

HP OpenVMS CIFS Version 1.1 Administrator's Guide



© Copyright 2008 Hewlett-Packard Company, L.P

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group.

Table of Contents

About This Document.....	9
Intended Audience.....	9
Document Organization.....	9
Typographic Conventions.....	10
HP Encourages Your Comments.....	10
 1 Introduction to the HP CIFS Server.....	11
Introduction to HP CIFS Server.....	11
What is the CIFS Protocol?.....	11
The Open Source Software (OSS) Samba Suite.....	11
Open Source Software.....	11
Samba Server Description and Features.....	12
HP CIFS Server Documentation: Online.....	12
HP CIFS Server Directory Structure.....	13
 2 Installing and Configuring the HP CIFS Server.....	15
HP CIFS Server Requirements and Limitations.....	15
Disk Space Requirements.....	15
Software Requirements.....	15
About the Release Notes.....	16
Preinstallation Tasks	16
OpenVMS Cluster Considerations.....	18
Installing HP CIFS Server Software.....	20
Upgrading HP CIFS Server Software.....	20
Moving the SAMBA\$ROOT Directory.....	21
Postinstallation Tasks.....	22
Configuring HP CIFS Server.....	23
Configuring a Cluster with Common SAMBA\$ROOT: Directory.....	23
Configure HP CIFS Using Samba Web Administration Tool (SWAT)	23
HP CIFS Configuration File.....	24
Configuration File Structure.....	24
Section Description.....	24
Verify the Configuration File.....	25
Supported Backend.....	26
Configuring SMB.CONF File in Cluster Environment.....	26
Configure SMB.CONF for OpenVMS File Format Support.....	27
Configuration Setting for International Character Set.....	27
Starting and Stopping the HP CIFS Server.....	28
Starting HP CIFS Server Manually.....	28
Starting HP CIFS Server When System Boots.....	28
Starting HP CIFS Server in an OpenVMS Cluster	28
Stopping HP CIFS Server.....	29
Troubleshooting Installation and Configuration Issues.....	29
Verifying the Client Connection.....	31
Other HP CIFS Server Configuration Issues.....	32
Performance Tuning.....	32
Special Concerns when Using HP CIFS Server on a Network File System (NFS)	33
NetBIOS Names Are Not Supported on Port 445.....	33
VMS Specific Configurations.....	33

Uninstalling the HP CIFS Server Software.....	34
3 HP CIFS Deployment Models.....	35
Domain Roles.....	35
Primary Domain Controllers.....	35
Backup Domain Controllers.....	35
Advantages of Backup Domain Controllers.....	35
Domain Member Servers.....	35
Samba Domain Model.....	36
Samba Domain Components.....	37
HP CIFS Server Acting as a PDC.....	38
Limitations.....	39
HP CIFS Server Acting as a BDC.....	39
Synchronizing the Account Database between the BDC and the PDC.....	40
HP CIFS Server Acting as a Member Server.....	40
Configure the HP CIFS Server as a Standalone Server.....	40
A sample SMB.CONF file for an HP CIFS Server as a Standalone Server.....	41
Configure the HP CIFS Server as a PDC.....	41
Join a Windows Client to a HP CIFS Domain.....	41
Step-by-step Procedure.....	41
Adding an HP CIFS Server to a Domain.....	42
Windows Domain Model.....	43
Components for Windows Domain Model.....	44
An Example of the ADS Domain Model.....	44
A sample SMB.CONF file For an HP CIFS ADS Member Server.....	45
Roaming Profiles.....	47
Configuring Roaming Profiles.....	47
Configuring User Logon Scripts.....	47
Trust Relationships.....	48
Establishing the Trust in the Trusted Domain.....	48
Establishing the Trust in the Trusting Domain.....	48
Viewing List of Trusts.....	49
Establishing a Two-way Trust Relationship between an HP CIFS Domain and a Windows Active Directory Domain.....	49
Validating the Trust Relationships.....	51
4 LDAP Integration Support.....	53
Overview.....	53
HP CIFS Server Advantages.....	53
Network Environments.....	53
Domain Model Networks.....	54
HP CIFS Server Acting as Primary Domain Controller (PDC).....	54
HP CIFS Server Acting as Backup Domain Controller (BDC) to Samba PDC.....	54
HP CIFS Server Acting as the Member Server.....	54
Workgroup Model Networks.....	54
The CIFS Authentication with LDAP Integration.....	54
Installing and Configuring Your Directory Server.....	55
Installing the Directory Server.....	55
Configuring the Directory Server.....	55
Configuring the HP CIFS Server.....	57
LDAP Configuration Parameters.....	57

5 Winbind Support.....	59
Overview.....	59
Winbind Features.....	60
Winbind Process Flow.....	61
Winbind Functionality.....	62
User and Group Mapping.....	63
User Authentication and Host Mapping Process Flow.....	63
Group Mapping Process Flow.....	64
Disabling Winbind.....	65
Configuring HP CIFS Server with Winbind.....	65
Winbind Configuration Parameters.....	65
A SMB.CONF Example.....	66
LDAP Backend Support	66
wbinfo Utility.....	66
 6 Managing Users, Groups, and File Access.....	 67
Introduction.....	67
Managing Local Users in Member Server or PDC or BDC.....	67
Managing Local Groups in Member Server	68
Managing Groups in PDC or BDC	70
Username Mapping.....	71
Managing HP CIFS Security.....	72
Managing File and Directory Protections	72
Managing File and Directory ACLs	74
 7 Configuring Printers.....	 77
Introduction.....	77
Configuring a Printer Share.....	77
Creating the Spool Directory.....	77
Queue Setup.....	78
DCPS Print Queues.....	78
TCPIP\$TELNETSYM Print Queues.....	78
LPD Print Queues.....	79
LPD Print Queue Setup.....	79
Installing Printer Drivers.....	80
Manual Driver Installation.....	80
Automatic Driver Installation.....	80
Creating the PRINT\$ Share.....	81
 8 Tool Reference.....	 83
HP CIFS Management Tools.....	83
smbpasswd	84
Syntax.....	84
Examples.....	85
pdbedit	85
Syntax.....	85
Examples.....	88
net	88
Net Commands.....	88
Syntax for net lookup.....	89
Examples.....	89
Syntax for net user.....	89

Examples.....	90
wbinfo	91
Syntax.....	91
Examples.....	92
smbclient.....	93
Syntax.....	93
Examples.....	94
smbstatus.....	95
Syntax.....	95
Examples.....	95
nmblookup.....	96
Syntax.....	96
Examples.....	97
smbshow.....	97
Examples.....	97
Smbver.....	98
Example.....	98
SAMBA\$DEFINE_COMMANDS.COM.....	98
SAMBA\$GATHER_INFO.COM.....	98
testparm.....	98
Syntax.....	98
Example.....	99
tdbbackup.....	99
Syntax.....	99
Tdbdump.....	100
Syntax.....	100
smbcontrol.....	100
Syntax.....	100
Example.....	101
 A Sample Installation and Removal Procedures.....	103
Sample Installation on OpenVMS Integrity server Systems.....	103
Sample Removal Procedure on OpenVMS Integrity server Systems.....	105
 Index.....	107

List of Figures

3-1	Standalone HP CIFS Server as a PDC.....	36
3-2	Standalone HP CIFS Server as a PDC with EDS backend.....	37
3-3	Multiple HP CIFS Servers with EDS backend.....	37
3-4	Windows Domain.....	44
3-5	An example of the ADS Domain Model.....	45
3-6	Direction of Trust.....	50
3-7	Active Directory.....	51
4-1	CIFS Authentication with LDAP Integration.....	55
5-1	Winbind Process Flow.....	61
5-2	User Authentication and Host Mapping Process Flow.....	63
5-3	Group Mapping Process Flow.....	64
6-1	Modifying ACE Permissions.....	73

List of Tables

1	Typographic Conventions.....	10
1-1	Files and Directory Description.....	13
2-1	Files Retained During Installation.....	21
2-2	SYSMAN Utility.....	29
4-1	Global LDAP Parameters.....	57
5-1	Global Parameters.....	65

About This Document

This document describes how to install, configure, and administer the HP CIFS Server product. It augments *The Samba HowTo Collection* and *Using Samba, 2nd Edition* books supplied with the HP CIFS Server product and provides additional OpenVMS variations, features, and recommendations.

Intended Audience

This document is intended for OpenVMS system administrators and network administrators. For more information about the HP CIFS Server, see the HP CIFS Server documentation:

<http://h71000.www7.hp.com/doc/CIFS.html>

Document Organization

The document is organized as follows:

- | | |
|------------|--|
| Chapter 1 | Introduction to the HP CIFS Server Introduces the HP CIFS Server architecture, summarizes the available documentation resources, and provides the product roadmap. |
| Chapter 2 | Installing and Configuring the HP CIFS Server Describes the procedure to install and configure the HP CIFS Server. |
| Chapter 3 | HP CIFS Deployment Model Describes how to configure the roles that an HP CIFS Server can play in an NT style domain, whether it is a Samba Domain model, consisting solely of HP CIFS Servers, or as an NT Domain with a Microsoft NT Primary Domain Controller (PDC). |
| Chapter 4 | LDAP Integration Support Describes how to install, configure, and verify the HP Enterprise Directory, HP LDAP Integration product, and HP CIFS Server software with LDAP feature support. |
| Chapter 5 | Winbind Support Describes how to set up and configure the HP CIFS Server with the winbind support. |
| Chapter 6 | Managing Users, Groups, and File Access Describes how to manage users and groups on the HP CIFS Server. This chapter also describes how to set and modify file access controls either from the OpenVMS host or from a Windows domain member. |
| Chapter 7 | Configuring Printers Describes how to configure Print Services on systems running HP CIFS Server software. |
| Chapter 8 | Tool Reference Describes some of the management tools included with HP CIFS for OpenVMS, including many native Samba utilities such as <code>pdbedit</code> and <code>smbclient</code> . |
| Appendix A | Sample Installation and Removal Procedure Provides sample installation and removal procedures for HP CIFS Server. |

Typographic Conventions

Table 1 lists the typographic conventions used in the document.

Table 1 Typographic Conventions

Convention	Description
...	A horizontal ellipsis in a figure or example indicates the following possibilities: <ul style="list-style-type: none">• Additional optional arguments in a statement have been omitted.• The preceding item or items can be repeated one or more times.• Additional parameters, values, or other information can be entered.
...	A vertical ellipsis indicates the omission of items from a code example or command format; the items are omitted because they are not important to the topic being described.
()	In command format descriptions, parentheses indicate that you must enclose choices in parentheses if you specify more than one. In installation or upgrade examples, parentheses indicate the possible answers to a prompt, such as: <code>Is this correct? (Y/N) [Y]</code> .
[]	In command format descriptions, brackets indicate optional choices. You can choose one or more items or no items. Do not type the brackets on the command line. However, you must include the brackets in the syntax for OpenVMS directory specifications and for a substring specification in an assignment statement.
{}	In command format descriptions, braces indicate required choices; you must choose at least one of the items listed. Do not type the braces on the command line.
Example	This typeface indicates code examples, command examples, and interactive screen displays. In text, this type also identifies website addresses, OpenVMS command and pathnames, PC-based commands and folders, and certain elements of the C programming language.
<i>italic type</i>	Italic type indicates important information, complete titles of manuals or variables. Variables include information that varies in system output (for example, Internal error number), in command lines (/PRODUCER=name), and in command parameters in text (where dd represents the predefined code for the device type).
UPPERCASE TYPE	Uppercase indicates the name of a command, routine, file, file protection code, or the abbreviation of a system privilege.
-	A hyphen at the end of a command format description, command line, or code line indicates that the command or statement continues on the following line.
WARNING	A warning calls attention to important information that if not understood or followed will result in personal injury or nonrecoverable system problems.
CAUTION	A caution calls attention to important information that if not understood or followed will result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	This alert provides essential information to explain a concept or to complete a task.
NOTE	A note contains additional information to emphasize or supplement important points of the main text.

HP Encourages Your Comments

HP encourages your comments and suggestions on this document. Please send comments to: openvmsdoc@hp.com

1 Introduction to the HP CIFS Server

This chapter introduces you to the HP CIFS Server. This chapter addresses the following topics:

- “The Open Source Software (OSS) Samba Suite”
- “HP CIFS Server Documentation: Online”
- “HP CIFS Server Directory Structure”

Introduction to HP CIFS Server

The HP CIFS Server provides OpenVMS with a distributed file system based on the Microsoft Common Internet File System (CIFS) protocols.

The current HP CIFS Server is based on the established open source software Samba, version 3.0.28a and provides file and print services to CIFS clients including Windows 2000, 2003, XP, and Vista.

What is the CIFS Protocol?

CIFS, or the Common Internet File System, is the Windows specification for remote file access. CIFS had its beginnings in the networking protocols, sometimes called Server Message Block (SMB) protocols, that were developed in the late 1980s for PCs to share files over the then nascent Local Area Network technologies (for example, Ethernet). SMB is the native file-sharing protocol in the Microsoft Windows systems and the standard way that millions of PC users share files and printers across corporate intranets.

CIFS is simply a renaming of SMB; and CIFS and SMB are, for all practical purposes, one and the same. (Microsoft now emphasizes the use of "CIFS," although references to "SMB" still occur.) CIFS is also widely available on UNIX, OpenVMS, Macintosh, and other platforms.

Despite its name, CIFS is not actually a file system unto itself. More accurately, CIFS is a remote file access protocol; it provides access to files on remote systems. It sits on top of and works with the file systems of its host systems. CIFS defines both a server and a client: the CIFS client is used to access files on a CIFS server.

HP CIFS provides the CIFS protocol on OpenVMS systems, which enables OpenVMS directories and printers to be accessed from Windows clients.

The Open Source Software (OSS) Samba Suite

The HP CIFS Server source is based on Samba, an Open Source Software (OSS) project developed in 1991 by Andrew Tridgell in Australia. This section includes a brief introduction to the Samba product. Because there are many publications about Samba available online and in most bookstores, HP recommends that you use these source materials, some of which were written by Samba team members, for more detailed information about this product.

Open Source Software

Samba has been made available to HP and other users under the terms of the GNU Public License (GPL). This means that Samba is "free software"; free, that is, of any copyright restrictions. The goal of this type of software is to encourage the cooperative development of new software.

For more information about GNU Public License, see the web address:

<http://www.fsf.org>

Samba Server Description and Features

With the Samba suite of programs, systems running OpenVMS and OpenVMS-like operating systems are able to provide services using the Microsoft networking protocol. This capability makes it possible for Windows machines, using native networking clients supplied by Microsoft, to access a OpenVMS file system and/or printers.

As a user, you will see the OpenVMS file system as a drive-letter or an icon in the "Network Neighborhood" and you will be able to open files from your Windows program as if they are stored on your local system.

To accomplish this, Samba implements the Server Message Block (SMB) networking protocol.

For more information about Samba and its protocols, see *Using Samba* by Robert Eckstein, David Collier Brown, and Peter Kelly.

To access the Samba website, go to <http://www.samba.org>.

HP CIFS Server Documentation: Online

The set of documentation that comprises the information you will need to explore the full features and capabilities of the HP CIFS product consists of non-HP books available at most technical bookstores. For online information, see the *HP OpenVMS CIFS Administrator's Guide*:

<http://h71000.www7.hp.com/doc/CIFS.html>

A list of current recommended non-HP Samba documentation is:

- The Official Samba-3 HOWTO and Reference Guide by John H. Terpstra and Jelmer R. Vernooij, ISBN: 0-13-145355-6.
- Samba-3 by Example Practical Exercises to Successful Deployment by John H. Terpstra, ISBN: 0-13-147221-6.
- Using Samba, 2nd Edition Robert Eckstein, David Collier-Brown, Peter Kelly and Jay Ts. (O'Reilly, 2000), ISBN: 0-596-00256-4.
- Samba, Integrating UNIX and Windows by John D Blair (Specialized Systems Consultants, Inc., 1998), ISBN: 1-57831-006-7.
- Samba website: <http://www.samba.org/samba/docs>.

When using the HP CIFS Server product, HP recommends that you refer to *The Samba HOWTO Collection*, *Samba-3 by Example*, and *Using Samba, 2nd Edition*. All three books are also available through the Samba Web Administration Tool (SWAT).



IMPORTANT: The book *Using Samba, 2nd Edition* describes a previous version of Samba (V.2.0.4). However, much of the information in *Using Samba, 2nd Edition* is applicable to this version of the HP CIFS Server. Readers should always use the SWAT help facility for the most definitive information on the HP CIFS Server.



NOTE:

- Non-HP Samba documentation might include descriptions of features and functionalities planned for future releases of Samba. The authors of these books do not always provide information indicating which features are in existing release and which features will be available in future Samba releases.
 - Not all the features that are available on Samba UNIX/Linux are applicable to HP OpenVMS CIFS. For OpenVMS specific features, see the *HP OpenVMS CIFS Release Notes*.
-

HP CIFS Server Directory Structure

The default base installation directory of HP CIFS Server product is `SAMBA$ROOT`. The HP CIFS configuration files are located in the directory `SAMBA$ROOT:[LIB]`. The HP CIFS Server log files and any temporary files are created in `SAMBA$ROOT:[VAR]`.

Table 1-1 lists the important directories and files that comprise the HP CIFS Server.

Table 1-1 Files and Directory Description

File/Directory	Description
<code>SAMBA\$ROOT:[000000]</code>	This is the base directory for most of the HP CIFS Server.
<code>SAMBA\$ROOT:[SRC]</code>	This directory contains the source code for the HP CIFS Server.
<code>SAMBA\$ROOT:[BIN]</code>	This directory contains binaries for the HP CIFS Server, including daemons and utilities. It also contains command scripts that starts the HP CIFS Server at boot time and stops it at shutdown (if it is configured to do so).
<code>SAMBA\$ROOT:[DOC]</code>	This directory contains documentation in various formats including PS (postscript).
<code>SYS\$COMMON:[SYSHLP]</code>	This directory contains the release notes for the HP CIFS Server.
<code>SAMBA\$ROOT:[SWAT]</code>	This directory contains html and image files for the Samba Web Administration Tool (SWAT).
<code>SAMBA\$ROOT:[VAR]</code>	This directory contains the HP CIFS Server log files and other dynamic files that the HP CIFS Server uses, such as lock files.
<code>SAMBA\$ROOT:[LIB]SMB.CONF</code>	This is the main configuration file for the HP CIFS Server, which is discussed in great detail elsewhere.
<code>SAMBA\$ROOT:[UTILS]</code>	This directory contains OpenVMS Savesets for the SWAT utility.

2 Installing and Configuring the HP CIFS Server

This chapter describes the procedures to install and configure the HP CIFS Server software. This chapter addresses the following topics:

- “HP CIFS Server Requirements and Limitations”
- “About the Release Notes”
- “Preinstallation Tasks ”
- “OpenVMS Cluster Considerations”
- “Installing HP CIFS Server Software”
- “Upgrading HP CIFS Server Software”
- “Moving the SAMBA\$ROOT Directory”
- “Postinstallation Tasks”
- “Configuring HP CIFS Server”
- “Configuration Setting for International Character Set”
- “Starting and Stopping the HP CIFS Server”
- “Troubleshooting Installation and Configuration Issues”
- “Other HP CIFS Server Configuration Issues”
- “Uninstalling the HP CIFS Server Software”

HP CIFS Server Requirements and Limitations

Prior to installing the HP CIFS Server product, verify that your system can accommodate the following product requirements and limitations.

Disk Space Requirements

HP CIFS Server requires approximately 32.68 MB of disk space for installation on the OpenVMS Alpha and 40 MB of disk space on the OpenVMS Integrity servers. The HP CIFS Server is composed of the following components:

- Utility to run and monitor HP CIFS — 92 KB
- Daemon process binaries — 13 MB
- HP CIFS source files (.BCK) — 23 MB
- SWAT Administrator Tool — 13 MB
- Documentation — 1 MB



NOTE: The HP CIFS Server source code files are not required for execution of HP CIFS Server. You can choose not to install them or you can remove them. The source code backup saveset is available at the location SAMBA\$ROOT: [SRC].

Software Requirements

The software requirements for the HP CIFS Server are:

- OpenVMS Alpha Version 8.2 or 8.3
- OpenVMS Integrity servers Version 8.2–1 or 8.3 or 8.3–1H1
- TCP/IP Services or MultiNet or TCPware — the transport software to support the network protocols used by other servers and network clients



NOTE: You must install the latest C RTL (C Run-Time Library) ECO kits before installing the HP CIFS Server kit. The latest C RTL ECO kits can be downloaded from the following web address:

ftp://ftp.itrc.hp.com/openvms_patches

About the Release Notes

The HP CIFS Release Notes document contains important information you must know before installing the product. HP recommends that you read the release notes before you install the product.

To extract the release notes before installation, follow these steps:

1. Load the installation kit on a drive.
2. Enter the following PCSI command, where *file_name.txt* is the name that you specify for the text file, and *directory-path* specifies the disk and directory name for the source drive that holds the HP CIFS Server software (for example, /SOURCE=SYS\$DEVICE:[TEST1]):

```
$ PRODUCT EXTRACT RELEASE_NOTES SAMBA/FILE=file_name.txt/SOURCE=directory-path
```

If the file name is not specified, the release notes are written to a file called CIFS_REL_NOTES.TXT in the current directory. If the destination qualifier is not specified, PCSI extracts the release notes to the current directory.

After the installation completes, you can read the release notes or print the file from SYS\$HELP:CIFS_REL_NOTES.TXT.

Preinstallation Tasks

This section lists the preinstallation tasks you must complete before installing HP CIFS Server software on your system.

Step 1: Check the Network Hardware

HP CIFS Server software runs on OpenVMS Alpha or OpenVMS Integrity server systems that meet the software requirements. The PC Local Area Network (LAN) requires the following:

- A supported network controller board in the server and in each client
- Cables to connect each client and server to the network

Step 2: Log in to the System Account

Before you install the HP CIFS Server software, log in using the system account or another account that has all the privileges enabled to run the installation procedure.

1. At the user name prompt, enter the following:
Username: SYSTEM
2. At the password prompt, enter the password to access the SYSTEM account.

Step 3: Check the Required Software

HP CIFS Server software requires:

- OpenVMS Alpha operating system Version 8.2 or 8.3
- OpenVMS Integrity servers operating system Version 8.2-1 or 8.3 or 8.3-1H1
- TCP/IP or MultiNet or TCPware transport for network communication
- Latest C RTL ECO kit must be installed.

Step 4: Back Up the System

To safeguard against the loss of valuable data, HP recommends that you back up all disks on your system (or at least the system disk) before you install any layered product.

To do a system backup, use the OpenVMS BACKUP command. For more information, see *HP OpenVMS System Management Utilities Reference Manual*.

Step 5: Read the Release Notes

Ensure that you have read the release notes before installing the HP CIFS Server software. For information on accessing release notes, see [“About the Release Notes”](#) (page 16).

Step 6: Check Disk Space

To determine the number of disk blocks required for installation, see [“Disk Space Requirements”](#) (page 15). To check the number of free blocks on the device, where you want to install HP CIFS Server, enter the following command:

```
$ SHOW DEVICE <device-name>
```

The OpenVMS system displays information about the system disk, including the number of free blocks.

For example, to check the free space on the device NEWTON\$DKA0 enter the following command:

```
$ SHOW DEVICE NEWTON$DKA0/unit=bytes
```

Device Name	Device Status	Error Count	Volume Label	Free Space	Trans Count	Mnt Cnt
NEWTON\$DKA0:	Mounted	0	V083	2.58GB	373	1

Step 7: Verifying the TCP/IP Status

Verify the TCP/IP status by entering the following command:

```
$ SYS$STARTUP:TCPIP$STARTUP.COM
```

```
%TCPIP-I-INFO, TCP/IP Services startup beginning at 22-JUL-2008 21:42:28.99
```

```
%TCPIP-I-NORMAL, timezone information verified
```

```
%TCPIP-I-NETSTARTED, network already started
```

```
%TCPIP-S-STARTDONE, TCP/IP Services startup completed at 22-JUL-2008 21:42:30.34
```



NOTE: The above command applies only if the system is running TCP/IP Services for OpenVMS. If you are running MultiNet or TCPWare, see the *MultiNet Installation and Administrator's Guide* and the *TCPware Management Guide* to verify the status of the transport.

Step 8: Check the OpenVMS Cluster Configuration

- Ensure that all cluster members on which the HP CIFS Server software will run are in the same TCP/IP subnet.
- A CIFS cluster is supported only on OpenVMS systems running OpenVMS Version 8.3 or higher. The C RTL for versions of OpenVMS prior to Version 8.3 do not support byte range locking in the FCNTL function. Therefore, files accessed by two or more cluster members simultaneously cannot coordinate byte range locking activity which can result in file corruption.

OpenVMS Cluster Considerations

You can install HP CIFS Server on each node separately in the cluster or on the common disk, which is accessible to all nodes.

If you install HP CIFS Server on each node separately which has separate SAMBA\$ROOT directory tree, it is equivalent to installing HP CIFS Server on standalone servers. In such environments, clusters features such as simultaneous file access through multiple cluster members, load balancing, and failovers are not supported.

In order to support the cluster features, the following prerequisites must be met:

1. All HP CIFS cluster nodes must share a common SAMBA\$ROOT directory tree. By default, HP CIFS Server will be installed on the SYS\$COMMON:[SAMBA] directory. Use the /DESTINATION qualifier of the \$ PRODUCT INSTALL command to install HP CIFS Server on a disk (accessible to all HP CIFS cluster nodes) other than the system disk.
2. A CIFS cluster is supported only on OpenVMS systems running OpenVMS Version 8.3 or higher. The C RTL for versions of OpenVMS prior to Version 8.3 do not support byte range locking in the FCNTL function and, thus, files accessed by two or more cluster members simultaneously cannot coordinate byte range locking activity which can result in file corruption.



IMPORTANT: The information in this document assumes all cluster members are running OpenVMS Version 8.3 or later.

3. Ensure that OpenVMS systems have the latest C RTL (Run-Time Library) ECO installed. There are changes that directly affect the HP CIFS Server behavior and reliability. One source (there are others) for obtaining OpenVMS ECOs is:
http://ftp.itrc.hp.com/openvms_patches
4. A common SYSUAF and RIGHTSLIST database is required.
5. Makeup a hostname for use with the CIFS for OpenVMS cluster. Register this hostname in DNS and associate it with the IP addresses of the individual nodes in the cluster that will be running CIFS for OpenVMS. Since this name will be used as a NetBIOS name it must not exceed 15 characters in length. HP CIFS Server relies on TCP/IP and DNS load balancing mechanisms to spread the client sessions across the HP CIFS cluster members. To gain the benefits of load balancing and failover, clients must connect to HP CIFS Server using the HP CIFS cluster name.

For example, if the CIFS cluster alias name is CIFSALIAS and it is used by 3 cluster nodes:

```
10.0.0.1 NODEA
10.0.0.2 NODEB
10.0.0.3 NODE
```

The DNS entries would be as below:

```
10.0.0.1 A NODEA
10.0.0.2 A NODEB
10.0.0.3 A NODEC
10.0.0.1 A CIFSALIAS
10.0.0.2 A CIFSALIAS
10.0.0.3 A CIFSALIAS
```

Since DNS provides addresses in "round robin" setup, it provides some measure of load balancing and failover.

To get true load balancing, based on system load and still have failover capability, TCP/IP Services for OpenVMS customers should use the functionality provided by the Load Broker

and METRIC Server to create a TCP/IP cluster name. The TCP/IP cluster name that is specified in the load broker configuration file has to be the same as the "CIFS cluster alias" name (whatever is specified in the NETBIOS NAME parameter in `SMB . CONF`) as this the name that gets registered in the DNS name space. For more information on the configuration of the Load Broker and Metric Server, see *TCP/IP Services for OpenVMS Management* and *TCP/IP Services for OpenVMS Concepts and Planning*.

You can also register Cluster name as a multihomed entry in WINS, unless the WINS server resides in the same IP sub-net as the CIFS for OpenVMS server. For more details, see step 6.

If you are running Multinet or TCPware, see the Process software documentation for more details regarding how load balancing and failover can be implemented.

6. The HP CIFS Server cluster should not be configured to use a WINS server because each HP CIFS cluster node attempts to register the HP CIFS cluster name as a Unique (NetBIOS) name rather than a Group name, which is not allowed. WINS will prevent the second and subsequent cluster members that start HP CIFS from associating their IP address with the cluster name in WINS. This restriction will be addressed in future release.
7. The WINS server restriction should not present a problem for clients as they (typically) resolve names using DNS queries. However, the inability to use a WINS server may present problems for the HP CIFS Servers if there are no domain controllers on the same IP subnet as the HP CIFS cluster members. In this case, use the `SAMBA$ROOT : [LIB] LMHOSTS. file` to map the IP address of remote domain controllers to their respective names (including the special names that only domain controllers register).

If you are installing HP CIFS Server on a cluster that does not have a common disk, you must install the HP CIFS Server software on each node separately and configure each node separately.

If you are installing HP CIFS Server on a cluster node running OpenVMS Version 8.2 or Version 8.2-1, you must install HP CIFS Server on each node separately, and these systems must use separate `SAMBA$ROOT` directory trees and care must be taken to prevent users from accessing the same files simultaneously on multiple cluster members (that is, offer a share only from one cluster member).

If you are installing HP CIFS Server on a cluster node running OpenVMS Version 8.3 and higher, you can have common `SAMBA$ROOT` directory tree in a cluster node.

If you are installing HP CIFS Server on a standalone server you can have a separate `SAMBA$ROOT` directory tree on each node.



NOTE: Ensure that nodes with Version 8.2 or earlier and Version 8.3 and higher, does not share a common location as a share to avoid corruption. This limitation is due to the locking feature as it does not work across Version 8.2 or earlier and Version 8.3 and higher versions. For more information, see [“OpenVMS Cluster Considerations” \(page 18\)](#).

If the HP CIFS cluster nodes use separate system disks, the installation does not accommodate such environments; thus, the following actions must be accomplished to update any other applicable system disks:

- The following files must be copied from the installation node system disk to `SYS$COMMON : [SYS$STARTUP]` on the other applicable system disk(s):
 - `SAMBA$DEFINE_ROOT.COM`
 - `SAMBA$STARTUP.COM`
 - `SAMBA$SHUTDOWN.COM`
- The TCP/IP service definitions for the SMBD and SWAT services must be added to the service database. The best way to accomplish this is to run the HP CIFS configuration procedure on any one HP CIFS cluster member that boots from that system disk:

```
$ @SYS$STARTUP : SAMBA$DEFINE_ROOT
```

\$ @SAMBA\$ROOT: [BIN] SAMBA\$CONFIG

Installing HP CIFS Server Software

This section describes how to install the HP CIFS Server software using the PCSI utility. For more information about the PCSI utility, see the *HP OpenVMS System Manager's Manual*.

Before you begin the installation procedure, ensure that you have completed the preinstallation tasks listed in “Preinstallation Tasks” (page 16) section.

To install the HP CIFS Server software, follow these steps:

1. Log into the SYSTEM account or a privileged account.
2. Start the PCSI utility by entering the PRODUCT INSTALL command with the directory path that is appropriate for your system as follows:

```
$ PRODUCT INSTALL SAMBA/DESTINATION = <directory-path>
```

where:

<directory-path> specifies the target disk and directory name where HP CIFS Server software kit is installed. For example, /DESTINATION=SYS\$SYSDEVICE:[000000] .

If you do not specify the destination qualifier, the PCSI utility searches for the location defined by the logical name PCSI\$DESTINATION. If not defined, the utility installs the HP CIFS Server software kit in the default directory, that is, SYS\$SYSDEVICE:[VMS\$COMMON] .



NOTE: The installation procedure will create the [.SAMBA] directory, for example, SYS\$SYSDEVICE:[000000.SAMBA] .

The installation of HP CIFS Server creates four OpenVMS user accounts, namely SAMBA\$NMBD, SAMBA\$SMBD, SAMBA\$TMPLT, and SAMBA\$GUEST. The UICs for these accounts are allocated dynamically based on the user input and availability in the SYSUAF database.



NOTE: To stop the installation at any time, press **Ctrl+Y**. The installation procedure exits, but does not delete any files that were created.

Upgrading HP CIFS Server Software

This section describes how to upgrade the HP CIFS Server software using the PCSI utility. For more information about the PCSI utility, see the *HP OpenVMS System Manager's Manual*.

Before you begin the installation procedure, ensure that you have completed the preinstallation tasks listed in “Preinstallation Tasks” (page 16) section.

When upgrading the HP CIFS Server software, all existing images and scripts are replaced with images and scripts in the new kit (in the location defined by the logical name SAMBA\$ROOT:).

Table 2-1 lists the database and configuration files that are backed up (to SAMBA\$ROOT:[BACKUP_RESTORE]) prior to installing the new files and are restored there after. Only the current version of each file is retained.



WARNING! The system administrator is responsible for saving and restoring any other files the server may require. HP recommends the file SAMBA\$ROOT:[LIB]SMB.CONF be reviewed for file references. Also, save and restore any scripts modified or created for local use that reside in the SAMBA\$ROOT: directory tree.

Table 2-1 Files Retained During Installation

Location	File Name
SAMBA\$ROOT:[PRIVATE]	*.TDB
SAMBA\$ROOT:[VAR.LOCKS]	*.TDB
SAMBA\$ROOT:[LIB]	SMB.CONF
SAMBA\$ROOT:[LIB]	USERNAME.MAP
SAMBA\$ROOT:[LIB]	LMHOSTS.

All the backed up data will remain in the SAMBA\$ROOT:[BACKUP_RESTORE] directory after installation.



NOTE: When installing a product that is already installed, the PCSI utility requires the new kit be installed to the same location as the existing kit (and will ignore the /DESTINATION qualifier, if specified). To change the product destination, see “Moving the SAMBA\$ROOT Directory” (page 21).

To upgrade the HP CIFS Server software, follow these steps:

1. Log into the SYSTEM account or a privileged account.
2. Shutdown HP CIFS Server:

```
$ @SYS$STARTUP: SAMBA$SHUTDOWN
```



NOTE: If HP CIFS Server is running on multiple cluster members that share the same SAMBA\$ROOT: directory, shutdown HP CIFS Server on all cluster members.

3. Start the PCSI utility:

```
$ PRODUCT INSTALL SAMBA
```



NOTE: To stop the installation at any time, press **Ctrl+Y**.

Moving the SAMBA\$ROOT Directory

To move the contents of SAMBA\$ROOT from one disk to another disk, backup the contents of the SAMBA\$ROOT using the BACKUP command. Then remove and reinstall HP CIFS Server with the /DESTINATION qualifier with the appropriate disk location as below:

```
$ PRODUCT REMOVE SAMBA
```

```
$ PRODUCT INSTALL SAMBA /DESTINATION = <new-location>
```

Now restore the contents of the SAMBA\$ROOT saveset to the <new-location> with /REPLACE qualifier.

Note that the above procedure may not work correctly in the mixed architecture cluster environment, clusters with multiple system disks and clusters with multiple instances of HP CIFS Server installed using separate SAMBA\$ROOT locations. Also, you may have to consider the other copies of SAMBA\$DEFINE_ROOT.COM may exist on other system disks. This depends on the installation and configurations that need to be taken care respectively.

Postinstallation Tasks

After the installation completes, follow these steps:

1. Verify if the SAMBA\$ROOT logical is set:

```
$ SH LOG SAMBA$ROOT
```

```
"SAMBA$ROOT" = "NEWTON$DKA100:[SAMBA.]"
```

If the logical name is not defined, execute the following command:

```
$ @SYS$STARTUP:SAMBA$DEFINE_ROOT
```

If you are installing HP CIFS Server on a cluster, this logical will be defined only on the NODE where HP CIFS Server is installed.

2. Execute the SAMBA\$ROOT: [BIN] SAMBA\$CONFIG.COM command procedure. This command procedure will add TCP/IP services, SMBD, SMBD445, and SWAT and the logical names required by HP CIFS.
3. Verify if the TCP/IP services, such as SMBD and SWAT, exist and also ensure that SWAT service is enabled. For example, if the system is running TCP/IP Services for OpenVMS, enter the following commands:

```
$ TCPIP SH SERVICE SMBD445
```

Service	Port	Proto	Process	Address	State
SMBD445	445	TCP	SMBD445	0.0.0.0	Disabled

```
$ TCPIP SH SERVICE SMBD
```

Service	Port	Proto	Process	Address	State
SMBD	139	TCP	SMBD	0.0.0.0	Disabled

```
$ TCPIP SH SERVICE SWAT
```

Service	Port	Proto	Process	Address	State
SWAT	901	TCP	SWAT	0.0.0.0	Disabled



NOTE: SMBD services will be enabled when the HP CIFS Server starts.

4. Execute @SAMBA\$ROOT: [BIN] SAMBA\$DEFINE_COMMANDS.COM to define symbols for all the HP CIFS utilities. This command procedure also defines symbols, namely, SMBSTART, SMBSTOP, SMBSHOW, and SMBVERSION.



NOTE: Edit the login.com and add the below line.

```
$ @SAMBA$ROOT: [BIN] SAMBA$DEFINE_COMMANDS.COM
```

This will ensure all the HP CIFS commands will be available after login.

5. On OpenVMS Alpha Version 8.2 and OpenVMS Integrity servers Version 8.2-1 define the following logical:

```
$ DEFINE/SYSTEM SAMBA$VMS_FCNTL 1
```

This logical is required as FCNTL byte range locking feature is not available on OpenVMS Alpha Version 8.2 and OpenVMS Integrity servers Version 8.2-1. For more information on the byte range locking restriction, see [“OpenVMS Cluster Considerations”](#) (page 18).

Configuring HP CIFS Server

HP CIFS Server requires configuration modifications for the following functionalities:

- “Configuring a Cluster with Common SAMBA\$ROOT: Directory”
- “Configure HP CIFS Using Samba Web Administration Tool (SWAT)”
- “HP CIFS Configuration File”
- “Supported Backend”
- “Configuring SMB.CONF File in Cluster Environment”
- “Configure SMB.CONF for OpenVMS File Format Support”

Configuring a Cluster with Common SAMBA\$ROOT: Directory

If not done previously, complete the following steps on each cluster member that will run HP CIFS Server:

1. Verify the SAMBA\$ROOT logical name is defined by executing the following command:

```
$ SHOW LOGICAL SAMBA$ROOT
```

If the logical name is not defined, execute the following command:

```
$ @SYS$STARTUP:SAMBA$DEFINE_ROOT
```
2. Execute the HP CIFS Server configuration procedure and respond to the prompts as follows:

```
$ @SAMBA$ROOT:[BIN] SAMBA$CONFIG
```

Now you will be prompted for the number of file server clients to be supported by the CIFS server

Enter the Client Capacity [50]:

Specify the number of client sessions this server should allow or press Return to accept the default of 50. The procedure continues with:

Now you will be prompted for the number of SWAT clients to be supported by the CIFS server

Enter the SWAT Client Capacity [100]:

Specify the number of SWAT connections to the SWAT service or press Return to accept the default of 100. HP recommends a minimum value of 15 to avoid SWAT interface issues.

Configure HP CIFS Using Samba Web Administration Tool (SWAT)

SWAT is a web-based interface that can be used to configure HP CIFS Server from Windows.

To use this utility, you must restore the SAMBA\$ROOT:[UTILS] SAMBA\$SWAT_FILES.BCK file under SAMBA\$ROOT:[SWAT...] directory by entering the following command:

```
$ BACKUP SAMBA$ROOT:[UTILS] SAMBA$SWAT_FILES.BCK/SAVE  
SAMBA$ROOT:[*...] *.*;*/LOG
```

For more information about SWAT, see the following web address:

<http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/SWAT.html>

HP CIFS Configuration File

HP CIFS configuration file, called `SMB . CONF` by default, uses the same format as Windows `. ini` files. The `SMB . CONF` file is a plain text file that you can edit using your preferred editing tool. The `SMB . CONF_TEMPLATE` file is provided along with `SMB . CONF` in the HP CIFS Server software kit. The `SMB . CONF` file contains mandatory configurable parameters.



NOTE: The `SMB . CONF` file is a very important file. You must be cautious while editing this file. For more information on Configuration files, see the following web address:

<http://www.samba.org>

Configuration File Structure

The following is a sample configuration file structure:

```
[global]
...
[homes]
...
[<file/printer share-name>]
...
```

The names within the square brackets delineate unique sections of the `SMB . CONF` file; each section names the share (or service) to which the section refers. For example, the `[homes]` sections are unique disk shares; they contain options that map to specific directories on the HP CIFS Server. All the sections defined in the `SMB . CONF` file, with the exception of the `[global]` section, are available as a disk or printer share to clients connecting to the HP CIFS Server.

Section Description

Each section in the `SMB . CONF` file represents a share on the HP CIFS Server. The section "global" is special because it contains settings that apply to the whole HP CIFS Server and not to one share in particular. There are three special sections, `[global]` , `[homes]` , and `[<file/printer share-name>]` , which are described under Special Sections.

Special sections

`[global]` section

Parameters in this section apply to the server as a whole or are defaults for sections which do not specifically define certain items.

`[homes]` section

This section is included in the configuration file. Services connecting clients to their home directories can be created on the fly by the server.

`[file/printer share-name>]` section

This section is included in the configuration file and if the `Printable` parameter is set to YES, this share functions as a printer share. If the `Printable` parameter is set to NO, this share functions as a file or disk share.

Parameters

Parameters define the specific attributes of sections. Following are the two types of parameters:

- Global Parameters - Parameter specific to the [global] section. For example, workgroup, security, and so on.
- Service Parameters - Parameter specific to the service-specific section. They are usable in all sections, for example, browsable.



NOTE: For more information on configuration (SMB.CONF), see the following web address:
<http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html>

Verify the Configuration File

Enter the following command to verify the contents of the SMB.CONF file:

```
$ TESTPARM
```

TESTPARM examines the SMB.CONF file for syntax errors and reports any found, along with a list of the services.



NOTE: If the TESTPARM reports no problems, it is NOT a guarantee that the services specified in the configuration file will be available or will operate as expected.

Sample Configuration File (SMB.CONF)

```
[global]
server string = Samba %v running on %h (OpenVMS)
security = user
passwd backend = tdbsam
domain master = yes
guest account = SAMBA$GUEST
domain logons = Yes
log file = /samba$root/var/log.%m
log level = 0
load printers = no
printing = OpenVMS
[homes]
comment = Home Directories
browsable = no
read only = no
create mode = 0750
[HPLASER]
path = /var/tmp
printable = yes
min print space = 2000
[test1]
browsable = yes
writeable = yes
path = /DKA0/users/test1
```

Supported Backend

This section describes the supported backend that can be specified in the `SMB.CONF` file by setting the `"passdb backend = <database>"` parameter in the `[global]` section.

smbpasswd Backend

This backend enables you to store user name and passwords similar to UNIX (`/etc/passwd`). By default, it stores the information in the `smbpasswd` file. It contains the LanMan or NT password hashes, password change times, and account flags information. This is a primitive type password backend that has several disadvantages that has been overcome by the `tdbsam` and `ldapsam` password backends.

TDBSAM Backend

This backend enables you to store user and machine account in a TDB database. By default, it stores the information in `SAMBA$ROOT: [PRIVATE] PASSDB.TDB`. The contents of the TDB file can be viewed using the `TDBDUMP` or `pdbedit` utility. This is the default password backend for the HP CIFS Server.

LDAPSAM Backend

This backend enables you to store both POSIX (UNIX) and CIFS user and group account information in a single repository. For more information about LDAPSAM backend, see [Chapter 4 \(page 53\)](#).

Configuring SMB.CONF File in Cluster Environment

Some servers in your network may be configured in an OpenVMS Cluster environment. HP CIFS Servers running in an OpenVMS Cluster that share a common `SAMBA$ROOT` directory also share the same copy of the user accounts and shares databases and assume a single role, either a primary domain controller, a backup domain controller, or a member server, or a Standalone server. They operate as a single entity identified by the HP CIFS Server TCP/IP cluster alias name.

To configure the `SMB.CONF` file on cluster members sharing the same `SAMBA$ROOT` directory, follow these steps:

1. Create a node-specific configuration file for each cluster member named `SMB.CONF_<hostname>` in the `SAMBA$ROOT: [LIB]` directory, where `<hostname>` is the hostname of the cluster member. For example, for cluster host REYGON, create the file `SAMBA$ROOT: [LIB] SMB.CONF_REYGON`.
2. Edit the node-specific configuration file and, at minimum, add the `[global]` section and the parameter `"netbios aliases"`, specifying the local hostname as an alias name. Add any additional node-specific parameters to this file. For example, for the node REYGON, add:

```
[global]
netbios aliases = reygon
```

3. Configure a generic, cluster-wide `SMB.CONF` file in the `SAMBA$ROOT:[LIB]` directory, which will be used by all cluster members running HP CIFS Server and which contains parameters and share definitions applicable to all.

The `[global]` section of this common `SMB.CONF` file must contain the following "INCLUDE" parameter so the appropriate node-specific configuration file is loaded:

```
include = SAMBA$ROOT:[LIB]SMB.CONF_%h
```

`%h` is one of several environment variables that may be used in the configuration files to fine-tune the configuration. For more information see the `SMB.CONF` manpage at <http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html>.

The `[global]` section must also contain the cluster name definition in the parameter:

```
netbios name = <TCPIP-cluster-alias-name>
```

Configure SMB.CONF for OpenVMS File Format Support

The HP CIFS Server supports accessing and creating OpenVMS files of various formats, but not all formats are supported. Additionally, some formats require the use of a Virtual File System (VFS) module to support them as noted below.

By default, the HP CIFS Server will create new files using a Stream record format with record attributes of Carriage return carriage control. Additionally, the server can read Stream and Stream_LF files without the need of a VFS module.

However, some Java applications require files be created in Stream_LF format. In such cases, the share section in the `SMB.CONF` file should include the line:

```
vfs objects = streamlf
```

Similarly, if a share may contain files with a Variable Length record format or a VFC (Variable Format Control) record format, the following line must be included in the share section in the `SMB.CONF` file:

```
vfs objects = varvfc
```



NOTE: This is applicable to both INDEXED and sequential file organization for the above-mentioned file formats.

The VTF module converts file names on Windows to VTF-7 Unicode file names on ODS-5 disks. To use VTF-7 format file names in a share, the following line must be included in the share section in the `SMB.CONF` file:

```
vfs objects = vtf
```



NOTE:

- The Japanese OpenVMS supports only Japanese/VTF-7 file names on ODS-5 disks.
 - Multiple VFS modules may be specified, separated by commas, and are used in the order specified. Optionally, place the "vfs objects" parameter in the `[global]` section to have it apply to all shares which do not include a "vfs objects" parameter in their share section.
-

Configuration Setting for International Character Set

HP CIFS Server supports ISO-8859-1 and UTF-8 character set for file names. The European characters are supported in ISO-8859-1 and other characters are supported in UTF-8. For ASCII or Latin-1 character set support, configure `SMB.CONF` file and add the following line to the `[global]` section:

```
[global]
```

```
unix charset = ISO-8859-1
```

For Japanese or Chinese character set support, configure `SMB.CONF` file and add the following line to the `[global]` section:

```
[global]
dos charset = <user local codepage>
unix charset = UTF-8
vfs objects = vtf
```



NOTE: For more information on the VTF module, see Limitations section in the *HP OpenVMS CIFS Release Notes* for using the VTF module.

where:

[<user local codepage>] is Windows codepage of the user. The value "CP850" is the default Windows codepage for English. For Japanese Windows, the value is "SJIS" or "CP932".

By default, the `SMB.CONF` file will have the following configuration settings for character set support:

```
[global]
dos charset = CP850
unix charset = UTF-8
```



NOTE: The character set applies only to the characters in the file names and not the contents of the files.

Starting and Stopping the HP CIFS Server

This section describes how to start and stop HP CIFS Server.

Starting HP CIFS Server Manually

To start HP CIFS Server manually, enter the following command:

```
$ @SYS$STARTUP:SAMBA$STARTUP.COM
```

The HP CIFS Server starts, and a message similar to the following is displayed:

```
Creating NMBD Process
%RUN-S-PROC_ID, identification of created process is 0000255C
```

Starting HP CIFS Server When System Boots

To ensure that the HP CIFS Server starts automatically each time you boot the OpenVMS system, edit the site-specific startup file, `SYS$STARTUP:SYSTARTUP_VMS.COM`. Add the CIFS startup commands below all lines that start network transports. For example,

```
$ @SYS$STARTUP:TCPIP$STARTUP.COM
.
.
.
$ @SYS$STARTUP:SAMBA$DEFINE_ROOT.COM
$ @SYS$STARTUP:SAMBA$STARTUP.COM
```

Starting HP CIFS Server in an OpenVMS Cluster

If you have installed and configured HP CIFS Server on multiple nodes of the same OpenVMS Cluster, HP recommends that you use the `SYSMAN` utility to start HP CIFS Server manually and simultaneously on all cluster members.

To start HP CIFS Server on all cluster nodes at the same time, ensure that you are logged in to the SYSTEM account on one of the member nodes, and then run SYSMAN. Table 2–2 lists the SYSMAN utility commands.

Table 2-2 SYSMAN Utility

Enter this command...	To...
<code>\$ RUN SYS\$SYSTEM:SYSMAN SYSMAN> SET ENVIRONMENT/NODE= (node1,node2,...)</code>	Start the SYSMAN utility. Define the OpenVMS Cluster members on which to start the server. For example, <code>SYSMAN> SET ENVIRONMENT/NODE= (SPEEDY, SPIN, SPAN)</code>
<code>SYSMAN> DO @SYS\$STARTUP:SAMBA\$STARTUP.COM</code>	Start the HP CIFS Server on all the nodes you defined in the previous command.
<code>SYSMAN> EXIT</code>	Exit the SYSMAN utility.

Stopping HP CIFS Server

To stop the HP CIFS Server manually, enter the following command:

```
$ @SYS$STARTUP:SAMBA$SHUTDOWN.COM
```

Troubleshooting Installation and Configuration Issues

The following sections describe some problems you can encounter during the installation and configuration of the HP CIFS Server.

- Installing the HP CIFS Alpha Kit on an OpenVMS Integrity System
If you attempt to install the Alpha kit on an Integrity server system, the PCSI utility procedure displays the following error message and terminates the installation:
`HP AXPVMS SAMBA Version 1.1 does not run on OpenVMS I64 systems.
You can install this product on OpenVMS Alpha systems only.`
- Installing the HP CIFS Integrity Kit on an OpenVMS Alpha System
If you attempt to install the Integrity server kit on an Alpha system, the PCSI utility procedure displays the following error message and terminates the installation:
`HP I64VMS SAMBA Version 1.1 does not run on OpenVMS Alpha systems.
You can install this product on OpenVMS I64 systems only.`
- HP CIFS Utilities
 - testparm
testparm is a program to test the contents of SMB.CONF file. Whenever you modify the SMB.CONF file, you need to run the testparm utility.
`$ testparm`
 - SWAT
SWAT is a web-based interface that can be used to configure HP CIFS Server from Windows. In addition, it provides online help for each configuration parameter. For more information, see “Configure HP CIFS Using Samba Web Administration Tool (SWAT)” (page 23).

- Logs
 - NMBD log files will be generated after startup. The SAMBA\$NMBD_<node-name>.log files are stored in SAMBA\$ROOT: [VAR] .
 - SMBD log files will be generated for each client that utilizes the HP CIFS Server. By default, these log files are stored in SAMBA\$ROOT: [VAR] as specified by the SMB .CONF parameter "log files".
- When you run the executable in the "-i" interactive mode, all the debug messages will be displayed on the screen and you can also know where exactly the SMBD process is hanging or aborting.
- SAMBA\$ROOT: [BIN] SAMBA\$GATHER_INFO.COM - This is the command procedure that gathers information and data files and creates a backup save set file for reporting problems.
- Packet sniffer (Wireshark, Microsoft Network Monitor, etc.) can be used to capture the network traces between the client and sever.
- The System Dump Analyzer can be used to analyze the process details.
- Ensure that "name of the services startup command file" points to the appropriate startup command procedure for the SMBD startup. To verify, enter the following command:

```
$ TCPIP SHOW SERVICE SMBD/FULL
```

For example,

```
$ TCPIP SHOW SERVICE SMBD445/FULL
Service: SMBD445
State: Enabled
Port: 445      Protocol: TCP      Address: 0.0.0.0
Inactivity: 5  User_name: SAMBA$SMBD  Process: SMBD445
Limit: 500     Active: 0             Peak: 0
```

```
File: SAMBA$ROOT: [BIN] SAMBA$SMBD_STARTUP.COM
Flags: Listen
Socket Opts: Rcheck Scheck
```

```
Receive: 0 Send: 0
Log Opts: Acpt Actv Dactv Conn Error Exit Logi Logo Mdfy Rjct TimO Addr
TimO Addr
File: SAMBA$ROOT: [VAR] SAMBA$SMBD_STARTUP.LOG
```

```
Security
Reject msg: not defined
Accept host: 0.0.0.0
Accept netw: 0.0.0.0
```

```
$ TCPIP SHOW SERVICE SMBD/FULL
Service: SMBD
State: Enabled
Port: 139      Protocol: TCP,UDP      Address: 0.0.0.0
Inactivity: 0  User_name: SAMBA$SMBD  Process: SMBD
Limit: 100     Active: 1             Peak: 1
```

```
File: SAMBA$ROOT: [BIN] SAMBA$SMBD_STARTUP.COM
Flags: Listen
Socket Opts: None
```

```
Receive: 0 Send: 0
Log Opts: Acpt Actv Dactv Conn Error Exit Logi Logo Mdfy Rjct
TimO Addr
File: SAMBA$ROOT: [VAR] SAMBA$SMBD_STARTUP.LOG
```

```
Security
Reject msg: not defined
Accept host: 0.0.0.0
Accept netw: 0.0.0.0
```



NOTE: Ensure that all the settings and log files are accessible.

Verifying the Client Connection

Ensure that all the security settings and configuration settings are completed before verifying the client connection. To verify whether users are able to connect from a client successfully, follow these steps:

1. Start the NMBD process by entering the following command:

```
$ @SYS$STARTUP:SAMBA$STARTUP.COM
```

2. From the client, verify whether it has registered the name query request. Enter the following command from the command prompt:

```
C:\ NBTSTAT -A <IP ADDRESS>
```

This gives the registered NetBIOS names of the server

For example,

```
C:\ NBTSTAT -A 16.148.18.31
```

```
Local Area Connection:
```

```
Node IpAddress: [16.38.47.15] Scope Id: []
```

```
NetBIOS Remote Machine Name Table
```

```
Name Type Status
```

```
-----
```

```
NEWTON <00> UNIQUE Registered
```

```
NEWTON <03> UNIQUE Registered
```

```
NEWTON <20> UNIQUE Registered
```

```
LANGROUP <00> GROUP Registered
```

```
LANGROUP <1C> UNIQUE Registered
```

```
LANGROUP <1E> GROUP Registered
```

```
MAC Address = 00-00-00-00-00-00
```

3. Connect from a client by entering the following address at the RUN prompt.

```
\\<ip-address-of-CIFS-server> OR <name of the server>
```

- a. The Enter Network Password screen is displayed.

- Enter the domain\user name in the 'User Name' field and the password in the 'Password' field.
- Click **OK**.

- b. A list of shared folders and files are displayed.



NOTE: If HP CIFS Server is configured as a member server to a domain <domain-name>, then you need to prefix the <user-name> with the "<domain-name>\\" as shown:

```
<domain-name>\<user-name>
```

Other HP CIFS Server Configuration Issues

Performance Tuning

1. HP CIFS Server Version 1.1 provides performance improvement for file shares present on ODS-5 disk. The `SMB.CONF` share section parameter `"vms_path_names"` disables or enables the performance improvement feature. By default, this parameter is enabled for ODS-5 disks and is disabled for ODS-2 disks. Make sure to never enable `"vms_path_names"` parameter for shares present on ODS-2 disk as it can lead to unpredictable results. On ODS-5 disks, if `"vms_path_names"` is enabled, you must not specify `"mangled_names = yes"` for that share in the `SMB.CONF` file. It is necessary to add `"change_notify = no"` in the `[global]` section of the `SMB.CONF` file.

In order to obtain performance benefit for shares present on ODS-2 disk or if you set `"vms_path_names = no"` for ODS-5 disks, you can specify the following `SMB.CONF` parameter for the corresponding `[<share>]` section:

```
case sensitive = yes
```

2. Do not host the `SAMBA$ROOT` directory on the system disk, instead host `SAMBA$ROOT` directory on another disk. If you have already hosted this on the system disk, follow the instructions about moving the `SAMBA$ROOT` directory tree in section [“Moving the SAMBA\\$ROOT Directory”](#) (page 21).
3. Disable volume highwater marking to improve writes.
 - a. Include the `/NOHIGHWATER_MARKING` qualifier while initializing the volume.
 - b. If the volume is already initialized, execute the following command to set volume to highwater marking:

```
$ SET VOLUME /NOHIGHWATER_MARKING <volumename>
```

You need to remount the disk for the changes to take effect.
4. Use ODS-5 disks for variable-length record formatted files.
5. Minimize debug logging and ensure that the log levels in the `SMB.CONF` file is set to minimum value as below:

```
log level = 0
```

6. Specify disk cluster size as a multiple of 16. You can achieve this during disk initialization by executing the command:

```
$ INITIALIZE disk /CLUSTER=16*n
```

Where:
`n` can range from 1 onwards.
7. Add the following line in `SAMBA$ROOT: [BIN] SAMBA$SMBD_STARTUP.COM:`

```
$ SET RMS_DEFAULT /EXTEND_QUANTITY=10240/BLOCK_COUNT=n/BLOCK_COUNT=8
```



NOTE: Specify `extend_quantity` in the multiple of 16 blocks.

Where:

`n` is 124 for EVA, 96 for XP, and 127 for all other disk types.

8. Disable Large File Copy
Whenever a copy to the server operation is initiated the HP CIFS Server by default starts copying the file without prior allocation. This enables copying large files without time out. If you want the server to allocate the space before starting the copy operation define the following logical:

```
$ DEFINE/SYSTEM SAMBA$DISABLE_LARGE_FILE_COPY 1
```


Since server takes some time to respond to the client as it needs to allocate the space, the large file copy to the server might fail, if the above logical is defined.

9. Execute the following command periodically on the directory containing large number of variable-length record formatted files.

```
$ ANALYZE/RMS/UPDATE_HEADER <filespec>
```



NOTE: The above command updates the "file length hint" fields of the file headers on ODS-5 disks. If these fields are invalidated, HP CIFS Server calculates the actual number file size by reading the contents of the file. This deteriorates the performance.

Special Concerns when Using HP CIFS Server on a Network File System (NFS)

Both NFS and CIFS provide file system access to a file storage from multiple systems. However, controlling access to files, particularly files open for write access, from NFS and CIFS systems simultaneously are not supported. Since NFS and CIFS have their own way of locking mechanism which is not known to each other, it will not be able to synchronize access to a specific resource.

NetBIOS Names Are Not Supported on Port 445

HP CIFS Server V1.1 (based and Samba 3.0.x) can accept connections on port 445 as well as the port 139. However, since port 445 connections are for SMB over TCP and do not support the NetBIOS protocol, NetBIOS names are not supported on port 445. This means features of HP CIFS Server that depend on NetBIOS will not work. For example, the "virtual server" technique depending on an "include = /etc/opt/samba/SMB.CONF.%L" which ends up referring to another SMB.CONF.<netbios name> will not work.

You can use the SMB.CONF parameter `smb ports` to specify which ports the server should listen on for SMB traffic. Set `smb ports` to 139 to disable port 445. By default, `smb ports` is set to 445 139.

VMS Specific Configurations

This section describes the VMS specific configurations.

Microsoft's Distributed File System (DFS)

If Microsoft's Distributed File System (DFS) is not utilized, disable DFS support on the HP CIFS Server by adding the following parameter to the [global] section in the SMB.CONF file. This will reduce network traffic and DFS related errors.

```
host msdfs = no
```

Configuring the Number of Client Connections

The maximum number of client connections that a server can handle is limited by the maximum number of processes (Process Entry Slots) that a server can handle. You can obtain this value by entering the following command:

```
$ SHOW MEM/SLOT
```

To modify the value of "Process Entry Slots" parameter, see *HP OpenVMS System Manager's Manual*.

VMS Specific SMB.CONF Configurations

store dgpackets

`store dgpackets` is a VMS specific SMB.CONF parameter which is specified in the [global] section. If you enable this parameter by adding the following line under the [global] section

of the `SMB.CONF` file, NMBD process will write or store the unwanted datagram (UDP) packets to the `unexpected.tdb` file:

```
[global]
```

```
store dgpackets = yes
```

require strongkey

`require strongkey` is VMS specific `SMB.CONF` parameter which is specified in the `[global]` section. Setting `require strongkey` to 'YES' specifies that an HP CIFS Server must use a strong (128 bit) session key. If the domain controller on the other side of the channel does not support strong (128 bit) session keys, then the HP CIFS server will refuse to establish a secure channel.

```
[global]
```

```
require strongkey = yes
```



NOTE: This registry parameter should be set to 'YES' only when all the other domain controllers support strong keys. Only Windows 2000 and above supports strong keys.

Token sid limit

`Token sid limit` is a VMS specific `SMB.CONF` parameter which is specified in the `[global]` section. It indicates the maximum number of domain groups to which an user can belong. By default, this parameter is set to 750.

Uninstalling the HP CIFS Server Software

This section describes how to remove HP CIFS Server software from your system.

To remove HP CIFS Server configuration on a particular node in a cluster, enter the following command:

```
$ @SAMBA$ROOT: [BIN] SAMBA$REMOVE_CONFIG.COM
```

This command procedure deassigns all the HP CIFS Server logical names defined on this node and also removes the TCP/IP services such as, SMBD and SWAT that are set during configuration.

To uninstall the HP CIFS Server software, follow these steps:

1. Ensure that you are logged in using the privileged account.
2. Stop the NMBD and all client SMBD processes by entering the following command:
\$ @SYS\$STARTUP: SAMBA\$SHUTDOWN.COM
3. Enter the following command:
\$ PRODUCT REMOVE SAMBA

The removal command procedure performs the following operation:

- Prompts if you wish to save configuration files. These include the HP CIFS database files (extension `.tdb`), the `SMB.CONF`, the `username.map` file, and the `LMHOSTS.file`.
 - Entering NO at the prompt deletes the TDB files, and the `SMB.CONF` file and HP CIFS Server related logical names are deassigned.
 - Entering YES results in a prompt to specify the location to which the files will be saved. Specify a device and directory or just press Return to accept the default of `SAMBA$ROOT: [BACKUP]`. The HP CIFS Server logical names will not be deassigned.
 - Removes all the HP CIFS Server accounts created during installation.

3 HP CIFS Deployment Models

This chapter describes how to configure an HP CIFS Server for different domain roles, whether it is in a Samba domain model, consisting solely of HP CIFS Servers, or a Windows NT or Active Directory domain model.



NOTE: At this time, the HP CIFS Server can join a Windows Active Directory domain only as an NT style member server, which relies on NetBIOS over TCP/IP to communicate with domain controllers. While the information in this chapter explains the Windows NT domain model, it can be directly applied to Active Directory domains as well. For example, a designated domain controller in every Active Directory domain functions as the "PDC Emulator" for the domain, to provide down-level compatibility.

Domain Roles

This section describes how to configure an HP CIFS Server for different domain roles.

Primary Domain Controllers

Each domain has one and only Primary Domain Controller. The Primary Domain Controller (PDC) is responsible for several tasks within the domain. These include:

- Authenticating user logons for users and workstations that are members of the domain
- Acting as a centralized point for managing user account and group information for the domain
- A user logged on to the Primary Domain Controller (PDC) as the domain administrator can add, remove or modify domain account information on any machine that is part of the domain
- Serving as the Domain Master Browser and the Local Master Browser for the domain on its IP subnet.

Backup Domain Controllers

Advantages of Backup Domain Controllers

Backup Domain Controllers (BDCs) provide the following benefits to the customer:

- The BDC can authenticate user logons for users and workstations that are members of the domain when the wide area network link to a PDC is down.
- A BDC plays an important role in both domain security and network integrity.
- The BDC can pick up network logon requests and authenticate users while the PDC is very busy on the local network. It can help to add robustness to network services.
- The BDC can be promoted to a PDC if the PDC needs to be taken out of services or fails. This is an important feature of domain controller management.

Domain Member Servers

Domain Member servers participate in domain security but do not have a copy of the domain accounts database. They maintain a separate, local accounts database but can utilize the accounts maintained by domain controllers or trusted domains.

- The following member servers are supported:
 - Windows NT
 - Windows 2000 and Windows 2003

- HP CIFS Server
- Advanced Server for OpenVMS
- Domain users may access resources of Domain Member servers such as file and printer shares.
- Member servers authenticate domain users by passing user authentication requests to domain controllers for processing.

Samba Domain Model

You can use the Samba Domain Deployment Model in environments with the following characteristics:

- A domain consisting of HP CIFS Servers and no Windows domain controllers.
- Support for any number of OpenVMS servers that provide file and print services for corresponding numbers of users.
- An HP CIFS Server is configured as a Primary Domain Controller (PDC). One or more HP CIFS Servers act as Backup Domain Controllers (BDCs).
- Domain accounts should be maintained in an LDAP directory such as one created using HP OpenVMS Enterprise Directory Server.
- The PDC and BDCs use the Samba LDAP backend (ldapsam) to access the LDAP directory servers, for example when authenticating users.

The Samba Domain Model provides the following benefits:

- It can be expanded easily.
- The HP CIFS Server acting as a BDC can pick up network logon requests and authenticate users while the PDC is busy on the network.
- The BDC can be promoted to a PDC if the PDC needs to be taken out of services or fails. The PDC-BDC model provides authentication load balancing for larger networks.
- The PDC, BDCs, and domain member servers store account databases in the LDAP directory to centralize administration regardless of network size.

Figure 3-1 shows a standalone HP CIFS Server as a PDC with the local password database:

Figure 3-1 Standalone HP CIFS Server as a PDC

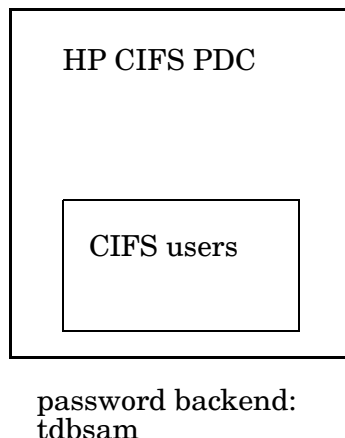
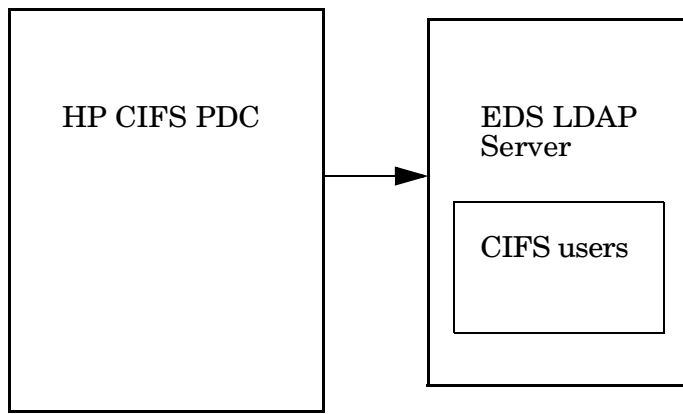


Figure 3-2 shows a standalone HP CIFS Server as a PDC using the Enterprise Directory Server (EDS) as an LDAP backend:

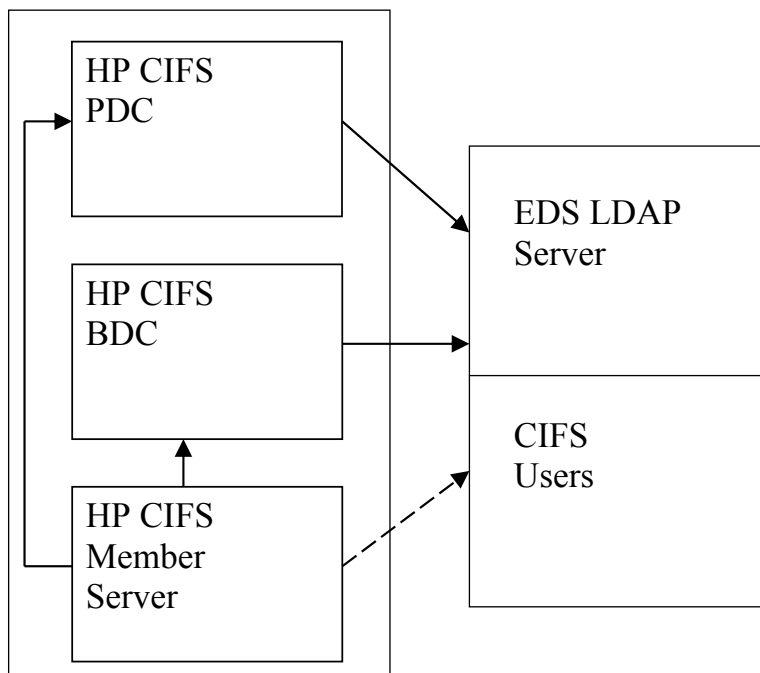
Figure 3-2 Standalone HP CIFS Server as a PDC with EDS backend



password backend:
ldapsam

Figure 3-3 shows multiple HP CIFS Servers using Enterprise Directory Server as an LDAP backend:

Figure 3-3 Multiple HP CIFS Servers with EDS backend



password backend:
ldapsam

The Samba Domain Deployment Model consists of a HP CIFS Server configured as a Primary Domain Controller (PDC), and one or more HP CIFS Servers acting as Backup Domain Controllers (BDCs). The PDC, BDCs, and member servers use the central LDAP backend to consolidate CIFS accounts on the LDAP directory.

Samba Domain Components

As demand requires multiple servers, this model makes use of a directory server and LDAP access. Use LDAP servers for centralization of both Posix and Windows user data. For more information about how to set up LDAP, see [Chapter 4 “LDAP Integration Support”](#).

WINS is used for multi-subnetted environments. Multi-subnetted environments require name-to-IP-address mapping to go beyond broadcast limits of a IP-subnet. PC client configurations also can specify the WINS server address to ensure that they are able to address systems outside their IP-subnet boundary. To configure the HP CIFS Server as a WINS client, use the `SMB.CONF` global parameter "wins server" and specify the IP address of the WINS server. At this time, the HP CIFS Server does not support being a WINS server.

HP CIFS Server Acting as a PDC

HP CIFS Server configured as a PDC is responsible for authentication throughout the domain. Set the `SMB.CONF` global parameters "security = user", "domain master = yes", and "domain logons = yes" to designate the server as the PDC of the domain.

Single server installations may use `tddb` password backend, but large installations should use the LDAP backend to provide centralized management of CIFS users. Configure LDAP with `passdb backend = ldapsam:ldap://<name or IP address of the node where LDAP server is running>`.

An important characteristic of a CIFS PDC is browsing control. The parameter, `domain master = yes`, causes the server to register the NetBIOS name <domain name>1B, where 1B is reserved for the domain master browser. Other systems will query for the <domain name>1B name when attempting to locate the PDC of the domain.

See the following example of `SMB.CONF` file

```
[global]
#SAMBA Domain name
workgroup = SAMBADOM
server string = PDC running on %h (OpenVMS)
security = user
encrypt passwords = Yes
domain logons = Yes
admin users = <privileged CIFS user>
os level = 65
preferred master = Yes
domain master = Yes
wins server = <server ip address>
log file = /samba$root/var/log_%h.%m
logon script = netlogon.bat
name resolve order = wins lmhosts bcst
idmap uid = 1000-10000
idmap gid = 1000-10000
[netlogon]
comment = The domain logon service
path = /samba$root/netlogon
browseable = no
guest ok = no
```

Limitations

The following is a list of limitations for the PDC support:

- HP CIFS Server cannot create Security Account Management (SAM) update delta files. It cannot interoperate with a PDC to synchronize the SAM from delta files that are held by a BDC.
- The HP CIFS Server PDC does not support replication to BDCs. Running BDCs with a backend other than LDAP can prove difficult if not impossible to keep account information synchronized. See the Table 5.1, Domain Backend Account Distribution Option, in the *Official Samba-3 HOWTO and Reference Guide* for more information on possible domain design configurations using LDAP.

HP CIFS Server Acting as a BDC

The configuration of BDCs is similar to that of the PDC. Set the `SMB.CONF` global parameters "security = user", "domain master = no", and "domain logons = yes" to designate the server as a BDC of the domain. This enables BDCs to carry much of the network logon processing. A BDC on a local segment handles logon requests and authenticates users when the PDC is busy on the local network. When a segment becomes heavily loaded, the responsibility is off-loaded to another segment's BDC or to the PDC. Therefore, you can optimize resources and add robustness to network services by deploying BDCs throughout the network.

If you set the `local master` parameter to `yes` in `SMB.CONF`, browsing can also be spread throughout the network.

You can promote a BDC to a PDC if the PDC needs to be taken out of service or fails. To promote a BDC to a PDC, change the `domain master` parameter from `no` to `yes`.

The PDC and BDCs use the central LDAP directory to store common CIFS accounts on the LDAP directory. When you integrate the HP CIFS Server acting as a BDC with the LDAP directory, you must install the HP LDAP software and configure the LDAP. The BDC can access the LDAP directory for Windows authentication.

- The `SMB.CONF` file is as shown if the HP CIFS Server acting as a BDC does not use the LDAP backend:

```
[global]
# Samba Domain
workgroup = SAMBADOM
security = user
domain logon = yes
domain master = no
encrypt passwords = yes
security = user
```

- The `SMB.CONF` file is as shown if the HP CIFS Server acting as a BDC uses the LDAP backend to store OpenVMS and HP CIFS account databases:

```
[global]
#Samba Domain
workgroup = SAMBADOM
security = user
domain logon = yes
domain master = no
encrypt passwords = yes
passdb backend = ldapsam:ldap://ldapserver:389
```

HP CIFS Server does not implement a true SAM database and nor its replication. HP CIFS Server implementation of BDCs is very much like a PDC with one important difference. A BDC is configured like a PDC except the `smb.conf` parameter, `domain master`, must be set to `no`.



NOTE: `security`: Set this parameter to `user` to ensure that Windows users, client machine accounts, and passwords are stored and managed in the `passdb` backend.

`domain master`: Set this parameter to `no` in order for the HP CIFS Server to act as a BDC.

`domain logon`: Set this parameter to `yes` to provide netlogon services.

`Encrypt passwords`: You set this parameter to `yes`, the passwords used to authenticate users are encrypted. You must set this parameter to `yes` when you configure HP CIFS Server to act as a BDC.

Synchronizing the Account Database between the BDC and the PDC

Unlike Advanced Server and Windows domain controllers, automatic replication of the user accounts database is not possible between a HP CIFS PDC and HP CIFS BDCs. To accomplish the same goal, HP CIFS requires the assistance of LDAP servers. By configuring the HP CIFS PDC and HP CIFS BDCs to use the LDAP backend, replication of the accounts database is achieved by virtue of the synchronization occurring between LDAP servers. HP CIFS can use the LDAP backend to store and obtain user and group account information in the LDAP directory (such as HP Enterprise Directory or an OpenLDAP server). Though a single LDAP server can be used for both the HP CIFS PDC and BDCs, it is highly recommended that separate LDAP servers be used by the HP CIFS PDC and BDCs for high availability and better performance.

If `tdbsam` is specified as the `passdb` backend, the replication between the BDC and PDC can be achieved by executing the following command:

```
$ NET RPC VAMPIRE -S [NT netbios name or IP] -W [domainname] -U  
administrator%password
```

HP CIFS Server Acting as a Member Server

You can join an HP CIFS Server to the Samba Domain. The Windows authentication requests are managed by the PDC or BDCs using LDAP, `tdbsam` or other backend. Set the `SMB.CONF` global parameters "`security = domain`", "`domain master = no`", and "`domain logons = no`" to designate the server as a member server. For more information on how to join an HP CIFS Server to the Samba Domain, see [“Adding an HP CIFS Server to a Domain”](#) (page 42).

The member server `SMB.CONF` configuration differs from that of the PDC and BDC. You must set the `SMB` global parameter "`security = domain`", which causes the member server to send authentication requests to the domain controllers for processing. Set the `domain master` parameter to `no` to let the PDC take control. As with the PDC and BDC, the `passdb` backend parameter may be set to `tdbsam` to store the member server accounts in a local HP CIFS Server database or to `ldapsam` to store accounts in an LDAP directory such as one created using HP Enterprise Directory Server for OpenVMS.

Configure the HP CIFS Server as a Standalone Server

Standalone servers are independent of Domain Controllers on the network. By definition, this means that users and groups will be created and controlled locally, and the identity of a network user must match a local user login. Set the `SMB.CONF` global parameters "`security = user`" and "`domain logons = no`" to designate the server as a Standalone server.

A sample SMB.CONF file for an HP CIFS Server as a Standalone Server

```
[global]
server string = Samba %v running on %h
security =user
passdb backend = tdbsam
log file = /samba$root/var/log_%h.%m
load printers = No
[homes]
comment = Home Directories
read only = No
browseable = No
```

Configure the HP CIFS Server as a PDC

To configure HP CIFS Server as a PDC, follow these steps:

1. Add or verify the following parameters in the SMB.CONF file:

The following parameters assist you in adding or deleting the users:

```
ADD USER TO GROUP SCRIPT = SAMBA$ROOT:[BIN] SAMBA$ADDUSERTOGROUP %G
%U
```

```
DELETE USER FROM GROUP SCRIPT =
SAMBA$ROOT:[BIN] SAMBA$DELUSERFROMGROUP %G %U
```

The above script gets executed automatically whenever the appropriate RPC commands are executed.

ADDUSERTOGROUP adds the user to domain group.

DELUSERFROMGROUP deletes the user from group.

2. Run the testparm utility and ensure the server is configured as the PDC.

```
$ @SAMBA$ROOT:[BIN] SAMBA$DEFINE_COMMANDS
$ testparm
```

3. Start the HP CIFS Server by entering the following command:

```
$ @SYS$STARTUP:SAMBA$STARTUP
```

Join a Windows Client to a HP CIFS Domain

This section describes how a Windows client can be added to a domain with an HP CIFS PDC.

Step-by-step Procedure

1. Create an OpenVMS account for the Windows client. The account name should be the same as the client computer name with a dollar sign (\$) appended to it. The dollar sign designates the account as a machine account. For example:

```
$ MC AUTHORIZE ADD winstatn01$$ /FLAG=NODISUSER/UIC=[1000,1]
```



NOTE: If HP CIFS Server is configured as PDC, the name of the workstations that are getting added to HP CIFS Server PDC must not exceed 11 characters. This limitation is due to the OpenVMS user name length limited to 12 characters in SYSUAF database..

2. Create a HP CIFS machine account for the client computer. Using the pdbedit tool create an account and designate it as a machine account (do NOT include the trailing dollar sign as part of the machine name; it will be appended by pdbedit automatically). Note that the account name must be identical to the name of the OpenVMS account created (in Step 1 above) for the machine.

```
$ pdbedit -am winstatn01
```

The account can be viewed like any other account, but the complete account name, which includes the dollar sign must be specified; for example:

```
$ pdbedit --list --verbose winstatn01$
```

3. Now that the necessary accounts exist, the Windows workstation may be added to the domain by an Administrator. From the Windows client, follow these steps:
 - a. Logon as any user.
 - b. Right-click on **My Computer** and select **Properties**.
 - c. Select the **Computer Name** tab.
 - d. Click the **Change** button.
 - e. In the "Member of" section, select the **Domain** option and specify the NetBIOS domain name of the HP CIFS domain. Click **OK**.
 - f. When prompted, enter the credentials of a domain administrator. If successful, the system will display a message "welcoming you to the domain". Click **OK**.
 - g. Click **OK** to acknowledge the message indicating the system must be rebooted.
 - h. Click **OK** to complete the name change and reboot.

After the system reboots the Windows Security logon screen appears. Enter a domain 'username' and 'password'. From the Logon to drop-down box, select the domain name. If the **Logon to** box is not present, click the **Options** button to expose it.

Adding an HP CIFS Server to a Domain

This section describes the procedure to join an HP CIFS Server to a domain. In order to be a member of a domain the HP CIFS Server requires an account in the domain. The account name must match the NetBIOS name of the HP CIFS Server as defined by the "netbios name" parameter in the SMB.CONF file. If the "netbios name" parameter is set to its default value of %h, %h is an environment variable that translates to the hostname of the local system. The account name will be appended with a dollar sign to designate it as a machine account. In an HP CIFS cluster environment where multiple cluster members share the same SMB.CONF configuration file, a single machine account is required for the cluster and the name must match the value specified in the SMB.CONF file "netbios name" parameter.

The machine account may be created either before attempting to add the HP CIFS Server to the domain or while adding the HP CIFS Server to the domain. In the former case, an administrator uses the appropriate method to add a computer to the domain which is dependent on the type of PDC, as follows:

- Windows Active Directory Domain (Windows 2000 and later) — Use the Active Directory Users and Computers management interface to add a new Computer account. During the Add Computer wizard, specify the NetBIOS name of the HP CIFS Server (omitting the trailing dollar sign) and you must select (only) the check box next to "Assign this computer account as a pre-Windows 2000 computer".
- Advanced Server for OpenVMS — Use the ADMIN interface to add the computer account as follows:

```
$ ADMIN ADD COMPUTER/TYPE=SERVER <CIFS-SERVER-NAME> ! Do not include a trailing $, it will be added automatically
```
- HP CIFS for OpenVMS — Add an OpenVMS account and a CIFS machine account as described in "Join a Windows Client to a HP CIFS Domain" (page 41)
- Windows NT PDC — The Server Manager application can be used to add a computer to the domain. From the top menu, select Computer and then select Add to Domain. Select the radio button next to "Windows NT Workstation or Server, specify the NetBIOS name of the HP CIFS Server (do not include a trailing dollar sign), and click **Add**.

When the computer account is created prior to the HP CIFS server joining the domain, the HP CIFS server administrator need not supply a domain user name and password of an account

with rights to add computers to the domain. In this case, after configuring the `SMB.CONF` file appropriately, join the domain by executing the command:

```
$ NET RPC JOIN
```

If the computer account for the HP CIFS server was not created prior to joining the domain, the administrator must supply the username and password of a domain account with rights to add computers to the domain. For example, the Administrator account. To join a domain and create a machine account (or resync the password of an existing machine account), execute the command:

```
$ NET RPC JOIN --user <username>
```

For more information on member server configuration, see “A sample `SMB.CONF` file For an HP CIFS ADS Member Server” (page 45).



NOTE:

1. HP CIFS does not need to be started before executing the `$ NET RPC JOIN` command.
 2. As specified above, the command is dependent upon the ability to locate the PDC of the domain using standard NetBIOS name resolution methods, including WINS (if `SMB.CONF` contains a valid wins server entry), entries in an `lmhosts.` file, or using broadcasts on the local subnet. Use the `nmblookup` tool as described in Chapter 8 (page 83) to determine if NetBIOS name resolution is effective.
 3. Alternately, the `$ NET RPC JOIN` command provides options to designate the name (`--server`) or the IP address (`--ipaddress`) of the domain PDC. If the name is specified, `$ NET RPC JOIN` will use NetBIOS name resolution to resolve the name to its IP address.
 4. The `$ NET RPC JOIN` command will not make use of the “password server” parameter if specified in the `SMB.CONF` file.
 5. Use the command `$ NET RPC TESTJOIN` any time after joining the domain to verify the server is joined to the domain properly.
-

Windows Domain Model

You can use the Windows Domain Model in environments with the following characteristics:

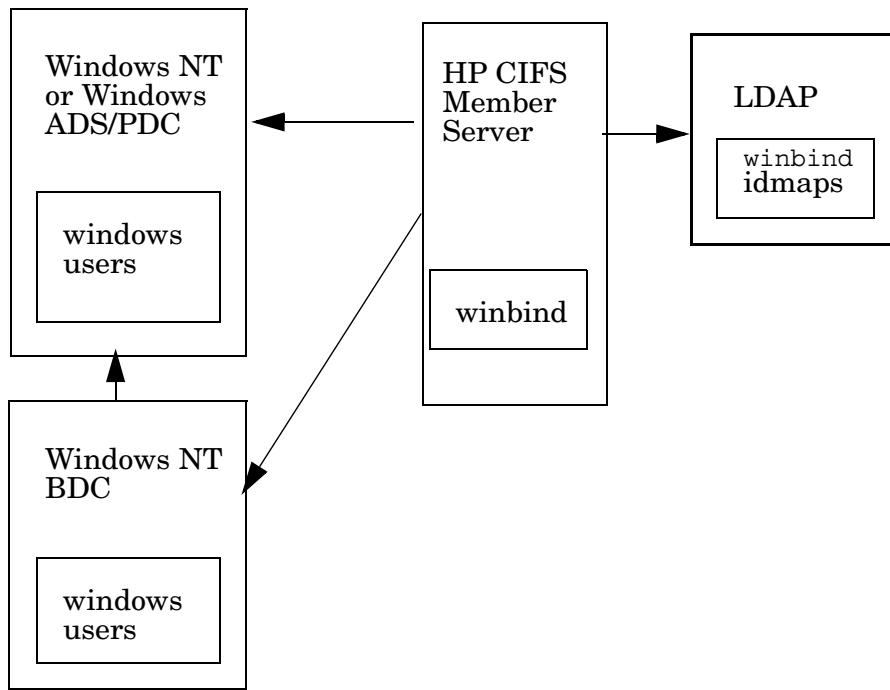
- Deploy Windows NT4, Advanced Server for OpenVMS, or Windows 200x servers (with NetBIOS enabled).
- Support for any number of HP CIFS member servers that provide file and print services.
- Access to an LDAP Enterprise Directory Server as the backend storage for larger deployments to maintain winbind ID maps across multiple HP CIFS Servers.

The Windows Domain Model provides the following benefits:

- Support for Windows domain member single sign on, network logon, and Windows account management system.
- Support for easy user management across multiple HP CIFS Servers by using winbind.
- Easy expansion capability.

Figure 3-4 shows the Windows Domain Deployment Model as follows:

Figure 3-4 Windows Domain



In the Windows Domain Model, HP CIFS Server can join a Windows domain as a member server with Windows NT or Windows 200x domain controllers. HP CIFS Server supports winbind to provide User ID (UID) and Group ID (GID) mappings for Windows users. For a larger deployment environment, you can use the LDAP directory to maintain unique ID maps across multiple HP CIFS Servers.

Components for Windows Domain Model

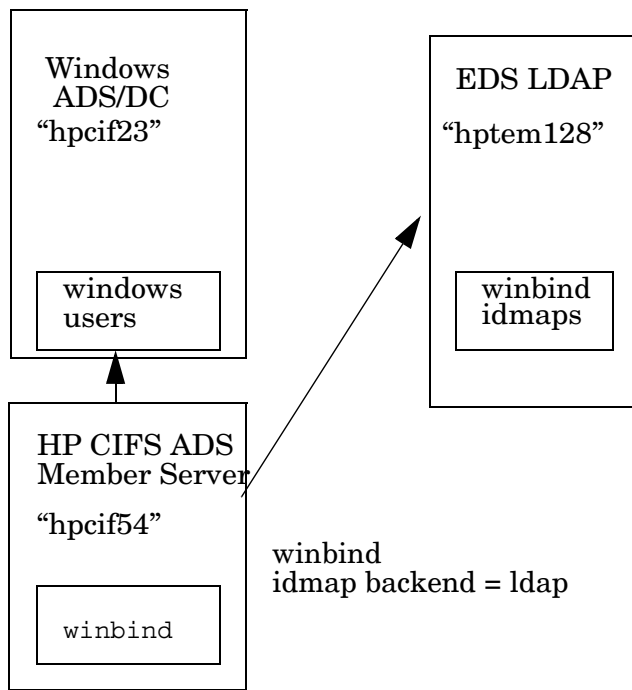
HP CIFS Server supports the NTLMv1/NTLMv2 security used for NT domain membership, so HP CIFS Servers can be managed in any Windows 2000/2003 ADS, Windows 200x mixed mode, or NT environment. HP CIFS Server does not support a true SAM database and can not participate as a domain controller in an Windows NT, Windows 2000 or Windows 2003 domain. HP CIFS Server supports winbind, which can be used to avoid explicitly allocating OpenVMS users and groups for Windows users and groups mapping. Winbind provides UID and GID generation and mapping for Windows users. Set `SMB.CONF` parameters to `idmap uid = <uid range>` and `idmap gid = <gid range>`. For more information on winbind, see [Chapter 5 \(page 59\)](#). When you deploy multiple HP CIFS Servers, you can use the LDAP directory to maintain unique ID maps across multiple systems. Otherwise, user mapping will not be consistent from system to system. To centralize management of ID maps in an LDAP directory, set the `idmap backend` parameter to `ldap:ldap://<ldap server name>` in the `SMB.CONF` file.

You can use `wins server = <Windows or NT WINS server address>` `SMB.CONF` parameter for access throughout a multi-subnetted network.

An Example of the ADS Domain Model

Figure 3-5 shows an example of the Windows 2000/2003 ADS Domain Model which has an domain controller machine `hpcif23`, an HP CIFS Server machine `hpcif54` acting as a member server and the Enterprise Directory Server system `hptem128`.

Figure 3-5 An example of the ADS Domain Model



A sample SMB.CONF file For an HP CIFS ADS Member Server

The following is a sample HP CIFS configuration File, SAMBA\$ROOT: [LIB] SMB.CONF, used for an HP CIFS Server machine hpcif54 acting as a ADS member server in the sample ADS Domain Model shown in Figure 3-5:

```

#####
#
# An sample smb.conf file for an HP CIFS ADS member server
#
# Global Parameters
[global]
# Domain Name
workgroup = hpcif23_dom
server string = CIFS Server as a domain member of hpcif23_dom
security = domain
netbios name = hpcif54
encrypt passwords = yes
password server = hpcifs23
passdb backend = ldapsam:ldap://<name or IP address of the node>
log level = 0
log file = /samba$root/var/log.%m
max log size = 1000
host msdfs = no

# For idmap configuration of winbind
idmap backend = ldap:ldap://hptem128
idmap uid = 1000-10000
idmap gid = 1000-10000
ldap server = hptem128
ldap admin dn = "cn=Directory Manager"
ldap suffix = dc=org, dc=hp, dc=com
ldap port = 389
ldap idmap suffix = ou=ldmap

[homes]
comment = Home Directory
browseable = no
writable = yes
  
```

```
create mode = 0664
directory mode = 0775
```

```
[share1]
path = /tmp
read only = no
```

```
[tmp]
path=/tmp
read only = no
browseable = yes
writable = yes
```

The following is a sample HP CIFS configuration File, `SAMBA$ROOT: [LIB] SMB.CONF`, used for an HP CIFS Server machine `hpcif54` acting as a ADS member server in the sample ADS Domain Model with `passdb` backend as `tdbsam`:

```
#####
#
# An sample smb.conf file for an HP CIFS ADS member server
#
# Global Parameters
[global]
# Domain Name
workgroup = hpcif23_dom
server string = CIFS Server as a domain member of hpcif23_dom
security = domain
netbios name = hpcif54
encrypt passwords = yes
password server = hpcifs23
passdb backend = tdbsam
log level = 0
log file = /samba$root/var/log.%m
max log size = 1000
host msdfs = no

# For idmap configuration of winbind
idmap uid = 1000-10000
idmap gid = 1000-10000

[homes]
comment = Home Directory
browseable = no
writable = yes
create mode = 0664
directory mode = 0775

[share1]
path = /tmp
read only = no

[tmp]
path=/tmp
read only = no
browseable = yes
writable = yes
```



NOTE: HP CIFS Server supports several ways to allocate and map OpenVMS users and groups to domain users and groups. If winbind is used, winbind can create and maintain mappings for users and groups. For more information about winbind mapping, see “[User and Group Mapping](#)” (page 63). If winbind is not used, a local OpenVMS account associated with each Windows user and group must be created.

Roaming Profiles

The HP CIFS Server, configured as a PDC, supports Roaming Profiles with the following features:

- A user's environment, preference settings, desktop settings, etc. are stored on the HP CIFS Server
- Roaming Profiles can be created as a share, and be shared between Windows clients
- When a user logs on to a workstation in the domain, the roaming profile is downloaded from the share which is on a HP CIFS Server configured as a PDC, to the local machine. Upon logout, the profile is copied back to the server

Configuring Roaming Profiles

Use the following procedure to configure roaming profiles:

1. Modify or enable roaming profiles by using the global parameter named `logon path`, in the `smb.conf` file. Example:

```
[global]
#%L substitutes for this servers NetBIOS name, %U is user name
logon path = \\%L\profile\%U
workgroup = SAMBADOM
security = user
encrypt passwords = yes
domain logon = yes
```
2. Create a `[profiles]` share for roaming profiles. Set `profile acls = yes` for the profile share used for the user profile files. Do not set `profile acls = yes` on normal shares as this will result in incorrect ownership of the files created on those shares. The following is an example configuration for the `[profiles]` share:

```
[profiles]
profile acls = yes
path = /samba$root/profiles
read only = no
create mode = 600
directory mode = 770
writeable = yes
browseable = no
guest ok = no
```

Configuring User Logon Scripts

The logon script configuration must meet the following requirements:

- User logon scripts should be stored in a file share called `[net logon]` on the HP CIFS Server.
- Should be set to OpenVMS executable permission.

- Any logon script should contain valid commands recognized by the Windows client.
- A logon user should have proper access permissions to execute logon scripts.

The following is an example configuration for user logon scripts:

```
[global]
logon script = %U.bat
[netlogon]
path = /samba$root/netlogon
browseable = no
guest ok = no
```

Trust Relationships

Trust relationships enable users authenticated in one domain, commonly referred to as the "trusted" domain, to access resources in another domain, commonly referred to as the "trusting" domain. There are various types of trusts, depending on the domain type. The concept of trusts was introduced in Windows NT domains and has been extended and expanded in Windows Active Directory domains. HP CIFS server supports the same types of trusts supported by Windows NT (and Advanced Server for OpenVMS). The characteristic of these trusts is they are one-way - one domain trusts another but the reverse does not automatically apply. If both domains are to trust each other, then two one-way trusts (commonly referred to as a two-way trust) are required, one in each direction. For more information on trusts, consult the Microsoft Technet papers at <http://technet.microsoft.com>.

The process of establishing a one-way trust involves administration in both domains. An administrator in the trusted domain must first establish the trust in the trusted domain (where the user logons are authenticated) and specify a password which is provided to the administrator of the trusting domain to use when completing the trust establishment in the trusting domain.

Establishing the Trust in the Trusted Domain

The method of establishing the trust in the trusted domain depends on the type of PDC. The procedure for an HP CIFS PDC is covered here. For information on other type of PDCs, refer to the documentation for that system.

1. Create an OpenVMS account name that matches the name of the trusting domain and append a dollar sign (\$).

For example, if the NetBIOS name of the trusting domain is `trustingdom`, execute the command:

```
$ MC AUTHORIZE ADD TRUSTINGDOM$ /UIC=[1000,1] /FLAG=NODISUSER
```

2. Create an interdomain trust account in the CIFS user database using the `$ NET RPC TRUSTDOM` command. Specify the name of the trusted domain (do not include the trailing dollar sign) a password of your choosing (used when establishing the trust in the trusting domain), and credentials of an administrator of the domain. The account name must be identical to the OpenVMS account created in step 1 above. In the following example, the name of the trusting domain is `trustingdom`:

```
$ NET RPC TRUSTDOM ADD TRUSTINGDOM ANYPASSWORDUChOOSE --USER
CIFSADMIN
```

```
Password: <cifsadmin-password>
```

Establishing the Trust in the Trusting Domain

After establishing the trust in the trusted domain, complete the trust creation by establishing the trust in the trusting domain. The password used in establishing the trust in the trusted domain

is required to complete the trust creation in the trusting domain. The method of establishing the trust in the trusting domain depends on the type of PDC. The procedure for an HP CIFS PDC is covered here. For information on other type of PDCs, refer to the documentation for that system.

To complete the trust, use the command below and supply the name of the trusted domain. You will be prompted for the trust password.

```
$ NET RPC TRUSTDOM ESTABLISH <TRUSTED-DOMAIN-NAME>
PASSWORD: <TRUST-PASSWORD>
```

Viewing List of Trusts

To view a list of trusts, use the `$ NET RPC TRUSTDOM list` command:

```
$ NET RPC TRUSTDOM LIST --USER CIFSADMIN
PASSWORD: <CIFSADMIN-PASSWORD>
```

Establishing a Two-way Trust Relationship between an HP CIFS Domain and a Windows Active Directory Domain

Step-by-Step Procedure

1. Configure HP CIFS Server as a PDC. For configuring HP CIFS Server as a PDC, see [“Configure the HP CIFS Server as a PDC”](#) (page 41).
2. If the HP CIFS domain PDC and Windows domain PDC Emulator are not on the same subnet, configure the PDC of both domains to use WINS or add the appropriate entries in the `lmhosts.` file on both.

The following example shows the `lmhosts.` file entries required on the Windows PDC emulator for the HP CIFS PDC named NEWTON at IP address 16.148.195.74 in domain NEWTONDOM:

```
16.148.195.74 newton #PRE #DOM:newtondom
16.148.173.74 "newtondom \0x1b" #PRE
```



NOTE: There must be exactly 20 characters between the quotes in the above entry. The domain name must be space-padded to 15 characters, followed by `\0x1b`.

The following example shows the `lmhosts.` file entries required on the HP CIFS PDC for the Windows PDC Emulator named WINPDC at IP address 16.138.185.206 in domain WINDOM:

```
16.138.185.206 WINPDC
16.138.185.206 WINDOM#1B
```

3. Establishing the Trust in the Trusted Domain

Since this is a two-way trust, you need to establish the trust in both HP CIFS and Windows domain.

For more information on establishing the trust in the trusted domain on HP CIFS, see [“Establishing the Trust in the Trusted Domain”](#) (page 48).

4. Establishing the Trust

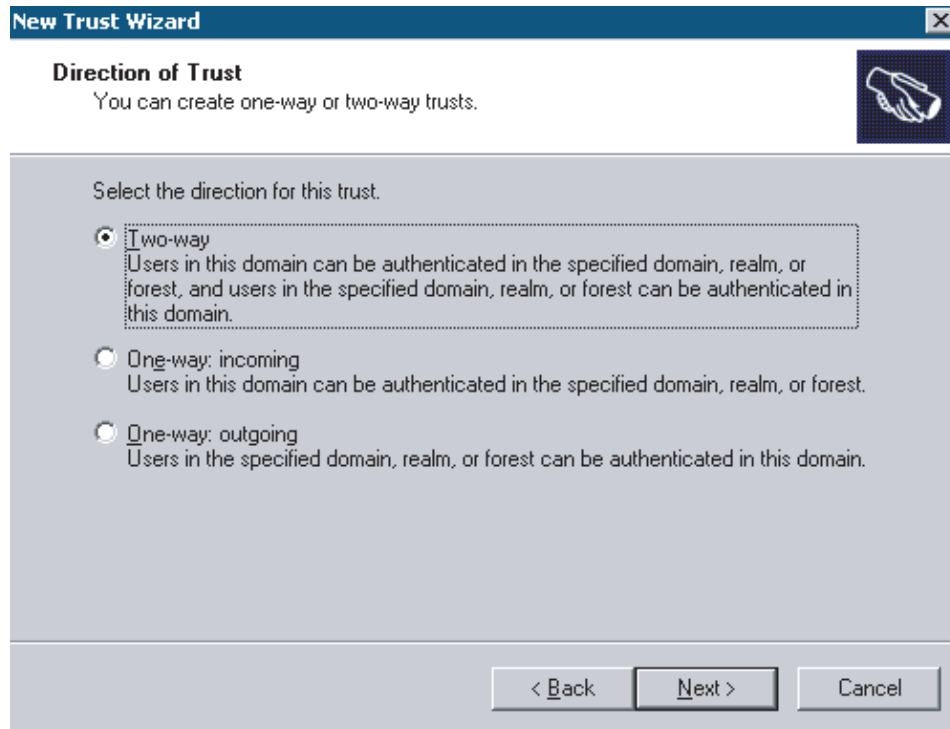
To establish two-way trust, follow these steps:

On Windows PDC

- a. Open Active Directory Domains and Trusts on the Active Directory controller of the domain whose resources you wish HP CIFS users to have access to.
- b. Click the **Trusts** tab, and then click **New Trust**.
- c. The New Trust Wizard appears. Click **Next**.

- d. Enter the HP CIFS Domain name in the **Name** box. For example, type newtondom, and then click **Next**.
- e. In the Direction of Trust Window, select **Two-way**.

Figure 3-6 Direction of Trust



- f. Click **Next**, and then select Domain-wide Authentication.
- g. Click **Next**, and then in the Trust password box, type a password for this trust.
- h. Type the password again in the Confirm trust password box, and then click **Next**.
- i. In the Confirm Outgoing Trust Window, select **Yes**, confirm the outgoing trust.
- j. In the Confirm Incoming Trust Window, enter the HP CIFS User name and Password. Click **Next**.



NOTE: The user must be a admin user.

On HP CIFS PDC

For more information on establishing the trust in the trusting domain, See “Establishing the Trust in the Trusting Domain” (page 48).

You will be prompted for the password that you entered on your Windows PDC box.



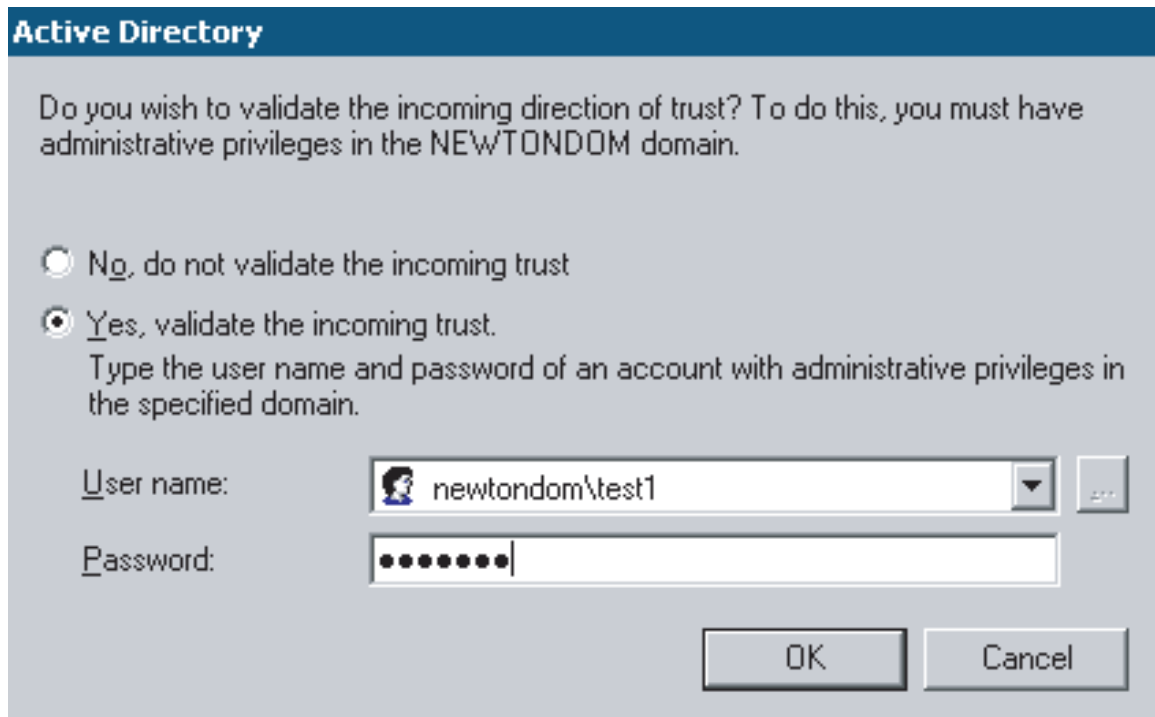
NOTE: An error message, "NT_STATUS_NOLOGON_INTERDOMAIN_TRUST_ACCOUNT," that may be reported periodically is of no concern and may safely be ignored. It means the password you gave is correct and the NT4 server says the account is ready for interdomain connection and not for ordinary connection. After that, be patient; it can take a while (especially in large networks), but eventually you should see the Success message.

Validating the Trust Relationships

To validate the trust relationship on Windows PDC, click **Validate**.

In the Active Directory Window, enter the HP CIFS User name and Password. Click OK.

Figure 3-7 Active Directory



The image shows a Windows dialog box titled "Active Directory". The text inside asks: "Do you wish to validate the incoming direction of trust? To do this, you must have administrative privileges in the NEWTONDOM domain." There are two radio button options: "No, do not validate the incoming trust" and "Yes, validate the incoming trust." The "Yes" option is selected. Below the options, it says "Type the user name and password of an account with administrative privileges in the specified domain." There are two input fields: "User name:" with the text "newtondom\test1" and a dropdown arrow, and "Password:" with a masked password field showing ten dots. At the bottom right are "OK" and "Cancel" buttons.

You will see the following success message " The trust has been validated. It is in place and active".

4 LDAP Integration Support

This chapter describes the HP CIFS Server with LDAP integration. It includes benefits of LDAP, procedures to configure HP CIFS Server software with LDAP as password backend. This chapter addresses the following topics:

- “Overview”
- “Network Environments”
- “Installing and Configuring Your Directory Server”
- “Configuring the HP CIFS Server”

Overview

Lightweight Directory Access Protocol (LDAP) provides a framework for the development of a centralized management infrastructure. LDAP supports directory enabled computing by consolidating applications, services, user accounts, Windows account, and configuration information into a central LDAP directory.

HP CIFS customer sites with large numbers of users and servers may want to integrate the HP CIFS Server with LDAP support. Configuring multiple HP CIFS Servers to communicate with the LDAP directory server provides a centralized and scalable management of user databases. When you integrate the HP CIFS Server with the LDAP product on OpenVMS, the HP CIFS Server can store user account information on the Enterprise Directory Server. The LDAP database can replace `tddbSam`, or NT server user databases.

The LDAP directory can be used to store Windows user information, which had previously been stored in the `passwd.tdb` file. When the HP CIFS Server is configured to use the LDAP password integration, the `SMBD` program uses the LDAP directory to look up the Windows user information during the authentication and authorization processes. Also, when you invoke the `pdbedit` program to add, delete, or change user information, updates are made in the LDAP user database rather than the `passwd.tdb` file used by the `tddbSam` backend.

You can enable the LDAP support with configuration parameters provided by the HP CIFS Server. HP CIFS Server will access an LDAP directory server for password, user, group, and other data when you set the `SMB.CONF passwd backend` parameter to `ldapsam`.

HP CIFS Server Advantages

The HP CIFS Server with LDAP support provides the following benefits to the customer:

- Reduces the need to maintain user account information across multiple HP CIFS Servers, as LDAP provides a centralized user database management.
- Easily adds multiple HP CIFS Servers or users to the LDAP directory environment. This greatly improves the scalability of the HP CIFS Server.
- Stores and looks up user account information in the LDAP directory.
- The amount of information stored in the `tddbSam` file has no room for additional attributes. With the LDAP support, the schema is extensible, you can store more user information in the LDAP directory. This also eliminates the need for additional employee and user databases.

Network Environments

The HP CIFS Server supports many different network environments. Features such as WINS, browser control, domain logons, roaming profiles, and many others continue to be available to support a diverse range of network environments. LDAP integration provides one more alternative solution for HP CIFS user authentication.

Domain Model Networks

HP CIFS Server Acting as Primary Domain Controller (PDC)

Since PDCs are responsible for Windows authentication, HP CIFS Servers configured as PDCs replace `tdbsam` with LDAP enabled directory servers for Windows authentication. Other Samba configuration items may remain unchanged.

HP CIFS Server Acting as Backup Domain Controller (BDC) to Samba PDC

Since BDCs are also responsible for Windows authentication, HP CIFS Servers configured as BDCs can access the LDAP directory for user authentication. BDC configuration is similar to PDC configuration with the exception that you can set the `SMB.CONF` parameter `domain master` to `no`.

HP CIFS Server Acting as the Member Server

HP CIFS Servers acting as member servers in the domain model network environment can continue to operate as member servers without changing their Samba configuration. The Windows authentication requests will continue to be managed by the PDC whether through LDAP or `tdbsam`.

If a member server (`security = domain`) is also configured to enable LDAP, it tries to authenticate via the PDC. If the PDC authentication fails, it tries to authenticate directly via the LDAP directory server set in its own `SMB.CONF` configuration file.

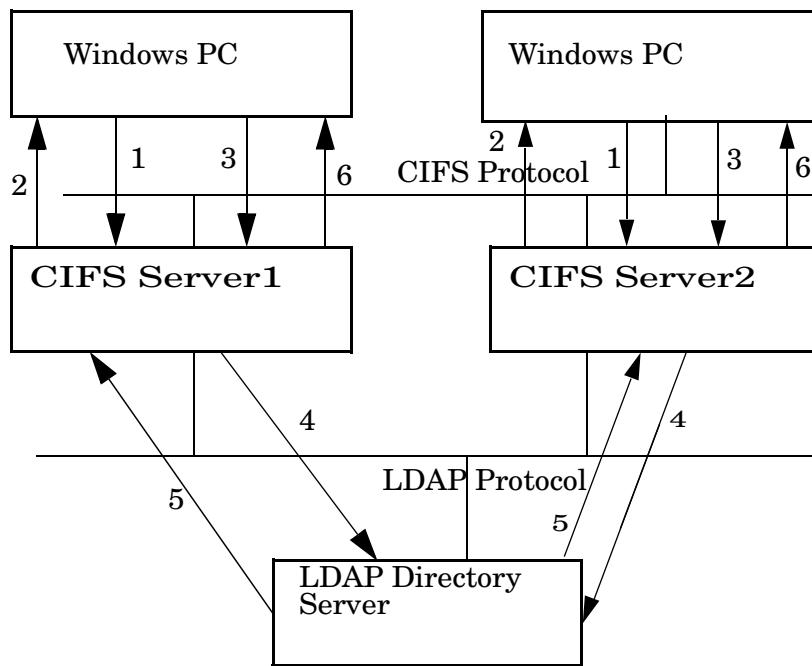
Workgroup Model Networks

If LDAP is enabled, authentication will fall back to the LDAP server if the user mode authentication fails. HP CIFS Servers configured as standalone user mode servers may replace `tdbsam` with an LDAP directory server.

The CIFS Authentication with LDAP Integration

With LDAP integration, multiple HP CIFS Servers can share a single LDAP directory server for a centralized user database management. The HP CIFS Server can access the LDAP directory and look up the Windows user information for user authentication. Figure 4-1 illustrates CIFS authentication in an LDAP network environment.

Figure 4-1 CIFS Authentication with LDAP Integration



The following describes the message exchanges between the Windows PC, CIFS Server, and LDAP directory server for user authentication shown in Figure 4-1:

1. A Windows user requests a connection.
2. The CIFS Server sends a challenge to the Windows PC client.
3. The Windows PC client sends a response packet to the CIFS Server based on the user password and the challenge information.
4. The CIFS Server looks up the LDAP directory server for user data and requests data attributes including password information.
5. The CIFS Server receives data attributes, including password information, from the LDAP directory server. If the password and challenge information match the information in the client response package, the user authentication succeeds.
6. If the user is authenticated and is successfully mapped to a valid OpenVMS user, the CIFS Server returns a user token session ID to the Windows PC client.

Installing and Configuring Your Directory Server

This section describes how to set up and configure the HP OpenVMS Enterprise Directory.

Installing the Directory Server

You need to set up the HP OpenVMS Enterprise Directory Server if it is not already installed. For more information on how to install a Directory Server, see the *HP OpenVMS Enterprise Directory Installing*.

Configuring the Directory Server

HP OpenVMS Enterprise Directory has been updated with a Samba Schema file to support the LDAP backend for HP CIFS. This is based on the assumption that the HP OpenVMS Enterprise Directory acts as the LDAP backend for HP CIFS. For more information on how to configure LDAP, see the *HP OpenVMS Enterprise Directory Management*.

Perform the following steps to configure LDAP as the HP CIFS password backend:

1. Invoke Network Control Language (NCL) from a privileged account, and enter the following command to create HP CIFS specific naming contexts:

```
$ MC NCL
```

```
NCL> CREATE DSA NAMING CONTEXT "/SAMBADOMAIN= <samba_domain_name>"
```

where:

/SAMBADOMAIN is part of the DIT structure that is created under LDAP (X500) tree.

SAMBA_DOMAIN_NAME is the domain name specified in the DIT structure and also defined in the SAMBA.SC Schema file.

2. Invoke DXIM, and enter the following command to create HP CIFS specific directory entries:

```
$ DXIM /I=C
```

```
DXIM> CREATE "/SambaDomainName = <samba_domain_name>" ATTRIBUTES -  
_DXIM>objectClass=(sambaDomain),sambaDomainName="<samba_domain_name>",sambaSID=<SID_VALUE>
```

where:

/SAMBADOMAIN is part of the DIT structure that is created under LDAP (X500) tree.

SAMBA_DOMAIN_NAME is the domain name specified in the DIT structure and the following sambaDomain, sambaDomainName and sambaSID are defined in the SAMBA.SC Schema file.



NOTE: You can obtain the sambaSID value using the NET RPC INFO command. To do so, enter the following command:

```
$ NET RPC INFO "-U" <adminuser%"passwordofadmin">
```

```
$ NET RPC INFO "-U" "administrator%Welcome123"
```

```
Domain Name: NEWTONDOM
```

```
Domain SID: S-1-5-21-2259843773-1199894201-4032371524
```

```
Sequence number: 33677
```

```
Num users: 5563
```

```
Num domain groups: 55
```

```
Num local groups: 58
```

3. Create an LDAP admin account in the LDAP directory. Use the distinguished name (dn) of that account as the value for the SMB.CONF global parameter ldap admin dn; for example:

```
ldap admin dn = cn=ldapadmin, cn=users, dc=my-domain, dc=mycompany,  
dc=com
```


Configuring the HP CIFS Server

You must set up and configure your HP CIFS Server to enable the LDAP feature support by adding password for the LDAP admin account created in step 3 in “[Configuring the Directory Server](#)” to the SAMBA\$ROOT: [PRIVATE] SECRETS . TDB file for use by HP CIFS, when accessing the LDAP server using the following command:

```
$ smbpasswd -"W" <ldap-admin-password>
```

LDAP Configuration Parameters

Table 4–1 lists the new global parameters available for you to configure the HP CIFS Server to enable LDAP. These parameters are set in the SAMBA\$ROOT: [LIB] SMB . CONF file global section.

Any global setting defined here is used by the HP CIFS Server with the LDAP support.

Table 4-1 Global LDAP Parameters

Parameter	Description
ldap port	Specifies the TCP port number used to connect to the LDAP directory server. By default, this parameter is set to 389.
ldap server	Specifies the host name or IP address of the LDAP server.
ldap suffix	Specifies the base of the directory tree where you want to add user and machine account information. It is also used as the distinguished name (dn) of the search base, which tells LDAP where to start the search for the entry. For example, if your base DN is "dc=org, dc=hp, dc=com", then use ldapsuffix = "dc=org, dc=hp, dc=com".
ldap user suffix	Specifies the base of the directory tree where you want to add users information. The suffix string is pre-pended to the ldap suffix string so use a partial distinguished name (dn). If you do not specify this parameter, HP CIFS Server uses the value of ldap suffix. For example, ldap user suffix = "ou=People".
ldap group suffix	Specifies the base of the directory tree where you want to add group information. The suffix string is pre-pended to the ldap suffix string so use a partial distinguished name (dn). If you do not specify this parameter, HP CIFS Server uses the value of ldap suffix instead. For example, ldap group suffix = "ou=Groups".
ldap admin dn	Specifies the user distinguished name (dn) used by the HP CIFS Server to connect to the LDAP directory server when retrieving user account information. The ldap admin dn is used in conjunction with the password stored in the secrets.tdb file. For example, ldap admin dn = "cn = directory manager cn=users, dc=org, dc=hp, dc=com".
ldap delete dn	Specifies whether a delete operation in the ldapsam deletes the complete entry or only the attributes specific to Samba. The default value is No , delete only the Samba attributes.
ldap passwd sync	Specifies whether the HP CIFS Server should sync the LDAP password with the NT and LM hashes for normal accounts on a password change. This option can be set to one of three values: <ul style="list-style-type: none">• Yes: Update the LDAP, NT, and LM passwords and update the pwdLastSet time.• No: Update NT and LM passwords and update the pwdLastSet time.• Only: Only update the LDAP password and let the LDAP server do the rest. The default value is No .

Table 4-1 Global LDAP Parameters *(continued)*

Parameter	Description
ldap replication sleep	When CIFS is requested to write to a read-only LDAP replica, it is redirected to talk to the read-write master server. This server then replicates the changes back to the local server. The replication might take a few seconds, especially over slow links. Certain client activities can become confused by the 'success' that does not immediately change the LDAP back-end's data. This option simply causes CIFS to wait a short time and allows the LDAP server to catch up. The value is specified in milliseconds, the maximum value is 5000 (5 seconds). By default, ldapreplication sleep = 1000 (1 second).
ldap timeout	Specifies, in seconds, how long the HP CIFS Server waits for the LDAP server to respond to the connect request if the LDAP server is down or unreachable. The default value is 15 (in seconds).
ldap idmap suffix	Specifies the suffix that is used when storing idmap mappings. If this parameter is unset, the value of ldap suffix will be used instead. The suffix string is pre-pended to the ldap suffix string so use a partial distinguished name (dn). By default, ldap idmap suffix = . For example, ldap idmap suffix = ou=Idmap.
ldap machine suffix	Specifies where machines should be added to the ldap tree. If this parameter is unset, the value of ldap suffix will be used instead. The suffix string is pre-pended to the ldap suffix string so use a partial distinguished name (dn). By default, ldap machine suffix = . For example, ldap machine suffix = ou=Computers.

5 Winbind Support

This chapter describes the HP CIFS winbind feature and explains when to use it and how best to configure its use. This chapter addresses the following topics:

- “Overview”
- “Winbind Features”
- “Winbind Process Flow”
- “User and Group Mapping”
- “Disabling Winbind”
- “Configuring HP CIFS Server with Winbind”
- “LDAP Backend Support ”

Overview

HP CIFS Server must resolve the fact that OpenVMS and Microsoft Windows use different technologies to represent user and group identity. Winbind is an HP CIFS feature which is one of several different ways in which HP CIFS can map the Windows implementation of user and group security identifiers, SIDs, to the OpenVMS implementation of user and group identifiers, UIDs, and GIDs. The purpose of winbind is to automate the creation of UIDs and GIDs and maintains their correspondence to the appropriate Windows SIDs to minimize identity management efforts.

Winbind must be understood before you configure HP CIFS Server because choosing an appropriate configuration for your environment is the key to minimize IT management problems. Choosing the best way to map identities for your environment is important because directories and files populate file systems with permissions based on the identities of the owners. Over time, the difficulty of changing user maps will increase unless the proper configuration is chosen initially. This chapter will help you understand winbind and configure HP CIFS appropriately.

For more information about winbind, see *Samba 3.0 HOWTO Reference Guide* at the following web address:

<http://us3.samba.org/samba/docs/man/Samba-HOWTO-Collection/>



NOTE: You can refer the *Samba 3.0 HOWTO Reference Guide* for the winbind functionality as it remains same on HP CIFS for OpenVMS, but the implementation method is different.

Winbind Features

Winbind provides the following features:

- User and group ID allocation

When winbind is presented with a Windows SID, for which there is no corresponding UID and GID, winbind generates a UID and GID. Depending on the configuration, winbind uses the following algorithm for creating IDs:

- Local increment

Winbind default settings result in ID values based on a simple increment above the current highest value within a defined range. The pool of values is confined to the local HP CIFS Server.



WARNING!

- You can back up and restore the idmap file to avoid recreating the UID and GID maps. The local increment model requires the idmap file to be backed up frequently.
 - The solution is limited by the fact that UID and GID values may differ between systems for the same Windows user. Also, if the idmap file is recreated, the UID and GID maps could differ from the previous map which can lead to serious security issues (file ownership may change).
-

- ID mapping

Winbind creates mappings between Windows SIDs and corresponding OpenVMS UIDs and GIDs. Winbind uses the method described above to create a mapping between OpenVMS UIDs/GIDs and Windows SIDs. With a Windows SID, winbind either finds the existing UID and GID map or creates a new map if none currently exists.

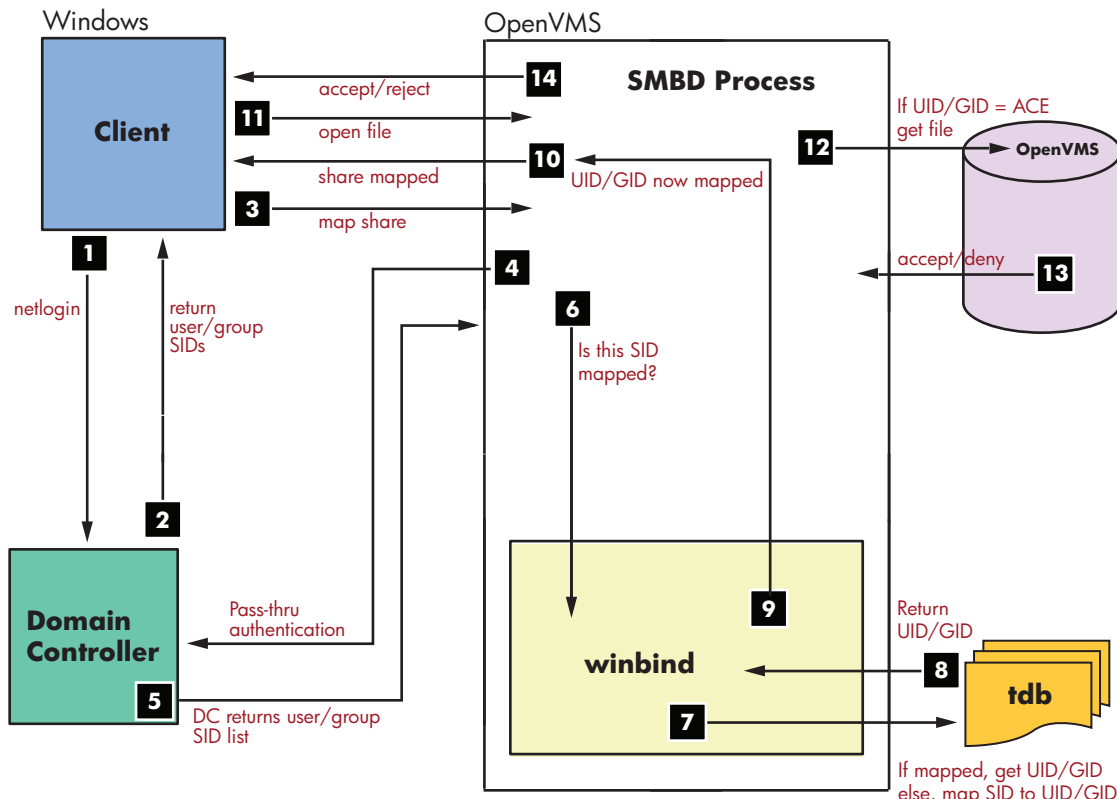
- Identity storage

Winbind maintains a database where it stores the mappings between OpenVMS UIDs and GIDs and Windows SIDs. In the simplest case, winbind maintains the database in a local Trivial Data Base (TDB) file called `winbind_idmap.tdb` in the directory `SAMBA$ROOT:[VAR.LOCKS]`.

Winbind Process Flow

Figure 5–1 shows the winbind process flow in a Windows Domain environment with HP CIFS configured as a member server.

Figure 5-1 Winbind Process Flow



The following describes the winbind process flow shown in Figure 5–1:

1. A Windows client logs in to the domain (authentication).
2. The Windows domain controller authenticates client and returns user security data.
3. The Windows client maps an HP CIFS share.
4. The HP CIFS Member Server passes the user name to Windows Domain Controller to verify the user is a domain member.
5. The Windows Domain Controller returns the user authorization and member SID list.
6. The smbd process passes the SID and user information to the winbind module internal to the Smbd process.
7. Winbind checks the SID and user name against ID mapping data in its mapping database. Winbind either finds the existing mappings between the Windows SID and the OpenVMS UID/GID or creates a new map if no mapping currently exists.
8. Return the mapped UID or GID from TDB database.
9. Winbind returns UID and GID mappings to smbd.
10. The HP CIFS Server presents the mapped share to the Windows client.
11. The Windows client opens file on the HP CIFS Server share.
12. UID and GID are compared with file owner, group, and any ACE in the ACL.
13. The File open action is accepted or denied based on the result in step 12.
14. The HP CIFS Server returns the open status to the Windows client.

Winbind Functionality

Winbind supports the following functionalities:

- Automatic Mapping
- Nested Group Support
- Trusts

Automatic Mapping

For domain users and groups, winbind automatically creates the corresponding OpenVMS user or group (resource identifier) on an HP CIFS Member server if one does not exist. Winbind obtains the user IDs (UIDs) used to assign a UIC value, and group IDs (GIDs) used to assign a value to the Resource Identifier from the `SMB.CONF` global parameters `"idmap UID"` and `"idmap GID"`, which must be set to a range of values allocated solely to winbind.

Winbind uses the chosen integer `"idmap UID"` value, to derive both the OpenVMS account name and the UIC. The UID value is converted to a hexadecimal value and appended to the string `"CIFS$"` to derive the OpenVMS account name. The UID value is converted to octal and the octal value is used as the UIC group and member number.



NOTE: Since UIC group numbers are limited to a maximum value of Octal 37776 (decimal 16382), the upper range limit on the `"idmap UID"` value is 16382. Similarly, because UIC groups numbers below Octal 376 are reserved for use by HP, do not specify a value below 255 as the lower range of `"idmap UID"`.

For example, if the `SMB.CONF` file contains:

```
idmap uid = 5000 - 10000
```

Winbind will allocate UID 5000 and create an OpenVMS account named `CIFS$1388` with a UIC of `[11610.11610]`. The mapping of UID 5000 to `CIFS$1388` is stored in the `SAMBA$ROOT: [VAR.LOCKS] WINBINDD_IDMAP.TDB` file. This file must be backed up regularly to avoid the loss of the required mappings necessary to maintain security.

A similar process occurs for groups. Winbind uses the chosen integer `"idmap GID"` value to derive the name of the OpenVMS identifier it creates. The GID is converted to a hexadecimal value which is appended to the string `"CIFS$GRP"` to derive the name.



NOTE: Because winbind creates Posix Group Resource Identifiers, the maximum value is limited to `%xFFFFFF` or `%d16777215`. The lower limit is 1. HP CIFS adds `%xA4000000` to the value chosen.

For example, if the `SMB.CONF` file contains:

```
idmap gid = 5000 - 10000
```

Winbind will initially allocate GID 5000 and create an OpenVMS Resource Identifier named `CIFS$GRP1388`. The mapping of GID 5000 to `CIFS$GRP1388` is stored in `SAMBA$ROOT: [VAR.LOCKS] WINBINDD_IDMAP.TDB`. It is critical that this file be backed up regularly as its loss will result in loss of the required mappings necessary to maintain security.

Nested Group Support

Winbind is required for nested group support. Nested groups are local groups that contain domain global groups (thus, a group-within-a-group, or "nested" groups). Nested groups are defined locally on any machine and can contain users and global groups from any trusted SAM.

Trusts

Winbind is required for all Trust functionality.

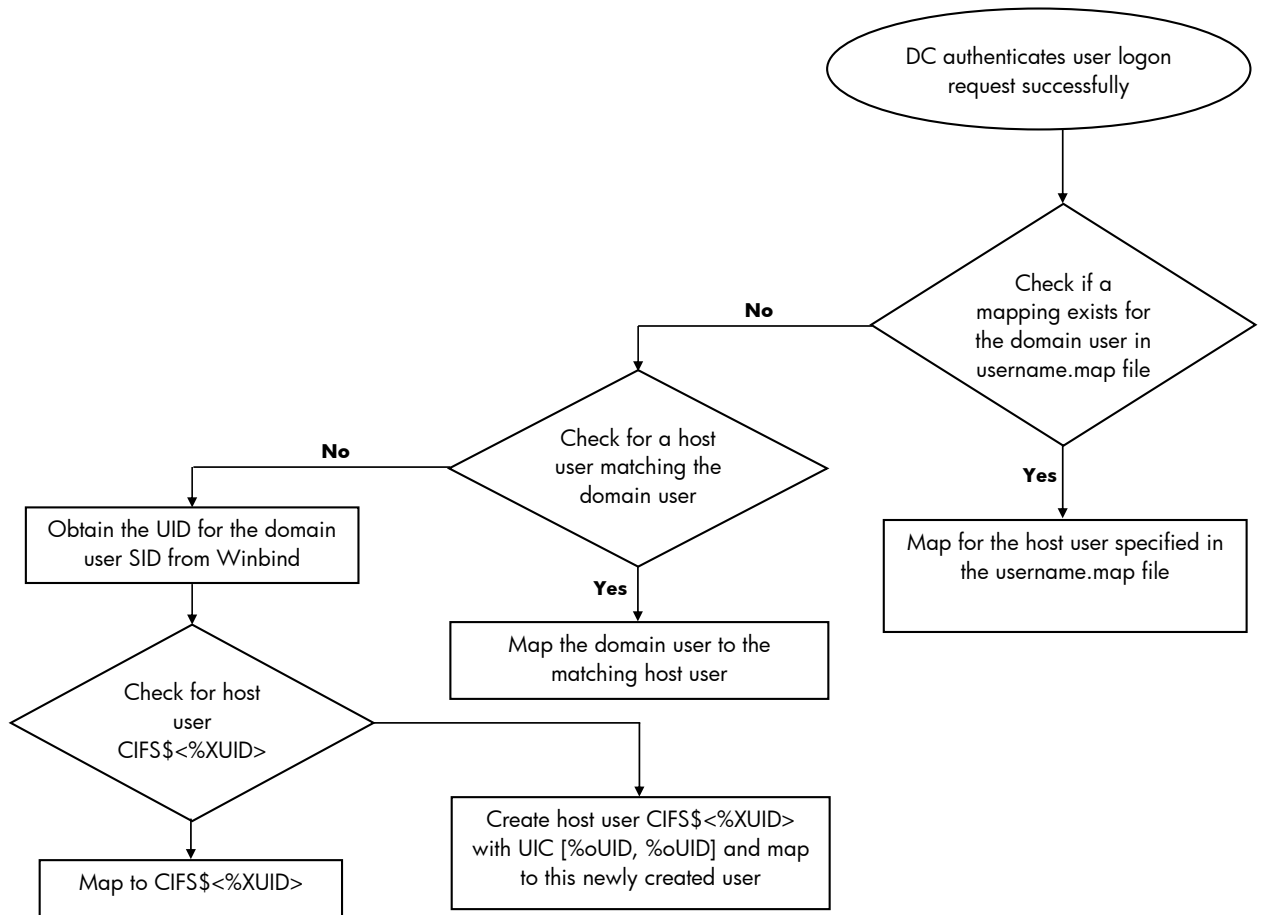
User and Group Mapping

This section describes automatic mapping of user authentication and host mapping and group mapping in a members server environment.

User Authentication and Host Mapping Process Flow

Figure 5–2 shows user authentication and host mapping process flow in a member server environment.

Figure 5-2 User Authentication and Host Mapping Process Flow



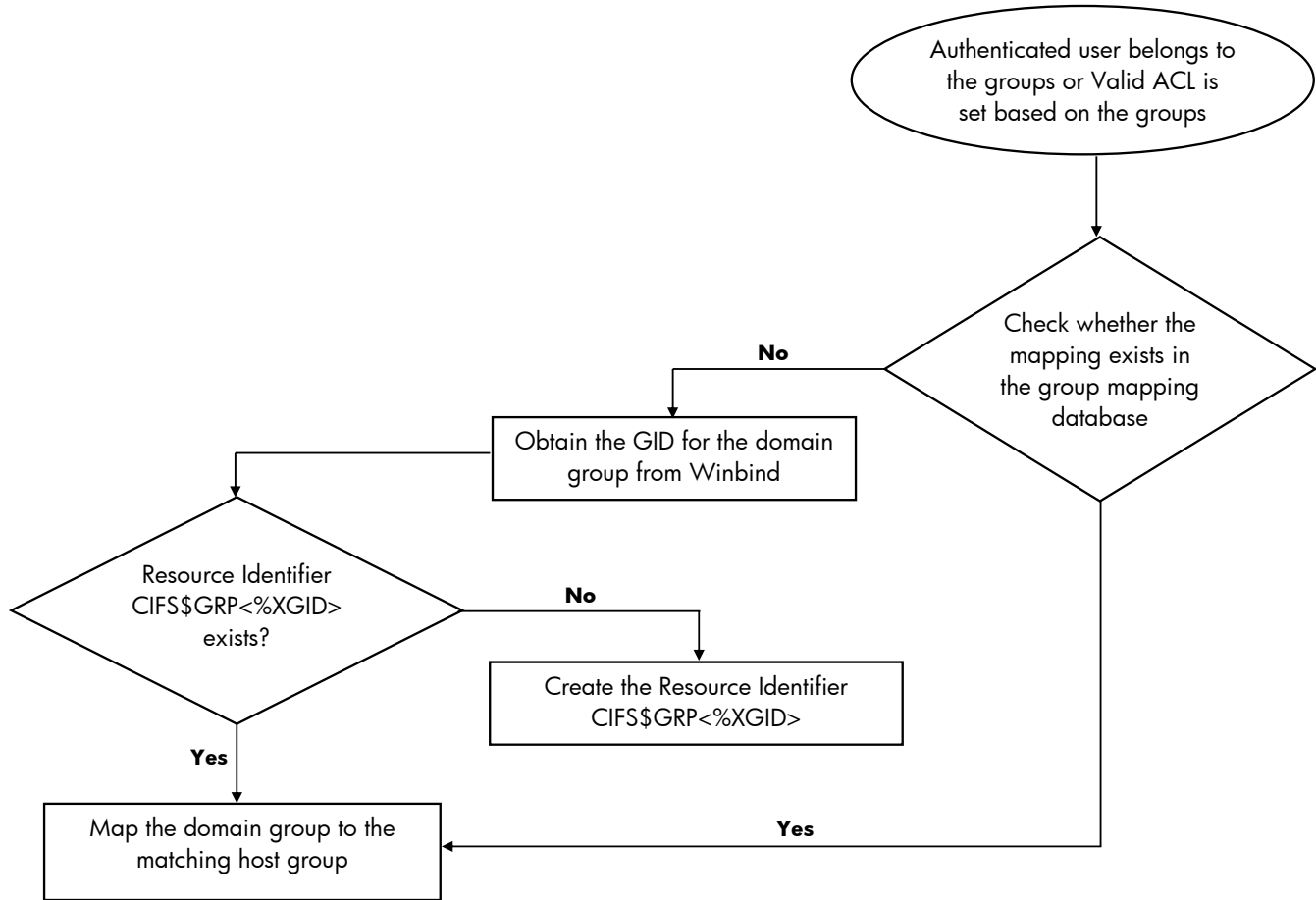
The following describes user authentication and host mapping process flow shown in Figure 5–2:

1. A domain user is authenticated successfully from the Domain Controller or an ACL is being added based on a user.
2. HP CIFS checks if a mapping exists for the domain user in username map file. If there is a corresponding mapping, CIFS uses the mapped user.
3. If there is no mapping, HP CIFS checks for a corresponding host user, matching the domain user. If there is a match CIFS uses that host user.
4. If there is no corresponding host user, it obtains the UID for the domain user SID from the winbind, if enabled.
5. With UID obtained, HP CIFS check for the host user in the format CIFS\$<hexadecimal-value-of-UID>. If there is a user already present in the host system database, HP CIFS maps to this user.
6. If no host account exists, HP CIFS creates one named CIFS\$<%XUID>, with a UIC value of [%oUID, %oUID] and maps this to the domain user.

Group Mapping Process Flow

Figure 5–3 shows group mapping process flow in a member server environment.

Figure 5-3 Group Mapping Process Flow



The following describes group mapping process flow shown in Figure 5–3:

1. An authenticated domain user belongs to a group or a valid ACL is being added based on a group.
2. HP CIFS obtains the GID for the domain group from winbind.
3. HP CIFS checks for a resource identifier of the format CIFS\$GRP<%XGID>. If there is a match, HP CIFS maps the domain group to the matching resource identifier.
4. If there is no corresponding Resource Identifier, HP CIFS creates it in the format CIFS\$GRP<%XGID>.

Disabling Winbind

Unlike in Samba Linux/UNIX in HP CIFS for OpenVMS, the Winbind functionality is integrated with the SMBD process. Hence, no separate winbind daemon process is created.

Winbind functionality is not required for all HP CIFS configurations. If CIFS needs to be configured as a standalone server, it is not mandatory to configure and enable winbind. To disable winbind on HP CIFS, define the following logical:

```
$ DEFINE/SYSTEM WINBINDD_DONT_ENV 1
```

Winbind is also disabled if the `SMB.CONF` does not contain the "idmap uid" and "idmap gid" parameters.

Configuring HP CIFS Server with Winbind

You must set up and configure your HP CIFS Server to use the winbind feature support.

Winbind Configuration Parameters

Table 5-1 lists the global parameters used to control the behavior of winbind. These parameters are set in the `SAMBA$ROOT:[LIB]SMB.CONF` file in the `[global]` section. For more information, see the `SMB.CONF` manpage.

Table 5-1 Global Parameters

Parameter	Description
security	Winbind requires Windows Domain authentication. security = domain or security = ads
winbind separator	This string variable specifies the separator to separate domain name and user name. For example, winbind separator = \.
idmap uid	This variable specifies the UID range for domain users. For example, idmap uid = 5000-6000
idmap gid	This variable specifies the GID range for domain groups. For example, idmap gid = 5000-6000
idmap backend	This string variable specifies the type of the idmap backend that is used. The syntax can be: <ul style="list-style-type: none">idmap backend = This is the default when the local idmap tdb file is used.idmap backend = ldap:ldap://<ldap server name>[:389] The ID mapping data is stored in a common LDAP directory server backend. For example, idmap backend = ldap:ldap://ldapserversA.hp.com.
winbind cache time	This integer variable specifies the number of seconds the winbind caches user and group information before querying a Windows NT server again. The default value is 300.

A SMB.CONF Example

An example of SMB . CONF file is shown below:

```
[global]
# Doamin name
workgroup = DomainA
security = domain
# Winbindd section
idmap uid = 5000-6000
idmap gid = 50000-60000
idmap backend = idmap_tdb
winbind cache time = 300
winbind separator = \
```

LDAP Backend Support

When multiple CIFS Servers participate in a Windows NT or Windows ADS domain and use winbind, you can configure multiple CIFS Servers to store ID maps in an LDAP directory. Using LDAP server and configuring CIFS servers with the `idmap backend` parameter in `SMB.CONF` will ensure that all UIDs and GIDs are unique across the domain.

wbinfo Utility

You can use the `wbinfo` tool to get information from winbind. For more information on this tool, see “[wbinfo](#)” (page 91).

6 Managing Users, Groups, and File Access

Introduction

This chapter describes how to manage users and groups on the HP CIFS Server. It also describes how to set and modify file access controls either from the OpenVMS host or from a Windows domain member.

Managing Local Users in Member Server or PDC or BDC

This section describes how to manage local users in an HP CIFS server that is configured as a member server in an active directory domain or PDC or BDC.

To add a local user in the member server or PDC or BDC database, follow these steps:

1. Verify whether the user exists on the host system. If not, add the user to the system. For more information about adding a user to the system, see the *HP OpenVMS System Manager's Manual*.
2. Ensure that the user added to the host system has unique UIC and ADD_IDENTIFIER qualifiers, that the rights identifier matches the user name, and that the flag is set to NODISUSER.



NOTE: The default template, SAMBA\$TMPLT, can be used to create a new OpenVMS user account for HP CIFS.

```
$ MC AUTHORIZE
```

```
UAF> COPY SAMBA$TMPLT TEST1 /UIC=[500,500]/add_identifier
```

3. Verify whether the user exists on the HP CIFS database. If not, add the user to the system by entering the following command. For more information on the `pdbedit` tool, see “[pdbedit](#)” (page 85).

```
$ pdbedit -a <USERNAME>
```

For example,

```
$ pdbedit -a TEST1
```



NOTE: Ensure that the user exists on the host system before adding the account to the HP CIFS database.

4. To delete the user account, enter the following command:

```
$ pdbedit -x <USERNAME>
```

5. You can modify the user account by entering the following command:

```
$ pdbedit -r <USERNAME>
```

6. On OpenVMS, only an administrator can change a HP CIFS user's password. To change the password, use the `smbpasswd` utility:

```
$ smbpasswd USER1
```

New SMB password:

Retype new SMB password:

Alternatively, the HP CIFS user password can be changed from Windows client by pressing **Ctrl+Alt+Delete** and then clicking **Change Password**.

Managing Local Groups in Member Server

This section describes how to set up groups in a HP CIFS Server that is configured as member server in the active directory domain.

To manage local groups in HP CIFS Server that is configured as member server, follow these steps:

1. When you execute any of the net commands that involve HP CIFS server management tasks, ensure that you have a privileged CIFS user account. For example, to create a privileged HP CIFS user account 'CIFSADMIN', follow these steps:
 - a. Create 'CIFSADMIN' as the OpenVMS account, and grant full privileges to this account.
 - b. Create a HP CIFS account by entering the following commands:

```
$ @SAMBA$ROOT: [BIN] SAMBA$DEFINE_COMMANDS.COM
$ pdbedit -a CIFSADMIN
```

2. In the SMB.CONF file, add "admin users = *<privileged account>*" under the [global] section or add this user to the "Administrators" group.

For example,

```
[global]
admin users = cifsadmin
```

3. On the PDC emulator of the active directory domain, create an account with the same name as used in step 1. You can either create a privileged domain account or a normal user account.
4. To add a local group on the CIFS member server, follow these steps:

- a. Add the resource identifier in the SYSUAF database by entering the following command:

```
$ MC AUTHORIZE ADD/IDENTIFIER/ATTRIBUTE=RESOURCE <vms-group>
```

For example, to add a resource identifier for the 'VMSGROUP':

```
$ MC AUTHORIZE ADD/IDENTIFIER/ATTRIBUTE=RESOURCE VMSGROUP
```

- b. Using the net command, map the member server local group and host group by entering the following command:

```
$ NET GROUPMAP ADD NTGROUP =<windows-group> UNIXGROUP =
<vms-group> TYPE="L" "-W" <workgroup> "-S" <cifs-node-name> "-U"
<adminuser>%"<password-of-adminuser>"
```

For example, to map the local member server group 'CIFSGROUP' to the group 'VMSGROUP':

```
$ NET GROUPMAP ADD NTGROUP=CIFSGROUP UNIXGROUP=VMSGROUP -
_$TYPE="L" "-W" PIANO "-S" CIFS-PIANO "-U" CIFSADMIN%"PWD OF
CIFSADMIN"
```

5. To list the local groups in an HP CIFS member server, enter the following command:

```
$ NET RPC GROUP LIST "-W" <workgroup> "-S" <cifs-node-name> "-U"
<adminuser>%"<password-of-adminuser>"
```

For example, to list the local group HP CIFS member server on the node 'CIFS-PIANO':

```
$ NET RPC GROUP LIST "-W" PIANO "-S" CIFS-PIANO "-U" CIFSADMIN%"PWD
OF CIFSADMIN"
```

6. To add the local member server user or group to the local group, enter the following command:

```
$ NET RPC GROUP ADDMEM <windows-group> <local-user-or-group> "-W"
<Workgroup> "-S" <cifs-node-name> "-U"
<adminuser>%"<password-of-adminuser>"
```

For example, to add the local member server user or group 'CATHY' to the group 'CIFSGROUP':

```
$ NET RPC GROUP ADDMEM CIFSGROUP CATHY "-W" PIANO "-S" CIFS-PIANO  
"-U" CIFSADMIN%"PWD OF CIFSADMIN"
```

7. To list the members of the local HP CIFS group, enter the following command:

```
$ NET RPC GROUP MEMBERS <windows-group> "-S" <cifs-node-name> "-U"  
<adminuser>%"<password-of-adminuser>"
```

For example, to list the members of the group 'CIFSGROUP':

```
$ NET RPC GROUP MEMBERS CIFSGROUP "-W" PIANO "-S" CIFS-PIANO "-U"  
CIFSADMIN%"PWD OF CIFSADMIN"
```

8. To add a domain user or group to a local HP CIFS group, enter the following command:

```
$ NET RPC GROUP ADDMEM <windows-group>  
<domain-name>\<domain-user-or-group> "-W" <workgroup> "-S"  
<cifs-node-name> "-U" <adminuser>%"<password-of-adminuser>"
```

For example, to add a domain user or group 'CIFSDOM\CINDY' to the local group 'CIFSGROUP':

```
$ NET RPC GROUP ADDMEM CIFSGROUP CIFSDOM\CINDY "-W" PIANO "-S"  
CIFS-PIANO "-U" CIFSADMIN%"PWD OF CIFSADMIN"
```

9. To delete a domain user or group from the local HP CIFS group, enter the following command:

```
$ NET RPC GROUP DELMEM <windows-group>  
<domain-name>\<domain-user-or-group> "-W" <workgroup> "-S"  
<cifs-node-name> "-U" <adminuser>%"<password-of-adminuser>"
```

For example, to delete a domain user or group from the local group 'CIFSGROUP':

```
$ NET RPC GROUP DELMEM CIFSGROUP "-W" PIANO "-S" CIFS-PIANO "-U"  
CIFSADMIN%"PWD OF CIFSADMIN"
```

10. To delete the local HP CIFS group, enter the following command:

```
$ NET RPC GROUP DELETE <windows-group> "-S" <cifs-node-name> "-U"  
<adminuser>%"<password-of-adminuser>"
```

For example, to delete the local group 'CIFSGROUP':

```
$ NET RPC GROUP DELETE CIFSGROUP "-W" PIANO "-S" CIFS-PIANO "-U"  
CIFSADMIN%"PWD OF CIFSADMIN"
```

Managing Groups in PDC or BDC

This section describes how to set up groups in a HP CIFS Server that is configured as PDC or BDC.

To manage groups in HP CIFS Server that is configured as PDC or BDC, follow these steps:

1. When you execute any of the net commands that involve CIFS server management tasks, ensure that you have a privileged CIFS user account. For example, to create a privileged HP CIFS user account 'CIFSADMIN', follow these steps:
 - a. Create 'CIFSADMIN' as the OpenVMS account, and grant full privileges to this account.
 - b. Create a HP CIFS account by entering the following commands:

```
$ @SAMBA$ROOT: [BIN] SAMBA$DEFINE_COMMANDS.COM
$ pdbedit -a CIFSADMIN
```

2. In the SMB.CONF file, add "admin users = *<privileged account>*" under the [global] section or add this user to the "Administrators" group and restart the HP CIFS Server.

For example,

```
[global]
admin users = cifsadmin
```

3. To add a local or domain group on the HP CIFS PDC or BDC, follow these steps:
 - a. Add the resource identifier in the SYSUAF database by entering the following command:

```
$ MC AUTHORIZE ADD/IDENTIFIER/ATTRIBUTE=RESOURCE <vms-group>
```

For example, to add a resource identifier for the 'VMSGROUP':

```
$ MC AUTHORIZE ADD/IDENTIFIER/ATTRIBUTE=RESOURCE VMSGROUP
```

- b. Using the net command, map the PDC or BDC local or domain group to host group by entering the following command:

```
$ NET GROUPMAP ADD NTGROUP =<LocalGroupName-or-DomainGroupName>
UNIXGROUP = <vms-group> TYPE=<LocalGroup-or-DomainGroup> "-W"
<workgroup> "-S" <cifs-node-name> "-U"
<adminuser>%"<password-of-adminuser>
```

For example, to map the local group 'CIFSGROUP' to the group 'VMSGROUP':

```
$ NET GROUPMAP ADD NTGROUP=CIFSGROUP UNIXGROUP=VMSGROUP -
_$ TYPE="L" "-W" PIANO "-S" CIFS-PIANO "-U" CIFSADMIN%"PWD OF
CIFSADMIN"
```

For example, to map the domain group 'CIFSDOMGROUP' to the group 'VMSGROUP':

```
$ NET GROUPMAP ADD NTGROUP=CIFSDOMGROUP UNIXGROUP=VMSGROUP -
_$ TYPE="D" "-W" PIANO "-S" CIFS-PIANO "-U" CIFSADMIN%"PWD OF
CIFSADMIN"
```

4. To list the local or domain groups of HP CIFS Server, enter the following command:

```
$ NET RPC GROUP LIST "-W" <workgroup> "-S" <cifs-node-name> "-U"
<adminuser>%"<password-of-adminuser>
```

For example, to list the local or domain group HP CIFS server on the node 'CIFS-PIANO':

```
$ NET RPC GROUP LIST "-W" PIANO "-S" CIFS-PIANO "-U" CIFSADMIN%"PWD
OF CIFSADMIN"
```

5. To add the local user or group to the local or domain group, enter the following command:

```
$ NET RPC GROUP ADDMEM <local-or-domain-group> <local-user-group>
-W" <Workgroup> -S" <cifs-node-name> -U"
<adminuser>%"<password-of-adminuser>
```

For example, to add the local user or group 'CATHY' to the group 'CIFSGROUP':

```
$ NET RPC GROUP ADDMEM CIFSGROUP CATHY -W" PIANO -S" CIFS-PIANO
-U" CIFSADMIN%"PWD OF CIFSADMIN"
```
6. To list the members of the local or domain HP CIFS group, enter the following command:

```
$ NET RPC GROUP MEMBERS <local-or-domain-group> -S" <cifs-node-name>
-U" <adminuser>%"<password-of-adminuser>
```

For example, to list the members of the group 'CIFSGROUP':

```
$ NET RPC GROUP MEMBERS CIFSGROUP -W" PIANO -S" CIFS-PIANO -U"
CIFSADMIN%"PWD OF CIFSADMIN"
```
7. To add a domain user or group to a local or domain HP CIFS group, enter the following command:

```
$ NET RPC GROUP ADDMEM <local-or-domain-group>
<domain-name>\<domain-user-or-group> -W" <workgroup> -S"
<cifs-node-name> -U" <adminuser>%"<password-of-adminuser>
```

For example, to add a domain user or group 'CIFSDOM\CINDY' to a HP CIFS local or domain group 'CIFSGROUP':

```
$ NET RPC GROUP ADDMEM CIFSGROUP CIFSDOM\CINDY -W" PIANO -S"
CIFS-PIANO -U" CIFSADMIN%"PWD OF CIFSADMIN"
```
8. To delete a domain user or group from the local or domain HP CIFS group, enter the following command:

```
$ NET RPC GROUP DELMEM <local-or-domain-group>
<domain-name>\<domain-user-or-group> -W" <workgroup> -S"
<cifs-node-name> -U" <adminuser>%"<password-of-adminuser>
```

For example, to delete a local or domain group from the local group 'CIFSGROUP':

```
$ NET RPC GROUP DELMEM CIFSGROUP -W" PIANO -S" CIFS-PIANO -U"
CIFSADMIN%"PWD OF CIFSADMIN"
```
9. To delete the local HP CIFS group, enter the following command:

```
$ NET RPC GROUP DELETE <local-or-domain-group> -S" <cifs-node-name>
-U" <adminuser>%"<password-of-adminuser>
```

For example, to delete the local or domain group 'CIFSGROUP':

```
$ NET RPC GROUP DELETE CIFSGROUP -W" PIANO -S" CIFS-PIANO -U"
CIFSADMIN%"PWD OF CIFSADMIN"
```

Username Mapping

Username map allows you to map domain user names to host names. Due to a restriction in the OpenVMS SYSUAF, HP CIFS does not support user accounts with more than 12 characters and does not allow some special character in the user name. However, this can be overcome by modifying the username map parameter under the [global] section in the SMB.CONF file.

In the member server configuration, username mapping is applied only after the user has been successfully authenticated by the domain controllers. In a standalone server configurations, the username mapping is applied before validating the user credentials.

Username mapping can be specified using the following parameter in the SMB.CONF file under [global] section:

```
username map = /samba$root/lib/username.map
```



NOTE: This `username.map` template file is provided with the HP CIFS Server software kit and can be located in the following directory `SAMBA$ROOT: [LIB] USERNAME.MAP`. If you create a user name map file on OpenVMS system, ensure that the file format is in Stream record format.

The map file is parsed line by line. Each line must contain a single *<vms-host-name>* on the left of a '=' sign followed by a list of user names on the right.

For example, to map administrator of "GANGES" to System, enter as follows:

```
System=GANGES\administrator
```

In the `username.map` file comment lines begin with '#' or ';'. For example,

```
#cifsuser = GANGES\Tunga
```

If a line begins with an '!' then the processing will stop after that line if a mapping was done by the line. Otherwise mapping continues with every line being processed. Using '!' is most useful when you have a wildcard mapping line later in the file. For example,

```
!cifsuser=GANGES\Tunga
```

Username mapping allows mapping Windows user names containing spaces in them by using double quotes around the name. For example, to map "Himalaya River" to the user Ganga, enter as follows:

```
Ganga="Himalaya River"
```

You can also map multiple users to a single hostname. For example, to map multiple users `GANGES\narmada` and `GANGES\kaveri` to user `asvuser`, enter as follows:

```
asvuser=GANGES\narmada GANGES\kaveri
```

To map all the users to a single hostuser, you can use the wildcard as shown in the example below.

```
cifs$default=*
```

Note that with this setting all the users will have similar permissions.

Managing HP CIFS Security

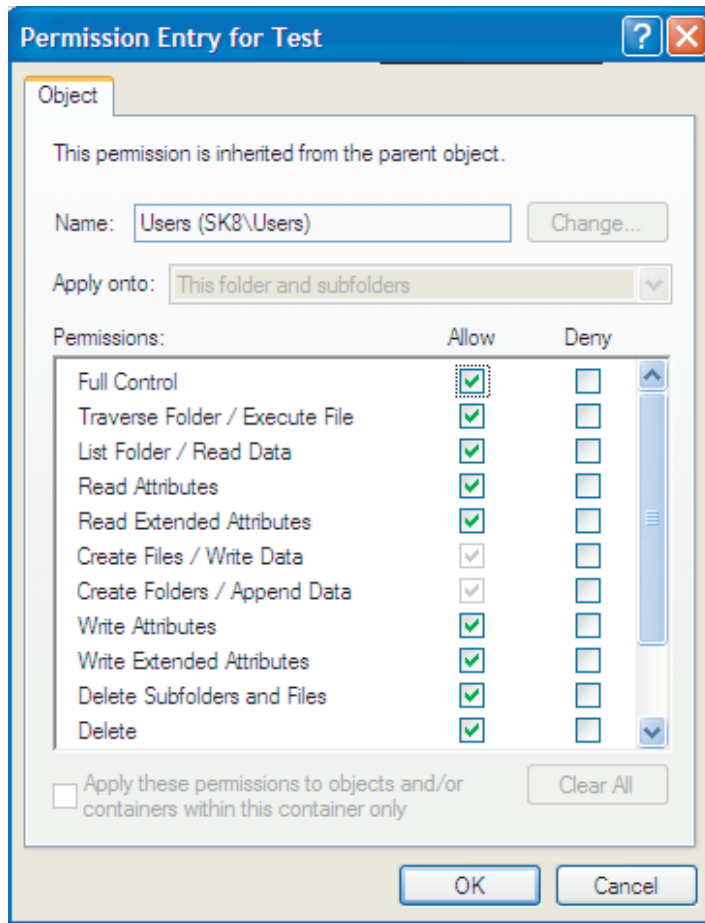
Managing File and Directory Protections

This section describes how to set or modify protection on a file or directory for member server, PDC, and BDC in HP CIFS Server. Use one of the following methods as explained below.

Method 1: Setting protections from Windows system which is a member of the domain

1. Connect to the HP CIFS Server using the privileged account.
2. Right-click on a file or a directory and select **Properties**.
3. Click **Security**.
4. Click **Advanced**.
5. Select an ACE or Permission entries, click **Edit**.
6. In the Permission Entry for test screen, check/uncheck the boxes next to each permission to add/remove any permission that you want. Figure 6–1 shows modifying ACE permissions.

Figure 6-1 Modifying ACE Permissions



7. Click **OK**. The Advanced Security Settings screen appears. Repeat step 4 through step 6 to modify or set other ACEs.
8. Click **OK** or **Apply** on the Advanced Security Settings screen.
9. Verify the security protection settings on the command-line in the host system by entering the following command:

```
$ DIR/PROT <file/directory path>
$ DIR/PROT/OWN TEMP.TXT
Directory DKA0: [SAMBA.TEMP.TEST2] temp.txt;1
temp.txt;1      [TELNETS,TEST1]          (RWED,RWED,RWD,R)
Total of 1 file
```



NOTE: An error message is displayed if you try to set protections from the windows system which is not a member of the domain.

To manage protection on PDC or BDC, first you need to add Windows client as workstation to the domain. For adding Windows client as workstation, see “Configure the HP CIFS Server as a PDC” (page 41). After adding Windows client as workstation, follow the procedure as described in section “Managing File and Directory Protections” (page 72) for settings protections on PDC or BDC.

Method 2: Setting protections using native VMS DCL command

Use the following DCL command to set or modify protection on a file or a directory:

```
$ SET SECURITY/PROT= (OWNERSHIP [:ACCESS] [, . . . ] )
```



NOTE: The above-mentioned methods are applicable for setting protections for files created on PDC or BDC.

Managing File and Directory ACLs

This section describes how to set or modify ACLs on a file or a directory that is configured as a member server in HP CIFS. Use one of the following methods as explained below.

Method 1: Setting ACLs from Windows system which is a member of the domain

1. Connect to the HP CIFS Server using the privileged account.
2. Right-click on a file or a directory and select **Properties**.
3. Click **Security**.
4. Click **Advanced**.
5. Click on **Add**. The *Select Users, Computers, or Groups* window is displayed.
6. Click **Locations** to specify the search location.
7. In the *Enter the object names to select (examples): box*, type the names of the objects you want to search for and click **Check Names**.

If Windows system can resolve the names it underlines the name that you have added by post fixing the corresponding domain names appropriately.

8. Click **OK**. A dialog box appears prompting you to enter ACE permissions and the type of ACE.
9. Enter the desired permissions and click **OK**.
10. Click **OK** or **Apply** on the *Advanced Security Settings* screen to add the new ACE.
11. Verify the ACL settings on the command-line in the host system by entering the following command:

```
$ DIR/SEC <file/directory path>
```

12. The appropriate ACEs are added with the host user names with the Identifiers.
13. Execute the `SAMBA$UAF_TO_CIFSNAME.COM` command procedure to get the user and group mappings. See the following for more information about user and group mappings:
 - “Managing Local Users in Member Server or PDC or BDC” (page 67)
 - “Managing Local Groups in Member Server ” (page 68)
 - “Managing Groups in PDC or BDC ” (page 70)



NOTE: Please note that `SAMBA$UAF_TO_CIFSNAME.COM` lists only those users or groups that are created by winbind.

Method 2: Setting ACLs using native DCL command for Member Server

1. Log into the SYSTEM account or a privileged account.

2. For setting ACLs based on the users, follow these procedures to find out the resource identifier for a user:
 - a. For local user, the identifier will be the local host user name.
 - b. For domain user, execute the following command procedure and then choose option 1.

```
$ @SAMBA$ROOT: [BIN] SAMBA$UAF_TO_CIFSNAME.COM
```

The host name displayed for each domain user is the identifier for that domain user.



NOTE: Please note that SAMBA\$UAF_TO_CIFSNAME.COM lists only those users or groups that are created by winbind.

3. For setting ACLs based on the groups, follow these procedures to find out the resource identifier for a group:
 - For local group, enter the following command:

```
$ NET GROUPMAP LIST
```

The name that maps to the corresponding local group is the resource identifier.
4. For domain group, execute the following command procedure and then choose option 2.

```
$ @SAMBA$ROOT: [BIN] SAMBA$UAF_TO_CIFSNAME.COM
```

The host name displayed for each domain group is the identifier for that domain group.



NOTE: The domain group has a resource identifier of the format CIFS\$GRP<hexa value of the number displayed>.

5. To add an ACL for a file or share or folder, enter the following command:

```
$ set security/acl=(identifier=<resource-identifier>,  
access=read+execute) <filename/share path directory/sub folder>
```

For example, if you want to grant "read" and "execute", permissions, you can execute:

```
$ set security/acl=(identifier=<resource-identifier>,  
access=read+execute) <filename/share path directory/sub folder>
```
6. To remove the ACL, execute the following command:

```
$ set security/acl=(identifier=<resource-identifier>)/delete  
<file/folder/share path directory name>
```

Setting ACLs using native DCL command for PDC or BDC

1. Log into the SYSTEM account or a privileged account.
2. For setting ACLs based on the users or group, follow these procedures to find out the resource identifier for a user:
 - a. For a user, the identifier will be the local host user name.
 - b. For a group, enter the following command:

```
$ NET GROUPMAP LIST
```

The name that maps to the corresponding group is the resource identifier.
3. To add an ACL for a file or share or folder, enter the following command:

```
$ set security/acl=(identifier=<resource-identifier>,  
access=read+execute) <filename/share path directory/sub folder>
```

For example, if you want to grant "read" and "execute", permissions, you can execute:

```
$ set security/acl=(identifier=<resource-identifier>,  
access=read+execute) <filename/share path directory/sub folder>
```

4. To remove the ACL, execute the following command:

```
$ set security/acl=(identifier=<resource-identifier>)/delete  
<file/folder/share path directory name>
```

7 Configuring Printers

Introduction

This chapter provides information about configuring Print Services on systems running HP CIFS version 1.1. The HP CIFS Server now provides the following NT printing functionalities:

- Printer driver files may be downloaded to Windows 2000, XP, and Vista clients that do not have them
- Printer driver files may be uploaded using the Windows 2000//XP/Vista Add Printer wizard
- Support for Windows Access Control Lists (ACL) on printer objects

Information about setting up and configuring each of the Print Services (except ACLs) is described in the following sections.

Configuring a Printer Share

The following is a minimal printing setup. Use either *one* of the following two procedures to create a printer share:

1. SWAT (Samba Administration Tool)
- or-
2. Create a share stanza in the `SMB.CONF` file. The name of the printer share must be the same as the OpenVMS print queue.



NOTE: If the share name and print queue name are different, create an OpenVMS logical name of the same name as the printer share and equate it to the OpenVMS queue name.

Include the line `"printable = yes"` in the share stanza to designate the share as a printer share. Also specify a path statement indicating the location where spool files will be stored while printing. For example, to add a printer share named `HPLASER`, add the following lines to `SMB.CONF` file:

```
[HPLASER]
    path = /samba$root/var/spool
    printable = yes
```

Creating the Spool Directory

To create a spool directory, follow these steps:

1. Create the spool directory by entering the following command:

```
$ CREATE/DIR SAMBA$ROOT: [VAR.SPOOL]
```
2. Set the security on the spool directory to allow users to write to it. For example, to allow all users to write to the directory:

```
$ SET SECURITY/PROT= (W:RWE) SAMBA$ROOT: [VAR] SPOOL.DIR
```
3. Change the ownership of spool directory by entering the following command:

```
$ SET SECURITY/PROT= (W:REW) / -
_$
ACL= (DEFAULT_PROTECTION, SYSTEM:RWED, OWNER:RWED) SAMBA$ROOT: [VAR] SPOOL.DIR
```



NOTE: Spool directory holds the print jobs when they are submitted for printing.

Queue Setup

This section describes the different OpenVMS queue setups that are supported by HP CIFS. It includes the following sections:

- DCPS Print Queues
- TCPIP\$TELNETSYM Print Queues
- LPD Print Queues

DCPS Print Queues

To add a DCPS print queue, edit `SYS$STARTUP:DCPS$STARTUP.COM` and add the following lines for the print queue as shown:

```
$ @SYS$STARTUP:DCPS$EXECUTION_QUEUE -
<print-queue-name> -                ! P1 - Execution queue name
"ip_rawtcp/<printer-ip-address>:9100" - ! P2 - Interconnect protocol
DCPS_LIB -                          ! P3 - Logical name for libraries
"DATA=<data-type>" -                 ! P4 - Default queue parameters
"/SEPARATE=(NOBURST,NOFLAG,NOTAIL)" - ! P5 - Default queue qualifiers
"" -                                ! P6 - Communication speed(serial
- ! devices only)
"" -                                ! P7 - Device characteristics
"" -                                ! P8 - Verify on/off
```

1. Substitute P1 with an appropriate name to create the DCPS execution queue name.
2. The "ip_rawtcp" in P2 enables DCPS to support "Raw TCP" printing.
3. The P2 can be replaced with "IP_LPD/<printer-ip-address>" if you want to use DCPS IP_LPD printing. HP CIFS VMS is also tested with DCPS IP_LPD print queues. However, you must define the logical "DCPS\$_<print-queue-name>_PRODUCT_NAME", which is required for the printer driver when using DCPS IP_LPD printing. For example, define DCPS\$_<print-queue-name>_PRODUCT_NAME as "HP LaserJet 8150 Series PS", if you want to use 8150 PS driver.

"9100" is the raw TCP printer port.

4. Specify "DATA=POSTSCRIPT" when PS drivers are used for printing.
5. Specify "DATA=PCL" when PCL drivers are used for printing.
6. The DCPS queues are not used when the printer supports only the PCL.

See the comments included in `DCPS$STARTUP.COM` for details. After editing `DCPS$STARTUP.COM`, execute the procedure to create the queue:

```
$ @SYS$STARTUP:DCPS$STARTUP
```

Add the above command to the site-specific system startup procedures to ensure the print queues are creating each time the system boots.

TCPIP\$TELNETSYM Print Queues

The HP CIFS Server software is bundled with a command procedure called `SAMBA$PRINT_QSETUP.COM` (in `SAMBA$ROOT:[BIN]`). Using this command procedure, you can set up the TCPIP\$TELNETSYM print queues, as shown in the following example:

```
$ @SAMBA$ROOT:[BIN] SAMBA$PRINT_QSETUP.COM
Enter unique number for print form: 3974
The print queue name entered here should match with printer name in SMB.CONF
Enter VMS print queue name: HPLASER
Enter Ip address of printer: 16.138.22.23
Enter printer port: 9100
Enter print form name: xyx
```

The following logical names may be helpful when using TCPIP\$TELNSYM print queues:

```
DEFINE/SYSTEM TCPIP$TELNETSYM_RAW_TCP 1
DEFINE/SYSTEM TCPIP$TELNETSYM_SUPPRESS_FORMFEEDS 35
```

Add the above definitions to the site-specific system startup procedures to ensure they are defined each time the system boots. For more information about TCPIP\$TELNETSYM print queues, see *HP TCP/IP Services for OpenVMS Management Guide*.

LPD Print Queues

Prerequisites

The following are prerequisites for LPD print queues:

- Ensure that HP TCP/IP Services for OpenVMS is running. For more information, see *HP TCP/IP Services for OpenVMS Installation and Configuration Manual*.
- Ensure that LPD services are enabled. For more information, see the documentation for the TCP/IP product installed on the server.
 - If you are running HP TCP/IP Services for OpenVMS Version 4.0 or earlier, enter the following command:

```
$ RUN SYS$SYSTEM:UCX$CONFIG.COM
```
 - If you are running HP TCP/IP Services for OpenVMS Version 5.0 or later, enter the following command:

```
$ RUN SYS$SYSTEM:TCPIP$CONFIG.COM
```
- Add an entry for the remote print server in the TCP/IP local host table (and use that name in the 'rm' parameter of the LPD queue setup). For example,

```
$ TCPIP SET HOST LPDSRV1/ADDRESS=10.0.0.1/ALIAS="ldpsrv1"
```

LPD Print Queue Setup

To setup the OpenVMS LPD print queue, run the TCPIP Printcap database utility program to add a remote printer.

```
$ RUN SYS$SYSTEM:TCPIP$LPRSETUP
TCPIP Printer Setup Program
Command < add delete view help exit >: add
Adding printer entry, type '?' for help.
Enter printer name to add : LPDPRINTER
Enter the FULL name of one of the following printer types:
remote local : remote
Enter printer synonym: LPDPRINTER
Enter printer synonym:
Enter full file specification for spool directory
SPOOLER DIRECTORY 'sd' : [TCPIP$LPD_ROOT:[LPDPRINTER]] ?
Set LPD PrintServer extensions flag 'ps' [] ?
Set remote system name 'rm' [] ? TEST123
Set remote system printer name 'rp' [] ? Text
Set printer error log file 'lf' [/TCPIP$LPD_ROOT/000000/LPDPRINTER.LOG] ?
Enter the name of the printcap symbol you wish to modify. Other
valid entry is :
'q' to quit (no more changes)
The names of the printcap symbols are:
sd for the printer spool directory
lf for the printer error log file
lp for the name of the local printer
ps for the LPD PrintServer extensions flag
rm for the name of the remote host
rp for the name of the remote printer
fm for the printer form field
pa for the /PASSALL flag
```

```

nd for the /NODELETE flag
cr for the cr flag
sn for the setup NoLF flag
p1-p8 for the /PARAMETER=(p1,...,p8) field
Enter symbol name: q
Symbol type value
-----
Error log file : lf STR /TCPIP$LPD_ROOT/000000/LPDPRINTER.LOG
Printer Queue : lp STR LPDPRINTER
PS extensions flag: ps STR
Remote Host : rm STR TEST123
Remote Printer : rp STR Text
Spool Directory : sd STR /TCPIP$LPD_ROOT/LPDPRINTER
Are these the final values for printer LPDPRINTER ? [y] y
Adding comments to printcap file for new printer, type '?' for help.
Do you want to add comments to the printcap file [n] ? : n
Do you want the queue to default to print flag pages [y] : n
Do you want this procedure to start the queue [y] : y
Creating execution queue: LPDPRINTER
Updating TCPIP$LPD_SYSTARTUP.COM
Updating TCPIP$LPD_SYSHUTDOWN.COM
*****
* TCPIP$LPD_SYSTARTUP.COM, the printcap file *
* and TCPIP$LPD_SYSHUTDOWN.COM *
* have been updated for this printer *
* *
* Set up activity is complete for this printer *
*****

```

Installing Printer Drivers

This section describes two methods for installing client printer drivers.

- Manual Driver Installation
- Automatic Driver Installation

Manual Driver Installation

Using this method, the user or administrator adds the driver on the client. To do so, follow these steps:

1. Browse to the server (that is, **Start --> Run --> \\servername**) to view a list of shares, including printer shares represented by a printer icon.
2. Right-click on the **printer-share** name you want to use, and then select the **Connect** option.
3. Select the **printer and driver** from the Print Driver Selection dialog box.
4. Click **OK**.
5. New printers appear in the Windows client local printer folder. Use any application to print on this printer.



NOTE: The print share-name, printer name, and Queue name must be same.

Automatic Driver Installation

This functionality requires a special share named PRINT\$ in which Windows client printer drivers are stored so that they can be downloaded automatically when adding a printer to your local workstation. Once the share is created, the Administrator uploads the necessary client printer drivers to the share from a Windows client. To add new drivers to the share, you must be an administrator or be granted the SePrintOperatorPrivilege user right. You must also have Write access to the PRINT\$ share directory tree.

Creating the PRINT\$ Share

To establish the PRINT\$ share, follow these steps:

1. Create a directory for the root of the share. For example,
`$ CREATE/DIRECTORY SAMBA$ROOT: [PRINT_DRIVERS]`
2. Create the subdirectory required for storage of Windows 2000 (and later) print drivers:
`$ CREATE/DIRECTORY SAMBA$ROOT: [PRINT_DRIVERS.W32X86]`
3. Set security to allow users Read access:
`$ SET SECURITY/PROT=W:R SAMBA$ROOT: [PRINT_DRIVERS] W32X86.DIR`
4. Add the PRINT\$ share stanza to SMB.CONF. For example,

```
[PRINT$]
path = /samba$root/print_drivers
browseable = no
read only = no
```
5. If necessary, start the HP CIFS Server:
`$ @SYS$STARTUP:SAMBA$STARTUP`

To upload the Windows printer drives to the PRINT\$ share, follow these steps:

1. From a Windows client, browse the HP CIFS Server (that is, Start --> Run --> \\servername) as an administrator or user with appropriate privileges.
2. Navigate to the **Printers and Faxes** folder.
3. Launch the **Add Printer** wizard.
4. Select **Local printer attached to this computer** and then click **Next**.
5. Select **Use the following port** and then click **Next**.
6. Select the appropriate printer manufacturer and printer model or click **Have Disk** to specify the location of the drivers.
7. Click **Next** and follow the instructions of the wizard to complete the installation.

To download the printer drivers to a Windows client automatically, follow these steps:

1. Using Network Neighborhood or **Start --> Run --> \\servername**, browse to the server.
2. Right-click on the desired printer and select **Connect**.

If necessary, the printer driver is downloaded and installed on the Windows client.

8 Tool Reference

This chapter describes some of the management tools included with HP CIFS for OpenVMS, including many native Samba utilities, such as `pdbedit` and `smbclient`. Other tools, such as `SMBSHOW`, are unique to HP CIFS for OpenVMS. For more information on Samba utilities, see Samba website:

<http://samba.org>

HP CIFS Management Tools

Several HP CIFS Server tools are available for management of HP CIFS. This section documents the following HP CIFS management tools:

<code>smbpasswd</code>	Tool for management of the HP CIFS encrypted password database.
<code>pdbedit</code>	Tool for management of the SAM database (Database of CIFS Users).
<code>net</code>	Tool for administration of HP CIFS and remote HP CIFS Servers.
<code>wbinfo</code>	Tool for querying winbind information.
<code>smbclient</code>	FTP-like client to access SMB/CIFS resources on servers.
<code>smbstatus</code>	Tool provides access to information about the current connections to the HP CIFS Server.
<code>nmblookup</code>	Tool allows NetBIOS name queries to be made from a OpenVMS host.
<code>smbshow</code>	This tool is used to get the information about all the HP CIFS Server processes that are being executed.
<code>smbver</code>	This tool is used to get information about the various images being used as part of the HP CIFS Server.
<code>SAMBA\$DEFINE_COMMANDS.COM</code>	This command procedure defines symbols for all the HP CIFS utilities.
<code>SAMBA\$GATHER_INFO.COM</code>	This command procedure gathers information and data files.
<code>testparm</code>	<code>testparm</code> utility is important to validate the contents of the <code>SMB.CONF</code> file.
<code>tdbbackup</code>	Tool for backing up and for validating the integrity of <code>samba.tdb</code> files
<code>tdbdump</code>	Tool for printing the contents of a TDB file.
<code>smbcontrol</code>	To send messages to <code>smbd</code> , <code>nmbd</code> process.

These management tools are available in the `SAMBA$ROOT: [BIN]` directory and are defined by executing the following command.

```
$ @SAMBA$ROOT: [BIN] SAMBA$DEFINE_COMMANDS
```

smbpasswd

This tool is used to manage a users' SMB password that is stored in the HP CIFS encrypted password file, `smbpasswd` or `tdbsam`, or in the LDAP directory server. The Samba password database contains the user name, OpenVMS user ID, the SMB hashed passwords of the user, account flag information, and the time the password was last changed.

Use `smbpasswd` to perform the following operations:

- Add user or machine accounts
- Delete user or machine accounts
- Enable user or machine accounts
- Disable user or machine accounts
- Set user passwords to NULL
- Manage inter-domain trust accounts

For more information on the `smbpasswd` command, see the SWAT or *The Official Samba HOWTO and Reference Guide*.

The `smbpasswd` tool performs its operations on the data store specified by the `passdb backend` parameter in the `SMB.CONF` file. If an LDAP directory must be used, this parameter is set to `ldapsam:ldap://<LDAP server name>`. If a Samba password file, `smbpasswd`, is used, this parameter is set to `smbpasswd`. If an NT-type SAM database is used, this parameter is set to `tdbsam` (the default).

Syntax

smbpasswd [*options*] [*username*]

where **options** can be any of the following:

- | | |
|----------------------------------|---|
| -L | Runs in the local mode (must be first option). |
| -h | Prints a list of options that the HP CIFS Server supports. |
| -s | Uses stdin for password prompt. This option causes <code>smbpasswd</code> to read passwords from standard input. |
| -c <config file> | Specifies the path and file name of the <code>SMB.CONF</code> configuration file when you want to use a file other than the default file. |
| -D <debug level > | Specifies the debug level. The debug level is an integer from 0 to 10. If this parameter is not specified, the default value is zero. |
| -r <remote machine name> | Allows users to specify which machine they want to change their password on. Without this parameter, <code>smbpasswd</code> defaults to the local host. The remote machine name is the NetBIOS name of the SMB/CIFS server to contact to attempt the password change. |
| -U <username [%password]> | Specifies the remote user name. This option may only be used in conjunction with the <code>-r</code> option. When changing a password on a remote machine, it allows the user to specify the user name on that machine whose password will be changed. |

Additional Options

- | | |
|-----------|---|
| -a | This option adds the username specified to the <code>passdb backend</code> . It prompts for the password to assign and request verification (enter Return to set a blank password). |
| -d | This option specifies that the account of the specified username must be disabled in the configured <code>passdb backend</code> . |

-e	This option specifies that the account of the specified username must be enabled if the account was previously disabled. If the account was not disabled, this option has no effect.
-i	This option specifies that the account is an inter- domain trust account.
-n	This option specifies that the specified username must have its password set to null (that is, a blank password) in the configured passdb backend.
-m	This option specifies that the account is a machine account.
-w < password >	This option specifies the password to be used with the <code>ldap admin dn</code> . The password is stored in the <code>SAMBA\$ROOT:[PRIVATE]SECRETS.TDB</code> file. If the password of <code>ldap admin dn</code> ever changes, the password must also be manually updated. The password is entered in the command line.
-W	Changes the LDAP directory manager password. With the <code>-w</code> option, the user is prompted for the password. The password is entered using <code>stdin</code> and thus the clear text password never appears on the command line.
-x	This option specifies that the specified username must be deleted from the configured passdb backend.
username	Specifies the username of the account.

Examples

Run the following command to create a CIFS account for the user `cifsuser1`:

```
$ smbpasswd -a cifsuser1
```

Run the following command to delete a CIFS account for the user `cifsuser2`:

```
$ smbpasswd -x cifsuser2
```

Run the following command to change the LDAP directory manager password:

```
$ smbpasswd -"W" <password of the LDAP Directory Manager>
```

For example, the following command changes the credentials of the LDAP directory manager:

```
$ smbpasswd -"W" dmpasswd
```

or you can run the `smbpasswd -"W"` command to change the LDAP directory manager password as follows:

```
$ smbpasswd -"W"
```

With the `-W` option, the user is prompted for the password. The password is entered using `stdin`.

pdbedit

You can use the `pdbedit` tool to manage the CIFS user accounts stored in the SAM database (database of CIFS users). You must be logged in as the privileged user to run this tool.

The `pdbedit` tool can be used to perform the following operations:

- Add, remove or modify user accounts
- List user accounts
- Manage account policies
- Manage domain access policy settings

For more information on the `pdbedit` command, see the SWAT or *The Official Samba HOWTO and Reference Guide*.

The `pdbedit` tool performs its operations on the data store specified by the `passdb` backend parameter in the `SMB.CONF` file. If an LDAP directory must be used, the parameter is set to `ldapsam:ldap://<LDAP server name>`. If the CIFS user account database file, `smbpasswd`, is used, the parameter is set to `smbpasswd`.

Syntax

```
pdbedit [options]
```

where *options* can be any of the following:

-L, --list	Lists all the user accounts in the users database. This option displays a list of uid/user pairs information separated by the ":" character.
-v, --verbose	Enables the verbose listing format. It causes <code>pdbedit</code> to list the users in the database, display the account fields in a descriptive format.
-w, --smbpasswd-style	This option enables <code>pdbedit</code> to list the users in the database, display the account fields in the <code>smbpasswd</code> style file format.
-u, --user=username	Specifies the user name to be used for the operation requested (listing, adding, modifying, and removing). It is required for add, remove, and modify operations and is optional for list operations.
-N, --account-desc=ARG	Specifies the account description to be set.
-f, --fullname=ARG	Specifies the user's full name. This option can be used while adding or modifying a user account.
-h, --homedir=ARG	Sets the user's home directory. This option can be used when adding or modifying a user account.
-D, --drive=ARG	Specifies the windows driver letter to be used to map the home directory. This option can be used while adding or modifying a user account.
-S, --script=ARG	Sets the user's logon script path. This option can be used while adding or modifying a user account.
-p, --profile=ARG	Specifies the user's profile directory. This option can be used while adding or modifying a user account.
-I, --domain=ARG	Specifies the user's domain name.
-U <user SID/RID>	Specifies the user's SID (Security Identifier) or RID. This option can be used while adding or modifying a user account.
-G <group SID/RID>	Specifies the user's group SID (Security Identifier) or RID. This option can be used while adding or modifying a user account.
-a, --create	Adds a CIFS user account. This command needs a user name specified with the <code>-u</code> option. When adding a new user, <code>pdbedit</code> prompts for the password to be used.
-r, --modify	Modifies an existing CIFS user account. This command requires a user name specified with the <code>-u</code> option.
-m, --machine	Adds a new machine account. This option may only be used in conjunction with the <code>-a</code> option. It will cause <code>pdbedit</code> to add a machine trust account instead of a user account (The <code>-m -u <machine name></code> option provides the machine account name).
-x, --delete	Deletes a CIFS user account. This command needs a user name specified with the <code>-u</code> option.
-b, --backend=ARG	Use a different <code>passdb</code> backend as the default password backend.
-i, --import=ARG <in-backend>	Use a different <code>passdb</code> backend to retrieve user accounts other than the one specified in the <code>SMB.CONF passdb</code>

backend parameter. This option can be used to import user accounts from this passdb backend.

This option eases migration of user accounts from one passdb backend to another.

-e, --export=ARG
<out-backend>

Exports all currently available user accounts to the specified password database backend.

This option eases migration of user accounts from one passdb backend to another.

-g, --group

Uses this option with the **-i <in-passdb backend>** option to import groups from this passdb backend.

You can use the **-g -e <out-passdb backend>** options to exports all currently available groups to the specified password database backend.

Account Policy Setting Options

Use the following options to manage account policy settings:

-P, --account-policy=ARG

Displays an account policy. Valid policies are minimum password age, reset count minutes, disconnect time, user must logon to change password, password history, lockout duration, min password length, maximum password age, and bad lockout attempt.

-C, --value=ARG

Sets an account policy to a specified value. This option may only be used in conjunction with the **-P** option.

-c, --account-control=ARG

Specifies the user's account control property. This option can be used while adding or modifying a user account. Possible flags are listed below:

- N: No password required
- D: Account disabled
- H: Home directory required
- T: Temporary duplicate of other account
- U: Regular user account
- M: MNS logon user account
- W: Workstation Trust Account
- S: Server Trust Account
- L: Automatic Locking
- X: Password does not expire
- I: Domain Trust Account

-z,
--bad-password-count-reset

Resets the bad password count value.

-Z, --logon-hours-reset
<logon-hours-reset>

Resets the login hours.

--pwd-can-change-time =ARG

Sets the password-can-change-time policy value.

--pwd-must-change-time =ARG

Sets the password-must-change-time policy value (UNIX time in seconds since 1970 if time format not provided).

--time-format=STRING

The time format for time parameters.

--t, -password-from-stdin

Reads password from standard input. If redirecting input from a file, the Record format of the file must be Stream_LF.

Help Options

- ?, -help** Show this help message.
- usage** Displays brief usage message.

Common CIFS Options

The following is a list of common CIFS options:

- d, --debuglevel=DEBUGLEVEL** Specifies the debug level, which is an integer from 0 to 10. If this parameter is not specified, the default value is zero.
- l, --log-basename=LOGFILEBASE** Specifies base name for log files.
- s, --configfile=CONFIGFILE** Specifies the alternative CIFS configuration file.
- V, --version** Prints the program version number.

Examples

Run the following command to display a list of the `pdbedit` options:

```
$ pdbedit -?
```

Run the following command to create a CIFS account for the user `cifsuser1` with the home directory `/home/cifsuser1`. The `pdbedit` tool prompts for input of an initial user password.

```
$ pdbedit -a cifsuser1 -h /home/cifsuser1
```

Run the following command to delete a CIFS account for the user `cifsuser2`:

```
$ pdbedit -x cifsuser2
```

net

This tool is used for administration of CIFS and remote CIFS servers. The CIFS `net` utility is meant to work just like the `net` utility available for windows and DOS. The first argument of the `net` utility is used to specify the protocol to use when executing the `net` command. The argument can be ADS, RAP, or RPC. ADS is used for Windows Active Directory, RAP is used for old Windows clients (Win9x/NT3) and RPC can be used for DCE-RPC.

The `net` tool performs its operations on the LDAP directory if the `SMB.CONF passdb backend` parameter is set to `ldapsam:ldap://<LDAP server name>`.

There are many `net` commands. This section describes a portion of the available commands. This section only describes syntaxes for the `net rpc user` command that you can use to manage CIFS user account database. For a complete description of how to use the `net` commands and syntaxes, see the SWAT, `net help` text or *The Official Samba HOWTO and Reference Guide*.

Net Commands

The following is a partial description of the `net` commands.

For more information on a specified command and its syntax, use `net help <command option>`.

- | | |
|---------------------|---|
| net time | Displays or set time information. |
| net lookup | Lookups the IP address or host name for a specified host. |
| net user | Manages users. |
| net group | Manages groups. |
| net groupmap | Manages group mappings. |
| net idmap | Manages the idmap id mappings. |
| net join | Joins a CIFS server to a domain. |
| net cache | Operates on cache Trivial Database (tdb) file. |

net getlocalsid [domain]	Displays the domain SID for the specified domain. If the [domain] parameter is not specified, The SID of the domain the local CIFS server is in.
net setlocalsid	Sets the local domain SID.
net changesecretpw	This command allows the CIFS machine account password to be set from an external application to a machine account password that has already been stored in a Windows Active Directory. Do not use this command unless you know exactly what you are doing. The use of this command requires that the force flag (-f) is used also. There will be no command prompt. Whatever information is input into stdin is stored as the literal machine password. Do not use this without care and attention because it will overwrite a legitimate machine password without warning.
net status	Displays machine account status of the local server.
net usersidlist	Gets a list of all users with their Windows SIDs.
net rpc <command>	Runs RPC commands.
net rap <command>	Runs RAP (pre-RPC) commands.

Syntax for net lookup

This section only includes syntaxes for the net lookup command.

net lookup [<host>]	Lookup the IP address of the given host with the specified type.
HOSTNAME[#<type>]	
net lookup ldap [<domain>]	Give IP address of LDAP server of specified DOMAIN.
net lookup kdc [<realm>]	Give IP address of KDC for the specified REALM.
net lookup dc [<domain>]	Give IP's of Domain Controllers for specified DOMAIN.
net lookup master [<domain/wg>]	Give IP of master browser for specified DOMAIN or workgroup.
net lookup name [<name>]	Display the SID (and account type).
net lookup sid [<sid>]	Give SID's name and type.

Examples

Run the following command to get the IP addresses of domain controllers for a specified domain:

```
$ net lookup dc cifsdom
```

Run the following command to list the SID and account type of the group account named sydney:

```
$ net lookup name sydney
```

Syntax for net user

This section only includes syntaxes for the net user command.

Use the following command syntax to list user account information:

```
net [<method>]user [options] [targets]
```

Use the following command syntax to delete a specified CIFS user account:

```
net [<method>]user DELETE <name> [options] [targets]
```

Use the following command syntax to list the domain groups of the specified CIFS user:

```
net [<method>]user INFO <name> [options] [targets]
```

Use the following command syntax to add a CIFS user account:

```
net [<method>]user ADD <name> [options]
[-c container] [-F user flags] [targets]
```

Use the following command syntax to rename a CIFS user:

```
net [<method>]user RENAME [oldname] [newname] [targets]
```

Valid Methods

The valid **methods** can be any of the following:

ads Can be used for Windows Active Directory.

rpc Can be used for systems with DCE-RPC.

rap Can be used for older systems such as Windows 9x or NT3 clients.

Valid Targets

The valid **targets** can be any of the following. If this argument is not specified, the default is the local host.

-S or **--server=<server>** Specifies the target server name.

-I or **--ipaddress=<ipaddr>** Specifies the IP address of the target server.

-w or **--workgroup=<wg>** Specifies the target workgroup or domain.

Valid Options

The valid **options** can be any of the following:

-p or **--port=<port>** Specifies the port number on the target server to connect to.

-W or **--myworkgroup=<wg>** Specifies the client workgroup or domain.

-d or **--<debuglevel=<level>** Specifies the debug level, which is an integer from 0 to 10. If this parameter is not specified, the default value is zero.

-n or **--myname=<name>** Specifies the NetBIOS name. This option allows you to override the NetBIOS name that CIFS uses. The command line setting takes precedence over parameter settings in the `SMB.CONF` file.

-U or **--user=<name>** Specifies the user name.

-s or **--configfile=<path>** Specifies the alternative path name of the CIFS configuration file.

-l or **--long** Displays full information on each item when listing data.

-V or **--version** Prints CIFS version information.

-P or **--machine-pass** Authenticate as the machine account.

-C or **--comment=<comment>** Specifies the descriptive comments. This option is only valid for the ADD operation.

-c Specifies the LDAP container when adding a user to the LDAP directory server. The default value is `cn=Users`.

help Prints a summary of command line options and usage.

Examples

Run the following command to create a CIFS user account for the user `cifsuser1`:

```
$ net rpc user ADD cifsuser1 --user administrator
```

Run the following command to delete a CIFS account for the user `cifsuser2`:

```
$ net rpc user DELETE cifsuser2 --user administrator
```

Run the following command to list the domain groups for the user `cifsuser3`:

```
$ net rpc user INFO cifsuser3 --user administrator
```

wbinfo

Use the wbinfo tool to get winbind information.

Syntax

wbinfo [*option*]

where *option* can be any of the following:

-u, --domain-users	Lists all domain users.
-g, --domain-groups	Lists all domain groups.
-N, --WINS-by-name=NETBIOS-NAME	Converts NetBIOS name to IP address.
-I, --WINS-by-ip=IP	Converts IP address to NetBIOS name.
-n, --name-to-sid=NAME	Converts name to SID.
h, --domainname-to-hostname=NAME	Converts domain-name to host-name.
-s, --sid-to-name=SID	Converts sid to name.
-R, --lookup-rids=RIDs	Converts RIDs to names.
-U, --uid-to-sid=UID	Converts uid to sid.
-G, --gid-to-sid=GID	Converts gid to sid.
-S, --sid-to-uid=SID	Converts sid to uid.
-Y, --sid-to-gid=SID	Converts sid to gid.
--allocate-uid	Get a new UID out of idmap.
--allocate-gid	Get a new GID out of idmap.
-t, --check-secret	Check shared secret.
-m, --trusted-domains	List trusted domains.
--all-domains	List all domains (trusted and own domain).
--own-domain	List own domain.
--sequence	Show sequence numbers of all domains.
-D, --domain-info=STRING	Show most of the info we have about the domain.
-i, --user-info=USER	Get user info.
--group-info=GROUP	Get group info.
-r, --user-groups=USER	Get user groups.
--user-domgroups=SID	Get user domain groups.
--user-sids=SID	Get user group sids for user SID.
-a, --authenticate=user%password	Authenticate user.
--set-auth-user=user%password	Store user and password used by winbind (root only).
--getdcname=domainname	Get a DC name for a foreign domain.
--get-auth-user	Retrieve user and password used by winbind (root only).
-p, --ping	Ping winbindd to see if it is alive.
--domain=domain	Define to the domain to restrict operation.
--separator	Get the active winbind separator.

Help Options

-?, -help	Show this help message.
--usage	Displays brief usage message.

Common CIFS Options

-V, --version	Prints the program version number.
----------------------	------------------------------------

For more information on how to use this tool, see `/opt/samba/man/man1/wbinfo.1` file.

Examples

The following is an example of the output using the `wbinfo -u` command:

```
$ wbinfo -u
```

```
DOMAIN_DOM\johnb  
DOMAIN_DOM\user1  
DOMAIN_DOM\user2  
DOMAIN_DOM\user3  
DOMAIN_DOM\user4  
DOMAIN_DOM\Guest  
DOMAIN_DOM\user5  
DOMAIN_DOM\ntuser  
DOMAIN_DOM\root  
DOMAIN_DOM\pcuser  
DOMAIN_DOM\winusr  
DOMAIN_DOM\maryw
```

The following is an example of the output using the `wbinfo -g` command:

```
$ wbinfo -g
```

```
DOMAIN_DOM\Domain Admins  
DOMAIN_DOM\Domain Guests  
DOMAIN_DOM\Domain Users  
DOMAIN_DOM\Domain Computers  
DOMAIN_DOM\Domain Controllers  
DOMAIN_DOM\Schema Admins  
DOMAIN_DOM\Enterprise Admins  
DOMAIN_DOM\Cert Publishers  
DOMAIN_DOM\Account Operators  
DOMAIN_DOM\Print Operators  
DOMAIN_DOM\Group Policy Creator Owners
```

smbclient

`smbclient` is a client that can 'talk' to an SMB/CIFS server. It offers an interface similar to that of the `ftp` program. Operations include functions, such as setting files from the server to the local machine, putting files from the local machine to the server, retrieving directory information from the server, and so on.

Syntax

SAMBA\$SMBCLIENT.EXE service <options>

where *options* can be any of the following

-R,	Use these name resolution services only.
--name-resolve=NAME-RESOLVE-ORDER	
-M, --message=HOST	This option allows you to send messages, using the "WinPopup" protocol, to another computer.
-I, --ip-address=IP	IP address is the address of the server to connect to.
-E, --stderr	Write messages to stderr instead of stdout.
-L, --list=HOST	Get a list of shares available on a host.
-t, --terminal=CODE	Terminal I/O code {sjis euc jis7 jis8 junet hex}.
-m, --max-protocol=LEVEL	Set the max protocol level.
-T, --tar=<c x>IXFqgbNan	This option may be used to create tar compatible backups of all the files on an SMB/CIFS share.
-D, --directory=DIR	Change to initial directory before starting.
-c, --command=STRING	Execute semicolon separated commands.
-b, --send-buffer=BYTES	This option changes the transmit/send buffer size.
-p, --port=PORT	This number is the TCP port number that is used when making connections to the server.
-g, --grepable	Produce grepable output.

Help Options

-?, --help	Show this help message.
--usage	Display brief usage message.

Common CIFS Options

The following is a list of common CIFS options:

-d, --debuglevel=DEBUGLEVEL	Specifies the debug level, which is an integer from 0 to 10. If this parameter is not specified, the default value is zero.
-l,	
-log-basename=LOGFILEBASE	Specifies base name for log files. The extension ".programe" is appended (for example, <code>log.smbclient</code> , <code>log.smbd</code>).
-s, --configfile=CONFIGFILE	Specifies the alternative CIFS configuration file.
-V, --version	Prints the program version number.

Connection Options

-O,	
--socket-options=SOCKETOPTIONS	TCP socket options to set on the client socket.
-n,	
--netbiosname=NETBIOSNAME	Primary NetBIOS name.
-W, --workgroup=WORKGROUP	Set the workgroup name.
-i, --scope=SCOPE	This specifies a NetBIOS scope that nmblookup uses to communicate with when generating NetBIOS names.

Authentication Options

-U, --user=USERNAME	Set the network user name.
-N, --no-pass	Does not prompt for password.
-k, --kerberos	Try to authenticate with kerberos. Only useful in an Active Directory environment.
-A,	Get the credentials from a file.
--authentication-file=FILE	
-S,	Set the client signing state.
--signing=on off required	
-P, --machine-pass	Use stored machine account password.

Examples

```
$ smbclient --list mtabca --user mtabca\dynac
Password:
Anonymous login successful
Domain=[CIFSDOM] OS=[Unix] Server=[Samba 3.0.24]
Sharename      Type          Comment
-----
IPC$            IPC           IPC Service (CIFS for OpenVMS 3.0.24)
Anonymous login successful
Domain=[CIFSDOM] OS=[Unix] Server=[Samba 3.0.24]
Server          Comment
-----
CIFSCUSTER      CIFS for OpenVMS 3.0.24
HOMERJ          CIFS for OpenVMS 3.0.24
HOMERJ_ALIAS    CIFS for OpenVMS 3.0.24

Workgroup       Master
-----
CIFSDOM
```

smbstatus

smbstatus is a simple program that lists the current Samba connections.

Syntax

smbstatus *<options>*

Where *options* can be any of the following

-p, --processes	Print a list of processes.
-v, --verbose	Gives verbose output.
-L, --locks	Causes smbstatus to only list locks.
-S, --shares	Causes smbstatus to only list share connection.
-u, --user=STRING	Selects information relevant to user name only.
-b, --brief	Gives brief output.
-P, --profile	If Samba has been compiled with the profiling option, print only the contents of the profiling shared memory area.
-R, --profile-rates	
-B, --byterange	Causes smbstatus to include byte range locks.
-n, --numeric	Numeric UID/GID.

Help Options

-?, --help	Show this help message.
--usage	Display brief usage message.

Common CIFS Options

The following is a list of common CIFS options:

-d, --debuglevel=DEBUGLEVEL	Specifies the debug level, which is an integer from 0 to 10. If this parameter is not specified, the default value is zero.
-l, --log-basename=LOGFILEBASE	Specifies base name for log files. The extension ".progname" is appended (for example, log.smbclient, log.smbd).
-s, --configfile=CONFIGFILE	Specifies the alternative CIFS configuration file.
-V, --version	Prints the program version number.

Examples

Run the following command to list the current Samba connections:

```
$ smbstatus
Samba version 3.0.28a
PID          Username      Group         Machine
-----
00000430     TEST1        TELNETS      test01 (16.91.77.23)

Service      pid          machine      Connected at
-----
IPC$         00000430     test01      Thu Apr 24 17:13:01 2008
```

nmblookup

nmblookup is used to query NetBIOS names and map them to IP addresses in a network using NetBIOS over TCP/IP queries.

Syntax

nmblookup *<options>*

where *options* can be any of the following

-B,	Specify address to use for broadcasts.
--broadcast=BROADCAST-ADDRESS	
-f, --flags	List the NMB flags returned.
-U, --unicast=STRING	Specify address to use for unicast.
-M, --master-browser	Search for a master browser.
-R, --recursion	Set recursion desired in package.
-S, --status	Once the name query has returned an IP address then do a node status query as well.
-T, --translate	Translate IP addresses into names.
-r, --root-port	Use root port 137 (Windows 95 only replies).
-A, --lookup-by-ip	Interpret <name> as an IP Address and do a node status query on this address.
-, --help	Show this help message.
--usage	Display brief usage message.
-d, --debuglevel=DEBUGLEVEL	Set debug level
-s, --configfile=CONFIGFILE	Use alternate configuration file.
-l,	Base name for log files.
--log-basename=LOGFILEBASE	
-V, --version	Prints the program version number.
-O,	TCP socket options to set on the client socket.
--socket-options=SOCKETOPTIONS	
-n,	Primary netbios name.
--netbiosname=NETBIOSNAME	
-W, --workgroup=WORKGROUP	Set the workgroup name.
-i, --scope=SCOPE	This specifies a NetBIOS scope that nmblookup uses to communicate when generating NetBIOS names.

Help Options

-, --help	Show this help message.
--usage	Display brief usage message.

Common CIFS Options

The following is a list of common CIFS options:

-d, -debuglevel=DEBUGLEVEL	Specifies the debug level, which is an integer from 0 to 10. If this parameter is not specified, the default value is zero.
-l,	Specifies base name for log files. The extension ".programe" is appended (for example, log.smbclient, log.smbd).
-log-basename=LOGFILEBASE	
-s, -configfile=CONFIGFILE	Specifies the alternative CIFS configuration file.
-V, -version	Prints the program version number.

Connection Options

-O, --socket-options=SOCKETOPTIONS	TCP socket options to set on the client socket.
-n, --netbiosname=NETBIOSNAME	Primary NetBIOS name.
-W, --workgroup=WORKGROUP	Set the workgroup name.
-i, --scope=SCOPE	This specifies a NetBIOS scope that nmblookup uses to communicate when generating NetBIOS names.

Examples

Run the following command to send a NetBIOS Node Status query to the IP address specified. The result, if successful, a list of NetBIOS name is registered by that system.

```
$ nmblookup --lookup-by-ip 16.105.15.72 -d0
Looking up status of 16.105.15.72
SYDNEY <00> - B <ACTIVE>
SYDNEY <03> - B <ACTIVE>
SYDNEY <20> - B <ACTIVE>
CIFSDOM <1e> -<GROUP> B <ACTIVE>
CIFSDOM <00> -<GROUP> B <ACTIVE>
```

MAC Address = 00-00-00-00-00-00

Run the following command to resolve the name 'Sydney' to its IP address and, if successful, send a NetBIOS Node Status request to the IP address returned.

```
$ nmblookup --status sydney
querying sydney on 16.105.15.72
16.105.15.72 sydney<00>
Looking up status of 16.138.185.72
SYDNEY <00> - B <ACTIVE>
SYDNEY <03> - B <ACTIVE>
SYDNEY <20> - B <ACTIVE>
CIFSDOM <1e> -<GROUP> B <ACTIVE>
CIFSDOM <00> -<GROUP> B <ACTIVE>
```

MAC Address = 00-00-00-00-00-00

smbshow

This tool is used to display system information about all the HP CIFS Server processes. When you start HP CIFS Server, NMBD process is created. As each client establishes a session with the server, a new SMBD process is created.

Examples

Run the following command to get the information about all the processes when a client session is not open:

```
NELTON\SYSTEM>smbshow
20203D7E NMBD LEF 6 421150 0 00:00:23.51 714 916
```

Run the following command to get the information about all the processes when a client session is open:

```
NELTON\SYSTEM>smbshow
20203D7E NMBD LEF 5 421976 0 00:00:23.59 714 916
20203E61 SMBD445_BG19299 LEF 8 2151 0 00:00:00.56 1643 1788 N
```

Smbver

This tool is used to get the information about various images being used as part of the HP CIFS Server.

Example

```
NELTON\SYSTEM>smbver
```

Information on NELTON for OpenVMS images installed on this system:

Image Name	Image Version	Link date	Linker ID
SAMBA\$ADD_DSKSHARE	T1.1-EFT2	18-AUG-2008 15:47	I02-31
SAMBA\$ADD_PRNFORM	T1.1-EFT2	18-AUG-2008 15:47	I02-31
SAMBA\$ADD_PRNQUEUE	T1.1-EFT2	18-AUG-2008 15:47	I02-31
SAMBA\$ADD_PRNSHARE	T1.1-EFT2	18-AUG-2008 15:47	I02-31
SAMBA\$NET	T1.1-EFT2	18-AUG-2008 15:47	I02-31
SAMBA\$NMBD	T1.1-EFT2	18-AUG-2008 15:47	I02-31
SAMBA\$NMBLOOKUP	T1.1-EFT2	18-AUG-2008 15:47	I02-31
SAMBA\$NTLMAUTH	T1.1-EFT2	18-AUG-2008 15:47	I02-31

SAMBA\$DEFINE_COMMANDS.COM

This command procedure defines symbols for all the HP CIFS utilities. It also defines symbols, namely, `SMBSTART`, `SMBSTOP`, `SMBSHOW`, and `SMBVERSION`.

SAMBA\$GATHER_INFO.COM

This is the command procedure that gathers information and data files and creates a backup save set file for reporting problems. All the log files, configuration file, lmhosts file, user mapping file, tdb files for password and other mapping related tdb's can be fetched from the saveset for debugging purpose.

testparm

`testparm` is a program to test the contents of `SMB.CONF` file. Whenever you modify the `SMB.CONF` file you need to run the `testparm` utility. The `testparm` examines the `SMB.CONF` file for syntax errors and reports them, if they are found, along with a list of the services enabled on your system.



NOTE: Run the `testparm` utility whenever you modify the `SMB.CONF` file.

Syntax

```
testparm <options>
```

Where *options* can be any of the following

-s, --suppress-prompt	Without this option, <code>testparm</code> will prompt for a carriage return after printing the service names and before dumping the service definitions.
-v, --verbose	Gives verbose output.
-L, --server=STRING	Sets the value of the <code>%L</code> macro to servername.
-t, --encoding=STRING	Prints parameters with encoding.
--show-all-parameters	Shows the parameter, type, and possible values.
--parameter-name=STRING	Limit <code>testparm</code> to a named parameter.
--section-name=STRING	Limit <code>testparm</code> to a named section.

Help Options

-?, --help Show this help message.
--usage Display brief usage message.

Common CIFS Options

-V, --version Prints the program version number.

Example

```
NELTON\SYSTEM>testparm
Load smb config files from /SAMBA$ROOT/LIB/SMB.CONF
Processing section "[homes]"
Processing section "[streamlf]"
Processing section "[vfc]"
Processing section "[shared]"
creating default valid table
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions

[global]
    workgroup = CIFSDOM
    server string = Samba %v running on %h (OpenVMS)
    security = DOMAIN
    client schannel = Yes
    server schannel = Yes
    username map = samba$root:[lib]usermap.map
    log level = 10
    log file = /samba$root/var/log_%h.%m
    name resolve order = lmhosts wins bcst
    add user script = @samba$root:[bin]useradd %u
    wins server = 16.138.16.104
    idmap uid = 2000-20000
    idmap gid = 5000-15000
    admin users = system
    create mask = 0755
    vms path names = No

[homes]
    comment = Home Directories
    read only = No
    create mask = 0750
    browseable = No
```

tdbbackup

tdbbackup is a tool that may be used to backup HP CIFS .tdb files. This tool may also be used to verify the integrity of the .tdb files prior to HP CIFS startup or during normal operation. If it finds file damage and it finds a prior backup the backup file will be restored.

The tdbbackup utility can safely be run at any time. It was designed so that it can be used at any time to validate the integrity of tdb files, even during HP CIFS operation. Typical usage for the command will be:

```
tdbbackup [-s suffix] *.tdb
```

Before restarting HP CIFS Server the following command may be run to validate .tdb files:

```
tdbbackup -v [-s suffix] *.tdb
```

Syntax

tdbbackup <options>

Where **options** can be any of the following

- h** Get help information.
- s suffix** This option allows the administrator to specify a file back-up extension.
- v** The -v will check the database for damages (corrupt data) which if detected causes the backup to be restored.
- n** Set the new hash size for the backup.

Tdbdump

Tdbdump is a very simple utility that 'dumps' the contents of a TDB (Trivial DataBase) file to standard output in a human-readable format. This tool can be used when debugging problems with TDB files.

Syntax

tdbdump *<options>*

Where *options* can be any of the following

- h** Get help information.
- k keyname** Dumps the value of the keyname.

smbcontrol

smbcontrol sends messages to the NMBD or an SMBD process.

Syntax

smbcontrol [OPTION...] *<destination>* *<message-type>* *<parameters>*

Where *options* can be any of the following

- t, --timeout=TIMEOUT** Set timeout value in seconds.

Help Options

- , --help** Show this help message.
- usage** Display brief usage message.

Common CIFS Options

The following is a list of common CIFS options:

- d, --debuglevel=DEBUGLEVEL** Specifies the debug level, which is an integer from 0 to 10. If this parameter is not specified, the default value is zero.
- l, --log-basename=LOGFILEBASE** Specifies base name for log files. The extension ".prognam" will be appended (for example, log.smbclient, log.smbd, and so on).
- s, --configfile=CONFIGFILE** Specifies the alternative CIFS configuration file.
- V, --version** Prints the program version number.

<destination> is the Process ID (PID) of the target process.

Message Types

Available message types are:

- close-share** Order smbd to close the client connections to the named share. Note that this does not affect client connections to any other shares. This message-type takes an argument of the share name for which client connections will be closed, or the "*" character which will close all currently open shares. This may be useful if you made changes to the access controls on the share. This message can only be sent to smbd.

debug	Set debug level to the value specified by the parameter. This can be sent to any of the destinations.
force-election	This message causes the nmbd daemon to force a new browse master election.
ping	Send specified number of "ping" messages and wait for the same number of reply "pong" messages. This can be sent to any of the destinations.
profile	Change profile settings of a daemon, based on the parameter. The parameter can be "on" to turn on profile stats collection, "off" to turn off profile stats collection, "count" to enable only collection of count stats (time stats are disabled), and "flush" to zero the current profile stats.
debuglevel	Request debuglevel of a certain daemon and write it to stdout.
profilelevel	Request profilelevel of a certain daemon and write it to stdout.
printnotify	Order smbd to send a printer notify message to any Windows NT clients connected to a printer. This message-type takes the following arguments:
queuepause printername	Send a queue pause change notify message to the printer specified.
queueresume printername	Send a queue resume change notify message for the printer specified.
jobpause printername unixjobid	Send a job pause change notify message for the printer and unix jobid specified.
jobresume printername unixjobid	Send a job resume change notify message for the printer and unix jobid specified.
jobdelete printername unixjobid	Send a job delete change notify message or the printer and unix jobid specified.

Note that this message only sends notification that an event has occurred. It does not actually cause the event to happen. This message can only be sent to smbd.

samsync	Order smbd to synchronize sam database from PDC (being BDC). Can only be sent to smbd.
samrepl	Send sam replication message, with specified serial. Can only be sent to smbd. Should not be used manually.
dmalloc-mark	Set a mark for dmalloc. Can be sent to both smbd and nmbd. Only available if samba is built with dmalloc support.
dmalloc-log-changed	Dump the pointers that have changed since the mark set by dmalloc-mark. Can be sent to both smbd and nmbd. Only available if samba is built with dmalloc support.
shutdown	Shut down specified daemon. Can be sent to both smbd and nmbd.
pool-usage	Print a human-readable description of all talloc(pool) memory usage by the specified daemon/process. Available for both smbd and nmbd.
drvupgrade	Force clients of printers using specified driver to update their local version of the driver. Can only be sent to smbd.
reload-config	Force daemon to reload smb.conf configuration file.

Example

```
NELTON\SYSTEM>smbshow
20203D7E NMBD          LEF      5   448071   0 00:00:25.02      714    916
20203E61 SMBD445_BG19299 LEF      6     3031   0 00:00:00.65    1647   1792   N
```

```
NELTON\SYSTEM>smbcontrol 20203D7E ping -d0
```

PONG from pid 538983806

A Sample Installation and Removal Procedures

This appendix provides sample procedures for installing and removing HP CIFS Server software.

Sample Installation on OpenVMS Integrity server Systems

```
$ PRODUCT INSTALL SAMBA
```

The following product has been selected:

```
HP I64VMS SAMBA V1.1          Layered Product
```

Do you want to continue? [YES]

Configuration phase starting ...

You will be asked to choose options, if any, for each selected product and for any products that may be installed to satisfy software dependency requirements.

HP I64VMS SAMBA V1.1: HP CIFS for OpenVMS I64 V8.2-1,V8.3 and V8.3-1H1.

Do you want the defaults for all options? [YES] YES

Do you want to review the options? [NO] YES

HP I64VMS SAMBA V1.1: HP CIFS for OpenVMS I64 V8.2-1,V8.3 and V8.3-1H1.

Do you want to download the Source files? : NO

Are you satisfied with these options? [YES] NO

Do you want to change any options? [YES] YES

If you say YES, the BCK file of the source files will be copied to SAMBA\$ROOT:[SRC] location.

Do you want to download the Source files? [NO] YES

Do you want to review the options? [NO]

Execution phase starting ...

The following product will be installed to destination:

```
HP I64VMS SAMBA V1.1 DISK$I6483VMS:[VMS$COMMON.]
```

Portion done: 0%...20%...30%...60%...70%...90%

User Accounts and User Identification Codes (UICs)

The HP CIFS for OpenVMS installation creates four OpenVMS accounts: SAMBA\$SMBD, SAMBA\$NMBD, SAMBA\$GUEST and SAMBA\$TMPLT. The default UIC group number for all these new accounts depends on the following:

- o If you are installing the product for the first time, the default is the first unused UIC group number, starting with 360.
- o If any of these account already exists, then the default UIC group number will not be used to change the UIC of any existing accounts.

For more information about UIC group numbers, see the OpenVMS System Manager's Manual.

```
Enter UIC group number for default accounts
Group: [360]
Creating CIFS User Accounts ...

User Accounts Creation Completed Successssfully ....

The release notes for HP CIFS on OpenVMS,
CIFS_REL_NOTES.TXT is available at SYS$COMMON:[SYSHLP]

To Configure HP CIFS, execute "$ @SAMBA$ROOT:[BIN] SAMBA$CONFIG.COM"

...100%

The following product has been installed:
  HP I64VMS SAMBA V1.1 Layered Product
$
```


Sample Removal Procedure on OpenVMS Integrity server Systems

```
$ PRODUCT REMOVE SAMBA
```

The following product has been selected:

```
HP I64VMS SAMBA V1.1          Layered Product
```

Do you want to continue? [YES] YES

The following product will be removed from destination:

```
HP I64VMS SAMBA V1.1 DISK$I6483VMS:[VMS$COMMON.]
```

Portion done: 0%...10%...20%

```
[ SAMBA shutdown being executed ]
```

```
[ Disabling TCPIP services SMBD ... ]
```

```
[ Terminating client SMBD_* processes... ]
```

```
[ Finished terminating client SMBD_* processes ]
```

```
[ Trying to terminate server-level NMBD process... ]
```

```
[ Finished NMBD process termination ]
```

```
[ SAMBA shutdown complete ]
```

```
!!!! WARNING !!!!
```

This procedure will remove all Samba configuration files.

Do you want to save them instead? [Yes] : Yes

Specify the location where you want to copy configuration files

By Default they will be copied to [SAMBA\$ROOT:[BACKUP]]:

Configuration files are copied to "SAMBA\$ROOT:[BACKUP]" directory.

This procedure will also remove CIFS Release notes available at SYS\$HELP.

Do you want to save them instead? [Yes] : No

```
...30%...40%...50%...60%...70%...80%...90%...100%
```

The following product has been removed:

```
HP I64VMS SAMBA V1.1 Layered Product
```

```
$
```

Index

B

- Backend
 - ldap, 26
 - smbpasswd, 26
 - tdbsam, 26

C

- CIFS
 - protocol, 11
- CIFS configuration file, 24
 - file structure, 24
 - sample configuration file, 25
 - verify, 25
- Cluster environment
 - configuring SMB.CONF file,, 26
- Common Internet File System. See CIFS, 11
- configuration
 - directory, 55
 - subsequent clients, 57
- Configuring
 - cluster environment, 26
 - cluster with common HP CIFS disk, 23
 - international character set, 27
 - OpenVMS File format, 27
 - using SWAT, 23
- configuring printers
 - queue setup, 78
 - spool directory, 77

D

- directory, 55
 - configuration, 55
- Disk space requirements, 15
- documentation
 - HP CIFS Server, 12
- documentations
 - and directory structure , 13

G

- GNU Public License, 11

H

- HP CIFS
 - description, 11
 - introduction, 11
- HP CIFS Server
 - directory structure, 13
 - disk space requirements, 15
 - documentation, 12
 - requirements and limitations, 15
 - software requirements, 15

I

- Installing
 - CIFS Server software, 20

L

- LDAP
 - advantages, 53
 - cifs authentication, 54
 - configuring, 55
 - domain model , 54
 - installing, 55
 - overview, 53
 - workgroup model, 54

M

- management tools
 - net commands, 88
 - nmblookup, 96
 - pdbedit, 85
 - smbclient, 93
 - smbcontrol, 100
 - smbpasswd, 84, 98
 - smbstatus, 95
 - smbver, 97
 - tdbbackup, 99
 - tdbdump, 100
 - testparm, 98
 - wbinfo, 91
- Managing
 - file and directory ACLs, 74
 - file and directory protections, 72
 - groups in PDC or BDC, 70
 - HP CIFS security, 72
- managing
 - local groups in member server, 68
 - local users, 67

N

- NetBIOS, 33
- Network File System, 33

O

- Open Source Software, 11
- OpenVMS cluster considerations, 18
- OSS. See Open Source Software, 11

P

- port 445, 33
- Postinstallation tasks, 22
- Preinstallation tasks, 16
- print driver files, 81
- print drivers
 - automatic driver installation, 80
 - manual driver installation, 80
- print queues
 - DCPS, 78
 - LPD, 79
 - TCPIP\$TELNETSYM, 78

R

release notes, 16

S

samba domain model , 36

Samba server

- description, 12

- features, 12

Server Message Block, 11, 12

SMB. See Server Message Block, 12

Starting HP CIFS

- automatically, 28

- in an OpenVMS cluster, 28

- manually, 28

Stopping HP CIFS, 29

T

Troubleshooting

- installation and configuration issues, 29

- verifying the client connection, 31

U

uninstalling HP CIFS server software, 34

Upgrading HP CIFS Server, 20

username mapping, 71

W

Winbind

- disabling, 65

- features, 60

- overview, 59

- parameters, 65

Winbind automatic mapping

- group mapping, 64

- user authentication and host mapping, 63

Winbind functionality

- automatic mapping, 62

- nested group, 62

- trusts, 62

windows domain model, 43