vms Software

ACME LDAP for OpenVMS Alpha and Integrity

February 2021

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 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. In this authentication method, users enter their LDAP entry name and password. An LDAP attribute is configured, which is used to match the entered username to the relevant OpenVMS credentials so that authentication can take place.

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

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.
- Users that upgrade from the old ACME LDAP agent and use the `ca_file` directive may find that the new LDAP ACME agent no longer accepts the LDAP server certificate as valid and that authentication fails.

  The ACME LDAP agent is an LDAP client and can be configured to use a CA certificate to verify the server certificate before establishing a SSL/TLS connection. However, the new OpenLDAP client used by ACME LDAP also includes additional check security step such that the Subject CN from the server certificate must match the server host name specified when connecting. If the names do not match the connection will fail to be established. The Subject CN can have only one name; however the server maybe connected to by the client using an IP address or alias as opposed to the actual host name.

  The limitation of the Subject CN allowing only one name can be overcome by using the x509v3 certificate extension Subject Alternative Name (SAN), which can contain a list of names to identify the server host, whereupon the LDAP client (in this case the ACME LDAP agent) will be check the list of names one by one until a match is found (or otherwise)

  Alternatively, it is noted that the `ca_file` directive is optional, and simply commenting out the `ca_file` directive and restarting ACME Server can resolve the problem; however this approach may be undesirable in some situations for security reasons.

3. Requirements

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

- VSI OpenVMS Version 8.4-2L1 or higher
- VSI TCP/IP Services for OpenVMS, HPE TCP/IP Services for OpenVMS, or MultiNet TCP/IP
- The SYS$ACM-enabled (ACMELOGIN) LOGINOUT.EXE and SETP0.EXE images must be installed
- VSI OpenLDAP 2.4.53 or later
- VSI SSL111 1.1-1g or later

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

In addition, the reader should be familiar with the configuration and use of Microsoft Active Directory, OpenLDAP Server, or other such LDAP server environment in the Windows or Linux environment.

4. Required reading

For more detailed information on installing and configuring ACMELDAP for VSI OpenVMS, see the document "*VSI OpenVMS ACME LDAP Installation and Configuration Guide*". This document is included in the ACME LDAP installation kit and can be found after installation in SYS$HELP:ACMELDAP2_STD_CONFIG_INSTALL.PDF

The reader should also review Section 5.1 of the document VMS842L1I_LDAP-V0400.RELEASE_NOTES, which describes new functionality added to ACME LDAP for the port_security directive that can be specified in the ACME LDAP configuration file. This change (introduced in VSI OpenVMS 8.4-2L1) expands TLS encryption options for ACMS LDAP to include targeted TLS versions, and allows TLS encryption for LDAPS connections (port 636) for enhanced security.

5. 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 can be installed by a suitably privileged user using the following command:

```
$ PRODUCT INSTALL ACMELDAP
```

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

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

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$IA21_842L1:[VMS$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

    While this kit does not require a system reboot, additional
    steps may be necessary to insure that active applications
    begin to use the newly supplied images. For most environments,
    this means restarting the ACME_SERVER if it is configured
    for external authentication.  If there are other applications
    which use LDAP directly, they may need to be restarted as well
    according to their own instructions.

    To restart the ACME_SERVER, use the command:

       $ SET SERVER ACME_SERVER /RESTART

    In a VMS cluster with a shared system disk, this command
    should also be performed on each node sharing the system disk
    with the installation system.

    Note that authentication requests currently in progress when
    the ACME_SERVER is restarted could fail, and any requests
    occurring while the server is restarting could be rejected.
    Therefore, care should be taken when choosing the time
    for such a restart.

    For additional information on setting up the LDAP persona
    extension and configuring the LDAP ACME agent, see the
    documentation of the LDAP ACME agent at
    SYS$HELP:ACMELDAP2_STD_CONFIG_INSTALL.TXT or
    SYS$HELP:ACMELDAP2_STD_CONFIG_INSTALL.PDF.
```

5.1. Post-installation steps

After the installation has successfully completed, follow the instructions provided in the document `SYS$HELP:ACMELDAP2_STD_CONFIG_INSTALL.PDF` to configure and start ACME LDAP.

In very general terms these steps can be summarized as follows:

- Install the SYS$ACM (ACMELOGIN) enabled login images
- Install the LDAP persona extension
- Configure the LDAP ACME agent
- Start the LDAP ACME agent
- Configure user accounts to use external authentication