Samba for OpenVMS

Version 4.6-5A for OpenVMS I64 servers, based on Samba 4.6.5
Release Notes
May 2019

Introduction

VMS Software Inc. (VSI) is pleased to provide you with a new VSI-supported version of Samba for OpenVMS. This release of Samba is based on Samba 4.6.5 and represents a significant update from previous versions for OpenVMS, providing many new features and numerous enhancements, including support for AES encryption, SMB2 and SMB3 protocols, and use of Heimdal Kerberos. `WINBIND` functionality has been moved into a separate process, simplifying name resolution and frequency of lookups.

For details of new features, enhancements, and known issues please review the release notes found at the following links. Please be aware that some product features may be platform-specific.

- https://www.samba.org/samba/history/samba-4.6.0.html
- https://www.samba.org/samba/history/samba-4.6.5.html

Note that previous versions of Samba for OpenVMS were known as CIFS (Common Internet File System) for OpenVMS. For this and future releases, VMS Software Inc. will use the product name “Samba” for consistency with other platforms that utilize the product.

Samba Documentation

For the latest information about Samba, see https://www.samba.org/samba/docs/. Please be aware that there may be some differences from this documentation that are specific to Samba on OpenVMS; any such known differences are identified elsewhere in this document.

New and changed features

This release of Samba for VSI OpenVMS is based on Samba 4.6.5. The following list identifies some of the major new and changed features provided by this release. Please be sure to read the online documentation for a full description of these and other changes.

- Ability to specify Kerberos client encryption types
- `WINBIND` changes (enhanced functionality)
- New tools and utilities

- Changes to `smb.conf` (new and modified parameters)

In general terms, this release of Samba for OpenVMS is a significant update from previous versions of CIFS for OpenVMS and accordingly there are a large number of new and changed features. Procedures for updating your environment are described below.

Requirements

Samba 4.6.5 for VSI OpenVMS I64 servers requires the operating system and layered product software versions listed below.

- VSI OpenVMS Version 8.4-1H1 or higher
- VSI TCP/IP, HPE TCP/IP Services for OpenVMS, or MultiNet TCP/IP stack for network communication
- The software must be installed and used on an ODS-5-enabled file system (The software cannot be installed on an ODS-2 file system and ODS-2 file systems cannot be used for file shares.)

The reader should be familiar with the installation, configuration, and use of open source products such as Samba in the OpenVMS environment.

Recommended reading

Before using Samba 4.6.5 on OpenVMS, VSI recommends that users read the documentation available at https://www.samba.org/samba/ in order to better understand how to configure and manage the software.

Before installing the kit

1. VSI strongly recommends that you back up the existing CIFS `SAMBA$ROOT` directory tree prior to installing Samba for OpenVMS.
2. If necessary, increase the following `SYSGEN` parameters to at least the values specified below, run `AUTOGEN`, and reboot the system in order to pick up the new values:

Parameter	Minimum value required	Add to `MODPARAMS.DAT`
`PROCSECTCNT`	`512`	`MIN_PROCSECTCNT = 512`
`CHANNELCNT`	`2560`	`MIN_CHANNELCNT = 2560`

Important cluster considerations

Running CIFS for OpenVMS and Samba for OpenVMS in the same cluster is not supported. Existing CIFS for OpenVMS configurations will be migrated to Samba for OpenVMS equivalents when `SAMBA$CONFIG.COM` is executed.

Though multiple cluster members may be configured to share the same `SAMBA$ROOT` directory tree, this release of Samba for OpenVMS does not support running Samba simultaneously on multiple

cluster members that share the same SAMBA$ROOT directory tree. When multiple cluster members share the same SAMBA$ROOT directory tree, they must operate in a (manual) failover mode only. Administrators must ensure Samba is running ony one cluster member sharing the same SAMBA$ROOT directory tree.

Running Samba simultaneously on multiple cluster members requires each such cluster member to have a separate SAMBA$ROOT directory tree. If the systems have separate system disks, Samba may be installed with the PRODUCT INSTALL command except that Samba must be installed to different locations (for example, each separate system disk). If the systems share a system disk, it is not possible to run Samba on more than one system simultaneously with this release. Additionally, when more than one cluster member runs Samba, care must be taken to ensure users are not able to access the same files simultaneously from multiple Samba cluster members, or data corruption may occur.[1]

Installing the kit

The Samba kit is provided as a compressed OpenVMS PCSI kit (VSI-I64VMS-SAMBA-V0406-5A-1.PCSI$COMPRESSED) that can be installed by a suitably privileged user using the following command:

```
$ PRODUCT INSTALL SAMBA
```

The installation directory of Samba for OpenVMS is associated with the SAMBA$ROOT logical name. SAMBA$ROOT is a rooted logical name that defines the root location for the Samba configuration files, logs, and other product files. Samba configuration files are stored in SAMBA$ROOT:[LIB] and, by default, logs are stored in SAMBA$ROOT:[VAR]. The SAMBA$ROOT logical name is defined in SYS$STARTUP:SAMBA$DEFINE_ROOT.COM (which is executed from Samba startup procedure, SYS$STARTUP:SAMBA$STARTUP.COM).

By default Samba will be installed to SYS$SYSDEVICE:[VMS$COMMON.SAMBA]. The PCSI /DESTINATION qualifier may be used to install the software into an alternative location.

The installation will then proceed as follows (output may differ slightly from that shown):

```
Performing product kit validation of signed kits ...

The following product has been selected:
    VSI I64VMS SAMBA V4.6-5A               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 VSI I64VMS SAMBA V4.6-5A: VSI OpenVMS SAMBA

    © (c) Copyright 2019 VMS Software, Inc.
```

[1] In general terms this means ensuring each Samba share is defined on and/or is accessible from only one cluster member.

```
    OpenVMS SAMBA 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 Itanium processor.
    2.  The system is running OpenVMS V8.4-1H1 or later.
    3.  All required privileges are currently enabled.
    4.  No CIFS or SAMBA images are running on this node.
    5.  ODS5 filesystem only.

Do you want to continue? [Please, type N or NO if you don't want to
continue, any other answer means 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:
    VSI I64VMS SAMBA V4.6-5A              DISK$I64SYS:[VMS$COMMON.]

Portion done: 0%...10%...20%...30%...40%...50%...60%...70%...80%...90%

   User Accounts and User Identification Codes (UICs)
   --------------------------------------------------

    The OpenVMS SAMBA V4.6 installation creates five OpenVMS
    accounts: SAMBA$SMBD, SAMBA$NMBD, SAMBA$GUEST, SAMBA$TMPLT
    and SMBADMIN. 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 SAMBA accounts
Group: [360]
Creating OpenVMS accounts required by SAMBA
Created account SAMBA$SMBD
Created account SAMBA$NMBD
Created account SAMBA$GUEST
Created account SAMBA$TMPLT
Created account SMBADMIN
SAMBA$ROOT is defined as "EXEC14$DKA200:[SYS0.SYSCOMMON.SAMBA.]"
Setting file protections...
  File protections are set
Creating CIFS root definition file
SYS$COMMON:[SYS$STARTUP]SAMBA$DEFINE_ROOT.COM...
  File created
Save startup files
Setup SAMBA logical environment
Successfully finished
```

```
   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 OpenVMS SAMBA during system startup,
   add the following line to the file SYS$MANAGER:SYSTARTUP_VMS.COM
   after the TCPIP startup command procedure:

        $ @SYS$STARTUP:SAMBA$STARTUP.COM

   To Configure OpenVMS SAMBA on this node, execute:

        $ @SAMBA$ROOT:[BIN]SAMBA$CONFIG.COM

...100%

The following product has been installed:
    VSI I64VMS SAMBA V4.6-5A              Layered Product
```

Post-installation steps

After you have successfully installed Samba, follow these steps to configure it:

1. Verify that the `SAMBA$ROOT` logical name is set:

   ```
   $ SHOW LOGICAL SAMBA$ROOT
   "SAMBA$ROOT" = "$1$DGA400:[SYS1.SYSCOMMON.SAMBA.]"
   ```

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

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

2. Define symbols for all Samba utilities:

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

3. Configure Samba server:

   Note that for this release of Samba for OpenVMS, the server must be configured as a standalone server or a domain member server.

   Run the Samba configuration utility to generate the Samba configuration files. These files are not created during installation and must be generated as described below. Note that the Samba configuration utility also migrates existing CIFS for OpenVMS configurations to Samba (see the "Migrating CIFS for OpenVMS" section of this document).

   ```
   $ SMBCONF


                   SAMBA Configuration Utility

   Use this utility to configure the server role, create TCP/IP
   services, and configure other options.

   The following conditions must be met prior to configuring SAMBA:

      1. Log into OpenVMS using a privileged system account.
   ```

```
   2. No SAMBA images are running on this node.

For more information about Samba Server configuration, please refer to
the Samba for OpenVMS release notes.

If Samba Server is being configured afresh on this node, choose
the following option from OpenVMS Samba Main Configuration
Options Menu:

      A - Configure options 1 - 3

Press Enter to continue:

Checking for existing SAMBA Server configuration...



        OpenVMS Samba Main Configuration Options Menu

Configuration options:

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

Enter configuration option:
```

Configure Samba as appropriate using the menu options provided. At a minimum (to generate a minimal basic configuration) you can select the "A" option and accept the defaults as you step through each sub-menu. For more detailed information on configuring Samba using the `SMBCONF` utility, please refer to the help available for each menu item.

The `TESTPARM` utility to should be used to review the final configuration.

For additional information about configuring Samba please refer to the documentation available at https://www.samba.org/samba/.

4. Start the Samba server:

```
$ SMBSTART

Creating NMBD Process...
%RUN-S-PROC_ID, identification of created process is 000143A2

Enabling SMBD services...

  Successfully enabled TCPIP SMBD services
```

5. Add the following command to the system startup procedure to start Samba when the system is booted. Note that this command must be added after the command that starts TCP/IP.

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

6. Add the following command to the system shutdown procedure to stop Samba during system shutdown:

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

7. Use the SMBMANAGE utility to manage Samba shares, users, groups, and account policies as necessary.

8. You may wish to run the following command to add a version limit on the sub-directories in samba$root:[var.cores] to prevent unnoticed process dump files from consuming huge amounts of disk space. You may wish to use an alternative value for the version limit as appropriate to your environment.

```
$ set file/version_limit=10 samba$root:[var.cores]*.dir
```

Migrating CIFS for OpenVMS

Run SAMBA$CONFIG.COM after installation to migrate an existing CIFS for OpenVMS configuration to Samba for OpenVMS. SAMBA$CONFIG.COM runs SAMBA$MIGRATION.COM, which renames the appropriate CIFS users/groups and their associated OpenVMS account and identifier names (changing "CIFS" to "SAMBA") and updates references in .CONF and USERNAME.MAP files. SAMBA$CONFIG.COM also has routines to migrate obsolete, deprecated, and modified parameters to their equivalents in Samba.

The Samba migration process saves the old CIFS for OpenVMS configuration files to a subdirectory in SAMBA$ROOT:[BACKUP_MIGRATION] and produces a log file named according to the format SAMBA$ROOT:[VAR]SAMBA$MIGRATION_<date>_<time>.LOG.

To undo or roll back the migration if problems were encountered with the migration, proceed as follows:

- Run the migration procedure (SAMBA$MIGRATION.COM) and specify the path where the backup migration files are stored. In the following example, the backed up CIFS configuration files are stored in the directory SAMBA$ROOT:[BACKUP_MIGRATION.30APR2019_103511]:

```
$ @SAMBA$ROOT:[BIN]SAMBA$MIGRATION -
_$ SAMBA$ROOT:[BACKUP_MIGRATION.30APR2019_103511]
```

- Reinstall CIFS for OpenVMS

WINBIND support

WINBIND is a component of Samba that provides user and group identity mapping. In Samba for OpenVMS, WINBIND is a separate daemon process with one to four subprocesses (in CIFS for OpenVMS there is no separate WINBIND process; the WINBIND functionality is instead included in each SMBD process).

When deciding whether to enable or disable WINBIND, consider the following points:

- If Samba is configured in a standalone server role, WINBIND provides no useful purpose and would typically be disabled.
- If Samba is configured as a member server, WINBIND provides three main functions:
    a) Ability to reference domain user and group accounts when managing Samba. For example, to add or remove domain user and group accounts as members of local Samba groups.

b) Ability to dynamically create OpenVMS user accounts. Each Samba user requires an OpenVMS account with a unique UIC in order to be distinguished from other users for security purposes. Administrators may create the necessary OpenVMS accounts manually or allow WINBIND to create OpenVMS accounts for Samba users dynamically, as they are needed. When properly configured, WINBIND creates a new OpenVMS account with a unique UIC for any domain user who successfully authenticates but does not already have an OpenVMS account mapped to their Windows account.

c) Ability to dynamically create OpenVMS resource identifiers. Identifiers are created for all domain groups for which any Samba user is a member. If properly configured, WINBIND creates an OpenVMS identifier for each Windows domain group contained in a user's access token when a new session is established. These group identifiers may subsequently be used to control access to resources, such as files and printers. For example, if a user is a member of 25 domain groups, when the user establishes a session to the Samba server for the first time, 25 new OpenVMS identifiers are created and mapped to the 25 domain groups (if the mappings do not already exist). This functionality is marginally useful and is disabled by default.

Configuring WINBIND

Before configuring WINBIND on a member server, determine what functionality is desired. If configured to dynamically create OpenVMS user accounts or group identifiers, WINBIND requires a range of values (specified in decimal) to allocate as user or group identifiers and from which a unique OpenVMS username and UIC or OpenVMS identifier name are derived.

The range is specified in decimal using the format “low-value - high-value”, where low-value must be less than high-value. Due to OpenVMS UIC number restrictions, the low-value should not be less than 256 and the high-value cannot exceed 16382.

The range specified should be large enough to accommodate the expected number of user accounts and group identifiers that could possibly be created. However, the high-value of the range can be increased at any time to provide additional user or group identifiers if necessary.

For example, a UIC number range of 5000 - 6000 allows WINBIND to create a total of 1001 user and/or group identifiers.

In the case of a user ID, the ID number allocated by WINBIND is converted to hexadecimal and appended to the string “SAMBA$” to derive the OpenVMS username. The allocated WINBIND ID number is also converted to octal and used as the UIC group and member number assigned to the OpenVMS account. For example, if WINBIND allocates ID 5200 to a new user, the OpenVMS account name will be SAMBA$1450 and its UIC will be [12120,12120].

In the case of a group ID, the ID number allocated by WINBIND is converted to hexadecimal and appended to the string “SAMBA$GRP” to derive the OpenVMS POSIX group Identifier name.

Configure WINBIND using the SAMBA$CONFIG utility. From the Main Configuration Options menu, option “3 - Core environment” includes the following WINBIND configuration options:

```
4. Enable WINBIND:
      4A. UIC number range:
      4B. Allow WINBIND to create OpenVMS accounts on-the-fly:
      4C. Allow WINBIND to create OpenVMS identifiers on-the-fly:
```

- To disable all WINBIND functionality, set option 4 to no. This will prevent the WINBIND process from starting. Also, to prevent WINBIND from starting during system startup, add the following command to the system startup procedures so it executes prior to starting Samba:

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

- To enable only the WINBIND functionality to reference domain user and group accounts (but prevent WINBIND from creating OpenVMS accounts and OpenVMS identifiers dynamically), set option 4 to yes and specify a UIC number range in decimal for option 4A (a range is required but will not be used). Set options 4B and 4C to no.
- To enable the WINBIND functionality to reference domain user and group accounts and allow WINBIND to create OpenVMS accounts dynamically, set option 4 to yes; specify a UIC number range in decimal for option 4A; set option 4B to yes; and set option 4C to no.
- To enable all WINBIND functionality, set option 4 to yes; specify a UIC number range in decimal for option 4A; set option 4B to yes; and set option 4C to yes.

Samba WINBIND configuration parameters

The Samba configuration parameter "idmap config * : range = " specifies the UIC number range that WINBIND uses when allocating user and/or group identifiers.

Note that the TESTPARM utility will display the following messages when no range is specified; these messages may be ignored:

```
idmap range not specified for domain '*'
ERROR: Invalid idmap range for domain *!
```

The Samba configuration parameter "idmap config * : read only" controls WINBIND ID allocation. If set to yes, WINBIND is prevented from allocating user and group IDs. If set to no (the default), WINBIND may allocate user and group IDs.

A new Samba configuration parameter named "vms group create" is used to enable/disable the WINBIND functionality that creates OpenVMS identifiers dynamically (option 4C on the SAMBA$CONFIG Core Configuration Menu). If this parameters is set to no, WINBIND will not create OpenVMS identifiers.

What's missing?

This initial release of Samba 4.6.5 for OpenVMS does not include the following functionality:

- Minimal OpenVMS cluster support. See the "Important cluster considerations" section above. Full cluster support will be added in a subsequent release of Samba for OpenVMS as per the product roadmap outlined below.
- The classic Primary Domain Controller (PDC) and Backup Domain Controller (BDC) roles are not supported in this release. Classic PDC/BDC support will be included in a subsequent release of Samba for OpenVMS as per the product roadmap illustrated below.
- The Active Directory Domain Controller role is not supported in this release. Support for this functionality is being considered and may be provided at a later date.
- It should be noted that a copy of the source code for Samba on OpenVMS is not included with the installation kit; however we would be happy to provide a copy of the code on request (email support@vmssoftware.com).
- No support for OpenVMS Alpha. A version of Samba for VSI OpenVMS Alpha versions will be made available at a later date.

Known issues

The following list identifies currently known problems and restrictions with this release of Samba for VSI OpenVMS.

- When SAMBA$CONFIG is run on an OpenVMS cluster member, the following issues may be observed:

  a) It does not retain changes to the Core Configuration menu option "5. Computer (NetBIOS) Name".

  On a cluster member, the Computer (NetBIOS) Name sets the value for the Samba netbios aliases parameter stored in SAMBA$ROOT:[LIB]<hostname>_SPECIFIC_SMB.CONF, where <hostname> is the TCP/IP host name of the OpenVMS system.

  b) It may duplicate the value of the netbios aliases parameter (which is stored in SAMBA$ROOT:[LIB]<hostname>_SPECIFIC_SMB.CONF).

  In both of these cases, the problem can be resolved by manually setting the netbios aliases parameter in SAMBA$ROOT:[LIB]<hostname>_SPECIFIC_SMB.CONF.

- If a file and directory have the same name and exist in the same directory, both objects are displayed as directories.
- Utilities such as SMBSTATUS and SMBCONTROL display OpenVMS PIDs in decimal format, not as hexadecimal values.
- The SMBCLIENT lcd command reports the current working directory only if debug level 2 or higher is enabled.
- To use Kerberos authentication (via the -k option) with the SMBCLIENT utility, perform the following steps:

  a. If necessary, disable elevated process privileges (NOIMPERSONATE, NOSYSPRV, NOREADALL, and NOBYPASS):

  ```
  $ SET PROCESS/PRIVILEGE=(NOALL,TMPMBX,NETMBX)
  ```

  b. Obtain a Kerberos ticket using your domain username:

  ```
  $ net ads kerberos kinit --user <domain-username>
  ```

  c. Optionally (and if possible) elevate process privileges (to avoid potential benign errors); for example:

  ```
  $ SET PROCESS/PRIVILEGE=ALL
  ```

  d. Run SMBCLIENT, specifying values for server and share names as appropriate:

  ```
  $ SMBCLIENT -k \\server\share
  ```

- The OpenVMS owner of new objects created by users with a local Samba account that is included in the admin users list is incorrectly set to SAMBA$SMBD instead of the owner of the parent directory. In many environments this issue can be avoided by adding the following line to the applicable share section in SAMBA$ROOT:[LIB]SMB.CONF:

  ```
  inherit owner = yes
  ```

- The "net rpc user rename" command is not supported by Samba for OpenVMS. This is consistent with previous CIFS for OpenVMS behaviour.

- It should be noted that use of Samba for OpenVMS is not supported for Microsoft Windows XP and Windows 7 clients.
- In some situations Samba incorrectly reports file allocation size (“Size on disk”) displayed on Windows Explorer properties page. This issue will be fixed in a future release.
- When configured in a member server role with WINBIND running, if a user connects to Samba using a local Samba account where the username is identical to a domain account username, attempts to create new objects fail with the error "access denied". This issue will be addressed in a future release.
- If the Samba share parameter “`inherit owner`'” equals “`no`” and a parent directory is owned by a resource identifier, when a user creates a new file or folder Samba sets the file owner to the UIC of the user creating the file rather than the resource identifier. To retain usual OpenVMS behaviour (that is, to set the resource identifier as the file owner), add “`inherit owner = yes`” to the applicable [share] sections in `SMB.CONF`.
- If the Samba share parameter “`inherit owner`” equals “`no`" and a user accesses a fileshare directory using the SYSPRV privilege, when the user creates a new file or folder Samba sets the file owner to the UIC of the user creating the file rather than the owner of the parent directory. To retain usual OpenVMS behaviour (that is, to set the parent directory owner as the pwner of the new object), add '”`nherit owner = yes`” to the applicable [share] sections in `SMB.CONF`.

DNS Requirements for Samba Member Servers

A Samba member server requires a proper DNS configuration to avoid long delays or timeouts when attempting to locate domain controllers.

If the OpenVMS host is configured to use the same DNS domain as the domain Samba will join, no changes are required.

However, if Samba will be joined to a domain which is not the same DNS domain configured on the OpenVMS host, the OpenVMS host should be configured as a cache-only BIND server and use a stub zone or conditional forwarding for the domain Samba will join. Additionally, the DNS name resolver on the OpenVMS host should be configured to use localhost as its DNS server.

Prior to joining the Samba server to a domain, customers should verify the OpenVMS host is capable of resolving DNS SRV record types for the domain. For example, use the following command to verify that Samba will join a domain named example.com:

```
$ dig SRV _kerberos._tcp.example.com +noall +answer +additional
```

The response should be a list of domain controllers.

Product roadmap

VSI intends to provide regular releases and updates of Samba to ensure that the following criteria are met:

- Support for the latest VSI OpenVMS Alpha and Integrity versions and other relevant software applications
- Support for OpenVMS on x86 when available

- Enhanced quality and functionality with every new release
- Security and performance enhancements
- Maintaining parity with Open Source versions