

# HP OpenVMS Common Internet File System CIFS v1.1 Training Seminar

OpenVMS Technical Update Days, September 2008  
Aravinda Guzzar – HP OpenVMS CIFS Engineering  
Paul Nunez – HP Services  
Hans Hosang – HP services



HP Restricted  
© 2008 Hewlett-Packard Development Company, L.P.  
The information contained herein is subject to change without notice

## Training Overview

- Introductions
- Installation & Configuration
- Management
- Troubleshooting
- Migrating Advanced Server to CIFS





## Introductions

### Objectives

- Introduce ourselves
- Explain Samba
- Explain why HP ported Samba to OpenVMS
- Explain CIFS services and features
- Describe CIFS Limitations



## What is CIFS for OpenVMS?

- CIFS for OpenVMS V1.1 is a port of the Samba for Linux v3.0.28a code base.
- Samba is an Open Source/Free Software suite that provides file and print services to SMB/CIFS (primarily Microsoft Windows) clients.
- Samba is freely available under the GNU General Public License.



## Services

### Key services offered by HP OpenVMS CIFS v1.1

- File & Print Services
- Authentication and Authorization
- Name Resolution
- Service Announcement (Browsing)

## Features

- Security
  - User authorization
  - Group support
  - POSIX ACL support for files and directories
- Windows client support
  - Windows 2000, Windows XP, Windows Server 2003 and Windows Vista
- Interoperability
  - Active Directory domains
  - NT4 domains
- ODS-2 and ODS-5 volume support
- Support for most RMS file formats

Can read all file formats (few issues with VFC files) and can create files in Stream or Stream\_LF formats. There are plans to add support for creating files with fixed length, 512-byte records.

## Limitations

- Cannot be a Backup Domain Controller
- Relies on OpenVMS auditing for auditing
- DENY permission is not supported
- Cannot be a WINS server (WINS client supported)
- No Kerberos support (no support for ADS security mode)
- Does not provide External Authentication (use OpenVMS ACME LDAP Agent)

8

[23-sept.2008] – HP OpenVMS Technical Update Days



PDC support expected in next release

OpenVMS Integrity systems can also provide external authentication if clustered with Alpha systems running Advanced Server for OpenVMS



## Installation & Configuration

### Objectives

- Describe pre-installation considerations
- Explain the CIFS installation process
- Describe the post-installation steps
- Explain how to configure CIFS



## Pre-installation Considerations

- Kit Information
- CIFS Patches
- Hardware Requirements
- Software Requirements
- OpenVMS Cluster Considerations
- Pre-installation Checklist



## HP OpenVMS CIFS Kits

- HP OpenVMS CIFS v1.1 was ported using the Samba V3.0.28a code
- Kit Location  
[http://h71000.www7.hp.com/network/cifs\\_download.html](http://h71000.www7.hp.com/network/cifs_download.html)
- Kit Names  
HP-I64VMS-SAMBA-V0101--1.PCSI\_SFX\_I64EXE  
HP-AXPVMS-SAMBA-V0101--1.PCSI\_SFX\_AXPEXE
- Run the downloaded file to create the PCSI kit files



## CIFS Patches

### Obtain important fixes

- Download the latest set of patches for CIFS v1.1

```
$ ftp hprc.external.hp.com
```

```
Username: pathwork
```

```
Password: support
```

- Sub-dir per product (ASV, ASU, CIFS, PW32)
- Unzip "-V" to extract the files
- See the release notes (included) for installation instructions



## Software Requirements

- Currently qualified on
  - OpenVMS I64 Version 8.2-1, 8.3 and 8.3-1H1
  - OpenVMS Alpha Version 8.2 and 8.3.
- TCP/IP
  - HP TCP/IP Services for OpenVMS
  - Process Software Multinet for OpenVMS
  - Process Software TCPware for OpenVMS
- C Run-Time Library (CRTL) ECO
  - [http://www12.itrc.hp.com/service/patch/search.do?BC=main  
&pageOsid=openvms](http://www12.itrc.hp.com/service/patch/search.do?BC=main&pageOsid=openvms)



## OpenVMS Cluster Considerations

- Each cluster node may be a distinct entity (separate configuration) or multiple may share an identity (common configuration) with other cluster nodes
- Restrictions for unique identity configurations
  - Should not share the same installation directory
  - Should not allow access to the same share thru multiple cluster members
- Restrictions for common identity configurations
  - OpenVMS v8.3 and later
  - Must share a common installation directory, SYSUAF and RIGHTLIST

15

[23-sept.2008] – HP OpenVMS Technical Update Days



- The C RTL for versions of OpenVMS prior to v8.3 lack support for 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.

## Pre-installation Checklist

- Connect the system to the network
- Login as SYSTEM (or other fully privileged account)
- Configure and start TCP/IP
- Install the latest CRTL ECO
- Read the CIFS documentation and release notes
- Determine installation location
- Back up the destination disk
- Ensure adequate disk space for installation



## Installation

- Privileges Required
- Installation Procedure
- CIFS Directories
- Post-installation Steps
- CIFS Commands and Utilities



## Privileges Required

Before you install HP OpenVMS CIFS software, log in to the SYSTEM (or other privileged) account

- Minimum Privileges Required:  
CMKRNL, DIAGNOSE, IMPERSONATE, NETMBX, OPER,  
SYSGBL, SYSLCK, SYSNAM, SYSPRV, TMPMBX, VOLPRO,  
WORLD




## Installation Procedure

- If necessary, shutdown CIFS
- Run the command
 

```
$ PRODUCT INSTALL SAMBA [/DESTINATION=<location>]
```

<location> = device and directory name, like:  
/DESTINATION = DISK\$APP1:[000000]
- No reboot necessary

19 [23-sept.2008] – HP OpenVMS Technical Update Days 

- To create the SAMBA directory under the Master File Directory (MFD) [000000], include the MFD specification, as in:

```
/DESTINATION = DISK$APP1:[000000]
```

- Installation options allow you to choose whether savesets containing source files and/or migration utilities are restored.
- Saveset containing SWAT files is placed in samba\$root:[utils]
- Creates OpenVMS accounts: SAMBA\$GUEST, SAMBA\$TMPLT, SAMBA\$NMBD and SAMBA\$SMBD. UIC check is basic at best.
- Creates SAMBA\$ROOT directory tree (see next slide)
- Check SYS\$STARTUP:SAMBA\$DEFINE\_ROOT.COM or do \$ PRODUCT SHOW OBJECT/FULL [SAMBA] to determine installation location.


## CIFS Directories

Directory	Description
SYS\$STARTUP:	Startup and shutdown procedures
SAMBA\$ROOT:	Main tree; Rooted logical name
SAMBA\$ROOT:[BIN]	Binaries, command procedures
SAMBA\$ROOT:[LIB]	SMB.CONF, lmhosts, config files, etc.
SAMBA\$ROOT:[PRIVATE]	Encrypted password and secrets files
SAMBA\$ROOT:[TMP]	User directories
SAMBA\$ROOT:[VAR]	Log files
SAMBA\$ROOT:[VAR.LOCKS]	TDB files
SAMBA\$ROOT:[SWAT]	Place holder for SWAT related files.
SAMBA\$ROOT:[UTILS]	Swat and Migration backup savesets



**Post-installation Steps**

- Define logical names and create services
  - \$ @samba\$root:[bin]samba\$config
- Define CIFS commands
  - \$ @samba\$root:[bin]samba\$define\_commands
- Install latest CIFS patches
- Update site-specific startup and shutdown procedures

21 [23-sept-2008] - HP OpenVMS Technical Update Days 

- SAMBA\$CONFIG defines SAMBA\$ROOT: logical (and others) and creates but disables the SMBD and SMBD445 service and creates and enables the SWAT services in the TCP/IP service database.

- To connect to the server using SWAT, connect to URL `http://<server>:901`.

- See next slide for list of commands defined by `samba$define_commands.com`

- The current patch installation procedure assumes the SAMBA\$ROOT logical is defined. If necessary, execute `@sys$startup:samba$define_root`.

- If desired, restore SWAT and/or source file savesets. The source file saveset resides in `samba$root:[src]`, the others in `samba$root:[utils]`; for example:

```
$ BACKUP
SAMBA$ROOT:[UTILS]SAMBAS$SWAT FILES BACK/SAVE -
```

## CIFS Commands and Utilities

Various Samba utilities are provided to help manage and troubleshoot CIFS

- Defined by \$ @samba\$root:[bin]samba\$define\_commands
- To obtain usage information use the -h option
- Most options have a short form and a long form
  - ["-V" | -version] Mind the quotes !
- Passwords containing uppercase characters must be quoted (except if prompted for password)

22

[23-sept.2008] – HP OpenVMS Technical Update Days



```

ADDSHARE == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$ADDSHARE.EXE;"
NET == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$NET.EXE;"
NMBLOOKUP == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$NMBLOOKUP.EXE;"
NTLMAUTH == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$NTLMAUTH.EXE;"
PDBEDIT == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$PDBEDIT.EXE;"
PROFILES == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$PROFILES.EXE;"
RPCCLIENT == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$RPCCLIENT.EXE;"
SMBCACLS == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$SMBCACLS.EXE;"
SMBCLIENT == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$SMBCLIENT.EXE;"
SMBCONTROL == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$SMBCONTROL.EXE;"
SMBCQUOTAS == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$SMBCQUOTAS.EXE;"
SMBPASSWD == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$SMBPASSWD.EXE;"
SMBSH*OW == "pipe show system | search sys$input nmbd,smbd_bg"
SMBSPool == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$SMBSPool.EXE;"
SMBSTA*RT == "@sys$startup:samba$startup.com"
SMBSTATUS == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$SMBSTATUS.EXE;"
SMBSTO*P == "@sys$startup:samba$shutdown.com"
SMBTREE == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$SMBTREE.EXE;"
SMBVER*SION == "@SAMBA$ROOT:[BIN]samba$version.com"
TDBBACKUP == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$TDBBACKUP.EXE;"
TDBDUMP == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$TDBDUMP.EXE;"
TDBTOOL == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$TDBTOOL.EXE;"
TESTPARM == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$TESTPARM.EXE;"
WBINFO == "$SAMBA$ROOT:[BIN.ALPHA]SAMBA$WBINFO.EXE;"

```

## Configuration

- Determine server's role
- Update the Samba configuration file - SMB.CONF
- Establish NetBIOS Name Resolution
- Verify the configuration with TESTPARM
- Starting/Stopping CIFS
- Removing CIFS

23

[23-sept.2008] – HP OpenVMS Technical Update Days



## Supported Roles

### Only Standalone and Member server roles supported

- Standalone
  - CIFS accounts are local to the system
  - No NETLOGON services (domain logon, trusts)
  - Share or user level security
  - Best when few users or security needs minimal
- Member server
  - Domain membership required
  - Domain security support including trusts
  - Best for larger environments with established domains
- PDC
  - All PDC functions supported except replication
  - Replication needs to be done manually (net rpc vampire)

24

[23-sept-2008] – HP OpenVMS Technical Update Days



Support for PDC role planned for next release

## The Samba Configuration File

- A text file named `samba$root:[lib]SMB.CONF` that uses the same format as Windows `.ini` files with section names within brackets and sections containing parameters with values assigned
- Use SWAT from any Web browser or use any OpenVMS text editor to modify the file
- Three section types:
  - The `[global]` section - Contains parameters that apply to the whole CIFS server.
  - The `[homes]` section - Facilitates connections to users "home" (login) directory. Eliminates the need for explicit share stanzas for each user.
  - The `[sharename]` section (or stanza)– These sections represent the directory and printer shares offered by the server. The name within the brackets represents the share name.

25

[23-sept.2008] – HP OpenVMS Technical Update Days



- Located in `samba$root:[lib]`
- OpenVMS record format may be Stream or Variable Length
- Template file contains many comments
- For more details about configuration file (SMB.CONF), refer to <http://www.samba.org/SAMBA/docs/man/manpages-3/smb.conf.5.html>
- Comments must be on separate lines which begins with `;` or `#`
- Device and directory paths may be specified using either UNIX or OpenVMS syntax

## The Samba Configuration File (continued)

### Parameters Description

- Parameters define the specific attributes of sections
  
- There are two types
  - Global Parameters – Used in the [global] section only.
  
  - Share Parameters – Used in any section. When they appear in the [global] section they apply to all shares that do not have the parameter included in their share stanza.



## The Samba Configuration File (continued)

### Example Samba configuration file:

```
[global]
workgroup = BIDAR
domain logons = yes
log level = 3
max log size = 1000
admin users = test1
wins server = 10.10.1.1
[homes]
browsable = no
read only = no
[printshare1]
samba$root:[spool]
printable = yes
min print space = 2000
[test]
browsable = yes
read only = yes
path = /DKA0/SAMBA/USERS/TEST
```

Diagram labels: Section (points to [global]), Parameters (points to the list of parameters under [global]).

27

[23-sept.2008] – HP OpenVMS Technical Update Days



### Default SMB.CONF:

[global]

```
server string = Samba %v running on %h (OpenVMS)
netbios name = %h
security = user
passwd backend = tdbsam
domain master = yes
guest account = SAMBA$GUEST
domain logons = Yes
log file = /samba$root/var/log_%h.%m
create mode = 0755
load printers = no
printing = OpenVMS
```

[homes]

```
comment = Home Directories
browseable = no
read only = no
create mode = 0750
```

### NOTES:

- Since “workgroup” parameter is not present, it defaults to LANGROUP.
- Default configuration is for a PDC.

## Samba Web Administration Tool (SWAT)

SWAT is a Web-based interface for configuring CIFS from a web browser.

- Connect to `http://<server>:901`
- Login using OpenVMS account credentials (i.e., SYSTEM)
- Capabilities limited if account has only read access to `smb.conf`
- From the SWAT MAN page (under WARNINGS):

swat will rewrite your `smb.conf(5)` file. It will rearrange the entries and delete all comments, `include=` and `copy=` options. If you have a carefully crafted `smb.conf` then back it up or don't use swat!

28

[23-sept-2008] – HP OpenVMS Technical Update Days



If connection fails (before prompt for username), verify the SWAT service on the server is enabled.

SWAT has several nice features:

- View the Samba help (MAN page) and documentation files (see “Known Problems” below)
- Join the Samba mailing lists (Feedback section at bottom of Home page)
- Change Global parameters
- Add or remove share definitions
- Wizards to help with role configuration (i.e., Standalone or Member server) and WINS client set up.
- View the server status (active connections, active shares, and open files).
- View the `smb.conf` file
- Change your CIFS or Windows password (on any server)

Known problems:

- SWAT process crashes if the OpenVMS account attempting to run it is DISUSER'd
- The functions on the “Printers” page do not work
- The images in the [Using Samba, 2ed](#) pages are not displayed
- The auto refresh feature on the “Status” page do not work (quits after one cycle)

## Member Server Configuration

### To configure CIFS as a Member server

- Essential SMB.CONF [global] section parameters

```
[global]
workgroup = <domainname>
security = domain
domain logons = no
domain master = no
```

- Join the domain

```
$ net rpc join ["-S" DC-name] ["-I" DC-IPaddress] ["-U"
administrator%password]
```

29

[23-sept-2008] – HP OpenVMS Technical Update Days




Regarding the NET RPC JOIN command:

- You do not need to start CIFS to run this command
- Does not make use the smb.conf parameter "password server"
- Both "-I" <address> and "-S" <fully.qualified.domain.name>, when used individually or together, fail with the STATUS\_INVALID\_COMPUTER\_NAME error (will be fixed in a future release)
- Using "-S" <servername> (not fully qualified domain name) works if:
  - "-I" <address> is also specified, or
  - <servername> can be resolved by means of either a DNS or NetBIOS name query (including LMHOSTS lookup)
- When both "-I" and "-S" options are omitted, it sends NetBIOS name queries for the name <workgroup>#1b only . If WINS is not used and the PDC is not on the same subnet as the CIFS SERVER LMHOSTS entries are necessary

### Standalone Server Configuration

- Standalone servers can use either share-level or user-level security as specified by the SMB.CONF parameter "security"  
  
    security = share  
or  
    security = user
- Essential SMB.CONF [global] section parameters  
  
    [global]  
    security = user  
    domain logons = no

30 [23-sept.2008] – HP OpenVMS Technical Update Days 

- Share-level security in Samba is not similar to share-level security used by Windows; see the smb.conf MAN page for further information.
- Share-level security should be reserved for situations requiring minimal security (i.e., a server used strictly as a print server or offering public, read-only shares).
- If not specified, the default workgroup name is LANGROUP.

## Browser Roles

- To designate as Domain Master Browser use "domain master = yes" in [global] section of smb.conf  
NOTE: only do this if you are PDC !!!!
- To designate as Local Master Browser use "local master = yes" in [global] section of smb.conf
- To force an election when CIFS starts use "preferred master = yes" in [global] section of smb.conf
- To boost election criteria so CIFS becomes a master browser use "os level = 65" in [global] section of smb.conf  
Never boost os level as this will cripple Windows browsing.

31

[23-sept.2008] – HP OpenVMS Technical Update Days



In a domain configuration, only the domain PDC should be designated as the Domain Master Browser

In a workgroup configuration, only one workgroup member should be designated as the Domain Master Browser

There should be only one Local Master Browser per subnet; use "os level = 65" to force CIFS to be the Local Master Browser

To prevent CIFS from becoming a master browser:

```
[global]
domain master = no
local master = no
```

## NetBIOS Name Resolution

CIFS uses WINS, LMHOSTS. file, DNS, and/or broadcasts

- Methods used and order are determined by SMB.CONF global parameter "name resolve order"
- Use the SMB.CONF global parameter "wins server" to specify the IP addresses of WINS servers
- Uses DNS resolver of host
- LMHOSTS. file resides in samba\$root:[lib]
- LMHOSTS. file must have Stream\_LF record format (use template file)
- LMHOSTS. syntax is different than that used on Windows
- Use NMBLOOKUP utility for testing

32

[23-sept.2008] – HP OpenVMS Technical Update Days



- Separate WINS server IP addresses with a space
- See LMHOSTS. MAN page for syntax
- Name Resolve Order default setting:

name resolve order = lmhosts wins host bcast

## TESTPARM Utility

Always use TESTPARM after modifying SMB.CONF

- Reports obvious mistakes in the SMB.CONF file
- Displays server role (based on SMB.CONF parameters)
- Lists non-default parameter settings and share stanzas
- For usage information, enter \$ testparm -? (not -h)

33

[23-sept.2008] – HP OpenVMS Technical Update Days



• \$ testparm --help

Usage: [OPTION...] <config-file> [host-name] [host-ip]

-s, --suppress-prompt      Suppress prompt for enter  
 -v, --verbose              Show default options too  
 -L, --server=STRING      Set %%L macro to servername

-t, --encoding=STRING      Print parameters with encoding  
 --show-all-parameters      Show the parameters, type, possible values  
 --parameter-name=STRING    Limit testparm to a named parameter  
 --section-name=STRING      Limit testparm to a named section

Help options:

-?, --help                  Show this help message  
 --usage                    Display brief usage message

Common samba options:

-V, --version              Print version

• To determine the current setting for any particular parameter or set of parameters:

```
$ pipe testparm -sv | search sys$pipe <search-string>
```

where <search-string> is a complete or partial parameter name

## TESTPARM Utility (continued)

### Sample output of the TESTPARM utility

```
$ TESTPARM
Load smb config files from /SAMBASROOT/LIB/SMB.CONF
Processing section "[homes]"
Processing section "[test]"
Loaded services file OK.
Server role: ROLE_DOMAIN_PDC
Press enter to see a dump of your service definitions

[global]
  server string = Samba %v running on %h (OpenVMS)
  passdb backend = tdbsam
  log file = /samba$root/var/log_%h.%m
  domain logons = Yes
  domain master = Yes
  admin users = test

[homes]
  comment = Home Directories
  read only = No

[test]
  comment = Test User's Home Directories
  path = dka0/test
  read only = No
```



## Starting and Stopping CIFS


- To start CIFS

```
$ @sys$startup:samba$startup ! $ smbstart
```
- To stop CIFS

```
$ @sys$startup:samba$shutdown ! $ smbstop
```

35

[23-sept.2008] – HP OpenVMS Technical Update Days



### Startup notes:

- SAMBA\$STARTUP.COM starts the NMBD process only. NMBD is responsible for NetBIOS name registration, resolution, and browser functions.
- Edit samba\$root:[bin]samba\$common\_startup.com and uncomment line to enable the SMBD service.
- When a client initiates a new session with the server, a new process is created by the TCP/IP dispatcher (based on the SMBD service) which calls SAMBA\$ROOT:[BIN]SAMBA\$SMBD\_STARTUP.COM to start a new process named SMBD\_BG<n> (where "BG<n>" is the TCP/IP BG device name).
- The SMBD process is responsible for processing service requests from the client.


### Shutdown notes:

- Terminates all client SMBD processes and the NMBD process
- Disables SMBD (and SWAT) service

### Process Log Files

Process log files are created for the NMBD process and each SMBD process

- Located in `samba$root:[var]`
- Names
  - `SAMBA$NMBD_<nodename>.LOG`
  - `SAMBA$SMBD_STARTUP.LOG`
  - `SAMBA$SWAT_STARTUP.LOG`
  - `Log_<nodename>.<PCname>`

36 [23-sept.2008] – HP OpenVMS Technical Update Days 

- The `SAMBA$SMBD_STARTUP.LOG` and `SAMBA$SWAT_STARTUP.LOG` names are controlled by a setting on the SMBD and SWAT TCP/IP services and, thus, cannot be node-specific.

- These files can be useful at times. For example, if the process shuts down immediately or crashes.

## Removing CIFS

- See the CIFS Cluster Setup document for instructions on removing CIFS from multiple cluster members
- To remove the product

```
$ PRODUCT REMOVE SAMBA
```

- If you wish to preserve the configuration files, choose YES when prompted, otherwise they are deleted
- Only User files under SAMBA\$ROOT:[USERS...], SECRETS.TDB, PASSDB.TDB and SMB.CONF are backed up (to a location you specify)
- Only removes the files in the installation directory tree that were created by \$ product install

37

[23-sept-2008] – HP OpenVMS Technical Update Days



Deletes the SAMBA\$\* OpenVMS accounts, but none of the CIFS\$\* user accounts nor CIFS\$GRP\* Resource Identifiers which may have been created by WINBIND.

# Management and Controlling access to Resources



## Agenda

- Managing File shares and VFS modules
- User/Group management (including winbind, username mapping)
- Controlling Access (permissions/protections/ACLs and inheritance)
- Tools and Utilities to Manage the CIFS server
- Configuring CIFS as Printer Server

# Managing File/Dir shares



## Managing File/Dir share - Adding share

- Edit the SAMBA\$ROOT:[LIB]SMB.CONF file and add the appropriate parameters depending on the file location and share name.

Example:

To create the share "test" with path DKA100:[TEST] add the following lines in SMB.CONF file.

```
[test]
comment = my directory test folder
path = /dka100/test
read only = No
valid users = user1, user2
inherit permissions = yes
inherit acls = yes
```

41

[23-sept.2008] – HP OpenVMS Technical Update Days



- To make a share publicly accessible, but read only, except for people in the user test1, use the below settings:

[public]

```
path = /home/samba
public = yes
read only = yes
write list = test1
```

- some of the most commonly used parameters:

Share level parameters:

1. browseable: This controls whether this share is seen in the list of available shares in a net view and in the browse list.
2. public or guest ok: If this parameter is yes for a service, then no password is required to connect to the service. Privileges will be those of the guest account.
3. admin users: This is a list of users who will be granted administrative privileges on the share. This means that they will do all file operations as the super-user i.e. samba\$smbd user.
4. create mask: This parameter may be thought of as a bit-wise MASK for the UNIX modes of a file. Any bit not set here will be removed from the modes set on a file when it is created.
5. directory mask: This parameter may be thought of as a bit-wise MASK for the UNIX modes of a dir. Any bit not set here will be removed from the modes set on a dir when it is created.
6. inherit acls: This parameter can be used to ensure that if default acls exist on parent directories, they are always honored when creating a subdirectory.
7. inherit permissions: The permissions on new files and directories are normally governed by create mask, directory mask, force create mode and force directory mode but the boolean inherit permissions parameter overrides this. New directories inherit the mode of the parent directory,
8. write list: This is a list of users that are given read-write access to a service. If the connecting user is in this list then they will be given write access, no matter what the read only option is set to.
9. read only: If this parameter is yes, then users of a service may not create or modify files in the service's directory.
10. valid users: This is a list of users that should be allowed to login to this service.
11. allow hosts, hosts allow: This parameter is a comma, space, or tab delimited set of hosts which are permitted to access a service.
12. oplocks: This boolean option tells smbd whether to issue oplocks (opportunistic locks) to file open requests on this share.

## Managing File/Dir share - VFS

- VMS specific features provided by VFS objects:
  - Variable Record Formatted files (VARVFC)
  - StreamLF
  - VTF
- VFS objects are specified as share level parameters using:  
vfs objects = <varvfc/StreamLF/VTF>
- Specifying the VFS module, passes the registered file operation through loaded VFS modules.
- VFS automatically selects ODS2 vfs object if the share is hosted on OSD2 disk



## Managing File/Dir share – VAR or StreamLF

- If a share contains Variable format files, add the below settings in the SMB.CONF

```
[share]
  vfs object = varvfc
```

- To make the default file creation to be Stream\_LF format specify the VFS object for a share as below:


```
[streamlf]
  vfs object = streamlf
```

- Needed for supporting Jar, Class files in Java on VMS.
- Text files by default will be created in Stream format.

### Managing File/Dir share - International Char support

- CIFS supports ISO-8859-1 and UTF-8 character set for file names.
- The European characters are supported in ISO-8859-1
- For configuring to support ISO-8859-1 characters specify the below parameter  
[global]  
dos charset = cp850  
unix charset = ISO-8859-1
- For Japanese or Chinese character set support specify the below:  
[global]  
dos charset = <user local codepage>  
unix charset = UTF-8  
vfs objects = vtf

Specify the Windows codepage in <user-local-codepage>  
For Windows codepage for English <user-local-codepage> is "cp850"  
For Windows codepage for Japanese <user-local-codepage> is "SJIS" or "CP932"

44 [23-sept-2008] – HP OpenVMS Technical Update Days 

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

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



# Managing Users and Groups

45

[23-sept.2008] – HP OpenVMS Technical Update Days



## Users and Groups

- CIFS users must have a corresponding host user.
- Groups are implemented using resource identifiers.
- Need to explicitly create host user before creating CIFS local user.
- Need to explicitly map CIFS local groups to resource identifiers.
- Domain users and groups are automatically mapped to host usernames and resource identifiers using winbind

### NOTE:

Winbind does not create host user if explicit mapping exists.

Winbind provides mapping between the Windows SIDs to host lds.

## Winbind

- Why is it needed?
  - Automatic mapping of users and groups.
  - Winbind is used for all queries to SAM (WNT) or Windows Active Directory (ADS).
  - Used for nested group support.
  - Trust functionality.
- If the above functionality is not required we recommend to disable the winbind.
- CIFS as Standalone server doesn't require winbind.
- By default winbind is enabled. To disable Winbind on CIFS, define the following logical:
 

```
$ DEFINE /SYSTEM WINBINDD_DONT_ENV 1
```
- It is also disabled if smb.conf does NOT contain the "idmap uid" and "idmap gid" parameters

47

[23-sept.2008] – HP OpenVMS Technical Update Days



Winbind automatically creates the user and group (resource identifier) in the CIFS member server, if there is no user or group corresponding to domain users and group, after successful authentication from Active Directory Service (ADS).

It uses the UIDs and GIDs allocated from the "idmap uid" and "idmap gid" range specified in the SMB.CONF file in [global] section.

The UID allocated by Winbind is used for generating UIC while creating the host user.

The GID is used as "gid value" while creating resource identifiers that are mapped to domain groups.

There must not be any existing UICs and GIDs in the range "idmap uid" and "idmap gid" range specified in the SMB.CONF file.

If for any reason the user and group mapping information has been lost and the corresponding security for shares, files and folder for these users will not be valid. So in order to avoid problems, it is highly recommended to backup the winbindd\_idmap.tdb and group\_mapping.tdb file periodically.

## Winbind

- Winbind functionality is integrated with SMBD process. Hence, no separate winbind process is created.
- Automatic mapping of CIFS users and groups to host users and resource identifiers:
  - After successful authentication
  - While setting permission
- SMB.CONF file must have the parameters:  
idmap uid = <uid range>  
idmap gid = <gid range>
- Idmapping is stored in winbindd\_idmap.tdb

48

[23-sept.2008] – HP OpenVMS Technical Update Days



### Winbind User Mapping procedure:

If "idmap uid" range is " 5000-10000", when a new user logs in and if there is no corresponding host account. UID 5000 for this user ID is obtained from Winbind and creates a user CIFS\$<hexadecimal-value-of-UID> which is CIFS\$1388 with a UIC of [<octal-value-of-UID>, <octal-value-of-UID>] which is [11610, 11610].

### Winbind Group Mapping procedure:

If "idmap gid" range is "5000-10000", when an user logs in and the user belongs to the groups for which there is no corresponding host group account. GID 5000 for group ID is obtained from the winbind and creates a resource identifier CIFS\$GRP<hexadecimal-value-of-gid> which is CIFS\$GRP<1388> with the value specified as GID, where GID represents the posix group identifier.

## Winbind, idmap uid and gid side effects

- Do not overlap these ranges, e.g.
  - Idmap uid = 5000 - 16382
  - Idmap gid = 20000 - 100000
- Example of an error:

```
test.txt;1      [CIFS$271B]          (RWED,RWED,RE,)
```

The UID 10011 (0x271b) is mapped to the SID:

```
key(10) = "UID 10011\00"
```

```
data(46) = "S-1-5-21-3788632709-619170709-2383488769-1155\00"
```

The GID 10011(0x271b) is mapped to the SID:

```
key(10) = "GID 10011\00"
```

```
data(45) = "S-1-5-21-1648954188-37496250-1844936127-6643\00"
```

The host user CIFS\$271B will have the UIC [23433,23433] where 23433 is the octal value of 0x271B.

49

[23-sept-2008] - HP OpenVMS Technical Update Days



From the SMB.CONF file provided, we see if the idmap uid and idmap gid ranges are same:

```
idmap uid = 10000-20000
```

```
idmap gid = 10000-20000
```

The owner of a file is cifs\$271b:

```
test.txt;1      [CIFS$271B]          (RWED,RWED,RE,)
```

The UID 10011 (0x271b) is mapped to the SID:

```
key(10) = "UID 10011\00"
```

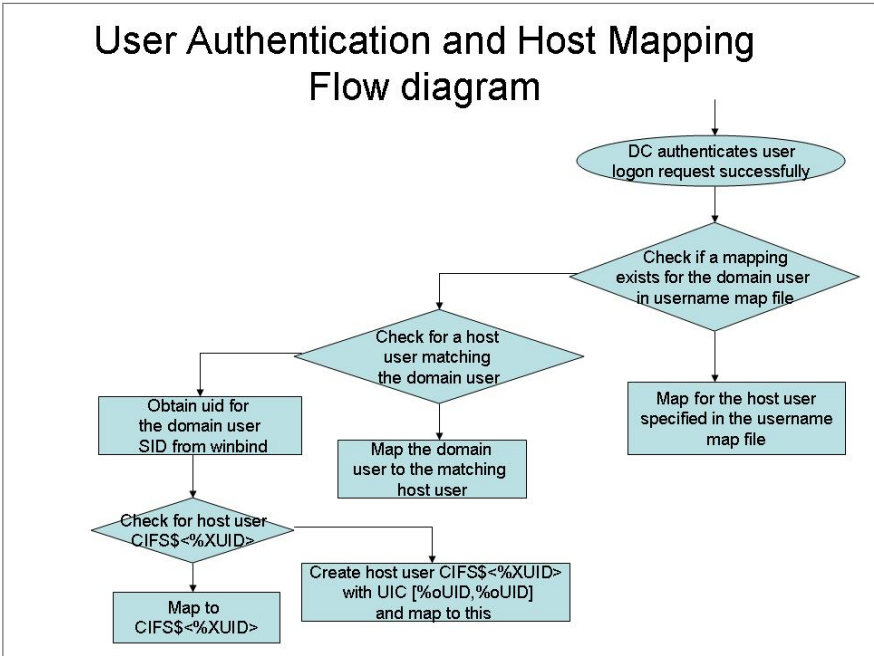
```
data(46) = "S-1-5-21-3788632709-619170709-2383488769-1155\00"
```

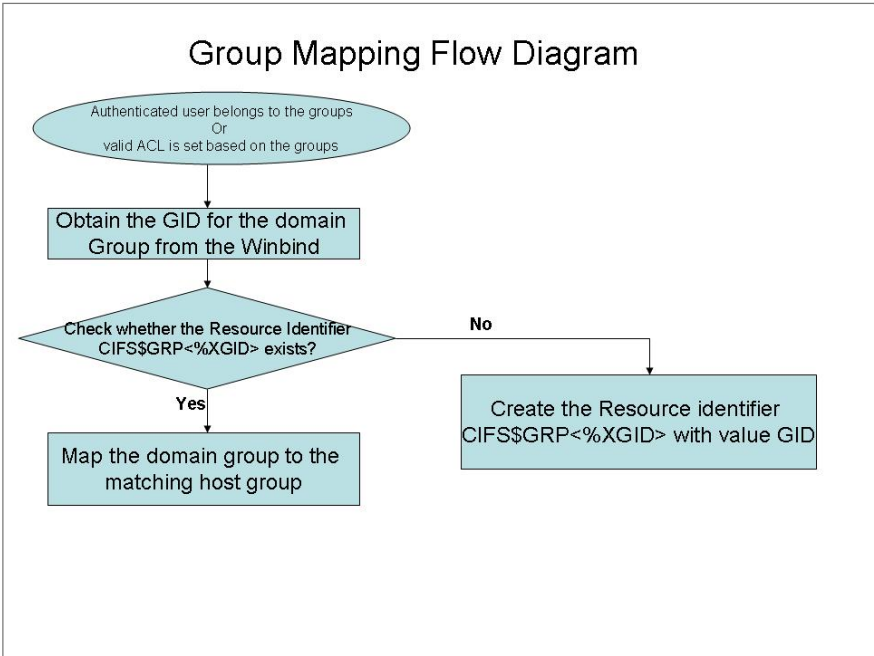
The GID 10011(0x271b) is mapped to the SID:

```
key(10) = "GID 10011\00"
```

```
data(45) = "S-1-5-21-1648954188-37496250-1844936127-6643\00"
```

The host user CIFS\$271B will have the UIC [23433,23433] where 23433 is the octal value of 0x271B. As you know, the first part 23433 represents the group id in the UIC. Based on the protections as shown





## Winbind – User and Group mapping

- To view the already mapped host users and resource identifiers, execute and select the required option:

```
$ @samba$root:[bin]samba$uaf_to_cifsname.com
```

VMS hostnames to CIFS domain names converter

This utility allows you to view CIFS domain names for the corresponding host users and resource identifiers

- 1 - Convert all CIFS\$XXXX VMS usernames to CIFS usernames
  - 2 - Convert all CIFS\$GRPXXXX VMS resource identifiers to CIFS groupnames
  - 3 - Convert a CIFS\$XXXX name to CIFS username
  - 4 - Convert a CIFS\$GRPXXXX name to CIFS groupname
- [E] – Exit

Enter your option:



## Username Mapping (1 of 3)

- Similar to host mapping in Advanced Server, which allows you to map domain usernames to host names.
- Specified using the following parameter in the smb.conf file under [global] section:  
username map = /samba\$root/lib/username.map  
NOTE: CIFS supplies the template file samba\$root:[lib]username.map. If you create your own username map file, make sure it is of STREAM\_LF format.
- In the map file “#” or “;” is used to indicate the comment line
- The entries includes a single <vms-host-name> on the left of “=” and a list of usernames on the right.  
system=GANGES\administrator



## Username Mapping (2 of 3)

- Allows you to map Windows usernames that have spaces in them by using double quotes around the name.

Ganga="Himalaya River"

- Allows you to map multiple users to a single hostname

asvuser=GANGES\narmada GANGES\kaveri

- Allows you to map all the users to a single hostuser

samba\$guest=\*

Note: this line overrules all others unless you FIRST do:

- "!" stops the search if mapping entry is found

!cifsuser=GANGES\Tunga

Note: Useful when you map all users to single hostuser as in  
samba\$guest=\*



## Username Mapping (3 of 3)

- For member server, username mapping is applied after successful authentication
- For domain Controllers and Standalone Servers, the username mapping is applied prior to validating the user credentials.



## Managing local member server users (1 of 2)

- Add hostuser to SYSUAF database with /ADD\_IDENTIFIER and /flag= NODISUSER
- Ensure that you create hostuser with UNIQUE UIC
- Local CIFS user account can be added using:  
\$ PDBEDIT -a <user-name>  
  
Note: <user-name> must be same as the created hostuser
- Local CIFS user account can be deleted using :  
\$ pdbedit -x <user-name>
- To set various flags, the CIFS user account can be modified using:  
\$ pdbedit -r <user-name>



## Managing local member server users (2 of 2)

- To change the local user password:
  - System Administrators can use the SMBPASSWD utility as below:
    - \$ smbpasswd user-name
    - New SMB password:
    - Retype new SMB password:

### NOTE:

Domain users should use the “change password” option by pressing the CTRL-ALT-DELETE from the Windows client.



## Managing local member server groups (1 of 4)

- Local CIFS groups are not needed unless you want to set permission based on local groups
- Using VMS security, you can also set permission for shares/directories/files without having local groups
- To manage a local group, login using privileged VMS account
- In the following examples we will use cifsadmin as the privileged user account



## Managing local member server groups (2 of 4)

- To add a "local" group on the CIFS member server, first add the "Resource Identifier" as below:

```
$mc authorize add/identifier/attribute=resource <vms-group>
```

- Add the "local" group on the CIFS member server, as below:

```
$ net rpc group add <local-group> "-L" "-S" <cifs-node-name> "-U"  
cifsadmin%"<pwd-of-cifsadmin>"
```

- Using the "net" command, map the VMS group represented by the "Resource Identifier" to the member server "local" group as below:

```
- $ net groupmap add unixgroup=<vms-group> type=local ntgroup=<local-  
group> "-S" <cifs-node-name> "-U" cifsadmin%"<pwd-of-cifsadmin>"
```



## Managing local member server groups (3 of 4)

- To list the "local" groups in the CIFS member server, use:  
`$ net rpc group list "-S" <cifs-node-name> "-U" cifsadmin%"<pwd-of-cifsadmin>"`
- To add "local" user to "local" CIFS group, use:  
`$ net rpc group addmem <local-group> <local-user> "-S" <cifs-node-name> "-U" cifsadmin%"<pwd-of-cifsadmin>"`
- To list the members of the "local" CIFS group, use:  
`$ net rpc group members <local-group> "-S" <cifs-node-name> "-U" cifsadmin%"<pwd-of-cifsadmin>"`



## Managing local member server groups (4 of 4)

- To add a "domain" user or group to a "local" CIFS group, use:  

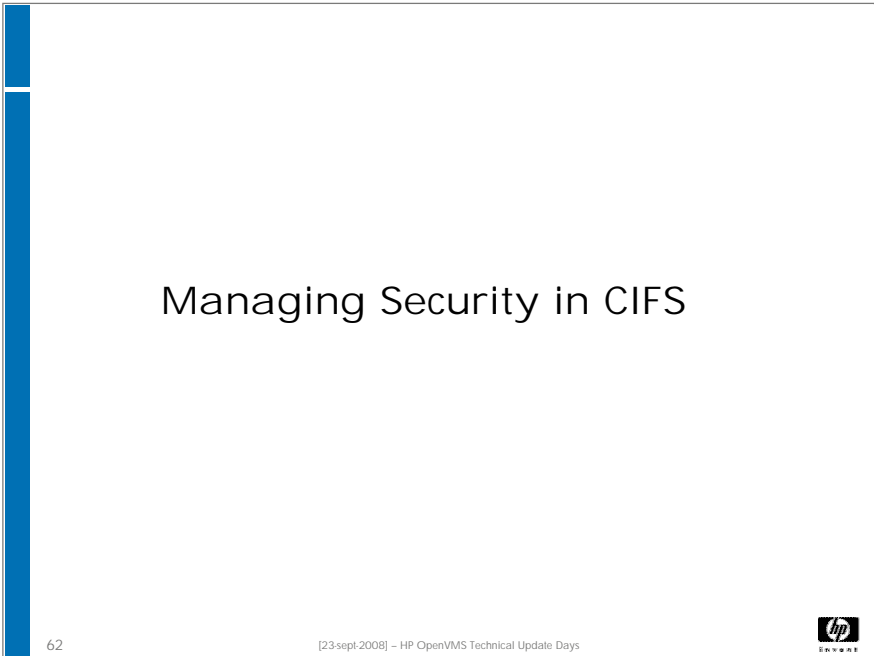
```
$ net rpc group addmem <local-group> <domain-name>\<domain-user-or-group>  
"-S" <cifs-node-name> "-U" cifsadmin%"<pwd-of-cifsadmin>"
```

Note: The domain user must have accessed the server before you can do this.  
Unless when he is mapped to a VMS user.
- To delete "domain" user or group from the "local" CIFS group, use:  

```
$ net rpc group delmem <local-group> <domain-name>\<domain-user-or-group>  
"-S" <cifs-node-name> "-U" cifsadmin%"<pwd-of-cifsadmin>"
```
- To delete the "local" CIFS group, use:  

```
$ net rpc group delete <local-group> "-S" <cifs-node-name> "-U"  
cifsadmin%"<pwd-of-cifsadmin>"
```






Managing Security in CIFS

62

[23-sept.2008] - HP OpenVMS Technical Update Days



## Security — Setting Protection (1 of 2)

File/Dir/Shares protection can be set/modified using either

- I. CIFS Member server files and directories' protection can be set from any Windows system in the domain as below:
  1. Make sure you connect to the CIFS share using the privileged user.
  2. Go to the directory or files that you want to set protection.
  3. Go to Properties -> Security tab, you will see the protection for <user>, <group> and <world/Everyone>.
  4. Select the <user>, <group> and <world/Everyone> that you want to edit for this <file/directory>" and click the proper permissions.
  5. Click "Apply" or "OK" to effectuate the permissions.
  6. Verify the security protection settings on the command line in the host system, using the below command.  
\$Dir/prot <file/dire path>



## Security — Setting Protection (2 of 2)

II. File/Dir protections can be set from native VMS DCL command as below:

- \$set security/prot=(ownership[:access][,...])
- \$ edit\acl <file>

## Security — Setting ACL

Setting permissions using \$ SET SECURITY DCL command:

1. Login to VMS system using a fully privileged VMS account, say "SYSTEM"
2. For setting ACLs based on the "users", find out the identifier of a user as below:
  - For "local" user, the identifier will be the local host username.
  - For "Domain" user execute the below script and choose the option 1  
\$ @samba\$root:[bin]samba\$uaf\_to\_cifsname.com  
The hostname displayed for each domain user is the identifier for that domain user.  
You may also have to take a look at the file samba\$root:[lib]username.map.
3. For setting ACL's based on the groups, find out the resource identifier of the group as below:
  - For "Domain" group execute the above script and choose the option 2
  - For "local" group execute the following command:  
\$ net groupmap list  
The name that maps to the corresponding local group is the resource identifier.



## Security — Setting ACL

4. Execute the following command to add an ACL to the file/share/folder.

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

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

5. To remove the ACL execute the following command:

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

- 4/5. It could be much easier to use the ACL editor in VMS

```
$ edit/acl <file>
```

## Security — ACLs

### Example

After setting the ACL for user and group the "Access control List" is as below:


```
$ dir/sec test123.dir
Directory DKA0:[ARAVINDA.SAMBA.TEMP.TEST]
test123.DIR;1 [TELNETS,TEST1] (RWED,RWED,.)
  (IDENTIFIER=CIFS$MASK,ACCESS=READ+WRITE+EXECUTE+DELETE)
  (IDENTIFIER=CIFS$GRP1389,ACCESS=READ+EXECUTE)
  (IDENTIFIER=[CIFS$2710],ACCESS=READ+EXECUTE)
```

Where CIFS\$GRP1389 is mapped to "Domain Users" and CIFS\$2710 has been mapped to one of the users in the domain.

- CIFS\$MASK acts as a permission mask for all ACLs that specifically mention a user or group.

NOTE: - If you need OPTIONS=DEFAULT or DEFAULT\_PROTECTION support in ACL's, you need explicitly set the "inherit acls = yes" for the share. (slide 41)






Tools & Utilities to manage CIFS

68

[23-sept.2008] – HP OpenVMS Technical Update Days



## Tools to manage CIFS Server — SMBSTATUS

- Reports current Samba sessions and share connections.
- Used to list locks and byte range locks.
- Reports current open files.
- Better overview if you put your monitor to 132 columns.



## Tools to manage CIFS Server — NET

- Tool for administration of local and remote CIFS servers.
- The CIFS net utility is meant to work just like the “net” utility available for Windows and DOS.
- NET is a generic command for various CIFS management.
- The first argument to NET is used to specify the protocol when executing certain commands.
- Below are the set of protocols available under NET:
  - ADS is used for Active Directory.
  - RAP is using for old (Win9x/NT3) clients
  - RPC is used for NT4 and Windows 200x.
- If this argument is omitted, net will try to determine it automatically.
- Not all commands are available on all protocols.



## Tools to manage CIFS Server — NET LOOKUP

- Lookup option is used for various "lookup" operation as noted below.
- To get the IP address of the given host with the specified type use the below command

```
$net lookup [host] HOSTNAME[#<type>]
```

where type is "netbios suffix". The type defaults to 0x20 which is server

- To get the IP of domain controller execute the below command

```
net lookup dc [domain]
```

- To get the IP of Master browser execute the below command

```
net lookup master [domain|wg]
```



## Tools to manage Samba — NET RPC

- RPC protocol option of the NET command provides number of samba management functionalities. Listed below are few of the same:

net rpc info	:	Shows the basic info about a domain
net rpc join	:	To join a domain as Member Server
net rpc testjoin	:	Tests whether join is valid or not
net rpc share	:	To add, delete, list shares of the domain database.
net rpc file	:	To list open files.
net rpc service	:	To start, stop and query services.
net rpc shell	:	To open an interactive shell for remote server/account management



## Tools to manage Samba — NMBLOOKUP

- NetBIOS over TCP/IP client used to lookup NetBIOS names.
- This is used to query NetBIOS names and map them to IP addresses in a network using NetBIOS over TCP/IP.
- The options allow the name queries to be directed at a particular IP broadcast area or to a particular machine like a WINS server .
- All queries are done over UDP.



## Wbinfo Utility

- “Wbinfo” tool can be used to query information from winbind.
- The “wbinfo” program queries and returns information created and used by winbind.
- Below are some of the most commonly used “wbinfo” options
  - Lists all domain users and domain groups
    - wbinfo --domain-groups / wbinfo -g
    - wbinfo --domain-users / wbinfo -u
  - Ping domain
    - wbinfo --version / wbinfo “-V”
  - wbinfo --own-domain
    - wbinfo --own-domain



## Winbind and Wbinfo Utility (Cont.)

- commonly used “wbinfo” options (Cont.)
  - Get the SID from the user or Group
    - `wbinfo --name-to-sid=test1`
  - Get the name from the SID value
    - `wbinfo --sid-to-name=<sid-value>`
  - lookup all groups that a user is a member of.
    - `wbinfo --user-groups=cifsdom\administrator`
  - Sequence number
    - `wbinfo --sequence`




Questions

# Questions ?

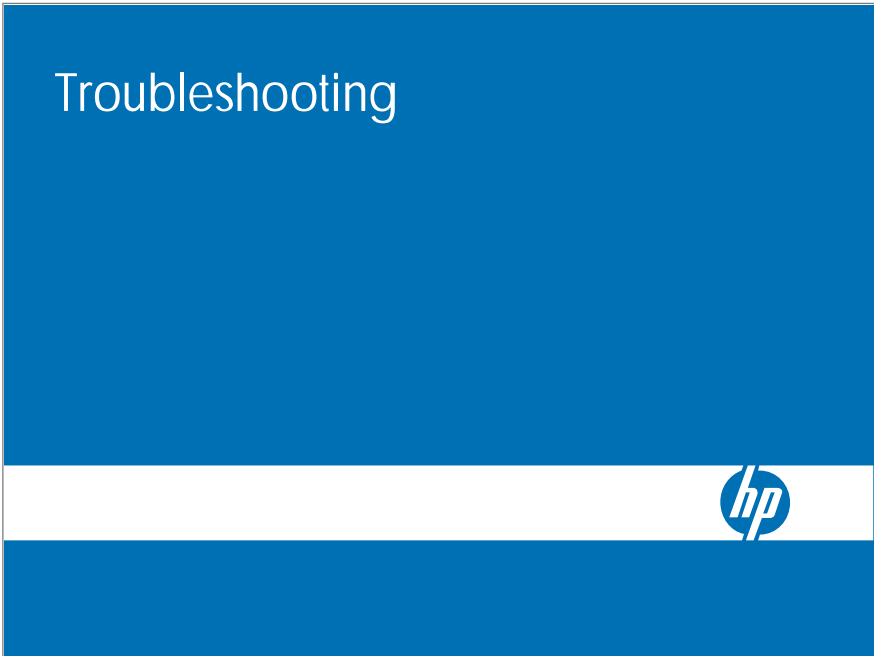
76

[23-sept.2008] – HP OpenVMS Technical Update Days



Have a break ??





## Overview

- Performance Issues
- TDB File Information
- Debug Logging
- Miscellaneous Utilities and Commands
- References



## Performance Issues (1 of 2)

### To improve CIFS performance:

- Install the latest CIFS version and patches
- Do not put the samba\$root: directory tree on the System disk
- Disable volume highwater marking to improve writes
- Use ODS-5 volumes (for variable length files)
- Use a disk cluster size that is a multiple of 16
- Modify SAMBA\$ROOT:[BIN]SAMBA\$SMBD\_STARTUP.COM
  - change the line "\$ set rms\_default /extend\_quantity=10240 /BUFFER\_COUNT=8 /BLOCK\_COUNT=127
  - " to:
  - \$ set rms\_default /extend\_quantity=10240 /BUFFER\_COUNT=8 [/BLOCK\_COUNT=m]

Note: For EVA and XP storage enclosures, specify a block\_count ('m') of 124 (EVA) or 96 (XP).

80

[23-sept-2008] - HP OpenVMS Technical Update Days



To move the samba\$root: directory tree to another disk:

1. Shutdown CIFS (cluster-wide, if CIFS configuration is shared by other cluster members)
2. Make note of the current definition of the logical name SAMBA\$ROOT (no colon)
3. Move the files using BACKUP
4. Update the definition of the samba\$root logical name in sys\$startup:samba\$define\_root.com (on each applicable system disk)
5. Execute \$ @sys\$startup:samba\$define\_root (on each CIFS cluster member, if applicable)
6. Start CIFS (on each CIFS cluster member, if applicable)
7. Verify functionality
8. Delete old files

```

$ @sys$startup:samba$shutdown
$ show logical samba$root
"SAMBA$ROOT" = "HOMERJ$DKAO:[SYSO.SYSCOMMON.SAMBA.]" (LNM$SYSTEM_TABLE)
$ backup HOMERJ$DKAO:[SYSO.SYSCOMMON.SAMBA...]*.*;*
  disk$data1:[samba...]
$ edit/edt sys$startup:samba$define_root.com
$ @sys$startup:samba$define_root
$ @sys$startup:samba$startup

```

- To disable highwater marking on a volume either:
  - a. Include the /NOHIGHWATER\_MARKING qualifier when initializing the volume, or
  - b. Dismount the volume and execute:

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

- File headers on ODS-5 volumes contain 2 additional fields which can improve read performance. These fields, collectively known as the "file length hints" are "Record count" and "Data byt

## Performance Issues (2 of 2)

### To improve CIFS performance:

- [Global] parameters in `samba$root:[bin]smb.conf` to improve performance:

<code>mangled names = no</code>	(Don't calculate 8.3 file names)
<code>host msdfs = no</code>	(Disable MS DFS support)
<code>msdfs root = no</code>	(Disable MS DFS support)
<code>log level = 0</code>	(Minimize debug logging)
<code>case sensitive = yes</code>	(Stop translating filenames)
<code>change notify = no</code>	(Don't scan directories for changes)

## TDB File Information

### TDB = Trivial Database

- Allow multiple, simultaneous writers
- Implemented using RMS Indexed files
- Locations: samba\$root:[private] & [var.locks...]
- Some are persistent and should be backed up
- Some are temporary and do not need to be backed up



- All persistent tdb files must be preserved during machine migrations, updates and upgrades.

#### •Persistent TDB Files/Descriptions

Name	Description
account_policy	Samba/NT account policy settings, includes password expiration settings.
group_mapping	Mapping table from Windows groups/SID to UNIX groups.
ntdrivers	Stores per-printer installed driver information.
ntforms	Stores per-printer installed forms information.
ntprinters	Stores the per-printer devmode configuration settings.
passdb	Exists only when the tdbsam passwd backend is used. This file stores the SambaSAMAccount information.
registry	Read-only database of a Windows registry skeleton; supports exporting various database tables via the winreg RPCs.
secrets	This file stores the Workgroup/Domain/Machine SID, the LDAP directory update password, and a further collection of critical environmental data that is necessary for Samba to operate correctly. This file contains very sensitive information that must be protected. It is stored in the SAMBA\$ROOT:[PRIVATE] directory.
share_info	Stores per-share ACL information.
winbindd_idmap	Winbindd local IDMAP database.

#### •Temporary TDB Files/Descriptions

Name	Description
brlock	Byte-range locking information.
connections	A temporary cache for current connection information used to enforce max connections.

## Debug Logging (1 of 3)

### Samba logging features can prove extremely useful

- The amount of debug information output is set using log levels
- Log levels range in values between 0 - 10 (10 = most verbose)
- The log level may be set in 3 ways:
  - Using the "log level" global parameter in smb.conf
  - Using the -d option on the command line (precedence)
  - Using the SMBCONTROL utility (\$ smbcontrol <PID> debug 5)
- Use the include statement for workstation specific debugging
  - Include = samba\$root:[lib]smb.conf-%m
  - This smb.conf-<PCname> should have: log level = 1 to 10

83

[23-sept-2008] - HP OpenVMS Technical Update Days



• Explicitly set "log level = 0" in smb.conf global section to keep logging to a minimum (can't be completely disabled).

• Most problems can be identified using a log level of 3. It may be necessary to increase the log level to 5 or even 10 in some cases.

• Alternately, fine-tune debug logging using Debug Classes in the smb.conf "log level" parameter. The following classes exist:

tdb, printdrivers, lanman, smb, rpc\_parse, rpc\_srv, rpc\_cli, passdb, sam, auth, winbind, vfs, idmap, quota, acls, locking, msdfs, dmapi

To specify a log level for a class, separate the class name and its log level by a colon. An example:

## Debug Logging (2 of 3)

- NMBD log file is `samba$root:[var]log_<nodename>.nmbd`
  - New version is NOT created each time NMBD process starts
  - Log level set in `samba$root:[bin]samba$nmbd_startup.com`
  - Must restart NMBD process to affect log level change
- CIFS utilities output debug information to the standard output device
  - E.g. `$ net rpc testjoin -d5`

84

[23-sept-2008] – HP OpenVMS Technical Update Days



Directory `SAMBA$ROOT:[BIN]`

`SAMBA$NMBD_STARTUP.COM;1`

`SAMBA$SWAT_NMBD_SHUTDOWN.COM;1`

`SAMBA$SWAT_NMBD_STARTUP.COM;1`

## Debug Logging (3 of 3)

### SMBD debug log file

- Name and location set by SMB.CONF global parameter "log file"
- Default setting creates separate log for each client
  - log file = /samba\$root/var/log\_%h.%m
  - %h = hostname of the server
  - %m = NetBIOS name of client
- New version is NOT created if one exists
- \$ @samba\$root:[bin]samba\$gatherinfo.com

85

[23-sept-2008] - HP OpenVMS Technical Update Days



• SMBD debug logs often the best source for determining problem cause

• Can also set the SMBD debug level using the logical name SAMBA\$SMBD\_OPTIONS:

```
$ DEFINE/SYSTEM SAMBA$SMBD_OPTIONS "-d3"
```

The logical is translated by SAMBA\$SMBD\_STARTUP.COM and included on the SMBD command line

## Miscellaneous Commands

- NMBLOOKUP – Test NetBIOS name resolution
- NET CACHE LIST – Display NetBIOS name cache
- NET CACHE FLUSH – Clear NetBIOS name cache
- SMBVER – Display image versions
- SMBSHOW – Display CIFS processes
- SMBCLIENT – Access SMB/CIFS resources
- SMBSTATUS – Display CIFS status information
- SMBCONTROL – Send signals to nmbd and smbd processes
- NET RPC TESTJOIN – Verify domain membership
- TDBDUMP – Dump the contents of a .TDB file
- TDBBACKUP – Make backup copies of .TDB file

86

[23-sept-2008] – HP OpenVMS Technical Update Days



- nmblookup - NetBIOS over TCP/IP client used to lookup NetBIOS names

Usage: <NODE> ...

-B, --broadcast=BROADCAST-ADDRESS	Specify address to use for broadcasts
-f, --flags	List the NMB flags returned
-U, --unicast=STRING	Specify address to use for unicast
-M, --master-browser	Search for a master browser
-R, --recursion	Set recursion desired in package
-S, --status	Lookup node status as well
-T, --translate	Translate IP addresses into names
-r, --root-port	Use root port 137 (Win95 only replies to this)
-A, --lookup-by-ip	Do a node status on <name> as an IP Address

To obtain a list of names, include "-S" or -status

To query by IP address, use "-A" (implies "-S" too)

To query a WINS server, include "-RU" <wins-server-address>

To query for a specific name type, append '#<type>' to the name (i.e., mydomain#1b).

- SMBCONTROL:

- Specifying a destination of "nmbd" or "smbd" does not work – use Process IDs (PID) displayed by \$ smbstatus or \$ smbshow

- Some useful options:

\$ smbcontrol <pid> close-share <sharename>   *	! Disconnect users from <sharename> or all shares (*)
\$ smbcontrol <pid> shutdown	! Terminate a process
\$ smbcontrol <pid> debug <n>	! Reset the debug level of a process
\$ smbcontrol <pid> debuglevel	! Show the debug level in use for a process

## References

- HP OpenVMS CIFS Home Page

[http://h71000.www7.hp.com/network/CIFS\\_for\\_Samba.html](http://h71000.www7.hp.com/network/CIFS_for_Samba.html)

- Samba Home Page

<http://www.samba.org>



# Migrating From Advanced Server to CIFS




## What Needs to be Migrated?

- SAM database accounts
- Host mappings
- File and Print shares and their security
- Files and Folders and their security
- Print queues, print forms, print drivers and queue logicals

## What will not be migrated?

- Alertnames
- Share and File Audit policies
- Registry parameters
- WINS address
- Number of clients configured on AS
- In case of MS: (is this in case of user accounts)
  - Workstation restriction details
  - Some of the logon flags viz. logon script, account policy etc.
  - Account passwords

90
[23-sept.2008] – HP OpenVMS Technical Update Days


Logon Flags which are not migrated in MS:

Login script is executed, Account cannot be deleted, Account is locked out, Password cannot be changed, Password is expired

Registry Parameters which are not migrated from MS:

listenname

maintainserverlist

Restrictanonymous

Domain

NT\_print\_enable

Lmcompatibilitylevel

EnableSecuritySignature (both rdr and server)

RequireSecuritySignature (both rdr and server)

Autodisconnect

Srvcomment

Srvhidden

Userpath

## Prerequisites

- HP Advanced Server V7.3B for OpenVMS is installed with minimal patch set 13 on Advanced Server system.
- CIFS V1.1 with minimal patch set 3 on the CIFS system.
- Backup all the Advanced Server shares and the related data.
- Migration can be done only if the Advanced Server and CIFS have been configured as Member Server and in the same domain.
- Migration across different AS and CIFS configurations is not supported
- Copy ASV\_MIGRATION.BCK file provided from our FTP site to the Advanced Server system



## Migration Process

Migration Process should follow the below procedure:

1. Migration steps on the Advanced Server
  - Generating reports for AS data
  - Cleanup of files
  - Transfer reports to CIFS node
2. Migration steps on CIFS
  - Run the reports from step 1



## Setting up reports software on AS

- Verify that the Advanced Server is running and configured as Member Server.
- Restore ASV\_MIGRATION.BCK to any work directory; for example

```
$ BACKUP ASV_MIGRATION.BCK/SAVE DISK$DATA1:[ASV_MIGRATION]
```

NOTE: ASV\_MIGRATION.BCK is supplied as part of CIFS installation.

- Install migration files; for example:

```
$ SET DEF DISK$DATA1:[ASV_MIGRATION]
$ COPY PWRK$MIGRATION.EXE;1 SYS$COMMON:[SYSEXE]
$ COPY GET_DRIVER_INFO.EXE SYS$COMMON:[SYSEXE]
$ COPY GET_QUEUE_INFO.EXE SYS$COMMON:[SYSEXE]
```



## Generating reports on AS.

- On AS node which is configured as MS:
  - Verify that same user name and password exists both in the local MS database and in the domain.
  - The local user account must be a privileged account (i.e., member of the local Administrators group)
- Execute the migration procedure:
  - \$ Set def DISK\$DATA1:[ASV\_MIGRATION]
  - \$ @PWRK\$CIFS\_MIGRATION.COM

94

[23-sept.2008] – HP OpenVMS Technical Update Days



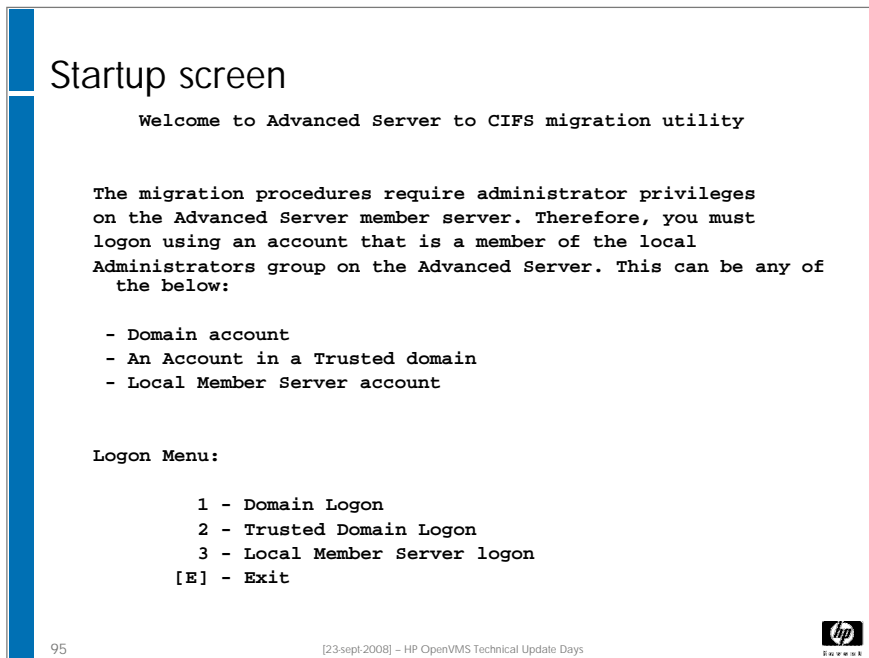
Verify that the same user name and password exist both in the local Member Server database and in the domain. If not, create an user account in the local Member Server database and on the domain PDC emulator. To do this, enter the following commands:

Adding CIFSADMIN user to domain database:

```
$ ADMIN LOGON ADMINISTRATOR
$ ADMIN ADD USER CIFSADMIN/PASSWORD="Any1willd0"
```

Adding CIFSADMIN user to local Member server database:

```
$ ADMIN LOGON ADMINISTRATOR /DOMAIN = \\<local member
server name>
$ ADMIN ADD USER CIFSADMIN/PASSWORD="Any1willd0"
/MEMBER="Administrators"
```



message shown:

Enter your option: 1

You have choosen to login to the Domain: EMEA

Please enter the username and password

=====  
=====

screen 2:

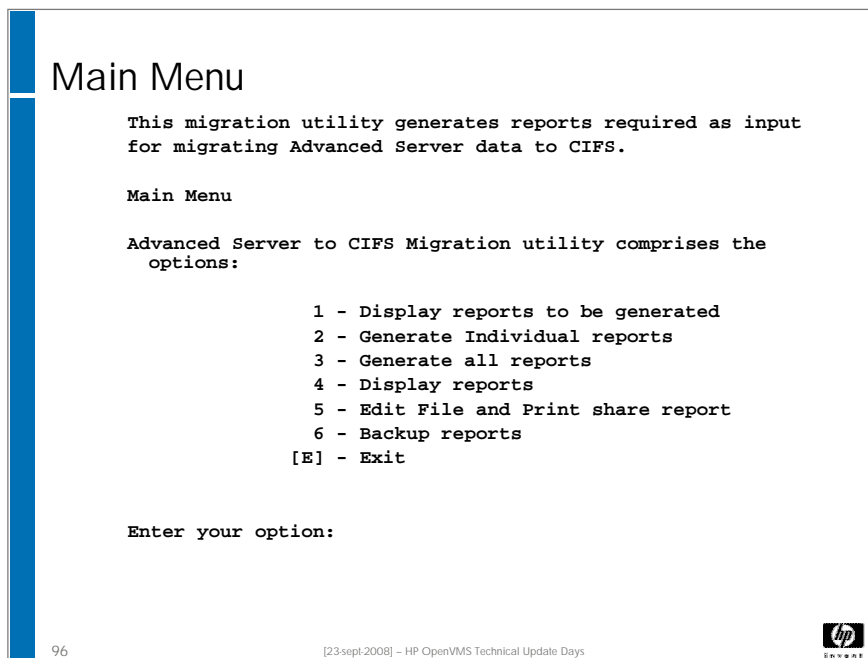
Username: hosang

Password:

The server \\G6W0031 successfully logged you on as Hosang.

Your privilege level on domain EMEA is USER.

The last time you logged on was 11/07/08 08:07 AM.



Option 1 - Displays the reports that can be generated on the Advanced Server node.

Option 2 - You can select this option to generate the individual reports. For example, you can generate report only for the File Security migration.

Option 3 - You can select this option to generate all reports at a time for the following:

- User and group migration report in the case of Member Server
- Hostmapping report
- File and print share related reports
- File security report

Option 4 - You can select this option to view any of the already generated reports

Option 5 - You can select this option to edit the file and print share report. You may have to change the device or logical names in share paths so that it is valid on the CIFS server, or you may have to remove shares from the report so that they are not migrated.

Option 6 - You can select this option to back up the generated Advanced Server reports. You must back up reports only after you have generated all the reports about the Advanced Server.

#### Note

If you select option 2 or option 3, you will be prompted for user credentials.

If the Advanced Server is configured as Member Server, you must enter local member server administrator credentials to generate the user and group reports.

To generate all other reports, you must enter domain administrator account credentials.

(both the local and domain account will be same)

If you select File and Print share related reports as part of option 2 or if you select option 3, you are prompted with the following:

Are you migrating Advanced Server data to CIFS on this node itself [N]?:

If you want to migrate data on the same node answer "YES" otherwise say "NO".

## Option 1, Display reports to be generated

for MEMBER server:

Display information Menu

The Advanced Server reports which can to be generated on this node:

- User and group reports
- Hostmapping report (If hostmap accounts exist)
- File and Print share report
- Print queues/drivers/forms/logical reports (if any)
- File security report

Press enter to return to the main menu:



## Option 1, Display reports to be generated

for PDC or BDC:

Advanced Server is configured as PDC or BDC on this node. Hence, you cannot generate SAM database related reports like users, groups, etc., using this utility. NET RPC VAMPIRE command should be executed on CIFS node to migrate SAM database information.

The Advanced Server reports which can to be generated on this node:

- Hostmapping report (If hostmap accounts exist)
- File and Print share report
- Print queues/drivers/forms/logical reports (if any)
- File security report

Press enter to return to the main menu:



## Option 3, generate individual or all reports

### Generate Individual report menu

- 1 - User and group reports
- 2 - Hostmapping report
- 3 - File and print share related reports  
[This option generates reports about File and Print shares, Print queues/drivers/forms/logicals (if any)]
- 4 - File Security report
- [E] - Exit Menu

Enter your option:



## Option 3. 1 - User and group reports

!!! Member Server only !!!

Generating user and group reports

Advanced Server user and group reports are being generated.  
Please wait until you receive completion message...

Now generating reports for migrating local users...  
Generating reports for local users is complete.

Now generating reports for migrating local groups...  
Generating reports for local groups is complete.

Generation of Advanced Server reports for users and Groups is  
complete.

Press enter to return to the previous menu:



## Option 3. 1 - User and group reports

in case of a second run the following messages are displayed:

```
A file named PWRK$USER_MIGRATION.COM is present in the current
directory location. It is now renamed to PWRK$USER_MIGRATION.OLD
%RENAME-I-RENAMED,
  PWRK$COMMONROOT:[MIGRATION]PWRK$USER_MIGRATION.COM;1 renamed
to PWRK$COMMONROOT:[MIGRATION]PWRK$USER_MIGRATION.OLD;1
```

```
A file named PWRK$GROUP_MIGRATION.COM is present in the current
directory location. It is now renamed to PWRK$GROUP_MIGRATION.OLD
%RENAME-I-RENAMED,
  PWRK$COMMONROOT:[MIGRATION]PWRK$GROUP_MIGRATION.COM;1 renamed
to PWRK$COMMONROOT:[MIGRATION]PWRK$GROUP_MIGRATION.OLD;1
```



## Option 3. 2 -Hostmapping report

Generating Hostmapping account report

Generating report for hostmapped accounts in Advanced Server...  
Please wait until you receive completion message...

```
%DELETE-I-FILDEL,  
  PWRK$COMMONROOT:[MIGRATION]ADMIN_HOSTMAP_INFO.TMP;1 deleted  
Generation of Hostmapping report completed.
```

Press enter to return to the previous menu:

Resulting file: AS\_HOSTMAP\_INFO.OUT  
Layout:  
RUSCH = EMEA\RuschP



### Option 3. 3 File and print share related reports

Generating File and Print share related reports

Are you migrating Advanced Server data to CIFS on this node  
itself [N]?:

Generating File and Print share related reports...

Please wait until you receive completion message...

```
%DELETE-I-FILDEL,  
PWRK$COMMONROOT:[MIGRATION]GATHER_QUEUE_INFO.COM;1 deleted  
Generation of File and Print share related reports is complete.
```

Press enter to return to the previous menu:

Resulting file: ASV\_SHARE\_INFO.COM

Layout for each share:

```
$ say "Adding Disk Share KITS"  
$ write SHARE_FILE_HNDL "Adding Disk Share KITS"  
$ add_dskshare "KITS|null|DKA0:[KITS]|0|2"
```



## Option 3. 4 - File Security report

Generating File security reports

Generating File security report...  
Please wait until you receive completion message...

Generating reports for migrating File security for share  
BAKKERP...

Completed generating reports for migrating File security for  
share BAKKERP.

Generating reports for migrating File security for share  
HOSANG...

!!!! This can take a long time !!!!  
Depending on the number of files in the share, the number of  
security records per file and the Domain topology.  
7 hours on a share with 28000 files and w2008 PDC overseas.  
8 minutes on same node as BDC in local domain.

Resulting files: PWRK\$FILEACLMIG\_<share>\_0000.COM



## Option 3. 5 - edit file share report.

you can edit the file `asv_share_info.com` to skip shares that should not be migrated like netlogon and users.

please remove or comment out the following lines.

```
$! say "Adding Disk Share NETLOGON"  
$! write SHARE_FILE_HNDL "Adding Disk Share NETLOGON"  
$! add_dskshare "NETLOGON|Logon Scripts  
Directory|PWRK$LMROOT:[LANMAN.REPL.IMPORT.SCRIPTS]|0|2"
```

There is such a part for each share.

## Cleanup of files

Once all the reports are generated on AS,  
make sure you backup all the reports using option:

6 - Backup reports

This will cleanup all report files in your current directory and put  
them in the files:

AS2CIFS\_MIGRATION\_REPORTS.BCK

PRINTER\_DRIVERS.BCK

Then delete the files:

PWRK\$MIGRATION.EXE,  
GET\_DRIVER\_INFO.EXE and  
GET\_QUEUE\_INFO.EXE in SYS\$COMMON:[SYSEXE]



## Transfer reports to CIFS node

- Verify AS2CIFS\_MIGRATION\_REPORTS.BCK is present in DISK\$DATA1 :[ASV\_MIGRATION]
- If not, execute pwrk\$cifs\_migration.com again and backup reports through option 6.
- Copy AS2CIFS\_MIGRATION\_REPORTS.BCK and PRINTER\_DRIVERS.BCK to CIFS node
- On CIFS node, restore files present in the backup saveset AS2CIFS\_MIGRATION\_REPORTS.BCK to the directory SAMBA\$ROOT:[BIN]

107

[23-sept.2008] – HP OpenVMS Technical Update Days



AS2CIFS\_MIGRATION\_REPORTS.BCK can contain hundreds of files (at least one for each share plus others) and there is no cleanup procedure.

It may be wise to unpack the saveset in another directory like samba\$root:[migration]

This will work for all reports EXCEPT the hostmapping report, this must be copied to samba\$root:[bin]

## Migration Steps on CIFS

- SAM database migration
- Hostmapping migration
- File migration
- File and Print share related migration
- Share Security migration
- File Security migration



## SAM database migration — MS (1 of 4)

Log in to OpenVMS (with a privileged account)

Verify CIFS is a Member Server

```
$ @SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
$ TESTPARAM
...
Server role: ROLE_DOMAIN_MEMBER
```

Verify CIFS is in the same domain as AS:

```
$ pipe testparm -sv | search sys$pipe workgroup
```

Create an OpenVMS account with full privileges  
(i.e., CIFSADMIN)

Create the same privileged account on the CIFS server

109

[23-sept.2008] – HP OpenVMS Technical Update Days



Create an OpenVMS account 'CIFSADMIN' and grant full privileges.  
For example, to add an OpenVMS account 'CIFSADMIN', enter the following command:

```
$ MC AUTHORIZE
```

```
UAF> ADD CIFSADMIN/UIC=[400,1]/PRIV=ALL/DEFPRIV=ALL /ADD_IDENTIFIER -
_UAF> /OWNER=CIFSDOM/DEVICE=SAMBA$ROOT/DIRECTORY=[USERS] -
_UAF> /NOBATCH/NOLOCAL/NODIALUP/NOREMOTE/FLAGS=NODISUSER
```

## SAM database migration — MS (2 of 4)

Create a local CIFS account, assuming the same username that you used while creating the reports.

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

```
$ PDBEDIT -a <username>
```

```
new password: Any1willd0
```

```
retype new password: Any1willd0
```

Edit SAMBA\$ROOT:[LIB]SMB.CONF and add the following line in the [global] section:

```
admin users = <username>
```



## SAM database migration — MS (3 of 4)

If migrating on the same node, shutdown AS

```
$ @SYS$STARTUP:PWK$SHUTDOWN          ($ pwstop)
```

Start CIFS

```
$ @SYS$STARTUP:SAMBA$STARTUP.COM      ($ smbstart)
```

Migrate users

```
$ @PWK$USER_MIGRATION
```

NOTE: Before running this command make sure the user can be created in the SYSUAF database.

- All the migrated accounts will have the password THISISCIFS
- The administrator user will give an error as there is normally no such user in the sysuaf and it is 13 characters long.

111

[23-sept-2008] – HP OpenVMS Technical Update Days



SAM database migration — PDC (1 of 2)

Configure CIFS as BDC in the same domain as AS.

Edit SAMBASROOT:[BIN]SMB.CONF and in the [global] section add:

```
workgroup = <Asdomainname>
domain logons = yes
domain master = no
add user script = @samba$root:[bin]useradd.com %u
delete user script = @samba$root:[bin]userdel.com %u
add machine script = @samba$root:[bin]useradd.com %u
```

Join the domain as a BDC

```
$ @SAMBASROOT:[BIN]SAMBA$define_COMMANDS
$ NET RPC JOIN "-U<adminusername>%password"
```

Replicate SAM accounts from the AS PDC

```
$ NET RPC VAMPIRE "S" <AS-NODE-NAME> .
$_-U<adminusername>%password"
```

Verify accounts exist on CIFS

```
$ PDBEDIT "L"
```

Shutdown the AS

```
$ @SYS$STARTUP:PWK$SHUTDOWN
```

Configure CIFS as the PDC.

Edit SAMBASROOT:[LIB]SMB.CONF and in the [global] section set, modify:

```
domain master = yes
```

Start CIFS

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

Note: Sometimes, SCSNODE name of OpenVMS system can be different from the listenname of AS. Here "AS-NODE-NAME" means listenname of AS server. To know the listenname, execute:

```
$ @sys$startup:pwk$define_commands.com
$ regutil show parameter * listenname
```

**SAM database migration — MS (4 of 4)**

Migrate groups


```
$ @PWRK$GROUP_MIGRATION
```

Starting creation of group accounts as as part of group migration from Advanced Server for OpenVMS to OpenVMS CIFS.

You need to provide privileged OpenVMS CIFS account credentials to add groups successfully.  
Please make sure that this account is also a domain account.

If you are not certain, exit this script now by answering the question  
Would you like to exit now [Y]?: n

When prompted, specify CIFSADMIN username/password

112 [23-sept.2008] - HP OpenVMS Technical Update Days 

```
@PWRK$GROUP_MIGRATION.COM;
%DELETE-I-FILDEL,
SAMBA$ROOT:[VAR]NETBIOSTEMP_00000401.TMP;1 deleted
(8KB)
```

Starting creation of group accounts as as part of group migration from Advanced Server for OpenVMS to OpenVMS CIFS.

You need to provide privileged OpenVMS CIFS account credentials to add groups successfully. Please make sure that this account is also a domain account.

If you are not certain, exit this script now by answering the question

Would you like to exit now [Y]?: n

Please enter CIFS account username: cifsadmin

Please enter password for the user CIFSADMIN:

## Hostmapping migration

- This migration should be performed only after successful SAM migration and it is assumed that AS users are migrated as part of SAM migration.
- Edit SAMBA\$ROOT:[LIB]SMB.CONF and in the [global] section set, add  
username map = /samba\$root/lib/username.map
- To Add the hostmappings execute the below command  
\$ @SAMBA\$ROOT:[BIN]SAMBA\$ADDDHOSMAP.COM
- This procedure assumes that CIFS accounts and domain accounts already exist. It does not verify the validity of the accounts.
- This migration adds VMS user account in SYSUAF database if it is not already present. The created user accounts
  - Do not have the EXTAUTH flag set
  - Non-interactive user
  - NETMBX and TMPMBX privileges

NOTE: SYSADMIN should verify the accounts that were created



## File Migration

- It is the system administrator's responsibility to transfer files and directories from AS to CIFS node
- Make sure the directory structure remains same on CIFS node just as it existed on AS node
- If the device names and logical names pointing to the share path differ on CIFS node, edit the File and print share report and update the device and logical name information
- This step can be skipped if it is a same node migration

## File and print share migration

- Before this procedure ensure successful migration of SAM database and hostmapping.
- It is most likely required to make changes to the share report if you didn't do that in step 5 on PWRK node.
 

```
$ EDIT SAMBA$ROOT:[BIN]ASV_SHARE_INFO.COM
Be it only to remove the shares pointing to pwrk$root:...
(users,netlogon,,)
```
- Perform the migration.
 

```
$ @SAMBA$ROOT:[BIN]CIFSS$SHARE_MIGRATION.COM
```
- Restore the printer driver files from the backup saveset PRINTER\_DRIVERS.BCK to the directory path pointed by the share, PRINT\$

115

[23-sept-2008] – HP OpenVMS Technical Update Days



To find out the directory path pointed by the PRINT\$ share, enter the following command:

```
$ SAMBA$ROOT:[BIN]SAMBA$DEFINE_COMMANDS.COM
$ TESTPARM
....
....
[Print$]
....
path = /SAMBA$ROOT/PRINT/DRIVERS
....
$ BACKUP SAMBA$ROOT:[BIN]PRINTER_DRIVERS.BCK/SAVE -
_ $ SAMBA$ROOT:[PRINT.DRIVERS...]*. *;*
```

## Share security migration

- The migration of share security is not currently supported
- This will be addressed in a future release



## File Security Migration

- Before this procedure ensure all the below are migrated to where CIFS is running:
  - Users and Groups
  - Advanced Server files
  - Advanced Server file and print shares
- Execute the command:  
`$ @PWRK$FILEACL_MIG_<share>*.COM`


NOTE: There can be hundreds of these procedures that needs to be run.

Questions

# Questions ?

118

[23-sept.2008] – HP OpenVMS Technical Update Days



Thanks

**Thank you**

