VSI OpenLDAP ACME Agent for OpenVMS

Configuration and User Guide

Operating Systems: VSI OpenVMS Alpha Version 8.4-2L1 or higher
VSI OpenVMS IA-64 Version 8.4-2L1 or higher
VSI OpenVMS x86-64 Version 9.2-3 + Update V3 or higher

Software Version: VSI OpenLDAP for OpenVMS Version 2.6-6A

VMS Software, Inc. (VSI)
Boston, Massachusetts, USA

VSI OpenLDAP ACME Agent for OpenVMS Configuration and User Guide

Legal Notice

Table of Contents

1. Introduction

VSI OpenLDAP ACME agent for 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 OpenLDAP ACME 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. With 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 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.

This manual details post-installation tasks and provides information on username mapping, troubleshooting help, a list of configuration directives, and several example configurations. It also includes details of existing issues and restrictions.

For installation instructions, as well as information specific to the latest release of VSI OpenLDAP, refer to the most recent version of the *VSI OpenLDAP for OpenVMS Release Notes and Installation Guide* available at https://docs.vmssoftware.com/.

Note

OpenVMS provides an LDAP-based ACME agent that is integrated into the operating system. In this document, this component is referred to as the **integrated ACME LDAP agent**, while the OpenLDAP-based implementation is referred to as the **OpenLDAP ACME agent**.

---

2. Post-Installation Tasks

For instructions on how to install VSI OpenLDAP, refer to the most recent version of the *VSI OpenLDAP for OpenVMS Release Notes and Installation Guide*.

After the VSI OpenLDAP product has been installed, perform the following tasks to configure and enable the OpenLDAP ACME agent.

2.1. Install the ACME LOGIN Images

In an OpenVMS cluster...

… complete this task on any one system that boots from a particular system disk.

To install the ACME LOGIN images (SYS$SYTEM:LOGINOUT.EXE and SETP0.EXE), run the command file SYS$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 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
```

2.2. Install the OpenLDAP Persona Extension

In an OpenVMS cluster...

… complete this task on any one system that boots from a particular system disk.

To set up the OpenLDAP persona extension, perform the following tasks:

1. Add an entry for the OpenLDAP persona extension image to the system images file as follows:

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

2. Generate a new system images data file via the following command:

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

3. **For x86-64 systems only –** Reconfigure the node memory disk using the following command procedure:

   ```
   $ @SYS$UPDATE:SYS$MD.COM
   ```

4. Reboot each applicable system via the following command:

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

   ### Note

   To avoid possible system-wide login issues, VSI recommends rebooting the system *before* initially enabling the OpenLDAP ACME agent.

2.3. Verify the OpenLDAP Persona Extension is Installed

In an OpenVMS cluster...

… perform this task on all cluster members that will run the Open LDAP ACME agent.

After rebooting a system, verify that the OpenLDAP persona extension is installed via the following commands:

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

The OpenLDAP persona extension has *not* been installed if the result looks similar to the following:

```
No loadable image matching "LDAPACME2$EXT" found
```

In that case, follow the instructions starting at *Section 2.1, "Install the ACME LOGIN Images"* to successfully install the OpenLDAP persona extension.

2.4. Configure the OpenLDAP ACME Agent

The OpenLDAP ACME agent uses a text configuration file that contains directives (described in *Appendix A, "Configuration Directives"*) 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 OpenLDAP ACME agent configuration file (i.e., by storing the configuration file on a disk that is mounted cluster-wide prior to restarting the ACME server during startup).
- Multiple OpenLDAP ACME agent configurations may be deployed in a single cluster using different file names for the OpenLDAP ACME agent configuration files.
- Each cluster member may use a unique OpenLDAP ACME 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[1] 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 OpenLDAP ACME agent configuration file to specify the directives that correspond to your requirements. For a description of the supported directives in the OpenLDAP ACME agent configuration file, see *Appendix A, "Configuration Directives"*. Example configurations are provided in *Appendix B, "Example Configurations"*.

Important

The OpenLDAP ACME agent requires the credentials of an account that 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 OpenLDAP ACME 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

[1] SYS$STARTUP:LDAPACME$CONFIG-STD.INI_TEMPLATE

require a change to the password specified in the OpenLDAP ACME agent configuration file (and the ACME server must be restarted).

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

- Comments, denoted by an exclamation point (!), are allowed. However, 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 OpenLDAP ACME agent configuration file requires the following six directives:

  - server
  - bind_dn
  - bind_password
  - base_dn
  - login_attribute
  - scope

- Any modifications to the configuration files will only take effect after the ACME server is restarted.
- Ensure that the OpenLDAP ACME agent 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 OpenLDAP ACME agent configuration file only for privileged users:

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

2.5. Define the LDAPACME$INIT Logical Name

In an OpenVMS cluster...

… perform this task on all cluster members that will run the OpenLDAP ACME 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 OpenLDAP ACME agent 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$INIT logical must be defined prior to starting the OpenLDAP ACME agent. VSI recommends adding this logical name definition to the command procedure SYS$MANAGER:ACME$START.COM so that it executes prior to starting the OpenLDAP ACME agent (see *Section 2.6, "Update SYS$MANAGER:ACME$START.COM"*).

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

The ACME$START.COM procedure runs automatically when restarting the ACME server. The current version of ACME$START.COM contains the command required to start the **integrated LDAP ACME agent**.[2] That command must be replaced with the command required to start the **OpenLDAP ACME agent**.

In an OpenVMS cluster...

… with multiple system disks, perform the procedure below on any one system that boots from a particular system disk.

Perform the following procedure:

1. Open ACME$START.COM in your editor of choice.
2. Locate and comment out the line:

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

3. Add the following line above or below the line that you just commented out:

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

4. Save the changes and close the file.

2.7. Restart the ACME Server

In an OpenVMS cluster...

… perform this step on all cluster members that will run the OpenLDAP ACME agent.

After modifying SYS$MANAGER:ACME$START, restart the ACME server via the following command:

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

2.8. Verify the ACME Agents Are Active

In an OpenVMS cluster...

… perform this step on all cluster members that run the OpenLDAP ACME agent.

[2] The LDAP-based ACME agent that is integrated into the operating system.

Execute the **SHOW SERVER ACME** command and verify that the VMS and LDAP ACME agents are both in the Active state. If both agents are not in the Active state, see *Section 5, "Troubleshooting"*:

```
$ 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$LDAPSTD_ACMESHR.EXE;1"
   Identification: "OPENLDAP ACME Standard V2.6-6A"
   Information: "ACME_LDAP_DOI Agent is initialized"
   Domain of Interpretation: Yes
   Execution Order:      2
```

Determining Which LDAP ACME Agent is Active

To determine which ACME 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 integrated LDAP ACME agent is active. If instead it displays `OPENLDAP ACME Standard V2.6-6A`, the OpenLDAP ACME agent is active.

Switching Between the Integrated LDAP and OpenLDAP ACME Agents

Warning

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

To switch between the integrated LDAP ACME agent and the OpenLDAP ACME agent, modify ACME$START.COM and restart the ACME server. For example, if the integrated LDAP ACME agent is active, perform the following procedure to switch to the OpenLDAP ACME agent:

1. Edit SYS$MANAGER:ACME$START.COM.
2. Uncomment the command that starts the OpenLDAP ACME agent:

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

3. Comment out the command that starts the integrated LDAP ACME agent:

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

4. Save the changes.

5. Restart the ACME server via the following command:

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

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

If a system is running VSI TCP/IP Services for OpenVMS, to allow externally authenticated users connecting via the TCP/IP Services SSH server 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
```

2.10. Configure OpenVMS User Accounts

For a user to be externally authenticated using the OpenLDAP ACME agent, set the EXTAUTH flag on the user's OpenVMS account as follows:

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

When the EXTAUTH flag is set on a user's account, the user is validated using only the external authenticator (LDAP). When a user successfully logs in using the OpenLDAP ACME 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 *Section 4.1, "Password Synchronization"*) 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 logins when using the TCP/IP Services SSH server.

---

3. Username Mapping

The OpenLDAP ACME 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 OpenLDAP ACME 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.

3.1. Global Username Mapping

To enable global mapping, perform the following steps:

1. 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 OpenLDAP ACME agent configuration file and set the "mapping_attribute" directive to the name of the chosen attribute. For example:

   ```
   mapping_attribute = description
   ```

2. Choose a string identifier that will precede the OpenVMS username. Edit the OpenLDAP ACME agent 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
   ```

3. Restart the ACME Server via the following command:

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

4. 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
   ```

3.2. Local Username Mapping

To enable local username mapping, perform the following steps:

1. Make a copy of SYS$STARTUP:LDAP_LOCALUSER_DATABASE.TXT_TEMPLATE and rename it to a file name of your choice. For example:

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

2. 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`.

3. Add the following directives to the OpenLDAP ACME agent 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
```

4. Restart the ACME server via the following command:

```
$ 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 OpenLDAP ACME agent configuration file.
- The domain name. This parameter is optional when the "domain" directive is not included in the OpenLDAP ACME agent configuration file. Otherwise, specify the same domain name as specified in the OpenLDAP ACME agent 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
```

4. Restrictions

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

4.1. 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 retains the case of the password and 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.

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.

4.2. 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 user is not externally authenticated during the session, the DCL command **SET PASSWORD** changes only the password of the user's OpenVMS account.
- 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.

4.3. 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
```

5. Troubleshooting

5.1. OpenLDAP ACME Agent Processing

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

The output from the **`SHOW SERVER ACME`** command shows the OpenLDAP ACME agent in an active state and the `OPENLDAP ACME Standard V2.6-6A` identification. For example:

```
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$LDAPSTD_ACMESHR.EXE;1"
   Identification: "OPENLDAP ACME Standard V2.6-6A"
   Information: "ACME_LDAP_DOI Agent is initialized"
   Domain of Interpretation: Yes
   Execution Order:      2
```

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

```
$ 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 the following:

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

Under normal working conditions, the following LDAP communication occurs between the VSI OpenLDAP ACME agent and the chosen LDAP directory server when a user is externally authenticated. After the user specifies their username at either the `Username:` prompt or the `Login:` prompt, the following happens:

1. OpenVMS LDAP client, if necessary, uses a DNS Type A query to resolve the server name specified for the "server" directive.
2. OpenVMS LDAP client establishes TCP session to LDAP server on port specified by "port" directive.
3. 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.
4. 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.
5. 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`.
6. If the search fails, the LDAP Server returns an error and the login fails. If the search succeeds, the server returns all attributes of user's account.
7. OpenVMS LDAP client sends a search request for the user's account attribute "passwordExpirationTime".
8. If the LDAP server is an Active Directory server (which means that no such attribute exists in the Active Directory schema), the search returns 0 attributes (the "passwordExpirationTime" attribute is present in some other 3rd party LDAP server implementations).
9. OpenVMS LDAP client unbinds from the LDAP server and terminates the TCP session.

If no errors have occurred up to this point, the user is prompted for a password. After the user enters the password, the following happens:

1. OpenVMS LDAP client establishes TCP session to LDAP server on port specified by "port" directive.
2. OpenVMS LDAP client binds to LDAP server using the distinguished name of the user's LDAP account and the password specified by the user.
3. 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.
4. OpenVMS LDAP client unbinds from the LDAP server and terminates the TCP session.

5.2. 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
```

5.3. 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.

5.4. OpenLDAP ACME Agent Start-up Issues

PROBLEM	System-wide login failures. Only a Console user can log in.
	
	The DCL command **SHOW SERVER ACME** shows the VMS and LDAP ACME 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`

CAUSE	This behavior can occur if the LDAPACME$INIT logical name equates to a non-existent file.
TEMPORARY SOLUTION	To resolve the system-wide login failures as quickly as possible, enable only the VMS ACME agent by editing SYS$MANAGER:ACME$START.COM and commenting out the line that starts the OpenLDAP ACME agent. Restart the ACME server using the command **SET SERVER ACME/RESTART** and then use the command **SHOW SERVER ACME** to verify that the VMS ACME agent is active.
SOLUTION	Verify that the LDAPACME$INIT logical name equates to an existing OpenLDAP ACME agent 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 and LDAP ACME agents are active.

PROBLEM	Server-wide login failures. Only a Console user can log in. 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 OpenLDAP ACME agent is LDAP-STD (not LDAP).

SOLUTION	It is not necessary to modify the AGENT_LIST symbol to start the OpenLDAP ACME 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 and LDAP ACME agents are active.

PROBLEM	System-wide login failures. Only a Console user can log in. 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 does not exist.
SOLUTION	Correct or comment out the "mapping_file" directive in the OpenLDAP ACME 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 and LDAP ACME agents are active.

PROBLEM	After starting the ACME server, **`SHOW SERVER ACME`** does not display the OpenLDAP ACME agent (only the VMS ACME 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 OpenLDAP ACME 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 and LDAP ACME agents are both active.

PROBLEM	After the OpenVMS host is rebooted, external authentication no longer works.
CAUSE	Verify that the OpenLDAP 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`

5.5. OpenLDAP ACME Agent Operating Issues

If external authentication using the OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME agent. If a failure occurs while communicating with an LDAP server, the OpenLDAP ACME 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).
SOLUTION	If this is the first time the OpenLDAP ACME agent is being deployed, it is often beneficial to reconfigure the OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME agent configuration file is incorrect.
SOLUTION	Obtain the correct bind credentials and update the "bind_dn" and/or "bind_password" directive in the OpenLDAP ACME agent 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 and LDAP ACME agents 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 OpenLDAP ACME agent configuration file contains a comma or other extraneous characters.
SOLUTION	Remove the extraneous characters from the value of the "server" directive in the OpenLDAP ACME agent 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 and LDAP ACME agents 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:ffffffff(Can't contact LDAP server)
CAUSE	The "server" directive in the OpenLDAP ACME agent configuration file contains a list of servers that 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 OpenLDAP ACME agent 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 and LDAP ACME agents 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 OpenLDAP ACME agent to use an option for the "port_security" directive other than NONE. See the options for the "server" directive in *Appendix A, "Configuration Directives"*. Restart the ACME server using the command **`SET SERVER ACME/RESTART`** and then use the command **`SHOW SERVER ACME`** to verify the VMS and LDAP ACME agents 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:
	`$ MCR AUTHORIZE SHOW/PAGE username`
	If necessary, set the EXTAUTH flag on the user's OpenVMS account:
	`$ MCR 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 *Section 3, "Username Mapping"* for more information.

6. Set Password Issues

PROBLEM	The DCL command **`SET PASSWORD`** returns: `%ACME-F-CONTACTSYSMGR, requested operation has failed; contact the system manager`
CAUSE	The VSI TCP/IP Services for OpenVMS SSH Server is not configured to use **`LOGINOUT`** for password changes.

SOLUTION	On systems running VSI TCP/IP Services for OpenVMS, to allow externally authenticated users connecting via the TCP/IP Services SSH server 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 OpenLDAP ACME 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 OpenLDAP ACME agent configuration to use one of the TLS option values for the "port_security" directive, as documented in *Appendix A, "Configuration Directives"*.

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 OpenLDAP ACME agent configuration file is not set to "active-directory".
SOLUTION	Set the "password_type" directive in the OpenLDAP ACME agent configuration file to the value "active-directory" and restart the ACME server using the command: `$ SET SERVER ACME/RESTART`

A. Configuration Directives

The following table lists the OpenLDAP ACME 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 OpenLDAP ACME agent tries to connect to the first server in the list. If the target server is unreachable, the next server is attempted. This process 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 OpenLDAP ACME agent must be present on all directory servers. ● Set the "bind_timeout" directive appropriately to ensure that when the OpenLDAP ACME 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 the value to 636 to use the standard, secure LDAP port (LDAPS).
port_security	Specify the minimum level of encryption required for communications over the LDAP port specified by the "port" directive. If a stronger encryption method than the one specified can be negotiated with the server, the stronger method will be used. 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).

Directive	Configuration Details
	Recommended only for troubleshooting purposes. Values for LDAPS options (when using "port = 636"): **SSLTLS** - Negotiate TLS encryption with the server. **SSLTLS12** - Select only TLSV1.2 encryption. Values for StartTLS options (when using "port = 389"): **StartTLS** - Negotiate TLS encryption with the server. **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 OpenLDAP ACME 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 OpenLDAP ACME agent 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 OpenLDAP ACME 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 OpenLDAP ACME agent 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 it in quotes.
bind_timeout	Specify a timeout value in seconds, which defines the maximum number of seconds the OpenLDAP ACME 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	Configuration Details
	directive value, the user login session (i.e., a TELNET session) may expire before the OpenLDAP ACME 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 OpenLDAP ACME 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 keywords[1] 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).

Directive	Configuration Details
mapping	Specify the username mapping mechanism to use. There are three options (more information, see *Section 3, "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 that the OpenLDAP ACME 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 OpenLDAP ACME agent 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`*

Directive	Configuration Details
	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 login 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 OpenLDAP ACME agent needs that public key to verify the LDAP

Directive	Configuration Details

	server's certificate (except when `port_security = none`). Verifying the server's certificate ensures that the OpenLDAP ACME 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 command **`SET PASSWORD`** 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.

[1]Note that keywords are case-sensitive.

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 OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME 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 OpenLDAP ACME agent configuration files are required, one for each domain. The configuration file for the US domain is as follows:

```
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 is as follows:

```
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 OpenLDAP ACME 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
```