VMS Software

ACME LDAP for OpenVMS Alpha and Integrity

May 2021

Operating System and Version: VSI OpenVMS I64 version 8.4-2L1 or higher
VSI OpenVMS Alpha version 8.4-2L1 or higher

Software Version: ACME LDAP version 2.0-1A

Contents

1. Introduction

ACME LDAP for VSI OpenVMS combines the Lightweight Directory Access Protocol (LDAP) with the VSI OpenVMS Authentication and Credentials Management Extension (ACME) authentication mechanism to provide a solution that allows VSI OpenVMS customers to extend single sign-on procedures to include OpenVMS hosts and manage user accounts in a centralized directory.

The ACME LDAP agent for VSI OpenVMS provides "simple bind" authentication during login using an LDAP-compliant directory server, such as a Microsoft Active Directory domain controller or an OpenLDAP server. In this authentication method, users enter the user ID and password of their LDAP directory account when accessing the OpenVMS host. When successfully authenticated, the external user ID is mapped to the appropriate OpenVMS username and the correct user profile is obtained.

The ACME LDAP agent supports logins from multiple user domains and provides multiple mechanisms to map domain usernames to OpenVMS usernames.

Secure Socket Layer (SSL)/Transport Layer Security (TLS) LDAP communication is supported to prevent user IDs and clear-text passwords from being exposed over the network.

For more information about the ACME server and agents, particularly if you plan to use external authentication with DECnet applications on systems running DECnet-Plus, see the section “Enabling External Authentication” in the *VSI OpenVMS Guide to System Security*.

2. What’s New in this Release

This release of ACME LDAP for VSI OpenVMS uses the new OpenLDAP client for VSI OpenVMS and OpenSSL 1.1.1g to support enhanced LDAP functionality and improved security.

To allow the customers who are currently using the legacy ACME LDAP agent to easily switch between the legacy ACME LDAP agent and the new ACME LDAP agent, the new ACME LDAP agent was designed to co-exist with the legacy ACME LDAP agent (although only one ACME LDAP agent may be active at any time). As a result, before the new ACME LDAP agent can be active, all customers must complete the initial configuration steps documented in section 5 – *Post-installation Tasks*.

Systems that are currently running the legacy ACME LDAP agent which use the ‘ca_file’ directive in the ACME LDAP agent configuration file may find that the new ACME LDAP agent no longer accepts the server certificate of the LDAP server as valid and, thus, external authentication fails.

The ACME LDAP agent can be configured to verify the certificate of the LDAP server before establishing an SSL/TLS connection. However, the new OpenLDAP client used by the new ACME LDAP agent features additional security checks which include verifying that the server’s name in the server certificate matches the server’s name specified when connecting. The ACME LDAP agent uses the host name, or the IP address specified by the ‘server’ directive in the ACME LDAP configuration file. If the specified ‘server’ name does not match the host name in the Subject CN or Subject Alternative Name fields of the server certificate, the connection will not be established. The Subject CN field can contain only one name, but this limitation may be overcome by using the x509v3 certificate

extension – the Subject Alternative Name (SAN) field. The Subject Alternative Name field may contain a list of names to identify the server host. The new LDAP client (used by the ACME LDAP agent) will then check the list of names one by one until a match is found or the list is exhausted.

Alternatively, it is noted that the 'ca_file' directive is optional, and simply commenting out the 'ca_file' directive and restarting the ACME Server can resolve problems associated with certificate verification. However, in some cases, this approach may be undesirable for security reasons.

To view an LDAP server certificate (i.e., to check the Subject CN and the Subject Alternative Name fields), execute the commands below (in the case shown). Substitute <LDAP-server> with the IP address or hostname of the target LDAP server:

```
$ @SSL111$COM:SSL111$UTILS
$ PIPE OPENSSL s_client -connect <LDAP-server>:636 | OPENSSL x509 -noout
-subject -ext subjectAltName
```

Or to view all certificate details:

```
$ PIPE OPENSSL s_client -connect <LDAP-server>:636 | OPENSSL x509 -noout
-text
```

3. Requirements

ACME LDAP version 2.0-1A for VSI OpenVMS servers requires the operating system and layered product software versions listed below.

- VSI OpenVMS I64 or Alpha version 8.4-2L1 or higher.
- VSI TCP/IP Services for OpenVMS, HP TCP/IP Services for OpenVMS, or MultiNet TCP/IP. However, SSH logins using external authentication are supported only on hosts running HP TCP/IP Services for OpenVMS.
- The `SYS$ACM`-enabled (`ACMELOGIN`) `LOGINOUT.EXE` and `SETP0.EXE` images must be in place. For more information, see *Post-Installation Tasks*.
- VSI OpenLDAP 2.4.53 or later.
- VSI OpenSSL111 1.1.1g or later.

  SSL/TLS support is dynamically linked into OpenLDAP for OpenVMS and requires OpenSSL 1.1.1g or later.

  NOTE: The VSI OpenLDAP and OpenSSL kits may be downloaded from:

  https://vmssoftware.com/products/list/?license=Open%20Source
- In addition, the reader should be familiar with the configuration and use of Microsoft Active Directory, OpenLDAP Server, or another 3rd party LDAP server in a Windows or Linux environment.
- An account on the LDAP directory server for the ACME LDAP agent to bind to and search the directory.
- In order to use SSL, TLS, or STARTTLS for the LDAP exchange encryption, the target LDAP directory servers must possess a digital certificate with the purpose of Server Authentication. For more information, see:

https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx

4. Installing the Kit

The kit is provided as an OpenVMS PCSI kit (`VSI-I64VMS-ACMELDAP-V0200-1A-1.PCSI` for i64 or `VSI-AXPVMS-ACMELDAP-V0200-1A-1.PCSI` for Alpha) that a suitably privileged user can install by entering the following command:

```
$ PRODUCT INSTALL ACMELDAP
```

NOTE: In a cluster with multiple system disks, install the software on each system disk.

The installation will then proceed as follows (output may differ slightly from that shown below depending on the platform and other factors):

```
Performing product kit validation of signed kits ...
%PCSI-I-VSIVALPASSED, validation of NODE1$DKA300:[KITS]VSI-I64VMS-
ACMELDAP-V0200-1A-1.PCSI$COMPRESSED;1 succeeded

The following product has been selected:
    VSI I64VMS ACMELDAP V2.0-1A            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 ACMELDAP V2.0-1A: LDAP agent for ACME server

    VMS Software Inc.

* This product does not have any configuration options.

Execution phase starting ...

The following product will be installed to destination:
    VSI I64VMS ACMELDAP V2.0-1A
DISK$I64V842L1SYS:[VMS$COMMON.]

Portion done: 0%...10%...20%...30%...50%...80%...100%

The following product has been installed:
    VSI I64VMS ACMELDAP V2.0-1A            Layered Product

VSI I64VMS ACMELDAP V2.0-1A: LDAP agent for ACME server

    Post installation notes

    Following installation, the system must be rebooted in order to
    load the newly installed LDAP persona extension (it is not
    sufficient to simply restart the ACME server). Once the system
    has been rebooted, follow the post installation instructions
    provided in the release notes to complete configuration of the
    software.
```

5. Post-installation Tasks

After the installation, complete the following tasks to configure and enable the new ACME LDAP agent.

5.1. Install the SYS$ACM (ACME LOGIN)-Enabled Login Images

If the system is currently using the legacy ACME LDAP agent, this step has already been completed – skip to the next step to continue.

In a cluster, complete this step on any one system which boots from a particular system disk.

To install the SYS$ACM-enabled LOGIN (previously known as ACMELOGIN) images (SYSSSYTEM:LOGINOUT.EXE and SETP0.EXE) run the command file SYS$MANAGER:SYS$LOGIN_SWITCH.COM. The procedure will display a message indicating which login images are currently in use and an option to switch to the other login images. If necessary, switch to using the ACME LOGIN. For example:

```
$ @SYS$MANAGER:SYS$LOGIN_SWITCH
You are currently using UAF LOGIN.
This procedure will switch to using ACME LOGIN
Do you want to continue? (YES or NO): YES
The replacement procedure is complete.  You must issue
the commands

$INSTALL REPLACE LOGINOUT
$INSTALL REPLACE SETP0

on any other cluster members using a common system
disk with NODE1.
```

As directed by SYS$LOGIN_SWITCH.COM, if SYS$LOGIN_SWITCH was executed on a system that uses a common system disk in an OpenVMS cluster, run the following commands on all cluster members that use the common system disk:

```
$ INSTALL REPLACE LOGINOUT
$ INSTALL REPLACE SETP0
```

5.2. Install the New LDAP Persona Extension

In a cluster, complete this step on any one system which boots from a particular system disk.

To set up the new LDAP persona extension, perform the following tasks:

- Add an entry for the new persona extension image to the system images file:

  ```
  $ MCR SYSMAN
  SYSMAN> SYS_LOADABLE ADD LDAPACME LDAPACME2$EXT
  SYSMAN> EXIT
  ```

- Generate a new system images data file:

  ```
  $ @SYS$UPDATE:VMS$SYSTEM_IMAGES.COM
  ```

5.3. Reboot

Reboot each applicable system, for example:

```
$ @SYS$SYSTEM:SHUTDOWN
```

NOTE: To avoid possible system-wide login issues, VSI recommends rebooting the system before initially enabling the ACME LDAP agent.

5.4. Verify the LDAP Persona Extension is Installed

After rebooting a system, verify the LDAP persona extension is installed. In a cluster, perform this step on all cluster members that will run the ACME LDAP agent:

```
$ ANALYZE/SYSTEM
SHOW EXECUTIVE LDAPACME2$EXT
```

If the result is "No loadable image matching "LDAPACME2$EXT" found", the new LDAP persona extension has NOT been installed. Follow the instructions starting at step 5.1 again to install the new LDAP persona extension.

5.5. Configure the ACME LDAP Agent

If the system is currently using the legacy ACME LDAP agent, this step has already been completed – skip to the next step to continue.

The ACME LDAP agent uses a text configuration file which contains directives (described in *Appendix A*) to control its operation. To support multiple user domains, use a separate configuration file for each domain.

In an OpenVMS cluster:

- The entire cluster may share a single ACME LDAP agent configuration file. I.e., by storing the configuration file on a disk which is mounted cluster-wide prior to restarting the ACME server during startup.
- Multiple ACME LDAP agent configurations may be deployed in a single cluster using different file names for the ACME LDAP agent configuration files.
- Each cluster member may use a unique ACME LDAP agent configuration file, i.e., by using configuration files with different names or by placing the configuration file in a SYS$SPECIFIC: directory, such as SYS$SPECIFIC:[SYS$STARTUP].

To assist new users, the template configuration file, SYS$STARTUP:LDAPACME$CONFIG-STD.INI_TEMPLATE, can be copied, renamed to a file name of your choice, and then modified to suit your needs. For example:

```
$ COPY SYS$STARTUP:LDAPACME$CONFIG-STD.INI_TEMPLATE -
SYS$STARTUP:LDAPACME$CONFIG-STD.INI
```

Edit the ACME LDAP agent configuration file to specify the directives that correspond to your requirements. For a description of the supported directives in the ACME LDAP agent configuration file, see *Appendix A – Configuration Directives*. Example configurations are provided in *Appendix B - Configuration Examples*.

IMPORTANT: The ACME LDAP agent requires the credentials of an account which exists in the LDAP directory for the purpose of performing a search of the username specified during login.

The distinguished name (NOT the username) and password of the designated account are required for proper configuration of the ACME LDAP agent.

The account should be an ordinary user account with no special privileges or rights. If possible, set up the account so that its password never expires and cannot be changed. Any change to the password will require a change to the password specified in the ACME LDAP agent configuration file (and the ACME server must be restarted).

When editing the ACME LDAP agent configuration file, consider the following:

- Comments, denoted by an exclamation point (!), are allowed but do not add a comment to the end of a line containing a directive (the comment is considered part of the value).
- Directives are not case-sensitive (i.e., bind_dn, BIND_DN, or Bind_DN are all acceptable).
- Directive order is irrelevant.
- Values, with the exception of those for the 'bind_password' directive and the 'scope' directive, are not case-sensitive.
- Do not enclose values in quotes, even if they contain spaces.
- At minimum, a functional ACME LDAP configuration file requires the following six directives:

  server
  bind_dn
  bind_password
  base_dn
  login_attribute
  scope

- Any modifications to the configuration files take effect only after the ACME server is restarted.

- Ensure that the LDAP configuration files are accessible to privileged users only. Set the security of these files appropriately based on your security requirements. For example, the following command grants access to the ACME LDAP agent configuration file only for privileged users:

```
$ SET SECURITY/PROTECTION=(S:RWED,O,G,W) -
SYS$COMMON:[SYS$STARTUP]LDAPACME$CONFIG-STD.INI
```

5.6. Define the LDAPACME$INIT Logical Name

If the system is currently using the legacy ACME LDAP agent, this step has already been completed – skip to the next step to continue.

In a cluster, perform this step on all cluster members that will run the ACME LDAP agent.

The Executive Mode system logical name LDAPACME$INIT must be defined prior to starting the ACME server and must equate to the full file specification of the ACME LDAP configuration file. For example:

```
$ DEFINE/SYSTEM/EXECUTIVE_MODE LDAPACME$INIT -
SYS$STARTUP:LDAPACME$CONFIG-STD.INI
```

When using multiple domain configuration files, define LDAPACME$INIT to equate to all such configuration files using a comma-separated list. For example:

```
$ DEFINE/SYSTEM/EXECUTIVE_MODE LDAPACME$INIT -
SYS$STARTUP:LDAPACME$CONFIG-STD-US.INI, -SYS$STARTUP:LDAPACME$CONFIG-
STD-EMEA.INI
```

IMPORTANT: The LDAPACME$INIT logical must be defined prior to starting the ACME LDAP agent. VSI recommends adding this logical name definition to the command procedure SYS$MANAGER:ACME$START.COM so that it executes prior to starting the ACME LDAP agent (see the next step).

5.7. Update SYS$MANAGER:ACME$START.COM

The ACME$START.COM procedure runs automatically when restarting the ACME server. Though ACME$START.COM currently contains the command required to start the legacy ACME LDAP agent, the command required to start the new ACME LDAP agent must be added (and the command which starts the legacy ACME LDAP agent must be commented out).

In a cluster with multiple system disks, complete this step on any one system which boots from a particular system disk.

The following example uses the EDT editor to modify ACME$START.COM. The 'c 40' EDT command advances to line 40 and displays several lines of the file. Use the up/down arrows to move between lines:

```
$ EDIT/EDT SYS$MANAGER:ACME$STARTUP.COM
    1       $! ACME$START.COM -- ACME_SERVER Restart File
*c 40
```

Note: If the 'c 40' EDT command results in the following response:

```
[$] if f$mode() .nes. "INTERACTIVE" then goto skip_interactive
C*
```

do the following:

Press Ctrl/Z to return to the * prompt.
Enter the EDT command 'set term vt100'.
Enter the EDT command 'c 40'.

Locate and comment out the line:

```
$ @SYS$STARTUP:LDAPACME$STARTUP-STD
```

Insert (press Enter at the start of a line to insert a new line) the following command, above or below the line noted above:

```
$ @SYS$STARTUP:LDAPACME2$STARTUP-STD
```

Save the changes and exit - press Ctrl/Z (to return to the * prompt) and enter EXIT.

5.8. Restart the ACME Server

After modifying SYS$MANAGER:ACME$START, restart the ACME server. In a cluster, perform this step on all cluster members that will run the ACME LDAP agent.

```
$ SET SERVER ACME/RESTART
```

5.9. Verify the ACME Agents are Active

Execute the $ SHOW SERVER ACME command and verify that the VMS and the LDAP agents are both in the Active state. If both agents are not in the Active state, see *Troubleshooting*.

In a cluster, perform this step on all cluster members that run the ACME LDAP agent.

```
$ SHOW SERVER ACME
ACME Information on node NODE1  23-MAR-2021 17:32:06.92  Uptime 0 00:00:42
ACME Server id: 3  State: Processing New Requests
   Agents Loaded:         2   Active:      2
   Thread Maximum:        1   Count:       1
   Request Maximum:     834   Count:       0
ACME Agent id: 1  State: Active
   Name: "VMS"
   Image: "DISK$I64V842L1SYS:[VMS$COMMON.SYSLIB]VMS$VMS_ACMESHR.EXE;1"
   Identification: "VMS ACME built  20-SEP-2006"
   Information: "No requests completed since the last startup"
   Domain of Interpretation: Yes
   Execution Order:       1
ACME Agent id: 2  State: Active
   Name: "LDAP-STD"
   Image: "DISK$I64V842L1SYS:[VMS$COMMON.SYSLIB]LDAPACME2$LDAP-
STD_ACMESHR.EXE;1"
   Identification: "LDAP ACME Standard V2.00"
   Information: "ACME_LDAP_DOI Agent is initialized"
   Domain of Interpretation: Yes
   Execution Order:       2
```

- Determining which ACME LDAP Agent is Active

  To determine which ACME LDAP agent is currently active, check the "Identification" displayed by the command:

  ```
  $ SHOW SERVER ACME
  ```

  If the Identification displayed is “LDAP ACME Standard V1.26”, the legacy ACME LDAP agent is active; if instead it displays “LDAP ACME Standard V2.00”, the new ACME LDAP agent is active.

- Switching Between the Legacy and New ACME LDAP Agents

  WARNING: This step assumes the legacy ACME LDAP agent is properly installed, configured, and was functional prior to activation of the new ACME LDAP agent. Do not attempt to switch to the legacy ACME LDAP agent otherwise.

  To switch between the legacy ACME LDAP agent and the new agent, modify ACME$START.COM and restart the ACME server. For example, if the legacy ACME

LDAP agent is active, perform the following procedure to switch to the new ACME LDAP agent:

- Edit SYS$MANAGER:ACME$START.COM.
- Uncomment the command that starts the new ACME LDAP agent:

```
$ @SYS$STARTUP:LDAPACME2$STARTUP-STD
```

- Comment out the command that starts the legacy ACME LDAP agent:

```
$! @SYS$STARTUP:LDAPACME$STARTUP-STD
```

- Save the changes.
- Restart the ACME server:

```
$ SET SERVER ACME/RESTART
```

5.10. Enable Password Changes in TCP/IP Services SSH Server

If a system is running TCP/IP Services for OpenVMS, to allow externally authenticated SSH users to change their LDAP account password with the $ SET PASSWORD command, define the following system logical name prior to starting the SSH Server:

```
$ DEFINE/SYSTEM TCPIP$SSH_SERVER_USE_LOGINOUT 1
```

5.11. Configure OpenVMS User Accounts

For a user to be externally authenticated (i.e., using an ACME LDAP agent), set the EXTAUTH flag on the user's OpenVMS account:

```
$ MCR AUTHORIZE MODIFY USER1 /FLAG=EXTAUTH
```

When the EXTAUTH flag is set on a user's account, the user is validated using only external authenticator (LDAP). When a user successfully logs in using the ACME LDAP agent, the OpenVMS host displays the message "Logon authenticated by LDAP" on the user's terminal. For example:

```
$ SSH USER1@NODE1
Welcome to OpenVMS (TM) Alpha Operating System, Version V8.4-2L2
user1's password:
Authentication successful.

    Last interactive login on Monday,  27-MAR-2021 12:36:51.62
    Last non-interactive login on Wednesday, 27-JAN-2021 14:07:16.75
**** Logon authenticated by LDAP ****
```

To allow the user to bypass external authentication and instead be authenticated locally (using the user's credentials stored in the SYSUAF.DAT file), also set the VMSAUTH flag on the user's account. However, the password of the user's OpenVMS account may not be synchronized with the password of their LDAP directory account (see the *Password Synchronization* section) and may need to be reset.

To bypass external authentication, the user must include the /LOCAL_PASSWORD qualifier when specifying their username (at the Username: prompt), for example:

```
Username: USER1/LOCAL_PASSWORD
```

NOTE: The /LOCAL_PASSWORD qualifier is not supported for SSH interactive logons.

6. Username Mapping

The ACME LDAP agent supports implicit and explicit username mapping. Implicit mapping occurs when no explicit mapping exists for a user's account, and the user's LDAP account username is identical to their OpenVMS account username. If the user's LDAP account username is not identical to their OpenVMS account username, explicit username mapping is required.

The ACME LDAP agent supports two forms of explicit username mapping – Global and Local. With global mapping, the user's OpenVMS username is mapped based on a value stored in a designated attribute of the user's account on the directory server. With local mapping, a text file on the OpenVMS host is used to store the mapping.

Global Username Mapping

To enable global mapping, perform the following steps:

- Choose the LDAP account attribute (field) that will be used to store the name of the user's OpenVMS username. The examples in this document use the 'description' attribute. Edit the ACME LDAP configuration file and set the 'mapping_attribute' directive to the name of the chosen attribute, for example:

  ```
  mapping_attribute = description
  ```

- Choose a string identifier that will precede the OpenVMS username. Edit the ACME LDAP configuration file and set the 'mapping_target' directive to this string (do not terminate the string with a slash). The examples in this document use the string "VMSUser"; for example:

  ```
  mapping_target = VMSUser
  ```

- Restart the ACME Server:

  ```
  $ SET SERVER ACME/RESTART
  ```

- For any user whose LDAP directory username is not identical to their OpenVMS username, add the string specified for the 'mapping target' directive and the user's OpenVMS username, separated by a slash, to the attribute field (specified by the 'mapping_target' directive) of the user's LDAP directory account. For example, if the user's OpenVMS username is JDOE, add the following string to the Description field of the user's LDAP directory account:

  ```
  VMSUser/jdoe
  ```

Local Username Mapping

To enable local username mapping, perform the following steps:

- Make a copy of SYS$STARTUP:LDAP_LOCALUSER_DATABASE.TXT_TEMP-LATE and rename it to a filename of your choice. For example:

```
$ COPY SYS$STARTUP:LDAP_LOCALUSER_DATABASE.TXT_TEMPLATE –
SYS$COMMON:[SYS$STARTUP]LDAP_USER_DB.TXT
```

- Update the file with a user's LDAP username and OpenVMS username separated by a comma (one or more space characters may follow the comma). If the LDAP username contains spaces, enclose it in quotes. For example:

  "John Doe", jdoe

  jhardy, hardyj

  In the example above, the LDAP account "John Doe" is mapped to the OpenVMS account JDOE and the LDAP account JHARDY is mapped to the OpenVMS account HARDYJ.

- Add the following directives to the ACME LDAP configuration file:

  mapping = local

  mapping_file = <File-Specification-of-Mapping-File>

  For example:

  mapping = local

  mapping_file = SYS$COMMON:[SYS$STARTUP]LDAP_USER_DB.TXT

- Restart the ACME server:

  ```
  $ SET SERVER ACME/RESTART
  ```

Further updates to the local username mapping file can be dynamically applied without restarting the ACME server using the LDAP_LOAD_LOCALUSER_DATABASE utility. The utility accepts two parameters:

- The file specification of the mapping file. This parameter is required and must be the same file specified by the 'mapping_file' directive of the applicable LDAP ACME agent configuration file.
- The domain name. This parameter is optional when the 'domain' directive is not included in the ACME LDAP configuration file. Otherwise, specify the same domain name as specified in the ACME LDAP configuration file. For example:

  ```
  $ load_ldapuser_db == "$LDAP_LOAD_LOCALUSER_DATABASE.EXE"
  $ load_ldapuser_db SYS$COMMON:[SYS$STARTUP]LDAP_USER_DB.TXT
  $ load_ldapuser_db SYS$COMMON:[SYS$STARTUP]LDAP_USER_DB_US.TXT US
  $ load_ldapuser_db SYS$COMMON:[SYS$STARTUP]LDAP_USER_DB_EMEA.TXT EMEA
  ```

7. Restrictions

This section lists the restrictions associated with the ACME LDAP agent.

Password Synchronization

The password specified by an externally authenticated user is typically validated against the password stored on the LDAP directory server, but some OpenVMS applications do not support external authentication and instead authenticate the user based on their OpenVMS account credentials (stored in SYSUAF.DAT).

During external authentication, if the user's password stored on the LDAP directory server is different from their OpenVMS account password but is still a valid OpenVMS password,

the OpenVMS account password of that user is set to be the same as the password stored on the directory server, so that they remain synchronized when possible.

VSI recommends setting the PWDMIX flag on OpenVMS accounts of externally authenticated users as this (a) retains the case of the password and (b) significantly expands the list of special characters allowed in a password. For more information see the output from:

```
$ HELP SET PASSWORD
```

Enabling the PWDMIX flag on externally authenticated accounts greatly increases the odds that a user's OpenVMS account password remains synchronized with their LDAP directory account password. This allows the user to access the OpenVMS host using one password, even for applications that do not support external authentication, such as Multinet Secure Shell (SSH) Server and VSI TCP/IP Secure Shell (SSH) Server.

If a user has been externally authenticated, the DCL command `$ SET PASSWORD` sends the password change request to the LDAP directory server and, if the request completes successfully, changes the user's OpenVMS account password.

Password synchronization can be disabled for a specific user or for all the users on the system.

Username and Password Restrictions

- The OpenVMS SYSTEM account cannot use External Authentication. If a user enters SYSTEM at the Username prompt, the user is always mapped only to the SYSTEM account in SYSUAF.DAT.

- If the system is running a TCP/IP stack other than HP TCP/IP Services for OpenVMS, when an SSH user executes the DCL $ SET PASSWORD command, it will change the password of the user's OpenVMS account only.

- If the 'port_security' directive is set to "NONE", externally authenticated users cannot change their Active Directory (LDAP) account password. Active Directory LDAP servers require an encrypted connection for password changes.

- Password modifications are made to the standard userPassword attribute or Active Directory's unicodePwd attribute. The ldap_modify "replace" or "remove-old/add-new" semantics for password modifications can be configured to support a variety of directory servers based on user requirements.

- The following LDAP password policy client controls are supported to warn users of password expiration events:

  Netscape "password has expired" "2.16.840.1.113730.3.4.4"
  Netscape "password expiration warning" "2.16.840.1.113730.3.4.5"

  NOTE: Netscape controls are supported by Netscape Directory Server, Netscape/Sun iPlanet and Red Hat/Fedora Directory Server.

- Password policy client controls other than the Netscape controls mentioned above are not supported.

- Password expiration warnings will not be seen during OpenVMS login when using directory server software that does not support Netscape password policy client controls, such as Active Directory and Novell eDirectory.

- Characters used in usernames and passwords are restricted to the 8-bit ISO 8859-1 (Latin-1) character set. UTF-8 support is not included in this release.

- Active Directory password changes are restricted to the 7-bit ASCII subset of the ISO 8859-1 (Latin-1) character set in this release. The reason for this restriction is that Active Directory expects UTF-8 character strings when updating the unicodePwd attribute.

Mapping Restrictions

- When executing DECnet operations, such as DECnet copy, users must specify their OpenVMS username and password.

- LDAP user accounts may not be mapped to the OpenVMS SYSTEM account. If a user's LDAP account is explicitly mapped to the OpenVMS SYSTEM account, the mapping does not occur and the user receives an "%ACME-E-FAILURE, operation failure" error when attempting to authenticate. The SYS$MANAGER:ACME$SERVER.LOG file contains:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE: The user name maps to
SYSTEM
```

8. Troubleshooting

ACME LDAP Agent Processing

This section documents the expected behavior when the ACME LDAP agent is operational.

The output from $ SHOW SERVER ACME shows the ACME LDAP agent in an Active state and Identification: "LDAP ACME Standard V2.00":

```
ACME Information on node NODE1  26-MAR-2021 22:05:28.13  Uptime 0 00:00:50

ACME Server id: 7  State: Processing New Requests
   Agents Loaded:         2   Active:       2
   Thread Maximum:        1   Count:        1
   Request Maximum:     834   Count:        0

ACME Agent id: 1  State: Active
   Name: "VMS"
   Image: "DISK$I64V842L1SYS:[VMS$COMMON.SYSLIB]VMS$VMS_ACMESHR.EXE;1"
   Identification: "VMS ACME built  20-SEP-2006"
   Information: "No requests completed since the last startup"
   Domain of Interpretation: Yes
   Execution Order:       1

ACME Agent id: 2  State: Active
   Name: "LDAP-STD"
   Image:           "DISK$I64V842L1SYS:[VMS$COMMON.SYSLIB]LDAPACME2$LDAP-
STD_ACMESHR.EXE;1"
   Identification: "LDAP ACME Standard V2.00"
   Information: "ACME_LDAP_DOI Agent is initialized"
   Domain of Interpretation: Yes
```

```
   Execution Order:      2
```

SYS$MANAGER:ACME$START.LOG contains information similar to:

```
$ Set NoOn
$ VERIFY = F$VERIFY(F$TRNLNM("SYLOGIN_VERIFY"))
%DCL-I-SUPERSEDE, previous value of LDAPACME$INIT has been superseded
  SYSTEM        job terminated at 26-MAR-2021 22:05:15.71

  Accounting information:
  Buffered I/O count:                419      Peak working set size:       5968
  Direct I/O count:                   94      Peak virtual size:         177888
  Page faults:                      1296      Mounted volumes:                0
  Charged CPU time:        0 00:00:00.07      Elapsed time:       0 00:00:36.11
```

SYS$MANAGER:ACME$SERVER.LOG contains information similar to:

```
%ACME-I-LOGOPEN, logfile opened on 26-MAR-2021 22:04:39.66
```

Under normal working conditions, the following LDAP communication occurs between the OpenVMS ACME LDAP agent and the chosen LDAP directory server when a user is externally authenticated:

After the user specifies their username at the Username: (or Login:) prompt:

OpenVMS LDAP client - If necessary, uses DNS Type A query to resolve server name specified for the 'server' directive.

OpenVMS LDAP client - Establishes TCP session to LDAP server on port specified by ‘port’ directive.

OpenVMS LDAP client - Binds to LDAP server using distinguished name (DN) specified by the 'bind_dn' directive and password specified by the 'bind_password' directive.

LDAP server – Returns an error if the bind credentials are invalid or other issues prevent a successful bind. If an error occurs, the user receives an error, and the login fails (the user is not prompted for a password). If the bind attempt is successful, processing continues.

OpenVMS LDAP client - Sends LDAP search request with search starting at the directory location specified by the ‘base_dn’ directive, using the scope specified by the 'scope’ directive, and a filter consisting of the value specified by the 'login_attribute' directive and the username specified by the user. For example, if ‘login_attribute = samaccountname’, the ‘filter’ directive is not specified, and the user enters a username of JDOE, the search filter is samaccountname=JDOE.

LDAP Server – If the search fails, an error is returned, and the login fails. If the search succeeds, the server returns all attributes of user's account.

OpenVMS LDAP client – Sends a search request for the user's account attribute 'passwordExpirationTime'.

LDAP Server – If the LDAP server is an Active Directory server, no such attribute exists in the Active Directory schema, so the search returns 0 attributes (the ‘passwordExpirationTime’ attribute is present in some other 3rd party LDAP server implementations).

OpenVMS LDAP client – Unbinds from the LDAP server.

OpenVMS LDAP client – Terminates the TCP session.

If no errors occur, the user is prompted for a password; after the user enters their password:

OpenVMS LDAP client – Establishes TCP session to LDAP server on port specified by 'port' directive.

OpenVMS LDAP client – Binds to LDAP server using the distinguished name of the user's LDAP account and the password specified by the user.

LDAP server – Sends either a bind success or failure (and reason code) message. If the bind succeeds, the user's credentials are valid and login processing continues. If the bind fails, an error is displayed, and the login attempt fails.

OpenVMS LDAP client – Unbinds from the LDAP server.

OpenVMS LDAP client – Terminates the TCP session.

Displaying Verbose Output

To display verbose output when restarting the ACME server, execute the following:

```
$ SET SERVER ACME/EXIT    ! Or use /ABORT (if /EXIT hangs)
$ SET SERVER ACME/START
$ SET VERIFY
$ @SYS$MANAGER:ACME$START
$ SET NOVERIFY
```

ACME Server Log Files

Errors during ACME server startup are written to SYS$MANAGER:ACME$START.LOG. Errors during ACME server execution are written to SYS$MANAGER:ACME$SERVER.LOG.

ACME LDAP Agent Start-up Issues

Problem

System-wide logins fail. Only a Console user can logon.

The DCL command `$ SHOW SERVER ACME` shows the VMS and LDAP agents in a Stopped state.

The SYS$MANAGER:ACME$SERVER.LOG file contains the messages:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE: Read_config() failed
...
...
-ACME-I-STATUSCODE, status = %X074AD832
```

NOTE: The status code %X074AD832 equates to:

```
$ EXIT %X074AD832
%ACME-E-INVPARAMETER, parameter selector or descriptor is invalid
```

Temporary Solution

To resolve the system-wide login failures as quickly as possible, enable only the VMS ACME agent by editing SYS$MANAGER:ACME$START.COM and commenting out the

line which starts the ACME LDAP AGENT. Restart the ACME server using the command `$ SET SERVER ACME/RESTART` and then use the command `$ SHOW SERVER ACME` to verify the VMS agent is active.

Cause

This behavior can occur if the LDAPACME$INIT logical name equates to a non-existent file.

Solution

Verify that the LDAPACME$INIT logical name equates to an existing ACME LDAP configuration file. If you are using multi-domain support, verify that each file in the LDPACME$INIT list exists. If necessary, correct the definition of the LDAPACME$INIT logical name and restart the ACME server using the command `$ SET SERVER ACME/RESTART`. Use the command `$ SHOW SERVER ACME` to verify the VMS agent and LDAP agent are active.

Problem

Server-wide logins fail. Only a Console user can login.

The DCL command `$ SHOW SERVER ACME` shows the VMS and LDAP ACME agents in a Stopped state.

The SYS$MANAGER:ACME$START.LOG file contains:

```
%ACME-E-NOSUCHDOI, the domain of interpretation does not exist
```

Cause

The AGENT_LIST symbol definition in SYS$MANAGER:ACME$START.COM has been modified but contains an invalid ACME agent name. For example:

```
$ SEARCH/NUMBER SYS$MANAGER:ACME$START.COM AGENT_LIST

    76  $ AGENT_LIST = "VMS,LDAP"
```

The correct name of the ACME LDAP agent is “LDAP-STD” (not “LDAP”).

Solution

It’s not necessary to modify the AGENT_LIST symbol to start the ACME LDAP agent. Reset the AGENT_LIST symbol in SYS$MANAGER:ACME$START.COM to a null value (“”). Restart the ACME server using the command `$ SET SERVER ACME/RESTART` and then use the command `$ SHOW SERVER ACME` to verify the VMS agent and LDAP agent are active.

.

Problem

System-wide logins fail. Only a Console user can logon.

The SYS$MANAGER:ACME$SERVER.LOG file contains:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE: Updating LocalLdap
mapfile is failed
```

Cause

The file specified by the 'mapping_file' directive doesn't exist.

Solution

Correct or comment out the ‘mapping_file’ directive in the ACME LDAP configuration file. Restart the ACME server using the command `$ SET SERVER ACME/RESTART` and then use the command `$ SHOW SERVER ACME` to verify the VMS agent and LDAP agent are active.

Problem

After starting the ACME server, `$ SHOW SERVER ACME` does not display the LDAP agent (only the VMS agent is loaded and in an Active state).

The SYS$MANAGER:ACME$START.LOG file contains:

```
Please ensure the following logical is defined /SYSTEM/EXECUTIVE_MODE
  LDAPACME$INIT
```

Cause

The required LDAPACME$INIT system logical name does not exist or is not defined as an EXECUTIVE_MODE system logical name.

Solution

Correctly define the LDAPACME$INIT logical name (with qualifiers /SYSTEM/EXECUTIVE_MODE) to equate to the file specification of the ACME LDAP agent configuration file. Restart the ACME server using the command `$ SET SERVER ACME/RESTART` and then use the command `$ SHOW SERVER ACME` to verify the VMS agent and LDAP agent are active.

Problem

After the OpenVMS host is rebooted, external authentication no longer works.

Cause

Verify that the LDAP ACME agent is active (`$ SHOW SERVER ACME`). If not, the likely cause is that the system startup procedure (i.e., SYS$MANAGER:SYSTARTUP_VMS.COM) does not contain the required command to restart the ACME Server.

Solution

Restart the ACME Server and update the system startup procedures to execute the following command:

```
$ SET SERVER ACME/RESTART
```

ACME LDAP Agent Operating Issues

If external authentication using the ACME LDAP agent has been functioning normally but unexpectedly begins failing, verify that the first LDAP directory server specified in the 'server' directive list is reachable using the `$ PING` command. If the PING fails and the 'server' directive value consists of a list of servers, use the `$ PING` command to determine whether the next server in the list is reachable. Continue this process until an LDAP directory server responds. Modify the 'server' directive in the ACME LDAP agent configuration file so that the reachable LDAP directory server is first in the list and restart the ACME server using the command `$ SET SERVER ACME/RESTART`.

NOTE: An LDAP server is considered reachable if it responds to any communication attempt by the ACME LDAP agent. If a failure occurs while communicating with an LDAP server, the ACME LDAP agent will *not* failover to the next server in the 'server' directive list.

Problem

External authentication is failing for all applicable users (login using /LOCAL_PASSWORD is working).

If this is the first time the ACME LDAP agent is being deployed, it is often beneficial to reconfigure the ACME LDAP agent so that the SSL/TLS encryption is disabled and then enable SSL/TLS encryption again once the problem is resolved.

To disable SSL/TLS encryption, use the following settings in the ACME LDAP agent configuration file:

```
port = 389
port_security = none
```

CAUTION: Using 'port_security = none' will result in all data, including passwords, being transmitted in clear text. This setting is meant for troubleshooting purposes only and should not be used on a permanent basis.

It may be necessary to obtain a network trace while duplicating the failure for analysis by VSI support.

Problem

External authentication is failing for all applicable users with the following error:

```
Operation failure; if logging is enabled, see details in the ACME$SERVER
log file
```

The SYS$MANAGER:ACME$SERVER.LOG file contains:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE: Internal error. LDAP
search operation failed. ldap_status:31(Invalid credentials)
```

Cause

The value of the 'bind_dn' and/or 'bind_password' directive in the ACME LDAP configuration file is incorrect.

Solution

Obtain the correct bind credentials and update the 'bind_dn' and/or 'bind_password' directive in the ACME LDAP configuration file accordingly. Restart the ACME server using the command `$ SET SERVER ACME/RESTART` and then use the command `$ SHOW SERVER ACME` to verify the VMS agent and LDAP agent are active.

Problem

External authentication fails for all applicable users.

The file SYS$MANAGER:ACME$SERVER.LOG contains:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE: Internal error. LDAP
search operation failed. ldap_status:fffffff7(Bad parameter to an ldap
routine)
```

Cause

The 'server' directive in the ACME LDAP agent configuration file contains a comma or other extraneous characters.

Solution

Remove the extraneous characters from the value of the 'server' directive in the ACME LDAP configuration file. When specifying a list of LDAP servers for the 'server' directive, delimit elements in the list with one or more space characters. Do not use tabs, commas, etc. Restart the ACME server using the command `$ SET SERVER ACME/RESTART` and then use the command `$ SHOW SERVER ACME` to verify the VMS agent and LDAP agent are active.

Problem

External authentication fails for all appliable users.

The SYS$MANAGER:ACME$SERVER.LOG file contains:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE: Internal error. LDAP
search operation failed. ldap_status:ffffffff(Can't contact LDAP server)
```

Cause

The 'server' directive in the ACME LDAP agent configuration file contains a list of servers which are delimited by a Tab character.

Solution

Replace all Tab characters with one or more space characters in the value of the 'server' directive in the ACME LDAP configuration file. When specifying a list of LDAP servers for the 'server' directive, delimit elements in the list with one or more space characters. Do not use tabs, commas, etc. Restart the ACME server using the command `$ SET SERVER`

`ACME/RESTART` and then use the command `$ SHOW SERVER ACME` to verify the VMS agent and LDAP agent are active.

Problem

External authentication fails for all applicable users.

The SYS$MANAGER:ACME$SERVER.LOG file contains:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE: Internal error. LDAP
search operation failed. ldap_status:8(Strong(er) authentication
required)
```

Cause

The LDAP directory server does not allow a simple bind over an unencrypted session.

Solution

Configure the ACME LDAP agent to use an option for the 'port_security' directive other than "NONE". See the options for the 'server' directive in *Appendix A*. Restart the ACME server using the command `$ SET SERVER ACME/RESTART` and then use the command `$ SHOW SERVER ACME` to verify the VMS agent and LDAP agent are active.

Problem

External authentication fails for one user (but not other externally authenticated users).

Cause

The user's OpenVMS account does not have the EXTAUTH flag set or the user's LDAP username is not identical to the user's OpenVMS username and no username mapping exists.

Solution

Verify that the user's OpenVMS account has the EXTAUTH flag, for example:

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

If necessary, set the EXTAUTH flag on the user's OpenVMS account:

```
$ MC AUTHORIZE MODIFY <username> /FLAG=EXTAUTH
```

If the user's LDAP username is not identical to their OpenVMS username, the user's LDAP username must be explicitly mapped. See the *Username Mapping* section for more information.

Set Password Issues

Problem

The DCL command `$ SET PASSWORD` returns:

```
%ACME-F-CONTACTSYSMGR, requested operation has failed; contact the
system manager
```

Cause

The HP TCP/IP Services for OpenVMS SSH Server is not configured to use LOGINOUT for password changes.

Solution

On systems running HP TCP/IP Services for OpenVMS, to allow externally authenticated users who login via SSH to change their LDAP account password by using the DCL command $ SET PASSWORD, define the system logical name TCPIP$SSH_SERVER_USE_LOGINOUT and restart the SSH Server as follows:

```
$ DEFINE/SYSTEM TCPIP$SSH_SERVER_USE_LOGINOUT 1
$ @SYS$STARTUP:TCPIP$SSH_SHUTDOWN
$ @SYS$STARTUP:TCPIP$SSH_STARTUP
```

WARNING: Stopping the SSH Server will result in termination of all SSH sessions. Consider using a TELNET or a DECnet login session to restart the SSH Server (or use the system Console).

Problem

The DCL command `$ SET PASSWORD` returns:

```
%ACME-F-FAILURE, operation failure; if logging is enabled, see details
in the ACME$SERVER log file
```

The SYS$MANAGER:ACME$SERVER.LOG file contains:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE: Error returned from LDAP
while setting password:x35, DSA is unwilling to perform
```

Cause

The ‘port_security’ directive in the ACME LDAP agent configuration file is set to “NONE”. Password changes by externally authenticated users are allowed by the LDAP directory server only when the LDAP communication is secure (using SSL/TLS).

Solution

Modify the ACME LDAP agent configuration to use one of the TLS option values for the ‘port_security’ directive as documented in *Appendix A*.

Problem

The DCL command $ SET PASSWORD returns the message “`**** The new password was not accepted ****`” and the user is prompted again for a new password:

The SYS$MANAGER:ACME$SERVER.LOG file contains the message:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE:
acmekcv$cb_queue_dialogue() failed to display  LDAP_CONSTRAINT_VIOLATION
while setting passwd
```

Cause

The new password does not meet the password policy requirements (i.e., minimum password length, password history, etc.) set on the LDAP directory server.

Solution

Set a new password that complies with the password policy.

Problem

The DCL command $ SET PASSWORD fails with the messages:

```
%ACME-F-FAILURE, operation failure; if logging is enabled, see details
in the ACME$SERVER log file
```

The SYS$MANAGER:ACME$SERVER.LOG file contains the message:

```
-ACME_-I-TRACE,  MESSAGE FROM THE MESSAGE FILE: Error returned from LDAP
while setting password:x32, Insufficient access
```

Cause

The 'password_type' directive in the ACME LDAP agent configuration file is not set to "active-directory".

Solution

Set the ‘password_type’ directive in the ACME LDAP agent configuration file to the value “active-directory” and restart the ACME server using the command `$ SET SERVER ACME/RESTART`.

Appendix A – Configuration Directives

The following table lists the ACME LDAP agent directive names and configuration details.

Directive	Configuration Details
server	This is a mandatory directive. Specify the DNS host names or IP addresses of one or more LDAP directory servers. Use one or more space characters between the server names or IP addresses (do not use commas or tabs to delimit). For example: server = dc1.corp.com dc2.corp.com 10.1.11.111 The ACME LDAP agent tries to connect to the first server in the list. If the target server is unreachable, the next server is attempted; this repeats until the list is exhausted. If the list contains more than one server, note the following: • The ‘base_dn’, ‘bind_dn’, and ‘bind_password’ directive values must be the same on all listed directory servers. • The accounts of users being authenticated by the ACME LDAP agent must be present on all directory servers. • Set the ‘bind_timeout’ directive appropriately to ensure that when the ACME LDAP agent attempts to reach all redundant servers, the client session does not time out. • If you plan to use the ‘ca_file’ directive to verify the certificate of the LDAP directory servers, the file must contain the public key of the Certificate Authority (CA) that signed the server certificate of each LDAP directory server. If the server certificates are signed by different CAs, include the public key of each CA in the same ‘ca_file’. For more information, see the ‘ca_file’ directive details below.
port	This is a mandatory directive. Specify the LDAP TCP port number that the directory servers listen on. Default value is “389” (the standard, insecure LDAP port). Set to “636” to use the standard, secure LDAP port (LDAPS).
port_security	Specify the method used to encrypt communications over the LDAP port specified by the ‘port’ directive. Possible values are: NONE - Clear text mode; all requests, responses and data (including passwords) are transmitted in clear text. The ‘port’ directive must be set to 389 (port = 389). Recommended only for troubleshooting purposes. Values for LDAPS options (when using ‘port = 636’):

SSLTLS - Negotiate TLS encryption with the server
SSL - Select only SSLV3 encryption (not recommended)
SSLTLS10 - Select only TLSV1.0 encryption
SSLTLS11 - Select only TLSV1.1 encryption
SSLTLS12 - Select only TLSV1.2 encryption

Values for StartTLS options (when using 'port = 389'):

StartTLS - Negotiate TLS encryption with the server
StartTLS10 - Select only TLSV1.0 encryption
StartTLS11 - Select only TLSV1.1 encryption
StartTLS12 - Select only TLSV1.2 encryption

bind_dn

This is a mandatory directive.

Specify the distinguished name (DN) of an LDAP directory server account that is created for and used by the ACME LDAP agent to bind to and search the directory server.

The 'bind_dn' and 'bind_password' directives provide the credentials used to bind (authenticate) to the directory servers.

If the directory server is an Active Directory domain controller, a domain administrator may obtain the distinguished name of an ACME LDAP user account using either of the following methods:

- Launch Active Directory Users and Groups. Under the View menu option, enable "Advanced Features" (a check mark should appear). Locate and double-click the user account created for the ACME LDAP agent to display its Properties page and then select the Attribute Editor tab. In the Attributes section, double-click the *distinguishedName* attribute to display its value.

- Run the Windows LDIFDE utility from a command prompt. Use the commands below to obtain the distinguished name of the account. In the example, the username of the LDAP ACME user account is LDAPAUTH:

```
ldifde -r samaccountname=LDAPAUTH -f ldifde.out
findstr dist ldifde.out
```

Set the 'bind_dn' directive to the distinguished name displayed.

bind_password

This is a mandatory directive.
Specify the password for the account specified by the 'bind_dn' directive. Specify the password using the correct case, but **do not** enclose in quotes.

bind_timeout

Specify a timeout value in seconds which defines the maximum number of seconds the ACME LDAP agent will wait for a response to a bind request before abandoning the attempt.
By default, if the target directory server is not reachable, each bind request to a directory server, can take as long as 75 seconds to timeout (TCPIP default connection establishment timeout). If multiple servers are specified in the 'server' directive value, the user login session (i.e., a TELNET

session) may expire before the ACME LDAP agent is able to contact a working directory server.
Use the 'bind_timeout' directive when listing multiple servers in the 'server' directive. For example, if the 'server' directive list consists of 3 servers and the 'bind_timeout' directive is set to three seconds, the overall timeout period is approximately 9 seconds.

login_attribute — This is a mandatory directive.
Specify the LDAP schema attribute that contains the username for login purposes. For Active Directory LDAP servers, this must be set to "samaccountname". For OpenLDAP servers, the attribute name is often "uid" but may be different in your configuration.

base_dn — This is a mandatory directive.
Specify the distinguished name of an LDAP directory element on the directory server where the search for a user account begins.

The LDAP users are stored in a tree structure in the directory server. The user entries must be present under the specified 'base_dn' tree element as sub-tree elements. The ACME LDAP agent will search for matching entries based on the attribute specified by the 'login_attribute' directive. To search the entire directory tree, specify the distinguished name of the domain. For example, if the domain name is CORP.COM:

base_dn = DC=corp,DC=com

scope — Indicates the set of entries at or below the LDAP directory location specified by the 'base dn' directive that may be considered potential matches for a search request. Valid (**case-sensitive**) keywords are:

sub – Searches the entry specified by the 'base_dn' directive and all of its subordinates to any depth. Most customers should choose this option.

one – Only the immediate children of the entry specified by the 'base_dn' directive should be considered. The 'base_dn' entry itself should not be considered, nor any descendants of the immediate children of the base entry.

base – (Default) Only the entry specified by the 'base_dn' directive should be considered. None of its subordinates will be considered.

filter — Specify an LDAP search filter. The default value is no filter.

search_timeout — Specify the number of seconds before an LDAP search request times out. The default is 20 seconds. Use the 'search_timeout' directive when listing multiple servers in the 'server' directive (see the 'bind_timeout' directive for more information).

mapping — Specify the username mapping mechanism to use. There are three options (more information, see *Username Mapping*):

Null (no value) – Indicates that only implicit username mapping occurs. In this case, the user's LDAP directory username must be identical to the user's OpenVMS username.

server – Indicates that global username mapping is enabled (which is managed on the directory server).

local – Indicates that local username mapping is enabled, and mapping is managed using a text file on the OpenVMS host (specified by the 'mapping_file' directive).

mapping_attribute

This directive is applicable only for global username mapping. Specify the name of the schema attribute on the LDAP directory server that will be used to specify username mapping data. For example, to use the Description field of user accounts, specify "mapping_attribute = description".

A newly created attribute on the directory server may also be created to store the username mapping data. This attribute should be an IA5 multi-valued string.

mapping_target

This directive is applicable only for global username mapping. The mapping_target is an arbitrary string of your choice which the ACME LDAP agent uses when searching for the user's OpenVMS username in the field specified by the 'mapping_attribute' value. The format of the entry is <string>/<OpenVMS-username>. For example, if the ACME LDAP configuration file contains:

mapping = server
mapping_attribute = description
mapping_target = VMSUser

To map a user's LDAP directory account to their OpenVMS account, populate the Description field of the user's LDAP directory account with the string "VMSUser/", followed by the user's OpenVMS username. For example, if the user's OpenVMS username is JDOE, specify:

VMSUser/jdoe

No extraneous text may precede the 'mapping_target' directive string or follow the username in the field specified by the 'mapping_attribute' directive. Neither the 'mapping_target' string, nor the username are case-sensitive.

mapping_file

This directive is applicable only for local username mapping. Specify the complete file specification of the text file used for mapping user accounts. Entries in the file use the syntax:

LDAP-username, VMS-username

where LDAP-username is the username of the user in the LDAP directory server.

Changes to a username mapping file are not dynamic; however, the username mapping file can be reloaded without restarting the ACME Server with SYS$SYSTEM:LDAP_LOAD_LOCALUSER_DATABASE.EXE (or restart ACME Server).

Comments (!) in the username mapping file are supported.

Do not include the domain name as part of the Windows username in the username mapping file, even when using a multi-domain configuration.

Enclose usernames containing spaces in quotes.
For information on how to populate and load the contents of the username mapping file, see the included template file – SYS$STARTUP:LDAP_LOCALUSER_DATABASE.TXT_TEMPLATE.

domain

This directive is applicable for multi-domain support. The name specified here should match the short domain name of the LDAP server's domain.

The definition of the LDAPACME$INIT logical name determines the "default" domain. The domain specified in the configuration file which corresponds to the first file in the list defined by LDAPACME$INIT, determines the "default" domain. Users in the "default" domain do not need to specify their logon domain name as part of their username when logging into the OpenVMS host. However, users of the other domains must include the domain name specified by the 'domain' directive as part of their username when logging into OpenVMS, using the syntax:

domain\username

For example, if the logical name LDAPACME$INIT is defined as:

```
$ SHOW LOGICAL LDAPACME$INIT
   "LDAPACME$INIT" =
"SYS$COMMON:[SYS$STARTUP]LDAPACME$CONFIG-STD-
US.INI" (LNM$SYSTEM_TABLE)
         = "SYS$COMMON:[SYS$STARTUP]LDAPACME$CONFIG-
STD-EMEA.INI"
```

And the configuration file LDAPACME$CONFIG-STD-US.INI contains:

domain = us

while the configuration file LDAPACME$CONFIG-STD-EMEA.INI contains:

domain = emea

When users in the EMEA domain login to the OpenVMS host, they must specify a username of EMEA\<username>, while users in the US domain do not need to (but may) specify the domain name (US) when logging in.

The domain name specified is not case sensitive, must not contain any special characters, and must not be longer than 25 characters.

ca_file

This directive is optional.
Specify the complete specification of a file containing the PEM-format public key of the certificate authority (CA) that signed the certificate of the LDAP directory server. The ACME LDAP agent needs that public key to verify the LDAP server's certificate (except when 'port_security = none'). Verifying the server's certificate ensures that the ACME LDAP agent is connecting to the intended directory server rather than an imposter. If this directive is not included, the LDAP server's certificate is not verified.

If the 'server' directive lists multiple servers and the certificates of those servers were signed by different CAs, add the public key certificate information for each CA into the same file. For example:

```
$ TYPE CACERTS.PEM
-----BEGIN CERTIFICATE-----
.......
CA 1 public key certificate in base64 encoded format
.......
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
.......
CA 2 public key certificate in base64 encoded format
.......
-----END CERTIFICATE-----
$
```

password_type

Specify one of the following values ("standard" is the default):

standard
active-directory

If you are using Windows Active Directory LDAP servers, specify 'password_type = active-directory', otherwise any attempts to use the DCL $ SET PASSWORD command by externally authenticated users will fail.

password_update

Specify one of the following values ("replace" is the default):

replace
remove-and-add

Applies only when the 'password_type' directive is set to "standard". Some directory servers require the old password to be supplied when changing the userPassword attribute; others do not.

Appendix B – Example Configurations

Example 1. The LDAP directory servers are Active Directory domain controllers named DC1.CORP.COM and DC2.CORP.COM. An Active Directory administrator has created a user account for the ACME LDAP agent to use. The account has the following characteristics:

Distinguished name: CN=LDAP AUTH,OU=SvcAccts,DC=corp,DC=com
Password: &RvAy*7bXh@2Si
Password never expires
Password cannot be changed

The ACME LDAP agent will also be configured to:

- Use port 636, the secure LDAPS port.
- Negotiate the version of TLS with the directory server.
- Use local username mapping with the file SYS$COMMON:[SYS$STARTUP]LDAP_USER_MAPPING.TXT.
- Begin each search at the top of the LDAP directory tree.
- Search the entire directory.

The ACME LDAP agent configuration file:

```
server = dc1.corp.com dc2.corp.com
bind_timeout = 3
bind_dn = CN=LDAP AUTH,OU=SvcAccts,DC=corp,DC=com
bind_password = &RvAy*7bXh@2Si
port = 636
port_security = SSLTLS
login_attribute = samaccountname
base_dn = DC=corp,DC=com
scope = sub
password_type = active-directory
mapping = local
mapping_file = SYS$COMMON:[SYS$STARTUP]LDAP_USER_MAPPING.TXT
```

Example 2. The LDAP directory servers are Active Directory domain controllers named DC1.CORP.COM and DC2.CORP.COM. An Active Directory administrator has created a user account for the ACME LDAP agent to use. The account has the following characteristics:

Distinguished name: CN=LDAP AUTH,OU=SvcAccts,DC=corp,DC=com
Password: &RvAy*7bXh@2Si
Password never expires
Password cannot be changed

The ACME LDAP agent will be also configured to:

- Use port 389, the insecure LDAP port, but secure it using the StartTLS protocol.
- Negotiate the version of TLS with the directory server.
- Use global username mapping.

- Use the ‘description’ field to store the mapped OpenVMS username, which will be preceded by string “VMSUser” (separated by a slash).
- Begin each search at the top of the LDAP directory tree.
- Search the entire directory.

The ACME LDAP agent configuration file:

```
server = dc1.corp.com dc2.corp.com
bind_timeout = 3
bind_dn = CN=LDAP AUTH,OU=SvcAccts,DC=corp,DC=com
bind_password = &RvAy*7bXh@2Si
port = 389
port_security = StartTLS
login_attribute = samaccountname
base_dn = DC=corp,DC=com
scope = sub
password_type = active-directory
mapping = server
mapping_attribute = description
mapping_target = VMSUser
```

Example 3. Configure the ACME LDAP agent to support logins for users from two Active Directory domains named US.CORP.COM and EMEA.CORP.COM. The US.CORP.COM domain contains domain controllers U1.US.CORP.COM and U2.US.CORP.COM while the EMEA.CORP.COM domain contains domain controllers E1.EMEA.CORP.COM and E2.EMEA.CORP.COM. The domain administrators have created a user account in both the US and EMEA domains for use by the ACME LDAP agent.

The Active Directory account in the US domain has the following characteristics:

```
Distinguished name:  CN=VMSLDAP,CN=Users,DC=US,DC=corp,DC=com
Password: bt!w$AAdvPn6AW
Password never expires
Password cannot be changed
```

The Active Directory account in the EMEA domain has the following characteristics:

```
Distinguished name:  CN=VMSLDAP,CN=Users,DC=EMEA,DC=corp,DC=com
Password: Sn5Yf&!JT5fQ6A
Password never expires
Password cannot be changed
```

The ACME LDAP agent will also be configured to:

- Use port 636, the secure LDAPS port.
- Negotiate the version of TLS with the directory server.
- Use local username mapping with a separate mapping file for each domain:
- US domain - SYS$COMMON:[SYS$STARTUP]LDAP_USER_MAPPING_US.TXT
- EMEA domain - SYS$COMMON:[SYS$STARTUP]LDAP_USER_MAPPING_EMEA.TXT
- Begin each search at the top of the LDAP directory tree.
- Search the entire directory.

Two separate ACME LDAP configuration files are required – one for each domain.

The configuration file for the US domain:

```
domain = US
server = u1.us.corp.com u2.us.corp.com
bind_timeout = 3
bind_dn = CN=VMSLDAP,CN=Users,DC=us,DC=corp,DC=com
bind_password = bt!w$AAdvPn6AW
port = 636
port_security = SSLTLS
login_attribute = samaccountname
base_dn = DC=us,DC=corp,DC=com
scope = sub
password_type = active-directory
mapping = local
mapping_file = SYS$COMMON:[SYS$STARTUP]LDAP_USER_MAPPING_US.TXT
```

The configuration file for the EMEA domain:

```
domain = emea
server = e1.emea.corp.com e2.emea.corp.com
bind_timeout = 3
bind_dn = CN=VMSLDAP,CN=Users,DC=emea,DC=corp,DC=com
bind_password = Sn5Yf&!JT5fQ6A
port = 636
port_security = SSLTLS
login_attribute = sAMAccountName
base_dn = DC=emea,DC=corp,DC=com
scope = sub
password_type = active-directory
mapping = local
mapping_file = SYS$COMMON:[SYS$STARTUP]LDAP_USER_MAPPING_EMEA.TXT
```

In this example, the logical name LDAPACM$INIT must equate to both configuration files. For example, if the configuration file names for the US and EMEA domains, respectively, are:

```
SYS$COMMON:[SYS$STARTUP]LDAPACME$CONFIG-STD-US.INI
SYS$COMMON:[SYS$STARTUP]LDAPACME$CONFIG-STD-EMEA.INI
```

Use the following command to define the LDAPACME$INIT logical name; add this command to SYS$MANAGER:ACME$START.COM, so that the logical name is defined prior to starting the ACME LDAP agent:

```
$ DEFINE/SYSTEM/EXECUTIVE_MODE LDAPACME$INIT -
SYS$COMMON:[SYS$STARTUP]LDAPACME$CONFIG-STD-US.INI, -
SYS$COMMON:[SYS$STARTUP]LDAPACME$CONFIG-STD-EMEA.INI
```

Legal Notice