HP Advanced Server for OpenVMS

Concepts and Planning Guide

Order Number: AA–R6G4D–TE

September 2006

This guide provides an overview and introduction to the Advanced Server software and associated networking concepts for system administrators and operators.

Revision/Update Information:	This manual supersedes the *HP Advanced Server for OpenVMS Concepts and Planning Guide*, AA–R6G4C–TE
Operating System Version:	OpenVMS Alpha Version 7.3-2, 8.2 and 8.3
Software Version:	Advanced Server V7.3B for OpenVMS

Hewlett-Packard Company
Palo Alto, California

Printed in the US

ZK6553

The HP Advanced Server for OpenVMS documentation set is available on CD-ROM.

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

Contents

3 User Accounts

4 Groups

5 Organizing Your Network into Domains

6 Managing Network Shares

7 Sharing Printers

Index

Figures

Tables

Preface

Welcome to the *HP Advanced Server for OpenVMS Concepts and Planning Guide*. The Advanced Server for OpenVMS and its associated OpenVMS system platform provide a powerful, reliable, and versatile operating environment that meets the demands of client/server computing.

This guide presents an overview of the many capabilities and features of the Advanced Server for OpenVMS. The guide also provides a useful introduction to many of the concepts you need to understand when planning to install the Advanced Server on a network.

For the purposes of this text, the Advanced Server for OpenVMS is referred to as the Advanced Server. The concepts and guidelines presented in this guide are equally applicable to:

- Advanced Server for OpenVMS
- PATHWORKS V6.1 for OpenVMS (Advanced Server)

Usage of the term "Advanced Server" in this guide refers to either version of the file and print server, except when the text explicitly specifies a version number.

Intended Audience

This guide is intended for new and experienced system administrators who are or will be supporting a network that includes an Advanced Server. It assumes you have:

- A basic understanding of a PC LAN network
- A basic understanding of managing the HP *OpenVMS* operating system
- Access to Advanced Server documentation

Document Structure

This guide contains the following sections:

Section	Description
Chapter 1, Introducing the Advanced Server	Introduces the main features and capabilities of the Advanced Server software
Chapter 2, Domains and Trusts	Explains domains and trust relationships between domains
Chapter 3, User Accounts	Outlines the types of accounts available (user, built-in user, and local) so that you can manage accounts easily and provide users with network access
Chapter 4, Groups	Explains the types of groups available and how you can arrange them to make granting capabilities and permissions faster and easier
Chapter 5, Organizing Your Network into Domains	Discusses how the OpenVMS and Advanced Server security models work and how to manage user security by setting up user accounts, organizing users into groups, and controlling user capabilities
Chapter 6, Managing Network Shares	Explains how the Advanced Server works with the OpenVMS file system (file and directory ownership) and how to manage network shares
Chapter 7, Sharing Printers	Offers guidelines on how to set up and share printers on an Advanced Server network to maximize printer usage and avoid printing delays
Appendix A, Differences Between Advanced Server and Windows NT Server	Discusses the similarities and differences between the Advanced Server and the Windows NT Server that you encounter in day-to-day management of a network that includes both types of servers
Appendix B, Worksheets	Provides worksheets that you can use to plan and track domains, groups, and shares
Glossary	Defines commonly used Advanced Server and networking terms used in the Advanced Server documentation

Related Documents

The following table lists Advanced Server for OpenVMS documents:

Document	Description
HP Advanced Server for OpenVMS Server Installation and Configuration Guide	Explains how to install and configure Advanced Server software
HP Advanced Server for OpenVMS Server Administrator's Guide	Explains how to manage and customize the Advanced Server software
HP Advanced Server for OpenVMS Commands Reference Manual	Provides command syntax descriptions for all ADMINISTER commands and NET command equivalents
HP 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 PATHWORKS for OpenVMS (Advanced Server) documents:

Document	Description
Compaq PATHWORKS for OpenVMS Server Migration Guide	Explains how to upgrade a PATHWORKS V5 for OpenVMS (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 PATHWORKS for OpenVMS (Advanced Server) Server Administrator's Guide	Explains how to manage and customize the PATHWORKS for OpenVMS (Advanced Server) software
HP Advanced Server for OpenVMS Commands Reference Manual	Provides command syntax descriptions for all ADMINISTER commands and NET command equivalents
HP 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
HP OpenVMS Version 8.3 Upgrade and Installation Manual	Describes how to install the latest OpenVMS Alpha system software
OpenVMS VAX Version 7.1 Upgrade and Installation Manual	Describes how to install the OpenVMS VAX V7.1 system software
OpenVMS VAX Version 7.2 Upgrade and Installation Manual	Describes how to install the OpenVMS VAX V7.2 system software
HP OpenVMS System Manager's Manual	A task-oriented guide (in two volumes) to managing an OpenVMS system
HP OpenVMS System Management Utilities Reference Manual	A reference guide (in two volumes) to the utilities and tools used in managing an OpenVMS system
HP OpenVMS License Management Utility Manual	Explains how to load and manage license Product Authorization Keys (PAKs)
HP C Run-Time Library Utilities Reference Manual	Describes utilities that help you manage localization and time zone data for international software applications
COM, Registry, and Events for OpenVMS Developer's Guide	Contains COM for OpenVMS, OpenVMS Registry, and OpenVMS Events information

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

`http://h71000.www7.hp.com/openvms`

Reader's Comments

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

Internet	**openvmsdoc@hp.com**
Mail	Hewlett-Packard Company OSSG Documentation Group, ZKO3-4/U08 110 Spit Brook Rd. Nashua, NH 03062-2698

How To Order Additional Documentation

Use the following World Wide Web address to order additional documentation:

`http://www.hp.com/go/openvms/doc`

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

Conventions

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

Convention	Meaning
Advanced Server	Advanced Server refers to PATHWORKS Advanced Server as well as Advanced Server for OpenVMS file server.
Italic	Italic text indicates a place holder 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. Italic text also indicates new terms and the titles of other documentation referenced.
`monospace text`	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	Uppercase text indicates OpenVMS commands and qualifiers. You can enter commands and qualifiers in any combination of uppercase and lowercase characters, unless otherwise noted.
Note	The use of **Note** provides information of special importance.
Caution	The use of **Caution** provides information that prevents damage to software or hardware.
Warning	The use of **Warning** provides information that is essential to people's safety.
/	A forward slash in command descriptions indicates that a command qualifier follows.
. . .	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.

Convention	Meaning
. . .	A vertical ellipsis in an example indicates that not all the data is shown.
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.) 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

Introducing the Advanced Server

The Advanced Server is a network operating system (NOS) based on OpenVMS that is fully compatible with Microsoft networking technology.

As a server for workstations on a network, the Advanced Server provides file and print services that enable a community of desktop users to share computing resources efficiently. The Advanced Server can function as a simple 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.

The Advanced Server represents the new generation of LAN Manager systems technology. It enhances the LAN Manager functionality by incorporating the latest Microsoft technology to deliver powerful new features for network administration and enhanced security. The Advanced Server interoperates with systems running Windows NT, Windows 2000, and Windows XP software.

The Advanced Server is based on Windows NT Server source code from Microsoft and AT&T. As a result, the Advanced Server can take advantage of the OpenVMS operating system's native ability to function simultaneously as a file, print, communications, and applications server while ensuring compatibility with Microsoft networking features and interoperability with Microsoft desktop environments. In fact, the Advanced Server provides networking that is functionally equivalent to that of the Windows NT Server. The Advanced Server can operate independently or in cooperation with the Windows NT, Windows 2000 or a Windows 2003 server.

The Advanced Server can be remotely administered from PATHWORKS and Microsoft Windows client workstations. These workstations include Windows NT, Windows 2000 and Windows XP. Advanced Server can also be managed remotely from Windows NT Servers and other Advanced Servers.

Advanced Server maintains full down-level compatibility with LAN Manager client and server software. LAN Manager users can add an Advanced Server to an existing network and migrate to the new technology at their own pace. A PATHWORKS LAN Manager server can be upgraded to Advanced Server technology or act as a backup domain controller, member server, or standalone

server in a network in which the primary domain controller is an Advanced Server or a Windows NT Server computer.

The Advanced Server can be deployed as the primary domain controller in a network comprising other Advanced Servers, Windows NT Servers, PATHWORKS for OpenVMS (LAN Manager) servers, or LAN Manager for OS/2 servers. It also can act as a backup domain controller for other Advanced Servers and Windows NT Server computers. In addition, the Advanced Server can act as a backup domain controller and/or as a member server in Windows 2000 mixed-mode domains and Windows 2003 interim domains. Also as a member server in native-mode Windows 2000 domains and in Windows 2003 domains. *Windows 2000 mixed-mode domains* and *Windows 2003 interim domains* contain both Windows 2000 domain controllers and Windows NT or HP Advanced Server domain controllers. *Windows 2000 native mode domains*, also referred to as *pure Windows 2000 domains*, are those whose domain controllers are Windows 2000 systems exclusively. *Windows 2003 domains*, are those whose domain controllers are Windows 2003 systems exclusively.

Support for WINS (Windows Internet Name Service) integration allows Advanced Server servers to act as WINS clients; that is, to use the name registration and resolution facilities available from a Microsoft WINS server across routed wide area TCP/IP networks, thus enabling WAN support via WINS for domain functions.

Support of LMHOSTS enables the Advanced Server to resolve NetBIOS names by looking them up in a local database that maps NetBIOS names to TCP/IP addresses.

The Advanced Server can also use the name resolution facilities available from a DNS (Domain Name System) server for WAN support.

Note

When DNS is configured for use by the Advanced Server, it does not replace WINS or LMHOSTS but rather supplements them. 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 LMHOSTS, WINS, or both methods for resolving domain names and certain other names.

This guide explains the concepts that support the Advanced Server.

Note

In this guide, the term "Advanced Server" may be applied to either version of the file and print server:

- Advanced Server for OpenVMS
- PATHWORKS for OpenVMS (Advanced Server)

For instructions on installation and initial configuration, see the appropriate *Server Installation and Configuration Guide*.

For instructions on administrative procedures, see your *Server Administrator's Guide*.

For descriptions of the syntax of ADMINISTER commands, see the *HP Advanced Server for OpenVMS Commands Reference Manual* or the ADMINISTER online help at the OpenVMS DCL prompt (the Advanced Server must be installed on the OpenVMS system).

The remaining sections of this chapter outline the features provided by Advanced Server.

1.1 Platform and Application Independence

The Advanced Server supports the full range of Microsoft desktop environments, allowing network clients to run favorite applications locally and access the Advanced Server's resources transparently through a familiar interface.

The Advanced Server supports connections from the following types of clients:

- Windows NT V4.0
- Windows 2000 and Windows 2000 Professional
- Windows XP
- Windows 2003
- HP PATHWORKS 32

1.2 Network Integration Transports and Protocols

Advanced Server accepts connections from systems with the following protocols:

- DECnet (Phase IV)
- DECnet-Plus (formerly known as DECnet/OSI)
- NetBEUI (recommended for use in small LAN-only environments of 50 nodes or less)
- TCP/IP (required for wide area networking)

For more information about network protocols, see your *Server Administrator's Guide*.

1.3 Integration with the OpenVMS System

The Advanced Server encompasses many of the features of the OpenVMS operating system, including OpenVMS Clusters and symmetric multiprocessing. OpenVMS Cluster configurations provide failover and extensive resource capacities by integrating multiple OpenVMS systems that can be accessed using a single cluster name. The Advanced Server provides load balancing of client access requests. (See your *Server Administrator's Guide* for more information on the load balancing supported by your server.)

The Advanced Server provides an extension to the Windows NT security model by supporting OpenVMS security enforcement as an optional enhancement. In addition, the Advanced Server supports password synchronization between OpenVMS and Advanced Server systems, and it supports user account lockout.

The Advanced Server includes full support for the latest features of OpenVMS, such as:

– Extended File Specifications and ODS-5 (On-Disk Structure 5) disk volumes, providing greater compatibility with the Windows NT, Windows 2000, Windows XP, and Windows 2003 file systems

– OpenVMS Registry

– OpenVMS infrastructure changes for External Authentication and the distributed common object module (COM for OpenVMS)

1.4 Down-Level Interoperability

The Advanced Server interoperates with the installed base of Microsoft server and desktop environments. For example:

- The Advanced Server interoperates with LAN Manager V2.*x* servers on any platform — even in the same domain. MS-DOS, OS/2, and Windows 3.1 computers running LAN Manager V2.*x* client software can access systems running the Advanced Server. See Section 2.5.4, LAN Manager V2.x Servers, for more information.
- The Advanced Server can act as a server for standard MS-DOS client networks, in configurations with or without PATHWORKS client software.
- The Advanced Server supports connectivity with Windows for Workgroups.

1.5 Management Interfaces

You can use any of the following interfaces with the Advanced Server:

- Advanced Server ADMINISTER command-line interface — This command-line interface conforms to standard DCL command syntax. (The ADMINISTER command-line interface also provides automatic translation of Net commands that have ADMINISTER command equivalents.)
- Windows NT server administration tools — These management tools are included in the Advanced Server software kit for you to install on Windows NT workstations or Windows-based computers. You can use these tools to manage the Advanced Server remotely from your client workstation.
- Windows NT Server tools — These tools are available as part of the Windows NT Server.
- Windows NT printer management — The Advanced Server for OpenVMS gives you the option of configuring the server to allow management of shared printers from Windows NT. For more information, see Section 7.4, Managing Print Shares, Print Queues, and Print Jobs.

To administer the Advanced Server from a Windows client workstation, you must install Windows NT server administration tools. This set of tools allows you to administer the Advanced Server and Windows NT Server computers from network clients, such as Windows NT V4.0, Windows 2000, and Windows XP. An installable version of the tools is available in the PWUTIL share. From Advanced Server V7.3B onwards, based on your choice, PWUTIL share may not be created by default during the installation and configuration of Advanced Server. If you want to use the tools present in PWUTIL share create it by executing the following command:

```
$ @SYS$UPDATE:PWRK$PWUTIL.COM
```

Note

If Advanced Server is running when PWRK$PWUTIL.COM is executed, the procedure will prompt for a user name and password. If Advanced Server is not running, user name and password are not required.

When prompted for a user name and password, if Advanced Server is configured as a PDC or BDC, supply the credentials of a privileged domain user in order to successfully add or delete the files and shares.

If Advanced Server is configured as a member server, supply the credentials of the local member server administrator account or any privileged member server local account. Note that if you supply the credentials of a domain user when Advanced Server is configured as a member server, addition or deletion of the shares will fail.

See the README.TXT file included with the Advanced Server software for installation instructions for the Windows NT server administration tools. See Appendix A, Differences Between Advanced Server and Windows NT Server, for more information about differences between the two network operating systems.

1.6 Security

The Advanced Server builds security into the operating system, thereby enabling efficient management of large networks. You can set up domains and trust relationships between domains to centralize user accounts and other security information, making the network easier to manage and use. Every user needs only one account. This account can provide the user with access to resources anywhere on the network.

The Advanced Server also incorporates enhanced features that provide you with a high level of control over user and resource permissions and auditing. These features include support of:

- Discretionary access control permissions on individual files, directories, and resources
- Complete auditing capabilities

Optionally, the Advanced Server accommodates both the Advanced Server and OpenVMS security models.

For more information about how the Advanced Server integrates network security and protections within domains, see Chapter 5, Organizing Your Network into Domains, in this guide.

1.7 Network File and Printer Sharing

An important use of servers on most networks is to share files and directories among network users. The Advanced Server provides high performance, reliability, and security for file sharing.

The Advanced Server enables the sharing of local OpenVMS files to network users. You can use discretionary access controls and Advanced Server security on each file and directory to specify the groups and users that can access files, to define the levels of access that each group or user is permitted, and to control auditing. Additional security is provided by file ownership and OpenVMS file and directory protections.

You can set up printers connected to the OpenVMS system for network access by creating print shares for OpenVMS print queues defined for the printers. Printers are accessible to local OpenVMS users and network users. Beginning with Version 7.3 of the Advanced Server for OpenVMS, the server can be configured to enable management of its network printers from a Windows NT Server or workstation. You add a printer and make it available to the network by using Windows NT print services. For more details, see Section 7.4, Managing Print Shares, Print Queues, and Print Jobs. By default, the ADMINISTER command-line interface is used to manage printers. PATHWORKS for OpenVMS (Advanced Server) servers allow printer management from the ADMINISTER interface only.

1.8 User Environment Management

You can use logon scripts to configure MS-DOS and Windows workstation user environments by making network connections and starting applications.

You can create user profiles to make workstation computers easier to use and to control workstation access to network resources.

For more information about using logon scripts and user profiles, see Chapter 2, Domains and Trusts, in this guide.

1.9 Monitoring and Tracking Network Activity

The Advanced Server provides event logging and the ability to monitor network activity and track computer usage.

You can display servers and see which resources they are sharing. You can display the users currently connected to any network server and see which files are open, log and display security auditing entries, keep sophisticated error logs, and specify that alerts be sent to administrators when certain events occur.

For information on how to monitor and track network activity, see your *Server Administrator's Guide*.

1.10 Network Browser Services

The Advanced Server can act as a Master Browser in a Windows NT network.

1.11 Server Configuration

The installation process includes a configuration procedure (PWRK$CONFIG) that you use to set up your initial configuration. You can make additional adjustments to the configuration after running the configuration procedure:

- You can modify parameters that 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). You can configure such elements as the data cache size, the security mode, and the number of clients supported. Use the Configuration Manager to modify these parameters. For information on how to modify an Advanced Server using the Configuration Manager, see your *Server Administrator's Guide*.
- You can modify server-specific parameters that affect the behavior of the Advanced Server but not, for the most part, file server resource consumption. These server parameters specify information that identifies the file and print server, controls the services that are started, and provides customization of the server.

  The Advanced Server for OpenVMS stores and retrieves these parameters in the OpenVMS Registry. You use the PWRK$REGUTL utility to modify these parameters. Refer to the *HP Advanced Server for OpenVMS Server Administrator's Guide* for more information about the Advanced Server parameters structure in the OpenVMS Registry and how to use PWRK$REGUTL.

The PATHWORKS for OpenVMS (Advanced Server) stores and retrieves these parameters in the LANMAN.INI file. For a list of the LANMAN.INI file parameters, and instructions for modifying their values, see the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Administrator's Guide*.

1.12 License Management

Advanced Server offers license management for both client-based and server-based licenses.

To connect to the Advanced Server, clients must be properly licensed. The Advanced Server licensing subsystem keeps track of the licensing database and validates client licenses when clients attempt their initial connection to the server. The Advanced Server licensing subsystem includes the following basic components, which are automatically installed with the Advanced Server software:

- License Registrar — Validates that clients accessing the Advanced Server are appropriately licensed. Also manages the assignment of server-based licenses. Runs on all Advanced Server systems.
- License Server — Performs license-related services, such as assigning, verifying, and managing client-based licenses.
- License Manager — An interface between the system administrator and the Advanced Server License Server that provides the ability to manage license groups, set alert levels, set logging levels for licensing events, enable or disable the License Server, and revoke assigned licenses.

  For a complete description of the licensing software and how to manage Advanced Server and PATHWORKS licenses, see the *HP Advanced Server for OpenVMS Guide to Managing Advanced Server Licenses*.

1.13 Remote Network Management

Using the Advanced Server management interfaces, you can remotely manage other servers in the domain. You can remotely manage the following kinds of servers:

- Windows NT Servers
- Other Advanced Server servers (OpenVMS and UNIX)
- PATHWORKS V5 LAN Manager servers (OpenVMS and UNIX)
- LAN Manager V2.*x* servers

You can use the ADMINISTER command-line interface to manage servers, services, and domains. (The functionality for managing PATHWORKS V5 for OpenVMS (LAN Manager) and LAN Manager V2.2 servers is limited.)

For information on how to manage remote servers, see your *Server Administrator's Guide*.

1.14 Upgrading from Previous Versions

You may install Advanced Server for OpenVMS on a system that was previously running PATHWORKS V6 for OpenVMS (Advanced Server). User, share, and security information in the Security Accounts Manager (SAM) database are automatically upgraded when you configure the Advanced Server.

If the system is running a server version previous to PATHWORKS V6.0C for OpenVMS (Advanced Server), then before you install the Advanced Server for OpenVMS, you should:

1. Upgrade the operating system to OpenVMS Version 7.2-1 (or higher)
2. Upgrade the server to V6.0C.

HP recommends the following migration path for systems running the PATHWORKS V5 for OpenVMS (LAN Manager) file server on OpenVMS Alpha Version 6.2 systems:

1. Upgrade the V5 file server to PATHWORKS V6.1 for OpenVMS (Advanced Server)
2. Upgrade the operating system to OpenVMS Version 7.3-2 (or higher)
3. Upgrade the Version 6 file server to Advanced Server V7.3B for OpenVMS

Refer to the appropriate Software Product Description (SPD) for information about the OpenVMS versions supported by each version of PATHWORKS for OpenVMS and Advanced Server for OpenVMS.

If you are running a version of PATHWORKS prior to V5, you must first upgrade to PATHWORKS V5 for OpenVMS (LAN Manager), and then upgrade to PATHWORKS V6 for OpenVMS (Advanced Server) before proceeding with the installation of your latest Advanced Server product.

When you install PATHWORKS V6 for OpenVMS (Advanced Server), the Upgrade utility is automatically included with it. You can use the Upgrade utility to upgrade the users, groups, shares, and security of a PATHWORKS V5 for OpenVMS (LAN Manager) server. If you want to continue running the PATHWORKS LAN Manager server while performing the upgrade, you must install the Upgrade utility separately before installing the PATHWORKS V6 for OpenVMS (Advanced Server).

For information on how to upgrade PATHWORKS LAN Manager servers to PATHWORKS V6 for OpenVMS (Advanced Server), see the *Compaq PATHWORKS for OpenVMS Server Migration Guide*. For information on installing the Upgrade utility, see the *Compaq PATHWORKS for OpenVMS (Advanced Server) Server Installation and Configuration Guide*.

1.15 Solving Problems with the Advanced Server

The Advanced Server provides event logs and an audit trail. These resources let you track and manage server events and performance and troubleshoot problems. You can monitor and log events on any Advanced Server.

For more information on solving problems with the Advanced Server, see your *Server Administrator's Guide*.

2
Domains and Trusts

The Advanced Server provides an administrative model for managing a large network efficiently. This model lets you manage and track the actions of users while allowing them to access the resources they need. Central to the idea of security in the Advanced Server is the concept that every resource and action is protected by *discretionary access control*. Discretionary access control allows you to permit some users to access a resource or perform an action while preventing other users from doing so.

Conventional OpenVMS file systems support simple file and directory protections — read, write, delete, and execute — for four categories of users: owners, members of the file owner's group, system administrators, and all others. The Advanced Server allows you to grant or deny users and groups a wide set of permissions; these permissions can work in concert with the standard OpenVMS file system protections. In addition, the Advanced Server allows you to apply a number of *user:permission* or *group:permission* pairs to any file, directory, or resource. You can set different permissions on different files in the same directory.

2.1 Domain and Trust Relationships

The basic administrative unit of Advanced Server is the *domain*. A domain is a collection of computers that share a common domain security accounts database (also called the domain's Security Accounts Manager (SAM) database or security database) and security policy. All of the Advanced Servers in a domain use the same set of user accounts. As a result, you need to enter information for a user account only once to allow all servers in the domain to recognize the user.

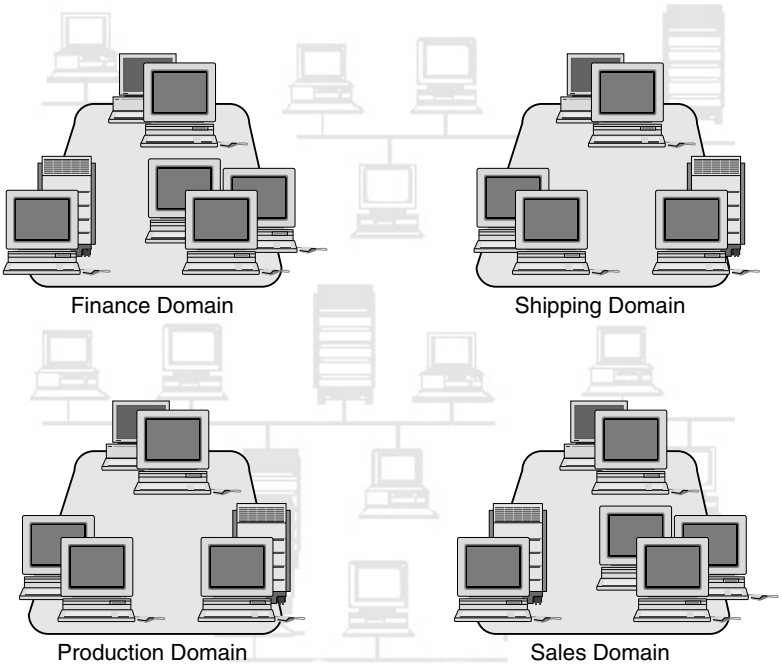
Trust relationships are links between domains. In a trust relationship, a user with an account in one domain can access resources provided by another domain. This feature is called *pass-through authentication*. If the domains and trust relationships on your network are well planned, all your Advanced Server computers can recognize every authorized user, so a user needs to log in only once to access any required resource on the network.

2.2 Benefits of Using Domains

Grouping computers into domains offers significant benefits to network administrators and users. The first and most important benefit is that servers in a domain form a single administrative unit that can share security and user account information. Every domain has one database, referred to as the *security accounts database* or the *Security Account Manager (SAM) database*, that contains user and group accounts and security policy settings. Every server in the domain (except member servers) can maintain a copy of this database. One server, designated as the *primary domain controller (PDC)*, maintains the master copy of this database. The master copy is synchronized with the copies of the database that are stored on the *backup domain controllers (BDCs)* in the domain. The primary domain controller replicates its databases to the backup domain controllers. Normally, synchronization occurs automatically at regular intervals. Administrators can also synchronize them manually. For more information, see your *Server Administrator's Guide*.

By extending the administrative unit from a single computer to an entire domain in this way, the Advanced Server saves administrators and users time and effort. For example, administrators need to manage only one account for each user, and each user needs to use only one account. The user account information is replicated to the security account databases maintained domain-wide. Figure 2–1 shows four domains set up as basic administrative units on a network.

Figure 2–1 Grouping Computers into Domains



The second benefit of domains is user convenience. When users browse the network for available resources, they see the network grouped into domains instead of viewing all the individual servers on the network. This implementation of domains is similar to the use of *workgroups* in Microsoft Windows for Workgroups. Advanced Server domains are compatible with workgroups in the Windows for Workgroups platform.

For more information about Windows for Workgroups, see Section 2.6.4, Windows for Workgroups Computers, in this guide.

Note

Do not confuse Advanced Server domains with TCP/IP network protocol domains. A TCP/IP domain describes part of the TCP/IP Internet and is not related to Advanced Server domains.

2.3 Allowing Users Access to Resources in Other Domains

You can provide a user with access to resources in a second domain without creating and maintaining a separate user account in the second domain, and without granting hard-to-maintain individual permissions directly to the person. A user can access resources in other domains as easily as those in the user's own domain.

To allow a user access to resources in a domain where the user has no user account, you can:

1. Establish a trust relationship between the two domains in which the user's domain becomes the *trusted domain*, and the domain the user must access becomes the *trusting domain*.
2. Create a *local group* in the trusting domain. Add to the local group the name of the user's account or the name of a global group to which the user belongs on the trusted domain. (If you add users as individuals rather than as members of global groups, the relationships are more difficult to maintain.)
3. Modify the *share* permissions to allow the local group to access the share.
4. Ensure that protections and permissions on the share are appropriate to the user's requirements.

The text and examples that follow will clarify several new terms introduced here, such as share, global group, and local group. For definitions of new terms, you can also see the Glossary in this guide.

2.4 Links Between Domains: Trust Relationships

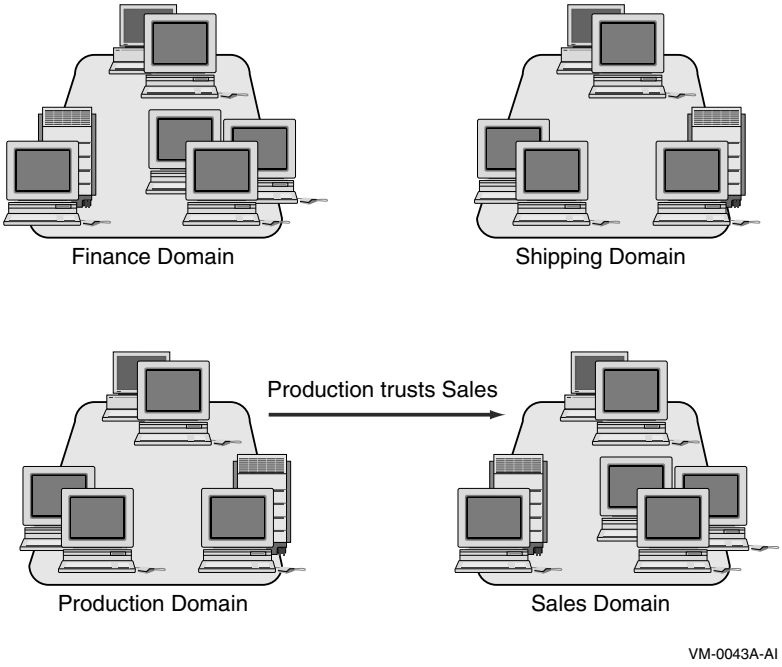
Trust relationships between domains enable user accounts to be used in domains other than the ones in which they reside. Trust relationships make administration easier because you create user accounts only once on your network. Then, you can give a user account access to any computer on the network, not only to the computers in one domain.

2.4.1 Establishing a One-Way Trust Relationship

When you establish a one-way trust relationship between domains, one domain (the *trusting domain*) trusts the other (the *trusted domain*). Figure 2–2 shows a one-way trust relationship in which the Production domain trusts the Sales domain. Users from the Sales domain can access resources in the Production domain even though they do not have accounts in the Production domain.

Sales, however, does not trust Production; therefore, resources from Sales cannot be used by users in the Production domain.

Figure 2–2 A One-Way Trust Relationship



Establishing this one-way trust relationship requires administrative access to both domains and a password. For example:

1. The administrator logs in to domain Sales and adds the trust with domain Production (this adds the domain Production to a list of domains permitted to trust Sales).
2. On domain Production, the administrator adds the trust with Sales (this adds Sales to a list of domains trusted by Production).

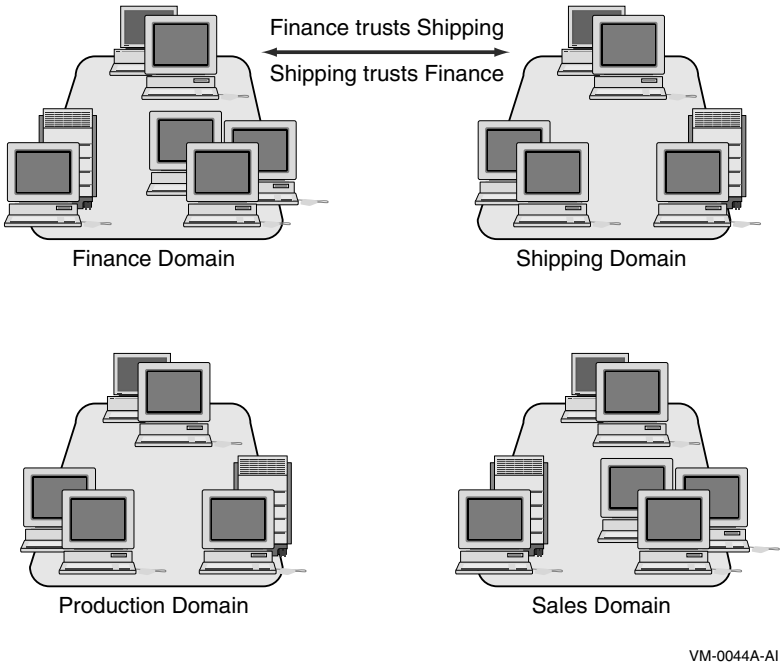
Subsequently, the trusting domain Production recognizes all user and global group accounts from the trusted domain Sales. These accounts can be used anywhere in the trusting domain: they can log on at workstations, reside in local groups, or be given access to resources in the trusting domain. For more information on establishing a one-way trust, see your *Server Administrator's Guide*.

2.4.2 Establishing a Two-Way Trust Relationship

A trust relationship can be one-way or two-way. A two-way trust relationship is a pair of one-way relationships in which each domain trusts the other.

In Figure 2–3, the Finance and Shipping domains trust each other; therefore, accounts in each of these domains can be used in the other. Users in the Finance domain can access resources in the Shipping domain, and users in the Shipping domain can access resources in the Finance domain.

Figure 2–3 A Two-Way Trust Relationship

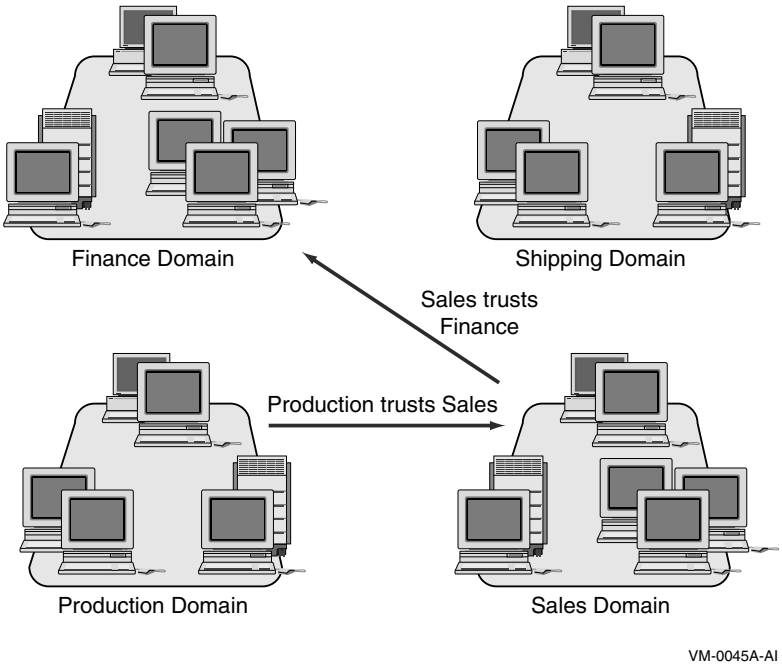


For more information on establishing a two-way trust relationship, see your *Server Administrator's Guide*.

2.4.3 Nontransitive Trust Relationships

Trust relationships among domains are not transitive. Although, as shown in Figure 2–4, Production trusts Sales and Sales trusts Finance, it does not follow that Production trusts Finance automatically. If Production needs to trust Finance and allow Finance accounts to be used in the Production domain, you must establish an explicit trust relationship between Production and Finance.

Figure 2–4 A Nontransitive Trust Relationship



Remember that you must take steps in each domain to define trusted and trusting domains, as discussed in the preceding sections and, in more detail, in your *Server Administrator's Guide*.

2.5 Domain Composition

The minimum requirement for an Advanced Server domain is one server running either Advanced Server (OpenVMS or UNIX) or Windows NT Server software. This computer serves as the primary domain controller (PDC) and stores the master copy of the domain's security accounts database. A domain can contain only one PDC. As discussed in Section 2.5.3, Member Server, Windows 2000 and Windows 2003 domains are composed differently. The Advanced Server can function in native-mode (pure) Windows 2000 domains and Windows 2003 domains as a member server, or in mixed-mode Windows 2000 domains and Windows 2003 interim domains as a backup domain controller (BDC) or member server.

A domain can include, as BDCs, other servers running Advanced Server (OpenVMS or UNIX), Windows NT Server, or LAN Manager V2.*x* software; it can also include Advanced Server, Windows NT Server, and LAN Manager V2.*x* servers as standalone or member servers. (The Advanced Server for OpenVMS can participate in Windows 2000 and Windows 2003 domains. For more information, see Section 2.5.2, Backup Domain Controller, and Section 2.5.3, Member Server.)

The clients in a domain can include Windows NT workstations; Windows 2000 and Windows XP workstations. The following sections discuss individual domain components in detail.

The following pertains to Advanced Servers operating in an OpenVMS Cluster:

- All cluster members running the Advanced Server share a common set of databases, including the Security Account Manager (SAM) and share databases.
- All cluster members serve the same domain role and function, as a single entity identified by the Advanced Server cluster alias name. When an Advanced Server cluster joins a domain, a hidden computer account is created in the domain SAM database using the Advanced Server cluster alias name (there are no computer accounts for individual cluster members running the Advanced Server).

2.5.1 Primary Domain Controller

The primary domain controller of an Advanced Server domain must be a server running either Advanced Server or Windows NT Server software. Every change made to a domain's user and group database is made to the database of the primary domain controller.

To change the user database when managing an Advanced Server with the ADMINISTER command, you specify only the name of the domain to which the change applies; you do not need to specify the server name. The Advanced Server makes the change automatically to the database of the primary domain controller. For more information on modifying the user database, see the ADD USER and MODIFY USER entry in the *HP Advanced Server for OpenVMS Commands Reference Manual* or the ADMINISTER commands online help.

2.5.2 Backup Domain Controller

In a domain, except for the primary domain controller, every server running Advanced Server or Windows NT Server is a backup domain controller or a member server. A backup domain controller stores a copy of the domain's security account database, which is automatically synchronized with the primary domain controller. You cannot change the user database on a backup domain controller.

Like the primary domain controller, a backup domain controller can process logon requests from users who want to log on to the domain. When the domain receives a request to log on, either the primary domain controller or any of the backup domain controllers can authenticate the logon attempt.

You should have at least one backup domain controller running Advanced Server or Windows NT Server in a domain. If the primary domain controller becomes unavailable, a backup domain controller can be promoted to primary domain controller and the domain can continue to function normally. Having multiple servers also distributes logon request processing; this is especially useful in domains with many user accounts.

In domains with multiple computers running Advanced Server, one acts as the primary domain controller and the other computers are designated as backup domain controllers or member servers. In domains with WAN configurations (with server computers at different locations), each site should have at least one backup domain controller running Advanced Server or Windows NT Server to permit logon validation if access to the primary domain controller becomes unavailable.

Note that as a BDC, the Advanced Server can partipate in Windows 2000 mixed-mode and Windows 2003 interim domains. To participate in a native-mode Windows 2000 domain or in a Windows 2003 domain, the Advanced Server must be configured as a member server, as described below.

2.5.3 Member Server

In addition to one primary domain controller and one or more backup domain controllers, the domain can contain one or more member servers. Advanced Server, Windows NT Server, and LAN Manager V2.*x* servers can function as member servers. (Support of member server functionality begins with V7.3 of the Advanced Server for OpenVMS.)

A domain can have several member servers, or none. A member server differs from a domain controller in the following ways:

- The member server does not store copies of the domain's security accounts database.
- The member server does not validate domain logon requests.

Member servers rely on domain controllers to validate credentials of users requesting access to member server shares. When a domain user attempts to access data on a member server's shares, the user's workstation sends user name and password information to the member server. The member server then relays this information to a domain controller to authenticate the user. The domain controller can authenticate domain user requests to member server resources.

You may want to configure your Advanced Server as a member server instead of a backup domain controller (or primary domain controller) for any of the following reasons:

- Member servers do not spend time processing logon requests. Thus, this role can be a good choice for servers that have heavy workloads or that perform extremely time-critical tasks.
- More important, configuring one or more servers as member servers rather than domain controllers can help decrease the network load, eliminating network traffic normally generated by domain controllers for replicating user databases and authenticating logon requests. (When a client attempts to find a logon server to authenticate a request, all domain controllers respond to the request. In some environments, this can generate a significant load on the network.)

- As a member server, the Advanced Server can participate in a native-mode Windows 2000 environment (also referred to as a pure Windows 2000 environment, this is a domain in which all domain controllers are Windows 2000 systems) or in Windows 2003 environment (this is a domain in which all domain controllers are Windows 2003 systems).

  In a native-mode Windows 2000 or Windows 2003 domain environment, domain controllers participate in a "multi-master domain controller model," meaning that changes to the security accounts database can be made on any domain controller. Any domain controller can be the replicator, sending copies of the updated security accounts database to the other domain controllers.

  This model contrasts to the primary/backup domain controller model used by Windows NT Servers and Advanced Server for OpenVMS servers configured as PDCs and BDCs. In the PDC/BDC model, changes to the security accounts database must be made on the primary domain controller first, which then replicates the database to the backup domain controllers.

  Configuring the Advanced Server as a member server, network administrators can include the Advanced Server for OpenVMS in a native-mode Windows 2000 or in a Windows 2003 domain, and the Windows 2000 and/or Windows 2003 domain controllers can continue using the multi-master model uninterrupted.

  The Advanced Server can also participate as a backup domain controller or member server in a mixed-mode Windows 2000 domain or in Windows 2003 interim domains.

- You can set up different administrator or user accounts from the rest of the servers in a domain. For example, you may have a person dedicated to administering a particular type of database. If you make the Advanced Server a member server, then you can make that person an administrator on the server with the special database. This way, he or she can manage that server but not have any control over the domain's master user accounts database or its other servers.

- If there is a possibility that your Advanced Server may be moved to a different domain in the future, it is simpler to move a member server from one domain to another than to move a BDC from one domain to another.

2.5.4 LAN Manager V2.x Servers

PATHWORKS for OpenVMS (LAN Manager) and LAN Manager V2.*x* servers can coexist in a domain with the Advanced Server. A LAN Manager server cannot be the primary domain controller in such a domain, however, because LAN Manager V2.*x* does not support all the types of information contained in Advanced Server accounts.

Under some circumstances, you may need to maintain LAN Manager servers. For example, you may need to have a PATHWORKS V5 for OpenVMS server to provide Remote Boot Services, which are not supported by Advanced Server. You can incorporate LAN Manager servers into your network as backup domain controllers, member servers, or standalone servers in an Advanced Server domain.

Adding a LAN Manager server to an Advanced Server domain presents a few challenges because of the following differences in server capabilities:

- The LAN Manager server receives a copy of the domain's user and group database, but the LAN Manager server does not recognize local groups. Therefore, you cannot assign permissions for resources on LAN Manager servers based on the domain's local groups.
- LAN Manager servers are limited to 256 groups, but there is no limit to the number of groups that can exist in an Advanced Server domain. If the number of groups in a domain containing a LAN Manager server exceeds 256, the replication process can break down, affecting the databases on LAN Manager servers.
- LAN Manager servers do not recognize trust relationships. Therefore, if the domain containing LAN Manager servers trusts other domains, you cannot assign permissions on the LAN Manager servers to users and global groups from the trusted domain.
- Domains composed entirely of LAN Manager servers cannot have trust relationships with other domains and therefore cannot allow users and global groups defined on other domains to access its resources. If a workstation user in an Advanced Server domain needs to access a resource in a LAN Manager domain, that user must also have an account in the LAN Manager domain, or that domain must allow guest logon.

If it is a backup domain controller or member server, a LAN Manager server stores a copy of the domain's security database. A LAN Manager server running as a backup domain controller can validate logon attempts from computers running Windows for Workgroups or LAN Manager software. A LAN Manager standalone server does not receive a copy of the domain

accounts database, and neither standalone nor member servers can validate client domain logon requests.

Note

Do not rely solely on LAN Manager servers as your backup domain controllers in an Advanced Server domain. LAN Manager servers cannot authenticate logon requests from Windows NT workstation computers, and they cannot be promoted to primary domain controller in an Advanced Server domain.

2.5.5 Windows NT Servers

A Windows NT Server can be part of the same domain as an Advanced Server and can be designated as the primary domain controller.

For more information about the differences between Windows NT Server and the Advanced Server, see Appendix A, Differences Between Advanced Server and Windows NT Server, in this guide.

2.5.6 Advanced Server for UNIX (Tru64 UNIX) Servers

An Advanced Server for UNIX (Tru64 UNIX) server can be part of the same domain as an Advanced Server for OpenVMS server and can be designated as the primary domain controller. For Advanced Server for UNIX (Tru64 UNIX) servers, you have the following options:

- You can remotely manage the Advanced Server for UNIX (Tru64 UNIX).
- From an Advanced Server for UNIX (Tru64 UNIX), you can remotely manage the OpenVMS Advanced Server.

For more information about the Advanced Server for UNIX (Tru64 UNIX) product, see the Advanced Server for UNIX (Tru64 UNIX) documentation set.

2.6 Workstation Environments

On an Advanced Server network, you can use user profiles to define and enhance workstation environments. A user profile contains the per-user settings of the Windows NT environment, including the following:

- *Logon script* specification

  A logon script can be a batch file containing Advanced Server and operating system commands, such as commands to make network connections or start application or executable programs. If a user has a logon script, that script is run whenever the user logs on at any type of workstation on the network.

  For more information about logon scripts, see Section 2.6.1, Tips for Using Logon Scripts, in this guide.

- *Home directory* location

  A home directory gives a user storage space. Normally, users also control access to their home directories and can restrict or grant access to other users.

  For more information about home directories, see Section 2.6.2, Tips for Using Home Directories , in this guide.

You manage user environments by editing the user profile. However, user profiles are applicable only at Windows NT workstation computers and have no effect on other types of client workstations.

2.6.1 Tips for Using Logon Scripts

A logon script is an executable or batch file composed of Advanced Server and operating system commands that runs automatically when a user logs on to the network. Logon scripts are used to configure users' work environments, make network connections, and start applications. They also can be used to run programs that scan for computer viruses on local workstations.

Advantages to using logon scripts include:

- You can manage part of the user's environment (such as network connections) without managing or dictating the entire environment.
- You can create common network connections for multiple users.
- Logon scripts are centrally located on the server and are easy to create and maintain.
- If you have a LAN Manager server running on your network, you can continue to use the logon scripts that you created for that system.

To assign a user a logon script, specify the path name of the logon script file in the user's account profile. Then, when the user logs on, the logon script downloads and runs. You can assign a different logon script to each user or create logon scripts for use by multiple users. For more information on user profiles, see Chapter 3, User Accounts.

The path name that you specify in the user's account profile is relative to the logon script path of the computer on which the script is stored. For example, if PWRK$LMROOT:[LANMAN.REPL.IMPORT.SCRIPTS] is the computer logon script path and PWRK$LMROOT:[LANMAN.REPL.IMPORT.SCRIPTS]*cristalw.bat* is the script for CristalW, then you need to specify only *cristalw.bat* as the logon script path name in CristalW's account profile.

To create a logon script, simply create an MS-DOS batch file. Table 2–1 describes several special parameters that you can use when creating logon scripts. Although a logon script works from any client, these parameters apply only when the user logs on from a Windows NT client.

Table 2–1 Parameters for Logon Scripts

Parameter	Description
%HOMEDRIVE%	The letter for the local workstation drive connected to the user's home directory.
%HOMEPATH%	The full path name of the user's home directory. This parameter applies only when the home directory is a local directory (absolute path) on the workstation.
%HOMESHARE%	The share name containing the user's home directory. This parameter applies only when the home directory is a shared network directory (UNC path).
%OS%	The operating system of the user's workstation.
%PROCESSOR_ ARCHITECTURE%	The processor type (such as 80386) of the user's workstation.
%PROCESSOR_ IDENTIFIER%	The processor model (such as Model 3, Intel) of the user's workstation.
%PROCESSOR_ LEVEL%	The processor level (such as 6) of the user's workstation.
%PROCESSOR_ REVISION%	The processor revision (such as 0304) of the user's workstation.
%USERDOMAIN%	The name of the domain containing the user's account.
%USERNAME%	The user's user name.

A logon script always downloads from the server that validates the user's logon request. To ensure that logon scripts always work, be sure that logon scripts for all user accounts in a domain exist on every server in the domain that validates logon requests.

2.6.2 Tips for Using Home Directories

Home directories can serve as private storage spaces for users. Users can control access to their home directories and can restrict or grant access to other users.

The home directory can be a local path on the server or a remote path located on another server on the network. If users have home directories on computers other than their own workstations, connections are made automatically to their home directories at every logon from a Windows NT workstation computer.

Whenever a user starts from the command prompt on a Windows NT workstation computer, the user's home directory is set as the default directory. The user's home directory also is set as the working directory for all applications that the user starts, except when those applications have a program item that specifies a different working directory. Note that the home directory takes effect only for users starting from a Windows NT workstation. When a user logs on from a non-Windows NT client, the usual default directory takes effect.

For information on file and directory permissions, see Chapter 6, Managing Network Shares, in this guide.

2.6.3 Windows NT, Windows 2000 and Windows XP Workstation Computers

Each Windows NT, Windows 2000, and Windows XP workstation computer on your network can participate in either a domain or a workgroup.

A Windows NT, Windows 2000, and Windows XP workstation computer participating in a workgroup has its own database of users, processes logon requests by itself, uses only its own users and groups, and is separate from all domains. Computers in a workgroup do not share account information. On this type of workstation, only the user accounts that were created at the workstation can be logged on to or given rights and permissions at the workstation.

Users can log on to an Advanced Server domain from a Windows NT, Windows 2000 or Windows XP workstation only if that workstation is part of the domain or of a trusted domain. A Windows NT, Windows 2000 or Windows XP workstation computer that participates in a domain does not get a copy of the domain's user database, but it does receive the benefits of the domain's user and group database. It can use user accounts and global groups from that domain, and the domains it trusts, to provide access to resources on the workstation.

At a Windows NT, Windows 2000 or Windows XP workstation computer participating in a domain, users can log on to user accounts located in the workstation domain (or in any domain the workstation domain trusts). For example, suppose a workstation is participating in the Sales domain, and Sales trusts the MIS domain. At the workstation, a user can log on to an account located in either the Sales domain or the MIS domain. You can place users and global groups from the domain (and domains trusted by the workstation domain) in local groups on the workstation, and you can assign permissions and rights on the workstation to users and global groups from the domain (and domains trusted by the workstation domain).

Even though a workstation participating in a domain can use accounts located in that domain, user accounts still can be created at the workstation itself. These accounts are local to that workstation and cannot be used on any other computer.

You should not create a local workstation account for a user who has a domain account. Instead, a user with a domain account always should log on to that account.

Note

Even if a Windows NT, Windows 2000 or Windows XP workstation computer participates in a domain, it cannot use local groups defined in the domain; however, it can use users and global groups defined in the domain. See Chapter 4, Groups, in this guide for more information about using groups.

2.6.4 Windows for Workgroups Computers

Windows for Workgroups computers generally are organized into *workgroups*. Workgroups are similar to domains in network browsing: When a user uses File Manager to browse the network, the user sees the network divided into domains and workgroups. If the user selects a domain or workgroup, then the user can browse the contents of that domain or workgroup.

Every Windows for Workgroups computer on your network can participate in a domain or in a workgroup. In most cases, you will want Windows for Workgroups computers to participate in a domain so that they can be integrated into the Advanced Server administrative models.

Windows for Workgroups computers can participate in workgroups containing Windows NT workstations. Similarly, on a Windows for Workgroups computer, you can specify the name of an Advanced Server domain as the computer's workgroup and the Windows for Workgroups computer can then function as a computer contained in the domain.

If a Windows for Workgroups user must access a resource in a domain that has no Windows for Workgroups computers, the user must know the name of the computer on which the resource is located. Whenever a Windows for Workgroups computer starts, the user can log on to the network using a user name and password previously specified at the computer. Alternatively, the user can wait to log on to the network until making an initial network access attempt.

If a Windows for Workgroups user has an account in an Advanced Server domain, you can specify the user name and password of that account to Windows for Workgroups and set the workgroup name on the computer to be the name of the domain. Then, users can log on to their domain accounts automatically when they log on to the network.

2.6.5 Windows 95 and Windows 98 Computers

You can choose whether you want the Windows 95 and Windows 98 computers on your network to participate in a workgroup or in a domain. In most cases, you will want them to participate in a domain, because a user with an account on an Advanced Server domain can log on to that account from a Windows 95 or Windows 98 computer only if that computer is part of the domain.

Windows 95 and Windows 98 computers that participate in a domain do not get a copy of the domain's user database, but they do receive the benefits of the domain's user and group databases.

You can configure a Windows 95 or Windows 98 computer to prevent users from logging on to the local workstation after an unsuccessful attempt to log on to the domain. This prevents users from gaining access to resources local to the Windows 95 or Windows 98 workstation if, for example, their domain user accounts have expired or have been disabled.

A Windows 95 or Windows 98 computer that participates in a workgroup has its own database of users and can process logon requests. However, computers in a workgroup do not share account information. This means that you can assign rights and enable users to log on only to accounts that are created on the Windows 95 or Windows 98 computer.

Windows 95 and Windows 98 computers that participate in a workgroup can control access to resources by running share-level security. Under share-level security, each shared resource on a local workstation is protected by a unique password. Users from remote computers can access the resource only if they enter the correct password.

2.6.6 Windows, MS-DOS, and OS/2 Computers

Windows V3.*x*, MS-DOS, and OS/2 computers cannot store user accounts. This makes them unable to participate in domains in the same way as Windows NT, Windows 95, Windows 98, Windows 2000, or Windows for Workgroups computers. However, with valid network logon, they can access resources on servers.

Windows, MS-DOS, and OS/2 computers usually have a default domain set for network viewing. If a user has a domain account, the domain into which the user logs on is always viewed. You can add other domains to the viewing list.

3
User Accounts

The Advanced Server makes account management easy for administrators and network access easy for users, while ensuring network security. The Advanced Server provides user, built-in user, global, and local accounts so that you can provide appropriate network access for users.

This chapter describes the types of user accounts and how to provide users access to resources they need.

3.1 What is a User Account?

A *user account* contains information about the user, which includes the name, password, and restrictions on how the user can use the network. Every person who uses the network must have a user account on a domain in the network. A user needs only a single, centrally stored account. This account can provide the user with access to resources anywhere on the network.

Table 3–1 shows the attributes of a user account.

Table 3–1 User Account Attributes

Account Attribute	Comment
User name	The unique name that the user types when logging on. Often a combination of parts of the user's first and last names; for example, EGIBBONS for Evan Gibbons. The user name is unique within the domain.
Account security identifier (SID)	The unique number that identifies the account (hidden). A SID is generated automatically when an account is entered.
Account type	The account type is either global or local. Most accounts you create will be global accounts.
Description	A brief description of the user (optional).

(continued on next page)

Table 3–1 (Cont.) User Account Attributes

Account Attribute	Comment
Domain	Name of the domain where the user logs on.
Expiration date	A future date when the account automatically becomes disabled; it is useful for ensuring that accounts for temporary employees or students are not kept active unnecessarily (optional).
Full name	The user's full name, up to 48 characters (optional).
Group names	Names of local and global groups to which the user belongs.
Logon hours	The hours during which the user is allowed to log on. The default is all hours. This attribute determines when the user can log on to the network and access servers. Whether users are forced to log off when their logon hours expire is determined by a setting in the domain's security policy. For more information, see Section 3.2, Setting Password and Account Policies for the Domain, in this guide.
Logon workstations	The computer names of the workstations from which the user can log on to the domain. By default, the user can use any workstation, but you can restrict logon access to particular workstations (optional).
Password	The user's password. Generally not displayed as the user enters it. The Advanced Server and OpenVMS have independent user accounts databases, so OpenVMS users can have two passwords — one for OpenVMS and one for Advanced Server. (Advanced Server passwords are case sensitive; OpenVMS passwords are not.) See Section 3.7, Password Synchronization, for more information on how to synchronize Advanced Server and OpenVMS account passwords.
User Profile	A file containing the user's home directory and logon script. The home directory is a directory on the server that is private to the user; the user controls access to this directory (optional). The logon script is a batch file or executable file that runs automatically when the user logs on (optional).

For each user account, several conditions are either true or false, as shown in Table 3–2.

Table 3–2 User Account Conditions

Account Condition	Default	Comments
Change Password at Next Logon?	Yes	If yes, users are forced to change the password the next time they log on. Then, after a user changes the password, this value is set to No.
User Cannot Change Password	No	If yes, users cannot change their own passwords. This is useful for shared accounts.
Password Never Expires	No	If yes, this user account ignores the password expiration policy set for the domain, and the password never expires. This is used for accounts that represent services, such as the Event Logger service. It is also useful for accounts for which you want the password never to change.
Account Disabled	No	If yes, this account is disabled and cannot be logged on to. It is not removed from the database, but no one can log on to the account until you again enable it. This is useful for "template accounts." See Section 3.3, Creating User Accounts, in this guide for more information.

3.2 Setting Password and Account Policies for the Domain

For each domain, you can specify every aspect of password policy: minimum password length (default is 6), minimum and maximum password age (defaults are 1 day and 90 days, respectively), and password uniqueness, which prevents a user from changing his or her password to a password that the user has used recently (the default is not to enforce password uniqueness). The Advanced Server ADMINISTER commands allow you to specify password and account policies.

You also can specify whether users are forced to disconnect from the domain's servers when their logon hours expire. If users have not ended their connections by the time their logon hours expire, the servers they are connected to will end the connections. Users are not forced to log off their workstations.

For more information on how to set password and account policies, see your *Server Administrator's Guide*.

3.3 Creating User Accounts

Because user accounts contain so much information, it can be time consuming to add individual user accounts manually. To simplify the process, you can create and then disable *template accounts* that include all of the information needed for typical users. Disabled template accounts cannot be used for logging on, but you can copy the information in them to new user accounts and add individual account information such as user name and password. When you enable new accounts created with a template, all of the account information carries over to the new users with the exception of passwords and permissions.

For more information on copying existing accounts, see the COPY USER entry in the *HP Advanced Server for OpenVMS Commands Reference Manual* or the ADMINISTER commands online help.

Note

Every user account contains a unique identifier that is not copied to new accounts. This unique identifier is used for granting permissions to resources. If you delete a user account and then add it again, the new account will not have the same access permissions to resources as those granted to the original account.

3.4 What Is a Built-In User Account?

A *built-in* user account is a user account automatically provided when an Advanced Server domain is created. When an Advanced Server is installed as a primary domain controller, you have two built-in user accounts:

- Administrator — The account used by the person who manages the overall configuration of the domain.
- Guest — An account provided so that the occasional or one-time user can log on to the system and be granted limited capabilities. By default, this account is disabled.

You can create additional user accounts for other users who log on, and you can modify existing accounts.

The remainder of this section further explains the Administrator and Guest built-in user accounts.

3.4.1 Administrator Account

The built-in Administrator account is a member of the Administrators, Domain Admins, and Domain Users built-in groups, and is granted the rights and permissions of those groups.

The Administrator account is the account used by the person who manages the overall configuration of the domain: the network administrator. The network administrator has more control over the domain and its workstations than does any other user. The network administrator can manage security policy, establish trust relationships, create, modify, or delete user accounts and groups, create and connect to shared directories (including administrative shares), share printers, take ownership of files and other objects, and shut down servers.

The Administrator account is a member of the Domain Admins global group, and the Domain Admins global group is by default a member of the Administrators local group of the domain. Therefore, a user logged on to the Administrator account is able to administer both the local domain and the Windows NT workstation computers in the local domain.

Note

You can rename the built-in Administrator account, but you cannot delete it. Also, you cannot remove it from the built-in Administrators and Domain Admins groups.

During the configuration of the primary domain controller of a new domain, the person doing the configuration is prompted to enter a password for the built-in Administrator account. This password should be guarded not only for security reasons, but also because if the password is forgotten or the person who knows the password is unavailable, the built-in Administrator account becomes unusable.

Following installation, it is strongly recommended that you create an additional administrative account for every person who needs administrative-level abilities and to reserve the built-in Administrator account for emergency purposes. When all administrative users have separate accounts, their actions can be audited.

3.4.1.1 Logging On as System Administrator

Most of the system administrators on your network have dual roles: they are both administrators and users. Although they perform network administration tasks, they also perform tasks as network users.

For this reason, every system administrator should maintain the following two accounts:

- An account in the Administrators group used to perform network tasks
- An account in the Users group used when not performing network management tasks

Your network will be more secure if your system administrator uses these two accounts. While a system administrator is logged on as a regular user, he or she will be unable to change aspects of the network that only system administrators can change. However, using this method will result in some inconvenience for system administrators, because they will have to log off and then log on again before they can administer the network. For more information on these two groups, see Section 4.7.1, Built-In Local Groups.

3.4.2 Guest Account

The built-in Guest account is a member of the Domain Guests built-in group and receives the rights and permissions granted to that group. The Guest account allows the occasional or one-time user to log on to the system with limited capabilities. When a user without an account on a domain attempts to use server resources, access is granted to the user based on the guest access permissions.

When you initially install the Advanced Server, the Guest account is disabled by default. You must explicitly enable the Guest account if you want to provide access to domain resources for users who do not have accounts on the domain.

The Guest account is installed with a blank password. If the password is left blank, users from untrusted domains (without accounts in this domain) can connect to this domain remotely using the Guest account.

Note

You can rename the built-in Guest account, but you cannot delete it.

3.4.2.1 Allowing Guest Access

The Guest account does not have a password and can be used to support network guest logons.

A *network guest logon* occurs when a user tries to access a computer over the network but does not have an account in the computer's domain or in a domain that the computer trusts. Because the account does not exist in the computer's domain, or in any domain that it trusts, the computer does not recognize the user who is trying to access it. In this case, the computer approves the access as a guest logon, as long as the Guest account of the target computer is enabled and has no password.

The guest user then has all of the rights, permissions, and group memberships on the computer that are granted to the Guest account, even though the guest user did not specify Guest as his or her user name.

Note

If you set up your Advanced Server network so that all of the Advanced Server domains in which user accounts are defined are trusted by other domains, network guest logons will rarely occur at servers.

A network guest logon can occur only when a user with no account on the domain or on a trusted domain tries to access the computer, and the guest account is enabled. By default, the guest account is disabled. To enable the guest account, the administrator must modify the guest disuser flag, using the MODIFY USER command. See the *HP Advanced Server for OpenVMS Commands Reference Manual* for information on how to enable the guest account.

3.5 Types of User Accounts

User accounts are divided into two types:

- Global accounts — A normal user account in a user's home domain.
- Local accounts — A user account restricted to the local domain.

3.5.1 How Global Accounts Work

Most of the user accounts that you create will be global user accounts. If there are multiple domains in the network, it is best if each user in the network has only one user account in only one domain, and each user's access to other domains is accomplished through the establishment of domain trust relationships.

3.5.2 How Local Accounts Work

If your network currently has servers other than the Advanced Server or Windows NT Server, such as a LAN Manager server, Novell NetWare, or IBM LAN server, you can use local user accounts (also called *local accounts*) to permit users of these systems to access network resources on Advanced Server systems.

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.

Local accounts can be placed in global and local groups; they can be assigned file permissions and rights. However, local accounts created in one domain cannot be used for resource access in domains that trust that domain; the use of each local account is limited to one domain.

You create and use local accounts in a domain as workarounds to existing restrictions, allowing Advanced Server resources to be accessed by:

- Users from LAN Manager servers in other domains
- Users whose home accounts are in untrusted domains, or domains not running the Advanced Server

3.6 Mapping OpenVMS Users to Advanced Server Users

By default, Advanced Server user accounts are mapped to OpenVMS accounts. If you use the Advanced Server ADMINISTER commands to create a new Advanced Server user account, you have the following options:

- You can map the new Advanced Server account to an existing OpenVMS account.
- Any Advanced Server account that you do not specifically map to an OpenVMS account, and which does not already have a matching OpenVMS account, maps to PWRK$DEFAULT.

The Advanced Server provides server configuration parameters that control user account mapping. You can set the parameters differently on different servers within a domain, depending on the OpenVMS security required on each server.

Host mapping is unique to each Advanced Server. It is not copied as part of user account database replication.

You can map multiple Advanced Server users to a single OpenVMS system user account. However, an Advanced Server user or group cannot map to more than one OpenVMS user account.

Note

Advanced Server groups do not map in any way to OpenVMS system groups.

For more information on how to modify server configuration parameters, see your *Server Administrator's Guide*.

3.7 Password Synchronization

Advanced Server users may have two passwords: one for the Advanced Server account and another for the OpenVMS account. The passwords can be synchronized through the implementation of external authentication on the OpenVMS account.

For more information about Advanced Server passwords and OpenVMS passwords, refer to your *Server Administrator's Guide*.

3.8 Allowing Users of Other Domains to Access the Advanced Server

As you begin adding Advanced Servers to your network, you may have occasions when some user accounts are on Advanced Server domains and other user accounts are on domains of other servers, such as LAN Manager or IBM LAN servers.

If users with accounts on other systems need access to Advanced Server resources during a migration of your systems to the Advanced Server, you can create local accounts for those users in the domains that contain the resources they need to use. You can place the local accounts in local or global groups in the domain and assign necessary permissions to those groups. (Although you can give permissions directly to local accounts, this is not recommended. These permissions are difficult to maintain if you later upgrade the systems to the Advanced Server and no longer require the use of local accounts.)

If you replace other systems with the Advanced Server after having given users on those systems local accounts, you should delete the local accounts and assign appropriate permissions to the users' new Advanced Server accounts.

Local accounts are different from other user accounts in one important way — a local account in one domain cannot be used in domains that trust that domain. Therefore, if you want to use local accounts to grant a user from another network operating system access to several Advanced Server domains, you must create a local account for the user on each of those domains.

3.9 Authenticating Logon Requests for Users

This section explains how the Advanced Server authenticates logon attempts from Windows NT Server and workstation computers; Windows 2000 Server and workstation computers; Windows, Windows 95, and Windows 98 workstations; and MS-DOS and OS/2 workstations.

3.9.1 Authenticating Requests from Windows NT, Windows 2000 and Windows XP Computers

When users log on at a Windows Server or workstation computer, they provide a user name, domain or workstation name, and password. If a user's name and password match an account, the server notifies the workstation to approve the logon. Logon information such as the user's profile, home directory, and environment variables is then used to complete the logon process.

3.9.2 Authenticating Requests from Windows, Windows 95, Windows 98, MS-DOS, and OS/2 Computers

Unlike Windows NT and Windows 2000 computer users, Windows, Windows 95, Windows 98, MS-DOS, and OS/2 workstation users do not require validation when logging on to the network to gain access to their computers' resources.

This means that Windows, MS-DOS, OS/2, Windows 95, and Windows 98 computers are not secure — there is no way to prevent an unauthorized user from sending network requests from one of these computers. However, you can prevent that user from accessing network resources by securing the resources themselves. This will prevent an unauthorized user's network requests from having any effect.

3.9.3 Authenticating Requests from LAN Manager Servers

The Advanced Server system of pass-through authentication depends on the principle that trust relationships allow servers in one domain to recognize user accounts from other domains. Even though LAN Manager servers can participate in Advanced Server domains and can recognize user accounts in their own domains, they will not be able to recognize user accounts from trusted domains; this is a limitation of LAN Manager servers.

For example, suppose that the Sales domain trusts the MIS domain. This allows you to assign permissions on the Advanced Server in Sales to users from MIS. However, you cannot assign permissions for resources on LAN Manager servers in Sales to users from MIS.

To solve this problem, you can create local user accounts in the domain containing the LAN Manager servers. You should create a local account for each user from a trusted domain who needs to access those servers. You create a local user account in the same way you create global user accounts except that as you create the user account, you designate it as a local account.

You then can place the local user account in global groups in your domain and assign those global groups the required permissions on LAN Manager servers. (You must use global groups because LAN Manager servers do not recognize local groups.)

Although you can give permissions directly to local user accounts, this is not recommended. They are difficult to maintain if you upgrade your LAN Manager servers to Advanced Servers and no longer require the use of local user accounts.

If you upgrade all of the servers in your domain to Advanced Servers, you can remove all local user accounts from the domain and create Advanced Server user accounts for those users when it is time to remove the local accounts.

3.10 Auditing User Actions

You can monitor the activities of users by *auditing* their actions and resources on your server. Auditing an action or resource causes an entry to be written to the security event log whenever that activity is performed or a resource is accessed. This helps to ensure that users are accountable for their actions.

Auditing in the Advanced Server is configured on the domain level. Every server in a domain is covered by the domain's audit policy.

You can specify that an audit entry is written to the security event log when certain actions are performed or files are accessed. An audit entry shows the action, the user, and the date and time of the action. Both successful and failed logon attempts can be audited. The audit trail shows who performed which actions on a network, and who tried to perform actions that are not permitted.

Table 3–3 lists the categories of events that you can choose to audit and which events are covered by each category. For each of the categories listed, you can choose whether to audit only successful actions in that category, failed attempts to perform actions in that category, both, or neither.

Table 3–3 Event Audit Categories

Category	Events
Logon and Logoff	Logon attempts, logoff attempts, and the creating and breaking of network connections to servers.
Object Access	Accesses of a directory or a file that is set for auditing in File Manager; uses of a printer managed by the computer.
Privilege Use	Successful uses of user or group rights, and failed attempts to use rights not assigned to users or groups.
Account Management	Creation, deletion, and modification of user and group accounts.
Security Policy Changes	Granting or revoking user rights to users and groups; changing the Audit policy; establishing and breaking trust relationships with other domains.
Restart [1], Shutdown [1], and System	Shutdowns and restarts of the computer, the filling up of the audit log, and the discarding of audit entries if the audit log is already full.
Process Tracking [1]	Starts and stops of processes on the computer.

[1]Applies only to the Windows NT Server.

Using ADMINISTER commands, you specify which types of security events are audited; designate which files are audited and how; set the size of the event log files; and save or clear the event logs when they become full.

Table 3–4 shows the types of directory and file accesses you can audit.

Table 3–4 Auditing Directories and Files

Directory access	File access
Displaying names of files in the directory	Displaying the file's data
Displaying directory attributes	Displaying file attributes
Changing directory attributes	Displaying the file's owner and permissions
Creating subdirectories and files	Changing the file

(continued on next page)

Table 3–4 (Cont.) Auditing Directories and Files

Directory access	File access
Going to the directory's subdirectories	Changing file attributes
Displaying the directory's owner and permissions	Running the file
Deleting the directory	Deleting the file
Changing directory permissions	Changing the file's permissions
Changing directory ownership	Changing the file's ownership

For more information, see your *Server Administrator's Guide*.

4
Groups

By organizing users into domains and setting up trust relationships, you can manage and track the actions of users while allowing them access to the resources they need.

In addition, you can arrange users into groups. Using groups makes it easier and faster to grant multiple users access to resources. You perform only one task to grant rights or permissions to a group; those rights and permissions are then active for all current and future group members.

Another advantage to using groups is evident when a new user joins the network. For example, a new accountant is hired and a group called Accountants has permissions to all of the network resources needed by accountants. Adding the new user to the Accountants group gives the new accountant all of the permissions that are needed.

Note

Advanced Server groups do not map in any way to OpenVMS groups.

This chapter describes the types of groups and identifies some strategies you can use to make your network simpler to administer and easier to maintain.

4.1 What Is a Group?

A group is an account containing other accounts called members. The permissions granted to a group are also granted to its members. Groups are a convenient means of granting common access and user rights to collections of user accounts.

You can use the ADMINISTER commands to create and manage user and group accounts, to grant permissions for files and directories to users and groups, and to give users and groups access to printers.

On Advanced Servers, rights are granted and restricted on the domain level; if a group has a right within a domain, its members have the right on all servers in the domain (but not on Windows NT workstation computers participating in the domain).

4.2 Types of Groups

You can group users who have similar jobs or resource needs into the following types of groups:

- Global group — A group that can be used in its own domain, on servers and workstations of the domain, and in trusting domains. In all of these instances, global groups can be granted rights and permissions and can become members of local groups. However, global groups can contain only user accounts from their own domains. A global group provides a way to create a set of users from inside the domain that can be used both in and out of the domain.
- Local group — A group that can be granted permissions and rights only for the servers of its own domain. However, it can contain user accounts and global groups both from its own domain and from trusted domains. Local groups provide a way to create sets of users from both inside and outside the domain that can be used only on servers of the domain.

Table 4–1 shows the contents of both local and global groups.

Table 4–1 Contents of Local and Global Groups

A global group contains . . .	A local group contains . . .
Name (up to 20 characters)	Name (up to 20 characters)
Description	Description
Members' user names	Members' user names or global group names; names of users and global groups from trusted domains

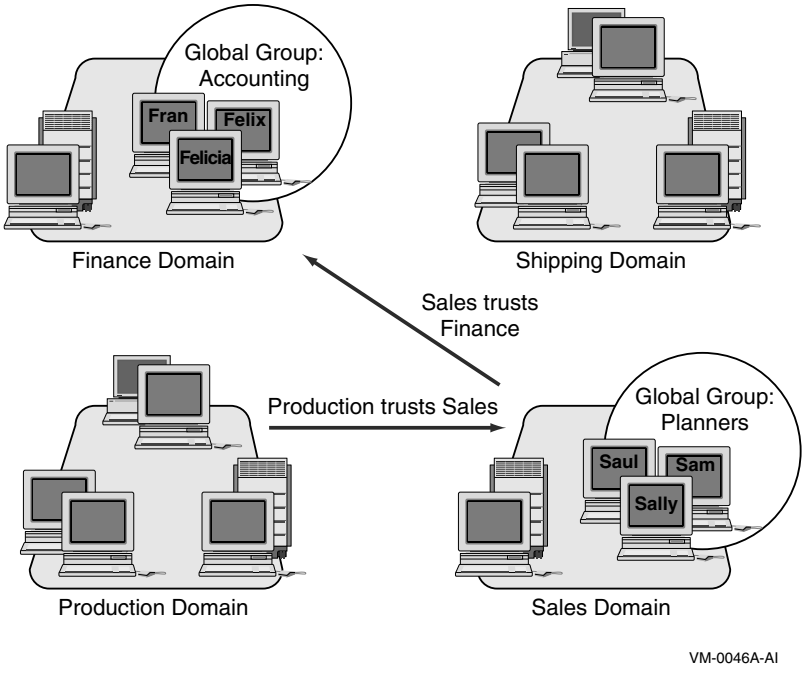
4.3 Global Groups

A global group is a collection of user accounts from one domain that are assembled under a single group name. A global group can contain user accounts from only one domain — the domain in which the global group was created. After a global group is created, it is available globally; that is, it can be granted permissions and rights in its own domain as well as in any domain

that trusts that domain. A global group can contain only user accounts; it cannot contain other global groups or local groups.

Figure 4–1 shows the global group Accounting, which can contain only users from the Finance domain, but which can appear in permissions lists in any domain that trusts Finance. In this example, the Accounting group can be granted permissions in the Sales domain. Likewise, the global group Planners can contain users only from the Sales domain, but the Planners group can appear in permissions lists in the Production domain.

Figure 4–1 Understanding Global Groups



4.4 Local Groups

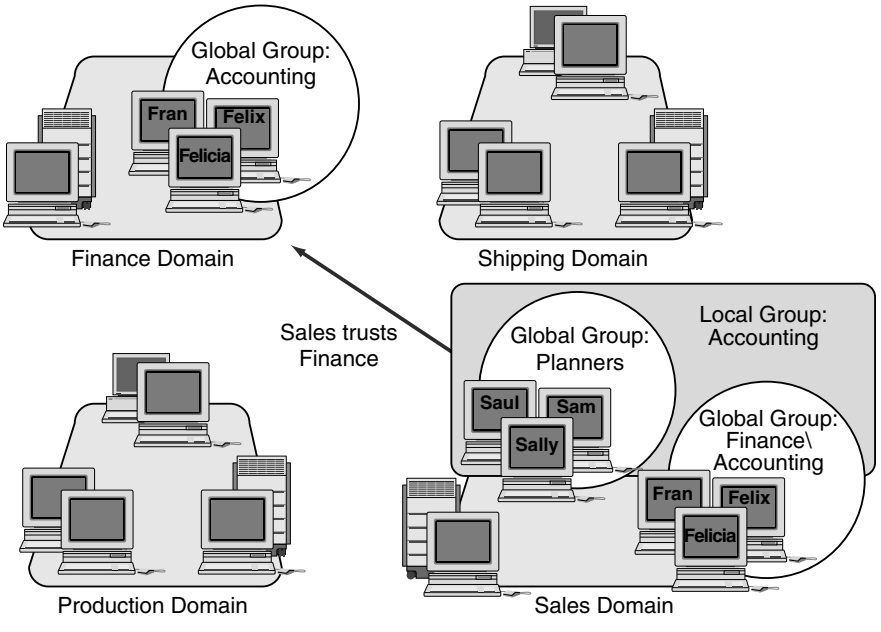
A local group is a collection of users and global groups from one or more domains that have been assembled under a single group name. Although a local group in a domain can contain users and global groups from that domain and any domain trusted by that domain, you can grant rights and permissions to a local group only for resources located in the domain in which the local group is defined.

Local groups also can be used to classify users and give them predefined sets of rights and permissions. For example, to make an account for a print operator in a domain, you would add the account to the Print Operators local group in the domain. The account then would have all the rights and abilities required for a print operator. The use of that group is local to the servers in that domain. A local group can contain users and global groups, but it cannot contain any other local groups.

In Figure 4–2, a local group, Accounting, has been added to the Sales domain. Although Accounting can contain users and global groups from Finance (and any other domains that Sales trusts), Accounting can be assigned permissions and rights only in Sales.

Local groups also exist on Windows NT workstation computers. A local group on a workstation can contain user accounts from the workstation itself, and users and global groups from the workstation's domain and domains trusted by the workstation's domain.

Figure 4–2 Understanding Local Groups



4.5 Differences Between Global and Local Groups

The terms *global group* and *local group* indicate the scope of a group, not the contents of the group; they refer to the rights and permissions that a group can be granted. Local groups can contain global groups, but global groups cannot contain either local groups or other global groups. Although global and local groups serve similar functions, different rules apply to their creation and use.

As shown in Figure 4–2, a global group, Accounting, created in the Finance domain can:

- Contain users from the Finance domain
- Be used in any domain that trusts the Finance domain

A local group created in the Sales domain can:

- Contain users and global groups from the Sales domain and any domain that the Sales domain trusts
- Be used on servers in the Sales domain only

4.6 Using Global and Local Groups

This section discusses strategies for using global and local groups that can make your network easier to administer and maintain.

If you organize your domains so that each represents a division or department of your company, you can think of a global group as being a group of users from the same department. This group of users can be assigned permissions and rights in other domains. In this way, the global group becomes a means of exporting a group of users as a single unit to other domains in the company.

When administering an Advanced Server, you may see that a global group name is preceded by the domain name in which the global group is located. You see both the types of users that the group represents (by the group name) and the origin or location of that group (by the domain name). For example, when you view file permissions on a server in the Sales domain, if the Accounting global group in the Finance domain has permissions, they are shown as Finance\Accounting. In this way, you can positively identify a global group when it is referred to in a domain other than its own. (A global group viewed in its own domain has no domain name prefix. For example, when you view file permissions on a server in the Sales domain, global groups located in the Sales domain, such as Planners in Figure 4–2, are shown by their group names only.)

A local group can include users and global groups from other trusted domains. Therefore, it is a way to import users and global groups from other domains into a single unit for use in the local domain.

For example, suppose that a domain called Engineering has a server with a shared directory containing documents that explain the new technologies that the company is investigating. If managers in other departments (domains) are interested in seeing these documents, network administrators can provide this ability by performing the following procedure:

1. Create global groups in the other domains (such as Marketing\Managers and Sales\Managers).
2. In the Engineering domain, create a local group called All Managers.
3. Put the Marketing\Managers and Sales\Managers global groups in the All Managers local group.
4. Grant All Managers permission to read the files in the directory.

In this example, you could give permission to read the files to all the Managers global groups from the other domains and thus bypass the step of creating the local group. However, in many cases, creating the local group saves time later. For example, imagine that later on you add two new directories containing files of interest to managers. If you have not created the All Managers local group, you need to grant access for the new directories separately to all the Managers global groups, instead of to the single local group. If the All Managers local group contains many global groups rather than just the two in this example, creating it could represent a significant savings of effort.

As this example illustrates, a local group is a way of assembling global groups and assigning them permissions in one step. If another global group needs the same permissions as an existing global group, you can add the new global group to the appropriate local group to give it all the permissions it needs.

Table 4–2 summarizes the uses of global and local groups.

Table 4–2 Purposes of Global and Local Groups

Purpose	Use	Comments
Group users of a domain into a single unit for use in other domains	Global group	The global group can be put into local groups, or given permissions and rights directly, in other domains.
Need permissions and rights only in one domain	Local group	The local group can contain users and global groups from other domains.
Need permissions to access resources on Windows NT workstation computers	Global group	A domain's global groups can be given permissions on Windows NT workstation computers, but a domain's local groups cannot.
Contain other groups	Local group	The local group can contain global groups and individual users; no group of any type can contain other local groups.
Include users from multiple domains	Local group	The local group can contain users and global groups. The local group can be used only in the domain in which it is created.

4.7 Built-In Groups

The actions that a user can perform depend on the group memberships of the user's account. The Advanced Server provides several default groups that have established collections of rights and abilities. *Built-in groups* are Advanced Server default groups that have established rights and abilities. The Advanced Server provides both global and local types of built-in groups:

- Built-in local groups — Groups that contain users from multiple domains. The Advanced Server provides the following types of built-in local groups: Administrators, Users, Guests, Server Operators, Print Operators, Backup Operators, and Account Operators.
- Built-in global groups — Groups that put users of a domain into a single unit for use in both their own and other domains. The Advanced Server provides the following types of built-in global groups: Domain Admins, Domain Users, and Domain Guests.

The built-in groups are explained in the sections that follow.

4.7.1 Built-In Local Groups

When the Advanced Server is installed on any computer, several default built-in local groups are created. Table 4–3 lists the built-in local groups, their initial contents, and who can modify them.

Table 4–3 Built-In Local Groups

Local Group†	Initial Contents	Who Can Modify
Administrators	Domain Admins (global group) Administrator (user account)	Administrators
Server Operators	None	Administrators
Account Operators	None	Administrators
Print Operators	None	Administrators
Backup Operators	None	Administrators
Users	Domain Users (global group)	Administrators, Account Operators
Guests	Domain Guests (global group)	Administrators, Account Operators

†You cannot delete any of these built-in local groups.

In addition to these built-in local groups, an identity called Everyone represents all known people on the network, including administrators, all

types of operators, users, users from other domains, and guests. You cannot change the membership of Everyone; it always contains all users. Everyone is not actually a local group and does not appear when groups are displayed, but you can assign file permissions and rights to Everyone.

Membership in built-in local groups gives a user certain privileges.

Table 4–4 shows the rights and abilities held by each built-in local group on an Advanced Server domain. The built-in global groups of a domain are not shown in this table because built-in global groups receive their rights and abilities indirectly through their memberships in built-in local groups.

Table 4–4 Rights and Abilities of Built-In Local Groups

Right or Ability	Admin-istrators	Server Operators	Account Operators	Print Operators	Backup Operators	Every-one	Users	Guests
Right								
Log on locally[1]	X	X	X	X	X			
Access this computer from network	X					X	X	X
Take ownership of files	X							
Manage auditing and security log	X							
Change system time[1]	X	X						
Shut down system[1]	X	X	X	X	X			
Force shutdown from a remote system[1]	X	X						
Back up files and directories[1]	X	X			X			
Restore files and directories[1]	X	X			X			

[1]Applies only to the Windows NT Server.

(continued on next page)

Table 4–4 (Cont.) Rights and Abilities of Built-In Local Groups

Right or Ability	Admin-istrators	Server Operators	Account Operators	Print Operators	Backup Operators	Every-one	Users	Guests
Ability								
Create and manage user accounts	X		X[2]					
Create and manage global groups	X		X[2]					
Share and stop sharing directories	X	X						
Share and stop sharing printers	X	X		X				

[2]Account Operators cannot modify Administrators' accounts, the Domain Admins global group, or the Administrators, Server Operators, Account Operators, Print Operators, or Backup Operators local groups.

The following sections describe the built-in local groups in the Advanced Server. For information about built-in local groups on a Windows NT Server, see the Microsoft Windows NT Server *Concepts and Planning Guide*.

4.7.1.1 Administrators

The Administrators local group is the most powerful group in the domain. Members of this group have more control over the domain than do any other users. They manage the overall configuration of the domain and the domain's servers. The built-in Administrator user account is a member of the Administrators local group and cannot be removed. By default, the Domain Admins global group is a member of this local group, but it can be removed.

In the Advanced Server, the user right "Access this computer from the Network" cannot be revoked from the Administrators local group.

Unlike administrators in LAN Manager servers, Advanced Server administrators do not automatically have access to every file in the domain. If a file's permissions do not grant access, the administrator cannot access the file. If needed, an administrator can take ownership of a file and thus have access to it. But if the administrator does so, this event is recorded in the security log (if auditing of files is turned on) and the administrator cannot give ownership back to the original owner. For more information about ownership of files and directories, see Chapter 6, Managing Network Shares, in this guide.

4.7.1.2 Server Operators

Members of the built-in Server Operators local group have many of the same abilities as built-in Administrators; however, they cannot manage security on the server. Specifically, Server Operators can share and stop sharing a server's files and printers, and they can start, stop, pause, and continue selected services.

4.7.1.3 Account Operators

Members of the built-in Account Operators local group can manage the server's user and group accounts. An Account Operator can create, delete, and modify most user accounts, global groups, and local groups. However, the Account Operators cannot modify the user accounts of Administrators, nor can they modify the Administrators, Server Operators, Account Operators, Print Operators, or Backup Operators local groups. They also cannot assign user rights.

4.7.1.4 Print Operators

Members of the built-in Print Operators local group can manage shared printers.

If you want a domain's Print Operators to administer printers managed by Windows NT workstation computers in the domain, as well as printers managed by the domain's servers, you must perform the following steps:

1. Create a Domain Print Operators global group in the domain. Make this global group a member of the domain's Print Operators local group.
2. Add the user account of each print operator to the Domain Print Operators group.
3. On each workstation that manages printers, place the Domain Print Operators global group in the workstation's Power Users local group.

4.7.1.5 Backup Operators

Members of the built-in Backup Operators local group have specific rights on any Windows NT Server in the domain, but no specific rights on Advanced Server.

4.7.1.6 Users

Membership in the Users local group provides the abilities most users need to perform normal tasks.

By default, the Domain Users global group is a member of the Users built-in local group, but it can be removed.

4.7.1.7 Guests

Differences between the rights granted to the Guests built-in local group and to the Users local group are minimal; both groups have the right to access the server over the network. For information on the built-in Guest account, see Section 3.4.2, Guest Account.

4.7.1.8 Using the Operators Local Groups

As an example of how to use operators local groups, consider a medium-sized department that is deciding how to assign its technical staff to the various administrator and operator groups.

At least one user must be an administrator. Members of the Administrators group have several unique abilities. These include taking ownership of files and managing auditing. Because of their unique abilities, members of the Administrators group are responsible for planning and maintaining network security for the department. They also can be allowed to administer Windows NT workstation computers.

If there is someone in the group who is responsible for helping new employees get started, it may be wise to make this person a member of the Account Operators group. This account operator then can create domain accounts for new employees and place these accounts in the appropriate groups.

If the domain's Administrators group has only a few members, you should assign at least one additional person to the Server Operators group. The basic function of the Server Operators group is to keep the domain servers running. This goal is reflected in their abilities to share directories and printers on servers. If possible, at least one member of either the Administrators or Server Operators group should be present at all hours during which people are using the network.

If the ability to print documents quickly is important to your group, you should add several people to the Print Operators group to ensure that printer problems can be addressed quickly.

4.7.1.9 Setting Up a Universal Operators Group

If your network has multiple domains, each containing computers with shared printers, and you have a single group of Print Operators who need the ability to administer printers in all domains, use a universal operators group (a combination of global groups and local groups) to set this up. By doing so, you ensure that your Print Operators group is easy to maintain as your network evolves, as print operators come and go, and as new computers or domains are added.

Follow these steps to establish a universal operators group:

1. In each domain where accounts of Print Operators are located, create a global group called Domain PrintOps and make all of the Print Operators in the domain members of this group.
2. In each domain where printers are to be administered, modify the Print Operators local group by adding the Domain PrintOps global groups to it. Be sure to make this change to the Print Operators local group in every domain.

After you complete these steps, every Print Operator has the ability to administer all printers.

If you also need to administer printers on Windows NT workstation computers, you will need to go a step further, because a domain's local groups (such as Print Operators) cannot be used by Windows NT workstation computers — even Windows NT workstation computers participating in that domain. To each Windows NT workstation computer with printers to administer, add all of the Domain PrintOps global groups to the workstation's Power Users local group.

4.7.2 Built-In Global Groups

Three global groups are built in:

- Domain Admins — The Domain Admins built-in group initially contains the Administrator account. When you create accounts for the administrators of your domain, you should add these accounts to the Domain Admins global group, which is already a member of the Administrators local group.
- Domain Users — The Domain Users built-in group initially contains the Administrator account. Administrators and Account Operators can modify these groups. Every user account you subsequently add to this domain is put automatically in the Domain Users global group.
- Domain Guests — The Domain Guests built-in group initially contains the Guest account. Administrators and Account Operators can modify the Domain Guests built-in group.

Table 4–5 lists the types of built-in global groups, their initial contents, and who can modify them.

Table 4–5 Built-In Global Groups

Global Group	Initial Contents	Who Can Modify
Domain Admins	Administrator	Administrators
Domain Users	Administrator	Administrators, Account Operators
Domain Guests	Guest	Administrators, Account Operators

The following sections further explain the built-in global groups and how to use them.

4.7.2.1 Domain Admins

The Domain Admins global group is a member of the Administrators local group for the domain and of the Administrators local group for every Windows NT workstation computer in the domain. The built-in Administrator user account is a member of the Domain Admins global group.

Because of these memberships, a user logged on to the Administrator account can administer the domain, the primary and backup domain controllers, the member servers, and all of the Windows NT workstation computers in the domain. (However, Domain Admins users can be prevented from administering a particular workstation by removing the Domain Admins global group from that workstation's Administrators group.)

To provide administrative abilities to a new account, make the new account a member of the Domain Admins global group. This allows that user to administer the domain, the workstations of the domain, and the trusted domains that have added the Domain Admins global group from this domain to their Administrators local group.

4.7.2.2 Domain Users

By default, all domain user accounts belong to the Domain Users group, including the built-in Administrator account and any new accounts that are created.

The Domain Users global group is by default a member of the Users local group for the domain and of the Users local group for every Windows NT workstation computer in the domain. Domain Users is the default group for each user.

Because of these memberships, users of the domain have normal user access to and abilities in the domain and the Windows NT workstation computers of the domain. (However, domain users can be prevented from being granted this access for a particular workstation by removing the Domain Users global group from that workstation's Users group.)

4.7.2.3 Domain Guests

The Domain Guests global group initially contains the domain's built-in Guest user account. If you add user accounts that are intended to have more limited rights and permissions than typical domain user accounts, you may want to add those accounts to the Domain Guests group and remove them from the Domain Users group.

The Domain Guests global group is a member of the domain's Guests local group.

4.8 Server-Specific Groups

In addition to the built-in groups mentioned, server-specific groups are created by the system and are used for special purposes. You cannot delete these special groups and should not modify them. When you administer a computer and are presented with a list of groups, these server-specific groups sometimes appear in the list. For example, they can appear when assigning permissions to directories, files, shared network directories, or printers.

Table 4–6 lists the server-specific groups provided and the purpose of each.

Table 4–6 Server-Specific Groups

Group	Refers to
EVERYONE	Anyone using the computer. This includes all local and remote users; that is, the INTERACTIVE and NETWORK groups combined. In a domain, members of EVERYONE can access the network, connect to a server's shared network directories, and print to a server's printers.
INTERACTIVE	Anyone using a computer locally.
NETWORK	All users connected over the network to a computer.
SYSTEM	The operating system.

4.9 Using Built-In Global and Local Groups

Use built-in global and local groups the same way you use global and local groups. The Administrators local group and Domain Admins global groups serve as examples.

Membership in an Administrators local group is what makes an account an administrator in an Advanced Server domain. However, when you create an account on an Advanced Server domain, you have two alternate ways of making that account an administrator account: You can place it directly into the Administrators local group, or you can put it in the Domain Admins global group, which is a member of the Administrators local group.

You should always use the second method, putting the account in the Domain Admins global group. In this way, you have a global group that represents all administrators in the domain. This global group can then be put in the Administrators local group of any other domain or Windows NT workstation computer that this domain's administrators need to administer. (When you set up a Windows NT workstation computer to participate in a domain, that domain's Domain Admins global group is added automatically to the workstation's Administrators local group. This allows the domain administrators to manage the workstations in the domain.)

Every domain also has a Domain Users global group. All the user accounts you create in the domain are placed in this group by default; you do not have to remember to add accounts to this group. A Domain Users global group is automatically a member of the Users local group in the same domain and is also a member of the Users local group on all Windows NT workstation computers participating in the domain.

Every domain also has a Domain Guests global group, which is a member of the domain's Guests local group. The Domain Guests global group initially contains the Guest user account.

Domain Admins, Domain Users, and Domain Guests are the only built-in global groups that correspond to built-in local groups. You can create other global groups that correspond to local groups if you want to use the same strategies for the users in the global and local groups.

5

Organizing Your Network into Domains

The way in which you organize the domains on your network is critical. If you set up your domains properly, you can simplify network administration significantly and ensure that users have access to the entire network.

You can manage user security by setting up user accounts, organizing users into groups, and controlling user capabilities. Through user accounts, you can assign user rights and passwords, grant user permissions for network file sharing, and audit users through the security event log. The server's security settings define the rules for changing user account passwords, sharing resources on the server, and handling logons that occur outside specified logon hours.

The Advanced Server accommodates both the Advanced Server user-level security model and the OpenVMS security model. This chapter describes both models and explains security integration considerations. It also includes the following examples that illustrate how Advanced Server network security works within domains:

- Single domain model
- Master domain model
- Multiple master domain model
- Complete trust model

You can use these examples as models as you plan and organize your network. You can follow the examples exactly, modify them, or mix and match them among various parts of your network to create the security configuration you want.

5.1 The Advanced Server Security Model

The Advanced Server employs a user-level security model. User-level security provides precise control over access to shared resources, including disk devices, directories, and printers. Security is based on users and collections of users, or groups. Each user is protected or secured by a password. Advanced Server user-level security takes advantage of the following features:

- User accounts — A user account consists of a user name, a password, and other attributes that define the user. An account determines when a user can log on, what workstations a user can log on from, and what groups an account belongs to (and therefore what the user's privileges are). Users who need infrequent or temporary access to a resource may be allowed to log on through a guest account.
- Groups — To simplify administration of user accounts, you can set up a group (or multiple groups) of users and assign access permissions to resources by group. When you change access permissions for a resource, such as group access permissions for a shared printer, you affect all users belonging to the group. You do not have to apply modifications individually to each of the group's members.

  For more information about global and local groups, see Chapter 4, Groups, in this guide.
- User authentication — Advanced Server uses logon security to allow server or domain access to users with valid accounts.
- Privileges — Privileges determine what range of actions a user can perform on the network. Advanced Server privileges are assigned based on group membership. For example, a user in the Administrators group can perform administrative functions.
- Access permissions — Permissions define the extent to which each user can employ a resource. You can assign access permissions to shares, directories, and files. You can tailor access to resources by assigning a set of permissions for each user or for groups of users. You can also use OpenVMS security features to further protect resources. (For more information on OpenVMS security features, see Section 5.2, OpenVMS Security, in this guide.) The interaction of these two security models is described in the Security Integration Considerations section in this guide.

You can use the ADMINISTER commands to define the Advanced Server security settings. Security settings made on a domain's primary domain controller are copied to the domain's backup domain controllers, just as user accounts and groups are.

The Advanced Server security settings are shown in Table 5–1.

Table 5–1 Advanced Server Security Settings

Security Setting	Description	Values
Minimum password length	Specifies the minimum number of characters for a password.	The default value is 6. The range of values is from 1 to 14 characters.
Password uniqueness	Prevents a user from reusing old passwords. The value you enter specifies the number of previously used passwords that are forbidden. For example, if you set a value of 3, users are prevented from reusing any of their last three passwords.	The default value is 0. The range of values is from 1 to 8 passwords.
Minimum password age	Specifies the minimum number of days that must elapse between password changes by a user. This restriction does not apply to administrators, who can change the password of a user at any time. Users must log on to change their passwords.	The default is 1. The range of values is from 1 to 999 days.
Maximum password age	Specifies the maximum number of days that a user is allowed to use the same password without changing it.	The default is 90 days. The range of values is from 1 to 999 days or never.
Force disconnect	Determines what happens if users have a connection to a server when their logon hours or accounts expire. You can specify that the server will terminate the session immediately or never.	The default is never. The values are immediately or never.
Lockout accounts	Specifies the number of failed logon attempts users are allowed before their accounts are disabled. A failed logon attempt occurs when the user supplies an incorrect password when logging on.	The default is never. The range of values is from 1 to 999 invalid attempts or never.

In a domain or network with only one server, you do not need to set up a domain-wide security accounts database for use by different servers. You maintain security in a single-server domain by setting up the server as the primary domain controller, taking advantage of the full range of Advanced Server features and preparing the server for possible future expansion of the network.

5.2 OpenVMS Security

The Advanced Server provides support for security features of the OpenVMS operating system. The degree to which these features are integrated with Advanced Server security varies, as discussed in Section 5.5, Security Integration Considerations, in this guide.

An OpenVMS account identifies a user to the OpenVMS operating system. An account includes the user's name, a password, privileges, and access to directories and files associated with the account. (See Chapter 3, User Accounts, for more information.)

The OpenVMS operating system provides the following methods of assigning protection to files and directories:

- RMS protection
- Access control lists (ACLs)

5.2.1 RMS Protections

The *Record Management Service (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 user by the system administrator. For example, UIC [320, 450] represents user number 450 in group 320. A UIC determines which of the following categories a user belongs to:

- System (S) includes users with system privileges (the OpenVMS privilege SYSPRV) or users with designated low group numbers in their UICs as specified by the system manager.
- Owner (O) includes only the owner of a file or directory. The user code of the UIC associated with the file or directory matches the user code of a user's UIC.
- Group (G) includes all users who have the same group code in their UICs.
- World (W) includes all users regardless of UIC.

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

- R for read access
- W for write access
- E for execute access
- D for delete access

The default protection is:

(System:RWED, Owner:RWED, Group:, World:)

This default RMS protection allows read, write, execute, and delete access to the system administrator and to the owner of the file; group and world UICs have no access to the file.

5.2.2 Access Control Lists

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 access. In contrast, with ACLs, you can provide users from several UIC groups 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 protection and ACLs, OpenVMS checks ACEs in the ACLs before it checks the RMS protection.

For more information about RMS protection and ACLs, see the OpenVMS documentation set.

5.3 Additional Resource Protection

You can take advantage of several other methods of protecting servers and network resources, as follows:

- Use logon security — In a domain where at least one server is running user-level security, the Advanced Server can validate user requests to log on to the network and access network resources through the logon security features implemented through the Netlogon service.

  Logon security authenticates users through the following controls:

  – Maintains a domain-wide security accounts database. You can create and, when necessary, make changes to the database for the entire domain from a single server.

  - Uses *logon validation* to control network access through individual user passwords.

- Use hidden servers — *Hidden servers* are servers you hide to protect them from unauthorized use. When users view the list of servers in the domain, hidden servers do not appear in the list. Users can still access a hidden server and its resources if they know the server's name, but they cannot use the Advanced Server to find out that the server exists. By default, a server is not hidden.

  You can hide a server by setting the SrvHidden server configuration parameter.

- Enable account lockout — You can enable *account lockout* after a specified number of failed logon attempts occurs. This protects your network from unauthorized users who attempt to break into the network by using password generation schemes. Once an account is locked out, it is disabled until an administrator reenables it. Lockout information is copied to all the servers in a domain.

- Use Advanced Server external authentication — This optional feature lets Advanced Server users log in to the OpenVMS operating system with the Advanced Server domain user name and password. With external authentication, you can avoid creating and maintaining dual accounts and passwords for users who need to use both OpenVMS and PCs. For more information on enabling external authentication, see your *Server Installation and Configuration Guide*.

5.4 Advanced Server Security

This section describes how the Advanced Server validates a file access request. Whether the Advanced Server grants or denies access depends on two factors:

- The security model in effect on the server
- How a user's Advanced Server account is mapped to an OpenVMS account

All Advanced Server systems implement user-level security. With user-level security, all Advanced Server users have an Advanced Server user account. File access by each account is determined by the Advanced Server permissions set on the file. Furthermore, each Advanced Server account is also mapped to an OpenVMS account. This mapping integrates Advanced Server security with OpenVMS file access security.

Using the Configuration Manager tool, you can specify the level of integration by setting a server configuration parameter that specifies one of the two Advanced Server security models: Advanced Server security only, or Advanced Server and OpenVMS security.

5.4.1 Advanced Server Security Only Model

Advanced Server security only is the default security model for all installations. Therefore, unless you change the defaults, installing Advanced Server software establishes Advanced Server security only, where Advanced Server security is enforced and OpenVMS access checks are bypassed.

The Advanced Server security only model is suitable for environments where the security features provided by the Advanced Server are sufficient, such as on a dedicated server or on a server with no interactive OpenVMS users who are also network users.

5.4.2 Advanced Server and OpenVMS Security Model

In addition to the default security model, Advanced Server security only, you can choose to use the combined Advanced Server and OpenVMS security model, in which both forms of security are enforced. If a user's access request passes the Advanced Server security check, the Advanced Server checks the OpenVMS security in effect (determined by the OpenVMS account to which the Advanced Server account maps) for the user's request. Access is granted if a user passes both security checks. For information on how Advanced Server accounts map to OpenVMS accounts, see Section 3.6, Mapping OpenVMS Users to Advanced Server Users, of this guide.

5.5 Security Integration Considerations

The level of Advanced Server and OpenVMS security integration that you select can affect how resources are shared among Advanced Server users. If you select the Advanced Server and OpenVMS security model, a resource created by one Advanced Server user may not necessarily be accessible to other Advanced Server users. For example, if Advanced Server security checks allow access, but the user's Advanced Server account maps to an OpenVMS account that is not granted access, the OpenVMS security check will fail and resource access will be denied.

The Advanced Server and OpenVMS security model provides the greatest level of security. However, use of the Advanced Server and OpenVMS security model results in the extra overhead of validating both the Advanced Server and OpenVMS settings. If you do not need this level of file access checking, you can use the Advanced Server security only model, in which OpenVMS file access checks are bypassed completely.

If you want the extra security provided by the Advanced Server and OpenVMS security model, ensure that the accounts of the Advanced Server users map to OpenVMS accounts that provide the access privileges that users require.

The remainder of this chapter describes examples you can use as models to set up network security within domains.

5.6 Single Domain Model

If your network does not have many users and does not need to be segmented for organizational reasons, you can use the simplest domain model, the single domain model. When you use the single domain model, trust relationships are not needed because there is only one domain on the network.

Because permission to administer servers is established at the domain level, having a single domain lets network administrators administer all of the network servers.

Table 5–2 summarizes the advantages and disadvantages of using a single domain model.

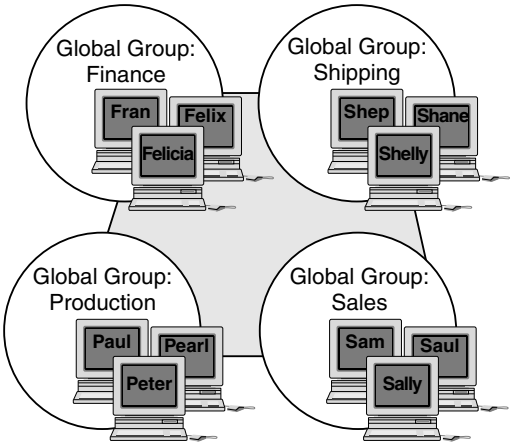
Table 5–2 Advantages and Disadvantages of the Single Domain Model

Advantages	Disadvantages
Best model for companies with few users and resources.	Poor performance results if the domain has many users and groups.
Centralized management of user accounts.	No grouping of users by department into separate domains.
No management of trust relationships necessary.	No grouping of resources by function into separate domains.
Local groups need to be defined only once.	Browsing is slow if the domain has many servers.

5.6.1 Single Domain Model: Example of Domain Configuration

In the single domain model shown in Figure 5–1, the network has only one domain and you create all the users and global groups in the domain.

Figure 5–1 Single Domain Model



A network can use the single domain model if it has a small enough number of users and groups to ensure good performance. The exact number of users and groups depends on the number of servers in the domain and the server hardware.

If your network has many servers sharing resources or your organization has many departments, the single domain model may not be the best. With multiple domains, a user browsing the network first browses among domains, then chooses a domain and views the resources it contains. If your network has many shared resources, segmenting it into domains may make browsing easier. Performance degrades when users browse a single domain with many servers.

5.6.2 Single Domain Model: Example of Network Security Configuration

A small college with a central MIS department contains one Windows NT Server and several Advanced Server computers that are used by departmental offices.

All user accounts and groups belong to the same domain, so access to resources is limited by permissions, and capabilities are restricted by group.

From any Advanced Server, local or remote, or from the Windows NT Server, the MIS department can monitor and manage the domain, the other servers, and the network resources (directories, files, printers, and so on) available throughout the domain. To make this possible, the MIS

department has at least one user in each department's global group that is a member of the Administrator's local group. The MIS users are included in the Domain Admins group to perform domain-wide procedures such as software upgrades, backing up the servers, and providing troubleshooting assistance to departmental users.

Departments can manage the Windows NT Server from their Advanced Server systems, as well as manage, share, and monitor access to resources on their departmental computers. This simplifies user account and local resource management because they are handled at departmental levels. Departmental administrators can add new user accounts and include new users in local groups specific to the department or to types of users. MIS users define new groups across the domain or include users in built-in groups. For these tasks, departmental and MIS users can use the Advanced Server ADMINISTER commands, which provide the ability to display, modify, and delete user accounts and groups. They can also use Windows NT Server administration tools.

5.7 Master Domain Model

The master domain model is a good choice for organizations in which the network needs to be arranged into domains for departmental reasons, but the number of users and groups is small. This model offers both centralized administration and the organizational benefits of multiple domains.

With this model, there is one domain — the master domain — in which all the users and global groups are created. All other domains on the network trust this domain and, therefore, can utilize its users and global groups. If your organization has a department that manages your LAN, it would be appropriate to have this department administer the master domain.

View the master domain as an account domain; its main purpose is to manage the network's user accounts. The other domains on the network are resource domains; they do not store or manage user accounts but provide resources such as shared files and printers to the network.

With the master domain model, only the primary and backup domain controllers in the master domain have copies of the network's user accounts. Be sure to have at least one backup domain controller in a master domain. In the event that the primary domain controller fails, the backup domain controller can take over and the network keeps running.

Table 5–3 summarizes the advantages and disadvantages of using a master domain model.

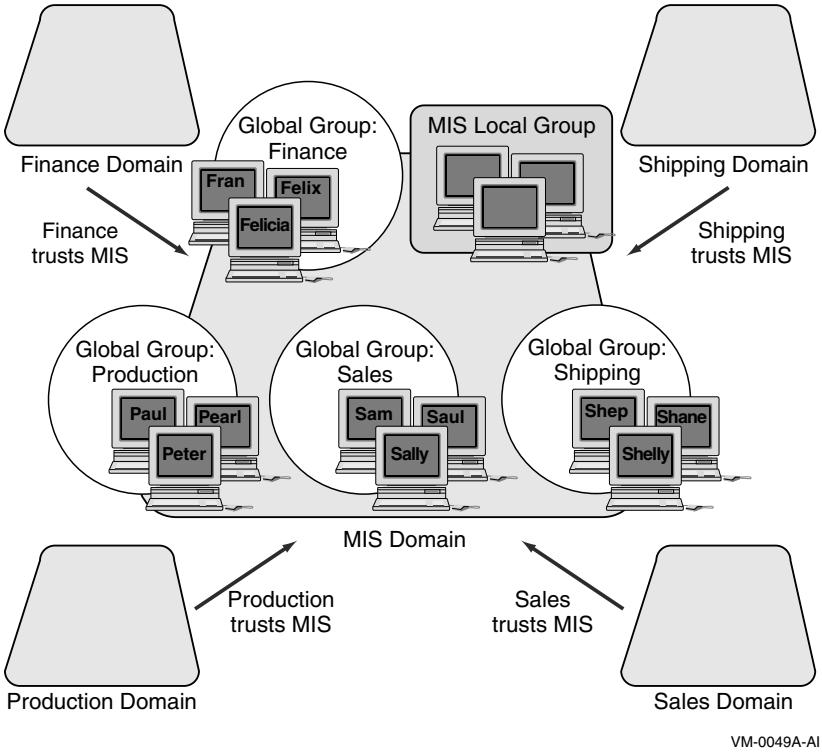
Table 5–3 Advantages and Disadvantages of the Master Domain Model

Advantages	Disadvantages
Best choice for companies that have few users and must share resources among groups.	Poor performance results if the domain has many users and groups.
User accounts can be managed centrally.	Local groups must be defined in every domain in which they will be used.
Resources are grouped logically.	
Department domains can have their own administrators, who manage the resources in the department.	
Global groups need to be defined only once (in the master domain).	

5.7.1 Master Domain Model: Example of Domain Configuration

Figure 5–2 shows an example of a company that is divided into several distinct departments and that uses the master domain model. All accounts are created in an MIS master domain, and there is a separate domain for each department. Within the master domain is a global group for each department that includes all user accounts for that department. Every departmental domain trusts the master domain and can make use of its global groups. The MIS domain serves as the account management domain, and a local group of MIS administrators has privileges limited to the MIS domain.

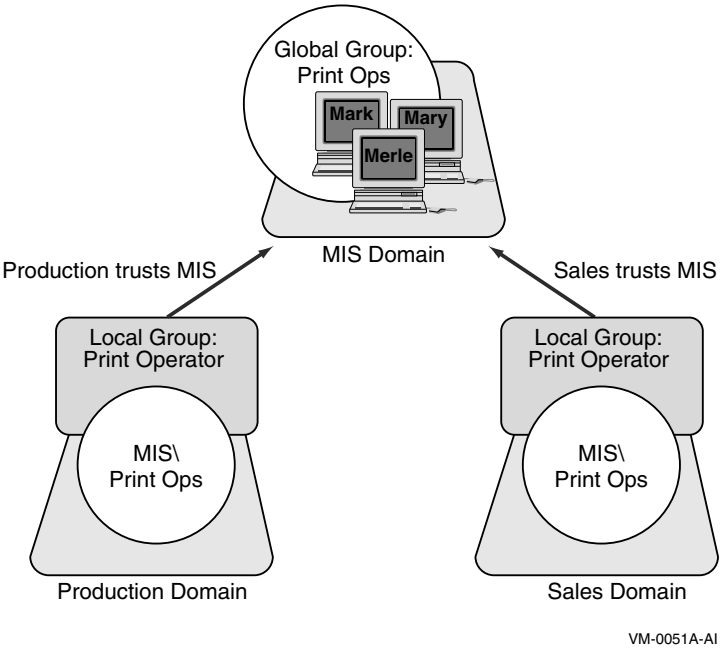
Figure 5–2 Master Domain Model



5.7.2 Master Domain Model: Example with MIS Master Domain

Figure 5–3 presents a setup using the master domain model with MIS as the master domain. Because MIS is the only master domain, all user accounts are located there, and all other domains trust the MIS domain.

Figure 5–3 Master Domain Model with MIS as the Master Domain



In this example, if you want to create a universal print operators group that can be used in every domain, you create a PrintOps global group in the MIS domain and then put MIS\PrintOps into a Print Operator local group in the Production and Sales domains. You then add the user accounts of each print operator to the PrintOps global group to manage all print operators as an entity.

5.7.3 Master Domain Model: Example of Network Security Configuration

A company of 3000 users, organized into 15 departments and a centralized MIS group, is setting up an Advanced Server network. The company selects the master domain model as its network security configuration.

The MIS group creates a domain named MIS to serve as the master domain. This domain has three servers running Advanced Server software; this ensures that the network is failover tolerant if one of the servers must go down for servicing.

All user accounts are created in the MIS domain. The MIS group also creates 15 global groups in the MIS domain. The name of each global group corresponds to one of the 15 departments in the company, and the members of each global group are the employees who work in that department. Initially, each employee is a member of only one of these global groups. No directories or printers are shared in the MIS domain; this domain serves only as an "account-management domain."

Each of the 15 departments has its own Advanced Server domain. Most of these department domains contain only one server running Advanced Server software. Directories and printers on the network are shared by the department domains. Every department domain trusts the MIS domain, but the department domains do not need to trust one another.

The Administrators local group of each department domain contains the user account of at least one user working in that department. This administrator can share resources, create local groups in the domain, and perform other necessary tasks. The MIS\Domain Admins group also is a member of the Administrators local group on every domain. This means that the MIS group can perform software upgrades, back up network servers, and help the departmental administrators with problems.

When a new group of users is needed for use only within a domain, the local department administrator can create a local group in the domain. For example, the administrator of the Sales domain can create a new local group in the Sales domain, containing the user accounts MIS\CristalW, MIS\BillO, and MIS\PegE. In this example, CristalW, BillO, and PegE work in the Sales domain, but their accounts, like those of all other company employees, are located centrally in the MIS domain.

Suppose that a new group of users is needed and this group needs permissions in more than one domain. In this case, a local department administrator could send a message to the MIS group, who could create a global group in the MIS domain with the appropriate members. For example, if the MIS group creates a global group named Budget Planners in the MIS domain, a department manager could grant permission to MIS\Budget Planners for the resources that this group needs.

A different option for this company would be to have departmental managers act as Server Operators in their own domains only; they would not be members of the Administrators group. The departmental managers would still share resources, but only the MIS group would create local groups and perform other administrative tasks.

5.8 Multiple Master Domain Model

For larger companies that want centralized administration, the multiple master domain model is a good choice because it is the most scaleable.

With this model, a small number of master domains serve as account domains, and every network user account is created on one of these master domains.

Table 5–4 summarizes the advantages and disadvantages of using a multiple master domain model.

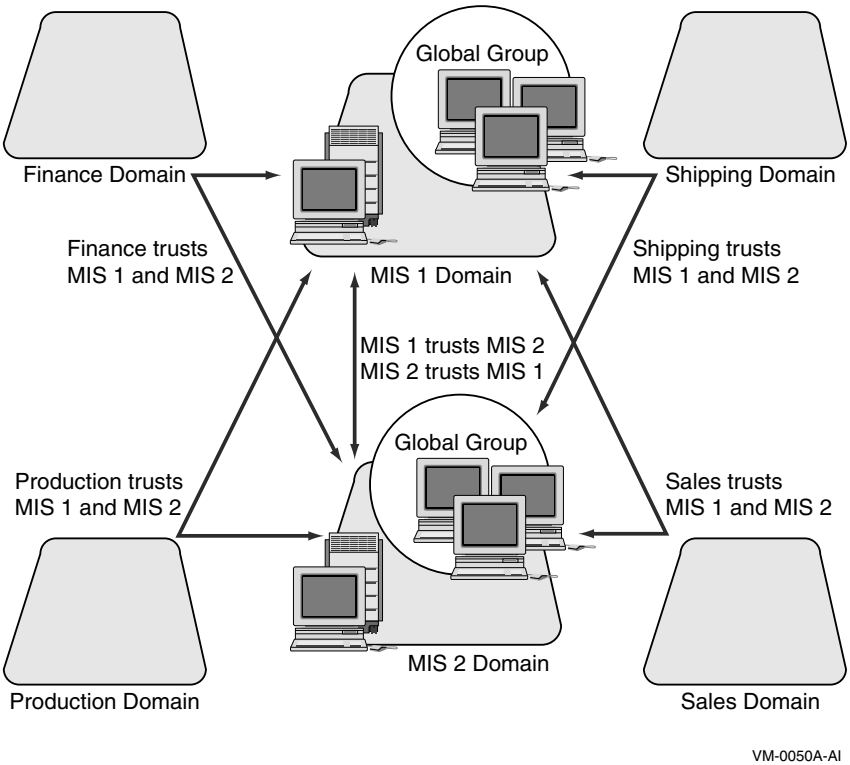
Table 5–4 Advantages and Disadvantages of the Multiple Master Domain Model

Advantages	Disadvantages
Best choice for companies with many users and a centralized MIS department.	Local and global groups may need to be defined multiple times.
Scaleable to networks with any number of users.	There are more trust relationships to manage.
Resources are grouped logically.	User accounts are located in more than one domain.
Department domains can have their own administrators, who manage the resources in the department.	

5.8.1 Multiple Master Domain Model: Example of Domain Configuration

Figure 5–4 shows an implementation of the multiple master domain model. The company's MIS group monitors the master domains. In addition to the master domains, many other domains, such as departmental domains, provide resources. The departmental domains can be managed by people in their own departments or by a centralized MIS department.

Figure 5–4 Multiple Master Domain Model



Every master domain trusts the other master domains. All domains in the company trust all master domains; therefore, every user account potentially can access every domain. The departmental domains, however, do not necessarily trust one another.

Note that the management of global groups is slightly more complicated in this model. If a global group needs to contain users from two or more master domains, you must:

1. Create global groups in each master domain.
2. Add the global groups to a local group in each domain to which users need access.

To minimize this inconvenience, distribute users among your master domains by department within your company rather than alphabetically or otherwise. In this way, the chance that you will need similar global groups from different master domains is reduced. Your company's central MIS department can manage the master domains.

5.8.2 Multiple Master Domain Model: Example of Network Security Configuration

A growing company of several thousand users organized into multiple departments and a centralized MIS department is setting up its Advanced Server network. Because of the high number of users, the company selects the multiple master domain model to ensure that performance in the master domains does not degrade.

The company creates two master domains, MIS1 and MIS2 — each with multiple servers running Advanced Server software. A high number of servers in each domain provides greater performance in approving logon requests. This is needed because many employees will be logging on at about the same time every morning.

Each user account is created in one of the MIS domains. A user's job determines which master domain contains the user's account.

Each department has its own domain with its own administrator who creates local groups, manages the sharing of the department resources, and keeps the department's servers running smoothly.

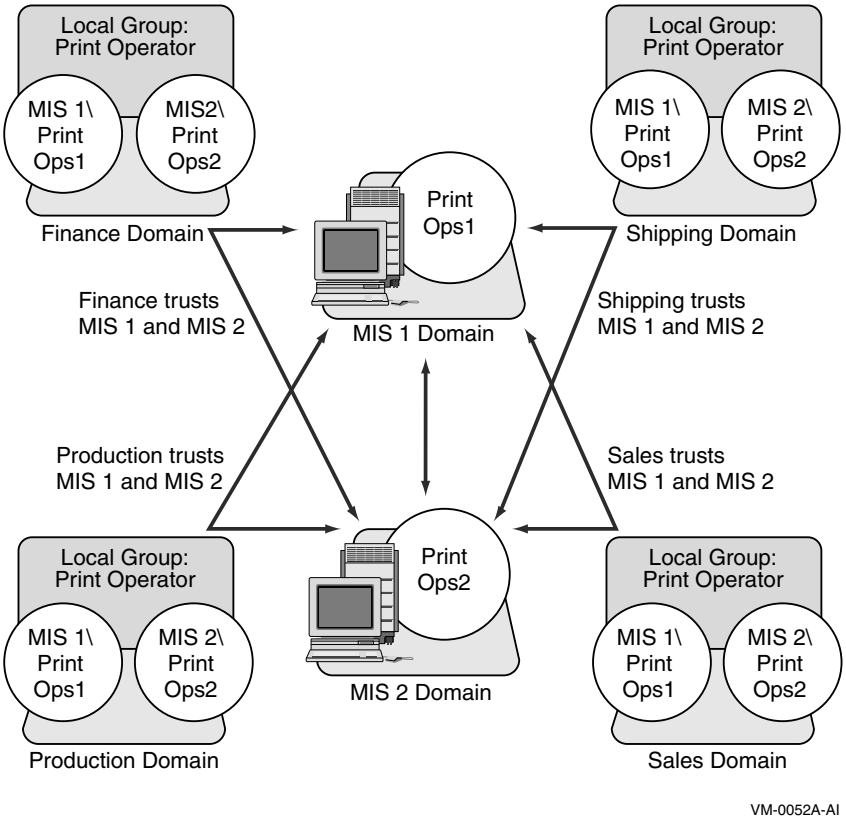
The two master domains trust one another and every department's domain trusts both of the master domains. Department domains do not need to trust one another.

If a new global group of users is needed, it must be created by the MIS department. If the global group needs to contain users from both of the network's master domains, the MIS department needs to create two global groups (one in each master domain) containing the users whose accounts are in that domain.

For example, a group containing users from both MIS1 and MIS2 may be needed to operate printers in the departments. In this situation, create PrintOps global groups in both MIS1 and MIS2 and put both MIS1\PrintOps1 and MIS2\PrintOps2 in a Print Operator local group in every domain.

Figure 5–5 illustrates this example of a multiple master domain model.

Figure 5–5 Multiple Master Domain Model with MIS1 and MIS2 as the Master Domains



Maintenance of this model is simple: If a print operator leaves the company or a new one joins, you simply remove the user's account from, or add it to, the Domain PrintOps global group in the domain where the user's account is, or should be, located. If new printers needing administration are added to an existing domain, all your print operators will be able to manage them automatically.

If you need to add a workstation with a printer to administer, add all the Domain PrintOps global groups to the workstation's Power Users local group. And if a new domain is added to your network, add all the Domain PrintOps global groups to the Print Operator local group in that domain.

5.9 Complete Trust Model

The complete trust model is ideal if you want the management of users and domains to be distributed among different departments rather than to be centralized.

With the complete trust model, every domain on the network trusts every other domain. In this way, every department can manage its own domain and define its own users and global groups, and these users and global groups can be used on all of the domains in the network.

Table 5–5 summarizes the advantages and disadvantages of using a complete trust model.

Table 5–5 Advantages and Disadvantages of the Complete Trust Model

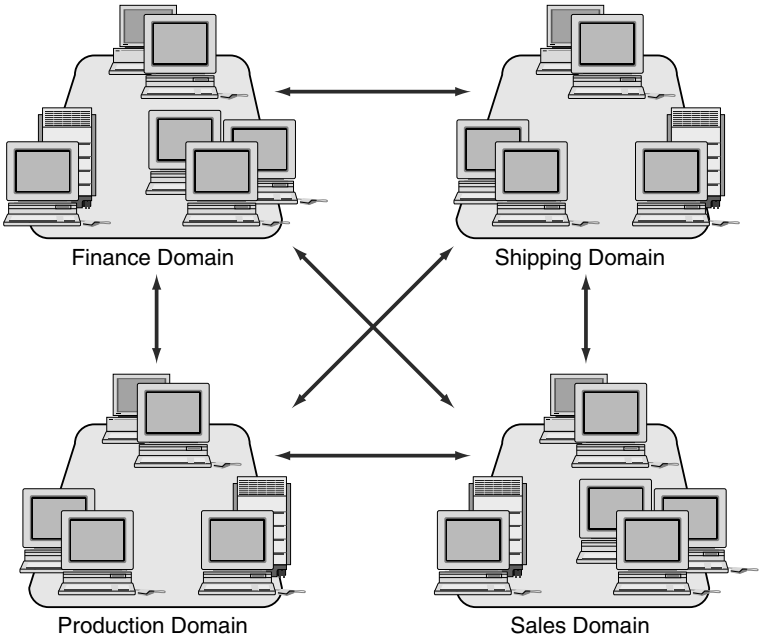
Advantages	Disadvantages
Best for companies with no central MIS group.	Does not provide for central management of users.
Scaleable to networks with any number of users.	Large number of trust relationships to manage.
Each department has full control over its user accounts and resources.	Each department must be confident that other departments will not add unauthorized users to global groups.
Both resources and user accounts are grouped into departmental units.	Difficult to add domains.

5.9.1 Complete Trust Model: Example of Domain Configuration

Figure 5–6 shows the trust relationships for a complete trust model. Because of the number of trust relationships required for this model, it is difficult to add domains. With the complete trust model, the number of trust relationships required for a company with *n* domains is *n*(n-1)*. For example, 10 domains require 90 trust relationships, and 20 domains require 380 trust relationships. Adding a new domain to an existing network of 10 domains requires establishing 20 new trust relationships.

However, this model may be the most suitable for companies that do not have centralized MIS departments. (See Chapter 2, Domains and Trusts, in this guide.)

Figure 5–6 Complete Trust Model



With the complete trust model, the term “trust” applies totally. Before you create a trust relationship with another domain, be sure that you have confidence in the administrator of that domain, especially if you will be giving permissions to global groups from that domain. After you give permission to a global group from another domain (or place that global group in a local group in your domain), you are trusting the administrator of the other domain not to add unauthorized users to that global group.

5.9.2 Complete Trust Model: Example of Network Security Configuration

A company of 1000 users with no centralized MIS group is setting up its Advanced Server network. Because there is no centralized computer management, each department needs to administer its own server. This makes the complete trust model the best choice.

Every department sets up its own domain and has its own domain administrator who is entirely responsible for both user accounts and shared resources in the domain. Each domain administrator creates user accounts for all employees who work in the department corresponding to that domain.

Each department administrator is also responsible for creating global groups and local groups in the domain. When the department administrator creates a group containing only users from that department's domain, he or she can create a global group. When a group containing users from other domains is needed, a local group is necessary.

Each department administrator can establish two-way trust relationships with other Advanced Server domains. Then users and global groups from one domain can be given rights and permissions or can be placed in local groups in the other domains.

In this case, department administrators must ensure that only authorized users are added to global groups. For example, if the Shipping department trusts the Sales department, the Shipping administrator can give permissions to the Accountants global group from the Sales domain. If the Sales administrator subsequently adds more users to the Accountants global group, these new users will have the permissions granted to Accountants in the Shipping domain. Therefore, the Shipping administrator must be careful to grant permissions only to appropriate global groups from domains with trusted administrators, and the Sales administrator has the responsibility to add only appropriate users to global groups.

6
Managing Network Shares

One of the most important functions of network servers is to share files and directories with network users. When a directory is shared, users can make connections to the directory from their workstations and access the files in the directory. The shared directory also serves as storage that is available to the network user.

The Advanced Server provides excellent performance, reliability, and security for file sharing. You can set file permissions on files and directories to grant access only to authorized users. With the Advanced Server, you can specify which groups and users can access each file and directory and the level of access that each group or user is permitted.

In addition, the Advanced Server provides audit capabilities for monitoring the access of files and directories on the server. When the Advanced Server audits a file or directory, an entry is written to the server security log when a user accesses the file. You can define the types of access for each file or directory that will cause audit entries to be written.

This chapter explains how the OpenVMS system supports the concept of file and directory ownership. The Advanced Server lets network clients view and change the ownership of files and directories, and it integrates standard OpenVMS system file and directory ownership into the enterprise-wide, network security model. This chapter also explains some features and concepts regarding file storage and file name conventions that help ensure greater compatibility with clients and legacy applications.

6.1 Sharing Files with Network Users

When a directory is shared on a server, a user potentially can gain access to that directory and to all of its subdirectories and files. Every point on the directory tree that is under the shared directory can be made available to network users.

You can block access to some of the directories in a shared directory tree and allow access to others by setting permissions on them.

When you share a directory, you assign it a *share name*. Network users use a share name to refer to the shared directory. Windows users see the share name when using File Manager or Windows Explorer to browse the network.

A share name can be (but is not required to be) the same as the actual directory name. A shared directory often is referred to simply as a *share*.

You can share multiple directories on the same directory tree. In this case, one shared directory might be accessible to users in different ways — as a directory that actually is shared and as a subdirectory of another shared directory.

6.1.1 Autoshares

The Advanced Server supports access to disk devices by offering disk devices as *shares* at server startup time. These special shares are referred to as *autoshares* (automatic shares) and are accessible only to users with Administrator rights.

Autoshares are hidden. They are visible only to members of the Administrators group, and only members of this group can connect to them. When connected to an autoshare, you are located at the top-level (root) directory of the device and have access to any subdirectory or file in the directory tree.

For more information on creating autoshares, see your *Server Administrator's Guide*.

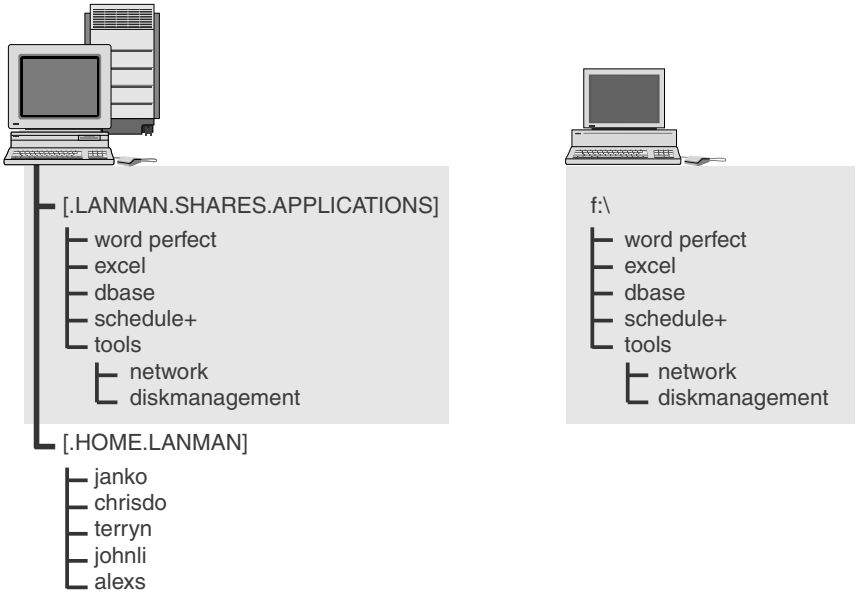
6.1.2 Connecting to Shared Resources

Network users generally make connections to shared directories by assigning a drive letter on their workstation to the shared directory. Then they use the assigned drive letter to refer to the directory to which they have made the connection.

For example, if a user makes a connection to the APPLICATIONS directory and assigns the drive letter F: to the directory, the user sees the contents of the APPLICATIONS directory on the server as the contents of his or her own F: drive. The subdirectory TOOLS appears as F:\TOOLS to the user.

In Figure 6–1, a workstation user assigns the drive letter F: to a directory when making a connection to it. Then, to the user, the contents of the shared directory are the contents of the user's drive letter.

Figure 6–1 Connecting to Shared Resources



After a Windows user has made a connection to a directory, the drive letter assigned to that directory and an icon appear in the Folders pane of Windows Explorer on Windows 95, Windows 98, Windows 2000, and Windows NT systems or in the drive bar of the File Manager window.

MS-DOS and OS/2 users with LAN Manager networking software (but without Windows) can use the NET USE command to make network connections. OS/2 users can use File Manager to view the connected drive. OS/2 users can use the NET USE command at the DOS prompt.

MS-DOS users (both with and without Windows 3.1 or Windows for Workgroups) have restrictions on how they access and view shared directories. These restrictions are described in Section 6.1.3, Considerations for MS-DOS Users .

6.1.3 Considerations for MS-DOS Users

In general, share names can include up to 12 characters. When assigning share names to shared directories, determine whether the directory will be accessed by users of MS-DOS, Windows 3.1, or Windows for Workgroups. If so, assign a share name that follows the MS-DOS 8.3 naming convention, where the share name can have up to eight characters, optionally followed by a period and up to three additional characters. MS-DOS users cannot access shares with share names that do not follow this convention. If a share will be accessed only by Windows NT, Windows 95, Windows 98, or Windows 2000 users, the share name can be up to 12 characters long.

6.2 Using Permissions

You set permissions on shared directories to ensure that only authorized users can access each file or directory and that those users can access them only in appropriate ways. The Advanced Server lets you set permissions differently for each file and directory.

Note

Security for access from network clients can work in conjunction with OpenVMS system protections. For information about how to set file and directory permissions, see your *Server Administrator's Guide*.

6.3 File Ownership

Both Advanced Server and OpenVMS support the concepts of file and directory ownership. Every file and directory has an *owner*. The owner controls how permissions are set on the file or directory and can grant permissions to others. File ownership provides a way for users to keep files on the server private.

Administrators create most of the files on network servers, often when they install applications on the server. Therefore, most files on a server will be owned by administrators, except for data files created by users and files in users' home directories.

When an Advanced Server user creates a file or directory, that user automatically becomes the owner of the file or directory. The Advanced Server sets the OpenVMS system owner of a file or directory created by an Advanced Server user to the OpenVMS system identity that has been mapped for that user's Advanced Server account.

For more information about how to set up user host mapping, see your *Server Administrator's Guide*.

Ownership can be transferred in the following two ways:

- The current owner can grant the Take Ownership permission to other users, in which case those users can take ownership at any time.
- An administrator can take ownership of any file on the computer. This is useful, for example, if an employee leaves the company suddenly and the administrator needs to take control of the employee's files.

Although an administrator can take ownership, the administrator cannot then transfer ownership to others. This prevents an administrator who wrongly takes ownership of a user's files from transferring ownership back to the original owner. When the original owner discovers that he or she is no longer the owner of the files, he or she can check the current ownership of the files and discover who took ownership of them.

6.4 Auditing Directories and Files

By auditing files and directories on a server, you can track their use and identify any attempted security violations. You can identify who took various types of actions with files and directories and hold those users accountable for their actions.

When a file or directory is audited, audit events are generated and written to the Advanced Server security log for all failed and successful attempts to perform the activities you want to audit.

Through the audit policy you set up, you can enable auditing on the server or domain for the types of directory and file access listed in Table 6–1. The audit policy applies domain-wide. If you set the audit policy on a backup domain controller, the change is actually made on the primary domain controller and is then replicated to all the backup domain controllers in the domain. A member server maintains its own audit policy.

Table 6–1 Audit Events for Directory and File Activities

Types of Directory Access	Types of File Access
Displaying contents of the directory	Displaying data in the file
Displaying directory attributes	Displaying file attributes
Changing directory attributes	Displaying the file owner and permissions
Creating subdirectories and files	Changing the file
Going to the directory's subdirectories	Changing file attributes
Displaying the directory owner and permissions	Running the file
Deleting the directory	Deleting the file
Changing directory owner and permissions	Changing the file owner and permissions

6.5 File Sharing Compatibility with Diverse Clients

The Advanced Server software helps ensure compatibility with a wide variety of clients and legacy applications attempting to share server resources. This section describes several of the features that provide this compatibility, including:

- Extended File Specifications
- Unicode or extended character sets
- Legacy applications with more restrictive file naming conventions

6.5.1 Extended File Specifications

With OpenVMS Version 7.2 and higher, you can use the Extended File Specifications feature to offer file system services that are compatible with Windows 95, Windows 98, Windows 2000, Windows XP, Windows 2003, and Windows NT file systems. Extended File Specifications provides the following capabilities to OpenVMS Alpha systems. The benefit to the Advanced Server client computers depend on the type of client, as noted.

- Deep directories, similar to Microsoft Windows NT. Previous versions of OpenVMS support a maximum of eight directory levels.

Deep directories allow network clients to use hierarchical storage of directories and files on the OpenVMS disk similar to the client-based disk. They are also of benefit to applications developers who are porting applications from other environments that have support for deep directories.

- Extended file names (using ODS-5 disk structures). Extended file names functionality is an optional feature originally provided with the OpenVMS V7.2 operating system that extends OpenVMS file name capabilities to more closely match those of Windows 95, Windows 98, Windows 2000, Windows XP, Windows 2003, and Windows NT computers. With this functionality, OpenVMS Alpha V7.2 (and higher versions) systems support long file names (up to 243 characters including the version number), and adds ISO Latin-1 characters to the supported character set.

To take advantage of the capabilities of Extended File Specifications, be sure to complete the following steps:

1. Convert disk volumes that are used for storing shared directories and files from the ODS-2 to ODS-5 file system. For instructions, refer to the *OpenVMS Guide to Extended File Specifications*.
2. Convert existing shared files on those disk volumes. For instructions, refer to the *HP Advanced Server for OpenVMS Server Installation and Configuration Guide*.

Note

If you plan to configure one of the alternative languages supported by the Advanced Server for OpenVMS (V7.3 and higher), and your ODS-2 disk device includes escape-encoded characters in file names (characters that are in the format *__XX*), you must convert all the file names, as explained in the *HP Advanced Server for OpenVMS Server Administrator's Guide*. Do this before configuring the new language. The support of alternative languages is described in Section 6.5.2, Unicode Characters in Share Names.

To simplify share access, you may want to set up all shared disk volumes as ODS-5 disk volumes.

6.5.2 Unicode Characters in Share Names

Unicode and *extended character sets* provide an extensive character coding system and standard designed to support written texts of the diverse languages of the modern world. The design of extended character sets is based on the simplicity and consistency of the ASCII encoding, but goes far beyond ASCII's limited ability to encode only the Latin alphabet.

A client computer that supports Unicode, or which is configured to use a code page that is not related to a Western European language, can create files with characters in the file name that are not part of the standard ISO Latin-1 character set. Any Advanced Server product previous to the Advanced Server V7.3B for OpenVMS could not store files using these file names. The latest version of the Advanced Server for OpenVMS file server can now support Unicode characters or extended character sets that are foreign to the Western European languages. The characters that the Advanced Server for OpenVMS can support at any time depend on the current language configured for the server. (You use the PWRK$CONFIG configuration procedure to configure the language.)

This support for alternative languages allows you to configure the Advanced Server to support the local language of the server users. You can select any one language from a list of 43 languages from all over the world. Two of the supported languages support the Euro currency symbol.

Support of the Unicode or extended character set characters makes available a broader set of characters not only for file and share names, but also for other objects manageable by the Advanced Server, such as user names and group names.

The languages and their associated ISO-8859 character sets are a subset of the Unicode (UCS-2) character sets supported on OpenVMS ODS-5 disk structures. On ODS-2 volumes, the Advanced Server stores these characters in an escape-encoded format. If you plan to use one of the alternative languages, and you have an ODS-2 disk device that includes escape-encoded characters in file names, you should convert all file names using the PWCONVERT utility, as explained in the *HP Advanced Server for OpenVMS Server Installation and Configuration Guide*. For more information on on Unicode and extended character sets, see the *HP Advanced Server for OpenVMS Server Administrator's Guide*.

6.5.3 Enhanced Support for Legacy Applications with Restrictive File Naming

Some applications and client applications are more restrictive than the Advanced Server and Windows NT in both the lengths of file names and in the set of valid characters supported for file names. 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 the capabilities of the OpenVMS ODS-5 disk volume and longer file names supported on Windows NT, the Advanced Server, and other systems.

To enable compatibility with legacy applications (such as MS-DOS) whose file naming conventions are more restricted than those used by the Advanced Server, Advanced Server for OpenVMS servers, Version 7.3 or later, automatically create MS-DOS-compatible alias file names for files whose names do not comply with the file naming standards of those applications. 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.

An alias file name is also created for any file whose real name contains any extended character set characters with values of 128 through 255 (hexadecimal 0080 through 00FF). This is done even when the real filename is MS-DOS-compatible (has the 8.3 format and contains no characters that are explicitly invalid in MS-DOS file names). The Advanced Server V7.3B for OpenVMS returns a file's alias name, instead of the real file name, to an MS-DOS client only if the real name is not MS-DOS-compatible, or if any extended character set character in the real name does not map to the client code page. Otherwise, the Advanced Server returns the file's real name to the MS-DOS client.

For more information on the alias file names created by the Advanced Server for OpenVMS, see the *HP Advanced Server for OpenVMS Server Administrator's Guide*.

7
Sharing Printers

This chapter offers guidelines on how to set up and share printers in an Advanced Server domain. By planning printer access, you can maximize use of each printer and at the same time avoid printing delays.

Advanced Server printing offers the following features:

- The ability to browse the network for available printers
- Printing to network-interface printers and to printers connected directly to print servers

7.1 Planning Your Printing Operations

Because every network user uses print services, make sure that network print operations are set up efficiently and cost effectively. The choices that you need to make may include the following:

- Which printers to use
- Which computers to use as print servers
- How to configure shared printers for maximum use

7.1.1 Choosing the Printers to Use for Network Print Operations

Determine which printers you want to make available to your server community. Some considerations regarding printers include their:

- Location

  Select printers that are closest to the physical location of those who will be requiring their output.

- Cost of use

  On one hand, you might not want to make expensive-to-use printers available to all network users. On the other hand, using one network printer for several groups in a building is less expensive than requiring separate printers for each group in the building.

- Resolution

  Users who frequently print graphics will require printers with higher resolution. Groups who usually print text files can use lower-resolution printers.

7.1.2 Choosing Computers to be Print Servers

A computer can act simultaneously as a print server and a file server. The decision to combine print and file servers may depend on security concerns. Although printers should always be available to their users, you may want to locate a file server in a secure place.

Regardless of the size of your network, you will most likely install printers at a few select computers. The only special hardware requirement for print servers is that if you are using parallel or serial printers, the print servers must have the correct output ports.

7.1.3 Sharing Printers and Print Queues

Traditionally, the Advanced Server has made printers available to network users through *print shares*. Generally, you use the Advanced Server ADMINISTER command line interface to add printers (as print queues) and print shares to the Advanced Server. Each print share points to a single print queue with the same name as the share. Permissions that you assign to the share are applied automatically to the associated print queue. A share can be accessed over the network by users who have the appropriate permissions, like any other shared resource. Four types of permissions apply to print shares: Print (the default), None (no access), Manage Documents, and Full (full control). For more information, see Section 7.2, Ensuring Print Share Security.

Beginning with V7.3 of the Advanced Server for OpenVMS, you can configure the server to allow management of shared printers from Windows NT, using the Windows NT print services. The default is to use the Advanced Server ADMINISTER command-line interface. To enable *Windows NT-compatible print management*, you must use PWRK$CONFIG, as explained in your *Server Installation and Configuration Guide*.

If you prefer the ADMINISTER command-line interface and the way you have worked with shared printers on the Advanced Server in the past, you can continue using the ADMINISTER command-line interface for print queue management.

If you prefer the advantages that Windows NT printer management offers, then you might consider enabling that style of management when you configure your server. Whichever style you choose, you only have full functionality from the style chosen — you cannot have full management functionality with both.

Some of the advantages of using Windows NT-style printer management include the following:

- Simple management of Advanced Server shared printers by using the Windows NT print services dialog boxes.
- When adding a printer to the Advanced Server, the Windows NT Add Printer Wizard installs the required drivers for the printer on the server; these drivers are provided by the administrator (such as from the Windows NT installation CD-ROM). When a client is set up to use the printer, these drivers are available for downloading.
- Use of Windows NT access permissions for Advanced Server shared printers.
- Printers or print queues that were already defined on the server are upgraded automatically so that clients can continue to share these printers; but the upgrade does not provide full Windows NT printer management functionality for these upgraded printers. (You can acquire full functionality by using Windows NT print services to delete the printers from the Advanced Server and then adding the printers back onto the Advanced Server.)

For more information on the differences between printer management using ADMINISTER commands and using Windows NT, see Section 7.4, Managing Print Shares, Print Queues, and Print Jobs.

For detailed information about creating, modifying, and managing print shares, see your *Server Administrator's Guide*.

7.1.3.1 Print Queues

A *print queue* allows users to submit jobs for printing, and in the Advanced Server, access to print queues is through associated Advanced Server print shares or Windows NT-style shared printers, depending on the style of printer management configured for the Advanced Server. Because the Advanced Server is based on OpenVMS, the print queues associated with Advanced Server shared printers are OpenVMS print queues.

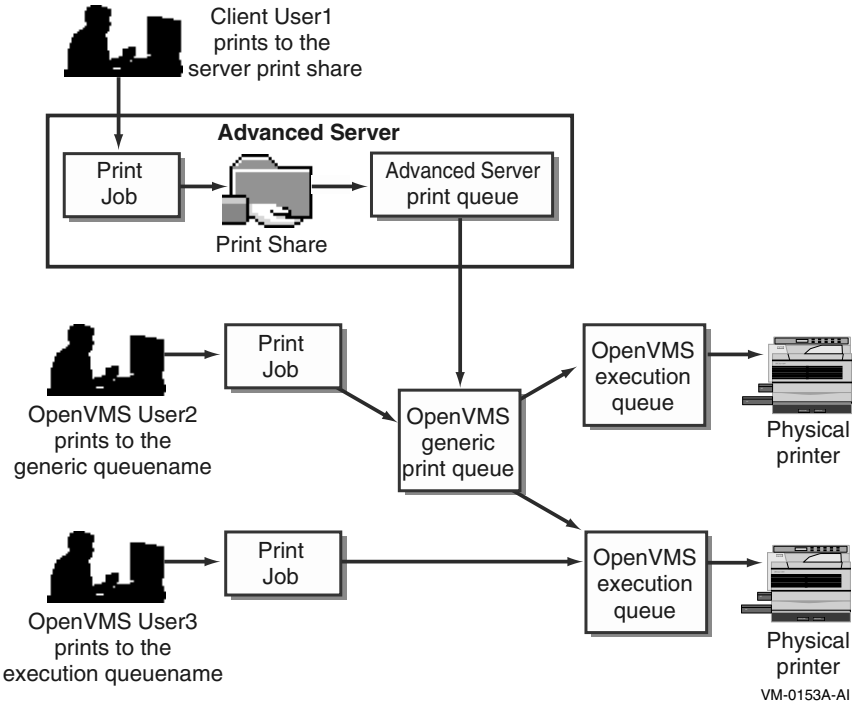
OpenVMS print queues include both *generic queues* and *execution queues*. Every OpenVMS printer is associated with one execution queue. In addition, you can use a generic queue when several like printers are available to the user. A generic queue can point to several execution queues and is used to

distribute printer workload among several like printers by routing a print job to the first available printer through that printer's execution queue. With the Advanced Server, a print queue that works like an OpenVMS generic queue is called a *routing queue*, and a queue that works like an OpenVMS execution queue is called a *printer queue*.

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. Printers can be connected directly to the server by a serial or parallel port or directly to the network with a network adapter card. The server's queuing system, providing OpenVMS system information for handling print jobs, mediates between the Advanced Server and the printer so that print jobs can execute while users perform other tasks at their client workstations.

Figure 7–1 shows an Advanced Server print share and queue configuration used by client User1. User1 prints to the shared printer. The Advanced Server print queue works in conjunction with the associated OpenVMS generic print queue to send the print job to one of the two printers shown. User2 and User3 are OpenVMS users (presumably without server accounts) who can also print to the same printers. OpenVMS User2 prints to the OpenVMS generic queue, which sends the job to either one of the two printers. OpenVMS User3 prints solely to the one printer shown, through the OpenVMS execution queue. Note that this figure illustrates server printing as configured by ADMINISTER command management. Server printing set up through Windows NT-style management would be different. For similar illustrations of Windows NT-style configurations, see Figure 7–9, Advanced Server Windows NT Printer, Queue, and Share, and Figure 7–10, Advanced Server Windows NT Printer Management: Setting Up Printer Pooling. For more information on Windows NT-style management, and the differences between the two styles of management, see Section 7.4, Managing Print Shares, Print Queues, and Print Jobs.

Figure 7–1 Print Shares and Print Queue Configurations



You can share existing OpenVMS queues or create and share new ones. Be aware that, if you are using the ADMINISTER management style for printers, then Windows NT, Windows 95, Windows 98, and Windows 2000 clients require that a print share name and queue name be the same. If you cannot create a share name that equals the OpenVMS queue name (for example, the OpenVMS queue name is more than 12 characters long), you can define a shorter system logical name that equates to the name of the OpenVMS queue, then create a share using the logical name of the queue.

For detailed information about OpenVMS print queues, see the OpenVMS documentation. For information on sharing queues and printers, see your *Server Administrator's Guide*.

The concepts and terminology used with printing vary according to the style of printer management in effect. In short, with Advanced Server ADMINISTER commands, you add a print queue, associating it with a printer, and you add a share pointing to that printer. You designate whether the print queue is to be a printer queue (OpenVMS execution queue) or routing queue (OpenVMS generic queue).

With Windows NT-style management, the manager or administrator adds a printer to the Advanced Server, and has the option of setting up the printer for sharing and to enable pooling. A *printer pool* is similar to an Advanced Server routing queue or OpenVMS generic queue — it is a group of printers connected to a server; when a print job is sent to the server, it goes to the first available printer in the pool. When printer pooling is enabled, the Advanced Server automatically sets up a queue of the same name for the printer. The Advanced Server also creates the following for the added printer:

- A print share (primarily used for client browsers) if you indicate that the printer is to be shared.
- A share named PRINT$ used for storing the printer drivers that can be downloaded to the clients that wish to use the printer.
- An entry in the OpenVMS Registry that defines printer parameters and includes the names and location of the driver files.

For more detailed discussion of the differences between the two management styles, see Section 7.4, Managing Print Shares, Print Queues, and Print Jobs.

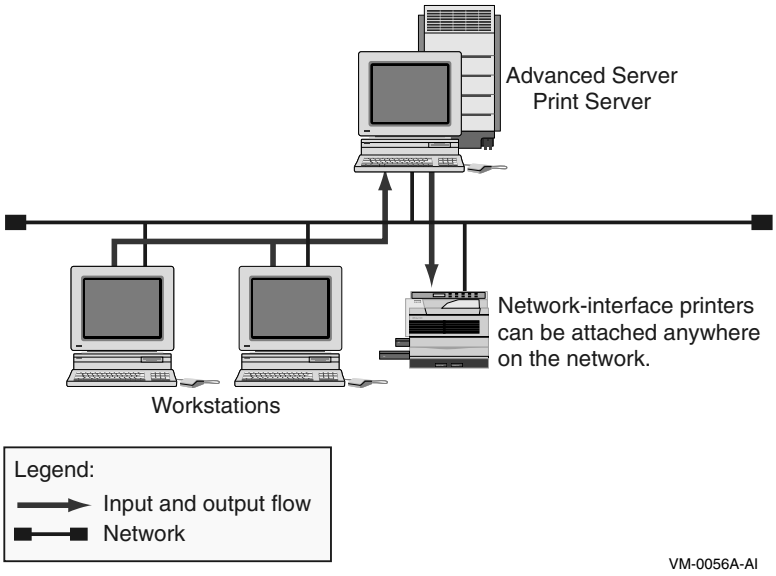
7.1.3.2 Setting Up OpenVMS Printers

If a printer is on the network, you must set it up like any OpenVMS printer. For information on setting up OpenVMS printers, see the OpenVMS documentation.

7.1.3.3 Network-Interface Printers

Unlike parallel and serial devices, printers with built-in network adapter cards do not have to be adjacent to the print server. Network-interface printers are attached to the network through a built-in adapter card. The location of this type of printer has no effect on printing performance, providing that users and printers are not on opposite sides of a network bridge. An Advanced Server print server can control a virtually unlimited number of network-interface printers. Figure 7–2 shows a network-interface printer configuration.

Figure 7–2 Configuring Network-Interface Printers



7.1.3.4 How a Shared Print Queue Operates

When a user sends a print job to a print queue associated with a print share, the shared print queue sends the print job to the server's queuing subsystem, which forwards the job to the appropriate printers.

The Advanced Server sends a message to the user indicating the share name and the job ID. The Advanced Server also notifies the user if there are problems with print jobs (if the printer is capable of such notification) or if there are changes in the status of print jobs (such as a pause in the queue).

The Advanced Server lets you create simple shared-printer arrangements that send print jobs to one printer and more sophisticated arrangements that send print jobs to any one of several queues or several printers of the same type. When setting up a print share, you should consider the following options:

- Which queues should receive print jobs sent to the shared printer?
- Which printer devices should receive print jobs from the queues?

7.1.3.5 Types of Shared Print Queue Configurations

You can configure shared printers and their queues in a number of ways. (The term “print share” is normal to the ADMINISTER management style; in Windows NT-style management, the equivalent of a print share is a logical printer that has sharing enabled. The logical printer is associated with a printer device (port).) In order of increasing complexity, the ways you can configure shared printers and their queues include:

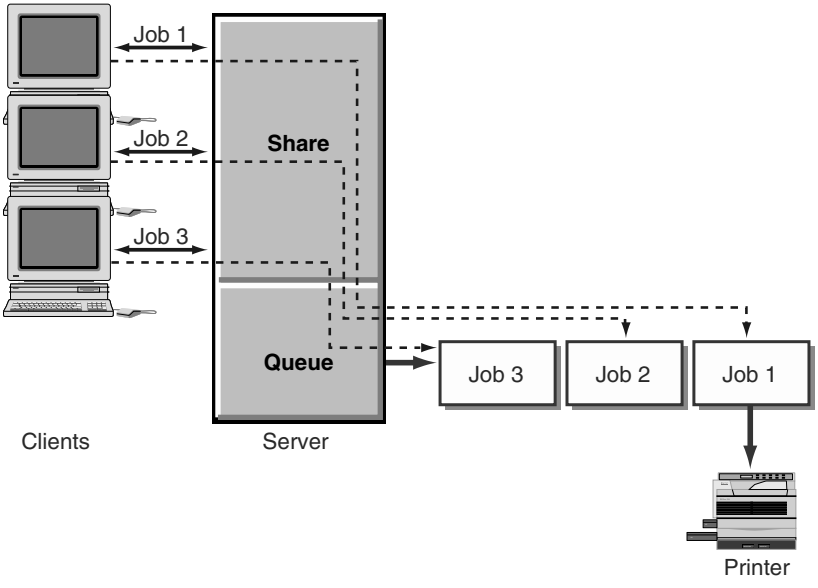
- A printer queue (as with an OpenVMS execution queue), associated with a single printer)
- A routing queue (as with an OpenVMS generic queue), pointing to multiple printers of the same type, each through its individual printer queue; with Windows NT-style printing, the group of printers is called a printer pool

You can control permissions on the print shares or Windows NT-compatible printers.

The following sections provide illustrations of the listed print share configurations.

7.1.3.5.1 Single Print Share and Print Queue — Single Printer The simplest print configuration is one that sends print jobs through a single print share and print queue to a single printer, as shown in Figure 7–3.

Figure 7–3 Single Print Share and Print Queue — Single Printer



To create such a configuration using the ADMINISTER interface, you must add the print queue, then add a share that allows users to connect to the queue (for an example, see Section 7.4, Managing Print Shares, Print Queues, and Print Jobs). You specify the same name for the share and for the queue that it points to. (For access from Windows 95, Windows 98, Windows 2000, and Windows NT clients, the share and queue name created with ADMINISTER commands must be the same. For other clients, such as Windows 3.1 and MS-DOS, the share and queue name can be different.)

Using the Windows NT interface, you add the printer and enable it for sharing (for an example, see Section 7.4, Managing Print Shares, Print Queues, and Print Jobs).

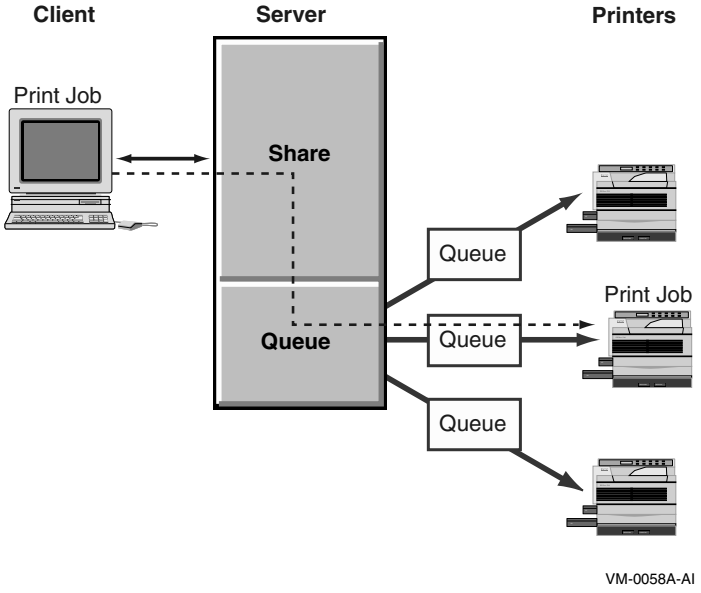
7.1.3.5.2 Single Print Share with a Single Queue — Multiple Printers

When print jobs are submitted through a print share to a generic or routing queue associated with multiple printers, the Advanced Server searches for an available printer and automatically routes a print job to the execution or printer queue of the first available printer. This is an efficient way to share a group of printers of the same type (a printer pool). The Alerter service sends a message to the user indicating when, and on which printer, the job was printed.

Using the ADMINISTER interface, to create a configuration that includes a generic or routing queue associated with multiple printers, you add a queue and a share with identical names and point the queue to a series of printers. With the Windows NT interface, you add the printer, enable it for sharing and printer pooling, and select multiple ports that can receive print jobs sent to that (logical) printer. (See the examples in Section 7.4, Managing Print Shares, Print Queues, and Print Jobs.)

Figure 7–4 illustrates a single generic or routing queue associated with multiple printers.

Figure 7–4 Single Print Share with a Single Queue — Multiple Printers

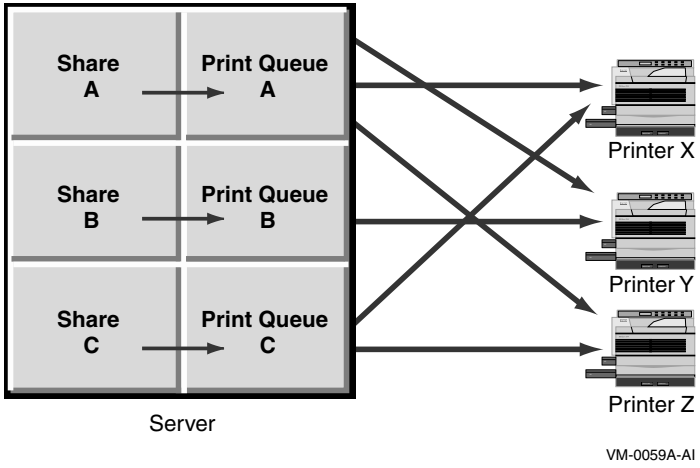


For information on how to share remote printers, see your *Server Administrator's Guide*.

7.1.3.5.3 Multiple Shared Queues — Multiple Printers You can assign two or more print shares and queues to the same printer or group of printers. This approach is especially useful if you configure the queues differently. For example, you can assign different permissions to different shares.

In the configuration shown in Figure 7–5, Queue A sends jobs to Printers X, Y, and Z; Queue B sends jobs only to Printer Y; and Queue C sends jobs to Printers X and Z. This configuration offers flexibility and convenience both to the administrator who needs to set up different shares and queues for different purposes and to users who need a share and queue that routes jobs to the next available printer.

Figure 7–5 Multiple Shared Queues — Multiple Printers



7.2 Ensuring Print Share Security

With the ADMINISTER interface, you can control printer usage through the Advanced Server by setting permissions for each print share. When you add or modify a print share, you specify the users or groups allowed to access the share. The permissions that you set on a share apply automatically to the queue that the share points to. Any changes made later to share permissions automatically affect the permissions on the associated queue.

By default, all the print shares you create are available to every network user (Everyone). Restricting access to a print share requires altering the share's permission settings for a particular group or user. To change permissions on a print share, you must have Full permission.

Four types of permissions apply to print shares:

- None — No access: does not allow use.
- Print — Allows user to print documents.
- Manage Documents — Allows user to control settings for print jobs and to pause, resume, restart, and delete print jobs.
- Full — Full control: Allows user to print documents; control settings for print jobs; pause, resume, restart, and delete print jobs; change the printing order of documents; pause, resume, and purge printers; change printer properties; delete print shares; and change share permissions.

Permissions granted directly to a user account and those granted by a user's membership in one or more groups are cumulative; that is, restrictions filter requests, and the most restrictive permissions apply. The None (no access) permission overrides all other permissions.

With the Windows NT interface, you can control access by modifying the access permissions for the shared printer. The permissions are similar to those discussed above.

7.3 Printing from MS-DOS Computers

Workstations running MS-DOS or versions of Windows for MS-DOS can access Advanced Server printers by redirecting their output ports to the correct *server**sharename*.

If you are sharing printers with MS-DOS workstations, share names must be no more than eight characters, optionally followed by a period and one to three characters.

7.4 Managing Print Shares, Print Queues, and Print Jobs

Beginning with Version 7.3 of the Advanced Server for OpenVMS, you have the choice of configuring the Advanced Server so that its printers can be managed from a Windows NT computer, using the easy-to-use Windows NT Print Manager dialog boxes. Prior to Version 7.3, management of Advanced Server for OpenVMS printers was limited to the Advanced Server ADMINISTER command-line interface, with the exception of minor printer management operations that can be done remotely from Windows NT (such as pausing and deleting print jobs). All PATHWORKS for OpenVMS (Advanced Server) servers

limit management of printers to the Advanced Server ADMINISTER user interface (with the few exceptions noted previously).

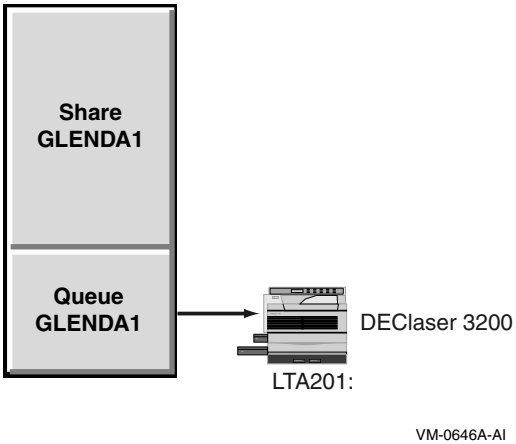
By default, printers shared on the server are managed with the ADMINISTER command-line interface. You must configure the Advanced Server (using PWRK$CONFIG) to allow full management of printers from Windows NT.

The concepts, terminology, and procedures used for managing Advanced Server shared printers differ significantly for each style of management.

The management of shared printers with the ADMINISTER command involves creating a print queue (ADD PRINT QUEUE command), defining it as either a printer queue (OpenVMS execution queue) or a routing queue (OpenVMS generic queue), and then creating a share for that queue. The ADD PRINT QUEUE command in the following example creates a printer queue (executive queue) called GLENDA1 on the Advanced Server. The printer queue points to a DEClaser 3200 printer that is connected to device (port) LTA201. The ADD SHARE/PRINT command creates a share for print queue GLENDA1. Figure 7–6 shows the arrangement of printer, print queue, and print share.

```
LANDOFOZ\\TINMAN> ADD PRINT QUEUE GLENDA1 /PRINTER=LTA201 /TYPE=DL3200
%PWRK-S-QUEADD, queue "GLENDA" added on server "TINMAN"
LANDOFOZ\\TINMAN> ADD SHARE/PRINT GLENDA1
%PWRK-S-SHAREADD, share "GLENDA1" added on server "TINMAN"
```

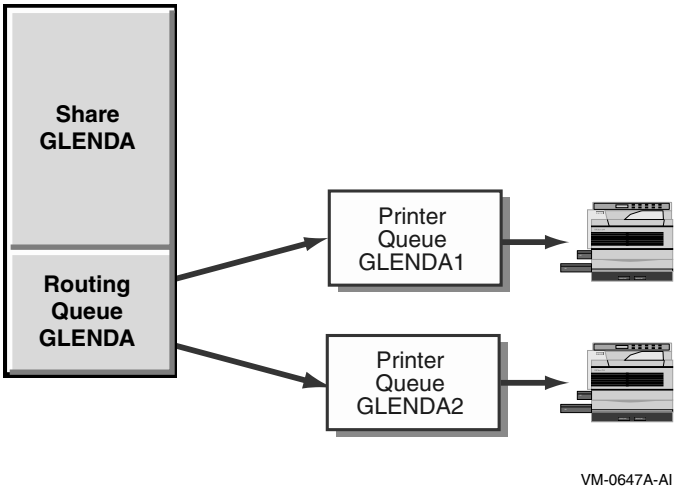
Figure 7–6 Advanced Server ADMINISTER Command Management: Printer Queue



The first of the next two commands creates a routing queue named GLENDA so that print jobs sent to GLENDA will go to either of the two printer queues, GLENDA1 or GLENDA2, for the associated printers, as illustrated in Figure 7–7. The second command creates share GLENDA for the routing queue (by default, the share points to the queue with the same name).

```
LANDOFOZ\\TINMAN> ADD PRINT QUEUE GLENDA /ROUTE_TO=(GLENDA1,GLENDA2)
%PWRK-S-QUEADD, queue "GLENDA" added on server "TINMAN"
LANDOFOZ\\TINMAN> ADD SHARE/PRINT GLENDA
%PWRK-S-SHAREADD, share "GLENDA" added on server "TINMAN"
```

Figure 7–7 Advanced Server ADMINISTER Command Management: Routing Queue



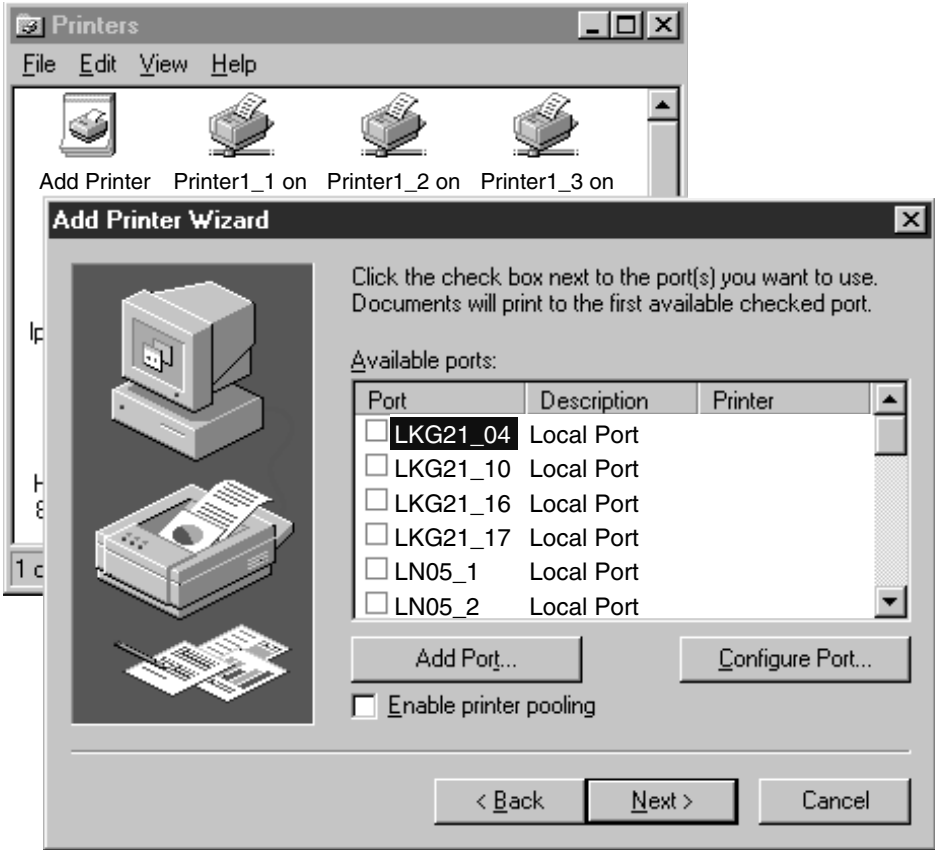
With Windows NT-style management, you manage printers, printer ports, print queues, and the associated parameters defined in each printer's OpenVMS Registry entry. Any administrators, print operators, or server operators on the Windows NT system can manage these printers. Notice that all users can add a server printer to their local Windows NT computer and manage their own print jobs from their Windows NT computer.

You use the Add Printer Wizard to add a printer to the server. In specific, from a Windows NT computer, double-click on the icon for the Advanced Server in the Network Neighborhood, select the Printers folder, then double-click on the Add Printer icon, and follow the instructions on the Add Printer Wizard screen. The Add Printer Wizard allows you to select:

- A port (an OpenVMS executive queue) to print to, as illustrated in Figure 7–8
- Whether to enable printer pooling, as illustrated in Figure 7–10
- The name of the printer
- Whether to share the printer, and the name of the share

- The type of printer

Figure 7–8 Advanced Server Windows NT Printer Management: Adding A Printer

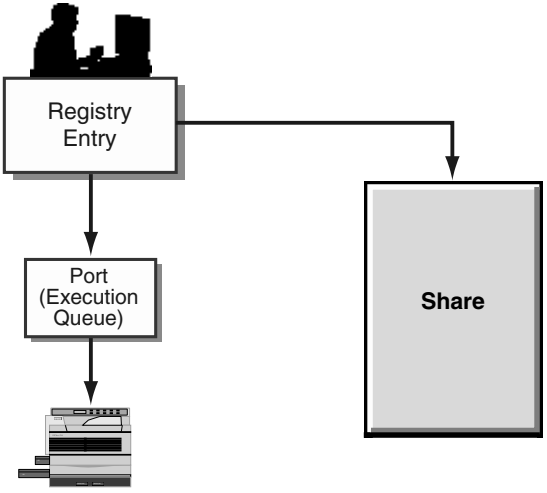


VM-0648A-AI

When a printer is added to the Advanced Server, with printer pooling disabled, an entry for the printer is added to the OpenVMS Registry. It points solely to the selected printer port. Client users who want to use the printer can then add it to their computer (in much the same way as described above for adding a printer to the server). The client user can have the printer drivers downloaded from the server to the client computer.

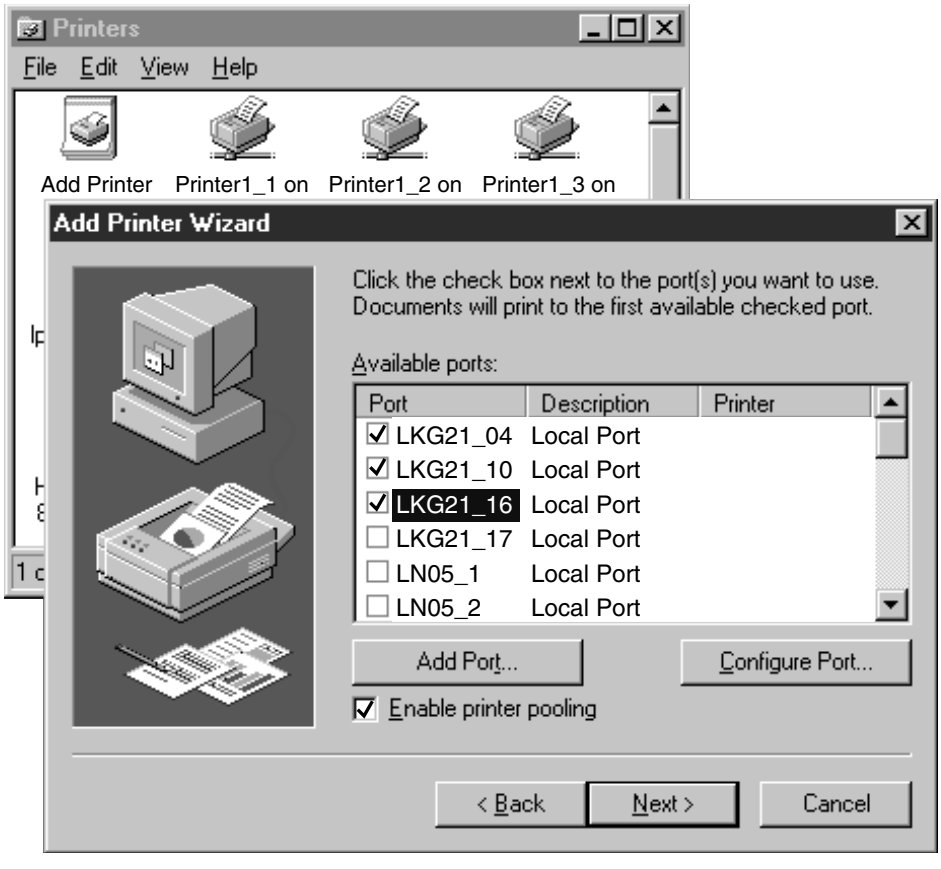
Figure 7–9 illustrates the basic relationship of printer, print queue, and share in the Windows NT environment.

Figure 7–9 Advanced Server Windows NT Printer, Queue, and Share



To use the Add Print Wizard to set up printers for printer pooling, check the box for enabling printer pooling and select several ports to point the printer to, as shown in Figure 7–10.

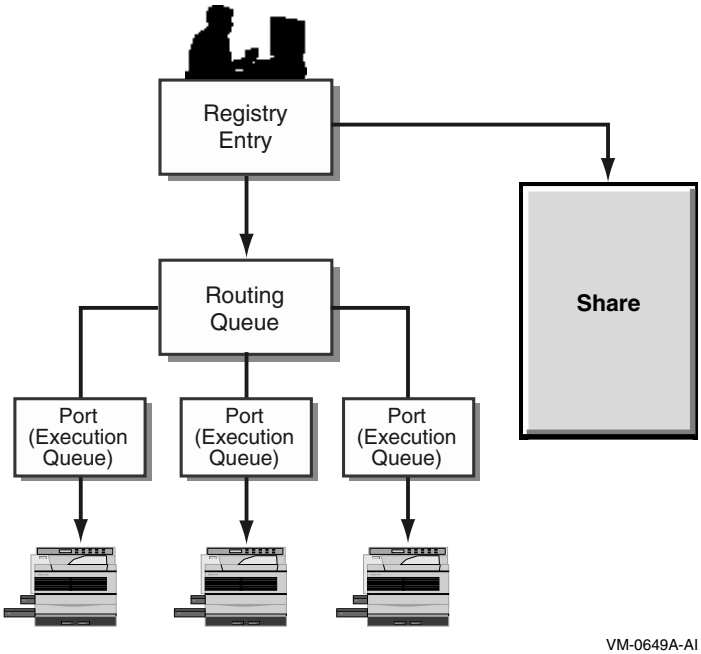
Figure 7–10 Advanced Server Windows NT Printer Management: Setting Up Printer Pooling



VM-0719A-AI

The Advanced Server creates a routing queue of the same name as the printer, pointing to the pool of printers. Figure 7–11 shows the printer pooling for three ports.

Figure 7–11 Advanced Server Windows NT Pooling



The Advanced Server ADMINISTER command-line interface lets you display a single share, a single queue, a list of all of the server's print queues, or the print jobs in each queue. Using Windows NT print services tools, you can view the printers on the Advanced Server and their properties, as well as the printer queue and the print jobs in each queue. These capabilities are useful because you may need to stop sharing a print share or queue under any of the following circumstances:

- To reorganize print shares (or shared Windows NT printers)
- To reorganize print queues
- To remove a printer (affects the shared queue only if this printer is the only printer in the queue)
- To remove a print share (or shared Windows NT printer) that is no longer needed

In addition, the Advanced Server has the following capabilities for managing printers and print jobs:

- Displaying (with ADMINISTER SHOW commands) a list of print shares and their respective print queues and print jobs
- Stopping print queue sharing
- Pausing, continuing, or deleting a print queue
- Deleting, holding, or restarting print jobs from a print queue
- Changing the position of a print job already in a queue, either to the top or bottom of the queue

For more information on how to control print jobs, see your *Server Administrator's Guide*.

A

Differences Between Advanced Server and Windows NT Server

The Advanced Server provides networking that is functionally equivalent to that of the Windows NT Server. The Advanced Server can operate independently or in cooperation with Windows NT Servers. This appendix discusses some differences you will encounter between the Advanced Server and Windows NT Server in day-to-day management of a network that includes both types of servers. These differences include how individuals are assigned as administrators and operators, how security works, and how resource permissions map between the systems.

A.1 Management Tools

The Advanced Server provides the Windows NT server administration tools for managing the network. Using these tools, you can administer the Advanced Server from a Windows 95, Windows 98, or Windows for Workgroups client. You can also administer the Advanced Server from a Windows NT workstation computer that has the Windows NT server administration tools installed, and from a Windows NT Server computer. The tools can also be used to manage Windows NT Server.

Installable versions of the Windows NT server administration tools are shared automatically by the Advanced Server.

A.1.1 Printer Management

Configured to support Windows NT-style printer management, the Advanced Server for OpenVMS provides similar printer management capabilities as provided by Windows NT. The only known exceptions are the following:

- You cannot adjust the scheduling properties (normally accessed from the Windows NT printer's Properties window) of Advanced Server printers.

- Upgraded printers (that is, printers or print shares that were already defined on an Advanced Server when Windows NT printer management was enabled) cannot be managed with all the management functionality available for printers that were added to the server by Windows NT print services. For example, you cannot use Windows NT to add an upgraded server printer to another workstation. You can gain full functionality for upgraded printers by removing them and then using Windows NT print services to add them back to the server again.

Configured to support printers with the ADMINISTER command-line interface, the Advanced Server provides only limited management capabilities from Windows NT, such as managing print jobs.

A.1.2 User Account Information

User accounts in Advanced Server domains maintain the same user account information as Windows NT Server accounts.

A.2 Services

The Advanced Server supports most Windows NT Server services. Table A–1 describes the Windows NT Server services that run on the Advanced Server.

Table A–1 Services Common to Advanced Server and Windows NT Server

Service	Description
Alerter	Notifies selected users and computers of administrative alerts on a computer. Used by the server and other services. Starts by default.
EventLog	Records system, security, and application events in the event logs, and enables remote access to those logs. Starts by default.
NetLogon	Verifies the user name and password of each person who attempts to log on to the network or gain access to the server. Starts by default.
Server	Provides file, print, and named pipe sharing, and support for remote procedure calls. Starts by default.
Time Source	Identifies a server as the domain time source.

A.3 Resource Permissions

This section compares the user-level permission settings available in Windows NT Server with the security settings that are available in the Advanced Server, including file, directory, printer, and named pipe settings. The Advanced Server does not support communication queues.

A.3.1 File and Directory Permissions

Advanced Server file and directory permissions are identical to Windows NT Server file and directory permissions. Both are typically applied in predefined sets, such as Full Control, Read, or Change.

The Advanced Server enhances the file and directory permissions on Windows NT Server by offering the additional option of enforcing OpenVMS security.

A.3.2 Printer Permissions

The Advanced Server and Windows NT Server implement identical printer security. Permissions are assigned to print shares, through which the user accesses print queues. The available printer permissions are Print, None, Manage Documents, and Full on Advanced Servers; these permissions correspond to Print, No Access, Manage Documents, and Full Control on Windows NT Server.

A.4 Disk Resources Shared by Default

With Windows NT Server and Advanced Server, you can share directories and specify which users can access them. To share a directory, assign a share name to it.

Table A–2 shows share names (or disk resources) that typically are set up automatically in Windows NT Server and Advanced Server. The number of shared resources on your server will vary depending on your implementation.

Table A–2 Share Names

Windows NT Server	Advanced Server	Description
ADMIN$	ADMIN$	A special administrative resource for remote administration. All share names that end in a dollar sign ($) are hidden; they do not normally appear when a user displays server resources.
C$	C$	A connection to the root of the file system. On Windows NT Server, this is the local C device. On the Advanced Server, this is PWRK$LMROOT:[LANMAN].
d$	*device*$	An administrative share. On Windows NT Server, a single letter from D to Z followed by $ identifies the drive letter; on OpenVMS, the name of the disk device or directory followed by $ identifies the disk.
IPC$	IPC$	Supports interprocess communication.
LIB	N/A	Contains header files and link-time libraries needed to create applications. Not supported by Advanced Server.
NETLOGON	NETLOGON	Shares the directory specified by scripts with the share name NETLOGON.
REPL$	N/A	On Windows NT Server, this directory is associated with the Directory Replicator service. It is available when the Directory Replicator service is active on the export server. Not supported by Advanced Server.
USERS	USERS	Contains user home directories.

B

Worksheets

It is useful to keep track of domains, groups, user accounts, and trust relationships you create as you build and modify your network. The information you record can help you manage your network and solve problems as they arise.

To record the way you build and modify your network, photocopy the worksheet templates provided in this chapter and fill them in as you plan your network; update the worksheets as you modify your network in the future.

The following is a list of worksheet templates provided:

- The Domain Worksheet — Lists the servers that are members of a domain, their configurations, and roles; records the domain's trust relationships with other domains.
- The Groups Worksheet — Lists and describes the user groups in a domain, and lists the members of each group.
- The Shares Worksheet — Lists a server's directory and print shares.

B.1 The Domain Worksheet

Use this worksheet to list all the servers in the domain with their configurations and roles and to record the domain's trust relationships with other domains.

Domain Name:		
Domain Members		
Type of Computer: [1]	Network Configuration: [2]	Role in Domain: [3]
Trust Relationships		
Trust This Domain: (Y,N)	Trusted By This Domain: (Y,N)	Name of Domain:

[1] Type of server or workstation; for example, PATHWORKS Advanced Server

[2] For example, TCP/IP, DECnet

[3] For example, PDC, BDC, Member Server

VM-0096A-AI

B.2 The Groups Worksheet

Use this worksheet to track the user groups created in the domain.

Domain Name:		
Date Created:	**Group Name:**	
Type: Global ___ Local ___	Description:	
Used in trusting domains:		
Members included:		
Date Created:	**Group Name:**	
Type: Global ___ Local ___	Description:	
Used in trusting domains:		
Members included:		
Date Created:	**Group Name:**	
Type: Global ___ Local ___	Description:	
Used in trusting domains:		
Members included:		

VM-0097A-AI

B.3 The Shares Worksheet

Use this worksheet to list the shares defined on the local server. Fill out a separate worksheet for each server.

Server:		**In Domain:**
Share Name:	Type:[1]	Description:
Path:	RMS File format:[2]	
OpenVMS Protection:[3]	Directory Permissions:	File Permissions:
Share Permissions:		
Group or User:	Permissions:	
Group or User:	Permissions:	
Group or User:	Permissions:	
Group or User:	Permissions:	
Share Name:	Type:[1]	Description:
Path:	RMS File format:[2]	
OpenVMS Protection:[3]	Directory Permissions:	File Permissions:
Share Permissions:		
Group or User:	Permissions:	
Group or User:	Permissions:	
Group or User:	Permissions:	
Group or User:	Permissions:	
Share Name:	Type:[1]	Description:
Path:	RMS File format:[2]	
OpenVMS Protection:[3]	Directory Permissions:	File Permissions:
Share Permissions:		
Group or User:	Permissions:	
Group or User:	Permissions:	
Group or User:	Permissions:	
Group or User:	Permissions:	

[1] Print, Directory, File

[2] Sequential Fixed, Stream, or Undefined

[3] Applicable if the Advanced Server and OpenVMS security model is enabled

VM-0098A-AI

Glossary

access control

The mechanism for validating the right to use a resource or service, such as a connection, logon, or file access, that is stored on or connected to a server. A user name and password combination is the most common means of access control.

access control entry (ACE)

An entry in an access control list (ACL). Each access control entry defines the protection or auditing to be applied to a file or other object for a specific user or group.

access control list (ACL)

The part of a security descriptor that restricts and audits access to an object. The owner of an object has discretionary access control of the object and can change the object's ACL to allow or disallow other users access to the object. Access control lists are ordered lists of access control entries (ACEs).

access permissions

See **permissions**.

access right

A permission that controls the way in which an object may be manipulated by a user or by members of a group. Different object types support different access rights; these are stored in an object's access control list (ACL).

access token (or security token)

An object that uniquely identifies a user who has logged on. An access token is attached to all of the user's processes. The token contains the user's security ID (SID), the SIDs of any groups to which the user belongs, the user's privileges, and information describing the ownership and access control list (ACL) to be applied to any objects that the user's processes create. *See also* **access control list, security ID,** and **user privilege**.

account

See **user account**.

account policy

Defines the way passwords are implemented by all user accounts.

ACE

See **access control entry**.

ACL

See **access control list**.

ADMIN$

An administrative resource that enables remote administration of servers. A server's ADMIN$ resource is automatically shared and the share cannot be deleted. *See also* **C$** and **IPC$**.

ADMINISTER commands

Commands used to manage an Advanced Server locally or remotely. The ADMINISTER commands are the Advanced Server command-line interface and they conform to standard OpenVMS DCL command syntax.

administrative alert

A message from the Advanced Server concerning server and resource use, or problems relating to security and access, user sessions, and printing. *See also* **Alerter service**.

administrative resource

A resource used when network users and administrators perform certain tasks on the server, including viewing the resources the server is sharing, administering the server remotely, and running shared applications. Administrative resources include ADMIN$ and IPC$.

administrator

The individual responsible for managing the network. Typically, this person configures the network, maintains the network's shared resources and security, assigns passwords and privileges, and helps users.

Advanced Server

A network operating system compatible with Microsoft Windows NT technology that provides domain, file, and print services.

alert

A message that the server sends under certain conditions. *See also* **administrative alert** and **error alert**.

alert level

A value that users can specify so that the software notifies them when licenses are fully consumed. For more information, see the *HP Advanced Server for OpenVMS Guide to Managing Advanced Server Licenses*.

Alerter service

A server component that notifies selected users and computers of administrative alerts that occur on a computer. It is used by the Server service and other services. *See also* **administrative alert**.

alias

See **alias file name**, **cluster alias**.

alias file name

An alternate file name that the Advanced Server generates for a file whose name is incompatible with the traditional 8.3 file name format used by MS-DOS and legacy PC applications. For example, if the length of a file's name exceeds the MS-DOS 8.3 file name length, the Advanced Server generates an alternate file name, the alias, which conforms to the MS-DOS 8.3 file name format. Either the full file name or the alias file name may be used by a client to access the file.

application programming interface (API)

A set of routines that an application program uses to request and carry out lower-level services performed by the operating system.

archive bit

An attribute of any file: a bit that backup programs use to mark files after backing them up with either the normal or incremental backup types.

audit policy

The policy that defines the types of events that are logged.

audit trail

The event and error messages that are saved in the event log file, as defined by the audit policy.

auditing

The process by which Advanced Server records an entry in the event log file whenever a user accesses a resource in a certain way or logs on to the network.

authentication

Validation of a user's logon information. *See also* **external authentication**, **pass-through authentication**.

backup domain controller (BDC)

In a domain, a server that keeps and uses a copy of the security accounts database to validate logon requests and that can take over the function of the primary domain controller if the primary domain controller fails. *Contrast with* **member server**, **primary domain controller**.

batch command file

A file that contains one or more commands to be processed sequentially. When a user types the file name at the command prompt, the commands contained in the file are executed.

BIND

Berkeley Internet Name Domain. The implementation of a DNS server developed and distributed by the University of California at Berkeley. Host name and address lookup service for the Internet; implemented in a client/server model.

boot (or bootstrap)

To run or initiate a program that loads the operating system into memory and starts or restarts the computer.

broadcast message

A message sent to client workstations on the network. Users cannot respond to this type of message.

browse

To look through lists of servers and workstations in a domain.

built-in groups

The default groups provided with the Advanced Server. They each have established rights and abilities. These groups cannot be deleted. *See also* **group.**

C$

The administrative resource that represents a server's disk drive. The Advanced Server points C$ to PWRK$LMROOT:[LANMAN].

cache memory

High-speed memory that contains copies of data recently used, or likely to be used again, by the processor. Cache memory avoids frequent disk input/output, thus providing faster operation.

check box

In a dialog box, an indicator that a user can select or clear to turn one or more options on or off. Used, for example, in the Configuration Manager to select transports. *Contrast with* **radio button**.

client

A personal computer or workstation, connected to the network, that can access resources on a server. *Contrast with* **server**.

Client License Requester

A client-based PATHWORKS utility that is responsible for requesting client-based licenses for clients so that they can access resources on the server.

Client License Transponder

A client-based PATHWORKS utility that responds to license authentication requests.

client-based license

A license that is assigned on a per-workstation basis and allows a client to access multiple file servers. *Contrast with* **server-based license.**

cluster alias

The OpenVMS Cluster alias acts as a single network node identifier for an OpenVMS Cluster system. The cluster alias makes all the OpenVMS Cluster nodes appear to be one node from the point of view of the rest of the network. Remote applications in DECnet or TCP/IP networks, for example, can use the alias to access services provided by the cluster. Access is ensured if at least one OpenVMS Cluster member is available to process the service request.

The Advanced Server cluster alias is the single identifier that all Advanced Servers in the cluster share (in addition to each server's individual server name). This alias lets remote nodes (including clients) treat the entire cluster as though it were a single server. The Advanced Server cluster alias is transport independent; the OpenVMS Cluster alias is unique to either TCP/IP or DECnet. The Advanced Server cluster alias is shared only by those members that are running the Advanced Server; the OpenVMS Cluster alias is shared by all the members of the cluster.

code page

An ordered set of 256 characters developed to expand beyond the limitations of the ASCII (American Standard Code for Information Interchange) character set. Language-specific code pages were developed because the sum of characters used in languages internationally far exceeds 255. All the language-specific code pages overlay the same set of 8-bit values. For example, a specific 8-bit value in a code page used for the English language can be used for another character used for the Cyrillic language. An application has to be set to interpret the codes in the context of the selected code page.

Each 8-bit index value or code position in a code page is called a code point or code value. Most code pages, including those of the Advanced Server, map values 0 to 128 to the ASCII character set.

computer name

A unique name that identifies a server, personal computer, or workstation to the network.

configuration

The set of hardware, hardware options, software, and software options on a computer or network.

Configuration Manager

An Advanced Server tool for modifying server configuration parameters.

connection

The software link between a workstation and a shared resource on a server. A connection is made by assigning a local device name on the workstation to a shared resource on a server, or by accessing the resource through a network path name with a command or from an application. *Contrast with* **session**.

country code

A code in a user account that specifies the language in which the server sends messages to the user.

DECnet-Plus

The HP family of peer-to-peer, Ethernet-based network products.

default

The value assigned by a program if a value is not supplied by the user.

default permissions

The permissions assigned to a share if no permissions are specified.

destination directory

The directory to which one or more files are to be moved or copied. *Contrast with* **source directory**.

device driver

A program that enables a specific device, such as a printer, to communicate with the operating system.

device name

The name by which a computer identifies a printer, disk, or other device.

dialog box

A window displayed in response to user action that allows users to enter information and presents choices for further action.

directory

Part of a structure for organizing files on a disk. A directory can contain files and other directories (called subdirectories). *See also* **directory tree**.

directory access permissions

The type of access that a group or user is granted to a particular directory, such as read-only. *See also* **share permissions** and **special access permissions**.

directory replication

The copying of a master set of directories from a server (called an export server) to specified servers or workstations (called import computers) in the same or other domains. *See also* **domain synchronization**.

Directory Replicator service

Replicates directories, and the files in those directories, between computers.

directory share

See **shared directory.**

directory tree

A conceptual representation of a disk's directory structure. The directories on the disk are organized in a hierarchy. The top-level directory is the root directory. *See also* **path**.

disabled user account

A user account that does not permit logons. The account can be restored to enabled status at any time. *See also* **user account**.

disk resource

A disk device that can be shared.

distributed computing

An application design and implementation strategy that divides the user interface, processing, and database storage components of an application into units that can execute on multiple networked computer systems.

DNS

Domain Name System. A distributed database system that allows TCP/IP applications to resolve a host name into a correct IP address. The Advanced Server for OpenVMS can be configured as a DNS client to use a DNS server for NetBIOS name resolution in a wide area network. The Advanced Server can use DNS for OpenVMS Cluster load balancing in a WAN environment.

domain

A collection of computers that share a common security database and policy. Each domain has a unique name. A network can have many domains. *See also* **workgroup** and **logon security**.

domain database

See **security accounts database**.

domain synchronization

The replication of one or more elements of the domain databases (security databases), from the primary domain controller to one or more backup domain controllers in the domain. Domain synchronization is usually performed automatically by the system, but can also be invoked manually by an administrator. *See also* **full synchronization** and **partial synchronization.**

downlevel

A term that refers to earlier network operating systems, such as LAN Manager, that can interoperate with the Advanced Server.

driver

See **device driver**.

dynamic data exchange (DDE)

A form of interprocess communications (IPC) in which two or more programs that support dynamic data exchange can exchange information and commands.

edit box

In a dialog box, a field for entering information. Used, for example, in the Upgrade utility to enter the domain name.

encapsulated PostScript (EPS)

A file format optimized for moving PostScript files between applications.

equivalence-name

The node name portion of a file server name.

error alert

A message from the Advanced Server about local area network or system errors. Error alerts are stored in the error log.

Ethernet address

An alphanumeric string, six bytes in length, that identifies a node on the Ethernet. The string is six pairs of hexadecimal digits, separated by hyphens (for example, AA-00-04-00-91-27).

event

Any significant occurrence in the system or in an application that requires users, operators, or administrators to be notified, or an entry to be added to a log.

EventLog service

The Advanced Server service that records events in the system, security, and application event log files.

export path

In directory replication, a path from which subdirectories, and the files in those subdirectories, are automatically copied from an export server. *See also* **directory replication**.

export server

In directory replication, a server from which a master set of directories is copied to specified servers or workstations (called import computers) in the same or other domains. *See also* **directory replication**.

extended character sets

Character sets that define 16-bit character mappings for values 0 to 255, and so are much more extensive than, for example, the conventional 7-bit ASCII set, which maps characters to values 0 to 127, and is limited to the standard characters of the English and Western European languages. Extended character sets can be used to encode more characters to support a wider variety of languages. The Advanced Server for OpenVMS can be configured to support one of several ISO-8859 character sets. The PATHWORKS for OpenVMS (Advanced Server) only supports ISO-8859-1 (ISO Latin-1). *See also* **Unicode.**

Extended File Specifications

On OpenVMS Alpha systems, provides deep directories and extended file names support. Deep directories support allows network clients to use an hierarchical arrangement of directories and files on the OpenVMS disk similar to the client-based disk. Extended file names support uses the On-Disk Structure (ODS-5), extending OpenVMS file name restrictions to support longer file names and adding extended character set characters to the supported character set. *See also* **ODS-5**.

external authentication

Allows users to log on to the OpenVMS operating system using their Advanced Server user names and passwords. This feature is useful to OpenVMS system managers who want to provide users with a single username and password combination for both OpenVMS login and Advanced Server network logon. *See also* **pass-through authentication**.

FAT

File allocation table. File system structure used by the MS-DOS operating system.

file extension

Any characters that follow a period at the end of a file name. A file extension usually identifies the file's type.

File Index Table (FIT)

A file name lookup table (with the .FIT extension) that consists of file translation pairs. FIT files map path names entered on a client workstation to the actual files on the server.

file name

The unique name that identifies a file. *See also* **file extension**.

file server

A system that enables a server to allow access to its local resources.

frame

A packet of information transmitted as a single unit. Every frame has the same basic organization and contains control information, such as synchronizing characters, station address, and an error-checking value, as well as a variable amount of data.

full name

A user's complete name, usually consisting of the last name, first name, and middle initial. Under the Advanced Server, the full name can be maintained as part of the information that identifies and defines a user account. *See also* **user account**.

full synchronization

Domain synchronization in which the primary domain controller replicates its domain databases (security databases) in their entirety to the backup domain controllers. *See also* **domain synchronization** and **partial synchronization.**

global account

A normal user account in a user's home domain. Most user accounts are global accounts. *See also* **local account** and **user account**.

global group

A user group that can be employed to define permissions and rights for accessing resources in its own domain and in trusting domains. A global group can contain user accounts only from its own domain. Global groups can become members of local groups. Global groups are a mechanism for creating sets of users that are available for use both in the domain where they are created and in other domains. *See also* **group** and **local group**.

group

A collection of user accounts that are called members. The permissions and rights granted to a group are also granted to its members, making groups a convenient way to grant common capabilities to collections of user accounts. *See also* **global group** and **local group**.

group memberships

The groups to which a user account belongs. Permissions and rights granted to a group are also granted to its members. In most cases, the actions a user can perform are determined by the group memberships of the user account through which the user logs on.

group name

A unique name identifying a local or global group to the Advanced Server. A group's name cannot be identical to any other group name or user name of its own domain or workstation. *See also* **group**.

guest account

An account on a server that a user without an individual user account can use to access the server's resources.

hidden server

A server that is part of a domain, but that does not appear in the list of servers.

hidden share

A share that is hidden from most network users. Hidden shares include ADMIN$, IPC$, and disk administrative shares. *See also* **shared directory.**

home directory

A directory that is accessible to a user and that contains files and programs for the user. A home directory can be assigned to an individual user or can be shared by many users.

Host mapping

The mapping (association) of an OpenVMS user account with an Advanced Server user account. When using external authentication to log on to an OpenVMS account, the host mapping determines the OpenVMS user name. *See* **external authentication.**

host system

A computer, such as an OpenVMS system, that runs the server services.

import computers

In directory replication, the servers or workstations that receive copies of the master set of directories from an export server. *See also* **directory replication**.

import path

In directory replication, the path to which imported subdirectories, and the files in those subdirectories, are stored on an import computer. *See also* **directory replication**.

inherited permissions

Implicit permissions based on permissions assigned to a parent directory. *See also* **permissions**.

Internet address

A 32-bit number identifying a host connection on the Internet. An Internet address consists of a network number and host number.

interprocess communications (IPC)

Communication among the component processes of a program, between different computers running parts of a single program, or between two programs working together.

IPC$

An administrative resource that controls how interprocess communications operate on servers. A server's IPC$ is automatically shared and cannot be deleted. *See also* **ADMIN$** and **C$.**

ISO Latin-1

A character set, also called ISO-8859-1. *See also* **extended character sets.**

keyword

On PATHWORKS V6 for OpenVMS (Advanced Server) only, a parameter name in the LANMAN.INI file that, with an associated value, establishes some aspect of server configuration.

LAN

Local area network. A self-contained network that offers a high-speed, reliable communications channel. LANs span a limited distance, such as a building or cluster of buildings, but can be connected to WANs with bridge devices. *Contrast with* **WAN**.

LAN Manager

A Network Operating System (NOS) from Microsoft that manages network tasks and coordinates communications between clients and servers.

LANMAN.INI file

On PATHWORKS V6 for OpenVMS (Advanced Server) only, an initialization file on each server and client. The values of the keywords in this file determine the option settings for computers on the network.

License Manager

The interface used to manage the Advanced Server License Server. The License Manager provides the ability to manage license groups, set alert levels, set logging levels for licensing events, enable or disable the License Server, and revoke assigned licenses.

License Manager Facility (LMF)

The OpenVMS facility that manages the product license database through a callable interface.

License Registrar

A component of the Advanced Server licensing subsystem that runs on the same node as the file server and validates whether a client is licensed to connect to the file server.

License Server

An Advanced Server software program that performs license-related services, such as assigning and verifying licenses.

License Server state file

The database on the system running the License Server. Includes client names, information about the types and quantities of licenses available, and license group information.

list box

In a dialog box, a box that lists available choices such as all the files in a directory. If the available choices do not fit in the viewable portion of the list box, a scroll bar allows users to move up and down the list.

LMHOSTS

LMHOSTS name resolution allows the server to resolve NetBIOS names by looking them up in a local database (the LMHOSTS file) that maps NetBIOS names to TCP/IP addresses. *Contrast with* **WINS** and **DNS**.

local account

A user account provided in a domain for a user whose global account is in a non-trusted domain. Not required where trust relationships exist between domains. *See also* **global account** and **user account**.

local area network

See **LAN**.

local boot

A process in which a client operating system is loaded and started locally from disk. *Contrast with* **remote boot**.

local computer

The workstation or server at which the user or administrator is currently working. *Contrast with* **remote computer**.

local group

For a backup domain controller, a user group that can be used to grant permissions and rights only for the servers of its own domain. A local group can contain user account names and global group names both from its own domain and from trusted domains. Local groups are a device for creating sets of users from both inside and outside the domain, to be used only at servers of the domain.

For a member server, a local group is one that can be granted permissions and rights only for the member server. However, it can contain user accounts from its own computer, and user accounts and global groups both from its own domain and from trusted domains. Local groups are a device for creating sets of users from both inside and outside the member server, to be used only at the member server.

See also **global group** and **group**.

local printer

A printer that is directly connected to one of the ports on a computer.

local user

The user or administrator working at the local computer.

lockout

A security feature that disables a user account if failed logon attempts exceed a specified limit.

log file

A history file. Advanced Server maintains a system log and optionally enabled security and application logs.

log on

To provide a user name and password to gain access to the network.

logical drive

On a PC, anything given a drive designation (for example, G:) that is not physically located on the system.

logon domain

The domain specified when a user logs on to the local area network.

logon hours

The days and times during which a user can access a server's resources.

logon restrictions

The logon hours during which a user can access a server's resources, and the workstations from which the user can access those resources.

logon script

A batch program containing Advanced Server and operating system commands used to configure workstations. Logon scripts can be written for one or more users. When the user logs on, the logon script is run.

logon script path

The path or location where the logon script is stored, if a logon script is assigned to the user's account.

logon security

A means of verifying the identity of users when they log on to the local area network or wide area network. *See also* **NetLogon service**.

logon server

For a domain, the primary domain controller and backup domain controllers. For a user, the server that processes the user's logon request — typically the server with the lightest load. *See also* **NetLogon service**.

logon validation

A process of verifying the identities of users when they log on to the network. *See also* **Netlogon service**.

logon workstations

The workstations from which a user is allowed to log on.

Master Browser

The system that maintains an authoritative browse list (the set of information required for the Browser service.) The Master Browser polls for domains, and builds and updates a master browse list of its domain. One or more backup Browsers send requests to the Master Browser to update their own lists.

maximum password age

The period of time a password can be used before the system requires the user to change it. Set in the account policy.

member server

A server in a domain that 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. *See also* **backup domain controller** and **primary domain controller.**

message forwarding

The method used to reroute messages from one client or server to another.

minimum password age

The period of time a password must be used before the user can change it. Set in the account policy.

Mixed-mode domain

A Windows 2000 domain that contains both Windows 2000 domain controllers and Windows NT or HP Advanced Server domain controllers. *Contrast with* **Native-mode domain**.

mount

To make a disk available as a shared disk to users on a network.

multi-master domain controller model

The model of domain security management implemented by pure Windows 2000 environments. Changes to the security accounts database can be made on any domain controller. Any domain controller can be the replicator, sending copies of the updated security accounts database to the other domain controllers. This model contrasts with the primary/backup domain controller model used by the Advanced Server and Windows NT Servers, in which changes must be made on the primary domain controller first, which replicates the changes to the backups.

named pipe

An interprocess communication mechanism that allows one process to communicate with another local or remote process.

Native-mode domain

A Windows 2000 domain whose domain controllers are Windows 2000 systems exclusively. *Contrast with* **Mixed-mode domain**.

NetLogon service

Performs authentication of domain logons, and keeps the domain's database synchronized between the primary domain controller and the backup domain controllers in the domain. *See also* **security accounts database**.

NetBEUI

A network transport on the Advanced Server. The term NetBEUI is derived from NetBIOS Extended User Interface.

NetBIOS

Network Basic I/O System interface device driver and transport interface developed by Microsoft and IBM, that allows applications on different computers to communicate within a local area network. In a wide area network, the Advanced Server can use NetBIOS with TCP/IP (in conjunction with LMHOSTS, WINS, or DNS for name resolution) to enable applications to communicate over the network.

network

A group of servers, clients, and devices connected to each other by communications lines in order to share information and resources.

network adapter (or network controller or network interface card)

A combination of hardware, firmware, and software that controls the transmission and reception of data between a workstation or server and the network.

network controller

See **network adapter.**

network directory

See **shared directory.**

network path

The computer name of a server followed by the share name of a shared resource and, optionally, a relative path. *See also* **Universal Naming Convention**.

node

An individual computer, such as a server or client, that can communicate with other computers in a network.

NOS

Network Operating System. *See* **Advanced Server**.

NT File System (NTFS)

Windows NT file system. A file system designed for use specifically within the Windows NT operating system.

object type

An entity shared by the server, such as a file, directory, or printer.

ODS-2

The traditional OpenVMS file system (On-Disk Structure), which is based on the Files-11 disk structure.

ODS-5

The optional extended file system supported on OpenVMS systems (beginning with Version 7.2) which provides Extended File Specifications and deep directories.

On-Disk Structure (ODS)

The structure of applications and files maintained by the Advanced Server.

OpenVMS Registry

A system-wide hierarchical database of configuration information about hardware and software (both the operating system and applications). The Advanced Server for OpenVMS software relies on the OpenVMS Registry to store and reference server configuration parameters. In previous versions of the server software — for example, PATHWORKS for OpenVMS servers — the LANMAN.INI file is used to store server parameters. The OpenVMS Registry is similar to the Windows NT Registry. *See also* **server configuration parameters**.

operator privilege

The privilege granted to a user that allows the user to perform certain administrative tasks.

partial synchronization

Domain synchronization in which the primary domain controller replicates to a backup domain controller only those elements in their domain databases (security databases) that have been changed since the last time a domain synchronization occurred. *See also* **domain synchronization** and **full synchronization.**

partition

A virtual division of a physical disk that functions as though it were a physically separate unit.

pass-through authentication

In a trust relationship, a user with an account in one domain can access resources provided by another domain that trusts the user's domain. *See also* **external authentication**.

path

Specifies the location of a file within the directory structure. For example, to specify the path of a file in the WINDOWS directory on drive C, a user types C:\WINDOWS\.

path name

A path that ends in a file name. A path specifies a directory; a path name specifies a file. For example, to specify the path name of a file named README.WRI located in the WINDOWS directory on drive C, a user types C:\WINDOWS\README.WRI.

pause

To suspend a service. When a service is paused, current requests are not stopped, but new requests are not allowed.

PC

Personal computer. *See* **client**.

permissions

Settings that define the type of access a user has, and the actions a user can take, with regard to specific objects. Permissions apply to these types of objects: shares, printers, directories and the files in them. Special access combines permissions for directory and file access.

personal share

A share typically used for sharing a user's OpenVMS login directory, pointing to the root directory of the user's OpenVMS account. Personal shares are unique in that they are hidden shares (they will not appear in the list of shares users can display, such as in Network Neighborhood), but their names do not end with a dollar sign ($). Thus, when a user wishes to map a drive to their OpenVMS login directory, they specify their personal share name (typically the same as their username) without having to include a dollar sign in the share name. *See also* **shared directory.**

personal computer

See **client.**

pipe

See **named pipe.**

port

A connection or socket used to connect a device, such as a printer, monitor, or modem, to a computer.

primary domain controller (PDC)

The server that maintains the master copy of the domain's security accounts database. The primary domain controller also validates logon requests. *Contrast with* **backup domain controller**, **member server**.

printer driver

A program that controls how a computer and printer interact. *See also* **device driver**.

printer fonts

Fonts that are built into a printer. These fonts are usually located in the printer's read-only memory (ROM).

print queue

A list of print jobs waiting to be sent to a printer or pool of printers. The Advanced Server print queue can be either a printer queue or routing queue. *See also* **printer queue**, **routing queue**.

printer queue

A print queue that points directly to a physical printer. It is equivalent to an OpenVMS execution queue. *See also* **print queue.** *Contrast with* **routing queue.**

print share

See **shared printer.**

priority level

An attribute assigned to each print queue that determines which job is processed first when several queues are trying to access the same printer at the same time.

privilege

See **user privilege.**

privilege level

A characteristic of a user group that defines the range of actions that members can perform on the network. *See also* **permissions**.

Product Authorization Key (PAK)

The vehicle for delivering HP product licenses. A PAK authorizes the use of the licensed software, identifies the license type, and represents either one or multiple licenses.

profile

See **user profile.**

program file

A file that starts an application or program.

program group

A collection of applications on a PC. Grouping applications makes them easier to find when a user wants to start them.

program-item icon

An application, accessory, or document represented as an icon in a group window on a PC.

protocol

A set of rules that governs the format and timing of messages sent and received over a communications link. For example, DECnet and TCP/IP are network protocols. *See also* **transport**.

radio button

In a dialog box, an indicator that the user can select or clear, where only one selection is allowed. *Contrast with* **check box**.

record management services (RMS)

An OpenVMS file management system that offers more sophisticated features than the default system. RMS supports three forms of file organization and three forms of file access. *See also* **On-Disk Structure**.

refresh

To update displayed information with current data.

Registry server

The OpenVMS Registry server controls all OpenVMS Registry operations, such as creating and backing up the OpenVMS Registry database, and creating, displaying, modifying, or deleting keys and values. *See also* **OpenVMS Registry**.

remote administration

Administration of one computer by an administrator logged on at another computer that is connected to the first computer across the network.

remote boot

The process by which a client's operating system is loaded and started remotely from a server's disk. *Contrast with* **local boot**.

Remote Boot service

A LAN Manager service that provides software support for starting workstations over the local area network.

remote computer

A server or workstation that is available over the network. *Contrast with* **local computer**.

remote procedure call (RPC)

A call from a distributed application for services available on various computers in a network. An RPC is used during remote administration of computers.

replication

See **directory replication.**

resource

Any disk drive or directory, printer, modem, image scanner, or other object that a server can share over a network. *See also* **shared resource**.

revision level

A revision identifier that is built into many Advanced Server structures, such as security descriptors and access control lists (ACLs). This identifier enables a structure to be passed between systems or stored on disk even though it is expected to change in the future.

rights

Authorization of a user to perform certain actions on the system. Rights apply to users and groups on a system-wide basis and are different from permissions, which apply to specific objects. *Contrast with* **permissions**.

routing queue

An Advanced Server print queue that points to several printer queues to distribute printer workload among several like printers. Equivalent to an OpenVMS generic queue. A print job is routed to the first available printer through that printer's queue. *See* **print queue**. *Contrast with* **printer queue.**

SAM

Security account manager. An Advanced Server protected subsystem that maintains the server security accounts database. Includes security information (such as user account names and passwords) and the settings of the security policies.

SAM database

See **security accounts database**.

scroll

To move through text or graphics (up, down, left, or right) to see parts of the file that cannot fit on the screen.

scroll bar

A bar that appears at the right or bottom edge of a window or list box that enables users to view contents that are not completely visible. *See also* **scroll**.

security

A method of controlling access to network resources.

security accounts database

The file that contains security information such as user accounts and passwords, and groups, and the settings of the security policies. This domain-wide database is stored on all domain controllers and used for logon validation. The master domain-wide security accounts database is stored on the primary domain controller; backup domain controllers store a copy of the master database. The backup domain controller copies are synchronized with the master copy on the primary domain controller. On the Advanced Server, the security accounts database is managed with the ADMINISTER command interface.

Also referred to as the **SAM database**, **security database**, or **domain database**. *See also* **logon validation**, **Netlogon service**.

security database

See **security accounts database**.

security ID (SID)

A unique value that identifies a user to the security system. Security IDs (SIDs) can identify one user or a group of users. Server SIDs identify servers within the network, enabling the network to recognize the primary domain controller.

security log

A file that records security events. *See also* **event**.

security policies

A selection of security models. For an Advanced Server domain, the security policies consist of the Account, User Rights, Audit, and Trust Relationships policies.

security token

See **access token.**

separator page

One or more cover sheets generated before a print job; also called a banner page.

server

A computer on the network that provides access to resources such as files, printers, and communications devices. *Contrast with* **client**.

server configuration parameters

Parameter names used by the Advanced Server to define certain aspects of the server configuration. The Advanced Server for OpenVMS server configuration parameters are stored in the OpenVMS Registry. Previous versions of the server software — for example, PATHWORKS for OpenVMS servers — use the LANMAN.INI file to store server parameters.

Server service

The Advanced Server software component that enables a computer to share resources on the network and that provides administrators with tools for controlling and monitoring resource use.

server-based license

A license assigned on a first-come, first-served basis that allows a client to access the resident file server only. Often referred to as a "concurrent use" license. *Contrast with* **client-based license.**

services

The main components of the server software. The basic service is the server service, which allows a computer to share network resources.

session

A link between a workstation and a server. More than one user session can be established over a network (machine to machine) connection. A session consists of one or more user connections to shared resources. *Contrast with* **connection**.

share

See **shared directory, shared printer, shared resource**.

share name

The name of a shared resource.

share permissions

Information the user can specify to control the type of access that the user or group has to all files and directories residing on that share. *See also* **directory access permissions** and **special access permissions**.

share-level security

In LAN Manager, a type of security that limits access to each shared resource by requiring a password. Permissions are assigned to the resource rather than to the user. *See also* **permissions** and **user-level security**.

shared directory

A directory to which network users can connect.

shared network directory

See **shared directory.**

shared file

A file in a shared directory, accessible to network users. *See* **shared directory.**

shared printer

A printer to which network users can print.

shared resource

Any device, data, or program that is used by more than one other device or program. For the Advanced Server, shared resources refer to any resources that are made available to network users, such as directories, files, and printers.

SID

See **security ID.**

SNMP Service

A service that allows a server to report its current status to a Simple Network Management Protocol (SNMP) or a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

source directory

The directory that contains the file or files that a user intends to copy or move. *Contrast with* **destination directory**.

special access permissions

A combination of individual permissions that can be set on files and directories. *See also* **directory access permissions** and **share permissions**.

standalone License Server

The configuration of software that includes the License Server without the file servers. *Contrast with* **file server**.

standalone logon

A logon request that is not validated by a logon server. In domains without logon security, each logon request is granted standalone logon. In domains with logon security, a logon request with a user name not found in the domain's security accounts database is granted standalone logon. *See also* **logon security** and **logon server**.

standalone server

A server that has its own (local) user accounts database (as opposed to a domain security database) and does not participate in logon security. *See also* **member server**.

status bar

A line of information related to the application in the window, usually located at the bottom of a window.

subdirectory

An entity that groups files within a directory or subdirectory. *See also* **directory**.

syntax

The order in which a user must type a command and the elements that follow the command. Advanced Server commands can have the following elements: command name, parameters, qualifiers, keywords, and values.

TCP/IP

Transmission Control Protocol/Internet Protocol. A network transport. Also a set of protocols that governs the transport of information between computers and networks of dissimilar types. *See also* **transport**.

time server

The computer with which other computers on the network synchronize their system time. For Advanced Server, a server designated to run the TimeSource service for its domain.

token

See **access token**.

transport

The software feature that allows OpenVMS systems to communicate using protocols. *See also* **protocol**.

trust relationship

Links between domains that enable pass-through authentication, in which a user has a user account in one domain, yet can access resources in another domain.

UCS-2

See **Unicode**.

Unicode

An extensive character coding system designed to support the interchange, processing, and display of the written texts of the diverse languages of the modern world. Unicode UCS-2 provides a unique 16-bit value for every character or glyph, independent of the platform, application, or language, and does not require the use of complex modes or escape codes. *See also* **extended character sets**.

Universal Naming Convention (UNC)

A standard way of representing a network path. The server name is preceded by two backslashes and followed by one backslash and the sharename, along with a path name; for example, \\SERVER\SHARE1\SHARE2.

Upgrade utility

An Advanced Server utility for upgrading server information from PATHWORKS V5 for OpenVMS (LAN Manager) to PATHWORKS V6 for OpenVMS (Advanced Server).

user account

A record on a server or in a domain that contains information about authorized users. *See also* **global account** and **local account**.

user default profile

The user profile that is loaded by a server when a user's assigned profile cannot be accessed, such as when a user without an assigned profile logs on to the computer for the first time, or when a user logs on to the Guest account.

user-level security

A type of security in which a user account is set up for each user. Permissions are granted to each user for specific resources, defining exactly what actions each user can take with each resource. *See also* **permissions** and **share-level security**.

user name

The user account name a user types when logging on to the system.

user privilege

An OpenVMS security mechanism that defines the type of access users have to a file or directory. *See also* **permissions** and **privilege level**.

user profile

The set of information that describes a user's operating environment, including workstation name, logon hours, and default path.

user rights

Definition of the access rights that users have to server resources.

User Rights policy

A method for managing the assignment of rights to groups and user accounts. *See also* **rights**.

virtual memory

Space on a hard disk that the operating system uses as if it were actually memory.

virtual printer memory

In a PostScript printer, a part of memory that stores font information.

WAN

Wide area network. A network configuration that covers an extended geographical area. A WAN consists of multiple LANs. *Contrast with* **LAN**.

Windows NT

The network operating system from Microsoft that replaces DOS and that can act as a server as well as a client.

WINS

Windows Internet Name Service, a service that registers and resolves names for NetBIOS clients on TCP/IP to dynamic addresses assigned by the Dynamic Host Configuration Protocol (DHCP). The Advanced Server can be configured as a WINS client, using a specified WINS server for NetBIOS name resolution in a wide area network. *Contrast with* **DNS** and **LMHOSTS**.

Windows NT-compatible print management

A feature of the Advanced Server for OpenVMS (V7.3 or later) allowing administrators to manage Advanced Server print shares from a Windows NT system. For Advanced Server for OpenVMSs prior to V7.3, and all versions of PATHWORKS for OpenVMS (Advanced Server), print shares can only be managed using the Advanced Server ADMINISTER user interface.

workgroup

A collection of computers that are grouped for viewing purposes. Each workgroup is identified by a unique name. *See also* **domain**.

workstation

A personal computer or client in the network. For example, Windows NT computers are called workstations.

Index

A

B

C

D

E

F

G

H

L

M

N

O

P

R

S

T

U

W