servername* section.

The following fragment of a LANMAN.INI file illustrates how you can share disk devices in an OpenVMS Cluster:

```
[VMSSERVER]
   AUTOSHARE = PCS524$DKA100=J,PCS524$DKA200=K
[NODE_DOT]
   AUTOSHARE = DUA1001=H,DUA1002=G,DUA1006=I
[NODE_TINMAN]
   AUTOSHARE = DUA1001=H,DUA1002=G
```

In this example:

- PCS524$DKA100 and PCS524$DKA200 are available as shared devices on autoshares J: and K: on all OpenVMS Cluster server nodes.
- DUA1001 and DUA1002 are available as shared devices on autoshares H: and G: on server nodes DOT and TINMAN, respectively.

- DUA1006 is available as a shared device on autoshare I: on node DOT only.

**Note**

For shares on a device to be available from any PATHWORKS Advanced Server node in an OpenVMS Cluster, you must enter the SET COMPUTER/AUTOSHARE_SYNCHRONIZE command on each node in the cluster after the device is available.

# A

# Network Protocols

With its open architecture, the Advanced Server software can operate over several popular protocols simultaneously, including:

- TCP/IP
- NetBEUI
- DECnet Phase IV or DECnet-Plus

This appendix provides information about the following topics:

- Section A.1, Understanding the OSI Reference Model, describes the seven-layer networking software model.
- Section A.2, Choosing a Network Adapter Card, provides pointers on how to select your network adapters.
- Section A.3, Choosing a Network Protocol, briefly describes the protocols you can use, including TCP/IP, NetBEUI, and DECnet-Plus.

Before you explore the specific drivers and protocols supported by the Advanced Server, you should understand both the OSI Reference Model and the purpose of network interface card drivers. If you already understand these topics, you can skip to Choosing a Network Protocol, which includes an overview and description of each protocol that interoperates with the Advanced Server.

## A.1 Understanding the OSI Reference Model

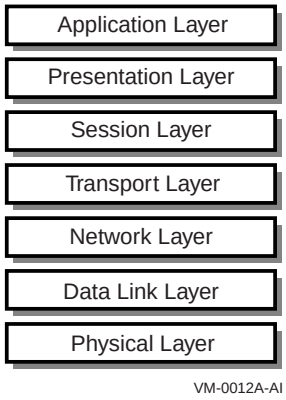
In 1978 the International Organization for Standardization (ISO) developed a model for computer networking called the Open Systems Interconnection (OSI) Reference Model. The model describes the flow of data in a computer network—from the physical connections of the network to the applications used by the end user.

The OSI Reference Model is an idealized version of networking; few systems follow it exactly. However, the model is useful for discussion and comparison of networks.

## Network Protocols
## A.1 Understanding the OSI Reference Model

The OSI Reference Model includes seven layers, as shown in Figure A–1, OSI Reference Model. Each of the layers is responsible for a specific and discrete aspect of networking.

**Figure A–1 OSI Reference Model**




The following list describes each OSI Reference Model layer in detail:

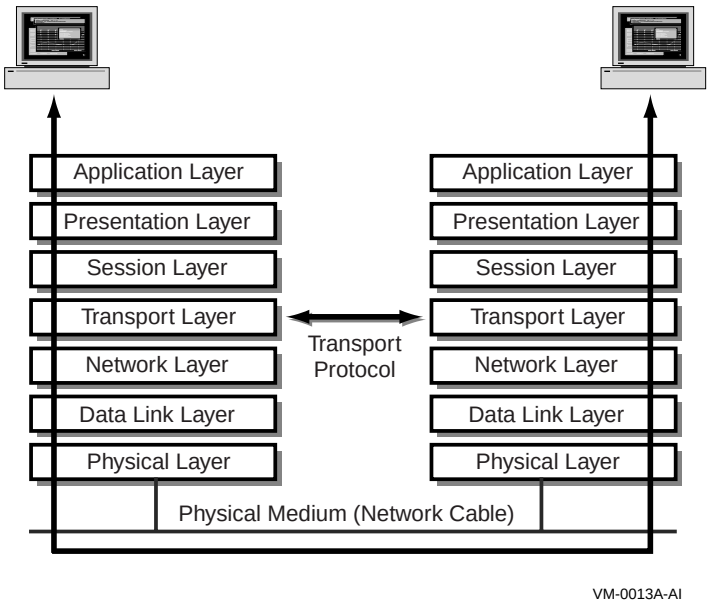
- The Physical Layer is responsible for getting bits from one computer to another. It also regulates the transmission of a stream of bits over a physical medium. This layer defines how the cable is attached to the network adapter card and which transmission technique is used to send data over the cable. It also defines bit synchronization and checking.
- The Data Link Layer packages raw bits from the Physical Layer into frames. A frame is a logical, structured packet in which data can be placed. The Data Link Layer is responsible for transferring frames from one computer to another without errors. After the Data Link Layer sends a frame, it waits for an acknowledgment from the receiving computer. Frames that are not acknowledged are resent.
- The Network Layer addresses messages and translates logical addresses and names into physical addresses. It also determines the route along the network from the source to the destination computer, and it manages traffic problems such as switching, routing, and controlling the congestion of data packets.
- The Transport Layer is responsible for error recognition and recovery, ensuring the reliable delivery of messages. It also repackages messages when necessary by dividing long messages into small packets for transmission. At the receiving end, it rebuilds the small packets into

the original message. The receiving Transport Layer also sends an acknowledgment of receipt.

- The Session Layer allows two applications on different computers to establish, use, and end a session. This layer establishes dialog control between the two computers in a session, regulating which side transmits, when, and for how long.
- The Presentation Layer translates data from the Application Layer into an intermediary format. This layer also manages security issues by providing services such as data encryption, and it compresses data to reduce the number of bits that need to be transferred on the network.
- The Application Layer enables end-user applications to access network services.

  When two computers communicate over a network, the software at each layer on one computer communicates with the same layer on the other computer. For example, the Transport Layer of one computer communicates with the Transport Layer on the other computer. As shown in Figure A–2, Transport Protocol, the Transport Layer on the first computer is not involved with how the communication actually passes through the lower layers of the first computer, passes across the physical media, and up through the lower layers of the second computer.

**Figure A–2 Transport Protocol**




## A.2 Choosing a Network Adapter Card

A network adapter card, also called a network interface card or a network interface controller (NIC), is an adapter board installed in a computer to let it function on a network. The network adapter card provides ports to which the network cable can connect physically. The card physically transmits data from the computer to the network cable, and back.

Every network computer must have a network adapter card driver, a software driver that controls the network card. Every network adapter card driver is configured to run with a certain type of network card.

When choosing network adapter cards, you first must choose cards that support your network's architecture (such as Ethernet or Token Ring) and cabling media (such as Thinnet or twisted pair). You also should consider the tradeoffs of performance and cost.

Performance for network adapter cards depends mostly on bus width and onboard memory. The best performance is achieved when the bus width of the card closely matches the internal bus width of the computer. Onboard memory enables a card to buffer frames going to and from the network. A card with the most memory is not always the best choice. At some point, diminishing returns

and the maximum speed of other network components limit the performance gains of onboard memory.

When you consider the cost of network cards, factor in the cost of buying spare cards to replace the ones that fail. You should also ensure that your network hardware budget allows for cable, hubs, repeaters, routers, and other hardware, as well as the labor costs associated with installing them.

Before you decide on a type of network card, make sure that the OpenVMS operating system you are using supports it. Also, make sure the vendor can support your business needs. If you are working with a reseller, check that the reseller has good communication with the card manufacturer.

## A.3 Choosing a Network Protocol

In addition to the network card and the network card driver, a network computer must have a protocol driver, also called a transport protocol or a protocol. The protocol driver works between the upper-level network software—such as the workstation and server—and the network adapter card. The protocol packages the data that are sent over the network in a way that the computer on the receiving end will understand.

The process of associating a protocol driver with the network adapter card with which it will work and establishing a communication channel between the two is called binding.

For two computers to communicate on a network, they must use identical protocols. In the case where computers are configured to use multiple protocols, they need to have only one protocol in common to communicate. For example, a server that uses both NetBEUI and TCP/IP can communicate both with workstations that use only NetBEUI and with workstations that use only TCP/IP.

The Advanced Server allows connections from the transports and protocols shown in Table A–1, Supported Transports and Protocols.

**Table A–1 Supported Transports and Protocols**

| Protocol | Client Transport | Server Transport Component |
|---|---|---|
| TCP/IP | Internet | Product-specific |
| NetBEUI (with NETBIOS) | LAN Manager | LAN Manager |
| DECnet (proprietary) | DECnet | DECnet |

The remainder of this section provides an overview of each of these protocols with basic information about each protocol and its advantages and disadvantages.

## A.3.1 TCP/IP Protocol

TCP/IP was developed in the late 1970s as a result of a research project on network interconnection by the Department of Defense Advanced Research Projects Agency (known as ARPANet, the precursor to the Internet). TCP/IP is actually a suite of protocols that defines various interactions between computers sharing the protocol.

Since the PC began its rise in popularity, TCP/IP has become a standard protocol for support in the PC networking environment.

TCP/IP has a reputation as a difficult protocol to configure and manage. However, current implementations are making it easier. For example, in TCP/IP, the Dynamic Host Configuration Protocol (DHCP) provides server support and is one of the most important advances in PC networking. Without DHCP, system administrators had to manually assign the four-byte IP addresses to each computer. With DHCP enabled, a DHCP server can manage a range of IP addresses and assign one to each computer as it logs on to the network.

The principal advantage of TCP/IP is that it provides communication across interconnected networks with different operating systems and hardware architectures.

TCP/IP provides compatibility with the Internet, a collection of networks and gateways linking universities, corporations, government offices, and military installations worldwide.

Table A–2, TCP/IP Protocol, summarizes the advantages and disadvantages of using the TCP/IP protocol.

**Table A–2 TCP/IP Protocol**

| Advantages | Disadvantages |
|---|---|
| Provides connectivity across different operating systems and hardware platforms. | Slower than NetBEUI on small LANs. |
| Provides Internet connectivity. | Can be difficult to administer. |
| Provides routing support. | More overhead than NetBEUI. |

### A.3.2 NetBEUI Protocol

The NetBIOS Extended User Interface (NetBEUI) was first introduced by IBM in 1985. NetBIOS, an integral part of the NetBEUI protocol driver, is a programming interface that implements many session layer functions. NetBEUI is a small, efficient, and fast protocol with low overhead.

**Note**

"Overhead" in this context refers to the additional network control information, such as routing and error checking, that the protocol adds to data that the application layer needs to send across the network.

One reason for NetBEUI's lower overhead is that NetBEUI does not require an explicit acknowledgment (ACK) of each frame before it sends the next. Instead, the computer packages up several ACKs and sends them all at once. Requiring an ACK for every packet wastes network resources. NetBEUI dynamically determines the number of frames the sender can transmit before receiving an ACK, based on the network's current conditions.

NetBEUI was developed for LANs segmented into workgroups of 20 to 200 computers, with gateways connecting LAN segments to one another or to mainframes. NetBEUI is optimized for very high performance when used in departmental LANs or LAN segments. For traffic within a LAN segment, NetBEUI typically is the fastest protocol.

While NetBEUI is fast on small LANs, it is not so effective on large networks because it has a poor addressing scheme. NetBEUI does not allow duplicate computer names on the same network. This prevents a network from having two computers with the same name—something difficult to eliminate on a large network.

Table A–3, NetBEUI Protocol, summarizes the advantages and disadvantages of the NetBEUI protocol.

**Table A–3 NetBEUI Protocol**

| Advantages | Disadvantages |
|---|---|
| Tuned for small LAN communication, and therefore is very fast on LANs. | Not routable. |
| Good error protection. | Performance across WANs is poor. |
| Small memory usage. | Requires each network computer to have a unique name. |

### A.3.3 DECnet-Plus Protocol

DECnet-Plus is a proprietary protocol; it is a collection of many layered protocols offered together as a major data communications network. Developed as a distributed network, it supports a wide range of applications and programs.

One of the DECnet protocol's major advantages is flexibility in network configuration and applications functionality. DECnet-Plus includes the Local Area Transport (LAT) protocol that terminal servers use to communicate with hosts.

Table A–4, DECnet-Plus Protocol, lists the advantages and disadvantages of the DECnet-Plus protocol.

**Table A–4 DECnet-Plus Protocol**

| Advantages | Disadvantages |
|---|---|
| Major flexibility in network configuration. | Complex network architecture. |
| Routable. | Proprietary. |
| Maintains a high level of availability, even in the event of node or link failure. | |
| Supports a wide range of communications facilities, such as Ethernet and X.25. | |

# Index

## A

## B



## C

## D



## E

## F



## G



## H

## I



## L



## M

## N



## O



## P

## Q



## R



## S

## T

## U



## V



## W