HP OpenVMS CIFS Version 1.2 Administrator's Guide

Table of Contents

List of Figures

List of Tables

List of Examples

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	Kerberos Support describes Kerberos protocol and also provides an example on a typical Kerberos logon and share service exchange using Kerberos authentication.
Chapter 5	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 6	User and Group Mapping describes how to manage users and groups on the HP CIFS Server. This chapter also describes various methods used by the HP CIFS Server to map Windows or CIFS domain users and groups to OpenVMS users and resource identifiers.
Chapter 7	WINBIND Support describes how to set up and configure the HP CIFS Server with the `winbind` support.
Chapter 8	Managing users, groups, account policies and trusts describes how the utility SAMBA$MANAGE_CIFS.COM can be used for managing CIFS Server users, groups, account policies and trusts. It also describes the commands that must be executed for managing the users, groups, account policies and trusts.
Chapter 9	Managing Shares and Printers describes how to manage shares and printers using a CIFS server.
Chapter 10	File and Print Security describes how the HP CIFS Server maps Windows permissions to OpenVMS file security as well as how to manage access to resources.
Chapter 11	Tool Reference describes some of the management tools included with HP OpenVMS CIFS, including many native Samba utilities such as pdbedit and smbclient.

Chapter 12	Performance Considerations and Troubleshooting Techniques describes methods to improve the performance of HP CIFS server and also troubleshooting problems with performance.
Chapter 13	SMB.CONF parameters describes HP CIFS Server configuration parameters that can be modified, parameters that must not be modified, and those parameters that are not supported.
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: • 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: `Is this correct? (Y/N) [Y].`
[ ]	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.
italic type	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 results in personal injury or nonrecoverable system problems.
CAUTION	A caution calls attention to important information that if not understood or followed results 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

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

1.1 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 HP CIFS Server is based on the open source software Samba Version 3.0.28a. The HP CIFS Server provides file and print services to CIFS clients, including Windows 2000, 2003, 2008, XP, and Vista.

1.1.1 What is 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.

1.2 Open Source Software 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. 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.

1.2.1 Open Source software

Samba is now available to HP and other users under the terms of the GNU Public License (GPL). The current version of Samba is released under GPLV3 license.

For more information about the GNU Public License, see:

http://www.fsf.org

1.2.2 Samba server

1.2.2.1 Description

HP OpenVMS CIFS is based on the Open Source Samba software.

"*Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients. Samba is freely available, unlike other SMB/CIFS implementations, and allows for interoperability between Linux/Unix servers and Windows-based clients. Samba is software that can be run on a platform other than Microsoft Windows, for example, UNIX, Linux, IBM System 390, OpenVMS, and other operating systems. Samba uses the TCP/IP protocol that is installed on the host server. When correctly configured, it allows that host to interact with a Microsoft Windows client or server as if it is a Windows file and print server.*" —source: http://www.Samba.org

Samba is based on Microsoft's Common Internet File System (CIFS) protocol. The CIFS protocol mainly uses Server Message Block (SMB) commands to communicate with different systems over the network.

Samba is an Open Source product with a worldwide community of developers. It is at par with the new Windows Operating System releases and provides seamless integration with Windows systems. To provide OpenVMS customers with file and print services that keep pace with new Windows releases, Open Source Samba has been ported to HP OpenVMS. This is intended as a replacement for the existing file and printer services product, Advanced Server for OpenVMS. HP OpenVMS CIFS is supported on OpenVMS Version 8.2 and later on Alpha, and OpenVMS Version 8.2-1 and later on HP Integrity servers.

1.2.2.2 Features

The main features of HP OpenVMS CIFS are (Note that HP OpenVMS CIFS will be referred to as HP CIFS Server in the rest of the manual):

- "Domain support" (page 20)
- "Authentication" (page 21)
- "Cluster services" (page 21)
- "Browsing" (page 21)
- "File and print services" (page 21)
- "File and print security" (page 22)

The following sections describe the features in detail.

Domain support

The HP CIFS Server can function as a native Member Server in an Active Directory domain, using Kerberos and LDAP to authenticate and authorize users. The HP CIFS Server may alternately function as a down-level NT4-style Member server in any domain.

The HP CIFS Server can function as an NT4-style Primary Domain Controller (PDC), but such a domain may only contain Backup Domain Controllers (BDCs) that run the HP CIFS Server. Similarly, it can function as an NT4-style BDC, only if the PDC is also running the HP CIFS Server. However, unlike HP Advanced Server for OpenVMS and Windows domain controllers, automatic replication of the user accounts database is not possible between Samba domain controllers, including the HP CIFS Server. To accomplish the automatic replication of account databases, Samba domain controllers require the assistance of LDAP servers.

By configuring the HP CIFS PDC and BDCs to use the LDAP backend, the accounts database is replicated by synchronizing the LDAP servers. The HP CIFS Server 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). Even though a single LDAP server can be used for both the HP CIFS Server PDC and BDCs, HP recommends that separate LDAP servers be used for high availability and better performance.

Authentication

The HP CIFS Server supports a basic and less secure share level security in which the password is supplied when accessing each share, and a more secure user level security, where the username and password must be supplied to establish connection to the HP CIFS Server before accessing shares.

In a user level security, HP CIFS Server supports the following authentication mechanisms:

1. LM : used by old Windows systems. For example, Windows 95 and Windows 98 systems.
2. NTLM : used by Windows NT and later.
3. NTLMv2 : used by Windows NT and later.
4. Kerberos, used by native Active Directory domain members.

HP CIFS Server also provides:

1. NT LAN Manager Security Support Provider (NTLMSSP) support for securing NTLM and NTLMv2 authentication.
2. Session security by signing and sealing secure channel data between a domain member and a domain controller. It supports 64-bit or 128-bit encryption keys.
3. SMB signing or security signatures.

Cluster services

The HP CIFS Server can be installed either on a single node in an OpenVMS Cluster or on multiple nodes that share the same the HP CIFS Server installation directory.

As a single node, the HP CIFS Server can be installed and function as a distinct entity (for any HP CIFS Server role) on each cluster node separately. As a result, each node acts as if it is on a non-clustered OpenVMS system. In this case, each node, where the HP CIFS Server is installed must not share the same installation directory and must not allow access to the same directories or files through multiple cluster members simultaneously.

A common cluster configuration is also possible, where multiple cluster members share the same HP CIFS Server installation, configuration directory, and data files. In such an environment, the HP CIFS Server functions as though the cluster is a single domain entity.

Browsing

HP CIFS Server supports traditional Windows browser service functionality. Browser service functionality is responsible for the “Network neighborhood” view provided by Windows.

File and print services

HP CIFS Server enables OpenVMS file and printer resources to be shared with network clients. These clients can view the shared files and printers as being present on a local system. Due to this, users can seamlessly work with shared files and printers using the available interfaces on the client system.

HP CIFS Server supports files present on ODS-2 and ODS-5 volumes. It can provide files with different OpenVMS file formats and file organizations to Windows clients in a Stream format. As a result, files with different formats are made readable to Windows clients. HP CIFS Server creates files in several formats, including Stream, Stream_LF, Fixed, or Undefined. By default, the HP CIFS Server supports the ASCII character set. Additionally, it also supports the Extended ASCII character set (CP850/ISO-8859-1) for some European characters and the Japanese character set (VTF-7) for the Japanese characters.

Using HP CIFS Server printing services, you can share any printer for which an OpenVMS print queue exists (or to printers directly connected to the OpenVMS host). These print queues can be set up using DCPS, TELNETSYM, LAT, or LPD. HP CIFS Server supports NT-style printing functionalities such as:

- Printer driver files can be downloaded locally on Windows clients.
- Printer driver files can be uploaded onto the HP CIFS Server from the Windows clients.

File and print security

Security is an important factor for any file and print service. Unlike Advanced Server for OpenVMS, which provides NT ACL-based file and printer security along with OpenVMS-based security, HP CIFS Server provides file and printer security using only OpenVMS file security. HP CIFS Server maps Windows security applied on the files and directories to OpenVMS file security. File and printer security can be set for any user or group.

Security auditing is not provided by HP CIFS Server, but standard OpenVMS auditing can be used for this purpose.

1.2.2.3 HP CIFS Server components

The main components of HP CIFS Server that provide the above features are:

- "SMBD processes" (page 22)
- "NMBD processes" (page 22)
- "WINBIND" (page 22)

1.2.2.3.1 SMBD processes

Each client session creates a new SMBD process. The SMBD process provides domain support, cluster services, authentication, file and printer services, and HP CIFS Server file security mapping functionality.

1.2.2.3.2 NMBD processes

The NMBD process provides traditional Windows browser service functionality apart from handling NetBIOS name registration and resolution.

1.2.2.3.3 WINBIND

WINBIND is a feature that supports automatic mapping of Windows domain users and groups to OpenVMS UICs and resource identifiers, nested groups (a group within a group) and trust functionality.

On platforms such as Linux, Samba provides WINBIND functionality through a process named, WINBINDD. On OpenVMS, WINBIND functionality is integrated into each SMBD process.

1.3 HP CIFS Server documentation

To explore the full features and capabilities of the HP CIFS product, you can refer to 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 can 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 or Linux are applicable to HP OpenVMS CIFS. For OpenVMS-specific features, see the *HP OpenVMS CIFS Release Notes*.

1.4 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 other 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
SAMBA$ROOT:[000000]	This is the base directory for most of the HP CIFS Server.
SAMBA$ROOT:[SRC]	This directory contains the source code for the HP CIFS Server.
SAMBA$ROOT:[BIN]	This directory contains binaries for the HP CIFS Server, including daemons and utilities. It also contains command scripts that starts the HP CIFS Server at boot time and stops it at shutdown (if it is configured to do so).
SAMBA$ROOT:[DOC]	This directory contains documentation in various formats including PS (postscript).
SYS$COMMON:[SYSHLP]	This directory contains the release notes for the HP CIFS Server.
SAMBA$ROOT:[SWAT]	This directory contains html and image files for the Samba Web Administration Tool (SWAT).
SAMBA$ROOT:[VAR]	This directory contains the HP CIFS Server log files and other dynamic files that the HP CIFS Server uses, such as lock files.
SAMBA$ROOT:[LIB]SMB.CONF	This is the main configuration file for the HP CIFS Server, which is discussed in great detail elsewhere.
SAMBA$ROOT:[UTILS]	This directory contains OpenVMS savesets for the SWAT utility.
SAMBA$ROOT:[LICENSES]	This directory contains the GPLV3 license description file.

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:

2.1 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.

2.1.1 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]`.

2.1.2 Software requirements

The software requirements for the HP CIFS Server are:

- OpenVMS Alpha Version 8.2 or 8.3 or 8.4
- OpenVMS Integrity servers Version 8.2–1 or 8.3 or 8.3-1H1 or 8.4
- TCP/IP Services or MultiNet or TCPware — the transport software to support the network protocols used by other servers and network clients
- Kerberos Version 3.0 and later

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.
- HP OpenVMS CIFS Server does not support Kerberos authentication on OpenVMS Integrity servers Version 8.2–1. You need not install the Kerberos Version 3.0 kit on OpenVMS Integrity servers Version 8.2–1.

2.2 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`.

2.3 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 or 8.4
- OpenVMS Integrity servers operating system Version 8.2-1 or 8.3 or 8.3-1H1 or 8.4
- TCP/IP or MultiNet or TCPware transport for network communication
- Latest C RTL ECO kit must be installed.
- Kerberos Version 3.0 and later

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 Section 2.2 (page 26).

Step 6: Check disk space

To determine the number of disk blocks required for installation, see Section 2.1.1 (page 25). 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 :

```
$ 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 runs 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.

2.4 OpenVMS Cluster considerations

HP CIFS Server supports the following configurations in an OpenVMS cluster:

- Installing the HP CIFS Server on each node as a standalone entity.
- Installing the HP CIFS Server as a common CIFS cluster with multiple nodes in the cluster sharing the same `samba$root` directory and shares.
- Combining a standalone HP CIFS Server and an HP CIFS Cluster in the same OpenVMS Cluster.

  For example, in a cluster with three nodes, two nodes can be a part of the HP CIFS cluster sharing the same `samba$root` directory and shares, while the third node can run a standalone instance of the HP CIFS Server.

NOTE: No two instances of the HP CIFS Server can share the same directories and files in a cluster because it can lead to data corruption. The reason for this is that each instance of the HP CIFS Server cannot share the file locking details with another instance of the HP CIFS Server.

Installing HP CIFS Server as a standalone entity in a Cluster

Installing the HP CIFS Server as a standalone entity on any node in the cluster is useful under following circumstances:

- Simultaneous file access through multiple cluster nodes is not required and there is no requirement for load balancing and failover.
- A node running OpenVMS version 8.2 or 8.2-1 cannot share the same `samba$root` directory with another node. Due to this, the HP CIFS Server must be installed as a standalone entity on a cluster node running OpenVMS version 8.2 or 8.2-1.
- There is no common SYSUAF and/or RIGHTSLIST database.

Installing HP CIFS Server on multiple nodes in the cluster

To obtain the load balancing and cluster failover features, the HP CIFS Server can be run as a common entity on multiple nodes in the cluster. In this case, the nodes that participate as members in the CIFS cluster:

- Share the same`samba$root` directory
- Share the same directories and files
- Allow clients to access the CIFS cluster nodes as a single entity by connecting to the HP CIFS Server cluster-alias name instead of the individual node name.

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

1. All HP CIFS cluster nodes must share a common SAMBA$ROOT directory tree. By default, HP CIFS Server is installed on the SYS$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.

   To allow mixed architecture cluster nodes (Alpha and Integrityservers) to participate as CIFS cluster nodes by sharing the same samba$root directory, install the HP CIFS Server on each node separately by specifying the same destination path for /DESTINATION qualifier of $ PRODUCT INSTALL command.

   For example:

   Consider a cluster with two Integrity server nodes and one Alpha node. To allow all the three nodes to share the same samba$root directory, install the HP CIFS Server on one of the Integrity server nodes and on the Alpha node by specifying the same destination path for the /DESTINATION qualifier of the $ PRODUCT INSTALL command.

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:

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

4. A common SYSUAF and RIGHTSLIST database must be used by all the cluster nodes that share the same samba$root installation directory.
5. Select a common CIFS cluster-alias name.
6. Select a common name resolution method. For information on available name resolution methods in the HP CIFS Server, see Section 2.5 (page 29).

2.5 Name resolution methods

The HP CIFS Server supports the following name resolution methods that can be used by the clients for resolving the HP CIFS Server name while connecting:

- “DNS name resolution” (page 29)
- “WINS name resolution” (page 30)
- “LMHOSTS name resolution” (page 31)

If the HP CIFS Server is configured as a standalone entity and the clients are configured to use DNS or WINS name resolution and are able to resolve the HP CIFS Server name using the configured DNS or WINS Server, no other action is required on the client or server. But, additional steps must be executed for a CIFS cluster, where more than one node shares the same samba$root directory.

2.5.1 DNS name resolution

In a CIFS cluster with more than one node sharing the same samba$root directory, to allow clients to access the resources using a common CIFS alias name, additional steps must be executed.

As a first step, make up 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 is running CIFS for OpenVMS. Since this name is 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 NODEC
```

The DNS entries are as shown:

```
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 is 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*.

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

2.5.2 WINS name resolution

To allow clients to access the resources using a common name in a CIFS cluster with more than one node sharing the same `samba$root` directory, the HP CIFS Server must be able to register the common CIFS cluster-alias with the WINS Server. The registered CIFS Server cluster-alias must point to the IP address of each node in the cluster that share the same `samba$root` directory. To do this, execute the following steps:

1. Add the HP CIFS Server configuration parameter *wins server* to point to the WINS Server IP address in the global section of the `SMB.CONF` file:

   ```
   wins server = <WINS-server-ip-address>
   ```

NOTE: You can provide multiple WINS Server IP addresses by separating them by a comma.

2. Specify the IP addresses of each the nodes in cluster that share the same`samba$root` directory in the global section for the HP CIFS Server configuration parameter *cluster addresses* by separating them using a comma.

   For example, if two nodes, NODEA and NODEB in a cluster share the same `samba$root` directory, specify the `cluster addresses` as:

   ```
   cluster addresses = <IP-address-of-NODEA>,<IP-address-of-NODEB>
   ```

NOTE: If you are using the `SAMBA$CONFIG.COM` configuration utility to configure the HP CIFS Server, the *wins server* and the *cluster addresses* parameters can be configured through the **Generic Options** menu in the configuration utility.

2.5.3 LMHOSTS name resolution

In a network, where the clients cannot resolve the HP CIFS Server name either by using the DNS or the WINS name resolution, LMHOSTS file can be used. This method can be used for resolving a name to a single IP address.

For a standalone HP CIFS Server node, this method can be used for resolving the HP CIFS Server name to the IP address of a node running HP CIFS Server.

For a CIFS cluster, where multiple nodes share the same `samba$root` directory and use the common CIFS cluster-alias, the LMHOSTS file can configured to resolve the CIFS cluster-alias to the IP address of one of the nodes running the HP CIFS Server.

Unless the LMHOSTS file is updated to point to the IP address of alternative node, the client continues to refer to the existing IP address as pointed by the CIFS cluster-alias. As such, the LMHOSTS name resolution method cannot provide load balancing or failover for the CIFS cluster nodes.

To allow a client to connect to the HP CIFS Server name or alias name for file access using the LMHOSTS name resolution, add the following line in the LMHOSTS file on the client:

```
<IP-address-of-node-running-CIFS-Server> <CIFS-Server-Name-or-Alias>
#PRE
```

For example, to add an entry for the HP CIFS Server name, PIANO with IP address 10.20.30.40, use:

```
10.20.30.40 PIANO #PRE
```

After updating the LMHOSTS file on Windows systems, reload the name cache by executing the following command at the CMD prompt:

```
nbtstat -R
```

2.6 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 pre-installation tasks listed in Section 2.3 (page 26).

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=DISK$DATA1:[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 creates the `[.SAMBA]` directory, for example, `DISK$DATA1:[000000.SAMBA].`
- It is recommended to install the HP CIFS Server on a non-system disk. For more information on the installation procedure, see Section 12.1 (page 189).

The installation of HP CIFS Server creates five OpenVMS user accounts:`SAMBA$NMBD`, `SAMBA$SMBD`, `SAMBA$TMPLT`, `SAMBA$GUEST`, and `CIFSADMIN`. 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.

2.7 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 Section 2.3 (page 26) 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:).

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.

NOTE: When upgrading a product that is already installed, $ PRODUCT INSTALL command of the PCSI utility installs the product in the SYS$SYSDEVICE:[VMS$COMMON] directory by ignoring the destination path that was specified with the /DESTINATION qualifier during the earlier installation of the product. This problem has been corrected on Version 8.4.

If you are using OpenVMS versions other than version 8.4, do the following:

1. Use the /DESTINATION qualifier with the $ PRODUCT INSTALL command while upgrading the HP CIFS Server software and specify the same destination path that was specified during earlier installation of HP CIFS Server.
2. Check if the latest PCSI kit solves this problem. You can read the PCSI ECO kit release notes file to confirm. If the PCSI kit does not solve the problem, download a PCSI sharable image from the HP CIFS Server download page and install it. And then upgrade the HP CIFS Server. This will solve the problem and allows the PCSI utility to automatically detect the correct destination path.

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

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

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

   NOTE: If the HP CIFS Server is running on multiple cluster members that share the same SAMBA$ROOT: directory, shut down the 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**.

2.8 Moving the SAMBA$ROOT directory

During re-installation, the PCSI utility does not allow a product to be installed on a different destination path other than the path used in the earlier installation of the product.

To move the contents of SAMBA$ROOT from one disk to another disk, back up the contents of the SAMBA$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.

The SAMBA$DEFINE_ROOT.COM file must be copied from the installation node system disk to the SYS$COMMON:[SYS$STARTUP] location on other applicable system disk(s). To define the new SAMBA$ROOT, run the following command:

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

Note that the above procedure may not work correctly in the mixed architecture cluster environment, clusters with multiple systems 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.

2.9 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 is defined only on the NODE where HP CIFS Server is installed.

2. 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 ensures that all the HP CIFS commands are available after login.

In an OpenVMS cluster, the SAMBA$DEFINE_ROOT.COM, SAMBA$STARTUP.COM, and SAMBA$SHUTDOWN.COM files that are present in the SAMBA$ROOT:[CLUSTER] directory must be copied from the installation node to the SYS$COMMON:[SYS$STARTUP] location on other nodes in the cluster, in the following conditions:

- Multiple nodes in the cluster share the same installation directory as the node, where HP OpenVMS CIFS is installed.
- Nodes in the cluster that use the same SAMBA$ROOT installation directory use separate system disks. In this case, copy the SAMBA$DEFINE_ROOT.COM, SAMBA$STARTUP.COM, and SAMBA$SHUTDOWN.COM files to each node that uses a separate system disk.

2.10 Configuring the HP CIFS Server

After installing the HP OpenVMS CIFS software, it must be configured to suit the CIFS setup requirements applicable at your site. The basic configuration considerations include (but, not limited to):

- HP CIFS Server role
- HP CIFS Server domain
- HP CIFS Server `passdb backend` type
- Configuring HP CIFS Server in a cluster
- Setting up CIFS services in TCP/IP database
- Character-set requirements

HP CIFS Server can be configured either from an OpenVMS system using the Samba configuration utility or by using the Samba Web Administration Tool (SWAT) through a Web browser.

NOTE: To configure HP CIFS Server, HP recommends that you use either HP OpenVMS CIFS—supplied Samba configuration utility `SAMBA$CONFIG.COM` or SWAT. They must not be used in combination.

2.10.1 Configuring the HP CIFS Server using the Samba configuration utility

From HP OpenVMS CIFS version 1.2 onwards, HP CIFS Server can be configured using an automated Samba configuration utility, `SAMBA$CONFIG.COM`. This utility can be used to set up a basic HP CIFS Server configuration. It must not be used to set up shares and trusts.

2.10.1.1 Preconfiguration tasks

Before executing the Samba configuration utility, the following pre-configuration tasks must be completed:

- In an existing HP CIFS Server configuration, shut down the HP CIFS Server if it is running on the node, where the Samba configuration utility is being executed.
- In an OpenVMS cluster, identify the nodes in the cluster that are required to share the same `samba$root` installation directory as the node on which HP OpenVMS CIFS software is installed.

  For example, consider there are four nodes in a cluster called NODE A, NODE B, NODE C, and NODE D. If the HP OpenVMS CIFS software is installed on NODE A, then do the following:

  — Identify the nodes that are required to share the same `samba$root` installation directory as NODE A. If NODE B and NODE C should share the same `samba$root` installation directory as NODE A, then check if NODE B and NODE C use the common OpenVMS system disk as NODE A. If they do not use common OpenVMS system disk as NODE A, then copy the `SYS$STARTUP:SAMBA$DEFINE_ROOT.COM` file from NODE A, to the `SYS$STARTUP` directory on the nodes, NODE B and NODE C.

  — In an existing HP CIFS configuration, shut down the HP CIFS Server on the nodes, NODE A, NODE B, and NODE C.
- Log in to OpenVMS using a privileged user account. For example, you can log in using the user account “SYSTEM”.

2.10.1.2 Configuration tasks

To run the Samba configuration utility from a DCL prompt on an OpenVMS system, execute the following commands:

```
$ @SYS$STARTUP:SAMBA$DEFINE_ROOT.COM
$ @SAMBA$ROOT:[BIN]SAMBA$CONFIG.COM
```

After the SAMBA$CONFIG.COM utility is executed, it performs the following tasks:

- Displays the help text.
- Checks if the pre-configuration requirements are met.
- Checks if an HP CIFS Server configuration already exists. If the configuration exists, it performs the following tasks:
  - Deletes all the temporary TDB files.
  - Converts or migrates the existing persistent TDB files to HP OpenVMS CIFS Version 1.2 TDB file format.
  - Gathers information about the current HP CIFS Server configuration.
- Displays Main Menu

NOTE: As part of the configuration of the HP CIFS Server, the SAMBA$CONFIG.COM utility does the following:

- Adds HOMES, NETLOGON, PRINT$, and PROFILES shares.
- Creates built-in CIFS Server groups as appropriate to the HP CIFS Server role.

The following sections describe various configuration options available through the Samba configuration utility.

2.10.1.3 Configuration options available through "Main Menu"

The Main Menu in the Samba configuration utility displays the following configuration options:

```
        HP OpenVMS CIFS Main Configuration Options Menu

Configuration options:

        1  - Core environment
        2  - Generic options
        3  - System specific setup
        A  - Configure options 1 - 3
       [E] - Exit Menu

Enter configuration option:
```

The options are explained as follows:

- The option Core environment allows you to configure HP CIFS Server core configuration such as server role, server domain, cluster alias, and so on.
- The option Generic options allows you to configure OpenVMS file format support, character set, server comment, guest account, cluster addresses, and so on.
- The option System specific setup sets up CIFS services (SMBD and SWAT services) in the TCP/IP database, the File Server client capacity and interfaces used by the File Server process (SMBD processes).

When HP CIFS Server is being configured for the first time, choose the option "A". Option "A" allows you to set up CIFS Server configuration for options 1 to 3 in the Main Menu. After configuring the HP CIFS Server using option "A" once, in future, if you have to re-configure the HP CIFS Server, you can select any other option in the Main Menu.

In an OpenVMS cluster, if multiple nodes share the same samba$root directory, execute option "A" of the "Main Menu" on just one of the nodes. On other nodes that are part of the CIFS cluster, execute option "3".

For example, if NODE A, NODE B, and NODE C are part of the CIFS cluster by sharing the same samba$root directory, execute option "A" of "Main Menu" on NODE A. On NODE B and NODE C, use option "3" of "Main Menu".

2.10.1.4 Configuring HP CIFS Server “Core environment”

In the `Main Menu` of the Samba configuration utility, to set up HP CIFS Server core environment, you can select either option “1” or “A”. In either case, the Samba configuration utility displays the following menu for the "Core environment":

```
HP OpenVMS CIFS Core Configuration Menu

  The CIFS core configuration menu allows you to configure basic server
   configuration parameters and to set the role of the server.

        1. Enable WINBIND mapping: yes
           1A. UIC Group number range:
           1B. POSIX Group IDentifier range:
        2. Passdb backend: tdbsam
        3. Domain/Workgroup name: LANGROUP
        4. Server role: PRIMARY
        5. Server computer/netbios name: PIANO

Enter item number or press Enter to accept current values [Done]:
```

Additionally, in case of an existing HP CIFS Server configuration, the following warning message is displayed:

```
************************* W A R N I N G *************************
  Changing any of the options in this menu may cause the existing
  databases to be RE-INITIALIZED resulting in the loss of any data
  currently in these databases (for example, user accounts, group
  names, identifier mapping information etc).
 ****************************************************************
```

In an OpenVMS cluster, the following option is displayed to allow you to specify HP CIFS Server cluster alias:

```
6. OpenVMS CIFS cluster alias: PIANO-ALIAS
```

The sub-options in `Core environment` menu are explained as follows:

2.10.1.4.1 Enable WINBIND mapping

Using option `1 Enable WINBIND mapping`, the WINBIND automatic mapping can be either enabled or disabled by specifying a “YES” or “NO”.

The WINBIND feature of the HP CIFS Server provides automatic mapping, nested group support, and trust functionality. The “automatic mapping” (WINBIND mapping) feature of WINBIND allows the HP CIFS Server to automatically create and map an OpenVMS user or group (resource identifier) to a corresponding domain user or global group. The OpenVMS username or group (resource identifier) is created, only if there is no existing mapping. For more information about WINBIND and the automatic mapping feature provided by it, see “WINBIND support”. If you enable WINBIND mapping by specifying “YES” to this option, the `Core environment` display two sub-options:

```
1A. UIC Group number range:
1B. POSIX Group IDentifier range:
```

If WINBIND mapping is enabled, you must specify values for the two sub-options, "1A" and "1B".

2.10.1.4.1.1 UIC Group number range

The range of values specified for `UIC group number range:` are mapped to the Samba configuration file parameter *idmap uid*.

When the option `. 1A. UIC Group number range:` is selected, it displays the following:

```
  Whenever a domain user connects to CIFS Server, it needs a matching
  OpenVMS username. If no such match exists, winbind can automatically
```

```
  create a new OpenVMS username to map the domain user. To achieve this,
  CIFS Server requires that a range of OpenVMS UIC group numbers is
  specified for its exclusive use.

  For example, the range can be specified as 1000-2000

  At the following prompt, enter HELP to obtain more information.

Enter UIC Group number range in decimal: []
```

At the prompt, if you enter "HELP", more information about `UIC group number range` is displayed.

For information about `UIC group number range`, see "WINBIND support".

2.10.1.4.1.2 POSIX Group IDentifier range

The range of values specified for the `POSIX Group IDentifier range` are mapped to the Samba configuration file parameter *idmap gid*.

When option `1B. POSIX Group IDentifier range` is selected, it displays the following:

```
  Whenever a domain group is referenced by CIFS Server, it needs a matching
  OpenVMS group (resource identifier). If a match is not found, winbind can
  automatically create the corresponding OpenVMS resource identifier. To
  achieve this, CIFS Server requires that OpenVMS resource identifier value
  is provided in POSIX GID format for its exclusive use.

  For example, the range can be specified as 5000-10000

  At the following prompt, enter HELP to obtain more information.

Enter POSIX group identifier range: []
```

At the prompt, if you enter "HELP", more information about `POSIX group identifier range` is displayed.

For information about POSIX group identifier range, see Chapter 7 (page 95).

2.10.1.4.2 Passdb backend

This option is mapped to the Samba configuration file parameter *passdb backend*.

When you select option `2. Passdb backend`, the configuration utility displays the following:

```
  Passdb Backend option allows you to choose the backend that will be
  used for storing user and possibly group information. This allows you
  to swap between different storage mechanisms.

  Available backends include -
       tdbsam - The TDB based password storage backend.
       ldapsam - The LDAP based passdb backend.

Enter Passdb Backend to use [TDBSAM/LDAPSAM]: [tdbsam]
```

By default, the *passdb backend* is set to "TDBSAM". You can change the *passdb backend* to "LDAPSAM" by specifying "LDAPSAM" at the prompt `Enter Passdb Backend to use`. When the *passdb backend* is specified as "LDAPSAM", HP CIFS Server stores the user and group information on the LDAP server that you specify. For more information about LDAPSAM backend, see Chapter 5 (page 81).

Apart from the *passdb backend*, the LDAPSAM backend also controls the following Samba configuration file parameters:

- *ldap admin dn*
- *ldap passwd sync*
- *ldap suffix*

When *passdb backend* is specified as “LDAPSAM”, you have to provide details of the LDAP server that can be used by HP CIFS Server for storing HP CIFS Server user and group information. When the *passdb backend* type is "LDAPSAM", to allow you to specify LDAP Server details, `Core environment` menu in the Samba configuration utility displays the following three sub-options of *passdb backend*:

- `2A. LDAP Server nodename`
- `2B. LDAP Server port`
- `2C. LDAP Server Admin dn`

LDAP Server nodename

When “LDAPSAM” is selected as *passdb backend*, the HP CIFS Server configuration utility requires you to specify the name of the system where LDAP Server is hosted. The LDAP Server system name can be a Fully Qualified Domain Name (FQDN) or an IP address of the system. The FQDN of the system will be of the format, `nodename.myorg.dom`. The FQDN of the system name that hosts LDAP server must be specified at the following prompt:

```
Enter Fully Qualified Domain Name of LDAP Server system: []
```

If the LDAP Server system name cannot be resolved using FQDN, you will be prompted to specify the LDAP server system IP address.

LDAP Server port

By default, LDAP Server listens on the TCP port 389. If the LDAP Server on the host system is configured to use a different port, then you must specify the port number on which the LDAP Server listens. The port number can be specified at the following prompt:

```
Enter the TCP port used by LDAP Server: [389]
```

LDAP Server Admin dn

LDAP Server Admin Distinguished Name (DN) is used by HP CIFS Server when retrieving user information from LDAP Server. The DN should be a fully specified DN similar to the following example:

dc=my-domain,dc=com

The configuration utility displays the following prompt, where you can specify the LDAP Server Admin DN.

```
Enter LDAP Server Admin DN: [dc=my-domain,dc=com]
```

2.10.1.4.3 Domain/Workgroup name

This option maps to the *workgroup* parameter in the Samba configuration file.

A domain is a collection of computers that share a common account database and policy. Each domain has a unique name. A network can have many domains. HP CIFS Server domain is the domain in which your HP CIFS server is located.

The HP CIFS Server domain name can be up to 15 characters long. The domain name must be different from the computer name. The default domain name is LANGROUP. You can specify a name that reflects your company or group.

At the following prompt that will be displayed by the Samba configuration utility, you can specify the name of the HP CIFS Server domain:

```
Enter CIFS Server domain name for this system: [LANGROUP]
```

2.10.1.4.4 Server role

The server role option controls the Samba configuration file parameters, *domain master*, *domain logons*, *add user to group script*, and *delete user from group script*. Additionally, if the HP CIFS Server role is PDC or BDC, it affects the *security* parameter.

Depending on the domain type, the HP CIFS Server can participate in a domain as a PDC, a BDC, or a member server or it can be configured independently as a standalone server. A brief description of each of the roles is provided in the following sections. For more information about server role, see Chapter 3 (page 59)

Primary Domain Controller

The Primary Domain Controller (PDC) stores the domain's master copy of the security accounts database. When you install the HP CIFS Server to create a new Windows NT domain, the new server becomes the PDC by default. When you install server software and specify an existing domain name, the server can join the existing domain only as a BDC or member server.

Backup Domain Controller (BDC)

A domain does not have to have BDCs, but one or more are recommended. A BDC stores a copy of the domain's master security accounts database. PDCs and BDCs can validate logon requests in the domain.

NOTE: HP CIFS Server can act as an NT4-style PDC, but such a domain may only contain BDCs that run HP CIFS Server. Similarly, it can function as an NT4-style BDC, only if the PDC is also running HP CIFS Server. However, unlike HP Advanced Server for OpenVMS and Windows domain controllers, automatic replication of the user accounts database is not possible between an HP CIFS Server PDC and BDCs. To accomplish the same goal, HP CIFS Server requires the assistance of LDAP servers.

By configuring the HP CIFS Server PDC and BDCs to use the LDAP backend, replication of the accounts database is achieved by the synchronization between LDAP servers. HP CIFS Server 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 Server PDC and BDCs, it is highly recommended that separate LDAP servers be used by the HP OpenVMS CIFS PDC and BDCs for high availability and better performance.

Member Server

A member server does not store a copy of the domain's security accounts database and does not validate logon requests. Member servers rely on domain controllers to validate credentials of users requesting access to member server shares.

From HP CIFS Server version 1.2 onwards, it can participate as a member in native mode Active Directory Windows domain that uses Kerberos authentication. It can also participate as an NT4–style member server in any domain.

Standalone server

Standalone servers are independent of domain controllers on the network. They are not domain members and function similar to workgroup servers. In many cases, a standalone server is configured with a minimum of security control so that all data served is readily accessible to all users.

Changing CIFS server role

When you configure the HP CIFS Server for the first time, you select the role your server will perform in the domain. There may be scenarios when you need to change the role of your server. The method you use to change the server depends on the current role of the server and the role

you want to change it to. Samba configuration utility allows you to change the server role with the following limitations:

- The Samba configuration utility allows you to change the role of the server from a BDC to a PDC, or vice versa. After changing the role, you must manually shut down the existing PDC in the domain or promote another BDC as PDC in the domain, depending upon whether the HP CIFS Server has been changed to a PDC or a BDC.
- If you re-configure a BDC as a member server, the Samba configuration utility automatically removes the domain controller's domain user and group account database.
- If you re-configure a member server to a BDC, the Samba configuration utility automatically removes the member server's local user and group account database.

NOTE: In case of role change from BDC to member server or vice versa, because of loss of local group information, access to some resources might be affected. If resource permissions have been set using local groups, those permissions will have to be reset. If resource permissions have been set using global groups or global user accounts, these permissions will remain in effect even after the role change.

- If the server role is changed from PDC to standalone server, this results in loss of any workstation accounts and the domain no longer functions as a domain. Instead, the domain starts functioning as a workgroup.
- If the server role is changed from standalone server to PDC, the workgroup starts functioning as domain and you can add workstation accounts and domain global groups.
- Other type of role changes are not supported.

2.10.1.4.5 Server computer/NetBIOS name

On a standalone OpenVMS system, this options maps to *netbios name* parameter in the Samba configuration file. On an OpenVMS cluster, this option maps to *netbios aliases* for that node.

This unique name identifies your server in the domain. You can define this name or accept the default value when you run the configuration procedure. The Samba configuration utility does not prevent you from specifying the same named PDC, if another node or cluster has previously been defined and is running in that role. However, this leads to name resolution conflicts. The PDC must be unique in the domain.

The default computer name is the same as the server's SCSNODE name.

2.10.1.4.6 OpenVMS CIFS cluster alias

In an OpenVMS cluster, this option maps to *netbios name* parameter in the Samba configuration file.

If your server is a member of an OpenVMS Cluster, *netbios name* (CIFS cluster alias) is the name that all servers in the cluster that use the same `SAMBA$ROOT` installation directory share. The alias lets remote nodes (including clients) treat all server members in the cluster as a single server. For example, a client user can specify the HP CIFS Server cluster alias to connect to any server in the cluster; the user need not know the specific node in the cluster to which it is connected.

The default HP CIFS Server cluster alias is nodename-ALIAS, where `nodename` is the SCSNODE name of the cluster member from which you initially run the Samba configuration utility.

2.10.1.4.7 Member Server specific configuration menu

When the HP CIFS Server role is selected as a member server, the Samba configuration utility displays the following menu:

```
Member Server Optional Parameters Configuration Menu

  The Member Server optional parameters configuration menu allows to
```

```
modify Member Server specific parameters which are required for
successful working of CIFS Server as member in a specified domain.


      1. Enable netlogon secure channel: auto
      2. Require strong session key: no
      3. Member of OpenVMS ASV Domain: no
      4. Password Server: *
      5. Security mode: DOMAIN

Enter item number or press Enter to accept current values [Done]:
```

If the `Security mode` is ADS, it additionally displays the following:

```
4. Kerberos realm:
```

2.10.1.4.7.1 Enable netlogon secure channel

This option maps to *client channel* parameter in the Samba configuration file.

The NETLOGON Secure Channel enables you to negotiate the level of security to be used for the communication of user authentication requests and the domain controllers. The highest security is provided by enabling signing and sealing. The three options available are:

- `auto`— offers signing and sealing but does not enforce it (default)
- `yes` — denies access if the server does not offer signing and sealing
- `no` — does not offer signing and sealing

NOTE: The Samba configuration utility prompts you for this option if the HP CIFS Server role is either BDC or Member Server. When prompted to select the netlogon secure channel, specify "NO", if you want to configure the HP CIFS Server as MEMBER or BACKUP to Advanced Server for OpenVMS domain. Otherwise, select the default option.

2.10.1.4.7.2 Require strong session key

This option maps *require strongkey* parameter in the Samba configuration file.

This is an HP OpenVMS CIFS specific option and it has no corresponding Open Source Samba equivalent parameter. The "Require strong session key" security setting determines whether 128-bit key strength is required for encrypting secure channel data.

- If set to yes, then the secure channel is not established unless 128-bit encryption can be performed.
- If set to no, then the key strength is negotiated with the domain controller.

NOTE: When Samba configuration prompts you for selecting `Require strong session key` option, specify "YES", if the HP CIFS Server acts as a member in Windows 2008 domain.

2.10.1.4.7.3 Member of OpenVMS ASV domain

This option maps to the HP CIFS Server-specific global section configuration parameter *vms asv domain*. In an Advanced Server for OpenVMS (ASV) domain, an OpenVMS system or a cluster of OpenVMS nodes that are running ASV will be acting as the PDC in the domain. To configure the HP CIFS Server as a MEMBER to such an ASV domain, specify "**YES**" at the prompt for "Member in OpenVMS ASV domain".

```
Member in OpenVMS ASV Domain [y/n]: [no]
```

While specifying a password server, you must:

- NOT specify the DC of another domain as Password Server.
- Specify the DC names as Fully Qualified Domain Names (FQDN) if you select security mode as ADS.
- Specify only the ASV PDC cluster alias as password server at the prompt when the HP CIFS Server is configured as Member Server in the Advanced Server for OpenVMS (ASV) domain where ASV PDC is running in an OpenVMS cluster.

```
Enter Password Servers (comma separated): [*]
```

2.10.1.4.7.4 Password server

This option maps to the global configuration parameter *password server*. When the HP CIFS Server is configured as a Member Server in a domain, it contacts one of the domain controllers in the domain to authenticate users belonging to the domain. By specifying a name of the domain controller in the domain as a Password Server, the HP CIFS Server can validate its username or password using the specific domain controller in the domain.

This option lets you set the name or IP address of the password server to use. If this option is set to the character "*", then CIFS Server will attempt to auto-locate the Primary or Backup Domain controllers to authenticate against by doing a query for the name DOMAINNAME<1C> and then contacting each server returned in the list of IP addresses from the name resolution source.

If the list of servers contains both names/IPs and the "*" character, the list is treated as a list of preferred domain controllers (DC), but an auto lookup of all remaining DC's will be added to the list as well. CIFS Server will not attempt to optimize this list by locating the closest DC.

2.10.1.4.7.5 Security mode

This option maps to the *security* Samba configuration file parameter. You can specify the security mode, when you configure HP CIFS Server role as member server or standalone server. When HP CIFS Server is configured as PDC or BDC, the security mode is set to “user”. Security mode affects how clients respond to HP CIFS Server.

As a member server, HP CIFS Server allows two security modes:

- DOMAIN: In this mode, the HP CIFS Server tries to validate the username or password by passing it to a domain controller in exactly the same way as a Windows NT Server.
- ADS: In this mode, the HP CIFS Server acts as a domain member in an ADS realm. To operate in this mode, the machine running the HP CIFS Server must have Kerberos installed. Select this mode if you want the clients to be authenticated using Kerberos.

On Standalone Servers, HP CIFS Server allows you to specify the security mode using which clients can decide whether (and how) to transfer user and password information to the server. The available security modes for Standalone Servers are:

- User, with user-level security: A client must first "log-on" with a valid username and password.
- Share: When clients connect to a share level security server, they need not log onto the server with a valid username and password before attempting to connect to a shared resource. Instead, the clients send authentication information (passwords) on a per-share basis, at the time they attempt to connect to that share.

2.10.1.4.7.6 Kerberos realm

This option maps to *realm* parameter in the Samba configuration file.

When HP CIFS Server is configured as member server with ADS security mode, the Samba configuration utility requires you to specify the Kerberos realm. The realm is used as the ADS equivalent of a Windows domain. It is usually set to the DNS name of the Kerberos server.

2.10.1.4.8 Domain controller optional parameters configuration menu

When the HP CIFS Server role is selected as PDC, the Samba configuration utility additionally displays the following menu as part of the core configuration:

```
Domain Controller Optional Parameters Configuration Menu

  The Domain Controller (DC) optional parameters configuration menu
  allows you to modify DC specific parameters which are required for
  successful working of CIFS Server as a DC in the specified domain.

        1. Logon Drive:
        2. Logon Path:
        3. Logon Script:

Enter item number or press Enter to accept current values [Done]:
```

When the HP CIFS Server role is selected as BDC, the Samba configuration utility additionally displays the following two options as part of “Domain Controller Optional Parameters Configuration Menu”:

```
        4. Enable netlogon secure channel: auto
        5. Backup in OpenVMS ASV Domain: no
```

2.10.1.4.8.1 Logon drive

This option maps to the *logon drive* parameter in the HP CIFS Server configuration file. The *logon drive* parameter specifies the drive letter Windows will assign your home directory. The drive letter can be from D to Z. This is an optional parameter.

2.10.1.4.8.2 logon path

This option maps to the parameter in the HP CIFS Server configuration file. The logon path directive is where you actually set up the roaming profiles. This directive must contain a Windows Network path to the location of the profile for each user. If the user's profile directory does not exist, a profile directory is created at that location (as long as the user has write access to that directory).

You can also take full advantage of the Samba's Variable Substitutions and separate user's profiles by architecture. You can use the following directive to separate the user's profiles relating to each version of Windows, such as WinXP, WinNT, and so on.

```
logon path = \\%L\profiles\%U\%a
```

This is useful if you have users who move from computer to computer that have different versions of Windows on them. In this case, the specified logon path is relative to the profiles share.

To disable roaming profiles, set the *logon path* parameter to empty string.

2.10.1.4.8.3 Logon script

This option maps to the *logon script* parameter in the HP CIFS Server configuration file. The logon script specifies a name for an optional logon script that runs each time the user logs on. A logon script can be a batch file (.BAT or .CMD file name extension) or an executable program (.EXE file name extension). A single logon script can be assigned to one or more user accounts. When a user logs on, the server authenticating the logon locates the logon script by following the server's logon script path that you specify.

The script must be a relative path to the `[netlogon]` share. If the `[netlogon]` share specifies a path of `SAMBA$ROOT:[NETLOGON]`, and `logon script = SCRIPTS\LOGON.BAT`, then the file that is downloaded is:

```
SAMBA$ROOT:[NETLOGON.SCRIPTS]LOGON.BAT
```

To disable the logon script from running when a user logs in, set the *logon script* parameter to empty string.

2.10.1.4.8.4 NETLOGON Secure Channel

This option maps to *client schannel* parameter in the HP CIFS Server configuration file. The NETLOGON Secure Channel provides a means to negotiate the level of security to be used for the communication of User Authentication requests and the domain controllers. The highest security is provided by enabling signing and sealing. The three options are:

1. auto — offers signing and sealing but does not enforce it (default).
2. yes — denies access if the server does not offer signing and sealing.
3. no — does not offer signing and sealing.

Specify `NO`, if you are configuring the HP CIFS Server as BACKUP to Advanced Server for OpenVMS domain, otherwise select the default option.

2.10.1.4.8.5 Backup in OpenVMS ASV domain

This option maps to the *vms asv domain* parameter in the HP CIFS Server configuration file. In an ASV domain, an OpenVMS system or a cluster of OpenVMS nodes that are running ASV act as a PDC in the domain. When configuring the HP CIFS Server as a BACKUP to such an ASV domain, specify "YES" at the prompt for "Backup in OpenVMS ASV domain":

```
Backup in OpenVMS ASV Domain [y/n]: [no]
```

2.10.1.4.9 Core environment setup

After you select the options from the `Core environment` menu, you can either terminate the configuration or proceed. After you select to configure HP CIFS Server, in case the HP CIFS Server role is BDC or Member Server, you are prompted to specify the FQDN (IP address if FQDN fails to resolve to IP) of the PDC for the domain. Additionally, you must also provide the credentials of a user belonging to the domain where HP CIFS Server is being added. The supplied domain user account must have the privilege to add machine account in the domain.

When an HP CIFS Server is configured for the first time, you can specify the domain user accounts to which you want to grant administrator privileges to manage HP CIFS Server.

After the necessary information is supplied, the Samba configuration utility sets up the HP CIFS Server core configuration environment. After successful configuration of the core environment, you can view the values for the corresponding parameters in the auto-generated core Samba configuration file `SAMBA$ROOT:[LIB]CORE_SMB.CONF` or using `TESTPARM` utility. You must not manually edit the `SAMBA$ROOT:[LIB]CORE_SMB.CONF` file to modify the parameters in it. Additionally, as part of “core environment” setup, the *log file*,*username map*,*printing* , and *load printers* parameters are also added to the core Samba configuration file.

NOTE: In an OpenVMS cluster, you are required to execute `core environment` menu only on a single node among the cluster nodes that share the same `SAMBA$ROOT` installation directory.

2.10.1.5 Setting up HP CIFS Server “Generic options”

After the HP CIFS Server core environment is set up, configure the HP Server for OpenVMS file format support, character set, homes (personal) share, and so on. Use the `Generic options` in the `Main Menu` of the Samba configuration utility by selecting option 2 or A. In the `Main Menu` , option `2`or `A` allows you to set up HP CIFS Server generic options. In either case, you can see the following `Generic options` menu displayed:

```
HP OpenVMS CIFS Generic Configuration Menu

This menu allows the administrator to specify character set, guest
```

```
account and other generic CIFS Server options.

        1. Character set: ASCII
        2. Guest account: SAMBA$GUEST
        3. Print command: /DELETE
        4. Server Comment String: Samba %v running on %h (OpenVMS)
        5. Enable WINS name resolution: no
        6. Name resolve order: lmhosts,host,wins,bcast

Enter item number or press Enter to accept current values [Done]:
```

2.10.1.5.1 Character set

This option maps to the Samba configuration file parameters *dos charset* and *unix charset*.

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. The user local code page (Windows codepage of the user) is set to CP850 to support European characters. To support Japanese and Chinese characters, the user local code page is set to CP932. The default user local code page is ASCII. The user local code page maps to *dos charset* parameter in the `SMB.CONF` file.

The Samba configuration utility displays the following options for the character set support:

```
The Samba configuration utility displays the following option to let you select the character set support of
your choice:

  By default, CIFS is configured to support the ASCII character set.
  For support of some European characters, select the Extended ASCII
  character set.  For support of Japanese characters, select the
  Unicode character set.

        1 - ASCII character support
        2 - Extended ASCII (CP850) character support
        3 - Japanese (CP932) character support

Enter option: [1]

Depending on your HP CIFS Server file name character support, choose the appropriate option.
```

2.10.1.5.2 Guest account

This option maps to the *guest account* parameter in the HP CIFS Server configuration file. Guest account is a username used for access to services, which are specified as guest access (guest ok) enabled. The privileges for this user are available to any client connecting to the guest service. The HP CIFS Server requires that the specified guest account must exist in the SYSUAF database. If the specified user is not present in the SYSUAF database, the utility can create the required guest account name in the SYSUAF database.

2.10.1.5.3 Print command

This option maps to the *print command* parameter in the HP CIFS Server configuration file. The print command accepts one or more of the following OpenVMS DCL PRINT command qualifiers:

- /BURST
- /DELETE
- /FEED
- /FLAG
- /FORM
- /HEADER
- /HOLD
- /OPERATOR
- /PAGES
- /PARAMETERS
- /PASSALL

- /PRIORITY
- /RESTART
- /RETAIN
- /SPACE

For information on any of these qualifiers, see the DCL help by executing "*$ HELP PRINT <qualifier>*"

While submitting a print job for the specified spool file to an OpenVMS system, the HP CIFS Server converts the specified print command qualifiers to the corresponding item codes of `SYS$SNDJBC` system service. The default *print command* value is "/DELETE".

2.10.1.5.4 Server Comment String

This options maps to the *server string* parameter in the Samba configuration file. The Server Comment String is the text that the HP CIFS Server displays when it announces its presence on the network and when you display a list of available servers. The default server announce string is ''Samba %v running on %h (OpenVMS)''. The "%v" is replaced with the Open Source Samba version and "%h" is replaced with the nodename.

2.10.1.5.5 Enable WINS name resolution

This option maps to the *wins server* parameter in the Samba configuration file. When HP CIFS Server initiates contact with other systems, such as Domain Controllers, HP CIFS Server must first resolve the NetBIOS name of the remote system to its IP address. HP CIFS Server can use several methods to resolve NetBIOS names to IP addresses, including WINS, an LMHOSTS file, broadcasts on its local subnet, or in some cases, DNS.

NOTE: DNS name resolution alone is often not sufficient, since certain NetBIOS names cannot be represented in a DNS name space.

By enabling the WINS name resolution, you can specify the WINS server IP address. HP CIFS Server uses this IP address to contact the WINS for name resolutions. You can specify more than one WINS server IP address after enabling `WINS name resolution`.

NOTE: In an OpenVMS cluster, if the *WINS name resolution* parameter is enabled, the following sub-options are displayed in the "Generic Options" menu to allow you to specify the WINS Server IP address and the cluster addresses:

```
5A. WINS Server IP address:
5B. Cluster addresses:
```

2.10.1.5.6 Cluster addresses

This option maps to the *cluster addresses* parameter in the HP CIFS Server configuration file. The Cluster addresses value must be entered if the *WINS name resolution* parameter is enabled.

In an OpenVMS cluster, if multiple nodes in a cluster share the same `samba$root` directory, the common CIFS cluster-alias name must be registered in the WINS Server. This common CIFS cluster-alias name must point to the IP addresses of all the nodes that share the same `samba$root` directory in that CIFS cluster. This ensures that clients can connect to any of the registered nodes using the CIFS cluster-alias name.

In a WINS Server, to successfully register the IP addresses of all the nodes in an OpenVMS cluster that share the same `samba$root` directory to a common CIFS cluster alias name, you must specify the IP addresses of all these nodes by separating them using a comma when the utility displays the following:

```
IP addresses of cluster nodes sharing same samba$root: []
```

2.10.1.5.7 Name resolution order

This option maps to the *name resolve order* parameter in the HP CIFS Server configuration file. The *Name resolution order* parameter is used by the programs in the Samba suite to determine what naming services to use and in what order to resolve host names to IP addresses. It controls the NETBios name resolution process. The option takes a comma separated string of name resolution options.

The options are: "lmhosts", "host", "wins" and "bcast".

When the WINS name resolution parameter is enabled, you might want to change the name resolution order such that the HP CIFS Server first uses the WINS option.

For example, you can specify the new name resolution order as:

```
wins,lmhosts,host,bcast
```

2.10.1.5.8 Generic options setup

After you specify the values for the options in the generic configuration menu, the Samba configuration utility creates a generic Samba configuration file, `SAMBA$ROOT:[LIB]GENERIC_SMB.CONF`. Apart from the parameters that are allowed to be modified through the generic configuration menu, the Samba configuration utility additionally adds the *vfs objects* parameter to support OpenVMS file formats. You must not manually modify any of the options in the `SAMBA$ROOT:[LIB]GENERIC_SMB.CONF` file.

NOTE: In an OpenVMS cluster, you are required to execute `Generic options` menu only on a single node among the cluster nodes that share the same `SAMBA$ROOT` installation directory.

2.10.1.6 HP CIFS Server system specific configuration

The third option in the `Main Menu` of Samba configuration utility is `System specific setup`. This option allows you to configure HP CIFS services such as SMBD and SWAT, file server client capacity, the network interfaces to use and open file caching. When option `3` or `A` is selected in the `Main Menu` of Samba configuration utility, the following menu for system-specific configuration is displayed:

```
HP OpenVMS CIFS System Specific Configuration Options Menu

In cluster, you can use this menu to setup node specific CIFS Server
configuration options.

        1. TCP Ports used by CIFS: [445,139]
        2. File Server client capacity: 50
        3. Enable SWAT service: yes
        4. Restrict Network interfaces: no

Enter item number or press Enter to accept current values [Done]:
```

2.10.1.6.1 TCP Ports used by CIFS

This option maps to the Samba configuration file parameter *smb ports*. This also controls the way the HP CIFS SMBD services are set up in the TCP/IP database. By default, the HP CIFS Server listens for incoming requests on both TCP port 139 (NetBIOS over TCP/IP) and TCP port 445 (SMB over TCP/IP). You can restrict the TCP port that can be used by HP CIFS Server to accept incoming requests. The port can be restricted to either 445 or 139.

2.10.1.6.2 File Server client capacity:

This options maps to *max smbd processes* in the Samba configuration file. On OpenVMS, the *max smbd processes* parameter cannot control the client limit. The client limit is controlled through the “Limit” qualifier while setting up SMBD services in TCP/IP database.

The client capacity determines the maximum number of clients which may access the HP CIFS Server concurrently. Samba configuration utility allows you to specify this client capacity. By default, the HP CIFS Server is set up to use TCP/IP ports 139 and 445. Unless the TCP/IP ports used by the HP CIFS Server are restricted, each port is set up to allow the specified number of client capacity. For example, if the specified client capacity is 100, HP CIFS Server specifies the limit on port 139 as 100 and that on port 445 as 100. Thus, by specifying 100 as the client capacity, HP CIFS Server is being set up for a maximum of 200 clients

2.10.1.6.3 Enable SWAT service

The Samba Web Administration Tool (SWAT) service allows a system administrator to view and modify the HP CIFS server configuration file (`SMB.CONF`) using a Web browser. For more information about SWAT, see Section 2.10.2 (page 51).

2.10.1.6.4 Restrict network interfaces

This options maps to *bind interfaces only* and *interfaces* parameters in the Samba configuration file. If the OpenVMS system is installed to use HP TCP/IP services, this option also affects the way the `/address` qualifier is used while setting up SMBD services in TCP/IP database. The SMBD services are registered with HP TCP/IP services using the command `$ TCPIP SET SERVICE`.

On a system with multiple network interfaces, Samba configuration utility allows you to specify the network interfaces that can by used by HP CIFS Server for accepting incoming requests. If you select to restrict network interfaces, you are prompted to specify the interface IP addresses. You can specify multiple interface IP addresses by separating them using a comma.

2.10.1.6.5 System specific configuration setup

Based on the options selected in the System specific configuration menu, the Samba configuration utility sets up the SMBD and SWAT services in TCP/IP database. Additionally, it creates a node specific configuration file `SAMBA$ROOT:[LIB]<SCSNODE>_SPECIFIC_SMB.CONF` with the parameters applicable. Do not edit this file manually to change any of the parameter values in it.

NOTE: In an OpenVMS cluster, after copying the `SAMBA$DEFINE_ROOT.COM` to all the nodes that are going to share the same `SAMBA$ROOT` installation directory as the node, where HP OpenVMS CIFS was installed, you must separately execute the Samba configuration utility on each node. When this utility is executed, options `1`, `2` and `3` in the `Main Menu` of the Samba configuration utility are required to be executed only on a single node among the nodes that share the same `SAMBA$ROOT` installation directory. Option `3` allows you to set up system specific configuration that must be run on all the nodes that share the same `SAMBA$ROOT` installation directory.

2.10.1.7 Limitations of the Samba configuration utility

The Samba configuration utility allows you to set up basic HP CIFS Server configuration. When the basic HP CIFS Server configuration is set up, you can start HP CIFS server and connect to it. Unless there are existing HP CIFS Server shares in the Samba configuration file, you must explicitly add shares in the Samba configuration file before you can access them. This utility does not provide an option to add shares. Among the many Samba configuration file parameters provided by the HP CIFS Server, only the basic parameters are set up though this utility. To add or modify rest of the parameters, you must manually edit the Samba configuration file, `SMB.CONF`.

NOTE:

- To configure shares in the HP CIFS Server, see Chapter 9 (page 133).
- The samba configuration utility must not be used if you have explicitly used the *lock dir* and *private dir* parameters in the existing HP CIFS Server configuration file.

2.10.2 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 :

```
$ 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

2.10.3 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` 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

2.10.3.1 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.

2.10.3.2 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.

If the *path* parameter is not specified in the `[homes]` section of the `smb.conf` file, then the HP CIFS Server uses the login device and directory specified in the user's `SYSUAF` account.

`[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

2.10.3.2.1 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 are available or operate as expected.

2.10.3.2.1.1 Sample Configuration File (SMB.CONF)

```
[global]
server string = Samba %v running on %h (OpenVMS)
security = user
passdb 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 = /samba$root/spool/
printable = yes
min print space = 2000
[test1]
browsable = yes
writeable = yes
path = /DKA0/users/test1/
```

2.11 Starting and stopping the HP CIFS Server

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

2.11.1 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
[ Creating NMBD Process... ]
%RUN-S-PROC_ID, identification of created process is 0004EA65

[ Enabling SMBD services... ]

[ Successfully enabled TCPIP SMBD services. ]
```

2.11.2 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
```

2.11.3 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 2-1 SYSMAN Utility

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

2.11.4 Stopping HP CIFS Server

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

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

2.12 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 1.2 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 1.2 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 Section 2.10.2 (page 51).

- Logs
  - NMBD log files are generated after startup. The `SAMBA$NMBD_<node-name>.log` files are stored in `SAMBA$ROOT:[VAR]`.
  - SMBD log files are generated for each client that utilizes the HP CIFS Server. By default, these log files are stored in `SAMBA$ROOT:[VAR]` as specified by the `SMB.CONF` parameter “log files”.
- When you run the executable in the `"-i"` interactive mode, all the debug messages are displayed on the screen and you can also know where exactly the SMBD process is hanging or aborting.
- `SAMBA$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.

2.12.1 Verifying the client connection

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

1. Start the NMBD process :

   ```
   $ @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>`

2.13 Additional HP CIFS Server configuration considerations

2.13.1 Special concerns when using HP CIFS Server on a Network File System

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, they cannot synchronize access to a specific resource.

2.13.2 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 that features of HP CIFS Server that depend on NetBIOS do not work. For example, the `"virtual server"` technique depending on an `"include = SAMBA$ROOT:[LIB]SMB.CONF.%L"` which ends up referring to another `SMB.CONF.<netbios name>` does 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.

2.13.3 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.

2.14 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 :

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

3. Enter the following command:

   ```
   $ PRODUCT REMOVE SAMBA
   ```

The removal command procedure performs the following operation:

- Prompts if you want to save the configuration files. These include the HP CIFS database files, a few utilities, 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 de-assigned.
  - Entering YES results in saving the specified files to the directory `SYS$COMMON:[SAMBA$SAFETY]`.
  - 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.

This chapter addresses the following topics:

3.1 Domain roles

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

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.2 Windows domain model

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

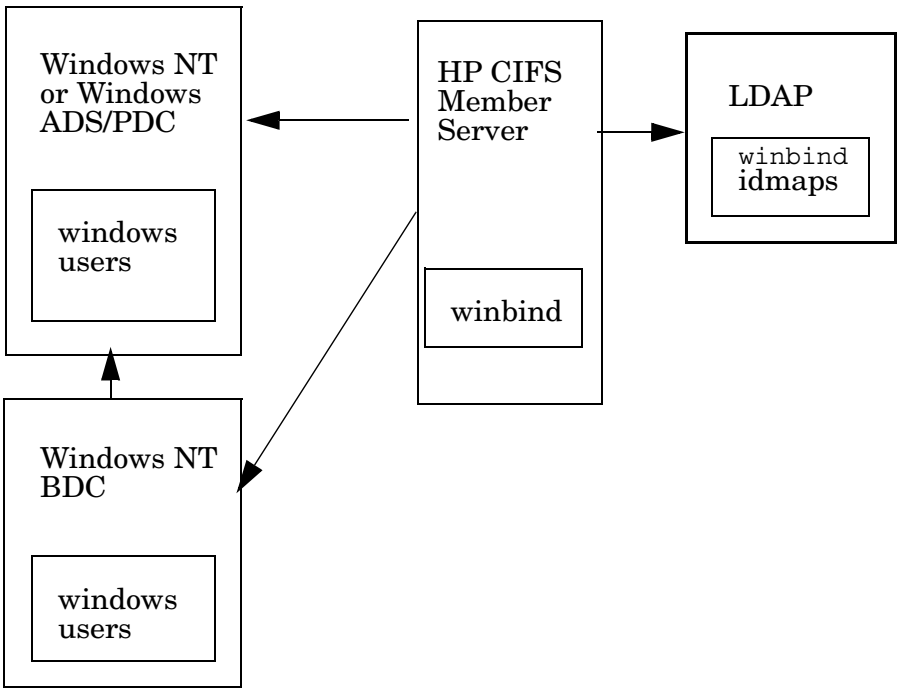
- Deploy Windows NT4, Advanced Server for OpenVMS, or Windows 200x servers (with NetBIOS enabled).
- Support for any number of HP CIFS member servers that provide file and print services.
- Access to an LDAP Enterprise Directory Server as the backend storage for larger deployments to maintain `winbind` 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 3-1 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.

3.2.1 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 7 (page 95). When you deploy multiple HP CIFS Servers, you can use the LDAP directory to maintain unique

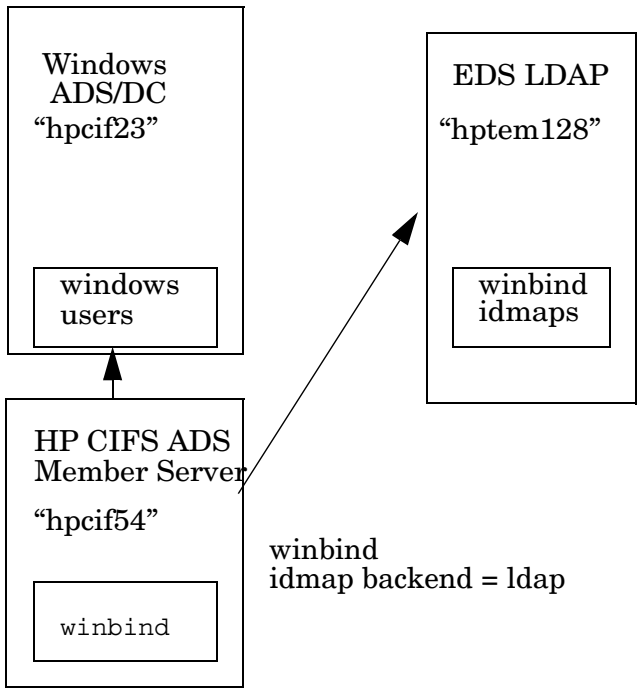
ID maps across multiple systems. Otherwise, user mapping is not consistent from system to system. To centralize management of ID maps in an LDAP directory, set the `idmap backend` parameter to `ldap:ldap://<ldap server name>` in the `SMB.CONF` file .

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

3.2.2 Example of 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 3-2 An example of the ADS Domain Model



3.2.3 Configuring HP CIFS Server as a native ADS Member Server

To configure the HP CIFS Server as an ADS member server, the following prerequisites must be met:

- Fully qualified Domain Name (FQDN) of the PDC of Windows domain, where HP CIFS Server participates as a Member Server must successfully resolve to IP using DNS Server.
- To avoid a Kerberos clock skew error, the time difference between PDC of the Windows Domain and the HP CIFS Server should be less than 5 minutes.

To add the HP CIFS Server as an ADS member server:

1. Set the following parameters in the SMB.CONF Samba configuration file :

```
[global]
workgroup = <NetBIOS domainname>
security = domain
domain logons = no
domain master = no
netbios name = <NETBIOSNAME or CIFS cluster-alias name
```

To successfully configure HP CIFS Server as a native ADS Member Server in the domain, you might need to set the following parameters. For a description about these parameters, see Section 2.10 (page 36):

```
security = ADS
realm = <ADS Realm>
password server = <Upper-cased FQDN of the
Domain Controller of a Windows Domain>
client schannel = <yes/no/auto>
require strongkey = <yes/no>
```

Additionally, in the same [global] section, add the following parameters, if required.

To specify generic Samba configuration parameters, add:

```
server string = Samba %v running on %h (OpenVMS)
username map = /samba$root/lib/username.map
log file = /samba$root/var/%h_%m.log
```

To use LDAP as a passdb backend for storing user and group account information, add the following parameters:

```
passdb backend = ldapsam:ldap://<name or IP address of the node where
LDAP server is running>
ldap admin dn = <LDAP Admin DN>
ldap passwd sync = yes
ldap suffix = <LDAP Admin DN>
```

NOTE: LDAP must be correctly set up before using it as passdb backend. For information about configuring HP CIFS Server to use LDAP as backend, see "LDAP integration support" (page 81).

To configure HP CIFS Server as a WINS client to allow HP CIFS Server to resolve NetBIOS names using a WINS Server, add the following parameters:

```
wins server = <WINS server IP address>
name resolve order = wins, lmhosts, bcast, hosts
```

To enable CIFS to create OpenVMS accounts and resource identifiers for domain user and group accounts, which have no explicit mapping, include the following parameters:

```
idmap uid = <UID range>
idmap gid = <GID range>
```

For information about *idmap uid* and *idmap gid* ranges, see (page 95).

To set up the "homes" share that allows users access to their OpenVMS login directory, add:

```
[homes]
 comment = User's home share
 browseable = no
 read only = no
```

2. Run the `testparm` utility and verify that the server is configured as the Member Server.

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

3. Join HP CIFS Server as an ADS Member Server :

   ```
   $ net ads join --user=<username in DOMAIN>
   Password:
   ```

4. Verify the join :

   ```
   $ net ads testjoin
   ```

5. Start the HP CIFS Server :

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

3.3 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 3-3 Standalone HP CIFS Server as a PDC

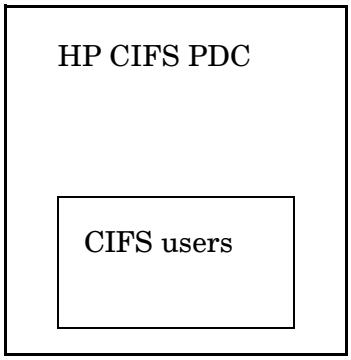


Figure 3-2 shows a standalone HP CIFS Server as a PDC using the Enterprise Directory Server (EDS) as an LDAP backend:

Figure 3-4 Standalone HP CIFS Server as a PDC with EDS backend

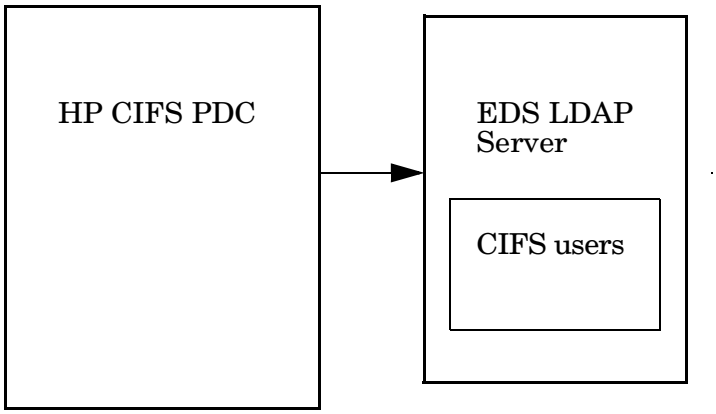
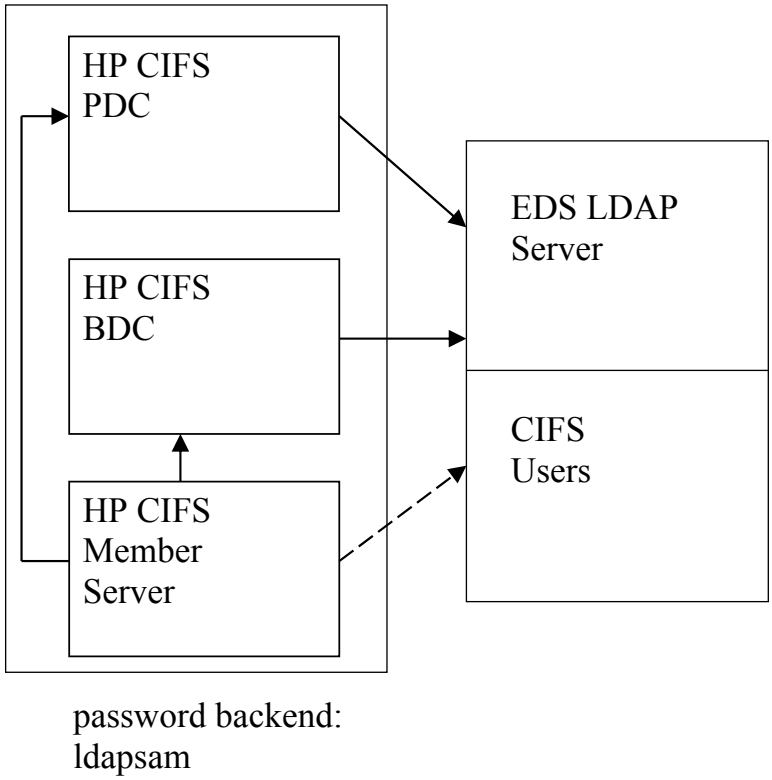


Figure 3-3 shows multiple HP CIFS Servers using Enterprise Directory Server as an LDAP backend:

Figure 3-5 Multiple HP CIFS Servers with EDS backend



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.

3.3.1 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 5 (page 81) .

WINS name resolution

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.

3.3.1.1 HP CIFS Server Acting as a PDC

The 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.

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 queries for the <domain name>1B name when attempting to locate the PDC of the domain.

Single server installations may use `tdbsam` password backend, but large installations should use the LDAP backend to provide centralized management of CIFS users.

For information about configuring HP CIFS Server as PDC, see Section 3.3.2.1 (page 67).

3.3.1.1.1 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 is not interoperable 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.

3.3.1.2 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.

To configure HP CIFS Server as BDC, see Section 3.3.2.1 (page 67)

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.

3.3.1.2.1 Synchronizing account Database between BDC and 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 :

```
$ NET RPC VAMPIRE -S [NETBios name of PDC] -W [domainname] –U
administrator%password
```

3.3.1.3 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 Section 3.3.2.3 (page 73).

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.

3.3.1.4 HP CIFS Server acting as a Standalone Server

Standalone servers are independent of Domain Controllers on the network. By definition, this means that users and groups are 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.

3.3.2 Configuring HP CIFS Server manually

The HP CIFS Server can be configured for various roles described Section 3.1 (page 59) section using either an automated configuration utility or by manually editing the Samba configuration file. The Samba configuration utility `SAMBA$ROOT:[BIN]SAMBA$CONFIG.COM` can be used to configure the HP CIFS Server. For more information about configuring the HP CIFS Server using this utility, see Section 2.10 (page 36) .

The following sections describe the steps for configuring HP CIFS Server by manually editing the Samba configuration file `SAMBA$ROOT:[LIB]SMB.CONF`. It describes the Samba configuration parameters and values required to configure HP CIFS Server for various roles. The same parameters can be selected from the SWAT utility to configure HP CIFS Server for the role mentioned under that section.

NOTE: For a description about the parameters that are mentioned in the following sections, see Section 2.10 (page 36).

3.3.2.1 Configuring HP CIFS Server as PDC

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

1. Add the following parameters in the SMB.CONFfile (and replace values specified within angle brackets < > with appropriate details):

```
[global]
 workgroup = <NetBIOS domain or workgroup name>
security = user
 domain logons = yes
 domain master = yes
netbios name = <NetBIOS Computer or Cluster-alias name>
add user to group script = @samba$root:[bin]samba$addusertogroup %g %u
 delete user from group script = @samba$root:[bin]samba$deluserfromgroup %g %u
```

Additionally, in the same [global] section, add the following parameters, if required.

To specify the generic Samba configuration parameters, add:

```
server string = Samba %v running on %h (OpenVMS)
 username map = /samba$root/lib/username.map
 log file = /samba$root/var/%h_%m.log
```

To use LDAP as a passdb backend for storing user and group account information, add the following parameters:

```
passdb backend = ldapsam:ldap://<name or IP address of the node where
LDAP server is running>
ldap admin dn = <LDAP Admin DN>
ldap passwd sync = yes
 ldap suffix = <LDAP Admin DN>
```

NOTE: LDAP must be set up before using it as a passdb backend. For information about configuring HP CIFS Server to use LDAP as backend, see Chapter 5 (page 81).

To facilitate joining workstations to the domain, enable WINBIND mapping by adding the following parameters:

```
idmap uid = <UID range>
idmap gid = <GID range>
```

NOTE: For information about *idmap uid* and *idmap gid* parameters, see Chapter 7 (page 95).

To configure the HP CIFS Server as a WINS client to allow the HP CIFS Server to resolve NetBIOS names using WINS, add the following parameters:

```
wins server = <WINServer1 IP Address> <WINServer2 IP Address>
name resolve order = wins, lmhosts, bcast, hosts
```

To enable roaming profiles, add:

```
logon path = \\%L\profiles\%U
```

For more information about roaming profiles, see Section 3.3.2.1.2 (page 70). Additionally, you can add a [PROFILES] share to SMB.CONF as described in the **Roaming Profiles** section.

To specify a netlogon script that will be executed when a user logs into the domain, add:

```
logon script = <logon script path>
```

To set up the “netlogon” share that allows user logon scripts to be executed when the user logs into the domain, add:

```
[netlogon]
 comment = Netlogon share
 path = /samba$root/netlogon
 read only = yes
 browseable = no
 guest ok = yes
 vms path names = no
 write list = @administrators, cifsadmin
```

For more information about the netlogon share, see Section 3.3.2.1.3 (page 70).

To set up the “homes” share that allows users to access their OpenVMS login directory, add:

```
[homes]
 comment = User's personal share
 browseable = no
 read only = no
```

2. Run the `testparm` utility and verify that it indicates that the server is configured as the PDC.

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

3. Start the HP CIFS Server :

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

3.3.2.1.1 Joining a Windows Client to an HP CIFS Domain

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

1. Create an OpenVMS account for the Windows client. The account name must 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 the HP CIFS Server is configured as a PDC, the name of the workstations that are getting added to the HP CIFS Server PDC must not exceed 11 characters. This limitation is due to the OpenVMS user name length limited to 12 characters in the `SYSUAF` database.

2. Create an 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 is 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$
   ```

NOTE: Step 1and Step 2 can be skipped if a valid *idmap uid* and *idmap gid* range is specified in the `SMB.CONF` Samba configuration file.

3. After creating an account, you can add a Windows workstation to the domain. From the Windows client, follow these steps:
   a. Log on 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 displays 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.

3.3.2.1.2 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

3.3.2.1.2.1 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. For example:

   ```
   [global]
   #%L substitutes for this server's NetBIOS name, %U is the user name
   logon path = \\%L\profiles\%U
   ```

2. Create a `[profiles]` share for roaming profiles. Set `profile acls = yes` for the profile share used for the user profile files. Otherwise, it can cause loading problems for roaming profiles. Do not set `profile acls = yes` on normal shares as this results 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 mask = 04600
   directory mask = 04700
   writeable = yes
   browseable = no
   guest ok = no
   vms path names = no
   ```

NOTE: When the HP CIFS Server is configured using the `SAMBA$CONFIG.COM` utility, it adds the PROFILES share by default.

3.3.2.1.3 Configuring user logon scripts

The logon script configuration must meet the following requirements:

- User logon scripts should be stored in a file share called `[netlogon]` 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
```

NOTE: When the HP CIFS Server is configured using the `SAMBA$CONFIG.COM` utility, it adds the NETLOGON share by default.

3.3.2.2 Configuring HP CIFS Server as BDC

To configure HP CIFS Server as BDC, follow these steps:

1. Set the following parameters in the Samba configuration file `SMB.CONF`:

```
[global]
 workgroup = <NetBIOS domain name>
 security = user
 domain logons = yes
 domain master = no
 netbios name = <NetBIOS Computer or Cluster-alias name>
 add user to group script = @samba$root:[bin]samba$addusertogroup %g %u
 delete user from group script = @samba$root:[bin]samba$deluserfromgroup %g %u
```

Additionally, in the same [global] section, add the following parameters, if required.

To specify generic Samba configuration parameters, add:

```
server string = Samba %v running on %h (OpenVMS)
username map = /samba$root/lib/username.map
log file = /samba$root/var/%h_%m.log
```

To use LDAP as a passdb backend for storing user and group account information instead of the default SAM database backup (tdbsam), add the following parameters:

```
passdb backend = ldapsam:ldap://<name
or IP address of the node where LDAP server is running>
ldap admin dn = <LDAP Admin DN>
ldap passwd sync = yes
ldap suffix = <LDAP Admin DN>
```

NOTE: LDAP must be correctly set up before using it as `passdb backend`. For information about configuring HP CIFS Server to use LDAP as backend, see Chapter 5 (page 81).

To replicate accounts from the PDC, enable WINBIND mapping by adding the following parameters:

```
idmap uid = <UID range>
idmap gid = <GID range>
```

NOTE: For information about *idmap uid* and *idmap gid* parameters, see Chapter 7 (page 95).

To configure the HP CIFS Server as a WINS client (to allow the HP CIFS Server to resolve NetBIOS names using WINS), add the following parameters:

```
wins server = <WINS server IP address>
 name resolve order = wins, lmhosts, bcast, hosts
```

To specify a netlogon script that is executed when a user logs into the domain, add:

```
logon script = <logon script path>
```

To set up the “netlogon” share that allows user logon scripts to be executed when a user logs into the domain, add:

```
[netlogon]
 comment = Netlogon share
 path = /samba$root/netlogon
 read only = yes
 browseable = no
 guest ok = yes
 vms path names = no
```

For more information about the netlogon share, see Section 3.3.2.1.3 (page 70).

To set up the “homes” share that allows users to access their OpenVMS login directory, add:

```
[homes]
 comment = User’s share
 browseable = no
 read only = no
```

2. Run the `testparm` utility and verify it indicates that the server is configured as the BDC.

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

   $ testparm
   ```

3. If not configured as a WINS client and the domain PDC is on a different subnet than the HP CIFS Server BDC, the `SAMBA$ROOT:[LIB]LMHOSTS.` file on the BDC must include the three entries as shown.

   ```
   <PDC-IP-Address> <PDCname>
   <PDC-IP-Address> <Domainname>#1b
   <PDC-IP-Address> <Domainname>#1c
   ```

   Replace *<PDC-IP-Addess>* with the IP address of the domain PDC, replace *<PDCname>* with the computer name of the PDC, and replace *<Domainame>* with the name specified in the SMB.CONF *workgroup* parameter.

   For example, if the name of the HP CIFS Server PDC in the HP CIFS Domain “VMSCIFSDOM” is ROX3 and its IP address is 10.20.20.40, then the LMHOSTS. entries must appear as follows:

   ```
   10.20.20.40 VMSCIFSDOM#1b
   10.20.20.40 VMSCIFSDOM#1b
   10.20.20.40 ROX3
   ```

4. Join the domain by executing the NET RPC JOIN command and supplying the name of the PDC as well as administrator credentials. For example:

   ```
   $ net rpc join “-S” <PDCname> --user administrator

   Password:
   ```

5. Verify the join:

   ```
   $ net rpc testjoin
   ```

6. Start the HP CIFS Server:

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

7. After the HP CIFS Server BDC is configured and started, the Account Database between the BDC and the PDC and the BDC must be synchronized. To do the same, see Section 3.3.1.2.1 (page 66).

3.3.2.3 Configuring HP CIFS Server as a Member Server

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 is 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 OpenVMS CIFS— Add an OpenVMS account and a CIFS machine account as described in Section 3.3.2.1.1 (page 69)
- 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 option next to "Windows NT Workstation or Server and 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.

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.

3.3.2.3.1 Adding HP CIFS Server to a domain as an NT-Style (Downlevel) Member Server

To configure the HP CIFS Server as an NT-style (downlevel) Member server in the domain, follow these steps:

1. Set the following parameters in the Samba configuration file SMB.CONF:

```
[global]

workgroup = <NetBIOS domainname>
security = domain
domain logons = no
domain master = no
netbios name = <NETBIOSNAME or CIFS cluster-alias name
```

To successfully configure HP CIFS Server as an NT-style (downlevel) Member server in the domain, you might have to set the following parameters.

For a description about these parameters, see Section 2.10 (page 36).

```
password server = <password server name>
client schannel = <yes/no/auto>
require strongkey = <yes/no>
vms asv domain = <yes/no>
```

Additionally, in the same [global] section, add the following parameters, if required.

To specify generic Samba configuration parameters, add:

```
server string = Samba %v running on %h (OpenVMS)
username map = /samba$root/lib/username.map
log file = /samba$root/var/%h_%m.log
```

To use LDAP as a passdb backend for storing user and group account information, add the following parameters:

```
passdb backend = ldapsam:ldap://<name or IP address of the node where
LDAP server is running>
ldap admin dn = <LDAP Admin DN>
ldap passwd sync = yes
ldap suffix = <LDAP Admin DN>
```

NOTE: LDAP must be correctly set up before using it as passdb backend. For information about configuring HP CIFS Server to use LDAP as backend, see Chapter 5 (page 81).

To configure the HP CIFS Server as a WINS client to allow the HP CIFS Server to resolve NetBIOS names using a WINS Server, add the following parameters:

```
wins server = <WINS server IP address>
name resolve order = wins, lmhosts, bcast, hosts
```

To enable CIFS to create OpenVMS accounts and resource identifiers for domain user and group accounts, which have no explicit mapping, include the following parameters:

```
idmap uid = <UID range>
idmap gid = <GID range>
```

NOTE: For information about *idmap uid* and *idmap gid* ranges, see Chapter 7 (page 95).

To set up the `homes` share that allows users access to their OpenVMS login directory, add:

```
[homes]
 comment = User's home share
 browseable = no
 read only = no
```

2. Run the `testparm` utility and verify that the server is configured as the Member Server:

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

3. If not configured as a WINS client and the domain PDC is not on the same IP subnet as the HP CIFS Server, the following entries are required in the file `SAMBA$ROOT:[LIB]LMHOSTS.`:

```
<IP address of PDC> <DOMAINNAME>#1b
<IP address of PDC> <DOMAINNAME>#1c
<IP address of PDC> <PDC name>
```

   For example, if the name of PDC in the domain "ACCOUNTSDOM" is PIANO and its IP address is 10.20.30.40, then the LMHOSTS.; entries must be added as follows:

```
10.20.30.40 ACCOUNTSDOM#1b
10.20.30.40 ACCOUNTSDOM#1c
10.20.30.40 PIANO
```

4. Join the HP CIFS Server as an NT-style (downlevel) Member Server:

```
$ net rpc join "-S" <PDC name> --user=<Domain administrator account name>
Password:
```

5. Verify the join:

```
$ net rpc testjoin
```

NOTE: To configure the HP CIFS Server as a native Active Directory Member server, see Section 3.2.3 (page 61).

6. Start the HP CIFS Server :

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

NOTE:

1. Do not start the HP CIFS Server 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 to determine if the NetBIOS name resolution is effective. For more information, see Chapter 11 (page 165)
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` uses NetBIOS name resolution to resolve the name to its IP address.
4. The `$ NET RPC JOIN` command does not use 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.

3.3.2.4 Configuring HP CIFS Server as a Standalone Server

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

1. Set the following parameters in the Samba configuration file SMB.CONF:

```
  [global]
workgroup=<NetBIOS workgroup name>
security =user
domain logons = no
domain master = no
netbios name = <NetBIOS computer or cluster-alias name>
```

Additionally, in the same [global] section, add the following parameters if required.

To specify generic Samba configuration parameters, add:

```
server string = Samba %v running on %h (OpenVMS)
 username map = /samba$root/lib/username.map
 log file = /samba$root/var/%h_%m.log
```

To use LDAP as a passdb backend for storing user and group account information, add the following parameters:

```
passdb backend = ldapsam:ldap://<name or IP address of the node where
LDAP server is running>
 ldap admin dn = <LDAP Admin DN>
 ldap passwd sync = yes
 ldap suffix = <LDAP Admin DN>
```

NOTE: LDAP must be correctly set up before using it as passdb backend. For information about configuring HP CIFS Server to use LDAP as backend, see Chapter 5 (page 81)

To configure HP CIFS Server as a WINS client to allow HP CIFS Server to resolve NetBIOS names using a WINS Server, add the following parameters:

```
wins server = <WINS server IP address>
 name resolve order = wins, lmhosts, bcast, hosts
```

To set up the “homes” share that allows users to access their OpenVMS login directory, add:

```
[homes]
 comment = User’s home share
 browseable = no
 read only = no
```

2. Because WINBIND is not required on a Standalone HP CIFS Server, disable WINBIND by defining the following system logical:

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

NOTE: In order that the logical persists acrossa system reboot, add the above line to `SYS$MANAGER:SYLOGICALS.COM`.

3. Run the `testparm` utility and verify that the server is configured as the Standalone Server:

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

4. Start the HP CIFS Server:

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

4 Kerberos support

The Kerberos protocol is regulated by the IETF RFC 1510. Kerberos was adopted by Microsoft for Windows 2000, and is the default authentication protocol for Windows 2000 and 2003 domains (including the Windows 2000 and XP clients that are part of those domains). For the HP CIFS Server, Kerberos authentication is limited to server membership in a Windows 2000 or 2003 domain, and only when the HP CIFS Server is configured with "security = ads".

This chapter describes Kerberos and a variety of Kerberos configuration information, which can be used when the HP CIFS Server co-exists with other OpenVMS applications that use the Kerberos security protocol.

This chapter addresses the following topics:

4.1 Overview

Kerberos is an authentication protocol that uses shared secrets and encryption methods to decode keys between an authenticator, an authenticatee, and the resources that the authenticatee requires access to. For HP CIFS Server, the following applies:

- Windows Key Distribution Center (KDC): Authenticator
- Windows client: Authenticatee
- HP CIFS Server: Resource

For more information about CIFS related Kerberos information, see the HP white paper *HP CIFS Server and Kerberos*: http://docs.hp.com/en/netcom.html .

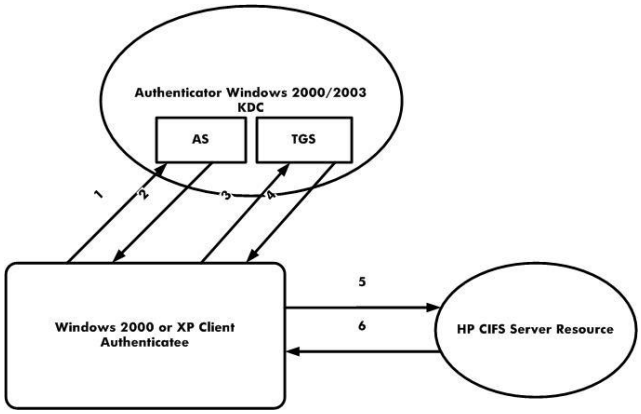
The protocol exchanges do not include actual passwords passed over the wire, therefore a password cannot be detected and unencrypted to gain access to a resource. Instead, encrypted keys are passed over the wire and each of the three principals (KDC, Windows client, and CIFS server) use pre-arranged secrets to decode the keys and allow access. The secrets are not transferred. The critical components of the exchanges are:

- Windows Key Distribution Center (KDC): Central Kerberos Authority for a domain
- Long-Term Key: Persistent key that is derived from a client's password
- Session Key: Short-term key that is used for authentication before it expires
- Ticket Granting Ticket (TGT): Allows a client access to the KDC to get a service ticket from TGS
- Ticket Granting Service (TGS): Exchange that provides client access to a CIFS server's service
- Authentication Service (AS): Exchange that actually allows client access to the KDC

For a comprehensive Microsoft Kerberos implementation white paper, see: http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/kerbers.mspx

4.2 Kerberos CIFS authentication example

Figure 4-1 Kerberos authentication environment



The following describes a typical Kerberos logon and share service exchange using Kerberos authentication in a Windows 2000 or 2003 domain environment shown in Figure 6–1:

1. The Windows client sends the principal name and password to the AS when running a user netlogon command.
2. The AS validates the principal and sends credentials to the Windows client, including a TGT and associated session key that allows the client to access the Windows KDC.
3. The Windows client uses the session key and the TGT to request a service ticket for a share service from TGS.
4. TGS sends the service ticket and other information to the Windows client.
5. The Windows client sends the service ticket to the HP CIFS Server for a share service.
6. The HP CIFS Server verifies the received information and authorizes the Windows client to access the server's share.

When `TESTPARAM` utility is executed, the following parameter values are displayed if HP CIFS Server is configured to use Kerberos authentication:

```
[global]
workgroup = MYREALM
realm = MYREALM.HP.COM
netbios name = atcux5
server string = Samba Server
security = ADS
password server = HPWIN2K3.MYREALM.HP.COM
```

These parameter values are used to configure the HP CIFS Server keytab. You can validate your configuration by starting the HP CIFS Server, logging on to the domain with clients, and mounting an HP CIFS share.

NOTE: On OpenVMS, for the HP CIFS Server to support Kerberos authentication, it is mandatory that the Kerberos kit is installed on the system, but Kerberos configuration is optional.

5 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:

5.1 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 `tdbsam`, or NT server user databases.

The LDAP directory can be used to store Windows user information, which had previously been stored in the `passdb.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 `passdb.tdb` file used by the `tdbsam` backend.

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

5.1.1 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 `tdbsam` 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.

5.2 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.

5.2.1 Domain model networks

5.2.1.1 HP CIFS Server acting as 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.

5.2.1.2 HP CIFS Server acting as 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`.

5.2.1.3 HP CIFS Server acting as 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 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 through 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.

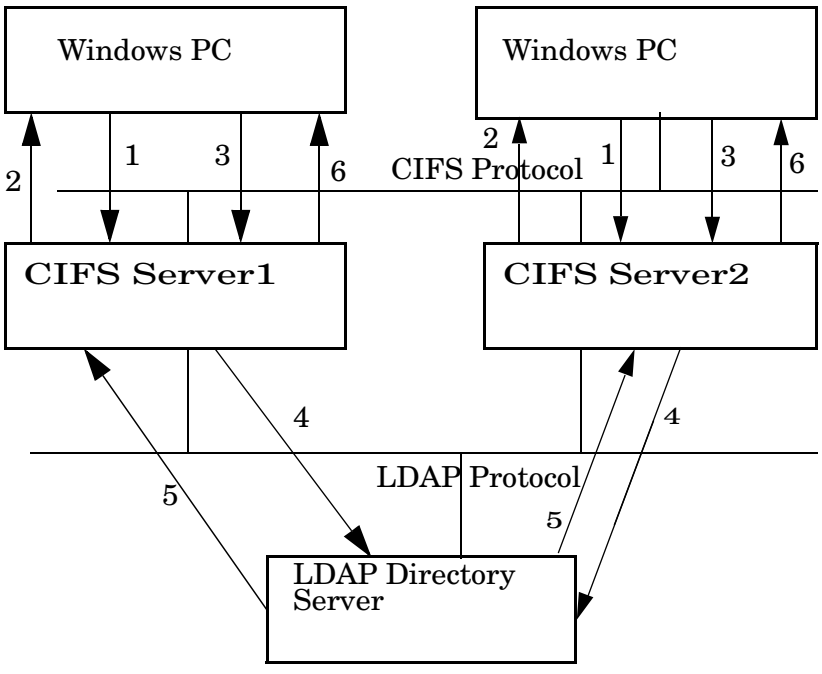
5.2.2 Workgroup model networks

If LDAP is enabled, authentication falls 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.

5.2.3 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 5-1 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.

5.3 Installing and configuring your directory server

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

5.3.1 Installing 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*.

5.3.2 Configuring 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 "/DC=<domcompnentname>"
   ```

   where:

   `/DC` is the domain name specified in the Directory Information Tree (DIT) structure that is created under the LDAP (X500) tree.

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

   ```
   $ DXIM /I=C
   DXIM> CREATE "/DC=<domcomponentname>" ATTRIBUTES —
   _DXIM>objectClass=domain,DC=<domcomponentname>
   ```

   where:

   `/DC` is the domain name specified in the DIT structure that is created under the LDAP (X500) tree.

3. `DXIM> SET PASSWORD "/DC=<domcomponentname>"`

   `Old Password>` Press **Enter**, if it is the first time.

   `New Password>` Specify your new password.

   Verify Password>

5.4 Configuring 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 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>
```

5.4.1 LDAP configuration parameters

Table 5–1 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 5-1 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 prepended 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 = sambaDomainName=<workgroup>` in SMB.CONF, if the HP CIFS Server is configured as a PDC. `ldap user suffix = sambaDomainName=<netbios name>`, if the HP CIFS Server is configured as a member server.
`ldap group suffix`	Specifies the base of the directory tree where you want to add group information. The suffix string is prepended 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 = sambaDomainName=<workgroup>` in SMB.CONF, if the HP CIFS Server is configured as a PDC. `ldap group suffix = sambaDomainName=<netbios name>`, if the HP CIFS Server is configured as a member server.
`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.

Table 5-1 Global LDAP parameters *(continued)*

Parameter	Description
`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: • **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**.
`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 not set, the value of ldap suffix is used instead. The suffix string is prepended 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 not set, the value of ldap suffix is used instead. The suffix string is prepended to the ldap suffix string so use a partial distinguished name (dn). By default, `ldap machine suffix = `. For example, `ldap machine suffix = ou=Computers`.

6 User and group mapping

This chapter addresses the following topics:

6.1 Introduction

As a file server that uses CIFS or SMB protocol, the HP CIFS Server is required to provide Windows-like file security based on Windows users and group accounts. Because HP CIFS Server is dependent upon host system file security, it has to use OpenVMS file security, which is based on UICs and resource identifiers. The implementation of Windows file security, which is based on user and group account Security Identifiers (SID) and ACLs is different from the OpenVMS file security that is based on user UICs, resource identifiers, and OpenVMS ACLs. The only way for HP CIFS Server to bridge the file security on these two different Operating Systems is by mapping:

- Windows users and groups to OpenVMS usernames (UICs) and resource identifiers.
- Windows permissions to OpenVMS permissions.

This chapter describes various methods used by the HP CIFS Server to map Windows or CIFS domain users and groups to OpenVMS users and resource identifiers. Chapter 10 (page 147) describes the Windows to OpenVMS file security mapping.

Using the user and group mapping mechanism, the HP CIFS Server maps the CIFS domain users to OpenVMS usernames and the CIFS domain groups to OpenVMS resource identifiers. Internally, the mapping is done between the CIFS domain user SIDs and the OpenVMS UICs and the CIFS domain group SIDs and the OpenVMS resource identifier values.

6.2 CIFS domain users and groups

The CIFS domain users and groups can refer to users and group accounts in any of the following databases:

- When the HP CIFS Server is a PDC or a BDC, the CIFS users and groups can be the user and group accounts in the HP CIFS Server domain database or in the domains trusted by HP CIFS Server.
- When the HP CIFS Server is Member Server, the CIFS users and groups can be the user and group accounts in any of the following:
  - HP CIFS Server local database,
  - In the domain, where the HP CIFS Server is Member Server, or
  - In the domains trusted by a domain, where the HP CIFS Server is Member Server.
- When the HP CIFS Server is Standalone Server, CIFS users and groups are the user and group accounts existing in the HP CIFS Server local database.

For easy readability, the CIFS domain user and group mapping to OpenVMS usernames (UICs) and resource identifiers is simply referred to as user and group mapping.

This chapter first explains the various methods of mapping users and then about mapping groups. Even though the user mapping is mandatory, group mapping is optional, provided the file security is based on the OpenVMS resource identifiers and these resource identifiers are directly granted to the mapped OpenVMS usernames in the `SYSUAF` file. This is explained in detail in Section 6.4 (page 92)". As the HP CIFS Server file security is set based on the mapped OpenVMS

user identifiers (UICs) and resource identifiers, it is important have knowledge of the user and group mapping before attempting to establish file security.

For more information about the HP CIFS file security implementation, see Chapter 10 (page 147).

6.3 User mapping

User mapping involves mapping the CIFS domain users to OpenVMS usernames (UICs). There are three ways using which the HP CIFS Server maps these CIFS domain users to OpenVMS usernames:

1. Automatic user mapping provided by WINBIND.

   This method is applicable only when the HP CIFS Server is configured as a Member server or when configured as a domain controller in a CIFS domain which trusts other domains.

2. Implicit user mapping.

   Implicit username mapping occurs when the HP CIFS Server username and OpenVMS username are identical and no explicit mapping exists. Before creating an HP CIFS Server user account (that is, using the PDBEDIT utility) an OpenVMS account with the same name must exist and must be assigned a unique identifier.

3. Explicit user mapping.

   When a user's Windows account name is not identical to their OpenVMS account name, the accounts can be mapped using a text file defined by the *username map* SMB.CONF parameter.

NOTE: The HP CIFS Server requires each user account to have a UIC identifier in the RIGHTLIST database.

For example, for a mapped OpenVMS user named, GANGA with a UIC of [600,600], there must be a corresponding identifier with a UIC of [600,600].

The following sections provide details about each of the user mapping mechanisms.

6.3.1 Automatic user mapping

Users belonging to the Windows domain, where CIFS is a member or the domains trusted by it can be automatically mapped to OpenVMS usernames, provided WINBIND is enabled and a valid idmap UID range is available in the `SMB.CONF` file. This mapping mechanism can also be used for user accounts that belong to a trusted domain, when the HP CIFS Server is a PDC or a BDC. For more information about automatic mapping, see Chapter 7 (page 95).

6.3.2 Implicit user mapping

A CIFS domain user can be implicitly mapped to an OpenVMS username provided the names are identical.

For example, the Windows user ANITA is implicitly mapped to an OpenVMS username ANITA, if it exists.

By default, the HP CIFS Server local users are implicitly mapped to OpenVMS usernames because the HP CIFS Server local account can only be created, if the OpenVMS account by the same name exists.

For example, to create a user STEFFI in HP CIFS Server database, you must first create or ensure that an OpenVMS username STEFFI exists in `SYSUAF` database. As such, if you want to create a user in the HP CIFS Server database, the following conditions must be met:

- An HP CIFS Server username must conform to OpenVMS user naming conventions, that is, a username can contain only alphanumeric characters, dollar ($) and an underscore(_). A username cannot begin with a number.
- OpenVMS usernames cannot exceed 12 characters in length. Due to this, the HP CIFS Server local user account names are restricted to a maximum of 12 characters .

Explicit mapping mechanism describes an alternative to overcome these limitations.

For more information about creating and managing user accounts in the HP CIFS Server database, Chapter 8 (page 103).

6.3.3 Explicit user mapping

Explicit user mapping allows you to:

- Map Windows usernames to OpenVMS usernames when they are not identical.
- Overcome the limitations imposed by implicit user mapping (discussed in the Implicit mapping section).

When a user's Windows username is not identical to their OpenVMS username, the usernames can be mapped explicitly using a text file defined by the SMB.CONF *username map* parameter.

For example, to map the Windows username "Andrew Smith" in the CORP domain to the OpenVMS user account ASMITH, edit `SAMBA$ROOT:[LIB]USERNAME.MAP` and add the line:

```
asmith=corp\"Andrew Smith"
```

To overcome the limitations imposed by the OpenVMS username conventions, when creating the HP CIFS Server local accounts, first create the required OpenVMS and CIFS Server local accounts and then add an entry to the username map file, mapping the desired Windows username to the OpenVMS account.

For example, to create a Windows user account named "Andrew Smith", follow these steps:

1. If necessary, create an OpenVMS account, ASMITH for example, with a unique UIC.
2. Using either the `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` utility or the PDBEDIT utility, create an HP CIFS Server local account named ASMITH (the name must be identical to the OpenVMS account in step 1).
3. Add an entry to the `username.map` file, mapping the Windows username "Andrew Smith", to the OpenVMS username ASMITH. For example:

   ```
   $ EDIT samba$root:[lib]username.map
   asmith="Andrew Smith"
   ```

When a Windows user establishes a session with the username "Andrew Smith", the user is mapped to the OpenVMS ASMITH account.

NOTE:

1. In step 3, it is assumed that the line `username map = samba$root:[lib]username.map` exists in the [global] section of the `SMB.CONF` file.
2. When you use the `SAMBA$CONFIG.COM` utility to configure HP CIFS Server, the `samba$root:[lib]username.map` template file is created and the *username map* parameter is added to the `SMB.CONF` file.
3. If you create a different file to use as the username map file, you must ensure the record format is Stream. Also, change the value of the *username map* parameter in the `SMB.CONF` file to reflect the path and name of the file.

HP CIFS supports the mapping of multiple domain users to a single OpenVMS username. In this case, the domain users that have been mapped to a single OpenVMS username share the same user persona and, thus, the same security context. Use this option of mapping multiple CIFS domain users to a single OpenVMS username only after understanding the file security

implications. This option cannot be used for user accounts that exist in CIFS Server account database, i.e., multiple CIFS Server users cannot be mapped to a single OpenVMS user account.

While explicitly mapping the CIFS domain users, the map file is parsed line by line. Following points must be noted while explicitly mapping a user:

- Each line must contain a single OpenVMS account on the left of an equal sign (=) followed by a list of CIFS domain user names on the right.
- There must be no space before or after the equal sign (=). For example, you must not add the mapping as: ASMITH = “Andrew Smith”. The correct mapping entry is: ASMITH=”Andrew Smith”.
- If the line is starting with a hash (#) or a semi-colon (;), then it is treated as a comment line and ignored. For example, following line is treated as comment line:

  ```
  #this file contains explicit user mapping entries for use by CIFS
  #Server
  ```

- If the user account exists in a domain (for example, WINDOM) where CIFS Server is a Member Server or in any of the domains trusted by WINDOM, then the user account must be prefixed with domain name followed by slash “\” when mapping. Similar syntax must be used for user accounts in trusted domains when CIFS Server is a PDC or BDC. For example, to map a user “GangaR” in the domain WINDOM to an OpenVMS account GANGA, use:

  ```
  ganga=windom\GangaR
  ```

- All the domain users connecting to HP CIFS Server can be mapped to a single OpenVMS user account. Note that with this setting all the users that are mapped to a single OpenVMS user account share the same user persona and, thus, the same security context. In the following example, all the Windows users are mapped to an OpenVMS user account CIFS$DEFAULT.

  ```
  cifs$default=*
  ```

- If a line begins with an '!', then the processing stops 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, if the user mapping file contains following mapping entries, mapping stops after encounter the line “!GANGA=windom\gangar”. In this case, the Windows user “GangaR” is mapped to an OpenVMS user account GANGA instead of CIFS$DEFAULT.

  ```
  !ganga=windom\gangar
  cifs$default=*
  ```

- When mapping multiple domain user accounts to a single OpenVMS user account, separate the domain user accounts using a space or a comma as in the following example:

  ```
  tunga=windom\kaveri,windom\neela
  ```

- If the user name contains a space in it, then the user name must be included within quotes when mapping.

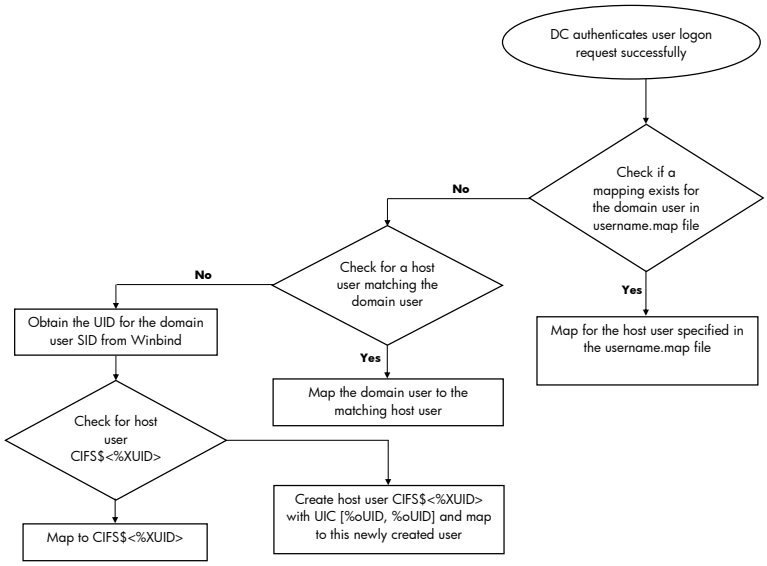
  For example, to map a user “Andrew Smith” to an OpenVMS account, use:

  ```
  asmith=“Andrew Smith”
  ```

6.3.4 User authentication and host mapping process flow

Figure 6-1 (page 91) shows user authentication and host mapping process flow in a member server environment.

Figure 6-1 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. The HP CIFS Server 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.

NOTE: For information on how the UID obtained from WINBIND is used for the automatic creation and mapping of OpenVMS username, see Chapter 7 (page 95).

6.3.5 Group mapping

Group mapping involves mapping CIFS domain groups to OpenVMS resource identifiers. There are two ways in which HP CIFS Server maps these CIFS domain groups to OpenVMS resource identifiers:

1. Automatic group mapping provided by WINBIND - This method may be used for domain global groups in the local domain only when HP CIFS Server is a member server. The method may also be used for domain global groups in trusted domains, regardless of the HP CIFS Server domain role. For more information about automatic mapping of group accounts, see Chapter 7 (page 95).
2. Explicit group mapping – This method allows you to create and map group accounts in HP CIFS Server database for any the HP CIFS Server roles.

6.3.5.1 Explicit group mapping

When an HP CIFS Server is configured as PDC or BDC, you can create two types of groups – local and global. The global groups are also referred to as domain groups. When the HP CIFS

Server is a Member Server or Standalone Server, only local groups should be created. In either case, the group account can be created in the HP CIFS Server database and simultaneously mapped to the OpenVMS resource identifiers using the HP CIFS Server management utility `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` or by executing the command "NET GROUPMAP ADD". While creating and mapping the group account, the HP CIFS Server management utility can additionally create the specified OpenVMS resource identifier if it does not exist.

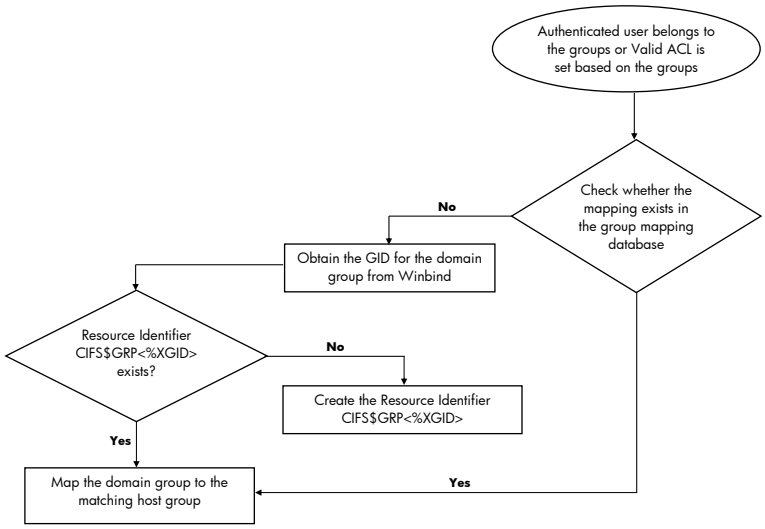
For more information about creating and managing group accounts in the HP CIFS Server database, see Chapter 8 (page 103).

By default, explicit group mappings are stored in the `SAMBA$ROOT:[VAR.LOCKS]GROUP_MAPPING.TDB` file.

6.3.5.2 Group mapping process flow

Figure 6-2 shows the group mapping process flow in a member server environment.

Figure 6-2 Group mapping process flow



The following describes group mapping process flow shown in Figure 6-2:

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>`.

NOTE: For information on how the GID obtained from WINBIND is used for the automatic creation and mapping of OpenVMS resource identifiers, see Chapter 7 "WINBIND support".

6.4 Alternate to group mapping mechanism

Instead of utilizing the group mapping mechanism discussed earlier, administrators may implement security groups by simply granting resource identifiers to the mapped OpenVMS accounts of CIFS domain users who are to be members. These resource identifiers are used in ACLs to control access to resources. However, this method does not allow the groups to be added when remotely managing the server (that is, they cannot be referenced when setting permissions from a Windows client). To expose groups to client systems for management purposes, they must be mapped using one of the group mapping mechanisms.

6.5 User persona creation

The HP CIFS Server obtains the mapping of the CIFS domain user and groups to the OpenVMS UIC and resource identifiers when a client successfully establishes a new session to HP CIFS server. If no mappings exist and WINBIND automatic mapping is enabled, the required OpenVMS user and resource identifiers are created and mapped.

For information about CIFS domain users and groups that can be automatically mapped using WINBIND, see Chapter 7 (page 95).

After the user is authenticated, the HP CIFS Server creates an OpenVMS persona for the user (defining the user's security profile). On behalf of the user, the SMBD process uses this persona to access objects such as files, directories, and print queues.

The user's persona is made up of the following:

- The UIC and identifiers of the mapped OpenVMS account as well as the resource identifiers of mapped groups of which the user is a member.
- Default privileges of the mapped OpenVMS user account.

When a user attempts to access an object, OpenVMS grants access to the object based on the persona of the mapped OpenVMS user. The only exception to this is when the user is included in the list of the *admin users* parameter in the HP CIFS Server configuration file. The persona of users included in the *admin users* list receive the UIC, identifiers, and default privileges of the `SAMBA$SMBD` account. The `SAMBA$SMBD` account default privileges include all privileges.

NOTE:

- The HP CIFS Server does not use the password of an OpenVMS account when authenticating a user.
- The `SAMBA$SMBD` account is created by the HP CIFS Server as part of the HP OpenVMS CIFS kit installation.

7 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:

7.1 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 increases unless the proper configuration is chosen initially. This chapter helps 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 OpenVMS CIFS, but the implementation method is different.

7.2 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.

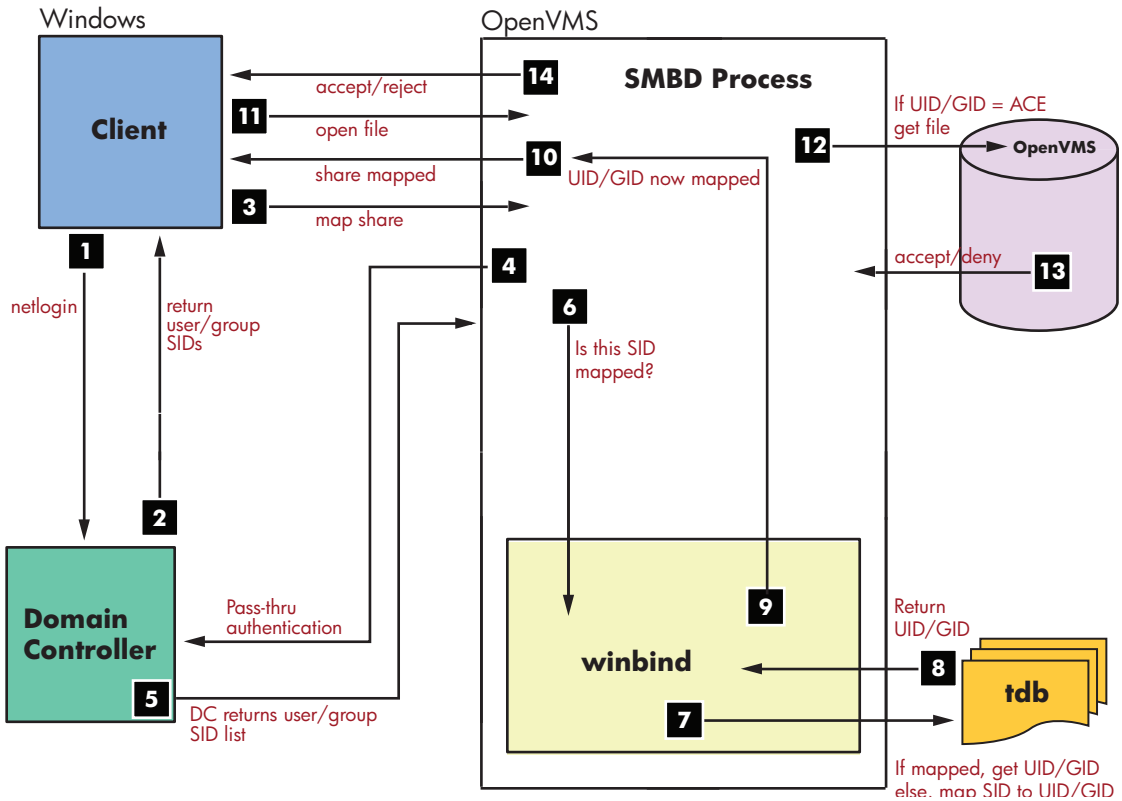
- Identity storage

  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].

7.3 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 7-1 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.

7.4 WINBIND functionality

WINBIND is a special feature of HP CIFS Server that provides the following functionality:

- Automatic Mapping — For users and groups belonging to trusted domains or to the domain, where HP CIFS Server is a Member Server, WINBIND automatically creates and maps the corresponding OpenVMS users and groups (resource identifiers).
- Nested Group Support — Using nested groups, domain global groups including those from trusted domains, can be members of local groups (a group-within-a-group, or "nested" groups). Nested groups may be used on any server, regardless of the role.
- Trusts — WINBIND is required for all trust functionality, when CIFS is a PDC or a BDC.

The WINBIND functionality provided by CIFS Server is controlled though the logical, WINBNDD_DONT_ENV. In addition, valid ranges for the "idmap uid" and "idmap gid" parameters must be specified in the HP CIFS Server configuration file. If the parameters are omitted, the automatic mapping functionality is not enabled. If this logical is disabled or not defined, HP CIFS Server provides WINBIND Functionality. Define the logical name to 1 to disable all WINBIND functionality. For example,

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

By default, the WINBINDD_DONT_ENV logical name is not defined. As WINBIND functionality plays an important role for handling users and groups belonging to the domain where CIFS Server is member or to the trusted domains, it is recommended not to disable WINBIND functionality except on a Standalone Server.

7.4.1 Automatic mapping

WINBIND can create OpenVMS user accounts and resource identifiers (in the POSIX GID format) and maintain their correspondence to the appropriate Windows SIDs to minimize identity management efforts. The WINBIND identity mapping database file, `SAMBA$ROOT:[VAR.LOCKS]WINBINDD_IDMAP.TDB` maintains the mapping between Windows SIDs and OpenVMS user accounts and resource identifiers. The mapping between a Windows SID and an OpenVMS user account or a resource identifier is created, only if there is no existing mapping entry in this database file. If the required mapping is missing, the automatic creation and mapping of OpenVMS user accounts and resource identifiers occurs under the following circumstances:

- After the user is successfully authenticated, HP CIFS Server attempts to map the user and all groups in which the user is a member, to an OpenVMS username (UIC) and a resource identifier. The domain or CIFS Server groups can be either nested groups or the groups to which the authenticated user directly belongs. In a scenario, where, there is no mapping or there exists an authenticated user (and if this user is also a domain user (where CIFS Server is a member)) or a trusted domain user, WINBIND can automatically create the required OpenVMS user account and then map the OpenVMS username to the authenticated user. Similarly, if no mapping exists for domain global groups in which the user is a member, WINBIND can create the required OpenVMS resource identifiers and map them to the domain groups.
- When setting security on files and directories, if the security principal (subject) to whom you are granting the permission is a user or global group in the domain, where CIFS Server is a member or in a trusted domain, WINBIND can create and map the required OpenVMS username (UIC) or resource identifier to a domain user or group SID.
- When the CIFS server is a PDC, while adding a workstation to the CIFS domain, an OpenVMS username is automatically created and mapped to the workstation account that is created. In this case, the workstation account name must conform to the OpenVMS user naming convention.

Every OpenVMS account requires a username and a UIC. WINBIND derives the account username and UIC for new accounts from the range specified for the HP CIFS Server configuration parameter

"idmap uid". The range start and end values are specified as integer numbers, separated by a hyphen. For example:

```
idmap uid = 1000 - 2000
```

Similarly, WINBIND derives the name and value of the OpenVMS (POSIX group) resource identifier it creates from the range specified for the HP CIFS Server configuration parameter "idmap gid". For example:

```
idmap gid = 1000 - 2000
```

The following sections describe how WINBIND performs the automation processes:

- Section 7.4.1.3 (page 99)

7.4.1.1 When is automatic mapping required?

- The HP CIFS Server uses WINBIND to map the domain global group names (belonging to the domain where CIFS Server is a member or to the trusted domains) to OpenVMS resource identifiers. The WINBIND feature is useful when you want to set permissions on files and directories based on the domain global groups.
- When the HP CIFS Server is a PDC, the creation of computer accounts in the CIFS accounts database is not possible unless an OpenVMS account first exists. WINBIND can create the necessary OpenVMS account and the associated CIFS account for a computer when it joins the domain. Otherwise, the administrator must ensure the OpenVMS account is created using other methods prior to joining the computer the domain.

7.4.1.2 When is automatic mapping not required?

Automatic mapping provided by WINBIND need not be used if the following conditions are satisfied:

- All the users that belong to the domain where the HP CIFS Server is a member or to the trusted domains when connecting to the HP CIFS Server are either explicitly or implicitly mapped to the OpenVMS usernames.
- Object permissions lists do not include domain global groups (either from the local or trusted domains).
- If HP CIFS Server is a PDC, computer accounts for systems which join the domain are created prior to the attempt to join the domain.

To set permissions for domain global groups, use one of the following methods:

1. Create OpenVMS resource identifiers to represent local groups. Create and map CIFS local groups to OpenVMS resource identifiers using the `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` or `NET GROUPMAP ADD` command. Use the `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` or `NET [RPC | ADS] GROUP ADDMEM` command to add domain global groups and domain users, either from the local domain or any trusted domain, or local CIFS users and groups as group members. For information on how to add domain global groups as members to CIFS Server local groups, see Section 8.3 (page 111)
2. Use the mechanism mentioned in Section 6.4 (page 92) to grant OpenVMS resource identifiers to OpenVMS usernames that are mapped to the CIFS domain users.

7.4.1.3 Creating and mapping OpenVMS user account

WINBIND uses the "idmap uid value to derive both the OpenVMS username and the UIC for the new account. The uid value is converted to a hexadecimal value and appended to the string "CIFS$" to derive the OpenVMS username. The uid value is converted to octal and the octal value is used as the UIC group and member number.

NOTE: Because the 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 group numbers below octal 376 are reserved for use by HP, it is recommended that the lower range of the "idmap uid" value not be less than 255.

For example, if the HP CIFS Server configuration file contains:

```
idmap uid = 1000-2000
```

WINBIND initially allocates uid 1000, converts the value to hexadecimal (3E8) and octal (1750), and creates an OpenVMS account with a username of CIFS$3E8 and a UIC of [1750,1750].

The accounts created by WINBIND do not allow interactive login and are granted only NETMBX and TMPMBX privileges. If the OpenVMS account is created successfully, the mapping of the assigned uid (1000 in the example above) to the user's domain account SID is stored in the file SAMBA$ROOT:[VAR.LOCKS]WINBINDD_IDMAP.TDB. This is a critical file and must be backed up regularly to avoid loss of the mappings necessary to maintain object security.

7.4.1.4 Creating and mapping resource identifiers

WINBIND uses the next "idmap gid" integer value to derive both the OpenVMS resource identifier (group) name and value. The "idmap gid" value is converted to a hexadecimal value and it is used as (1) the value assigned to the resource identifier, and (2) appended to the string "CIFS$GRP" to derive the name of the resource identifier.

NOTE: Because WINBIND creates POSIX Group Resource Identifiers (POSIX GID), the maximum value is limited to %xFFFFFF or %d16777215. The lower limit is 1. OpenVMS automatically adds %xA4000000 to the value chosen. Values 1616777200 – 16777215 are reserved for use by HP CIFS Server; therefore, the upper range of the "idmap gid" value should not exceed 167777199.

For example, if the SMB.CONF file contains:

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

WINBIND initially allocates GID 5000 and crates an OpenVMS resource identifier named CIFS$GRP1388.

If the identifier is created successfully, the mapping of the assigned gid (5000) to its corresponding domain group SID is stored in the file SAMBA$ROOT:[VAR.LOCKS}WINBINDD_IDMAP.TDB. important that you back up this file regularly to avoid losing the mappings necessary to maintain object security.

NOTE:

- Only the upper range value of the "idmap uid" and "idmap gid" parameters can be increased to extend the range. The lower range value should never be changed. For example, A range of 1000 – 2000 may be changed to 1000 – 3000 to provide an additional 1000 uids for allocation by WINBIND. WINBIND automatically adjusts the existing "idmap uid" range while retaining the current mapping entries in the WINBIND identity mapping database file. This guarantees that the existing security on files and directories that might have been set based on the existing mapping entries are still valid.
- For information about the User and Group Mapping Flow chart, see Chapter 6 (page 87)

7.4.1.5 Managing users and groups created by WINBIND

WINBIND uses the range of values specified for "idmap uid" and "idmap gid" parameters in the CIFS Server configuration file when creating OpenVMS usernames and resource identifiers. When WINBIND runs out of either of these idmap ranges, it reports errors in the CIFS client log files. The client log files are created in the directory `SAMBA$ROOT:[VAR]`, by default (the location is specified in the "log file" parameter of the HP CIFS Server configuration file).

A utility named WBINFO is included which can be used for viewing the OpenVMS usernames and resource identifiers created by WINBIND and the corresponding mapping to domain users and groups. You can execute the WBINFO utility as:

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
$ WBINFO --hostusers-to-domainusers
$ WBINFO --hostgroups-to-domaingroups
```

The option “--hostusers-to-domainusers”, displays the CIFS domain users and their mapped OpenVMS usernames. The option “--hostgroups-to-domaingroups”, displays the CIFS domain groups and their mapped OpenVMS resource identifiers. These two options are meant only for viewing the mapped users and groups. It cannot be used for enumerating all users and groups.

To check for the mapping between a single OpenVMS username or resource identifier (group) and a domain user or group, execute the command:

```
$ WBINFO --hostname-to-domainname=<OpenVMS-identifier>
```

Where:

<OpenVMS-identifier> is either an OpenVMS username or resource identifier name.

7.4.2 Nested group support

A group-within-a group is referred to as nested grouping. Using the nested group support provided by WINBIND, you can add the following users and groups as members to CIFS local groups:

1. Users and domain global groups that belong to the domain where CIFS Server is a member.
2. Users and domain global groups that belong to the domains trusted by the domain where CIFS Server is a member.
3. Users and domain global groups belonging to the trusted domains when CIFS Server is a PDC or BDC.
4. Users and local groups in CIFS server database

The nested group functionality allows you to establish file security based on CIFS local groups. WINBIND supports nested groups, even when the automatic mapping feature is not enabled.

7.5 Disabling WINBIND

Unlike in Samba Linux/UNIX in HP OpenVMS CIFS, the `Windbind` 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
```

NOTE: In order that the logical persists across a system reboot, add the following logical to the `SYS$MANAGER:SYLOGICALS.COM` file.

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

7.6 Configuring HP CIFS Server with WINBIND

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

7.6.1 WINBIND configuration parameters

Table 7-1 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 7-1 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: • `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://ldapserverA.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.

8 Managing users, groups, account policies and trusts

This chapter addresses the following topics:

8.1 Introduction

To manage users in the HP CIFS Server database, you can use either the CIFS Server management utility SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM, or the pdbedit command-line utility. For more information about using the SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM utility to add, modify, and delete the HP CIFS Server users, see Section 8.2.1 (page 103). For more information on the pdbedit utility, see Section 8.2.2 (page 108)

8.2 Managing users

Users in the HP CIFS Server database can be managed using the HP CIFS Server management utility, SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM or by using pdbedit command line utility. The section Section 8.2.1 (page 103) describes how to use SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM to add, modify, and delete CIFS Server users while the section Section 8.2.2 (page 108) describes how to use the pdbedit utility to achieve the same.

8.2.1 Managing users using CIFS Server management utility

The SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM utility can be used for listing, adding, modifying or deleting users from the HP CIFS Server account database using menu options.

To invoke the CIFS Server management utility, execute the following command:

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

OR

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

This displays the HP OpenVMS CIFS Server Management Main Menu. Use option 3, "Manage Users", to display the user management menu:

```
HP CIFS Server User Management Menu

                 1  - List users
                 2  - List a user
                 3  - Add user
                 4  - Modify user
                 5  - Remove user
                [E] - Exit
Enter CIFS user management option:
```

8.2.1.1 Listing users

Use option 1, "List users", to list all the user and machine accounts that exist in the CIFS Server account database. An output similar to the following is displayed:

```
Enumerating users in the domain PIANODOM.
  Please wait...

User name             Comment
---------------------------------------
sso                   Generic account for SSO team
ganga
cifsadmin
tunga                 Account for user Tunga

Press Enter to continue:
```

8.2.1.2 Listing full information for a user

Use option 2, “List a user”, to list full information for a user or machine account that exists in the HP CIFS Server account database. The procedure prompts for the account name and displays an output similar to the following:

```
 This option displays full information for the specified user.

Enter the username: tunga

OpenVMS username:     tunga
NT username:
Account Flags:         [U          ]
User SID:              S-1-5-21-4210255526-1716153954-2929367854-1005
Primary Group SID:     S-1-5-21-4210255526-1716153954-2929367854-513
Full Name:
Home Directory:        \\piano\tunga
HomeDir Drive:
Logon Script:
Profile Path:
Domain:                PIANODOM
Account desc:          Account for user Tunga
Workstations:
Munged dial:
Logon time:            0
Logoff time:           never
Kickoff time:          never
Password last set:     Mon, 03 May 2010 13:18:48 PDT
Password can change:   Mon, 03 May 2010 13:18:48 PDT
Password must change: never
Last bad password   :  0
Bad password count  :  0
Logon hours         :  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Press Enter to continue:
```

8.2.1.3 Adding a user

Use option 3, “Add user”, to add a user or machine account to the CIFS Server account database. The procedure displays an output similar to that shown for adding a user account.

When CIFS Server role is a PDC or a BDC, the menu displayed is:

```
HP CIFS Server User Account Creation Menu

                1. User name (*):
```

```
                2. Full name:
                3. Description:
                4. Home drive:
                5. Logon script:
                6. Profile path:

                * = required field

Enter item number or press Enter to accept current values [Done]:
```

When the CIFS Server role is a Member Server or a Standalone Server, the menu displayed is:

```
HP CIFS Server User Account Creation Menu

                1. User name (*):
                2. Full name:
                3. Description:

                * = required field

Enter item number or press Enter to accept current values [Done]:
```

After entering the values for the selected options, the utility displays a menu for modifying the account flags as follows:

```
HP CIFS Server User Account Flags Menu

                1. Disable Account: no
                2. Password not required: no
                3. Password does not expire: yes
                4. Automatic locking: no
                5. Account Type: user
Enter item number or press Enter to accept current values [Done]:
```

Each of these options is described in detail in the following sections.

NOTE: The option “5. Account Type: user” is displayed only if the CIFS Server role is PDC or BDC.

8.2.1.3.1 User name

User name specifies the account name to be added. This field is mandatory. The user name cannot be identical to any other user or group name of the domain or server being administered. CIFS Server requires that every user account created in CIFS Server database must have a corresponding OpenVMS username. When specifying a user name, ensure that the user name:

- Includes only alphanumeric characters, the dollar sign ($) and an underscore (_)
- Does not start with a numeric character
- Does not have more that 12 characters

While creating the user account, if the utility finds that the specified username is not present in the SYSUAF database, it provides an option to create an identical username in SYSUAF. To do this, you might be required to specify the group id number to generate a UIC for the OpenVMS account.

8.2.1.3.2 Full name

The full name is the user's complete name and is optional. It can be up to 256 characters in length. You do not have to include the full name in quotes while entering it.

8.2.1.3.3 Description

An account description is optional and it specifies a string of characters used to provide descriptive information about the user account.

8.2.1.3.4 Home drive

Home drive is optional and it specifies the drive letter to use for connecting to the home directory if the home directory for the user is a shared network directory. The drive letter can be from D to Z. The home driver specified for the user account overrides the “logon drive” SMB.CONF parameter if it exists in the global section of the Samba configuration file.

8.2.1.3.5 Logon script

Logon script is optional and it specifies a name for an optional logon script that runs each time the user logs on. A logon script can be a batch file (.BAT or .CMD file name extension) or an executable program (.EXE file name extension). A single logon script can be assigned to one or more user accounts. When a user logs in, the server authenticating the logon request locates the logon script by following the server's logon script path that you have specified.

The script must be a relative path to the [netlogon] share. If the [netlogon] share specifies the path as /SAMBA$ROOT/NETLOGON/, and the logon script is specified as SCRIPTS/STARTUP.BAT, then the file that is downloaded is:

```
SAMBA$ROOT/NETLOGON/SCRIPTS/STARTUP.BAT
```

The logon script specified for the user account overrides the “logon script” SMB.CONF parameter if it exists in the global section of the Samba configuration file.

8.2.1.3.6 Profile path

Profile path is optional and it specifies the directory where user’s roaming profiles (Desktop, NTuser.dat, etc) are stored. It specifies the directory from which the "Application Data", desktop, start menu, network neighborhood, programs and other folders, and their contents, are loaded and displayed on your Windows NT client. You can specify the profile path relative to the profiles share as “\\%L\profiles\%U”. In this case, %L is replaced by the NetBIOS name of CIFS Server and %U is replaced by the session username.

The profile path specified for the user account overrides the “logon path” SMB.CONF parameter, if it exists in the global section of the Samba configuration file. Roaming profiles for a user is disabled if user’s profile path as well the SMB.CONF parameter “logon path” point to empty string.

8.2.1.3.7 Account flags menu

The User Account Flags menu provides options to disable the account, enable automatic locking when the bad password count is exceeded, indicate no password is required and sets or clears the account expired flag. Additionally, if the CIFS Server role is PDC or BDC, the account type may be set.

8.2.1.3.8 Disable account

By setting “disable account” flag to yes, you can disable the user account.

8.2.1.3.9 Password not required

By setting “password not required” flag to yes, a user can login without supplying password for the specified user account.

8.2.1.3.10 Password does not expire

By default, a user account is created without setting the flag “password does not expire”. Due to this, the account password is subject to password expiration account policy. Irrespective of

the password expiration account policy setting, if “password does not expire” flag is set to yes, password for the specified user account will not expire.

8.2.1.3.11 Automatic locking

Automatic locking determines whether the account is subject to the automatic account locking mechanism controlled through the server account policies. If enabled, the account is locked automatically if the user exceeds the “bad password count” account policy.

8.2.1.3.12 Account type

The account type designates the account as a normal user account, a workstation trust account, a server trust account, or a domain trust account. The CIFS Server management utility may be used to create only two account types :

- Normal user account (the default) – Standard user accounts
- Workstation trust account – Valid only when HP CIFS server is a PDC or BDC. Creates a machine account for a workstation (client) system to allow it to join the domain.

To create a user account, specify “U”; to create a workstation trust account, specify “W”.

8.2.1.4 Modifying a user

Use option 4, “Modify user”, to modify a user or machine account in the CIFS Server account database. The procedure prompts you for the account name to modify and displays an output similar to that shown.

When CIFS Server role is a PDC or a BDC, the menu displayed is:

```
        HP CIFS Server User Account Modification Menu


                1. User name (*): cifsadmin
                2. Full name: CIFS Administrator
                3. Description: CIFS Server administrator account
                4. Home drive: H:
                5. Logon script:
                6. Profile path:
                7. Reset logon hours: no
                8. Reset bad password count: no

                * = required field

Enter item number or press Enter to accept current values [Done]:
```

When the CIFS Server role is a Member Server or a Standalone Server, the menu displayed is:

```
HP CIFS Server User Account Modification Menu


                1. User name (*): cifsadmin
                2. Full name: CIFS Administrator
                3. Description: CIFS Server administrator account
                4. Reset logon hours: no
                5. Reset bad password count: no

                * = required field

Enter item number or press Enter to accept current values [Done]:
```

In “HP CIFS Server User Account Modification Menu”, the two additional options are “reset logon hours” and “reset bad password count”. Otherwise, it is similar to the “HP CIFS Server

User Account Creation Menu". You can modify any of the options in the "HP CIFS Server User Account Modification Menu" except for the "User name".

After modifying values for the selected options, the utility displays a menu for modifying account flags. This menu is similar to the "HP CIFS Server User Account Flags Menu" that is displayed at the time of creating a user account. When CIFS Server is a PDC or BDC, any of the flags except "Account type" can be modified.

The description for "reset logon hours" and "reset bad password count" are provided in this section. For description about rest of the fields in the "HP CIFS Server User Account Modification Menu" and "HP CIFS Server User Account Flags Menu", see Section 8.2.1.3 (page 104)

8.2.1.4.1 Reset logon hours

Reset logon hours allows you to reset logon hours for a user and it is optional.

8.2.1.4.2 Reset bad password count

Reset bad password count allows you to reset the "bad password count" value of the account to 0. It is optional.

8.2.1.5 Deleting a user

Use option 5, "Remove user", to delete a user or machine account from the CIFS Server account database. The procedure prompts you for an account name to delete and displays output similar to that shown:

```
Enter the username to remove: tunga

Username tunga deleted.
```

8.2.2 Managing users using the pdbedit utility

This section describes how to manage user accounts in CIFS Server account database using the pdbedit utility.

Adding a user account

To add a user account in CIFS Server database:

1. To add a user account in CIFS Server database, an identical OpenVMS user account that is assigned a unique UIC. To determine if the account exists with a unique UIC identifier, execute:
   a. Verify whether the user account exists in the SYSUAF database:

   ```
   $ MC AUTHORIZE SHOW <username>
   ```

   For example, execute:

   ```
   $ MC AUTHORIZE SHOW GANGA
   ```

   If the account exists, verify it is assigned a unique UIC identifier:

   ```
   $ MCR AUTHORIZE SHOW /IDENTIFIER<username>
   ```

   For example:

   ```
   $ MCR AUTHORIZE SHOW /IDENTIFIER GANGA
   ```

   If the account does not exist, create it and assign it a unique UIC. For example:

   ```
   $ MCR AUTHORIZE COPY SAMBA$TMPLT GANGA/UIC=[500,1]
   ```

   If the account exists, but is not assigned a unique UIC identifier (that is, because it shares its UIC with other accounts), the account cannot be used to access the CIFS server.

   In order to correct this:

   - Assign the account a unique UIC and then create the identifier for the account. For example:

     ```
     $ MCR AUTHORIZE MODIFY GANGA/UIC=[500,1]/NOMODIFY_IDENTIFIER
     $ MCR AUTHORIZE ADD/IDENTIFIER/USER=GANGA
     ```

   - Assign the other accounts unique UICs and create identifiers for those which have none.
   - Continue sharing the UIC between multiple accounts, but remove the existing identifier associated with the UIC and create a new identifier for the UIC. The name of the new identifier must match the account name of the user who requires access to the CIFS Server.

   b. If it does not accept, add the user account to the `SYSUAF` database. When adding the user account to the SYSUAF database, specify a unique `UIC (/uic=[<uic value>]` and /ADD_IDENTIFIER and /flags= NODISUSER qualifiers or use the default user account template `SAMBA$TMPLT` as shown:

   ```
   $ MC AUTHORIZE COPY SAMBA$TMPLT GANGA /UIC=[500,500]
   ```

2. Add a user account in the HP CIFS Server account database:

   ```
   $ pdbedit –a <username>
   ```

   For example,

   ```
   $ pdbedit –a GANGA
   new password:
   retype new password:
   ```

8.2.2.1 Modifying a user account

To modify a user account in CIFS Server database:

- `$ pdbedit –r <username> <options>`

  For example:

  — To modify account description for a user, execute:

  ```
  $ pdbedit –r ganga --account-desc="User account for Ganga Roy"
  ```

  — To modify user's full name, execute:

  ```
  $ pdbedit –r ganga --fullname="Ganga Roy"
  ```

  — To reset bad password count for a user account, execute:

  ```
  $ pdbedit –r ganga --bad-password-count-reset
  ```

  — To reset logon hours for a user account, execute:

  ```
  $ pdbedit –r ganga --logon-hours-reset
  ```

  — To change any of the account control flags, execute:

  ```
  $ pdbedit –r ganga --account-control=[<flags>]
  ```

  Replace <flags> with any or a combination of the following values:

  - N: No password required
  - D: Account disabled
  - L: Automatic Locking
  - X: Password does not expire

  For example, to set the flag "automatic locking" and clear the other modifiable flags on the GANGA account, execute:

  ```
  $ pdbedit –r ganga --account-control="[L]"
  ```

NOTE: For a description about each of the options mentioned in the earlier section, see Section 8.2.1.3 (page 104)

Multiple options may be included in a single command line.

8.2.2.2 Deleting a user account

To delete an account in CIFS Server database, the syntax is:

```
$ pdbedit –x <username>
```

For example, to delete user account GANGA, execute:

```
$ pdbedit –x ganga
```

8.2.2.3 Listing users

To list all the users in a CIFS Server account database, execute:

```
$ pdbedit --list
```

Or

```
$ net sam list users
```

8.2.2.4 Listing account details

To view full details of an account, execute:

```
$ pdbedit --list --verbose <username>
```

For example, to list the details of an user account GANGA, execute:

```
$ pdbedit --list --verbose ganga
```

8.2.3 Changing user account password

On OpenVMS, only an administrator can change a HP CIFS Server 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 the Windows client by pressing **Ctrl+Alt+Delete** and then clicking `Change Password`.

8.3 Managing groups

The groups in the HP CIFS Server database can be managed using the HP CIFS Server management utility, `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` or by using the NET command line utility. The section "Managing groups using CIFS Server management utility" (page 111) describes how to use `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` to add, modify, and delete CIFS Server groups while the section "Managing groups using NET command" (page 115) describes how to use the NET command to achieve the same.

8.3.1 Managing groups using CIFS Server management utility

The `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` utility can be used for listing, adding, modifying, or deleting groups from the CIFS Server account database.

To invoke the CIFS Server management utility, execute the following command:

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

Or

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

This displays the HP OpenVMS CIFS Server Management Main Menu. Use option 2, "Manage groups", to display the group management menu.

```
        HP CIFS Server Group Management Menu

        Group Management Options:

                 1  - List groups
                 2  - Add group
                 3  - Remove group
                 4  - List group members
                 5  - Add group members
                 6  - Remove group members
                [E] - Exit
Enter group management option:
```

8.3.1.1 Listing groups

Use option 1, "List groups", to list all group accounts that exist in the CIFS Server account database. An output similar to the following is displayed:

```
Enumerating groups in the domain PIANODOM.
  Please wait...

Domain Admins
Domain Users
Domain Guests
Print Operators
```

```
Backup Operators
Replicator
RAS Servers
Pre-Windows 2000 Compatible Access
Administrators
Users
Guests
Power Users
Account Operators
Server Operators

Press Enter to continue
```

8.3.1.2 Adding a group

Use option 2, “Add group”, to add a group account in the CIFS Server account database. The procedure displays an output similar to that shown for adding a group account.

```
HP CIFS Server Group Account Creation Menu

        1. CIFS Server group name (*):
        2. OpenVMS resource identifier name (*):
        3. Group account description:
        4. Group Type (*): domain

        * = required field

Enter item number or press Enter to accept current values [Done]:
```

NOTE: When CIFS Server role is Member Server or Standalone server, the option “4. Group Type (*): domain” is not displayed.

8.3.1.2.1 CIFS Server group name

Group name specifies a 1 to 256 character name for the group to be added and it can include any valid Windows group account name characters. A group name cannot be identical to any other group or user name of the domain or server being administered. This is a mandatory field.

8.3.1.2.2 OpenVMS resource identifier name

To create a group name in the HP CIFS Server account database, it must be first mapped to an OpenVMS resource identifier. You can either specify an existing or a non-existing OpenVMS resource identifier. The specified OpenVMS resource identifier name can be identical to the CIFS Server group name even though it is not mandatory.

During the creation of group account, if the utility finds that a non-existing OpenVMS resource identifier name has been specified, it creates the specified resource identifier in the OpenVMS RIGHTSLIST database. This is a mandatory field.

8.3.1.2.3 Group account description

Group account description is optional and it specifies a string of characters used to provide descriptive information about the group.

8.3.1.2.4 Group account type

Group account type is applicable only when CIFS Server role is a PDC or BDC. On a CIFS Server that is configured as a Member Server or Standalone Server, all group accounts must be of type, LOCAL. When the CIFS Server role is Member Server or Standalone Server, the utility creates the group accounts of type, LOCAL.

When CIFS Server role is a PDC or BDC, two types of group accounts can be created in the CIFS Server database:

- LOCAL, A local group is local to the security system in which it is created. A local group created on a Domain Controller is available on all Domain Controllers within the same domain. A local group can contain users and global groups created on the CIFS Sever. A local group can also contain a user or global group from another domain by passing through trust relationships. Local groups cannot traverse trust relationships.
- DOMAIN, Domain or Global groups can contain user accounts from the CIFS Server domain grouped together as one group name. A global group cannot contain another global group or a local group as member. A global group can be a member of a local group that is present either in the same domain or in the domains trusted by it.

8.3.1.3 Removing a group account

Use option 3, “Remove group”, to delete a group account from the CIFS Server account database. The procedure prompts you for a group account name to delete and displays an output similar to that as shown:

```
Enter the group name to delete: testgroup
  Deleting group testgroup. Please wait...
Sucessfully removed testgroup from the mapping db
```

8.3.1.4 Listing group members

Use option 4, “List group members”, to list members of a group account that exists in the CIFS Server database. The procedure prompts you for an account name whose members must be listed and displays an output similar to that as shown:

```
Enter group name to list members: administrators

BUILTIN\administrators has 1 members
 PIANODOM\Domain Admins

Press Enter to continue:
```

8.3.1.5 Adding group members

Use option 5, “Add group members”, to add members to the membership list of the group. The procedure prompts you for a group name to which the members must be added.

When the CIFS Server role is a Member Server, the following user and group accounts can be added as members:

- user and group accounts present in CIFS Server database
- user and domain global group accounts present in the domain where CIFS Server is a member
- user and domain global group accounts present in the domains trusted by the domain where CIFS Server is a member

When the CIFS Server role is a PDC or BDC, the following user and group accounts can be added as members to DOMAIN (or GLOBAL) groups:

- user accounts present in CIFS Server database

When the CIFS Server role is a PDC or BDC, the following user and group accounts can be added as members to LOCAL groups:

- user and group accounts present in CIFS Server database
- user and domain global group accounts present in the domains trusted by the CIFS domain

When the CIFS Server role is a Standalone Server, the following user and group accounts can be added as members:

- user and group accounts present in CIFS Server database

For specifying group member account names, following syntax must be used:

```
<DOMAINNAME>\<GROUP-MEMBER-NAME>
```

- The *<DOMAINNAME>*\component can be excluded if a user or group account to be added is present in the CIFS Server database.
- Replace *<GROUP-MEMBER-NAME >* with a user or group account name that must be added as a member to the group.
- Replace *<DOMAINNAME>* with the trusted domain name if a user or group account that must be added, is present in the trusted domain.
- When the HP CIFS Server is a Member Server, if a user or group account to be added is present in the domain (for example, WINDOM), where the HP CIFS Server is a member, replace *<DOMAINNAME>* with the domain name WINDOM.

The procedure allows you to add multiple accounts as members to a group at the same time. To do this, it prompts you to enter the next group member name until you press "Enter" key without specifying a group member name.

The output is similar to the following:

```
Enter group name: cifsteam

Enter group member name: ganga
Added PIANODOM\ganga to PIANODOM\cifsteam

Enter next group member name: tunga
Added PIANODOM\tunga to PIANODOM\cifsteam

Enter next group member name: domain admins
Added PIANODOM\domain admins to PIANODOM\cifsteam

Enter next group member name:
```

8.3.1.6 Removing group members

Use option 6, “Remove group members”, to remove the specified members from the membership list of the group. The procedure prompts you for a group account name from which the members must be removed apart from prompting you to specify the group member account names that have to be removed.

To specify group member account names, type:

```
<DOMAINNAME>\<GROUP-MEMBER-NAME>
```

where,

- The *<DOMAINNAME>*\ component can be excluded if a user or group account to be removed is present in the CIFS Server database.
- Replace *<GROUP-MEMBER-NAME>* with a user or group account name that must be removed as member from the group.
- Replace *<DOMAINNAME>* with the trusted domain name if a user or group account that must be removed is present in the trusted domain.
- When the HP CIFS Server is a Member Server, if a user or group account to be removed is present in the domain (for example, WINDOM) where the HP CIFS Server is member, replace *<DOMAINNAME>* with the domain name WINDOM.

The procedure allows you to remove multiple accounts from the membership list of a group at the same time. To do this, it prompts you to enter the next group member name until you press the **Enter** key without specifying a group member name.

The output is similar to the following:

```
Enter group name: cifsteam

Enter group member name to remove: ganga
```

```
Deleted PIANODOM\ganga from PIANODOM\cifsteam

Enter next group member name to remove: tunga
Deleted PIANODOM\tunga from PIANODOM\cifsteam

Enter next group member name to remove: domain admins
Deleted PIANODOM\domain admins from PIANODOM\cifsteam

Enter next group member name to remove:
```

8.3.2 Managing groups using NET command

This section describes the steps and commands that can be manually executed for managing CIFS Server groups.

8.3.2.1 Group type

While creating groups using the `NET` command, it is important to specify the group account type. On an HP CIFS Server that is configured as a Member Server or a Standalone Server, all group accounts must be of type, LOCAL.

When the HP CIFS Server role is a PDC or a BDC, two types of group accounts can be created in the CIFS Server database:

- LOCAL, A local group is local to the security system in which it is created. A local group created on a Domain Controller is available on all Domain Controllers within the same domain. A local group can contain users and global groups created on the CIFS Server. A local group can also contain a user or a global group from another domain by passing through trust relationships. Local groups cannot traverse trust relationships.
- DOMAIN, Domain or Global groups can contain user accounts from the CIFS Server domain. A global group cannot contain another global group or a local group as member. A global group can be a member of a local group that is present either in the same domain or in the domains trusted by it.

8.3.2.2 Group members

After group accounts are added in the CIFS Server database, multiple user or group accounts can be added as members to these group accounts. The user and group accounts that can be added as members depends on the CIFS Server role. When CIFS Server role is a Member Server, the following user and group accounts can be added as members:

- user and group accounts present in CIFS Server database
- user and domain global group accounts present in the domain, where CIFS Server is a member
- user and domain global group accounts present in the domains trusted by the domain, where CIFS Server is a member

When the CIFS Server role is a PDC or BDC, following user and group accounts can be added as members to the group account that is of type DOMAIN (or GLOBAL):

- user accounts present in the CIFS Server database.

When the HP CIFS Server role is a PDC or BDC, the following user and group accounts can be added as members to the group account that is of type LOCAL:

- user and group accounts present in the CIFS Server database.
- user and domain global group accounts present in the domains trusted by the CIFS domain.

When the HP CIFS Server role is a Standalone Server, following user and group accounts can be added as members:

- user and group accounts present in the CIFS Server database.

8.3.2.3 Commands for managing HP CIFS Server groups

To manage the HP CIFS Server groups, complete the following steps:

1. Login to the OpenVMS system and define commands:
   1. Login to an OpenVMS system. For example, login to an OpenVMS system (PIANO) where CIFS Server is configured, using a fully privileged OpenVMS user account (for example, SYSTEM).
   2. Define symbols for CIFS Server utilities:

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

2. Create a privileged CIFS user:

   To manage groups requires an account with administrator privileges. If no such account exists, it must be created before continuing. From CIFS version 1.2 onwards, CIFS Server by default creates CIFSADMIN account in the SYSUAF database.

   1. Create an OpenVMS username.

      For example CIFSADMIN.

      ```
      $ MCR AUTHORIZE COPY SAMBA$TMPLT
      CIFSADMIN/UIC=[600,600]/FLAG=NODISUSER
      ```

   2. Create a CIFS user account with the same name as the OpenVMS username created in the previous step:

      ```
      $ PDBEDIT "-a" CIFSADMIN
      new password: any1willdo
      retype new password: any1willdo
      ```

   3. Update *admin users* parameter:

      The user, to whom you want to grant administrator privileges, must be added to the *admin users* parameter in the [global] section of the server configuration file.

      1. If the HP CIFS Server has previously been configured using the utility `SAMBA$CONFIG.COM`, edit the configuration INCLUDE file `SAMBA$ROOT:[LIB]ADMIN_USERS_SMB.CONF` and add the account name to the list of "admin users".
      2. If the HP CIFS Server has not previously configured using `SAMBA$CONFIG.COM`, update the main configuration file `SAMBA$ROOT:[LIB]SMB.CONF`. If necessary, add the *admin users* parameter in the [global] section and specify the name of the account to be granted administrator privileges.

3. Adding group accounts:

   To add a group account in the CIFS Server database, you are required to specify an OpenVMS resource identifier to which the group account must be mapped. You can either map the group account to an existing OpenVMS resource identifier or create a new resource identifier in RIGHTSLIST database and map to it.

   Creating resource identifier

   To create a resource identifier in the RIGHTSLIST database, execute the following command:

   ```
   $ MCR AUTHORIZE ADD/IDENTIFIER/ATTRIBUTE=RESOURCE
   <OpenVMS-resource-id-name>
   ```

For example:

```
$ MCR AUTHORIZE ADD/IDENTIFIER/ATTRIBUTE=RESOURCE CIFSUSERS
```

Creating group accounts

To create a group account of type “LOCAL” in the CIFS Server database, execute:

```
$ NET GROUPMAP ADD NTGROUP=<CIFS Server group-name>-
UNIXGROUP=<OpenVMS resource-id-name>TYPE=LOCAL
```

For example, to create a CIFSUSERS group account, execute:

$ NET GROUPMAP ADD NTGROUP=CIFSUSERS UNIXGROUP=CIFSUSERS TYPE=LOCAL

When CIFS Server is a PDC or BDC, to create a group account of type “DOMAIN” in the CIFS Server database, execute:

```
$ NET GROUPMAP ADD NTGROUP=<CIFS Server group-name>-
UNIXGROUP=<OpenVMS resource-id-name> TYPE=DOMAIN
```

For example, to create DOMAINGROUP group account, execute

```
$ NET GROUPMAP ADD NTGROUP= DOMAINGROUP UNIXGROUP= DOMAINGROUP –
TYPE=DOMAIN
```

NOTE: Group names containing spaces must be enclosed in quotes. For example, “Account Team”.

4. Listing groups:

   To list all group accounts that exist in CIFS Server database including the mapped OpenVMS resource identifiers, enter the following command:

   ```
   $ NET GROUPMAP LIST
   ```

   To list group accounts based on group type, use the NET SAM LIST command.

   To list all built-in groups, execute:

   ```
   $ NET SAM LIST BUILTIN
   ```

   To list local groups, execute:

   ```
   $ NET SAM LIST LOCALGROUPS
   ```

   When CIFS Server is a PDC or BDC, to list domain groups, execute:

   ```
   $ NET SAM LIST GROUPS
   ```

   To list all group accounts (of all types), including their description, use the NET RPC GROUP LIST command. Note, however, that this command requires the user specify the credentials of an administrator account. For example:

   ```
   $ net rpc group list --user cifsadmin
   Password:
   ```

5. Deleting groups:

   Before deleting a group account, it is recommended to remove the group members using `$ NET RPC GROUP DELMEM` command and then remove the group account from CIFS Server database.

   Use the `NET RPC GROUP DELETE` command to remove a group account from the CIFS Server database.

NOTE: This command requires the user specific credentials of an administrator account.

For example:

```
$ net rpc group delete GROUP1 --user cifsadmin
Password:
```

OR

Use the `NET GROUPMAP DELETE` command to remove a group account from the CIFS Server database. For example:

```
$ net groupmap delete ntgroup=GROUP1
```

6. Adding group members:

   To add group members, use the `NET RPC GROUP ADDMEM` command.

NOTE: This command requires the user specific credentials of an administrator account.

For example, to add group PLAYERS in domain PIANODOM to the CIFS Server group CIFSUSERS, execute:

```
$ net rpc group addmem cifsusers pianodom\players --user cifsadmin
Password:
```

7. Deleting group members:

   To remove members from a group, use the `NET RPC GROUP DELMEM` command.

NOTE: This command requires the user specific credentials of an administrator account.

For example, to remove group PLAYERS in the PIANODOM domain from the CIFS Server group CIFSUSERS, execute:

```
$ net rpc group delmem cifsusers pianodom\players --user cifsadmin
Password:
```

8. Listing group members:

   To list group members, use the NET RPC GROUP MEMBERS command. Note, this command requires the user specify credentials of an administrator account. For example, to list members of the group CIFSUSERS, execute:

```
$ net rpc group members cifsusers --user cifsadmin
Password:
```

8.4 Managing account policies

The HP CIFS Server account policies can be managed using the CIFS Server management utility, `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` or by using NET command line utility. Section 8.4.1 (page 118)describes how to use the `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` utility to set and list the CIFS Server account policies while the Section 8.4.2 (page 121)describes how to use the NET command to achieve the same.

8.4.1 Managing account policies using CIFS Server management utility

The `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` utility can be used to list and set account policies in the HP CIFS Server database using menu options.

To invoke the CIFS Server management utility:

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

OR

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

This displays the HP OpenVMS CIFS Server Management Main Menu. Use option 4, “Manage account policies”, to display the account policies management menu.

```
HP CIFS Server Account Policies Management Menu

                 1  - List Account policies
                 2  - Set Account policies
                [E] - Exit
Enter account policies menu option:
```

8.4.1.1 Listing account policies

Use option 1, “List Account policies”, to list CIFS Server account policies. An output similar to the following is displayed:

```
 Account Policy for domain "PIANODOM":

Account policy "min password length" value is: 5
Account policy "password history" value is: 0
Account policy "user must logon to change password" value is: 0
Account policy "maximum password age" value is: -1
Account policy "minimum password age" value is: 0
Account policy "lockout duration" value is: 30
Account policy "reset count minutes" value is: 30
Account policy "bad lockout attempt" value is: 3
Account policy "disconnect time" value is: -1
Account policy "refuse machine password change" value is: 0

Press Enter to continue:
```

8.4.1.2 Setting account policies

Use option 1, “Set Account policies”, to set account policies in the CIFS Server database. An output similar to the following is displayed:

```
    HP CIFS Server Set Account Policies Management Menu

                 1  - Minimum password length
                 2  - Password history
                 3  - User must logon to change password
                 4  - Maximum password age
                 5  - Minimum password age
                 6  - Lockout duration
                 7  - Reset count minutes
                 8  - Bad lockout attempt
                 9  - Disconnect time
                10 - Refuse machine password change
                [E] - Exit
Enter set account policies menu option:
```

The remainder of this section details each of the options available when setting an account policy. To change a parameter setting, specify its option number in the “Enter set account policies menu option” prompt.

8.4.1.2.1 Minimum password length

Minimum password length sets the minimum length of a password. This policy specifies the minimum number of characters required in the password and can be from 0 to 4294967295. A value 0 means that a blank password is permitted.

8.4.1.2.2 Password history

Password history sets the number of new passwords that must be used by a user before an old password can be reused. The value specifies the number of passwords to maintain in the password history, from 0 to 4294967295.

8.4.1.2.3 User must logon to change password

By enabling "User must logon to change password" policy, a user is forced to logon to the CIFS Server before changing the password. In case of user account's password expiry, only an administrator can change the password for the user account. A value of 0 (zero) disables this account policy and a value of 2 or more, enables this policy.

8.4.1.2.4 Maximum password age

Maximum password age sets the maximum number of seconds a user's password can be used before the server requires the user to change it. The value can be from 0 to 4294967295.

8.4.1.2.5 Minimum password age

Minimum password age sets the minimum number of seconds a user's password must be used before a user can change it. CIFS Server does not allow immediate password change if a password history value is set. The value can be from 0 to 4294967295.

8.4.1.2.6 Lockout duration

Lockout duration specifies the number of minutes before a locked out account is automatically unlocked. The value can be from 0 to 4294967295.

8.4.1.2.7 Reset count minutes

Reset count minutes specifies the number of minutes from the most recent failed login attempt before the failed login count is reset to zero. For example, if the "reset count minutes" is set to 30 minutes, then thirty minutes after the most recent failed login attempt, the failed logon count is reset to zero. The value can be from 0 to 4294967295.

8.4.1.2.8 Bad lockout attempt

Bad lockout attempt specifies the failed logon count. The Account is locked out after the specified number of failed attempts. The value can be from 0 to 4294967295. A value of 0 (zero) disables this policy and a value greater than 0 (zero) enables this policy.

8.4.1.2.9 Disconnect time

Disconnect time controls whether a user's connections to any server in the domain are forcibly disconnected when the user account exceeds its logon hours. This interacts with the logon hours defined for a user account. The value can be from 0 to 4294967295. A value of 0 (zero) indicates that a user is disconnected and thus the policy is enabled. To disable this policy, set the value to 4294967295.

8.4.1.2.10 Refuse machine password change

Refuse machine password change, if set, will disallow changing machine account password. A value of 0 (zero) indicates that the policy is disabled and a value higher than 0 indicates that the policy is enabled.

8.4.2 Managing account policies using the NET command

CIFS Server supports following account policies:

```
min password length
password history
user must logon to change password
maximum password age
minimum password age
lockout duration
reset count minutes
bad lockout attempt
disconnect time
refuse machine password change
```

For a description of these account policies, see Section 8.4.1.2 (page 119).

To view the value of any account policy:

```
$ NET SAM POLICY SHOW "<account policy>"
```

For example, to view the value of “min password length” account policy:

```
$ NET SAM POLICY SHOW "min password length”
```

To change the value of any account policy,:

```
$ NET SAM POLICY SET "<account policy>"<value>
```

For example, to change the value of “password history” account policy:

```
$ NET SAM POLICY SET "password history” 3
```

8.5 Managing trust relationships

When the CIFS Server role is PDC in a CIFS domain, the HP CIFS Server can establish trust relationships with other domains (foreign domains). A trust relationship is a link between two domains, where one domain honors the users of another domain, trusting the logon authentications performed by that other domain for its own users. User accounts and global groups defined in a trusted domain can be granted rights, resource permissions, and local group memberships in a trusting domain and its member computers, even though those accounts do not exist in the trusting domain's security database. When trust relationships are properly established between all the domains in a network, they allow a user to have only one user account and one password in one domain, yet have access to the resources anywhere in the network.

Establishing a trust relationship requires two steps in two different domains: first one domain must permit a second domain to trust it, and then the second domain must be set to trust the first domain. Establishing a two-way trust relationship (where each domain trusts the other) requires that both steps be performed in both domains.

Trust relationships can be managed using the CIFS Server management utility `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` or using the NET command utility. Section 8.5.1 describes how to use `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` to view and establish trust relationships while the section Section 8.5.2 (page 124) describes how to use the NET command to achieve the same.

8.5.1 Managing trusts using the CIFS Server Management utility

The SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM utility can be used to view and establish trust relationships using menu options.

To invoke the CIFS Server management utility:

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

OR

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

This displays the HP OpenVMS CIFS Server Management Main Menu. Use option 5, “Manage trusts”, to display the trust relationship management menu.

```
        HP CIFS Server Trust Relationship Management Menu

                 1  - List trusts
                 2  - Add in-coming trust
                 3  - Remove in-coming trust
                 4  - Add out-going trust
                 5  - Remove out-going trust
                 6  - Help
                [E] - Exit
Enter item number:
```

The remainder of this section details each of the options available in the trust relationship management menu. To select a parameter setting, specify its option number in the “Enter item number:” prompt.

8.5.1.1 Listing trust relationships

The option “list trusts” will list the trusting (in-coming) and trusted (out-going) relationships that currently exist in the CIFS Server database. The display is similar to the following output:

```
Trusted domains list:

CIFSDOM             S-1-5-21-160935111-2493731623-2036278074

Trusting domains list:

CIFSDOM             S-1-5-21-3707034097-1477131719-1377839329

Press Enter to continue:
```

8.5.1.2 Adding in-coming trust

To allow users belonging to the CIFS domain to access resources in the foreign domain, the CIFS domain must be allowed to trust the foreign domain. This is a two-step process:

1. On the CIFS domain, create an in-coming trust account (trusting account) for the foreign domain and note down the specified trust account password. The option “Add in-coming trust” in the “trust relationship management menu” can be used for adding the in-coming trust account.

2. On the foreign domain, create an out-going trust (trusted account) to the CIFS domain. During this process, you must supply the trust account password that was specified in step 1.

   While adding the in-coming trust account using the utility, it prompts you for:

   - Foreign domain name for which the in-coming trust account must be added.
   - Credentials of an administrator user of CIFS domain.
   - OpenVMS user account group id if “idmap uid” and “idmap gid” parameters are missing from the configuration file SMB.CONF.
   - Trust account password. You must remember the trust account password that you specify as it is required during step 2 process execution on the foreign domain.

   To successfully add the in-coming trust account in CIFS Server database, the utility adds a corresponding OpenVMS account name in the SYSUAF database if it doesn’t exist. An OpenVMS account name for the foreign domain is added in the SYSUAF database only after suffixing the foreign domain with a dollar sign ($). For example, if the foreign domain name is WINDOM, then the OpenVMS account name added in the SYSUAF database will be WINDOM$.

NOTE:

- If the foreign domain is a Windows domain, see Section 8.5.2.9 (page 126)for adding an out-going or two-way trust between the CIFS domain and a Windows domain to complete step 2 process.
- Currently, the utility is limited to creating incoming trust accounts for domain names less than 12 characters, due to OpenVMS account name restrictions.

8.5.1.3 Removing in-coming trust

The option “Remove in-coming trust” can be used to delete an in-coming trust account. Deleting the in-coming trust for a domain will remove the ability for users from the CIFS domain to access resources in the foreign domain. To successfully delete the in-coming trust account, the utility prompts you for credentials of an administrator user of CIFS domain.

8.5.1.4 Adding out-going trust

To allow users belonging to the foreign domain to access resources in the CIFS domain, a trust must be established with the foreign domain. This is a two-step process:

1. On the foreign domain, create an in-coming trust account for CIFS domain and note down the specified trust account password.
2. On the CIFS domain, create an out-going trust (trusted account) to the foreign domain. The option “Add out-going trust” can be used for adding an out-going trust account. The out-going trust can be successfully established with foreign domain only after the in-coming trust account for the CIFS domain is created in the foreign domain (as noted in step 1 above).

While adding the out-going trust account using the utility, it will prompt you for:

- Foreign domain name for which the out-going trust must be established
- Trust account password. This must be the same password specified when the in-coming trust account for the CIFS domain was created in the foreign domain (in step 1).
- Fully Qualified Domain Name (FQDN) of the PDC emulator of the foreign domain. If the PDC emulator cannot be reached using the FQDN, the utility prompts for the IP address of the PDC emulator.

NOTE: If the foreign domain is a Windows domain, Section 8.5.2.9 (page 126) for adding an in-coming or two-way trust between the CIFS domain and Windows domain to complete step 1 process.

8.5.1.5 Removing out-going trust

The option “Remove out-going trust” can be used to remove out-going trust relationship. By removing the out-going trust relationship for a domain, the ability for foreign domain users to access resources in the CIFS domain is removed. To successfully remove the out-going trust, the utility will prompt for credentials of an administrator user of CIFS domain, as well as the out-going trust name (foreign domain) to remove.

8.5.2 Managing trusts using the NET command

The command “$ NET RPC TRUSTDOM” can be used to manually view, add and remove trust relationships.

8.5.2.1 Listing trust relationships

The syntax for listing existing trust relationships in the CIFS Server database is,

```
$ NET RPC TRUSTDOM LIST "-U" <CIFS domain administrator user>
Password: <CIFS domain administrator user password>
```

For example, to list trust relationships using the account CIFSADMIN, execute:

```
$ NET RPC TRUSTDOM LIST "-U" CIFSADMIN
Password: <password-of-cifsadmin-account>
```

8.5.2.2 Adding in-coming trust

The method for adding in-coming trust (trusting account) for a foreign domain on the CIFS Server PDC is described below.

1. Create an OpenVMS account whose name matches the name of the foreign domain for which you would like to create an in-coming trust account (trusting account) and append a dollar sign ($) to it (required).

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

   ```
   $ MC AUTHORIZE COPY SAMBA$TMPLT TRUSTINGDOM$ /UIC=[1000,1]
   ```

2. Execute NET command to add in-coming trust account. The syntax is:

   ```
   $ NET RPC TRUSTDOM ADD "<foreign-domain-name>"
   "<trust-account-password>"-
   "-U"<CIFS domain administrator user>
   Password: <CIFS domain administrator user password>
   ```

   For example, if the NetBIOS name of the foreign domain is trustingdom and CIFS domain administrator username is CIFSADMIN, execute the command:

   ```
   $ NET RPC TRUSTDOM ADD TRUSTINGDOM "TrustPwd1" "-U" CIFSADMIN
   Password: <password-of-cifsadmin-account>
   ```

NOTE:

- To complete the trust relationship, on the foreign domain you must add an out-going trust (trusted domain account) to the CIFS domain (for example, on TRUSTINGDOM domain) using the same trust account password that you specified in the step 2 above.
- If the foreign domain is a Windows domain, Section 8.5.2.9 (page 126) for adding an out-going or two-way trust between the CIFS domain and Windows domain.

8.5.2.3 Removing in-coming trust

The syntax to remove the in-coming trust account (trusting account) for a foreign domain is:

```
$ NET RPC TRUSTDOM DEL <foreign-domain-name>"-U" <CIFS domain
administrator user>
Password: <CIFS domain administrator user password>
```

For example, to remove in-coming trust account for a foreign domain, trustingdom and if the CIFS domain administrator username is CIFSADMIN, execute the command:

```
$ NET RPC TRUSTDOM DEL TRUSTINGDOM "-U" CIFSADMIN
Password: <password-of-cifsadmin-account>
```

8.5.2.4 Adding out-going trust

After adding an in-coming trust account (trusting account) for the CIFS domain on a foreign domain, an out-going trust (trusted domain relationship) must be established on the CIFS domain for a foreign domain to complete the trust relationship. This involves setting the "idmap domains" parameter value if required apart from using NET RPC TRUSTDOM command to establish out-going trust relationship.

8.5.2.5 Setting idmap domains parameter

You can set the idmap domains parameter value to allow trusted domain users to access resources on the CIFS Server PDC. This is optional and needs to be set only if the CIFS Server uses WINBIND's automatic mapping for creation and mapping of OpenVMS user accounts and resource identifiers. The idmap domains parameter defines a list of domains, each of which has a separately configured backend for managing the WINBIND's SID/UID/GID tables. The list includes short domain name for the WINBIND's primary or collection of trusted domains. There is no default value for the idmap domains parameter.

For example, if adding an out-going trust on the CIFS Server to the foreign domain WINDOM, set:

```
idmap domains = WINDOM
idmap alloc backend = tdb
```

Multiple domain names can be specified for idmap domains by separating the domain names using a comma.

8.5.2.6 Updating LMHOSTS. File

Determine the name resolution method used by the CIFS Server PDC on a CIFS domain and the PDC emulator on a foreign domain to which the out-going trust relationship must be established. If they do not use WINS Server for resolving names, update the samba$root:[lib]lmhosts. file on the CIFS Server PDC with entries for the foreign domain.

The following example shows the lmhosts. file entries required on the CIFS Server PDC for the Windows PDC Emulator named WINPDC at IP address 10.20.20.40 in domain WINDOM:

```
10.20.20.40 WINPDC
```

```
10.20.20.40 WINDOM#1B
10.20.20.40 WINDOM#1C
```

8.5.2.7 Establishing out-going trust

The syntax for establishing out-going trust on the CIFS Server to a foreign domain is:

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

The TRUST-PASSWORD must be same as the trust account password supplied while adding the in-coming trust account (trusting account) for the CIFS domain on a foreign domain.

NOTE:

- Before adding out-going trust relationship to the foreign domain on a CIFS Server, an in-coming trust account (trusting account) must have been added for the CIFS domain on the foreign domain.
- If the foreign domain is a Windows domain, see Section 8.5.2.9 (page 126) for adding an in-coming or two-way trust between the CIFS domain and Windows domain.

8.5.2.8 Removing out-going trust

To remove an out-going trust relationship to the foreign domain on a CIFS Server, use:

```
$ NET RPC TRUSTDOM REVOKE <foreign-domain-name> "-U" <CIFS domain
administrator user>
Password: <CIFS domain administrator user password>
```

If you have logged into the OpenVMS system using a fully privileged OpenVMS account (for example, SYSTEM), following command can be used:

```
$ NET RPC TRUSTDOM REVOKE <foreign-domain-name>
```

8.5.2.9 Establishing trusts in the Windows domain

To complete in-coming (trusting) and out-going (trusted) relationships between a CIFS domain and Windows domain, it is necessary to establish two-way (in-coming and out-going) trust relationships on the CIFS domain and the Windows domain. The Section 8.5.1 (page 122) and Section 8.5.2 (page 124) described how to add in-coming and out-going trusts on an HP CIFS Server either through automated steps or by manually executing commands. This section describes how to add in-coming and out-going trusts on a Windows system separately as well as how to establish two-way trust relationships.

8.5.2.9.1 Updating LMHOSTS. File

Before adding any type of trust relationship between a CIFS domain and Windows domain, you must determine the name resolution method used by the CIFS Server PDC in CIFS domain and the PDC emulator of a Windows domain. If the PDC emulator of a Windows domain cannot resolve the PDC name of CIFS domain using WINS Server, lmhosts file on the Windows PDC emulator must be updated with entries for CIFS Server PDC of CIFS domain.

The following example shows the lmhosts. file entries required on the Windows PDC emulator for the CIFS Server PDC named PIANO at IP address 10.20.30.40 in the CIFS domain PIANODOM:

```
10.20.30.40 piano #PRE #DOM:pianodom
10.20.30.40 "pianodom       \0x1b" #PRE
10.20.30.40 "pianodom       \0x1c" #PRE
```

NOTE: There must be exactly 20 characters between the quotes in the above entries. The domain name must be space-padded to 15 characters, followed by \0x1b or \0x1c.

8.5.2.9.2 Establishing two-way trust

To establish both the in-coming and out-going trusts on the Windows domain, execute the following steps on the PDC emulator of Windows domain:

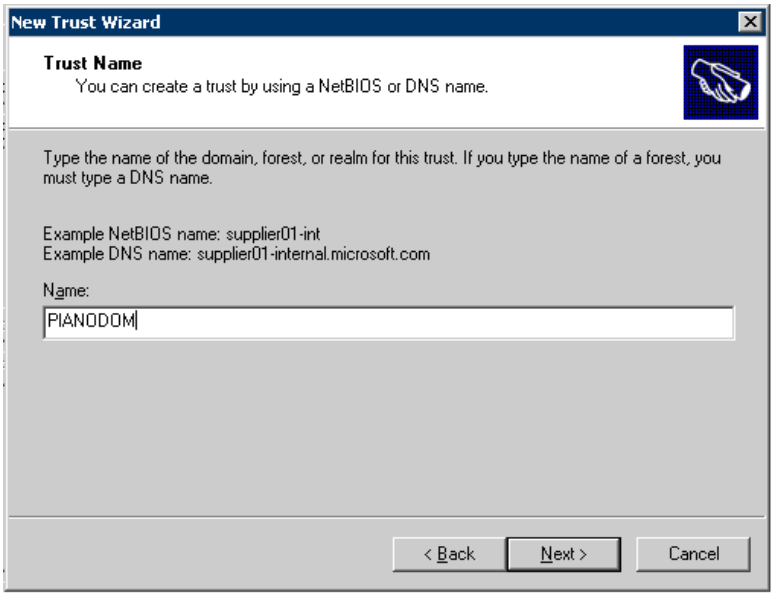
1. Open **New-trust Wizard**.

   To do this, select the Windows domain name from the **Active Directory Domains and Trusts** applet on a Windows PDC emulator, right-click **Properties**. From the **Properties** dialog box displayed for the Windows domain, click **New Trust**.

   When the **New Trust Wizard** , click **Next** and to open the **Trust Name** window of **New Trust** Wizard.

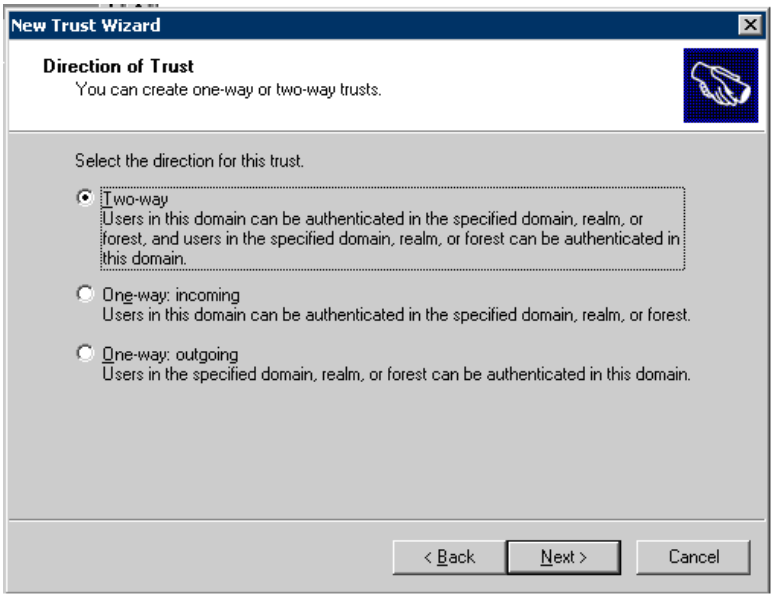
2. Under the **Trust Name**, type the NetBIOS name of the CIFS domain. For example, if the CIFS domain name is pianodom, type PIANODOM as shown and click **Next**.

Figure 8-1 Entering CIFS domain name



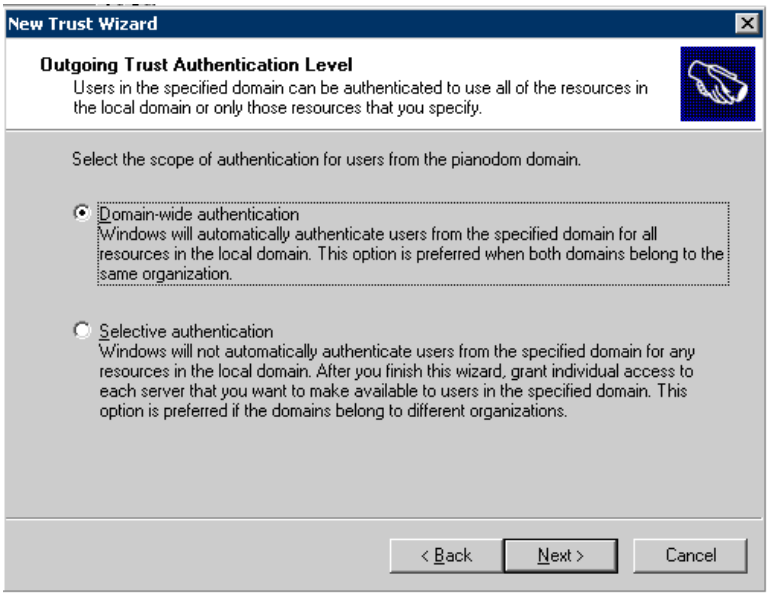
3. In the **Direction of Trust** window, select **two-way** to establish both the in-coming and out-going trust and click **Next**.

Figure 8-2 Selecting direction for the trust



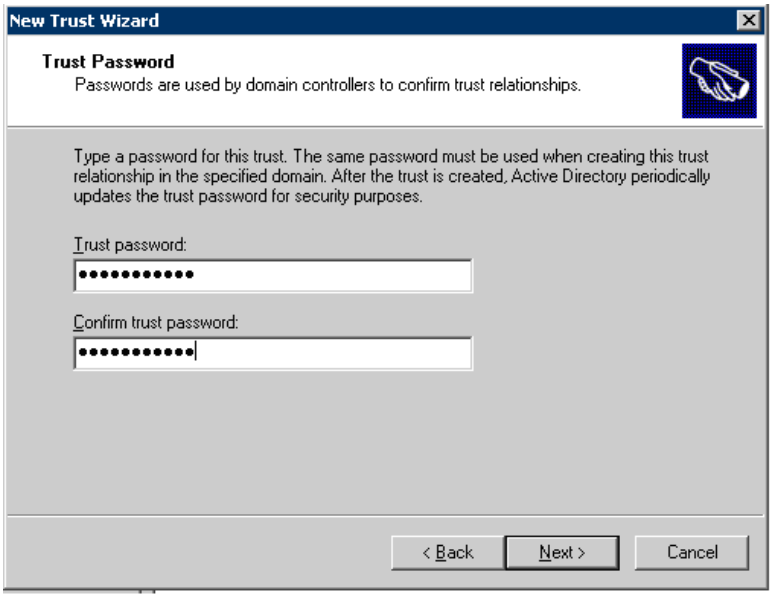
4. In the **Out-going Trust Authentication Level** window, select the option **Domain-wide authentication** and click **Next**.

Figure 8-3 Selecting authentication level



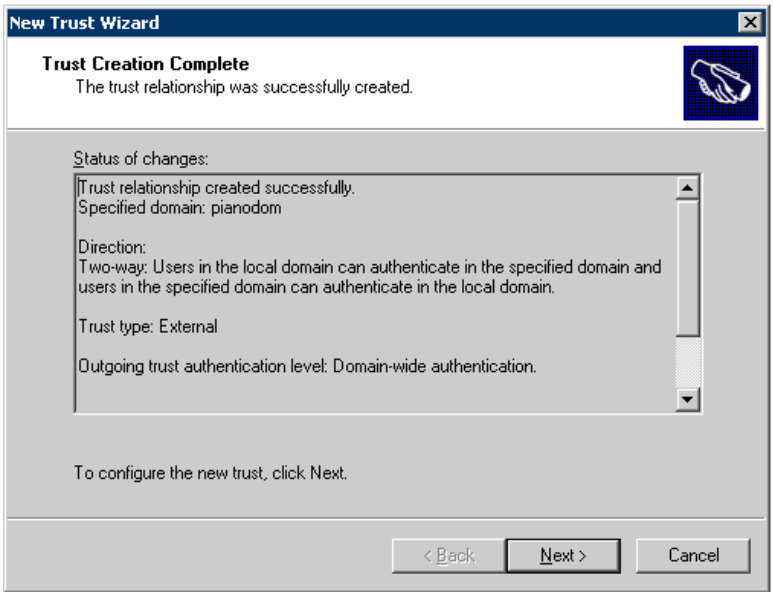
5. In the **Trust Password** window of **New Trust Wizard**, type the trust account password. Make a note of the password as it is required while adding in-coming and out-going trusts on the CIFS Server PDC of CIFS domain. Click **Next** to display **Trust Selections Complete** window.

Figure 8-4 Advanced Security Settings window



6. The **Trust Selections Complete** windows shows information about the type of trust being added and it says it is ready to create the trust. Click **Next** in this window. The **Trust Creation Complete** window appears.

Figure 8-5 Advanced Security Settings window



7. The **Trust Creation Complete** window is displayed after successfully creating the required trust. Click **Next**.
8. In the **Confirm out-going trust** window, select the option “No, do not confirm the out-going trust” and click **Next**.
9. In the **Verify in-coming trust** window, “No, do not confirm the in-coming trust” and click **Next**.
10. In the **Complete the New Trust Wizard**, click **Finish** to close the Wizard.
11. To complete the trust relationships, add in-coming and out-going trusts on the CIFS Server PDC of CIFS domain by specifying the same trust password that was entered in **Trust Password** window of **New Trust Wizard** in step 5.

8.5.2.9.3 Establishing in-coming trust

You may only want to allow one-way trust between CIFS domain and Windows domain. For allowing users in the CIFS domain to access resources in the Windows domain, you can establish in-coming trust for the CIFS domain on the Windows domain. The steps to be followed for establishing in-coming trust on the PDC emulator of Windows domain are:

1. Open **New Trust Wizard**.

   To do this, select the Windows domain name from the **Active Directory Domains and Trusts** applet on a Windows PDC emulator, right-click **Properties**. From the **Properties** dialog box displayed for the Windows domain, click **New Trust**. In the displayed **New Trust Wizard**, click **Next** to display **Trust Name** window of **New Trust Wizard**.

2. Under the **Trust Name**, type the NetBIOS name of the CIFS domain and click **Next**. For example, if the CIFS domain name is pianodom, type PIANODOM.
3. In the **Direction of Trust** window, select **one-way: incoming** to establish in-coming trust and click **Next**.
4. In the **Trust Password** window of **New Trust Wizard**, type the trust account password and note it down as it required while adding out-going trust on the CIFS Server PDC of CIFS domain. Then, click **Next**.
5. The **Trust Selections Complete** window shows information about the type trust being added. Click **Next** in this window which will then display **Trust Creation Complete** window.
6. The **Trust Creation Complete** window is displayed after successfully creating the required trust. Click **Next**.
7. In the **Verify in-coming trust**, select "No, do not confirm the in-coming trust" and click **Next**.
8. In the **Complete the New Trust Wizard**, click **Finish** to close the Wizard.

8.5.2.9.4 Establishing in-coming trust

You may only want to allow one-way trust between CIFS domain and Windows domain. For allowing users in the CIFS domain to access resources in the Windows domain, you can establish in-coming trust for the CIFS domain on the Windows domain. The steps to be followed for establishing in-coming trust on the PDC emulator of Windows domain are:

1. Open **New Trust Wizard**.

   To do this, select the Windows domain name from the **Active Directory Domains and Trusts** applet on a Windows PDC emulator, right-click **Properties**. From the **Properties** dialog box displayed for the Windows domain, click **New Trust**. In the displayed **New Trust Wizard**, click **Next** to display **Trust Name** window of **New Trust Wizard**.

2. Under the **Trust Name**, type the NetBIOS name of the CIFS domain and click **Next**. For example, if the CIFS domain name is pianodom, type PIANODOM.
3. In the **Direction of Trust** window, select **one-way: incoming** to establish in-coming trust and click **Next**.
4. In the **Trust Password** window of **New Trust Wizard**, type the trust account password and note it down as it required while adding out-going trust on the CIFS Server PDC of CIFS domain. Then, click **Next**.
5. The **Trust Selections Complete** window shows information about the type trust being added. Click **Next** in this window which will then display **Trust Creation Complete** window.
6. The **Trust Creation Complete** window is displayed after successfully creating the required trust. Click **Next**.
7. In the **Verify in-coming trust**, select "No, do not confirm the in-coming trust" and click **Next**.
8. In the **Complete the New Trust Wizard**, click **Finish** to close the Wizard.

9. To complete the trust relationship, add out-going trust on the CIFS Server PDC of CIFS domain by specifying the same trust password that you entered in “Trust Password” window of “New Trust Wizard” in step 4.

8.5.2.9.5 Establishing out-going trust

You may only want to allow one-way trust between CIFS domain and Windows domain. For allowing users in the windows domain to access resources in the CIFS domain, you can establish out-going trust to the CIFS domain on the Windows domain. Before establishing out-going trust on the Windows domain, add in-coming trust for the Windows domain on the CIFS Server PDC of CIFS domain and note down the trust password. To complete the trust relationship, add out-going trust to the CIFS domain on a Windows domain.

To establish an out-going trust on the PDC emulator of Windows domain are:

1. Open **New Trust Wizard**.

   Select the Windows domain name from the **Active Directory Domains and Trusts** applet on a Windows PDC emulator, right-click **Properties**. From the **Properties** dialog box displayed for the Windows domain, click **New Trust**. In the displayed **New Trust Wizard**, click **Next** to display **Trust Name** window of **New Trust Wizard**.
2. Under the **Trust Name**, type the NetBIOS name of the CIFS domain and click **Next**. For example, if the CIFS domain name is pianodom, type PIANODOM.
3. In the **Direction of Trust** window, select **one-way: outgoing** to establish in-coming trust and click **Next**.
4. In the **Out-going Trust Authentication Level** window, select **Domain-wide authentication** and click **Next**.
5. In the **Trust Password** dialog box of **New Trust Wizard**, type the trust account password and note it down as it required while adding out-going trust on the CIFS Server PDC of CIFS domain. Then, click **Next**.
6. The **Trust Selections Complete** window shows information about the type trust being added. Click **Next**

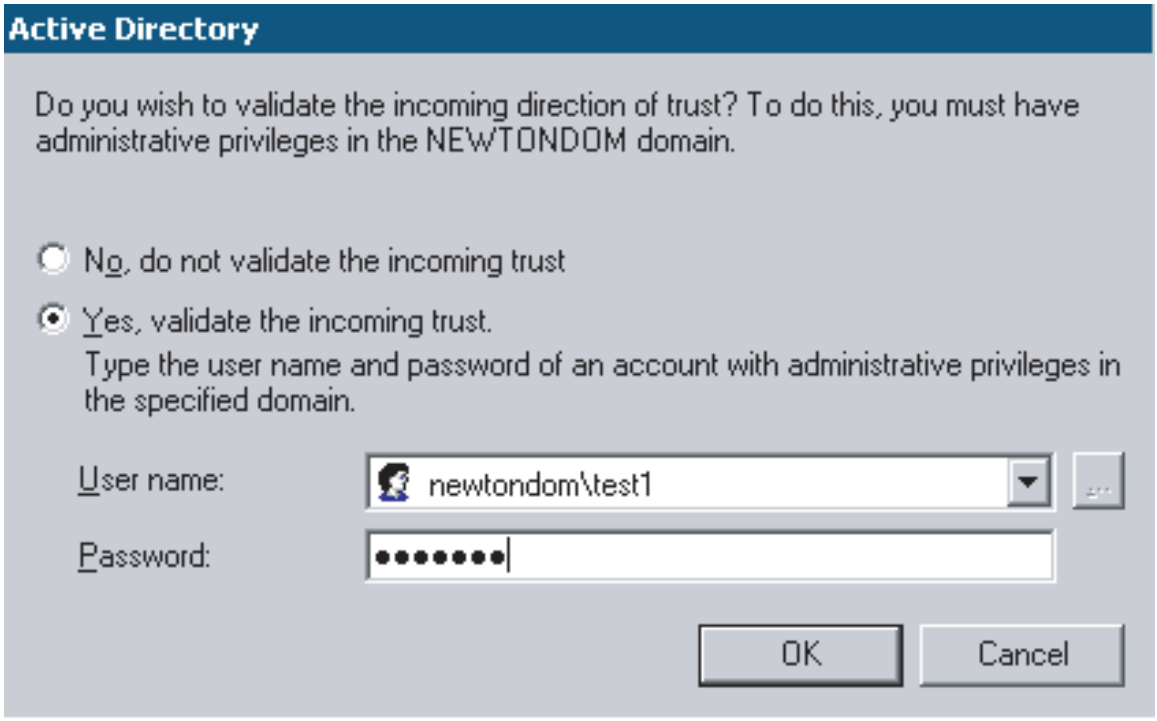
   The **Trust Creation Complete** window is appears.
7. Click **Next**. The Confirm out-going trust dialog box appears.
8. Select “No, do not confirm the out-going trust” and click **Next**.
9. In the **Complete the New Trust Wizard**, click **Finish**.

8.5.3 Validating trust relationships

The steps for validating the trust relationships on a Windows PDC are:

1. Select the Windows domain name from the **Active Directory Domains and Trusts** applet, right-click **Properties**.
2. From the **Properties** dialog box displayed for the Windows domain, select the CIFS domain name to which the trust relationship must be validated and click **Properties**.
3. From the **Properties** dialog box displayed for the CIFS domain, click **Validate**.
4. In the **Active Directory** window, enter the HP CIFS User name and `Password`. Click **OK**.

Figure 8-6 Active Directory



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

9 Managing shares

This chapter discusses the following topics:

- “Managing shares” (page 133)
- “Managing printers” (page 141)

Share management provides information on managing disk (directory) and print shares, while the printer management deals with adding print queues, uploading print driver files and adding printers on clients. Chapter 10 (page 147) explains how to establish security on directory and print shares.

9.1 Managing shares

This section provides information on managing disk (Directory) and print shares using the utility `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` or by manually editing the HP CIFS Server configuration file. The methods explained in this section allow you to list, add, modify and delete disk and print shares.

9.1.1 Automated CIFS share management

The `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` utility can be used for listing, adding, modifying or deleting shares from the HP CIFS Server configuration file `SMB.CONF`.

NOTE: The Modify and Delete share operations are usable only when the share definitions are present in the main CIFS Server configuration file, `SMB.CONF`. For a share definition that is present in any of the INCLUDE files, the `SAMBA$ROOT:[BIN]SAMBA$MANAGE_CIFS.COM` utility cannot correctly perform the Modify and Delete operations on that share.

To invoke the HP CIFS Server management utility, execute the following command:

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

OR

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

This displays an HP OpenVMS CIFS Server Management Main Menu. Select option 1, “Manage Shares” to display the HP CIFS Server Share Management Menu:

```
HP CIFS Server Share Management Menu

        Share Management Options:

                 1  - List shares
                 2  - List a share detail
                 3  - Add share
                 4  - Modify share
                 5  - Delete share
                [E] - Exit
Enter share management option:
```

9.1.1.1 Listing shares

Use option 1, “List Shares”, to list all directory and print shares that are not hidden (“browseable=yes”). For example, when you specify “1” at the “Enter share management option:” prompt, the output is similar to:

```
Enumerating shares available through the CIFS Server PIANO.
  Please wait...

Enumerating shared resources (exports) on remote server:


Share name   Type     Description
----------   ----     -----------
projects     Disk     Project Share
DCPS_PRINTER Print    Printer share
udfprint     Print
IPC$         IPC      IPC Service (Samba 3.0.28a running on piano (OpenVMS))

Press Enter to continue:
```

9.1.1.2 Listing a share detail

Use option 2, "List a share detail" to view the configuration parameters and their values set for the specified share.

```
This option displays CIFS Server configuration parameters and
   their values set for the specified share

Enter the share name: projects

Samba configuration details for the share:
[projects]
        comment = Project Share
        path = dka0:[projects]
        read only = No
        vms rms format = stream

Press Enter to continue:
```

This option can be used to view details of hidden shares ("browseable=no") as well.

9.1.1.3 Adding a share

Use the `SAMBA$MANAGE_CIFS.COM` utility to add a share and to modify any of the following share configuration parameters:

- path
- comment
- browseable
- read only
- valid users
- admin users
- guest ok
- inherit owner
- vms rms format
- vms inherit rms protections
- force create mode
- create mask
- directory create mask
- force directory create mode

- directory security mask
- force directory security mode
- store dos attributes
- printable
- printer name
- use client driver

Use option 3, “Add share”, to add a share definition to the `SMB.CONF` configuration file. The utility prompts for the share type:

```
A share can be of 2 types:
   - Disk, for sharing directories and files on the disk
   - Printer, for sharing printers

  For adding a disk share, specify the share type as D
  and for printer share, specify the share type as P.

Enter the share type [D/P]: [D]
```

To add a disk share, choose the default option “D” or to add a print share, enter “P”. If the disk share option is selected, the following menu is displayed:

```
HP CIFS Server Menu for Adding a Disk Share

         1. Share name (*):
         2. Share path (*):
         3. Share comment:
         4. Valid users:
         5. Admin users:
         6. Hide share: no
         7. Enable guest access: no
         8. Inherit owner: no
         9. RMS file format: stream
        10. Allow write access: yes
        11. Inherit RMS protection: no
        12. Store DOS attributes: no

        * - required field

Enter item number or press Enter to accept current values [Done]:
```

The “Share name” and “Share path” are mandatory fields while all other fields are optional. After you specify “Done” to accept the values displayed, if option “11. Inherit RMS protection” is “no”, a menu for modifying the mask and mode parameters are displayed:

```
HP CIFS Server Share Section Mask and Mode Parameters Menu

                1. Directory security mask: 07777
                2. Directory force security mode: 0
                3. File create mask: 07777
                4. File force create mode: 0
                5. Directory create mask: 07777
                6. Directory force create mode: 0
                H. Display help text
Enter item number or press Enter to accept current values [Done]:
```

When adding a print share, the following menu is displayed:

```
HP CIFS Server Menu for Adding a Print Share

         1. Share name (*):
         2. Share path (*): SAMBA$ROOT:[SPOOL]
         3. Share comment:
         4. Valid users:
         5. Admin users:
         6. Hide share: no
         7. Enable guest access: no
         8. Use client drivers: no

        * - required field

Enter item number or press Enter to accept current values [Done]:
```

The rest of this section describes each of the options available when adding a directory or print share. To change a parameter setting, specify its option number in the “Enter item number” prompt. To select and modify any of the options, specify the item number at the prompt for entering the item number in the add share menu.

9.1.1.3.1 Share name

Share name specifies a name that can be used to identify and connect to the shared resource. While adding a disk share, the shared resource must be a directory on the disk. When adding a printer share, the share name must be the name of an OpenVMS printer queue. The share name maps to [<share section name>] in the HP CIFS Server configuration file.

9.1.1.3.2 Share path

Share path specifies a directory to which the user of the share is to be given access. For example, if you want to share the directory `DISK$DATA:[PROJECTS]`, specify `DISK$DATA:[PROJECTS]` when prompted for the share path.

In the case of printable shares, CIFS Server will spool print data in the share path directory before submitting it to the print queue for printing. For printable shares, you can select the default directory `SAMBA$ROOT:[SPOOL]` as share path. This option maps to the share section Samba configuration parameter “path”.

The share path can be entered in the UNIX path format or the OpenVMS path format. A valid share path must be entered because the utility cannot create the share path.

9.1.1.3.3 Share comment

Share comment specifies a string of characters for providing descriptive information about the shared resource. This option maps to the share section parameter “comment”.

9.1.1.3.4 Valid users

Valid users are a list of users that must be allowed to access the shared resource. In case of print shares, “valid users” are a list of users that are allowed to print to that print share. This option maps to the share section parameter “valid users”.

When “valid users” value is null (the default), then any authenticated user can access the share provided the security settings on the share path grants them access.

To specify valid users, the following guidelines must be taken into account:

- While specifying users or groups belonging to a trusted domain or to the domain where CIFS Server is a Member Server, you must prefix the user or group name with the domain

name (separated by a backslash. For example, to specify user ANITA in domain CIFSDOM, specify: CIFSDOM\ANITA

- To specify a group name, you must prefix it with the "@" character. For example, to specify all the users belonging to the group ENGPROJECT as valid users, you must enter "@ENGPROJECT".
- The utility allows you to enter multiple names as valid users. It will continue to prompt for "valid users" until no name is entered.

9.1.1.3.5 Admin users

Admin users are a list of users who will be granted administrative privileges to all the objects in a share. The users identified as admin users will have all the privileges of a fully privileged OpenVMS user while accessing any object in that share. An admin user of one share section cannot be an admin user of another share section unless the user has "admin users" privilege in both share sections. This option maps to the share section parameter "admin users".

To specify admin users, the following guidelines must be taken into account:

- While specifying users or groups belonging to a trusted domain or to the domain where CIFS Server is a Member Server, the user or group name must be prefixed by the domain name (separated by a backslash). For example, to specify user ANITA in domain CIFSDOM, enter: CIFSDOM\ANITA
- To specify a group name, you must prefix it with the "@" character. For example, to specify all the users belonging to the group SHAREADMIN as admin users, you must enter "@SHAREADMIN".
- The utility allows you to enter multiple names as admin users. It continues to prompt for "admin users" until no name is entered.

9.1.1.3.6 Hide share

A hidden share will not be seen in the list of available shares in a net view and in the Windows explorer browse list. Shares that point to a root directory on a disk can be hidden such that they do not appear in the Windows explorer browse list. For example, if you are sharing the directory DISK$DATA:[000000], you may want to hide this share so that it is not seen in the Windows explorer browse list. This option maps to the share section parameter "browseable".

9.1.1.3.7 Enable guest access

When guest access is enabled for a share, access to the share can be granted based on guest account privileges. Users connecting as a guest are mapped to the OpenVMS account designated as the "guest account" in the HP CIFS Server configuration file, (SAMBA$GUEST, by default). To allow guest users access to resources, set the appropriate protections on the objects.

It is useful to enable guest access for a print share so that any user connecting to the CIFS Server can print using the CIFS print share. Another instance, where you may want to enable guest access is when HP CIFS Server is configured as Standalone server with share security mode and you want to allow guest access to users so that they can connect to the share without specifying a password.

This option maps to the share section parameter "guest ok".

9.1.1.3.8 Inherit owner

When inherit owner is set to "yes", CIFS Server sets the owner of newly created objects to that of the parent directory. This option maps to the share section parameter "inherit owner" and it is applicable only to disk shares.

9.1.1.3.9 RMS file format

RMS file format specifies the OpenVMS RMS record format of files created in the shared directory. Irrespective of the record format specified, the created files are sequentially organized.

The record-format keyword can be one of the following:

Table 9-1 Record-format keyword

Record Format	Description
FIXED	Files created in the shared directory are RMS sequential files with fixed length 512 byte records.
STREAM	Files created in the shared directory are RMS Stream format files. This is the default.
STREAMLF	Files created in the shared directory are RMS Stream_LF format files.
UNDEFINED	Files created in the shared directory have no specific RMS format. The format is defined by the application writing the file.

The RMS file format option maps to the share section parameter “vms rms format” and it is applicable only to disk shares.

9.1.1.3.10 Enable write access

By default, all shares are read-only, regardless of file permissions. To allow users to create or modify files, write access must be enabled. This option maps to the share parameters “read-only” and “writeable”; it is applicable to disk shares only.

9.1.1.3.11 Inherit RMS protection

If this option is enabled, it causes HP CIFS Server to:

- Set the RMS protection of the newly created file/directory to that of parent directory.
- Ignore a DEFAULT_PROTECTION ACE, if present on the parent directory.
- Ignore the RMS protection mask specified by the SYSGEN parameter RMS_FILEPROT.
- Ignore the mask and mode parameter values specified for the share.

The Inherit RMS protection option maps to the share parameter “inherit vms rms protection” and is applicable only to disk shares.

9.1.1.3.12 Store DOS attributes

If this option is enabled, the HP CIFS Server attempts to read DOS attributes (SYSTEM, HIDDEN, ARCHIVE, or READ-ONLY) from an HP CIFS Server ACE existing on the object. When a client tries to set the DOS attributes, they are stored in an HP CIFS Server ACE that is present on the object. A new HP CIFS Server ACE that stores these attributes is applied on the object, if none exists. This option can be enabled if you plan to use DOS attributes. This option maps to the share section parameter “store dos attributes” and it is applicable only to disk shares.

9.1.1.3.13 Mask and Mode parameters

For information about various file and directory mask and mode parameters, which are applicable to disk shares, see Section 10.1.5 (page 150)

9.1.1.3.14 Use client drivers

When serving a printer to Windows clients without first uploading a valid printer driver on the CIFS Server, the client is required to install a local printer driver. From this point on, the client treats the printer as a local printer and not a network printer connection. Due to this, the OpenPrinterEx() calls issued by the non-privileged users fails, resulting in access denied error on the client. If this option is enabled for a printer, then any attempt to open the printer with the PRINTER_ACCESS_ADMINISTER right is mapped to PRINTER_ACCESS_USE instead enabling the OpenPrinterEx() call to succeed. This parameter MUST not be enabled on a print share which

has a valid print driver uploaded on to the CIFS server. This option maps to the share section parameter “use client drivers” and it is applicable only to print shares.

NOTE: Before adding a print share, the OpenVMS print queue must exist or be created. If the print queue name and print share name are not identical, a logical name must be used to link the two. The logical name must be the same name as the print share and must equate to the name of the OpenVMS print queue. For example, if an existing print queue is named HPLASERJET4100_PORTRAT, but the print share name is HP4100POR, define the following system logical name:

```
$ define/system HP4100PORT HPLASERJET4100_PORTRAIT
```

For steps to add a print queue, see Section 9.2.1 (page 141)

9.1.1.4 Modifying a share

Select option 4 to modify a share. The procedure prompts for the share name:

```
Enter the share name to modify:
```

Specify the name of the share to modify. For example, to modify a share “PROJECTS”, enter the share name as “PROJECTS”. When the share name is entered, it gathers current parameters for the share and identify the share type. For modifying a directory share, it displays the menu similar to the “HP CIFS Server Menu for Adding a Disk Share” described earlier. For modifying a print share, it displays a menu similar to the “HP CIFS Server Menu for Adding a Print Share” menu. The only difference between the add share and the modify share menu is that the modify share menu displays the current parameter values for each of the options. For example, if you are trying to modify “PROJECTS” share, the menu displayed is:

```
HP CIFS Server Menu for Modifying a Disk Share

         1. Share name (*): projects
         2. Share path (*): dka0:[projects]
         3. Share comment: project share
         4. Valid users:
         5. Admin users:
         6. Hide share: no
         7. Enable guest access: no
         8. Inherit owner: no
         9. RMS file format: stream
        10. Allow write access: yes
        11. Inherit RMS protection: no
        12. Store DOS attributes: no

        * - required field

Enter item number or press Enter to accept current values [Done]:
```

Any option may be modified except option 1, “Share name”.

9.1.1.5 Deleting a share

Select option 5 to delete a share. The procedure prompts for the share name:

```
Enter the share name to delete:
```

If the specified share name exists in the HP CIFS Server configuration file, `SMB.CONF`, the share name is removed.

9.1.2 Managing CIFS shares manually

9.1.2.1 Listing shares

To list the shares while HP CIFS Server is running, execute the following commands:

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
$ net rpc share --long --user=""%
```

To view the Samba configuration File details of a single share, execute the following commands:

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
$ testparm --suppress-prompt --section-name=<share name>
```

9.1.2.2 Adding disk and print shares

1. To add a disk share, edit the `SAMBA$ROOT:[LIB]SMB.CONF` file and add a disk share entry using the following format:

```
[<DISK_SHARE_NAME>]
path = <OpenVMS Directory name that must be shared>
comment = <Directory Share description>
read only = no
```

NOTE: Depending upon the disk share configuration parameter requirements, you can add any of the share section parameters to the above disk share definition.

2. To add a print share, edit the `SAMBA$ROOT:[LIB]SMB.CONF` file and add a print share entry using the following format:

```
[<PRINT_SHARE_NAME>]
printer name = <Same as PRINT_SHARE_NAME>
path = samba$root:[spool]
comment = <Print Share description>
printable = yes
read only = yes
guest ok = yes
```

NOTE:

- Before adding a print share, the OpenVMS print queue must exist or be created. If the print queue name and print share name are not identical, a logical name must be used to link the two. The logical name must be the same name as the print share and must equate to the name of the OpenVMS print queue. For example, if an existing print queue is named HPLASERJET4100_PORTRAT, but the print share name is HP4100POR, define the following system logical name:

  ```
  $ define/system HP4100PORT HPLASERJET4100_PORTRAIT
  ```

  For steps to add a print queue, see Section 9.2.1 (page 141).

- Depending upon the print share configuration parameter requirements, you can add any of the share section parameters to the above print share definition.

9.1.2.3 Modifying disk and print shares

To modify a disk or print share, edit the HP CIFS Server configuration file, where the share definition exists. For example, to modify a disk share “PROJECTS” that is present in the HP CIFS

Server configuration file SAMBA$ROOT:[LIB]SMB.CONF, edit this file and go to the line where the “[PROJECTS]” share definition starts, modify the share parameters as required, and save the file.

9.1.2.4 Deleting disk and print shares

To delete a disk or print share, edit the HP CIFS Server configuration file, where the share definition exists, remove the complete share section, and save the file.

9.2 Managing printers

Managing printers involves setting up print shares, print queues, uploading driver files, adding printers on the client either as network printers or local printers and setting up print security, if required. Section 9.1: “Managing shares” (page 133) discusses listing, adding, modifying and deleting print shares. A primary requirement for adding a print share is setting up a print queue.

9.2.1 Adding print queues

A primary requirement for adding a print share is setting up a print queue. This section describes the different OpenVMS queue setups that are supported by HP CIFS. It includes the following sections:

- “DCPS print queues” (page 141)
- “TCPIP$TELNETSYM print queues” (page 142)
- “LPD print queues” (page 143)

9.2.1.1 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,NOTRAIL)" -        ! 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 OpenVMS CIFS is also tested with DCPS IP_LPD print queues. However, you must define the logical "DCPS$_<print-queuename>_ PRODUCT_NAME", which is required for the printer driver when using DCPS IP_LPD printing. For example, to use “8150 PS driver”, you can define “DCPS$_<print-queuename>_PRODUCT_NAME” as:

   ```
   $ define/system DCPS$_<print-queuename>_PRODUCT_NAME – "HP LaserJet
   8150 Series PS
   ```

4. "9100" in P2 parameter is the raw TCP printer port.
5. For the P4 parameter, specify:
   - "DATA=POSTSCRIPT", if PS drivers are used for printing,
   - “DATA=PCL", if 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 following 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 created each time the system boots.

Execute the following command to verify the newly created print queues:

```
$ show queue
```

Verify that the logical DCPS_LIB is defined:

```
$ show logical DCPS_LIB
```

If the logical DCPS_LIB does not exist, remove the comment from the following line in the file SYS$STARTUP:DCPS$STARTUP.COM:

```
$ DEFINE /EXECUTIVE_MODE /SYSTEM DCPS_LIB DCPS$DEVCTL
```

9.2.1.2 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 must 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*.

9.2.1.3 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$MANAGER:UCX$CONFIG.COM
    ```

  - If you are running HP TCP/IP Services for OpenVMS Version 5.0 or later, enter the following command:

    ```
    $ RUN SYS$MANAGER:TCPIP$CONFIG.COM
    ```

- Add an entry for the remove print server (IP=10.0.0.1) 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"
  ```

9.2.1.3.1 LPD print queue setup

To set up 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 : HPLASER (The printer share mentioned in smb.conf)
Enter the FULL name of one of the following printer types:
remote local : remote
Enter printer synonym: HPLASER
Enter printer synonym:
Enter full file specification for spool directory
SPOOLER DIRECTORY 'sd' : [TCPIP$LPD_ROOT:[HPLASER]] ? SAMBA$ROOT:[VAR.SPOOL]
Set LPD PrintServer extensions flag 'ps' [] ?
Set remote system name 'rm' [] ? lpdsrv1
Set remote system printer name 'rp' [] ? Text
Set printer error log file 'lf' [/TCPIP$LPD_ROOT/000000/HPLASER.LOG] ?
Enter the name of the printcap symbol you wish to modify. Other
valid entry is :
'q' to quit (no more changes)
The names of the printcap symbols are:
sd for the printer spool directory
lf for the printer error log file
lp for the name of the local printer
ps for the LPD PrintServer extensions flag
rm for the name of the remote host
rp for the name of the remote printer
fm for the printer form field
pa for the /PASSALL flag
Queue Setup 79
nd for the /NODELETE flag
cr for the cr flag
sn for the setup NoLF flag
p1-p8 for the /PARAMETER=(p1,...,p8) field
Enter symbol name: q
Symbol type value
------ ---- -----
Error log file : lf STR /TCPIP$LPD_ROOT/000000/HPLASER.LOG
Printer Queue : lp STR HPLASER
PS extensions flag: ps STR
```

```
Remote Host : rm STR lpdsrv1
Remote Printer : rp STR Text
Spool Directory : sd STR /SAMBA$ROOT/VAR/SPOOL
Are these the final values for printer HPLASER ? [y] y
Adding comments to printcap file for new printer, type '?' for help.
Do you want to add comments to the printcap file [n] ? : n
Do you want the queue to default to print flag pages [y] : n
Do you want this procedure to start the queue [y] : y
Creating execution queue: HPLASER
Updating TCPIP$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 *
**********************************************
```

9.2.2 Uploading printer drivers

A CIFS print share can be added as a network printer or a local printer on the client. If you want to add a printer as a network printer, it is recommended that you first upload the printer drivers to the HP CIFS Server. This ensures that when the printer is added as a network printer on a client, the required driver is automatically downloaded from the HP CIFS Server. You must upload a printer driver for the printer only once for each of the client Operation Systems.

For example, if you want to configure the CIFS printer HP_LASER_PRINTER on Windows XP and Windows Vista clients, then you need to upload the driver files specific to Windows XP and Windows Vista separately only once. The option of uploading driver files is useful if you want the Windows users to automatically add CIFS Printers on their client system without installing the print drivers manually.

When adding a printer as a local printer on the Windows system, the driver files can be installed on the client itself and you do not need to upload printer driver files to the HP CIFS Server. This method involves manually installing printer drivers on each client while adding the printer on that client.

9.2.2.1 Creating PRINT$ share

The first part of uploading printer drivers is the creation of a share named PRINT$ that Windows clients automatically connect to when downloading printer drivers. From HP OpenVMS CIFS V1.2 onwards, if you have used the Samba configuration utility `SAMBA$CONFIG.COM` at least once, the PRINT$ share is automatically added. To verify if the PRINT$ share is present in the HP CIFS Server configuration file, either execute the utility `SAMBA$MANAGE_CIFS.COM` to list a share detail or execute the following commands:

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

```
$ testparm --suppress-prompt --section-name=print$
```

If the PRINT$ share section is found missing, edit the `SAMBA$ROOT:[LIB]SMB.CONF` file and add the PRINT$ share as follows:

```
[print$]
        comment = Printer Driver Download Area
        path = /samba$root/print_drivers/
        guest ok = yes
        read only = yes
        browseable = no
        vms path names = no
        write list = @Administrators, "@Print Operators", cifsadmin
```

NOTE:

- Additional user or group names can be added to "write list" by separating them using a comma. While specifying a group name, prefix the name with the "@" character.
- The list of users or the users belonging to the specified groups in the write list will be allowed to upload printer driver files for any of the CIFS Printer shares.
- To allow a user to upload printer driver files without granting admin privileges, you can make that user as a member of the HP CIFS Server "Print Operators" built-in group.
- The directory `samba$root:[print_drivers]` is created by default when the HP OpenVMS CIFS kit is installed.

9.2.2.2 Uploading drivers

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

1. From a Windows client, connect to the HP CIFS Server (that is, **Start** --> **Run** --> **\\servername**) as an administrator or a user with appropriate privileges (Using a username that is part of "write list" for the PRINT$ share).
2. Open the **Printers and Faxes** folder.
3. Right-click the printer for which you want to upload drivers, and select **Properties**.

NOTE: You are now trying to view printer and driver properties for a queue that has a default NULL driver assigned. This results in the following error message:

```
"The printer driver is not installed on this computer. Some printer
properties will not be accessible unless you install the printer
driver. Do you want to install the driver now?"
```

IMPORTANT: Do not click Yes! Instead, click **No** in the error dialog. The properties window for the selected printer is displayed.

4. In the **Properties** window, select the **Advanced** tab. On the **Advanced** dialog box, click **New Drive**. This launches the `Add Printer Driver` wizard.
5. Click **Next** in the **Add Printer Driver** wizard.
6. In the **Printer Driver Selection** box, select the applicable **Manufacturer** and **Printer** driver. For example, if the printer is an "HP" printer, select "HP" as the manufacturer. Then choose an appropriate printer driver from Printers drop—down list. If the driver is not listed under **Printer** drop box, click **Have Disk** and choose the location of the printer driver on the disk. Once the **Manufacturer** and **Printer** driver are selected, click **Next**.
7. Click **Finish** to start uploading the printer driver.
8. After the printer driver is uploaded, click **Apply**. The name of the printer is changed to the printer driver that you installed.
9. To rename the printer name to the original name, click the **General** tab. Replace the driver name (opposite the printer icon) with the original printer name and then click **OK**.
10. To upload additional drivers for a different version of a Windows Operating System, go to the **Sharing** tab in the printer properties and click on **Additional Drivers** to display **Additional Drivers** dialog box. Select the operating system for which you want to upload the additional driver and click **OK**. Using the displayed **Printer drivers** dialog box, you can copy the driver files present on the disk for the selected Operating system.

9.2.3 Adding a printer as network printer on the client

1. Connect to the CIFS server from a Windows client.

2. Open the **Printers and Faxes** folder and select the desired printer. Right-click and select **Open** or **Connect**. If required, a printer driver is downloaded from the CIFS server. A new printer icon for the CIFS print share appears in the **Printer and Faxes** folder on the client system.

NOTE: You must first upload printer driver files to the HP CIFS Server to configure a CIFS printer as a network printer.

9.2.4 Adding a printer as local printer on the client

1. On the system that is running Windows, click **Start** > **Settings**, and then click **Printers and Faxes**.
2. In the **Printers and Faxes** folder, right-click and select **Add Printer**.
3. Click **Next**.
4. Click **Local printer**, click to clear the **Automatically detect and install my Plug and Play printer** check box, and then click **Next**.
5. Click **Create a new port**, and then select **Local Port** from the drop-down next to **Type of Port**.
6. In the **Port Name** dialog box, type the path of the printer by using the following syntax:

   \\<cifs server name>\<printer share name>
7. Click **Next**.
8. In the **Install Printer Software** page, click the correct manufacturer under the **Manufacturer** panel, click the name of a printer that supports the same printer emulation as your printer, click **Next**, and then click **Finish**.

10 File and print security

An important requirement for any file and print services is file security. Unlike Advanced Server for OpenVMS, which provides NT ACL based file security as well as OpenVMS based file security, the HP CIFS Server provides file security to Windows clients using the OpenVMS file security alone. That is, it maps the Windows security applied on the files and directories to OpenVMS file security. File security can be set for any CIFS domain user or group. File and directory access auditing is not provided by CIFS, but standard OpenVMS auditing can be used for this purpose. CIFS file security comprises two steps:

1. User and group mapping
2. Permission mapping

This chapter addresses the following topics:

The chapters Chapter 6 (page 87) and Chapter 7 (page 95) explain the first aspect of CIFS File Security, mapping the CIFS domain users and groups to OpenVMS usernames and resource identifiers. This chapter describes how the HP CIFS Server maps the Windows permissions to OpenVMS file security as well as how to manage access to resources.

The HP CIFS Server supports Access Control Lists (ACLs) on printer objects as well and this is explained in the Section 10.8 (page 161).

10.1 Mapping file permission

The Windows to OpenVMS file permission mapping involves mapping Windows file permissions to OpenVMS file security. This chapter also explains how the OpenVMS RMS protection code on new files and directories can be controlled through the HP CIFS Server configuration file parameters.

10.1.1 Mapping permission from Windows to OpenVMS

OpenVMS allows you to specify READ (R), WRITE (W), EXECUTE (E), DELETE (D) or CONTROL (C) access permission on an object or a combination of RWEDC permissions (See note [p. 148]). On Windows standard permissions, on the other hand, include 'Full Control, Modify, Read and Execute, List Folders Contents (for directories only), Read, and Write' standard permissions on an object using the **Security** dialog box. Windows also provides special permissions settings, available through the **Advanced** button on the **Security** tab of the **Properties** page.

(page 148) lists the Windows permissions that are mapped to the corresponding OpenVMS permissions by CIFS. The *Advanced* in parenthesis indicates that this permission is available on Windows only from the **Advanced Security Setting** dialog box. 'Full Control' and 'Read' permissions are part of standard as well as special permissions.

Table 10-1 Mapping Windows permissions to OpenVMS permissions

Windows Permissions	OpenVMS Permissions
Full Control	RWEDC
Modify	RWED
Read and Execute	RE
Read	R
Write	W
Full Control (Advanced)	RWEDC
Traverse Folder / Execute File (Advanced)	E
List Folder / Read Data (Advanced)	R
Read Attributes (Advanced)	R
Read Extended Attributes (Advanced)	R
Create Files / Write Data (Advanced)	W
Create Folder / Append Data (Advanced)	W
Write Attributes (Advanced)	W
Write Extended Attributes (Advanced)	W
Delete Subfolders and Files (Advanced)	Not supported
Delete (Advanced)	D
Read Permissions (Advanced)	R
Change Permissions (Advanced)	C
Take Ownership (Advanced)	C

NOTE: Though the `ACCESS=NONE` access control directive is considered if present on an object, the HP CIFS Server does not support the `DENY` permission options available when setting permissions from Windows.

10.1.2 Mapping Windows inheritance value to OpenVMS inheritance

On a Windows system, when setting permissions on a directory, you can specify if the access is applicable only to that directory or to the subfolders and files that will be created under it or to a combination of these.

Similarly, OpenVMS provides DEFAULT ACLs for the directories that are applicable only to the files and directories created under it while the access to the directory is controlled by the access ACE on the directory.

For example, on an OpenVMS, if the parent directory has the following security:

```
PROJECTS.DIR;1          [SYSTEM]                        (RWE,RWE,E,E)
DEFAULT_PROTECTION,SYSTEM:RWED,OWNER:RWED,GROUP:,WORLD:)
IDENTIFIER=ADMIN_USER,ACCESS=READ+WRITE+EXECUTE+DELETE)
IDENTIFIER=ADMIN_USER,OPTIONS=DEFAULT,ACCESS=READ+WRITE+EXECUTE+DELETE)
```

For a user with normal OpenVMS privileges, the access to the directory `PROJECTS.DIR` is controlled through the `ACE (IDENTIFIER=ADMIN_USER,ACCESS=READ+WRITE+EXECUTE+DELETE).`

The ACE
`(IDENTIFIER=ADMIN_USER,OPTIONS=DEFAULT,ACCESS=READ+WRITE+EXECUTE+DELETE)`
is applied for all the newly created files and directories in the parent directory `PROJECTS.DIR`.

(page 149) lists the Windows to OpenVMS inheritance mapping provided by CIFS.

Table 10-2 Windows inheritance value to OpenVMS inheritance mapping

Windows inheritance value	OpenVMS inheritance mapping
This Folder only	Maps to access ACE.
This Folder, Subfolders and Files	Maps to both access and OPTIONS=DEFAULT ACE.
This Folder and Subfolders	Maps to access ACE.
This Folder and Files	Maps to access ACE.
Subfolders and Files only	Maps to OPTIONS=DEFAULT ACE for this directory.
Subfolders only	Not supported; ignored.
Files only	Not supported; ignored.

10.1.3 Mapping OpenVMS RMS protection code to Windows permissions

An OpenVMS RMS protection code consists of Read, Write, Execute, and Delete permissions for four categories of users: System, Owner, Group, and World. A typical RMS protection code is (S:RWED,O:RWED,G:RE,W), which indicates members of the System and Owner categories have Read, Write, Execute, and Delete access, while members of the Group category have only Read and Execute access, while members of the World category have no access. All objects obtain an RMS protection code when created. The OpenVMS security conventions for assigning the RMS protection mask are beyond the scope of this guide and are fully documented in the *HP OpenVMS Guide to System Security*.

In general, however, new directories inherit their RMS protection code from the parent directory. The RMS protection code applied to new files is based on the RMS protection mask in effect for the process creating the file. The default RMS protection mask is controlled by the SYSGEN parameter RMS_FILEPROT (but can be changed using the `$ SET PROTECTION/DEFAULT` command). The default value for RMS_FILEPROT results in an RMS protection mask of (S:RWED,O:RWED,G:RE,W).

Additionally, OpenVMS provides a DEFAULT_PROTECTION ACE which, if present on a directory, determines the RMS protection code applied to new files (but not new directories) created in the directory. The DEFAULT_PROTECTION ACE is propagated to the Access Control List of any new directory created in the directory, but it never affects the RMS protection mask applied to those new directories.

While Windows has no concept of a similar protection code, Windows does provide some equivalent functionality in this area. Windows does maintain the Owner of an object, similar to OpenVMS. Windows has a special group known as Everyone which is similar in concept to the OpenVMS World category of the RMS protection code. On directories, Windows also maintains permissions for CREATOR OWNER and CREATOR GROUP which represent the permissions to be applied to new objects for the file owner and the primary group of the file owner, respectively.

"OpenVMS RMS protection code to Windows security mapping " (page 150) shows the association between the RMS protection code categories and Windows security concepts.

Table 10-3 OpenVMS RMS protection code to Windows security mapping

RMS Protection code category	Windows mapping
Owner and SYSTEM	Owner
Group	(Displayed as) Unix Group
World	Everyone
Owner in Default Protection ACE	CREATOR OWNER on the directory
Group in Default Protection ACE	CREATOR GROUP on the directory
World in Default Protection ACE	Everyone for Subfolder and Files

10.1.4 Mapping RMS protection mask RMS_FILEPROT to CREATOR OWNER and CREATOR GROUP

For a directory, Windows requires that CREATOR OWNER permission is present on it. While viewing/setting permissions on a directory from the Windows system, if a DEFAULT_PROTECTION ACE is not present on the directory, CIFS Server maps the CREATOR OWNER, CREATOR GROUP to the protection mask in OpenVMS SYSGEN parameter, RMS_FILEPROT as shown in Table 10-4 (page 150):

Table 10-4 Mapping RMS protection mask RMS_FILEPROT to Windows

RMS Protection mask RMS_FILEPROT	Windows mapping
Owner of RMS_FILEPROT	CREATOR OWNER on the directory
Group of RMS_FILEPROT	CREATOR GROUP on the directory
World of RMS_FILEPROT	Everyone for Subfolder and Files

10.1.5 Controlling RMS protection code using configuration parameters

The HP CIFS Server provides several configuration parameters that may be used to affect the RMS protection code applied when a new object is created or when setting Windows permissions. While the parameter names may be familiar to Samba administrators, their implementation in the HP CIFS Server is quite different when compared to Open Source versions of Samba (which are primarily based on the UNIX security model).

By default, the HP CIFS Server relies on OpenVMS to determine the security profile for new objects based on standard OpenVMS security rules. The HP CIFS Server adjusts the security only when non-default values are specified for certain configuration parameters.

NOTE: The HP CIFS Server grants Delete access to the Owner of any new directory, thereby conforming to standard Windows behavior, which allows the creator to rename or delete the new folder (standard OpenVMS behavior is to remove all Delete access when a directory inherits the RMS protection mask from its parent).

The following configuration parameters can be used to modify security applied by OpenVMS:

- inherit owner - The default value is "no". If set to "yes", causes the HP CIFS Server to set the RMS owner of new objects to that of the parent directory.

NOTE: If `inherit owner = no` and a parent directory is owned by a resource identifier, when a non-privileged user who has WRITE access to this directory, creates a new file, the HP CIFS Server sets the Owner to the UIC of the user creating the file, rather than the Resource Identifier. To retain the OpenVMS behavior (that is, to set the resource identifier as owner), add `inherit owner = yes` to the applicable [share] sections of the `SMB.CONF` file.

- *inherit vms rms protections* - This is a new parameter with a default value of "no". If set to "yes", causes the HP CIFS Server to:
  - Set the RMS protection code to that of the parent directory.
  - Ignore a DEFAULT_PROTECTION ACE, if present.
  - Ignore the RMS protection mask specified by the SYSGEN parameter *RMS_FILEPROT*.
  - Ignore the mask and mode parameter values specified in the `SMB.CONF` file.
- Table 10-5 (page 151) lists the mask and mode parameters supported by HP CIFS Server.

Table 10-5 Mask and Mode Parameters

Parameter Name	Affects RMS protection code when
create mask	Creating new files
force create mode	Creating new files
directory mask	Creating new directories
directory security mask	Windows users and applications modify security on the directory.
force directory security mode	Windows users and applications modify security on the directory

NOTE:

- CIFS for OpenVMS does not use the configuration parameters *security mask* and *force security mode* when a Windows user and application modifies the security of a file.
- The *create mode* parameter is synonymous with *create mask*. HP recommends using *create mask* to avoid confusion.

10.1.5.1 Non-modifiable configuration parameters

The values for the configuration parameters listed in Table 10-6 (page 151) cannot be modified from their defaults (changes are ignored):

Table 10-6 Configuration parameters

inherit acls	Default is "yes"; you cannot disable inheritance of ACLs
inherit permissions	Replaced by the "inherit vms rms protections" parameter
security mask	Not supported
force security mode	Not supported

10.1.5.2 Mask and mode parameter values

One of the significant file security changes introduced in HP CIFS Server concerns granting DELETE access in the RMS protection code on new objects. Previously, the various mask and mode parameters tied DELETE access to the WRITE bit; that is if you enabled WRITE access you also enabled DELETE access. However, DELETE and WRITE protections have now been separated as shown:

The values for the mask and mode parameters now have this significance:

```
<mask or mode parameter name>= 0dogw
```

where:

`0`= Indicates the value is Octal.

`d` = Controls granting DELETE access across all categories of the RMS protection code (see DELETE [p. 152])

`o` = Controls granting READ, WRITE, and EXECUTE access for the Owner category of the RMS protection code

`g` = Controls granting READ, WRITE, and EXECUTE access for the Group category of the RMS protection code

`w` = Controls granting READ, WRITE, and EXECUTE access for the World category of the RMS protection code

NOTE: The System category of the RMS protection code receives the same permission as the Owner category; there is no option to modify this behavior.

DELETE access is signified using a bitmask with the following values:

4 — Grant DELETE access to Owner category of RMS protection code

2 — Grant DELETE access to Group category of RMS protection code

1 — Grant DELETE access to World category of RMS protection code

The Owner, Group, and World access values are also bitmasks which signify the following access:

4 —Grant READ access

2 —Grant WRITE access

1 —Grant EXECUTE access

In addition, the default values for the mask and mode parameters have been changed such that they will not adjust the security that OpenVMS would itself apply (except where noted).

The following mask and mode parameter are related for doing AND & OR operation to generate a resultant RMS protection code:

- *create mask* and *force create mode*
- *directory mask* and *force directory mode*
- *directory security mask* and *force directory security mode*

The value of the appropriate *mask* parameter is AND'd with the result of the RMS protection code provided by OpenVMS. This result is then OR'd with the value of the appropriate *mode* parameter.

By default, the value of the *mask* parameters is 07777 and that of *mode* parameters is 00000 with the only exception of *force directory mode*. From HP CIFS version 1.2 onwards, the default value for *force directory mode* is 04000. This is to allow DELETE permission for the OWNER category of the protection code when a new directory is created.

10.2 Storing DOS attributes

The HP CIFS Server supports storing of DOS attributes SYSTEM, HIDDEN, ARCHIVE or READ-ONLY on a file. This functionality is disabled, by default. To enable storing of DOS attributes, specify:

```
store dos attributes = yes
```

The parameter *store dos attributes* is a share level parameter and may be set on an individual share basis.

The following configuration parameters, which previously mapped the storing of DOS attributes in the RMS protection code, are no longer supported:

- *map system*
- *map hidden*
- *map archive*
- *map readonly*

10.3 ACL order while applying CIFS file security

On an OpenVMS system, the order of ACEs in an ACL is a critical factor when determining access as compared to Windows. They are applied on the files and directories and has a lot of importance while the same does not hold for Windows systems.

Due to the contrasting nature of the ACL processing between Windows and OpenVMS, it is important to understand the order in which the ACEs are applied by the HP CIFS Server when setting security on an object. While applying OpenVMS ACEs on an object, HP CIFS Server must also preserve any existing OpenVMS-specific ACEs (see NOTE [p. 153]) and, ideally, in their original order. The following design is implemented by the HP CIFS Server when applying security on an object from a Windows system:

1. When a new entry is added to the permissions list, the corresponding ACE is placed at the top of the ACL.
2. When an existing permissions list entry is modified, the ACL order is not affected.
3. All OpenVMS-specific ACEs are retained in their existing order.

NOTE: OpenVMS-specific ACEs include Audit and Alarm ACEs, ACEs containing IDENTIFIER=*, as well as protected or hidden ACEs. Such ACEs cannot be viewed, modified, nor removed using a Windows system.

10.4 Limitations due to file security mapping

The earlier sections of this chapter explained how Windows file security is mapped to OpenVMS file security. This mapping mechanism is not without its limitations as Windows and OpenVMS systems vastly differ in the way they process ACLs on an object to grant access to the object. The limitations due to file security mapping provided by HP CIFS Server are in the following areas:

10.4.1 Object access limitation

Windows systems allow access to an object based on the accumulated access permissions for an object unless the user has special rights. For example, if a user is a member of a group which has only Read access to an object as well as a group which has only Write access, the user's effective permissions are Read and Write. Due to this, the ACL order is not relevant in Windows (with the exception of DENY permissions).

On OpenVMS systems, the order in which the ACLs appear on an object is very important. OpenVMS grants access to an object based on the first matching ACE that it encounters from the top of the ACE list unless the user has special privileges or is an owner of the file.

This can result in unexpected access failures. For example, if a user is a member of two groups, one of which has only Read access while the other group has only Write access, the user will only be granted Read or Write access, never both. Whether the user receives Read or Write access

depends on which permission entry is listed first. This and other scenarios may require the administrator to manage security on objects using OpenVMS commands such as $ SET SECURITY, rather than Windows, and adhere to the recommendation in the OpenVMS Guide to System Security to place ACEs granting the greatest access above ACEs granting less access. To achieve the same result when setting permissions from a Windows system, the Administrator must ensure entries remain in order from greatest access to least access, when viewed top to bottom. Doing so may require all existing entries be removed and added anew when a new entry is added to the list.

10.4.2 Non-inheritable OpenVMS ACE limitation (on files only)

When the ACL of a file contains OpenVMS-specific ACEs (such as Audit, Alarm, Protected or Hidden ACEs) which have been explicitly and exclusively added (rather than inherited from an OPTIONS=DEFAULT ACE on the parent directory), the HP CIFS Server may not retain these OpenVMS-specific ACEs if the file is modified. This restriction does not apply to directory files.

For example, you may have explicitly set an Audit ACE on a single file without applying a corresponding inheritable ACE on the parent directory. If a user modifies the file, the Audit ACE that was explicitly set on this file may be lost when the file is closed. This is particularly applicable to files modified using Microsoft Office applications. To avoid the possibility of losing OpenVMS-specific ACEs on such files, apply an inheritable OPTIONS=DEFAULT ACE on the parent directory that will result in the OpenVMS-specific ACE being applied to any new file created therein. However, this will result in the ACE being applied to all new files created in the directory.

10.4.3 Built-in administrators group limitation

Prior to HP CIFS V1.1 ECO1, all members of the built-in local Administrators group were granted two special OpenVMS privileges, BYPASS and SYSPRV. This allowed local administrators to access all files on all shares from a Windows client for the intended purpose of managing file security. However, this conflicts with standard Windows behavior whereby Administrators may only access resources to which they have explicitly been granted access.

Members of the Administrators group are no longer granted BYPASS and SYSPRV privilege. As a result, though members of the local Administrators group may still perform other administrative duties, they cannot set security on files and folders until they are granted the right to do so. For information on the permissions required to set privileges, see Section 10.5 (page 155).

10.4.4 Windows inheritance value mapping limitation

When setting permissions on a directory from a Windows system, Windows provides multiple options controlling the propagation of permissions. The HP CIFS Server does not support the “Subfolder only” nor the “Files only” options. For details on how the HP CIFS Server processes other options, see Table 10-2 (page 149)

10.4.5 Windows special permission limitation

The HP CIFS Server does not support the Windows special permission “Delete Subfolders and Files”. Attempts to set this option may result in an “Access denied” error.

10.4.6 Limitation when viewing directory or share permissions

When viewing directory or share permissions from a Windows system, it is imperative to use the **Advanced Security Settings** window as the permissions displayed in the basic **Security** dialog box may not correctly reflect the true set of permissions on the object. This limitation does not apply to files.

Click the **Advanced** button on the basic Security properties dialog window to open the **Advanced Security Settings** window.

10.5 Permissions and privileges required to set file security

Setting file security from Windows requires the user have certain permissions or privileges. This section describes these permissions and privileges.

10.5.1 Providing administrators access to files from Windows

Administrators are unable to affect file permissions from a Windows system unless at least one of the following is true:

- They are a member of the local Administrators group and the local Administrators group has been granted access to the files. The local Administrators group is created by the HP CIFS Server and is mapped to the OpenVMS resource identifier CIFS$ADMINISTRATORS. Grant the CIFS$ADMINISTRATORS identifier at least Read access to the directory and files. This method allows access to be controlled on a file-by-file basis.
- The user is listed in the “admin users” configuration parameter. This method may be implemented on a share-by-share basis, either on all or individual shares, and applies to all files in those shares (see details below).
- The user’s mapped OpenVMS account has special OpenVMS default privileges such as BYPASS, GRPPRV, READALL, or SYSPRV. In this case, the access applies to all files in all shares which the user may access.

10.5.2 “admin user” configuration parameter

Another method for granting users Administrator access, either on a server-wide basis, or on a share-by-share basis, is by using the configuration file parameter *admin users*. The *admin users* is a share-level parameter which may be specified in individual share sections, to bestow full access rights to the listed users, or in the [global] section, to bestow both full access to all files in all shares and also grant full Administrator rights, allowing the user to manage users, groups, and shares.

NOTE: The syntax of the users or groups listed in this parameter depends on the role of the server. When the server is a Member Server in a domain, the domain name must be included as part of the user or group name, when appropriate. For all other roles, the domain name is required only if the user or the group is from a trusted domain (if applicable).

For example, if the server is a Member Server in the domain `CORPDOM` which trusts domain `OPERS` and you want to designate local user `CIFSADMIN`, `CORPDOM` user `ANITA`, and `OPERS` group "`Domain Admins`" as administrators for the PROJECTS share, add the following line to the [PROJECTS] section of the HP CIFS Server configuration file:

```
admin users = CIFSADMIN, CORPDOM\ANITA, OPERS\"DOMAIN ADMINS"
```

10.5.3 Windows “Change Permissions” and “Take Ownership” permissions

The Windows “Change Permissions” and “Take Ownership” permission are both mapped to OpenVMS Control access. Therefore, users granted either “Change Permissions” or “Take Ownership” may both change permissions and take ownership.

10.6 File security

This section outlines the procedures for setting permissions on files either from a Windows system or from the OpenVMS host. It is assumed the necessary user and group accounts exist.

10.6.1 Modifying file security from a Windows system

Follow the guidelines below to view and manage file permissions from a Windows 2003 system (procedures may vary slightly on other Windows versions).

Displaying Existing Permissions

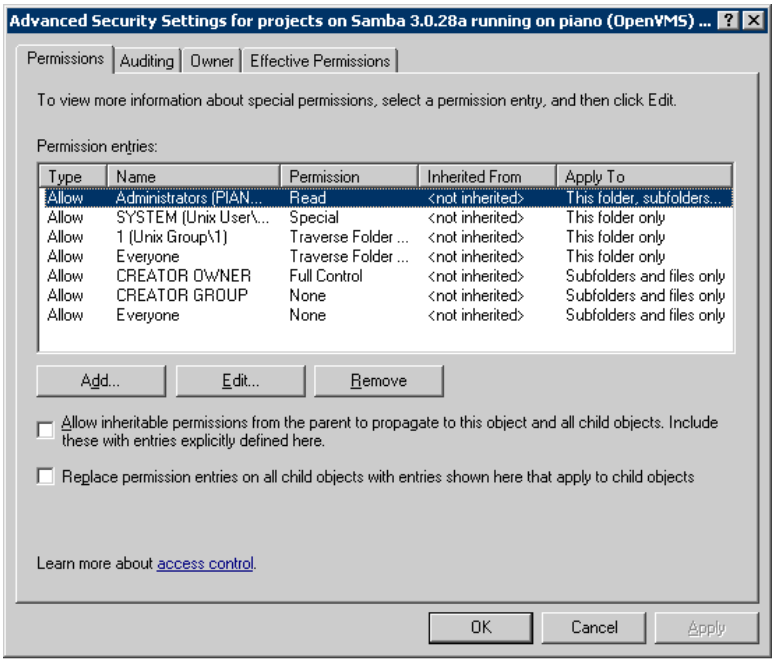
To display the existing set of permissions on an object:

1. Establish Identity.

   Connect to the HP CIFS Server such that it identifies you as a user with rights to change permissions on the objects. For example, if you are logged into the domain as a user who has administrator rights on the HP CIFS Server, click Start -> Run and enter the name of the server. A list of available share directories is displayed. However, if you are not logged into the domain as a user with administrator rights on the HP CIFS Server, establish a new session to the HP CIFS Server using the "Connect As" functionality and specify a user with administrator access. Then click Start -> Run and enter the server name to obtain the list of share folders.

2. **1.** Select a folder or navigate to the desired folder and select a folder or file.
   2. Right-click on the object and select **Properties**.
   3. On the **Properties** window, select the 'Security' tab.
   4. On the **Security** window, click the **Advanced** button to open the **Advanced Security Settings** window.

Figure 10-1 Advanced Security Settings window

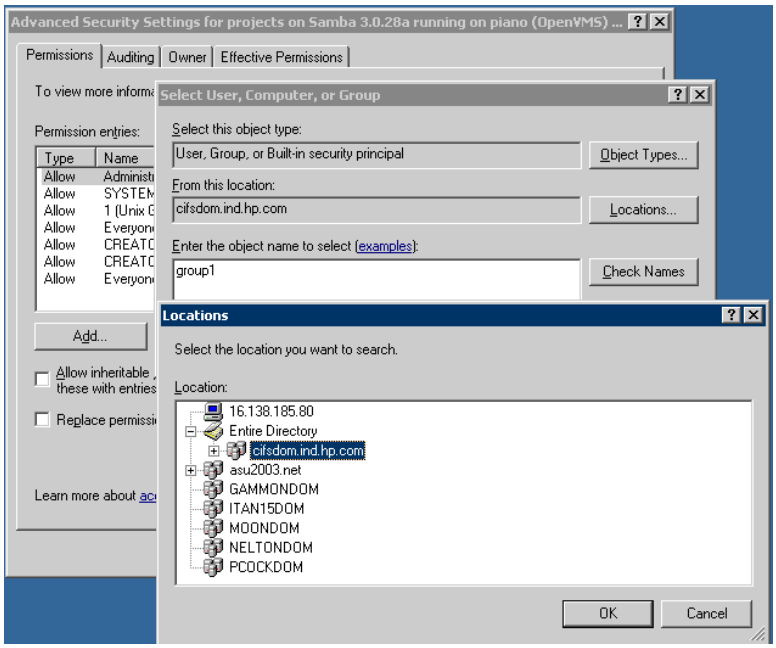


3. Setting Permissions on a Directory/Folder

Adding permissions

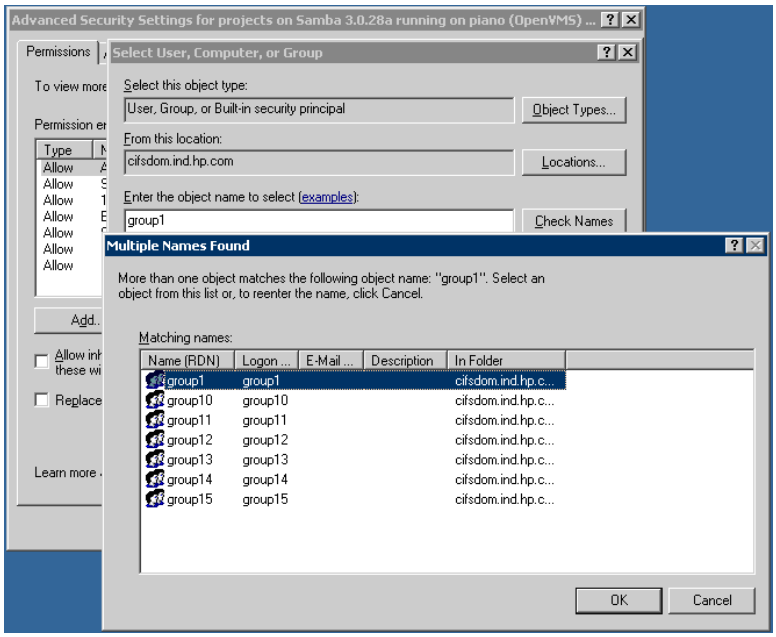
1. Click the **Add** button to display the **Select User, Computer, or Group** dialog box.
2. If necessary, click the **Locations…** button and select the appropriate account location.

Figure 10-2 Adding Permissions



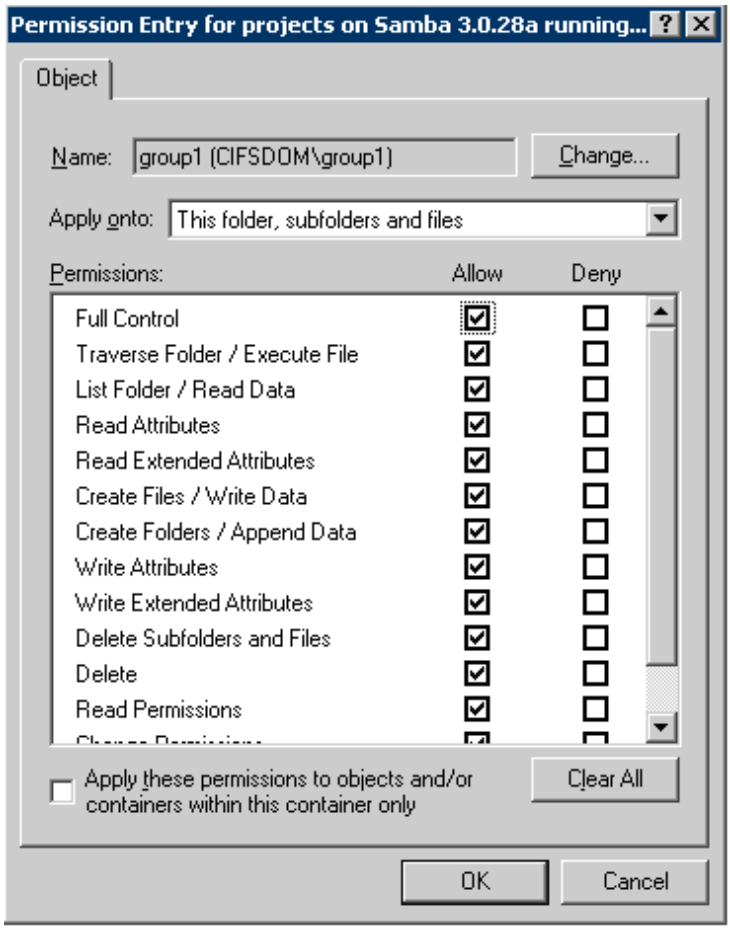
3. Specify the user or group name in the **Enter the object name to select** section and click the **Check Names** button.
4. If the **Multiple Names Found** window is displayed, select the user or group and click **OK** to return to the **Select User, Computer, or Group** dialog box.

Figure 10-3 Selecting users or groups



5. Click **OK**. Windows displays the Permission Entry window for the object. Select the required Allow permissions.

Figure 10-4 Permissions



6. If this is a folder, if appropriate, select the option “Apply these permissions to objects and/or containers within this container only”.
7. Click **OK** to return to the Advanced Security Settings window.
8. Click Apply to save changes immediately and continue modifying permissions. Otherwise, click OK to return to the Properties dialog box and commit the operation.
9. Click **OK** on the Properties window to exit.

Modifying Existing Permissions

1. Select the entry from the ‘Permission entries’ list presented in the Advanced Security Settings window and click Edit.
2. From the permission Entry window displayed for the Object, change the permissions as desired.
3. If the object is a folder, if appropriate, select the option “Apply these permissions to objects and/or containers within this container only”.
4. Click **OK** to return to the Advanced Security Settings window.
5. Click **Apply** to save changes immediately and continue modifying permissions. Otherwise, click **OK** to return to the Properties dialog box and commit the operation.
6. Click **OK** on the **Properties** window to exit.

Removing permissions

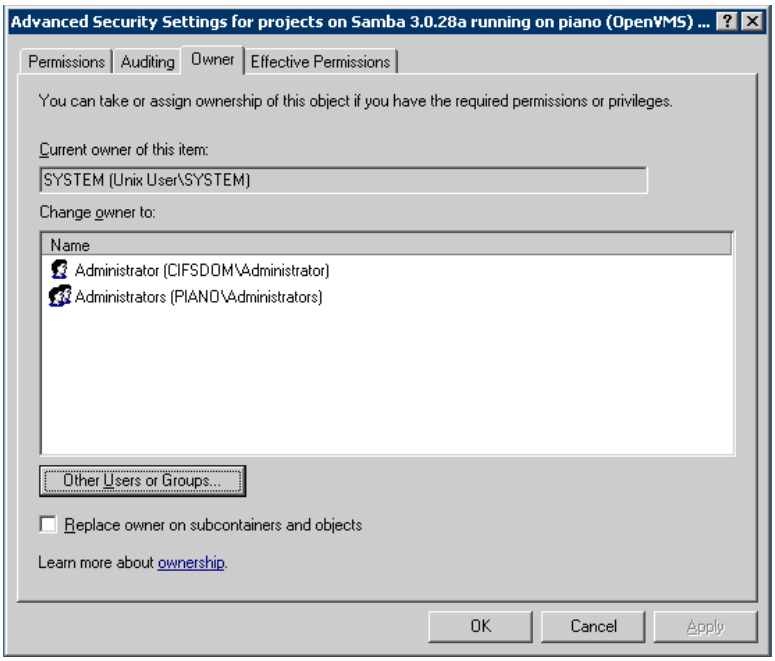
1. Select the entry from the list and click the Remove button.
2. Click **Apply** to save changes immediately and continue modifying permissions. Otherwise, click **OK** to return to the Properties dialog box and commit the operation.
3. Click **OK** on the **Properties** window to exit.

10.6.2 Taking and assigning ownership

At times it may be necessary to change the Owner of an object. By default, non-administrator users who have Take Ownership privilege on an object may only assign themselves as the object owner. Administrators and Backup Operators are able to assign ownership to other users and groups. To assign ownership of an object from a Windows 2003 system (procedures may vary slightly for other Windows versions), follow these steps:

1. Right-click on the object and select **Properties**.
2. From the **Properties** window, select the **Security** tab.
3. Click the **Advanced** button.
4. Select the **Owner** tab.

Figure 10-5 Owner tab



5. If the name of the user or group is listed in the "**Change owner to**" section, select the user. Otherwise, click the "**Other Users or Groups…**" button, specify a name and click **OK**.
6. If the **Multiple Names Found** window appears, select a name from the list and click **OK**.
7. Click **Apply** to save changes immediately.
8. Click **OK** to return to the **Properties** window.
9. Click **OK** to exit.

10.6.3 Modifying file security from an OpenVMS host

This section briefly describes how to set file security from the OpenVMS host.

1. Determine the name of the OpenVMS account or resource identifier to be granted access. If the name of the mapped OpenVMS account or resource identifier is not known, use the WBINFO and supply the domain name and Windows account or group name to which permissions are to be granted. If the account or group is local to the CIFS server, omit the domain name (but see note below).

   For example, to determine the name of the OpenVMS resource identifier mapped to the group named ACCTNG in the domain named CORPDOM:

   ```
   $ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
   $ WBINFO --DOMAINNAME-TO-HOSTNAME=CORPDOM\ACCTNG
   ```

NOTE:

- The `WBINFO` utility requires the SYSPRV privilege.
- If the user or group exists in the HP CIFS Server local database, the domain name may be omitted, except for BUILTIN groups such as Administrators, "Domain Admins". To specify a Built-in group, prefix the group name with `BUILTIN\`. For example, to determine the name of the OpenVMS resource identifier mapped to the Administrators group:

  ```
  $ WBINFO --DOMAINNAME-TO-HOSTNAME=BUILTIN\ADMINISTRATORS
  ```

2. Once the name of the OpenVMS account or resource identifier has been identified, use the DCL command $ SET SECURITY to modify the security on an object. If necessary, see the *HP OpenVMS Guide to System Security* and DCL Manual for detailed information on managing access to objects and the `SET SECURITY` command.

10.7 Critical database files

By default, the HP CIFS Server stores server data in various database files. Several of these files must be backed up regularly as their loss can result in serious security implications. In order to ensure the files are viable upon restore, they must not be open when backed up. Therefore, the HP CIFS Server must be shutdown during the backup. If multiple cluster members share the same `SAMBA$ROOT:` directory tree, they also share these database files; therefore, HP CIFS Server must be shutdown on all applicable cluster members during the backup. Table 10-7 (page 160) lists the name, default location, and purpose of each of these database files.

Table 10-7 Critical database files

Name	Location	Purpose
WINBINDD_IDMAP.TDB	SAMBA$ROOT:[VAR.LOCKS]	Used if WINBIND automatic mapping is enabled. Maps domain SIDs to idmap UID/GID values.
GROUP_MAPPING.TDB	SAMBA$ROOT:[VAR.LOCKS]	Stores group accounts, their members, and mappings to OpenVMS resource identifiers.
PASSDB.TDB	SAMBA$ROOT:[PRIVATE]	Stores user and machine accounts (i.e., created using PDBEDIT).
SECRETS.TDB	SAMBA$ROOT:[PRIVATE]	Stores information that must remain secure such as machine account password, trust account passwords, and the ldap admin distinguish name and password.
ACCOUNT_POLICY.TDB	SAMBA$ROOT:[VAR.LOCKS]	Stores account policy settings, such as maximum password age, minimum password length, and password history.

Table 10-7 Critical database files *(continued)*

Name	Location	Purpose
SHARE_INFO.TDB	SAMBA$ROOT:[VAR.LOCKS]	Stores share ACLs (permissions at the share level).
NTDRIVERS.TDB	SAMBA$ROOT:[VAR.LOCKS]	Stores information about installed printer drivers.
NTFORMS.TDB	SAMBA$ROOT:[VAR.LOCKS]	Stores information about installed printer forms.
NTPRINTERS.TDB	SAMBA$ROOT:[VAR.LOCKS]	Stores information about installed printers such as printer permissions.

10.8 Print security

Both Windows security and OpenVMS security can be employed to provide printer security.

Using Windows permissions to control printer security is useful when printer driver files for the printers are stored on the server, available to be downloaded automatically whenever a printer is added on Windows clients. When Windows permissions are applied to printers, those permissions are stored in the database file `SAMBA$ROOT:[VAR.LOCKS]NTPRINTERS.TDB`. The OpenVMS security present on the print queue is not affected.

NOTE: You must upload print drivers to the server before attempting to establish Windows-style printer security.

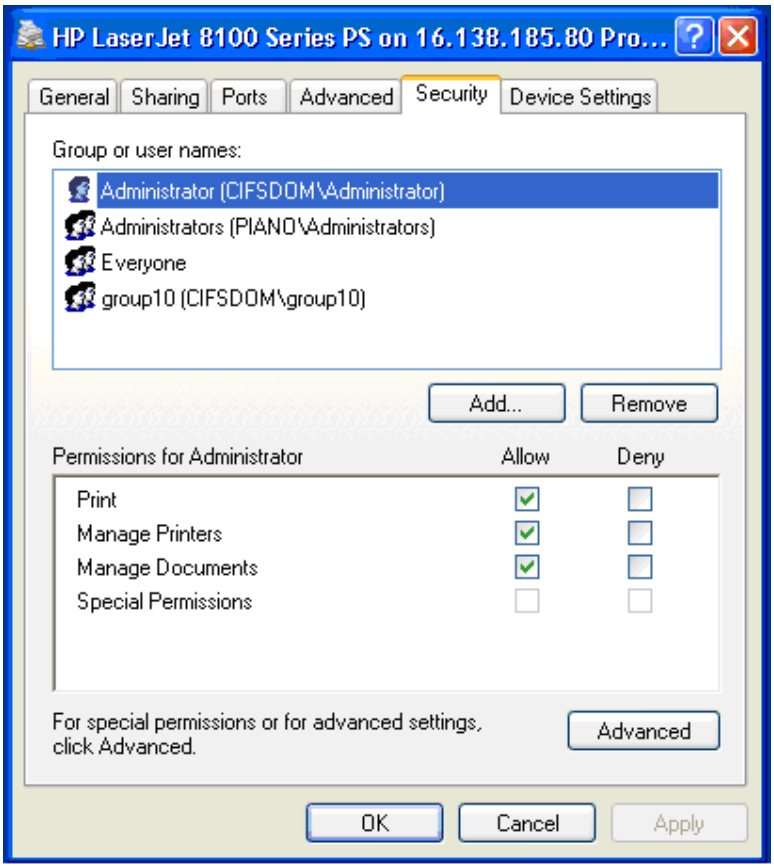
OpenVMS security may also be used on OpenVMS print queues to control access, either alone or in combination with Windows security. This method of security is useful when configuring HP CIFS Server print shares as local printers on Windows clients.

10.8.1 Setting up Windows-style printer security

To set up Windows-style printer security:

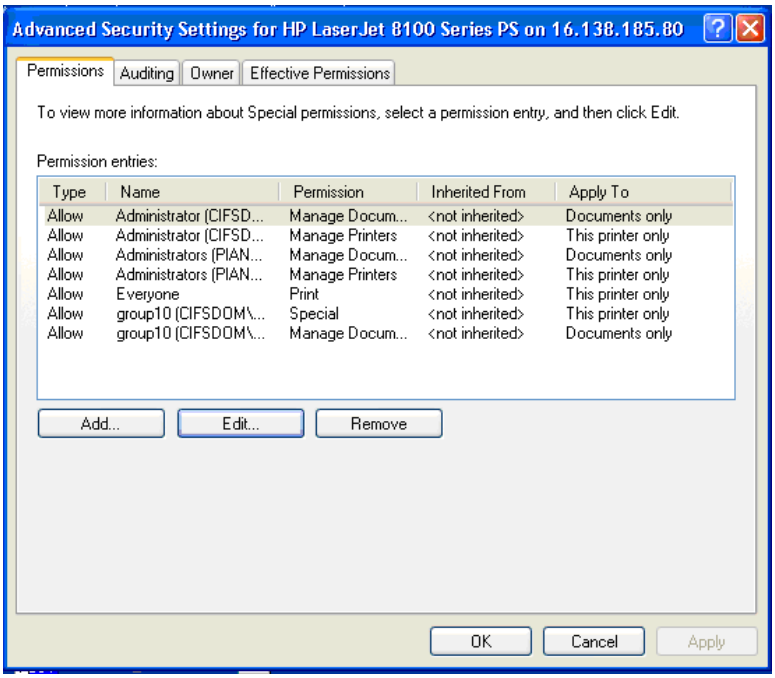
1. Navigate to the HP CIFS Server using an account that has privileges to modify printer security.
2. Open the **Printers and Faxes** folder.
3. Right-click on the printer and select **Properties**.
4. In the **Printer Properties** dialog box, select the **Security** Tab.

Figure 10-6 Security tab



5. Click the **Advanced** button to display the **Advanced Security Settings** dialog box. This dialog box allows you to Add, Modify (Edit), or Remove permissions.

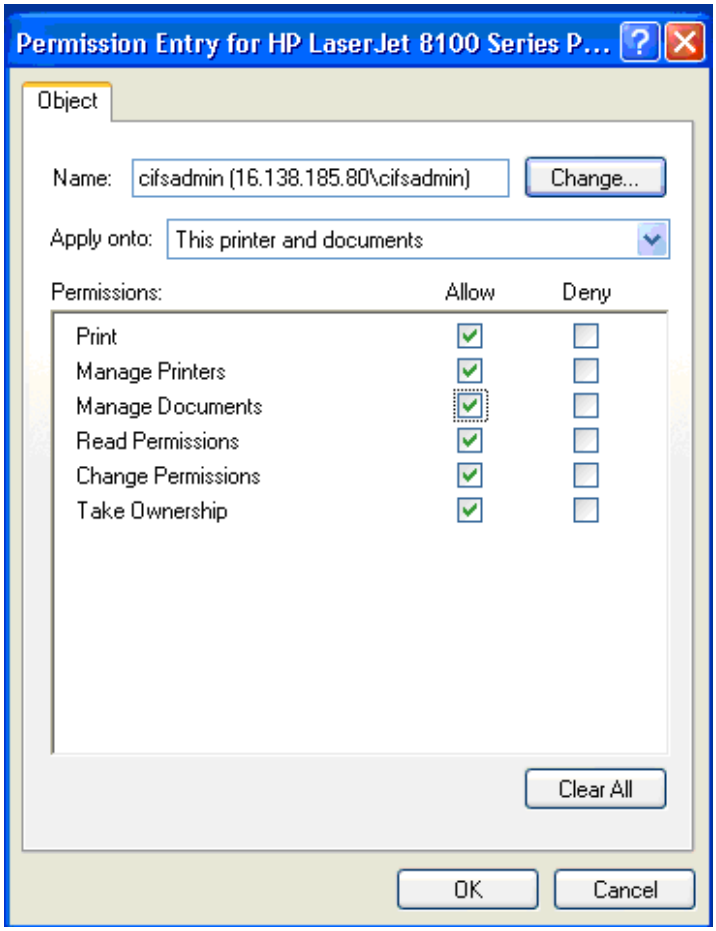
Figure 10-7 Permissions tab



Adding permissions

1. To add permissions, click the **Add...** button to display the **Select User or Group** dialog box. If necessary, select the appropriate account location.
2. Enter the user or group name in the **Enter the object name to select** box and click the **Check Names** button.
3. If there are multiple names, select the required names and click **OK**.
4. Click **OK** on the "**Select Users, Computers, and Groups**" dialog box to display the **Permission Entry** dialog box for the 'object'.

Figure 10-8 Permissions for Printers



5. Select the required permissions.
6. Select the desired entry from the **Apply onto:** drop-down list and click **OK**.
7. In the **Advanced Security Settings** dialog box, click **OK** or **Apply**.

Modifying permissions

1. Select a user or group account and click the **Edit...** button to display the **Permission Entry** dialog box.
2. Modify the permissions.
3. Select the desired entry from the **Apply onto:** drop-down list and click **Ok**.
4. In the **Advanced Security Settings** dialog box, click **OK** or **Apply**.

Removing Permissions

- To remove permissions, select a user or group account, click **Remove** , and then click **Apply**.

6. Click **OK** to exit from **Advanced Security Setting** dialog box.
7. Click **OK** to exit from **Properties…** dialog box for the printer share.

10.8.2 OpenVMS print queue security

OpenVMS security can be used to control access to printers. However, rather than Windows user and group names, security is set using the OpenVMS account and resource identifier names that map to the Windows user or group names, respectively, to which access is to be granted.

If the name of the mapped OpenVMS account or resource identifier is not known, use the WBINFO and supply the domain name and Windows account or group name to which permissions are to be granted. If the account or group is local to the CIFS server, omit the domain name (but see note below). For example, to determine the name of the OpenVMS resource identifier mapped to the group named ACCTNG in the domain named CORPDOM:

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS
$ WBINFO --DOMAINNAME-TO-HOSTNAME=CORPDOM\ACCTNG
```

NOTE:

- The `WBINFO` utility requires the SYSPRV privilege.
- If the user or group exists in the CIFS Server local database, the domain name may be omitted, except for BUILTIN groups such as Administrators, Users. To specify a Built-in group, prefix the group name with "BUILTIN\". For example, to determine the name of the OpenVMS resource identifier mapped to the Administrators group:

  ```
  $ WBINFO --DOMAINNAME-TO-HOSTNAME=BUILTIN\ADMINISTRATORS
  ```

After the name of the OpenVMS account or resource identifier has been identified, use the DCL command `$ SET SECURITY` to modify the security on the appropriate print queue. For more information on managing access to objects and the SET SECURITY command see the *HP OpenVMS Guide to System Security*and the *HP OpenVMS DCL Dictionary Manual*.

11 Tool reference

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

http://samba.org

This chapter describes the following topics:

11.1 HP CIFS management tools

The HP CIFS Server tools enable you to manage the HP CIFS Server. This section includes a list of the HP CIFS management tools:

smbpasswd	Tool for management of the HP CIFS encrypted password database. For more information on using smbpasswd command to change user account password, see Section 8.2.3 (page 111).
pdbedit	Tool for management of the SAM database (Database of CIFS Server user accounts). For more information on managing users using pdbedit utility, see Section 8.2.2 (page 108).
net	Tool for administration of HP CIFS and remote HP CIFS Servers.
wbinfo	Tool for querying `winbind` information.
smbclient	FTP-like client to access SMB/CIFS resources on servers.
smbstatus	Tool provides access to information about the current connections to the HP CIFS Server.
nmblookup	Tool allows NetBIOS name queries to be made from an OpenVMS host.
smbshow	Tool to obtain the information about all the HP CIFS Server processes that are being executed.
smbversion	Tool to obtain information about the various images being used as part of the HP CIFS Server.
SAMBA$DEFINE_COMMANDS.COM	Command procedure to define symbols for all the HP CIFS utilities.
SAMBA$GATHER_INFO.COM	Command procedure to gather information and data files.
testparm	Utility to validate the contents of the `SMB.CONF` file.
tdbbackup	Tool for backing up and for validating the integrity of `samba .tdb` files
tdbdump	Tool for printing the contents of a TDB file.
smbcontrol	To send messages to smbd, nmbd process.
delete_ace	To delete PATHWORKS and Advanced Server ACEs, along with the HP CIFS Server APPLICATION ACE.

tdb_convert	To convert persistent TDB files by using the CONVERT.FDL file.
ods2_convert	Removes escape-encoded characters in file names, changing the file names to ISO-8859-1 characters.
SAMBA$CONFIG.COM	To configure HP CIFS Server for various roles. For more information on the usage of this utility, see Chapter 2 (page 25).
SAMBA$MANAGE_CIFS.COM	To manage shares, users, groups, account policies, and trusts on HP CIFS Server. For more information on using this utility, see Chapter 8 (page 103) and Chapter 9 (page 133)
SAMBA$UPDATEFILEHINTVALUE.COM	To update the file length hint values stored in the ODS-5 file header of files with Variable Length or VFC record formats.

The management tools are available in the SAMBA$ROOT:[BIN] directory and are defined by:

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

11.1.1 net

This tool is used to manage CIFS and remote CIFS servers. The CIFS net utility works similar to 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 the 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*.

11.1.1.1 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 sets time information.
net lookup	Looks up the IP address or host name for a specified host.
net cache	Operates on cache Trivial Database (tdb) file.
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 it is required. The use of this command requires that the *force flag (-f)* is used also. There is no command prompt. Whatever information is input into stdin is stored as the literal machine password. Use this with caution because it overwrites a legitimate machine password without warning.
net status	Displays the machine account status of the local server.

11.1.1.2 Syntax for net lookup

This section only includes the syntaxes for the `net lookup` command.

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

11.1.1.2.1 Examples

Run the following command to get the IP addresses of the 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
```

11.1.2 wbinfo

Use the `wbinfo` tool to get `winbind` information.

The wbinfo utility can be used to obtain detailed domain information, including user and group names, and mappings between domain user and group names and OpenVMS user and resource identifier names.

11.1.2.1 Syntax

`wbinfo [`*`option`*`]`

where:

`options` can be any of the following:

`-u, --domain-users`	Lists all domain users.
`-g, --domain-groups`	Lists all domain groups.
`-h, --domainname-to-hostname=NAME`	Converts domain-name to host-name
`-H, --hostname-to-domainname=HOSTNAME`	Maps hostname to domainname
`-o, --hostgroups-to-domaingroups`	Maps all CIFS hostgroups to domaingroups
`-O, --hostusers-to-domainusers`	Maps all CIFS hostusers to domainusers
`-D, --domain-info=STRING`	Displays information about the domain.
`-r, --user-groups=USER`	Gets user groups.
`--user-domgroups=SID`	Gets user domain groups.
`-a, --authenticate=user%password`	Authenticate user.
`--getdcname=domainname`	Gets a DC name for a foreign domain.
`-p, --ping`	Pings WINBINDD to see if it is alive.
`-K, --krb5auth=user%password`	Authenticates user using Kerberos

NOTE: The options **`--hostusers-to-domainusers`**, **`--hostgroups-to-domaingroups`** and **`--hostname-to-domainname`** can be used irrespective of whether WINBIND is disabled (by defining WIBINDD_DONT_ENV to 1) or not. The remaining options can be used only if WINBIND is enabled.

Help Options

`-?, –help`	Shows 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.

11.1.2.2 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
```

11.1.2.2.1 WBINFO --domainname-to-hostname

To find the mapped OpenVMS user account name or the resource identifier name for a CIFS domain user or group account, execute the command:

```
$ wbinfo --domainname-to-hostname=<CIFS-domain-account>
```

where:

<CIFS-domain-account> is a user or a group account in the HP CIFS Server account database, or a user or a global group account in a domain, where the HP CIFS Server is a Member Server, or a user or a global group account in the trusted domain irrespective of the role of the HP CIFS Server.

Except for the accounts existing in the HP CIFS Server account database, the *<CIFS-domain-account>* must be of the format <DOMAINAME>\<ACCOUNT-NAME>.

For example, to find a mapped OpenVMS user account for a user “Administrator” existing in the domain CIFSDOM, where CIFS Server is a Member Server, execute:

```
$ wbinfo --domainname-to-hostname=CIFSDOM\Administrator
CIFS$3E8
```

If the user or the group exists in the HP CIFS Server local database, the domain name may be omitted, except for BUILTIN groups such as Administrators and Users. To specify a built-in group, prefix the group name with `BUILTIN\`.

For example, to determine the name of the OpenVMS resource identifier mapped to the Administrators group:

```
$ wbinfo --domainname-to-hostname=BUILTIN\Administrators
CIFS$ADMINISTRATORS
```

11.1.2.2.2 WBINFO --hostusers-to-domainusers

The `--hostusers-to-domainusers` option, displays the CIFS domain users and their mapped OpenVMS usernames:

```
$ wbinfo --hostusers-to-domainusers
```

```
$ wbinfo --hostusers-to-domainusers
CIFSADMIN                                PIANO\cifsadmin
GANGA                                    PIANO\ganga
CIFS$3E8                                 CIFSDOM\Administrator

3 VMS users are currently mapped to CIFS domain users
```

11.1.2.2.3 WBINFO --hostgroups-to-domaingroups

The **`--hostgroups-to-domaingroups`** option displays the CIFS domain groups and their mapped OpenVMS resource identifiers.

```
$ wbinfo --hostgroups-to-domaingroups
CIFSUSERS                                PIANO\cifsusers
PLAYERS                                  PIANO\players
CIFS$GRP1388                             CIFSDOM\Domain Users
CIFS$GRP1389                             CIFSDOM\Enterprise Admins
CIFS$GRP138A                             CIFSDOM\Domain Admins
CIFS$GRP138B                             CIFSDOM\Group Policy Creator Owners
CIFS$GRP138C                             CIFSDOM\Schema Admins
CIFS$GRP138D                             CIFSDOM\test_grp
CIFS$PRINTOPERATORS                BUILTIN\Print Operators
CIFS$GUESTS                              BUILTIN\Guests
CIFS$USERS                               BUILTIN\Users
CIFS$ADMINISTRATORS               BUILTIN\Administrators

12 VMS resource identifiers are currently mapped to CIFS domain groups.
```

11.1.2.2.4 WBINFO --hostname-to-domainname

To find the CIFS domain user or group account that is mapped to an OpenVMS user account or a resource identifier, execute the command:

```
$ wbinfo --hostname-to-domainname=<OpenVMS-identifier>
```

where:

<OpenVMS-identifier> is either an OpenVMS user account name or resource identifier name.

For example, execute:

```
$ wbinfo --hostname-to-domainname=CIFS$3E8
CIFSDOM\Administrator   - USER

$ wbinfo --hostname-to-domainname=CIFS$GRP1388
CIFSDOM\Domain Users    - GROUP

wbinfo --domain-info
$ wbinfo --domain-info=cifsdom
Name                 : CIFSDOM
Alt_Name            : cifsdom.ind.hp.com
SID                  : S-1-5-21-160935111-2493731623-2036278074
Active Directory  : Yes
Native              : No
Primary              : Yes
Sequence            : 53966
```

11.1.3 smbclient

`smbclient` is a client that can 'talk' to an SMB or CIFS server. It provides an interface similar to that of the FTP program. Operations include functions, such as getting 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.

11.1.3.1 Syntax

```
SAMBA$SMBCLIENT.EXE service <options>
```

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

-R, --name-resolve=NAME-RESOLVE-ORDER	Uses these name resolution services only.
-M, --message=HOST	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	Writes messages to stderr instead of stdout.
-L, --list=HOST	Gets 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	Sets 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	Changes to initial directory before starting.
-c, --command=STRING	Executes semicolon separated commands.
-b, --send-buffer=BYTES	Changes the transmit or send buffer size.
-p, --port=PORT	This number is the TCP port number that is used when making connections to the server.
-g, --grepable	Produces grepable output.

Help Options

-?, --help	Shows this help message.
--usage	Displays a brief usage message.

Common CIFS Options

The following is a list of the 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.

Connection Options

-O, --socket-options=SOCKETOPTIONS	TCP socket options to set on the client socket.

-n, --netbiosname=NETBIOSNAME	Primary NetBIOS name.
-W, --workgroup=WORKGROUP	Sets the workgroup name.
-i, --scope=SCOPE	Specifies a NetBIOS scope that nmblookup uses to communicate with when generating NetBIOS names.

Authentication Options

-U, --user=USERNAME	Sets the network user name.
-N, --no-pass	Does not prompt for password.
-k, --kerberos	Tries to authenticate with Kerberos. Only useful in an Active Directory environment.
-A, --authentication-file=FILE	Gets the credentials from a file.
-S, --signing=on|off|required	Sets the client signing state.
-P, --machine-pass	Uses stored machine account password.

11.1.3.2 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
  ---------            -------
  CIFSCLUSTER          CIFS for OpenVMS 3.0.24
  HOMERJ               CIFS for OpenVMS 3.0.24
  HOMERJ_ALIAS         CIFS for OpenVMS 3.0.24

  Workgroup            Master
  ---------            -------
  CIFSDOM
```

11.1.4 smbstatus

`smbstatus` is a simple program that lists the current Samba connections.

11.1.4.1 Syntax

`smbstatus <`*`options`*`>`

where:

`options` can be any of the following

`-p, --processes`	Prints a list of processess.
`-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 the user name only.
`-b, --brief`	Gives a brief output.
`-P, --profile`	Prints only the contents of the profiling shared memory area if Samba is compiled with the profiling option.
`-B, --byterange`	Causes smbstatus to include byte range locks.
`-n, --numeric`	Numeric UID or GID.

Help Options

`-?, --help`	Shows 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. 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.

11.1.4.2 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
```

11.1.5 nmblookup

`nmblookup` is used to query NetBIOS names and map them to the IP addresses in a network using NetBIOS over TCP/IP queries.

11.1.5.1 Syntax

`nmblookup <`*`options`*`>`

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

`-B, --broadcast=BROADCAST-ADDRESS`	Specifies address to use for broadcasts.
`-f, --flags`	Lists the NMB flags returned.
`-U, --unicast=STRING`	Specifies the address to use for unicast.
`-M, --master-browser`	Searches for a master browser.
`-R, --recursion`	Sets the recursion desired in package.
`-S, --status`	After the name query has returned an IP address then do a node status query as well.
`-T, --translate`	Translates the IP addresses into names.
`-r, --root-port`	Uses the root port 137 (Windows 95 only replies).
`-A, --lookup-by-ip`	Interprets *<name>* as an IP Address and queries the node status on this address.
`-?, --help`	Shows this help message.
`--usage`	Displays a brief usage message.
`-d, --debuglevel=DEBUGLEVEL`	Sets the debug level
`-s, --configfile=CONFIGFILE`	Uses an alternate configuration file.
`-l, --log-basename=LOGFILEBASE`	Base name for log files.
`-V, --version`	Prints the program version number.
`-O, --socket-options=SOCKETOPTIONS`	TCP socket options to set on the client socket.
`-n, --netbiosname=NETBIOSNAME`	Primary NetBIOS name.
`-W, --workgroup=WORKGROUP`	Sets the workgroup name.
`-i, --scope=SCOPE`	Specifies a NetBIOS scope that `nmblookup` uses to communicate when generating the NetBIOS names.

Help Options

`-?, --help`	Shows this help message.
`--usage`	Displays a 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 the 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.
Connection Options	
-O, --socket-options=SOCKETOPTIONS	TCP socket options to set on the client socket.
-n, --netbiosname=NETBIOSNAME	Primary NetBIOS name.
-W, --workgroup=WORKGROUP	Sets the workgroup name.
-i, --scope=SCOPE	Specifies a NetBIOS scope that `nmblookup` uses to communicate when generating the NetBIOS names.

11.1.5.2 Examples

Run the following command to send a NetBIOS Node Status query to the IP address specified. A list of NetBIOS name registered by that system is displayed.

```
$ 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
```

11.1.6 smbshow

This tool displays system information about all the HP CIFS Server processes. When you start HP CIFS Server, an NMBD process is created. As each client establishes a session with the server, a new SMBD process is created.

11.1.6.1 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
```

11.1.7 Smbversion

This tool is used to get the information about the various images being used as part of the HP CIFS Server.

11.1.7.1 Example

```
$ smbversion

Information on ANDICE for OpenVMS images installed on this system:

Image Name                     Image Version    Link date          Linker ID
------------------------------ ---------------- -----------------  -------------
SAMBA$ADD_DSKSHARE              V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$ADD_PRNFORM               V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$ADD_PRNQUEUE              V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$ADD_PRNSHARE              V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$DELETE_PWRKACE            V1.1-010-PS010    17-FEB-2010 12:34  I02-31
SAMBA$IMPORTPWD                 V1.1-010-PS010   17-FEB-2010 12:34  I02-31
SAMBA$NET                       V1.1-010         9-FEB-2009 13:52  I02-31
SAMBA$NMBD                      V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$NMBLOOKUP                 V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$NTLMAUTH                  V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$PDBEDIT                   V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$PROFILES                  V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$RPCCLIENT                 V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SHR                       V1.1-010-PS010   17-FEB-2010 12:34  I02-31
SAMBA$SMBCACLS                  V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SMBCLIENT                 V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SMBCONTROL                V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SMBCQUOTAS                V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SMBD                      V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SMBPASSWD                 V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SMBSPOOL                  V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SMBSTATUS                 V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SMBTREE                   V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$SWAT                      V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$TDBBACKUP                 V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$TDBDUMP                   V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$TDBTOOL                   V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$TDB_CONVERT               V1.1-010-PS010   17-FEB-2010 12:34  I02-31
SAMBA$TDB_MIGRATION              V1.1-010          9-FEB-2009 13:53  I02-31
SAMBA$TESTPARM                  V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$WBINFO                    V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$WINBINDD                  V1.1-010          9-FEB-2009 13:52  I02-31
SAMBA$ODS2                      V1.1-010-PS010   17-FEB-2010 12:34  I02-31
SAMBA$STREAMLF                  V1.1-010          9-FEB-2009 13:53  I02-31
SAMBA$VARVFC                    V1.1-010-PS010   17-FEB-2010 12:34  I02-31
SAMBA$VTF                       V1.1-010         9-FEB-2009 13:53   I02-31
```

11.1.8 SAMBA$DEFINE_COMMANDS.COM

This command procedure defines symbols for all the HP CIFS utilities. It also defines symbols such as `SMBSTART, SMBSTOP, SMBSHOW,`, and `SMBVERSION`.

To define the symbols:

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

11.1.9 SAMBA$GATHER_INFO.COM

This command procedure 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 tdbs can be fetched from the save set for debugging purpose.

11.1.10 testparm

The `testparm` utility is a program to test the contents of the `SMB.CONF` file. Whenever you modify the `SMB.CONF` file you need to run the `testparm` utility. The `testparm` utility examines the `SMB.CONF` file for syntax errors and reports them and 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.

11.1.10.1 Syntax

```
testparm <options>
```

where:

options can be any of the following

-s, --suppress-prompt	Without this option, `testparm` prompts for a carriage return after printing the service names and before dumping the service definitions.
-v, --verbose	Gives a verbose output.
--show-all-parameters	Shows the parameter, type, and possible values.
--parameter-name=STRING	Limit `testparm` to a named parameter.
--section-name=STRING	Limit `testparm` to a named section.

Help Options

-?, --help	Shows this help message.
--usage	Displays brief usage message.

Common CIFS Options

-V, -version	Prints the program version number.

11.1.10.2 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 bcast
        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
```

11.1.11 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 before starting the HP CIFS Server or during normal operation. If the tool detects any file damage and it finds a previous backup, the backup file is 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 the HP CIFS operation. To use this command:

```
tdbbackup [-s suffix] *.tdb
```

Before restarting the HP CIFS Server, the following command may be run to validate the `.tdb` files:

```
tdbbackup -v [-s suffix] *.tdb
```

11.1.11.1 Syntax

tdbbackup <*options*>

where:

options can be any of the following

-h	Gets help information.
-s suffix	Allows the administrator to specify a file back-up extension.
-v	Checks the database for damages (corrupt data) which if detected causes the backup to be restored.
-n	Sets the new hash size for the backup.

Example 11-1 Examples for tdbbackup

To back up all the TDB files in the `samba$root:[private]` directory:

```
$ tdbbackup samba$root:[private]*.tdb


The backup of the TDB file samba$root:[private]passdb.tdb is samba$root:[private]passdb.tdb_bak
The backup of the TDB file samba$root:[private]secrets.tdb is samba$root:[private]secrets.tdb_bak
```

By default, the `tdbbackup` utility appends `_BAK` to a `TDB` filename to create a TDB backup file name. A TDB backup file can be created with another suffix by using **`-s`** option. For example, to create a TDB backup file with `_OLD` suffix:

```
$ tdbbackup -s _old samba$root:[private]*.tdb
The backup of the TDB file samba$root:[private]passdb.tdb is samba$root:[private]passdb.tdb_old
The backup of the TDB file samba$root:[private]secrets.tdb is samba$root:[private]secrets.tdb_old
```

To check the validity of a TDB file:

```
$ tdbbackup –v samba$root:[private]passdb.tdb
samba$root:[private]passdb.tdb : 5 records
```

11.1.12 Tdbdump

Tdbdump is a utility that 'dumps' the contents of a TDB file to a standard output in a human-readable format. This tool can be used when debugging problems with TDB files.

11.1.12.1 Syntax

`tdbdump <`*`options`*`>`

where:

`options` can be any of the following

`-h` Gets help information.

`-k keyname` Dumps the value of the keyname.

11.1.13 smbcontrol

`smbcontrol` sends messages to the NMBD or an SMBD process.

11.1.13.1 Syntax

`smbcontrol [OPTION...] <destination> <message-type> <parameters>`

where:

`options` can be any of the following

`-t, --timeout=TIMEOUT` Sets timeout value in seconds.

Help Options

`-?, --help` Shows this help message.

`--usage` Displays brief usage message.

Common CIFS Options

The following is a list of the common CIFS options:

-l, -log-basename=LOGFILEBASE Specifies base name for log files. The extension `.progname`is appended (for example, `log.smbclient`, `log.smbd`, and so on).

`<destination>` is the process name or 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:

This does not affect client connections to any other shares. This message-type takes an argument of the share name for which client connections are closed, or the "*" character, which closes all currently open shares. This may be useful if you have made changes to the access controls on the share. This message can only be sent to `smbd`.

debug Sets the 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 Sends the 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 Changes 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 Requests the debug level of a certain daemon and write it to stdout.

profilelevel Requests the profile level of a certain daemon and write it to stdout.

printnotify Orders `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 Sends a queue pause change notify message to the printer specified.

queueresume printername Sends a queue resume change notify message for the printer specified.

jobpause printername unixjobid Sends a job pause change notify message for the printer and unix jobid specified.

jobresume printername unixjobid Sends a job resume change notify message for the printer and unix jobid specified.

jobdelete printername unixjobid Sends a job delete change notify message or the printer and unix jobid specified.

NOTE: 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.

shutdown	Shuts down the specified daemon. Can be sent to both smbd and nmbd.
drvupgrade	Forces clients of printers using specified driver to update their local version of the driver. Can only be sent to smbd.
reload-config	Forces daemon to reload the `SMB.CONF` configuration file.

Example 11-2 Examples for smbcontrol

```
$ smbshow
0004E32D NMBD              LEF      6      747   0 00:00:00.15       826    1063
0004E334 SMBD445_BG1309   LEF      7     2366   0 00:00:00.79      1408  1762  N

$ smbcontrol SMBD445_BG1309 ping
PONG from pid 320308

$ smbcontrol 0004E334 ping
PONG from pid 320308
```

To increase the log (debug) level of a process to 5 as an example, execute:

```
$ smbcontrol SMBD445_BG1309 debug 5
```

To verify current log (debug) level of a process:

```
$ smbcontrol SMBD445_BG1309 debuglevel -d0
PID 320308: all:5 tdb:5 printdrivers:5 lanman:5 smb:5
rpc_parse:5 rpc_srv:5 rpc_cli:5 passdb:5
sam:5 auth:5 winbind:5 vfs:5 idmap:5 quota:5 acls:5 locking:5 msdfs:5 dmapi:5
```

To reload CIFS Server configuration file:

```
$ smbcontrol SMBD445_BG1309 reload-config
```

To shutdown a CIFS Server process, execute:

```
$ smbcontrol SMBD445_BG1309 shutdown
```

11.2 Converting encoded file names from ODS-2 to ODS-5

The existing HP OpenVMS CIFS shares may be converted from ODS-2 to ODS-5 to take advantage of the OpenVMS support of extended file specifications. The HP OpenVMS CIFS software provides a conversion utility for converting ODS-2 encoded file names on ODS-5 devices that have been converted from ODS-2. The conversion utility removes escape-encoded characters in file names, changing the file names to ISO-8859-1 characters.

For example, if a file name is created on an ODS-2 disk containing the character-encoding sequence *_ _E4,* to represent the lowercase a-umlaut (*ä*), the conversion utility removes the encoding and replaces it with the *ä* character.

You can convert the ODS-2 file names to ODS-5 file names after completing the following tasks:

- Installing and configuring the HP OpenVMS CIFS.
- Converting the disk device containing escape-encoded file names from ODS-2 to ODS-5. For information about converting disk devices to ODS-5, see the *OpenVMS Guide to Extended File Specifications*.

NOTE: The conversion utility provided by HP OpenVMS CIFS can convert the escape-encoded characters in file names, only if the resulting character is either an ASCII or an extended ASCII character.

11.2.1 Using the file name conversion utility

The file name conversion utility that converts file names from the encoding used on ODS-2 file systems to ISO-8859-1 file names is:

```
SAMBA$ROOT:[BIN.<ARCH_TYPE>]SAMBA$ODS2_CONVERT.EXE
```

where:

ARCH_NAME is either “ALPHA” or “IA64” depending on the OpenVMS system architecture.

When the Samba commands have been defined, you can use the ODS2_CONVERT system management command to invoke the file name conversion utility.

To manually define the ODS2_CONVERT command, enter the following DCL command:

```
$ ODS2_CONVERT :== SAMBA$ROOT:[BIN.<ARCH_NAME>]SAMBA$ODS2_CONVERT.EXE
```

where:

ARCH_NAME is either “ALPHA” or “IA64” depending on the OpenVMS system architecture.

11.2.2 ODS2_CONVERT

The ODS2_CONVERT utility supports encoded file name character conversion to ASCII and extended ASCII characters.

11.2.2.1 Syntax

$ ODS2_CONVERT /qualifiers file-spec

where:

- ***qualifiers*** are optional. They are described in Table 11–1. The default setting is used if you omit the qualifier.
- ***file-spec*** argument is required, and may include the device name, directory name, and file name.
  - If you specify only a disk device, the conversion utility scans the entire device for file names that are encoded, and converts them, if necessary.
  - If you specify a disk device and a directory, all the files in the specified directory are scanned and converted, if necessary. You may include wildcard characters in directory names and file names.
  - If you specify a disk device, a directory, and a single file name, only that file is converted.
  - If you enter the ODS2_CONVERT command with no file specification, it prompts you for a file specification.

    For example:

    ```
    $ ODS2_CONVERT

    FILENAME:
    ```

    At the FILENAME prompt, you must supply a device name, and optionally a directory and a file name to convert. You may include qualifiers.

Table 11-1 ODS2_CONVERT Qualifiers

Qualifier	Description	Default
/DISABLE=*keyword*	Disables the function of the conversion utility specified by the keyword. The keyword is `STRUCTURE_LEVEL`, which specifies that the conversion utility does not check the file system type (ODS-2 or ODS-5).	/NODISABLE
/LOG=*log-filespecification*	Creates a log file containing the file names converted. You can specify the location and name of the log file using this qualifier.	/NOLOG. Information is displayed but no log file is created.
/VERBOSE	Displays all the file names scanned during the conversion operation.	/NOVERBOSE
/NOLIST	Suppresses the display of all the file names that are converted. Only error messages are displayed.	/LIST

11.2.3 Examples

Example 11-3 Example of converting an encoded file name

In this example, the file named A FILE.TXT has been created by a Windows client on DISKA, and has been encoded as A_ _20FILE.TXT. The device DISKA has been converted from ODS-2 to ODS-5. In an OpenVMS system, the file is displayed as follows:

```
$ DIRECTORY DISKA:[FILES]
Directory DISKA:[FILES]
.
.
.
A__20FILE.TXT
$
```

Use the PWCONVERT command to convert this file name, as follows:

```
$ ODS2_CONVERT/VERBOSE DISKA:[FILES]A__20FILE.TXT
```

The ODS2_CONVERT utility supports encoded file name character conversion to ASCII and extended ASCII characters.

```
Scanning file - DISKA:[FILES]A__20FILE.TXT;1
Renamed A__20FILE.TXT to A FILE.TXT
Convert Utility Complete
$
```

Example 11-4 Example of converting all encoded file names

To convert all the encoded file names on a disk device and directory, enter the ODS2_CONVERT command, specifying the disk device and directory without a file name. For example, to convert all the encoded file names stored on device DISK$USER1, enter the following:

```
$ ODS2_CONVERT/VERBOSE DISKA:[FILES]A__20FILE.TXT
```

The ODS2_CONVERT utility supports encoded file name character conversion to ASCII and extended ASCII characters.

```
FILENAME: DISK$USER1:
Renamed A__20FILE.TXT to A FILE.TXT
.
.
.
Convert Utility Complete
```

11.2.4 delete_ace

The delete_ace utility deletes all PATHWORKS or Advanced Server for OpenVMS ACEs, as well as the APPLICATION ACE applied by the HP CIFS Server without changing the modified date and time of the file.

To use this utility, define a symbol such as:

```
$ delete_ace :== $SAMBA$EXE:SAMBA$DELETE_ACE.EXE
```

Or execute:

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

To delete a PATHWORK or SAMBA ACE, execute:

```
$ delete_pwrkace <p1 parameter> <p2 parameter>
```

The <p1 parameter>accepts most valid OpenVMS file specification formats such as:

```
dka100:[test...]
dka100:[test.testing]temp.doc
```

```
dka100:[test]*.*,dka200:[temp]*.*
dka100:[test...]*.*;*
dka100:[test.testing]temp.doc,tester.doc
```

The <p2 parameter> can be any of the following:

- pwrk — To delete PATHWORKS and Advanced Server ACES (default).
- samba — To delete the HP CIFS Server ACE.

NOTE: This utility permanently deletes PATHWORKS and Advanced Server ACEs. Use this utility cautiously in an OpenVMS cluster where other cluster nodes continue to run PATHWORKS or Advanced Server or in environments migrating from PATHWORKS or Advanced Server to HP CIFS Server.

Example 11-5 Examples for delete_ace

To delete PATHWORKS and Advanced Server ACEs on all the files in a particular directory, execute:

```
$ delete_ace dka100:[test]*.* pwrk
```

To delete CIFS Server (SAMBA) ACE on a particular file, execute:

```
$ delete_ace dka100:[test.testing]temp.doc samba
```

11.2.5 tdb_convert

The tdb_convert utility converts the existing persistent TDB files by using the values present in the `samba$root:[lib]convert.fdl` file. The `CONVERT.FDL` file can be modified to contain optimized FDL values.

NOTE: The `CONVERT.FDL` file must be modified with caution otherwise any incorrect values in it can create an unusable TDB file after conversion.

If the HP CIFS Server was configured by default using the `SAMBA$CONFIG.COM` file, a `SAMBA$ROOT:[LIB]CONVERT.FDL` file is created by the HP CIFS Server as part of the configuration. If there is no `CONVERT.FDL` file in the directory `SAMBA$ROOT:[LIB]`, edit the `SAMBA$ROOT:[LIB]CONVERT.FDL` file and paste the contents between the lines `<Data begin>` and `<Data end>` while excluding these two lines:

```
<Data begin>
SYSTEM
        SOURCE                  "OpenVMS"

FILE
        ORGANIZATION              indexed
        PROTECTION                (system:RWD, owner:RWD, group:, world:)
        GLOBAL_BUFFER_COUNT        0
        GLBUFF_CNT_V83            200
        GLBUFF_FLAGS_V83         none

RECORD
        CARRIAGE_CONTROL          carriage_return
        FORMAT                    variable
        SIZE                      0

AREA 0
        ALLOCATION                 240
        BEST_TRY_CONTIGUOUS           yes
        BUCKET_SIZE                4
        EXTENSION                  80
```

```
AREA 1
        ALLOCATION                  48
        BEST_TRY_CONTIGUOUS            yes
        BUCKET_SIZE                 4
        EXTENSION                   48

KEY 0
        CHANGES                     no
        DATA_AREA                   0
        DATA_FILL                   100
        DATA_KEY_COMPRESSION           no
        DATA_RECORD_COMPRESSION        yes
        DUPLICATES                  no
        INDEX_AREA                  1
        INDEX_COMPRESSION            no
        INDEX_FILL                  100
        LEVEL1_INDEX_AREA             1
        NAME                        "TDBHASH.1/16"
        PROLOG                      3
        SEG0_LENGTH                  16
        SEG0_POSITION                0
        TYPE                         string

<end of data>
```

NOTE:

- For OpenVMS version 8.2 or 8.2-1, the following two lines must be removed from the `convert.fdl` file:

  ```
  GLBUFF_CNT_V83            200
  GLBUFF_FLAGS_V83         none
  ```

- For OpenVMS version 8.2 or 8.2-1, the global buffer count value can be set using the following field:

  ```
  GLOBAL_BUFFER_COUNT      60
  ```

To convert the TDB file:

1. Edit the `samba$root:[lib]convert.fdl` file to modify the required values and save it.

   For example, in order to reduce the number of global sections used by the HP CIFS Server, you may want to reduce the “GLBUFF_CNT_V83” to 50.

   To do this, change the value of “GLBUFF_CNT_V83” to 50 in the `samba$root:[lib]convert.fdl` file.

2. Execute the following commands:

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

   $ TDB_CONVERT SAMBA$ROOT:[<subdir>]<TDB-File-Name>

   where:

   - <subdir> — PRIVATE or VAR.LOCKS.
   - <TDB-File-Name> — Any of the persistent TDB filenames.

   For example, to convert `passdb.tdb` file that is present in the `samba$root:[private]` directory:

   ```
   $ TDB_CONVERT SAMBA$ROOT:[PRIVATE]PASSDB.TDB
   ```

   For more information on persistent TDB files, see Chapter 10 (page 147)

11.3 Updating the hint value of VAR or VFC files

For sequential VAR and VFC files on an ODS–5 disk, OpenVMS provides file length values to indicate the actual data and number of records in the file. This feature is useful while enumerating these files, as the SMBD process need not read the entire file to calculate the file size, but just has to use these hint values. The disadvantage is that these hint values can become invalid. When the SMBD process tries to enumerate these files and if the hint values are invalid, it has to read the entire file content to calculate the actual file size. This can slow down the performance of the SMBD process for the VAR and VFC files.

The HP OpenVMS CIFS software kit includes a utility called `SAMBA$UPDATEFILEHINTVALUE.COM` to update the file hint value of VAR and VFC files.

This utility can go through each file in the file share paths (from `SMB.CONF`) that are present on the ODS–5 disk and identify if they are of sequential VAR and VFC format. If the files are in the sequential VAR and VFC format and if the file length hint values for the file are invalid, the utility calls the `analyze/rms/update_header` command to update the file length hint value for the file.

NOTE: The `SAMBA$UPDATEFILEHINTVALUE.COM` script can be either run interactively or through a batch script at periodic intervals in order to update the hint value, so that SAMBA does not have to read the entire file content to find the file size.

The location of the utility file is: `SAMBA$ROOT:[BIN]SAMBA$UPDATEFILEHINTVALUE.COM`.

Syntax

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

The results obtained are stored in the following files:

`samba$root:[var]FileHintUpdate.output` : Contains the detailed output of the analyze command execution.

`samba$root:[var]FileHintUpdatefile.list`: Contains the list of filenames that are VAR and VFC files, which are updated with the correct hint value.

Example 11-6 Updating File Hint Value of VAR and VFC files

This example shows the execution of the SAMBA$UPDATEFILEHINTVALUE.COM utility to update the hint values of VAR and VFC files.

```
$ @SAMBA$UPDATEFILEHINTVALUE.COM

****************************************
Script to update the File Hint Value of the VAR  &  VFC files
****************************************
Following are the share paths found in smb.conf
        path = DKA100:[SAMBA.523]
        path = DKA100:[SAMBA.510]
        path = DKA100:[SAMBA.511]

****************************************
Analysing each share path
****************************************
Results
****************************************
Following  VAR  & VFC  files have been updated
----------------------------------------
DKA100:[SAMBA.523]OUTFILE_ VFC .TXT;1
DKA100:[SAMBA.523.VAR]SAMBA$INFO.TXT;3
DKA100:[SAMBA.523.VAR]SAMBA$NMBD_AQUILA.LOG;35
DKA100:[SAMBA.523.VAR]SAMBA$SMBD_STARTUP.LOG;4458
DKA100:[SAMBA.510]OUTFILE_ VFC1 .TXT;1
DKA100:[SAMBA.511]OUTFILE_ VFC2 .TXT;1

----------------------------------------
****************************************
Please find the detailed log in samba$root:[var]FileHintUpdate.output.
```

12 Performance considerations and troubleshooting techniques

This chapter addresses the following topics:

12.1 Hosting SAMBA$ROOT directory on a non-system disk

Hosting the `SAMBA$ROOT` directory tree on a system disk can degrade the HP CIFS Server performance due to heavy usage of the system disk by the Operating System. Because of this, it is recommended to install the HP CIFS Server on a non-system disk using the /DESTINATION qualifier of the `PRODUCT INSTALL` command. If the `SAMBA$ROOT:` directory tree is already hosted on the system disk, follow the instructions provided in Section 2.8 (page 33).

12.2 Directory enumeration performance

Directory enumeration performance is most affected by the share-level configuration parameter, *vms path names*. When enabled (the default), the HP CIFS Server provides improved performance when listing directories on both ODS-2 and ODS-5 volumes. Unless recommended by HP, do not disable the *vms path names* parameter.

12.3 Tuning disk volumes

1. To improve write performance, disable the volume highwater marking:
   a. Include the /NOHIGHWATER_MARKING qualifier while initializing the volume.
   b. If the volume is already initialized, execute the following command to set the volume to highwater marking:

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

      The change will not take effect until the volume is remounted.
2. Specify the disk cluster size as a multiple of 16. You can do this during the disk initialization using the /CLUSTER_SIZE qualifier of the `INITIALIZE` command.
3. Add the following line in the `SAMBA$ROOT:[BIN]SAMBA$SMBD_STARTUP.COM` file:

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

   where n is:

   - 124 for EVA
   - 96 for XP
   - 127 for all other disk types

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

4. Use ODS-5 volumes rather than ODS-2.

   File headers of files with variable length or VFC record formats on ODS-5 volumes contain additional file length hint values that assist the HP CIFS Server in determining the number of data bytes in the file.

   When the file length hint values are not present or are not valid, the HP CIFS Server must read the entire file just to determine the size displayed on Windows clients.

12.4 Updating file length hint values

Execute the following command procedure periodically to update the file length hint values of variable-length record formatted files.

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

For more information, see Section 11.3 (page 187).

12.5 CIFS Server ACE

From HP CIFS Server version 1.2 onwards, the HP CIFS Server stores the file size of files with a record format other than `Stream` or `Stream_LF` in an application ACE that is stored on the file. When reading such files for the first time (excluding files with a variable length record format that have valid file length hint values), the HP CIFS Server calculates the file size by reading the entire file contents. The calculated file size is then stored in the HP CIFS Server ACE and is applied on the file. Unless the file is modified, the HP CIFS Server obtains the file size from the HP CIFS Server ACE existing on the file, thereby improving performance. After the file is modified, the file size is calculated again and stored in the ACE. Though the `DELETE_ACE` utility can delete the HP CIFS Server ACE on a file, unless required, it is not recommended to delete the HP CIFS Server ACE.

NOTE: The HP CIFS Server ACE can additionally store the DOS attributes, if they are enabled.

12.6 vms estimate file size parameter

With certain OpenVMS files formats, the HP CIFS Server might be required to read the entire contents of the file to determine its size. As a result, the enumeration of a directory containing such files might be slower than expected. File formats EXCEPT the following are subject to this behavior:

- Sequential files with Stream or Stream_LF record formats (on both ODS-2 and ODS-5 volumes).
- Sequential files with Fixed Length record format, an even-numbered record size, and record attributes of `None` or `Carriage return carriage control` (on both ODS-2 and ODS-5 volumes).
- Sequential files with Variable Length or VFC record formats on ODS-5 volumes (only) whose file header contains valid file length hint values.

The slower performance may only be temporary as the HP CIFS Server applies an APPLICATION ACE on the file in which it stores the calculated file size. Thereafter, the file size is obtained from this APPLICATION ACE and the ACE is updated whenever a client modifies the file.

However, if the file is subsequently modified by an OpenVMS application other than the HP CIFS Server, this APPLICATION ACE will be invalidated, requiring the HP CIFS Server to read the entire file again to calculate its size. Also, if the content of a directory containing such files changes often, the APPLICATION ACE may not provide the desired performance improvement.

Therefore, if the problem is persistent, it might help to configure the share to estimate the size of such files. When the share parameter *vms estimate file size* is enabled by setting it to `YES`, the HP CIFS Server estimates the size of these files using the values stored in their file header, significantly improving the directory enumeration performance. The *vms estimate file size* share parameter may be included in the individual share sections or placed in the [GLOBAL] section of the configuration file to affect all shares (which does not have an explicit *vms estimate file size* entry in their share section).

When a client is enumerating the directory contents, if the directory contains one or more very large sized files whose contents needs to be read to determine the file size, the client may timeout while the HP CIFS Server is determining the file size. In this case, enabling the *vms estimate file size* can improve the directory enumeration performance.

WARNING! The size calculated from the file header data will always be greater than the size calculated by the HP CIFS Server by reading the entire file contents. Therefore, when enabling the *vms estimate file size* parameter, customers are advised to verify if the client applications that access these files are able to function without any adverse effect. If the client applications are adversely affected, other options, such as moving the files to ODS-5 volumes, must be explored.

12.7 vms open file caching parameter

From HP OpenVMS CIFS version 1.2 onwards, two new HP CIFS Server-specific share configuration parameters are provided:

- *vms open file caching*
- *vms ofc time interval*

The *vms open file caching* share parameter controls the Open File Caching (OFC) feature provided by the HP CIFS Server. By default, this feature is disabled. When OFC is enabled, the HP CIFS performance may improve considerably when serving a file, which is repeatedly opened and closed in quick succession. For example, clients executing DOS batch files, such as login scripts, stored on the server. Files remain open on the server for a specified period after the last client accessing the file closes it. This cache is similar to the OFC used by Advanced Server for OpenVMS. The OFC feature provided by HP CIFS Server can be enabled by adding the following line to the share section in the HP CIFS Server configuration file:

```
vms open file caching = yes
```

The duration for which the file is kept open in the cache is determined by the OFC time interval, which can be specified in milli seconds. The share parameter that controls the OFC time interval is *vms ofc time interval*. The default value for this parameter is 5000 milliseconds. The default value of OFC time interval can be changed by specifying the following line to the share section in the HP CIFS Server configuration file. For example, to specify 1000 milliseconds as the OFC time interval, use:

```
vms ofc time interval = 1000
```

12.8 Microsoft's Distributed File System

If the Microsoft's Distributed File System (MS 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 reduces network traffic and DFS related errors.

```
host msdfs = no
```

NOTE: After MS DFS is disabled, you might have to restart those clients that had already established connection to the HP CIFS Server before disabling it.

Disabling MS DFS can avoid client system crash when the client system tries to access a share with non-existing share path or if there is no access to it.

12.9 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 support. To obtain this value:

```
$ SHOW MEMORY/SLOT
```

For information on how to modify the value of *Process Entry Slots* parameter, see the *HP OpenVMS System Manager's Manual*.

12.10 Ignoring unwanted datagram packets

The HP CIFS Server `SMB.CONF` global parameter *store dgpackets* when set to `no` (default) causes the NMBD process to ignore unwanted datagram (UDP) packets. Setting store `dgpackets = yes` causes the NMBD process to write unwanted datagram packets to the `unexpected.tdb` file causing it to grow in size and this may lead to the NMBD CPU consumption problem. Do not set the value of this parameter to `yes` unless recommended by HP.

12.11 Optimizing TDB database files

The HP CIFS Server stores data in files commonly referred to as "TDB files", due to the file extension they all share - `.TDB`. The HP CIFS Server emulates the TDB files using the RMS Indexed files. Like all RMS indexed files, these database files can benefit from a periodic maintenance and optimization. The following procedures describe how to analyze and optimize the TDB databases using FDL.

12.11.1 Processing FDL file names

When creating the TDB files, the HP CIFS Server uses the first FDL file it locates in the order listed:

1. `SAMBA$ROOT:[LIB]<tdb-filename>.FDL`

   where:

   `<tdb-filename>` is identical to the name of the TDB file.

   For example, when creating `LOCKING.TDB`, if the `SAMBA$ROOT:[LIB]LOCKING.FDL` file exists, the HP CIFS Server creates the new `LOCKING.TDB` using this FDL file.

2. `SAMBA$ROOT:[LIB]]GENERIC_TDB.FDL`

   This file is used by the HP CIFS Server to create any TDB files for which there is no TDB-specific FDL file.

3. If the HP CIFS Server finds neither a TDB-specific FDL file nor the `GENERIC_TDB.FDL` file, it uses the default FDL values.

   For more information about the default FDL values, see Section 12.11.3 (page 193).

12.11.2 Creating an optimized FDL file

To improve the performance of a TDB file, use a three-step procedure that includes analysis, FDL optimization, and creating a new TDB file. If used periodically during the life of a data file, this procedure yields a file that performs optimally. The resultant file can then be used either as a TDB-specific FDL file or a GENERIC_TDB.FDL file so that the HP CIFS Server will continue to create the TDB files using the optimized FDL values. To generate an optimized FDL:

1. Analyze a Data File.

   Use the `ANALYZE/RMS_FILE/FDL` command to create an output file (analysis-fdl-file) that reflects the current state of the data file. The command syntax for creating the analysis FDL file is:

```
$ ANALYZE/RMS_FILE/FDL/OUTPUT=<analysis-fdl-file>
<original-data-file>
```

The output file *<analysis-fdl-file>* contains all the information and statistics about the data file, including create-time attributes and information that reflects the changes made to the structure and contents of the data file over its life.

For example, to obtain the analysis FDL file of LOCKING.TDB, execute:

```
$ ANALYZE/RMS_FILE/FDL/OUTPUT=ANALYSIS_LOCKING.FDL –
SAMBA$ROOT:[VAR.LOCKS]LOCKING.TDB
```

The ANALYSIS_LOCKING.FDL is created in the current working directory.

2. FDL optimization.

   Use the Edit/FDL utility to produce an optimized FDL file (optimized-fdl-file).

   You can modify an FDL file either interactively using a terminal or non-interactively by allowing the Edit/FDL utility to calculate the optimal values based on the analysis report.

   To optimize the file interactively, use the OPTIMIZE script:

   ```
   $ EDIT/FDL/ANALYSIS=<analysis-fdl-file>/SCRIPT=OPTIMIZE -
   /OUTPUT=<optimized-fdl-file> <analysis-fdl-file>
   ```

   To optimize the file non-interactively:

   ```
   $ EDIT/FDL/ANALYSIS=<analysis-fdl-file>/NOINTERACTIVE -
   /OUTPUT=<optimized-fdl-file> <analysis-fdl-file>
   ```

   For example, to generate the optimized FDL using the ANALYSIS_LOCKING.FDL non-interactively, execute:

   ```
   $ EDIT/FDL/ANALYSIS=ANALYSIS_LOCKING.FDL/NOINTERACTIVE-
   /OUTPUT=OPTIMIZED_LOCKING.FDL ANALYSIS_LOCKING.FDL
   ```

3. File conversion.

   Conversion is the process of applying the optimized FDL file to the original data file.

   Use the Convert utility:

   ```
   $ CONVERT/FDL=<optimized-fdl-file>
   <original-data-file>[<new-data-file>]
   ```

   For example, to obtain a new version of the LOCKING.TDB file using the optimized FDL file, execute:

   ```
   $ CONVERT/FDL=OPTIMIZED_LOCKING.FDL -
   SAMBA$ROOT:[VAR.LOCKS]LOCKING.TDB
   ```

4. After verifying the values in the optimized FDL file, rename it to either GENERIC_TDB.FDL or *<tdb-datafile-name>.FDL* (that is, LOCKING.TDB) and copy it to the SAMBA$ROOT:[LIB] directory.

12.11.3 Default FDL values

The following default FDL values are used by the HP CIFS Server when creating the .TDB files:

```
SYSTEM
        SOURCE                      "OpenVMS"
FILE
        ORGANIZATION                indexed
        PROTECTION                  (system:RWD, owner:RWD, group:, world:)
        GLOBAL_BUFFER_COUNT         0
        GLBUFF_CNT_V83              200
        GLBUFF_FLAGS_V83             none
```

```
RECORD
        CARRIAGE_CONTROL          carriage_return
        FORMAT                    variable
        SIZE                      0
AREA 0
        ALLOCATION                240
        BEST_TRY_CONTIGUOUS       yes
        BUCKET_SIZE               4
        EXTENSION                 80

AREA 1
        ALLOCATION                48
        BEST_TRY_CONTIGUOUS       yes
        BUCKET_SIZE               4
        EXTENSION                 48

KEY 0
        CHANGES                   no
        DATA_AREA                 0
        DATA_FILL                 100
        DATA_KEY_COMPRESSION      no
        DATA_RECORD_COMPRESSION   yes
        DUPLICATES                no
        INDEX_AREA                1
        INDEX_COMPRESSION         no
        INDEX_FILL                100
        LEVEL1_INDEX_AREA         1
        NAME                      "TDBHASH.1/16"
        PROLOG                    3
        SEG0_LENGTH               16
        SEG0_POSITION             0
        TYPE                      string
```

13 SMB.CONF parameters

This chapter addresses the following topics:

13.1 Introduction

This chapter describes the HP CIFS Server configuration parameters that may be modified, parameters that must not be modified, and the parameters that are unsupported. For descriptions about these parameters, see the *SWAT utility* help page. This chapter also describes the configuration parameters unique to the HP CIFS Server.

13.2 Modifiable configuration parameters

```
- abort shutdown script
- add group script
- add machine script
- add share command
- add user script
- add user to group script
- addport command
- addprinter command
- admin users
- administrative share
- algorithmic rid base
- allocation roundup size
- allow trusted domains
- available
- bind interfaces only
- browse list
- browseable
- change share command
- check password script
- client NTLMv2 auth
- client lanman auth
- client plaintext auth
- client schannel
- client signing
- client use spnego
- cluster addresses
- comment
- create mask
- csc policy
- deadtime
- debug hires timestamp
- debug pid
- debug prefix timestamp
- debug timestamp
- debug uid
- default service
- delete group script
- delete readonly
- delete share command
- delete user from group script
- delete user script
```

- delete veto files
- deleteprinter command
- directory mask
- directory name cache size
- directory security mask
- disable netbios
- disable spoolss
- display charset
- domain logons
- domain master
- dont descend
- dos charset
- enable asu support
- enhanced browsing
- enumports command
- fake oplocks
- follow symlinks
- force create mode
- force directory mode
- force directory security mode
- force security mode
- force unknown acl user
- fstype
- guest account
- guest ok
- guest only
- hide unwriteable files
- host msdfs
- hostname lookups
- hosts allow
- hosts deny
- idmap alloc backend
- idmap backend
- idmap cache time
- idmap domains
- idmap gid
- idmap negative cache time
- idmap uid
- inherit owner
- inherit vms rms protections
- interfaces
- invalid users
- lanman auth
- large readwrite
- ldap admin dn
- ldap debug level
- ldap debug threshold
- ldap delete dn
- ldap group suffix
- ldap idmap suffix
- ldap machine suffix
- ldap page size
- ldap passwd sync
- ldap replication sleep
- ldap ssl
- ldap suffix
- ldap timeout
- ldap user suffix
- level2 oplocks
- lm announce
- lm interval
- local master
- lock directory
- lock spin time
- log file

- log level
- logon drive
- logon home
- logon path
- logon script
- lppause command
- lpq command
- lpresume command
- lprm command
- machine password timeout
- map to guest
- max connections
- max disk size
- max log size
- max open files
- max print jobs
- max protocol
- max reported print jobs
- max ttl
- max wins ttl
- max xmit
- message command
- min print space
- min protocol
- min wins ttl
- msdfs proxy
- msdfs root
- name cache timeout
- name resolve order
- netbios aliases
- netbios name
- netbios scope
- ntlm auth
- null passwords
- only user
- oplock break wait time
- oplock contention limit
- oplocks
- os level
- passdb backend
- password server
- path
- pid directory
- postexec
- preexec
- preexec close
- preferred master
- print command
- printable
- printer name
- private dir
- profile acls
- queuepause command
- queueresume command
- read list
- read only
- read raw
- realm
- remote announce
- remote browse sync
- rename user script
- require strongkey
- reset on zero vc
- restrict anonymous
- root postexec

- root preexec
- root preexec close
- security
- security mask
- server schannel
- server signing
- server string
- set primary group script
- show add printer wizard
- shutdown script
- smb ports
- socket options
- store dgpackets
- store dos attributes
- strict allocate
- strict sync
- svcctl list
- sync always
- template homedir
- time offset
- token sid limit
- unix charset
- unix extensions
- use client driver
- use kerberos keytab
- use spnego
- username map
- valid users
- veto files
- veto oplock files
- vfs objects
- vms asv domain
- vms estimate file size
- vms file flush
- vms ofc time interval
- vms open file caching
- vms path names
- vms rms format
- volume
- winbind cache time
- winbind nested groups
- winbind offline logon
- winbind refresh tickets
- winbind trusted domains only
- winbind use default domain
- wins server
- wins support
- workgroup
- write list
- write raw

13.3 Non-modifiable configuration parameters

The following configuration parameters are set to the default values and these values must not be changed to ensure proper operation of the server:

- acl check permissions
- acl map full control
- announce as
- announce version
- auth methods
- block size
- blocking locks
- case sensitive

```
- default case
- default devmode
- defer sharing violations
- dos filetimes
- enable core files
- enable privileges
- encrypt passwords
- getwd cache
- hide dot files
- inherit acls
- locking
- mangle prefix
- mangled map
- mangled names
- mangling char
- mangling method
- max mux
- nt acl support
- nt pipe support
- nt status support
- paranoid server security
- password level
- posix locking
- preserve case
- printing
- printjob username
- root directory
- set directory
- share modes
- short preserve case
- strict locking
- template shell
- update encrypted
- username level
- winbind separator
- wins proxy
```

13.4 HP CIFS Server-specific configuration parameters

The following configuration parameters have been introduced by and are unique to the HP CIFS Server. Those listed as *Global* parameters may only be used in the [GLOBAL] section of the configuration file, while those listed as *Share* parameters may be used in both the [GLOBAL] section and share sections.

Global parameters

```
- store dgpackets
- require strongkey
- token sid limit
- vms asv domain
```

Share parameters

```
- vms rms format
- vms path names
- inherit vms rms protections
- vms estimate file size
- vms open file caching
- vms ofc time interval
- vms file flush
```

13.5 Unsupported configuration parameters

The following configuration parameters are unsupported and must not be used:

- acl compatibility
- acl group control
- afs share
- afs token lifetime
- afs username map
- aio read size
- aio write behind
- aio write size
- change notify
- config file
- cups options
- cups server
- dfree cache time
- dfree command
- dmapi support
- dns proxy
- dos filemode
- dos filetime resolution
- ea support
- eventlog list
- fake directory create time
- force group
- force printername
- force user
- get quota command
- hide files
- hide special files
- hide unreadable
- homedir map
- inherit permissions
- iprint server
- kernel change notify
- kernel oplocks
- load printers
- log nt token command
- magic output
- magic script
- map acl inherit
- map archive
- map hidden
- map readonly
- map system
- max smbd processes
- max stat cache size
- NIS homedir
- obey pam restrictions
- open files database hash size
- os2 driver map
- pam password change
- panic action
- passdb expand explicit
- passwd chat
- passwd chat debug
- passwd chat timeout
- passwd program
- preload
- preload modules
- printcap cache time
- printcap name
- printer admin

- read bmpx
- set quota command
- smb passwd file
- socket address
- stat cache
- syslog
- syslog only
- time server
- unix password sync
- use mmap
- username
- username map script
- use sendfile
- usershare allow guests
- usershare max shares
- usershare owner only
- usershare path
- usershare prefix allow list
- usershare prefix deny list
- usershare template share
- wide links
- winbind enum groups
- winbind enum users
- winbind normalize names
- winbind nss info
- wins hook
- write cache size

A Sample installation and removal procedures

This appendix provides sample procedures for installing and removing the HP CIFS Server software.

A.1 Sample installation on OpenVMS Integrity server systems

```
$ PRODUCT INSTAL SAMBA /DESTINATION=PIANO$DKA0:[CIFS]

Performing product kit validation of signed kits ...

The following product has been selected:
    HP I64VMS SAMBA V1.2                    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.

Configuring HP I64VMS SAMBA V1.2: HP OpenVMS CIFS

    © Copyright 2010 Hewlett-Packard Development Company, L.P.

    HP OpenVMS CIFS is released under the terms of GNU Public License.

    This installation procedure requires that all the following
    conditions are satisfied:

    1.  This procedure is running on an Alpha or a IA64 processor.
    2.  On an Alpha, the system is running OpenVMS V8.2 or later
        or on a IA64 system, OpenVMS V8.2-1 or later.
    3.  All required privileges are currently enabled.
    4.  No CIFS images are running on this node or anywhere in
        the cluster that make use of common samba$root installation
        directory.

    This procedure checks if the conditions are satisfied.
    If they are satisfied, the procedure continues.
    If not, the procedure stops.
Do you want to continue? [YES]

Do you want the defaults for all options? [YES]

Do you want to review the options? [NO]

Execution phase starting ...

The following product will be installed to destination:
    HP I64VMS SAMBA V1.2                    DISK$V083:[CIFS.]

Portion done: 0%...30%...40%...60%...90%

   User Accounts and User Identification Codes (UICs)
   --------------------------------------------------

    The HP OpenVMS CIFS V1.2 installation creates five OpenVMS
    accounts: SAMBA$SMBD, SAMBA$NMBD, SAMBA$GUEST, SAMBA$TMPLT
    and CIFSADMIN. The default UIC group number for these new
    accounts depends on the following:

    o If you are installing the server 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 default UIC group number for CIFS accounts
Group: [360]
Creating OpenVMS accounts required by CIFS
Created account SAMBA$SMBD
Created account SAMBA$NMBD
Created account SAMBA$GUEST
Created account SAMBA$TMPLT
Created account CIFSADMIN

   The release notes for HP OpenVMS CIFS, CIFS_REL_NOTES.TXT
   is available at SYS$COMMON:[SYSHLP].

   To automatically define SAMBA$ROOT logical during system
   startup, add the following line in SYS$MANAGER:SYLOGICALS.COM:

        $ @SYS$STARTUP:SAMBA$DEFINE_ROOT.COM

   To automatically start HP OpenVMS CIFS during system startup,
   add following line to the file SYS$MANAGER:SYSTARTUP_VMS.COM
   after TCPIP startup command procedure:

        $ @SYS$STARTUP:SAMBA$STARTUP.COM

   To Configure HP OpenVMS CIFS on this node, execute:

        $ @SAMBA$ROOT:[BIN]SAMBA$CONFIG.COM
...100%

The following product has been installed:
    HP I64VMS SAMBA V1.2                  Layered Product
$
```

A.2 Sample removal procedure on OpenVMS Integrity server systems

```
$ PRODUCT REMOVE SAMBA

The following product has been selected:
    HP I64VMS SAMBA V1.2                    Layered Product

Do you want to continue? [YES]

The following product will be removed from destination:
    HP I64VMS SAMBA V1.2                    DISK$V083:[CIFS.]

Portion done: 0%...10%

Cleaning up temporary TDB files before initiating
HP OpenVMS CIFS product removal...

  This utility will remove all CIFS configuration files.

Save CIFS configuration files? [y/n]: [n] y

  Some portions of CIFS may be useful even after CIFS is
  removed.

Save utility tools? [y/n]: [n]

Do you want to save CIFS release notes? [y/n]: [y]

Deleting CIFS files...

Completed deleting CIFS files.

Saved files are in SYS$COMMON:[SYSUPD]SAMBA$SAFETY.DIR

CIFS Installation, configuration and data files have
been removed from PIANO$DKA0:[CIFS.SAMBA]

...20%...30%...40%...50%...60%...70%...80%...90%...100%

The following product has been removed:
    HP I64VMS SAMBA V1.2                    Layered Product
$
```

Index

W