HP OpenVMS ACME LDAP Installation and Configuration Guide



© Copyright 2010 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Table of Contents

Al	bout This Document Intended Audience Typographic Conventions HP Encourages Your Comments	9 9
1	Overview	11
	Installing and configuring ACME LDAP agent Prerequisites General setup Installing the ACMELOGIN and ACMELDAP_STD kits Setting up LDAP persona extension Configuring ACME LDAP agent Editing LDAP configuration file Starting ACME LDAP agent Specifying EXTAUTH and VMSAUTH flags on OpenVMS Examples of configuration files	13 13 15 15 15 19 19 21
	Global and local mapping User Scenario: Configuring global and local mapping User Scenario: Configuring a simple standalone Active directory server and	
		~ -
\mathbf{O}		· ') /
	penVMS ACME LDAP agent	
	Configuring Active directory	28
	Configuring Active directory Setting Active directory as the domain controller	28 28
	Configuring Active directory Setting Active directory as the domain controller Installing Active directory	28 28 32
	Configuring Active directory Setting Active directory as the domain controller	28 28 32 38
	Configuring Active directory Setting Active directory as the domain controller Installing Active directory Creating accounts on Active directory	28 28 32 38 41
	Configuring Active directory Setting Active directory as the domain controller Installing Active directory Creating accounts on Active directory Extracting ACME LDAP configuration parameter values Querying LDAP port Extracting base_dn, bind_dn, and login_attribute	28 32 38 41 41 41
	 Configuring Active directory Setting Active directory as the domain controller Installing Active directory Creating accounts on Active directory Extracting ACME LDAP configuration parameter values Querying LDAP port Extracting base_dn, bind_dn, and login_attribute Configuring ACME LDAP agent for non-secure port 	28 28 32 38 41 41 41 43
	 Configuring Active directory Setting Active directory as the domain controller Installing Active directory Creating accounts on Active directory Extracting ACME LDAP configuration parameter values Querying LDAP port Extracting base_dn, bind_dn, and login_attribute. Configuring ACME LDAP agent for non-secure port. Enabling ACME LDAP for secure ports 	28 32 32 41 41 41 43 46
	 Configuring Active directory Setting Active directory as the domain controller Installing Active directory Creating accounts on Active directory Extracting ACME LDAP configuration parameter values Querying LDAP port Extracting base_dn, bind_dn, and login_attribute Configuring ACME LDAP agent for non-secure port. Enabling ACME LDAP for secure ports Creating Active directory certificates 	28 32 38 41 41 41 43 46 46
	Configuring Active directory Setting Active directory as the domain controller Installing Active directory Creating accounts on Active directory Extracting ACME LDAP configuration parameter values Querying LDAP port Extracting base_dn, bind_dn, and login_attribute Configuring ACME LDAP agent for non-secure port. Enabling ACME LDAP for secure ports Creating Active directory certificates Configuring ACME LDAP for secure port.	28 32 38 41 41 41 43 46 51
	Configuring Active directory Setting Active directory as the domain controller Installing Active directory Creating accounts on Active directory Extracting ACME LDAP configuration parameter values Querying LDAP port Extracting base_dn, bind_dn, and login_attribute Configuring ACME LDAP agent for non-secure port. Enabling ACME LDAP for secure ports Creating Active directory certificates Configuring ACME LDAP for secure port. Providing Active directory certificates to ACME LDAP	28 28 32 38 41 41 41 43 46 46 51 51
	Configuring Active directory Setting Active directory as the domain controller Installing Active directory Creating accounts on Active directory Extracting ACME LDAP configuration parameter values Querying LDAP port Extracting base_dn, bind_dn, and login_attribute Configuring ACME LDAP agent for non-secure port. Enabling ACME LDAP for secure ports Creating Active directory certificates Configuring ACME LDAP for secure port.	28 28 32 31 41 41 41 43 46 46 51 51 52
	Configuring Active directory. Setting Active directory as the domain controller. Installing Active directory Creating accounts on Active directory. Extracting ACME LDAP configuration parameter values. Querying LDAP port. Extracting base_dn, bind_dn, and login_attribute. Configuring ACME LDAP agent for non-secure port. Enabling ACME LDAP for secure ports. Creating Active directory certificates. Configuring ACME LDAP for secure port. Providing Active directory certificates to ACME LDAP. Viewing the certificate on Active directory. Adding the certificate to OpenVMS.	28 32 32 38 41 41 43 46 51 51 52 60
	Configuring Active directory. Setting Active directory as the domain controller. Installing Active directory Creating accounts on Active directory Extracting ACME LDAP configuration parameter values. Querying LDAP port. Extracting base_dn, bind_dn, and login_attribute. Configuring ACME LDAP agent for non-secure port. Enabling ACME LDAP for secure ports. Creating Active directory certificates. Configuring ACME LDAP for secure port. Providing Active directory certificates to ACME LDAP. Viewing the certificate on Active directory. Adding the certificate to OpenVMS.	28 32 32 38 41 41 43 46 51 51 52 60
5	Configuring Active directory. Setting Active directory as the domain controller. Installing Active directory Creating accounts on Active directory. Extracting ACME LDAP configuration parameter values. Querying LDAP port. Extracting base_dn, bind_dn, and login_attribute. Configuring ACME LDAP agent for non-secure port. Enabling ACME LDAP for secure ports. Creating Active directory certificates. Configuring ACME LDAP for secure port. Providing Active directory certificates to ACME LDAP. Viewing the certificate on Active directory. Adding the certificate to OpenVMS.	28 28 32 32 41 41 41 43 46 51 51 52 60 61 65
5	Configuring Active directory Setting Active directory as the domain controller Installing Active directory Creating accounts on Active directory Extracting ACME LDAP configuration parameter values. Querying LDAP port Extracting base_dn, bind_dn, and login_attribute. Configuring ACME LDAP agent for non-secure port. Enabling ACME LDAP for secure ports Creating Active directory certificates. Configuring ACME LDAP for secure port Providing ACME LDAP for secure port Providing Active directory certificates to ACME LDAP. Viewing the certificate on Active directory Adding the certificate to OpenVMS Troubleshooting FAQ	28 32 32 38 41 41 43 46 51 51 52 60 61 65

7 References	
Index	71

List of Figures

3-1	One-to-One Mapping	23
	One-to-One Mapping Issue	
	Global Mapping	
	Local Mapping	
	ACME LDAP Process Flow Diagram	
	Sample LDF file	
	1	

List of Tables

1	Typographic Conventions	.9
	LDAP configuration attributes	
	Bitmask	

List of Examples

2-1	Red Hat or Fedora Directory Server configuration file	21
	Active Directory configuration file	

About This Document

This guide describes how to configure ACME LDAP agent and Directory server to enable external authentication for users. This guide also describes how to enable global and local mapping for external user logins.

Intended Audience

This document is intended for OpenVMS system administrators. For more information about security, see the HP OpenVMS Guide to System Security:

http://h71000.www7.hp.com/doc/

Typographic Conventions

Table 1 lists the typographic conventions used in the document.

Convention	Description			
	 A horizontal ellipsis in a figure or examples indicates the following possibilities: Additional optional arguments in a statement have been omitted. The preceding item or items can be repeated one or more times. Additional parameters, values, or other information can be entered. 			
	A vertical ellipsis indicates the omission of items from a code example or command format; the items are omitted because they are not important to the topic being described.			
()	In command format descriptions, parentheses indicate that you must enclose choices in parentheses if you specify more than one. In installation or upgrade examples, parentheses indicate the possible answers to a prompt, such as: Is this correct? (Y/N) [Y].			
[]	In command format descriptions, brackets indicate optional choices. You can choose one or more items or no items. Do not type the brackets on the command line. However, you must include the brackets in the syntax for OpenVMS directory specifications and for a substring specification in an assignment statement.			
{}	In command format descriptions, braces indicate required choices; you must choose at least one of the items listed. Do not type the braces on the command line.			
Example	This typeface indicates code examples, command examples, and interactive screen displays. In text, this type also identifies website addresses, OpenVMS command and pathnames, PC-based commands and folders, and certain elements of the C programming language.			
italic type	Italic type indicates important information, complete titles of manuals or variables. Variables include information that varies in system output (for example, Internal error number), in command lines (/PRODUCER=name), and in command parameters in text (where dd represents the predefined code for the device type).			
UPPERCASE TYPE	Uppercase indicates the name of a command, routine, file, file protection code, or the abbreviation of a system privilege.			
-	A hyphen at the end of a command format description, command line, or code line indicates that the command or statement continues on the following line.			
WARNING	A warning calls attention to important information that if not understood or followed will result in personal injury or nonrecoverable system problems.			
CAUTION	A caution calls attention to important information that if not understood or followed will result in data loss, data corruption, or damage to hardware or software.			

Convention	Description
IMPORTANT	This alert provides essential information to explain a concept or to complete a task.
NOTE	A note contains additional information to emphasize or supplement important points of the main text.

Table 1 Typographic Conventions (continued)

HP Encourages Your Comments

HP encourages your comments and suggestions on this document. Please send comments to: openvmsdoc@hp.com

1 Overview

Lightweight Directory Access Protocol (LDAP) is combined with the Authentication and Credentials Management Extension (ACME) authentication mechanism to provide a solution to customers to manage all accounts in a centralized directory.

The ACME LDAP agent provided with 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 so that the authentication can take place. The following sections provide information on how to install and configure the standard ACME LDAP agent.

Secure Socket Layer (SSL)/Transport Layer Security(TLS) LDAP communication is supported to prevent cleartext passwords from being exposed over the network. Dedicated SSL port and the startTLS operation over the standard port are supported.

2 Installing and configuring ACME LDAP agent

Prerequisites

- You must be running OpenVMS Alpha or Integrity Version 8.3 or later.
- You must install the SYS\$ACM-enabled LOGINOUT.EXE (<osversion>_ACMELOGIN, for example, V84_ACMELOGIN-V0101) kit.

The ACMELOGIN kit can be found in the SYS\$UPDATE:ACME_DEV_KITS.BCK save set. For more information, see the SYS\$HELP:ACME_DEV_README.TXT file.

General setup

You must first configure and populate your LDAP directory server with user entries.

The ACME LDAP agent is configured by performing the following steps.

- 1. "Installing the ACMELOGIN and ACMELDAP_STD kits" (page 13)
- 2. "Setting up LDAP persona extension" (page 15)
- 3. "Configuring ACME LDAP agent" (page 15)
- 4. "Starting ACME LDAP agent" (page 19)

Installing the ACMELOGIN and ACMELDAP_STD kits

NOTE: If you are using OpenVMS Version 8.4 and later, the files inside ACMELDAP_STD kit is already a part of the operating system. You do not have to install the ACMELDAP_STD kit separately.

To install the ACMELOGIN and ACMELDAP_STD kits, perform the following steps:

- 1. Restore the PCSI kits by executing the following command:
 - \$ BACKUP/VERIFY/LOG SYS\$UPDATE:ACME_DEV_KITS.BCK/SAVE -
 - _\$ [destination_directory]*.*

Check if the following files have been restored:

- HP-I64VMS-<os version>_ACMELOGIN-VXXXX--4.PCSI
 - or

DEC-AXPVMS-<os version>_ACMELOGIN-VXXXX--4.PCSI

Where <os version> is the version of the OpenVMS operating system version and "XXXX" is the version of ACMELOGIN kit. For example, V84_ACMELOGIN_V0106.

The ACMELOGIN kit contains the sys\$acm-enabled LOGINOUT.EXE and SETP0.EXE. For more information on the kit contents, see SYS\$HELP:ACME_DEV_README.TXT.

• HP-I64VMS-<os version>_ACMELDAP_STD-VXXXX--4.PCSI

or

DEC-AXPVMS-<os version>_ACMELDAP_STD-VXXXX--4.PCSI

This kit is not provided with OpenVMS Version 8.4 and later and the files are already part of the operating system.

• HP-I64VMS-<os version>_LOGIN-VXXXX--4.PCSI

or

DEC-AXPVMS-<os version>_LOGIN_STD-VXXXX--4.PCSI

The LOGIN kit contains the non-sys\$acm-enabled LOGINOUT.EXE and SETP0.EXE, which is shipped by default on your operating system. For more information, see SYS\$HELP:ACME_DEV_README.TXT.

2. Install sys\$acm-enabled LOGINOUT.EXE and SETP0.EXE using the following command:

\$ PRODUCT INSTALL/SAVE <OS Version>ACMELOGIN

3. Check the image identification using the following commands:

ANALYZE/IMAGE/INTER SYS\$COMMON:[SYSEXE]LOGINOUT.EXE

ANALYZE/IMAGE/INTER SYS\$COMMON:[SYSEXE]SETP0.EXE

You must get LOGIN98 as a part of the Image file identification: field.

It is recommended to login to the system using any user account to test after installing the ACMELOGIN kit.

- 4. Install ACMELDAP_STD kit on OpenVMS Version 8.3 or 8.3–1H1 using the following command:
 - \$ PRODUCT INSTALL/SAVE <OS Version>ACMELDAP_STD

When the ACME LDAP agent is installed, proceed to the next section, "Setting up LDAP persona extension" (page 15).

For more detailed steps on installation, see the SYS\$HELP:ACME_DEV_README.TXT.

Setting up LDAP persona extension

To set up the persona extension, do as follows:

1. Install the persona extension image using the following commands:

\$ MCR SYSMAN
SYSMAN> SYS_LOADABLE ADD LDAPACME LDAPACME\$EXT
SYSMAN> exit
\$ @SYS\$UPDATE:VMS\$SYSTEM IMAGES.COM

2. Reboot the system:

\$ @SYS\$SYSTEM:SHUTDOWN

During reboot, an error message appears if the persona extension image is not loaded. If the error message is not displayed, it means that the image is loaded as required.

After setting up the LDAP persona extension, you can proceed towards configuring your ACME LDAP agent, "Configuring ACME LDAP agent" (page 15).

Configuring ACME LDAP agent

Configuration of ACME LDAP agent involves the following:

- **1.** "Editing LDAP configuration file" (page 15)
- 2. "Starting ACME LDAP agent" (page 19)

The attribute used for usernames is specified by the *login_attribute* directive in your ACME LDAP INI configuration file. For more information about *login_attribute*, see Table 2-1 (page 16).

The ACME LDAP agent searches this attribute on directory server for matching usernames (entered at "Username" prompt during login). The search is done in the set of LDAP entries below the point in your directory tree specified by the *base_dn* directive.

The username (entered at "Username" prompt during login) is mapped to the username in the SYSUAF.DAT file. This mapping is one-to-one on OpenVMS Version 8.3 and 8.3–1H1. In one-to-one mapping, the username entered must be the same as the username in the SYSUAF.DAT file. On OpenVMS Version 8.4 and later, global and local mappings are also supported. For more information on global and local mapping, see "Global and local mapping" (page 23).

OpenVMS-specific information, such as privileges, identifiers, and so on are taken from SYSUAF.DAT file.

A user scenario on configuring ACME LDAP and sample login is provided in Chapter 4 (page 27).

Editing LDAP configuration file

To edit the ACME LDAP INI file, perform the following steps:

1. Make a copy of SYS\$STARTUP:LDAPACME\$CONFIG-STD.INI_TEMPLATE and rename it to any file name of your choice. For example,SYS\$STARTUP:LDAPACME\$CONFIG-STD.INI using the following command:

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

2. Edit SYS\$STARTUP:LDAPACME\$CONFIG-STD.INI to specify the directives that correspond to your requirements.

For description on the directives present in the LDAPACME\$CONFIG-STD.INI file, see Table 2-1.

Column Head	Column Head		
server	This is a mandatory directive. The IP address (or DNS host name) for your directory server.		
port	This is a mandatory directive.		
For	The port that your directory server is listening for. Defaults to the standard port 389 (or 636 for SSL/TLS).		
login_attribute	This is a mandatory directive.		
	The LDAP schema attribute that contains the username for login purposes. This is often specified as 'uid', but may be different in your configuration. For Active Directory, this is usually <i>samaccountname</i> .		
password_type	Select one of the following:		
	• standard (default)		
	active-directory		
	If this directive is not specified, the command \$ SET PASSWORD will not work.		
	If using active directory server, \$ SET PASSWORD will not work if <i>password_type</i> is not set to "active-directory"		
password_update	Applies only when password_type = standard is set. Some directory servers require the old password to be supplied when changing userPassword attribute; others do not.		
	Select one of the following:		
	 replace (default) 		
	 remove-and-add 		
base_dn	The LDAP users are stored in a tree structure in your directory server.		
	The base_dn directive is the distinguished name of a tree element on the directory server. All the user entries must be present under this tree element as sub-tree elements. The ACME LDAP will search for matching entries within this sub-tree based on the attribute specified by <i>login_attribute</i> . (See the <i>scope</i> directive.)		
scope	Controls the depth of the search beneath the <i>base_dn</i> . Valid keywords are:		
	 sub: searches the base entry and all entries at all levels below the base entry 		
	 one: searches all entries at one level below the base entry 		
	• base: searches only the base entry		
	If you are not sure about the keyword to be used, you can use "sub" as the keyword.		
filter	This directive is optional.		
	Search filter for limiting the objects that will be searched for users in the LDAP tree. Defaults to objectclass=*.		

Table 2-1 LDAP configuration attributes

Column Head	Column Head
bind_dn	The distinguished name (DN) of a user account (directory entry) that is granted "search" permission through the directory sub-tree specified by <i>base_dn</i> .
	The <i>bind_dn</i> along with the <i>bind_password</i> is used to bind to your directory servers, before searching for users on the directory servers.
	Some directory servers (such as Active directory) will not allow the ACME LDAP agent to bind to them by default without <i>bind_dn</i> and <i>bind_password</i> . The <i>bind_dn</i> and <i>bind_password</i> must be specified in such cases.
	Some directory servers will support anonymous binds to happen and you do not have to provide the <i>bind_dn</i> and <i>bind_password</i> directives for working with these directory servers.
bind_password	The password for the directory DN specified by <i>bind_dn</i> .
port_security	This is a mandatory directive.
	Specifies the method used to encrypt communications over the LDAP port. Possible values are "starttls" (the default), "ssl" (dedicated SSL port) or "none" (not recommended).
ca_file	This directive is optional.
	Specifies the file path of a PEM-format file containing the public key of the certificate authority that signed your directory server's public key.
	The ACME LDAP agent checks this certificate file and whether it is connecting to the right directory server, when the <i>port_security</i> is set to "ssl" or "starttls".
	If this attribute is not used, the LDAP server's certificate is NOT verified.
mapping	Specifies whether the mapping is global or local. You are provided two options for this directive:ServerLocal
	For example: mapping=server indicates that global mapping is enabled for the user. mapping=local indicates the local mapping is enabled for the user. If "mapping" directive is not used, mapping will be one-to-one.
mapping_attribute	This directive is applicable only for global mapping. Set this to the attribute on directory server that is used for user mapping.
	For example:
	<i>mapping_attribute</i> can be referenced to the description attribute for the user in the directory server.
	mapping_attribute=description
	You can also use any newly created attribute on the directory server for mapping. The attribute should be an IA5 multi-valued string.

Table 2-1 LDAP configuration attributes (continued)

Column Head	Column Head		
mapping_target	This directive is applicable only for global mapping. The <i>mapping_target</i> is searched in the value of directory server's <i>mapping_attribute</i> field. For example:		
	Let the LDAP INI file have:		
	mapping_attribute=description		
	mapping_target= VMSUsers.hp.com		
	Let the description (field in Directory Server) be populated with:		
	VMSUsers.hp.com/jdoe		
	The ACME LDAP agent then searches in <i>VMSUsers.hp.com/jdoe</i> , for a prefix of <i>VMSUsers.hp.com/</i> (with a forward slash (/) along with the <i>mapping_target</i>). The rest of the value that is, "jdoe" is considered as the user name present in SYSUAF.DAT file. If a multi-valued string attribute is used, the "VMSUsers.hp.com/jdoe" must be one of the array elements of the multi-valued string.		
mapping_file	This directive is applicable only for local mapping.		
	Set this to the complete path of the text database file to be searched for mapping users.		
	A template file is available in SYS\$STARIUP:LDAP_LOCALUSER_DATABASE.TXT_TEMPLATE.		
	This file includes the LDAP username and VMS username separated by a comma, where LDAP username is the name of the user in the domain (entered at the "username" prompt during login).		
	For information on how to populate and load the contents of the database file, see SYS\$STARIUP:LDAP_LOCALUSER_DATABASE.TXT_TEMPLATE		

Table 2-1 LDAP configuration attributes (continued)

3. Edit SYS\$MANAGER : ACME\$START . COM and define the following logical names: The LDAPACME\$INIT logical must contain the path name to the initialization for the ACME LDAP Agent Server.

\$ DEFINE/SYSTEM/EXECUTIVE LDAPACME\$INIT SYS\$STARTUP:LDAPACME\$CONFIG-STD.INI

4. Remove the comment from the following line from SYS\$MANAGER:ACME\$START.COM: \$! @SYS\$STARTUP:LDAPACME\$STARTUP-STD ! LDAP



IMPORTANT: The LDAPACME\$INIT logical must be defined prior to starting the ACME LDAP agent. HP recommends that you place this logical name in SYS\$MANAGER: ACME\$START. COM before the SYS\$STARTUP: LDAPACME\$STARTUP-STD procedure executes.

5. Ensure that the LDAP configuration file and the LDAP local database mapping file are accessible for privileged users only. You can set the security of these files appropriately based on your security requirements. For example, the following command sets the accessibility of LDAPACME\$CONFIG-STD.INI and LDAP_LOCALUSER_DATABASE.TXT files only for system user:

```
SET SECURITY / PROTECTION = (system:"RWED", OWNER:"", GROUP:"",
WORLD:"") SYS$COMMON:[SYS$STARTUP]LDAPACME$CONFIG-STD.INI
SET SECURITY / PROTECTION = (system:"RWED", OWNER:"", GROUP:"",
WORLD:"") SYS$COMMON:[SYS$STARTUP]LDAP LOCALUSER DATABASE.TXT
```

Starting ACME LDAP agent

Restart the ACME_SERVER process:

- \$ SET SERVER ACME/EXIT/WAIT
- \$ SET SERVER ACME/START=AUTO



NOTE: You can place this command in your SYS\$MANAGER:SYSTARTUP_VMS.COM procedure to have the ACME LDAP agent started automatically at boot.

Specifying EXTAUTH and VMSAUTH flags on OpenVMS

For any user to be externally authenticated (via LDAP), the **ExtAuth** flag has to be set for the user account in SYSUAF.DAT. When the **ExtAuth** flag is specified for a user account, the user is validated only externally using external authenticator (LDAP). If you want this user to be authenticated locally as well against SYSUAF.DAT file, set **VMSAuth** flag for the user account in SYSUAF.DAT file and use "/local" qualifier during login as described in the following section.

To set ExtAuth flag to the user, enter the following:

\$ SET DEFAULT SYS\$SYSTEM

\$ MCR AUTHORIZE MODIFY <username> /FLAGS=(EXTAUTH,VMSAUTH)MC AUTHORIZE

A sample user profile is shown as follows:

```
$ SET DEF SYS$SYSTEM
$ MC AUTHORIZE
UAF> modify jdoe/flags=(EXTAUTH,VMSAUTH)
%UAF-I-MDFYMSG, user record(s) updated
UAF> sh jdoe
Username: JDOE
                                                          Owner:
                                                                    [201,2011] ([JDOE])
Account: TEST
                                                          UIC:
            DCL
                                                         Tables: DCLTABLES
CLI:
Default: SYS$SYSDEVICE: [JDOE]
LGICMD:
Flags: ExtAuth VMSAuth
Primary days: Mon Tue Wed Thu Fri
Secondary days:
                                                Sat Sun
No access restrictions
No access restrictionsExpiration:(none)Pwdminimum: 6Login Fails: 1Pwdlifetime:90 00:00Pwdchange:(pre-expired)Last Login:(none)(interactive),(none)Maxjobs:0Fillm:128Bytlm:128000Maxacctjobs:0Shrfillm:0Maxdetach:0BIOlm:150JTquota:4096
```

Prclm:	8	DIOlm:	150	WSdef:	4096	
Prio:	4	ASTlm:	300	WSquo:	8192	
Queprio:	4	TOElm:	100	WSextent:	16384	
CPU:	(none)	Englm:	4000	Pgflquo:	256000	
Authorized Privileges:						
NETMBX	TMPM	ВΧ				
Default Privileges:						
NETMBX	TMPM	BX				
UAF>						
T (1)						

If your directory server is configured and your SYSUAF account is mapped with the user name on the directory server, you can now login to the system using ACME LDAP as the authentication agent as shown in the following example.

The password for user "jdoe" is validated against the password from directory server. Note that if the password in directory server is different from the password in SYSUAF.DAT file, then the password on SYSUAF.DAT file will be synchronized to the password on directory server. You can disable the password synchronization for a specific user or for all the users on the system. For more information on disabling the password synchronization, see the sections "Enabling External Authentication" and "Authentication and Credentials Management Extensions (ACME) Subsystem" in *HP OpenVMS Guide to System Security*.

```
$ telnet 127.0.0.1
%TELNET-I-TRYING, Trying ... 127.0.0.1
%TELNET-I-SESSION, Session 01, host 127.0.0.1, port 23
-TELNET-I-ESCAPE, Escape character is ^]
Welcome to HP OpenVMS Industry Standard 64 Operating System, Version V8.3-1H1
Username: jdoe
Password:
    HP OpenVMS Industry Standard 64 Operating System, Version V8.3-1H1
    **** Logon authenticated by LDAP ****
    OpenVMS password has been synchronized with external password
```

In the following example, the user "jdoe" is validated against the SYSUAF.DAT file. Note that the user will not be mapped when the "/local" qualifier is provided during login. The username "jdoe" must be present in SYSUAF.DAT file.

```
$ telnet 127.0.0.1
%TELNET-I-TRYING, Trying ... 127.0.0.1
%TELNET-I-SESSION, Session 01, host 127.0.0.1, port 23
-TELNET-I-ESCAPE, Escape character is ^]
Welcome to HP OpenVMS Industry Standard 64 Operating System, Version V8.3-1H1
Username: jdoe/local
Password:
    HP OpenVMS Industry Standard 64 Operating System, Version V8.3-1H1
    Last interactive login on Tuesday, 1-DEC-2009 01:34:50.26
***** Logon authenticated by LDAP ****
```

For a user scenario on configuring a standalone Active directory server, see "User Scenario: Configuring a simple standalone Active directory server and OpenVMS ACME LDAP agent" (page 27).

Examples of configuration files

Example 2-1 Red Hat or Fedora Directory Server configuration file

A sample configuration file using the Red Hat or Fedora directory server

```
server = roux.zko.hp.com
port = 636
port_security = ssl
bind_dn = uid=acme-admin,ou=people,dc=acme,dc=mycompany,dc=com
bind_password = swordfish
base_dn = ou=people,dc=acme,dc=mycompany,dc=com
login_attribute = uid
scope = sub
ca_file = sys$manager:acme_ca.crt
```

Example 2-2 Active Directory configuration file

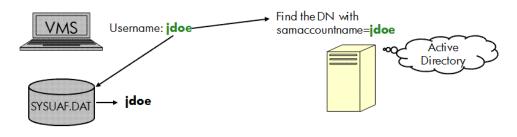
```
server = acme.mycompany.com
port = 636
port security = ssl
password type = active-directory
bind dn = cn=acme-admin, cn=users, dc=acme, dc=mycompany, dc=com
bind password = swordfish
base dn = cn=users, dc=acme, dc=mycompany, dc=com
login attribute = samaccountname
scope = sub
ca file = sys$manager:acme ca.crt
server = cssn-ddrs.testdomain.hp.com
port = 389
bind dn = CN=query account, CN=Users, DC=testdomain, DC=hp, DC=com
bind_password = welcome@123
base dn = DC=testdomain,DC=hp,DC=com
scope = sub
port security = none
password_type = active-directory
server = cssn-ddrs.testdomain.hp.com
port = 389
bind_dn = CN=query_account,CN=Users,DC=testdomain,DC=hp,DC=com
bind_password = welcome@123
base_dn = DC=testdomain,DC=hp,DC=com
scope = sub
port_security = starttls
password_type = active-directory
ca_file = sys$manager:cssn-ddrs.cer
```

3 Global and local mapping

The authentication method for OpenVMS version ACME LDAP agent on Version 8.3 and Version 8.3-1H1 supports only one-to-one mapping for users. In one-to-one mapping, the user logging in to an OpenVMS system from an LDAP server must have a matching username in the SYSUAF.DAT file. Hence, a user must login with the exact username entry stored in the SYSUAF.DAT file. To overcome this issue of one-to-one mapping, the ACME LDAP agent uses the concept of global and local mapping.

The following diagrams explain the issues of one-to-one mapping and how global or local mapping solves the issue. In this section, "jdoe" is used as a sample account in SYSUAF.DAT file and "John Doe" as the sample domain user name.

Figure 3-1 One-to-One Mapping





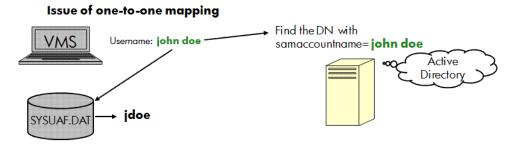


Figure 3-2 illustrates that in one-to-one mapping, the system is not able to match the username "John Doe" with the username in the SYSUAF.DAT, where it is stored as "jdoe".

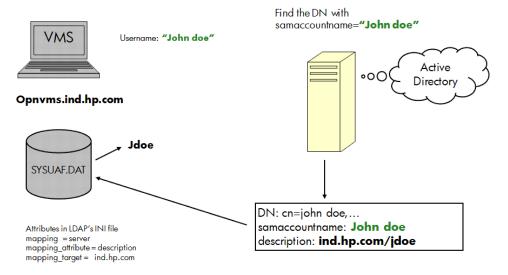
Using the global and local mapping:

- Users can enter the user name that is common across the domain, at the user name prompt of OpenVMS.
- User name is mapped to a different name in the SYSUAF.DAT file during login.
- OpenVMS session after login uses the name and the privileges in the SYSUAF.DAT for all purposes.
- SET PASSWORD command has the capability to understand that this is a mapped user and synchronize any password change to the directory server.

In global mapping, the user's login name is mapped based on some attributes stored in the directory server. In local mapping, a text database file is used to store the LDAP user name (name of the user in the domain) and the name in SYSUAF.DAT in the .CSV format.

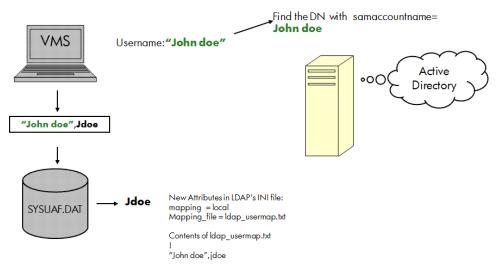
Figure 3-3 illustrates global mapping and local mapping:

Figure 3-3 Global Mapping



In Figure 3-4, the user name "John Doe" is mapped with "jdoe" in the SYSUAF. DAT and "John Doe" in the Active Directory. Three new directives, namely *mapping, mapping_attribute*, and *mapping_target* are added to configure global mapping. For more information on the global mapping directives, see Table 2-1 (page 16).

Figure 3-4 Local Mapping



In this figure, the username "John Doe" is mapped with "jdoe" and "John Doe" in the local database file.

Two new directives, namely *mapping* and *mapping_file* are added to configure local mapping. For more information local mapping directives, see Table 2-1 (page 16).

User Scenario: Configuring global and local mapping

Global mapping configuration

In the SYSUAF.DAT file, the username is stored as "jdoe" and "jhardy". To enable global mapping, perform the following steps:

1. Update the attributes in SYS\$STARTUP:LDAPACME\$CONFIG-STD.INI file along with the other mandatory attributes:

```
mapping = server
mapping_attribute = description
mapping_target = VMSusers.hp.com
```

For example: Two users, John Doe and Joe Hardy have the following attributes specified in the user profile of the Active directory:

```
DN: cn=john doe,...
samaccountname: John Doe
description: VMSUsers.hp.com/jdoe
DN: cn=jhardy,...
samaccountname: jhardy
description: VMSUsers.hp.com/jhardy
```

2. Restart the ACME server:

-Z

- \$ SET SERVER ACME/EXIT/WAIT
- \$ SET SERVER ACME/START=AUTO
- 3. Login to the host system using the login "John Doe" for the user "John Doe"

NOTE: Note that at the user name prompt, you must give this name in quotes, as the name has a space (special character) in-between.

4. Login to the host system using the login jhardy for the other user.

Local mapping configuration

To enable local mapping, perform the following steps:

- 1. Make a copy of the SYS\$STARTUP:LDAP_LOCALUSER_DATABASE.TXT _TEMPLATE and rename it to a filename of your choice. For example, SYS\$STARTUP:LDAP_LOCALUSER_DATABASE.TXT on the OpenVMS system.
- 2. Update the SYS\$STARTUP:LDAP_LOCALUSER_DATABASE.TXT with the LDAP username and VMS username separated by a comma. If the LDAP username contains spaces, commas, or exclamation, provide it within quotes.

```
"John Doe",jdoe
jhardy,jhardy
```

For example, two users John Doe and Joe Hardy have the following attributes specified in the user profile of the Active directory:

```
DN: cn=john doe,...
samaccountname: John Doe
DN: cn=jhardy,...
samaccountname: jhardy
```

3. Update the directives in the SYS\$STARTUP:LDAPACME\$CONFIG-STD.INI file along with the other mandatory attributes:

```
mapping = local
mapping_file = SYS$COMMON:[SYS$STARTUP]LDAP_LOCALUSER_DATABASE.TXT
```

- 4. Load the new database file by performing the following:
 - Restart the ACME server: a.

\$ SET SERVER ACME/EXIT/WAIT

\$ SET SERVER ACME/START=AUTO

OR:

- b. Using LDAP_LOAD_LOCALUSER_DATABASE.EXE:

 - \$ load_localuser_db:=="\$SYS\$SYSTEM:LDAP_LOAD_LOCALUSER_DATABASE.EXE" \$ load_localuser_db SYS\$COMMON:[SYS\$STARTUP]LDAP_LOCALUSER_DATABASE.TXT
- Login to the host system using the login "John Doe" and jhardy. 5.

4 User Scenario: Configuring a simple standalone Active directory server and OpenVMS ACME LDAP agent

This chapter provides a user scenario on how to configure an Active directory server with an OpenVMS ACME LDAP agent. This user scenario guides the user through the various steps of configuring a sample standalone Active directory server, creating an account, and creating certificates. It also provides the steps to extract the relevant values from the Active directory server to populate the ACME LDAP configuration file.

IMPORTANT: This chapter aims at providing the end-user with a detailed overview of configuring a sample directory server (here, Active directory is chosen as the sample directory server) and an OpenVMS ACME LDAP agent.

Note that in most of the system administration setup, the sub-procedures for certain sections such as "Configuring Active directory" (page 28), "Creating Active directory certificates" (page 46) may have been already completed. Therefore, you may not have to perform these steps again.

Sample account names such as, "query_account" have been used throughout this chapter and must not be considered as a standard proxy account name. You can create any account of your choice.

Similarly, other accounts and system names used in this chapter are also examples and you can use any account name or system of your choice.

Figure 4-1 illustrates how an ACME LDAP agent configured with an Active directory server works.

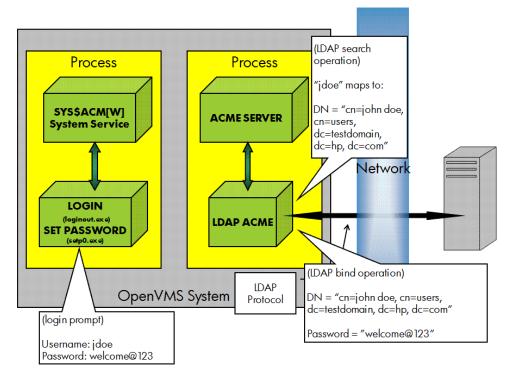


Figure 4-1 ACME LDAP Process Flow Diagram

Figure 4-1 illustrates how a VMS user logs in to a VMS system using LDAP authentication. In this figure, two systems are involved, which communicate over TCP/IP.

The gray box on the left is the VMS system with enhanced versions of LOGINOUT.EXE and SETP0.EXE installed and the ACME LDAP agent running within the ACME_SERVER process.

On the right, is the Active directory server running Windows Server 2003. Active Directory is also an LDAP server.

The ACME LDAP agent communicates with Active directory using LDAP protocol over a TCP session, which can be protected by SSL (required for Active directory LDAP password changes). The LDAP "search" and "bind" operations are standard LDAP operations accessed through standard C bindings. These are operations that work with any standard LDAP server and are used pervasively in many applications to provide LDAP-based authentication services.

Enabling your Active Directory to use ACME LDAP agent for authentication on OpenVMS system involves the following steps:

- 1. "Configuring Active directory" (page 28)
 - **a.** "Setting Active directory as the domain controller" (page 28)
 - **b.** "Installing Active directory " (page 32)
- 2. "Creating accounts on Active directory" (page 38).
- 3. "Extracting ACME LDAP configuration parameter values" (page 41)
- **4.** "Creating Active directory certificates" (page 46)
- 5. "Viewing the certificate on Active directory" (page 52)
- 6. "Adding the certificate to OpenVMS" (page 60)

Configuring Active directory

Configuring active directory involves the following:

- 1. "Setting Active directory as the domain controller" (page 28)
- 2. "Installing Active directory " (page 32)
- **3.** "Creating accounts on Active directory" (page 38)

Setting Active directory as the domain controller

The following procedure describes how to set up Active directory as a standalone domain controller on a Windows 2003 server.



NOTE: In a corporate network, the Active directory might not be standalone and usually the Active directory may have been already set up.

1. Go to Start > All Programs > Manage Your Server to open the Manage Your Server window.

Manage Your Server	Search Help and Suppo	rt Center
Managing Your Server Roles Use the tools and information found here to add or remove roles and perform your daily administrative tasks. Your server has been configured with the following roles:	 Add or remove a role Read about server roles Read about remote administration 	<u>T</u> ools and Updates Administrative Tools More Tools Windows Update Computer and Domain Name Information Internet Explorer Enhanced Security Configuration
File Server File servers provide and manage access to files. Application Server	 Manage this file server Add shared folders Review the next steps for this role 	Sge Also Help and Support Microsoft TechNet Deployment and Resource Kits List of Common Administrative Tasks
Application servers provide the core technologies required to build, deploy and operate XML Web Services, Web applications, and distributed applications. Application server technologies include ASP.NET, COM+, and Internet Information Services (IIS).	 Manage this application server Read about application servers Read about Web Interface for Remote Administration of Web servers Review the next steps for this role. 	Windows Server Communities What's New Strategic Technology Protection Program

2. Select the **Add or remove a role** option in the **Manage Your Server** window. The **Configure Your Server Wizard** dialog box is displayed.

Configure Your Server Wizard	×
Preliminary Steps You can ensure that you successfully configure your server by completing the following steps before continuing.	No.
Before continuing, verify that the following steps have been completed.	
 Install all modems and network cards. 	
 Attach all necessary cables. 	
 If you plan to use this server for Internet connectivity, connect to the Internet now. 	
 Turn on all peripherals, such as printers and external drives. 	
 Have your Windows Server 2003 Setup CD available, or know your network installation path. 	
When you click Next, the wizard will search for network connections.	
< <u>B</u> ack Cancel H	Help

3. Click **Next**. Wait while the wizard detects your network settings. The **Server Role** dialog box is displayed.

Configure Yo	ur Server Wizard
	while the wizard detects your network settings. This may take a minute ach network connection on this server.
Detecting se	tings for Local Area Connection

4. Select the **Domain Controller (Active Directory)** server role to set Active Directory as the domain controller and click **Next** to display the **Summary of Selections** dialog box.

You can set up this server to perform one role to this server, you can run this wizard Select a role. If the role has not been adde	again. ed, you can add it. 1	If it has already been added, you can
remove it. If the role you want to add or re Server Role File server Application server (IIS, ASP.NET) Mail server (POP3, SMTP) Terminal server Remote access / VPN server Domain Controller (Active Directory) DNS server DHCP server Streaming media server WINS server	emove is not listed, No No No No No No No No No No No No	open Add or Remove Programs. Domain Controller (Active Directory) Domain controllers store directory data and manage user logon processes and directory searches. <u>Read about domain controllers</u>
	1	View the <u>Configure Your Server log</u> .

5. Click **Next** to start installing the Active Directory server as the domain controller. You will get the Active Directory Installation Wizard.

igure Your Server Wizard ummary of Selections	
View and confirm the options you have selected.	
Summary:	
Run the Active Directory Installation Wizard to set up this server as a doma	ain controller
	L . 4
To change your selections, click Back. To continue setting up this role, click N	lext.
< <u>B</u> ack	Cancel Help

Installing Active directory

The **Active Directory Installation Wizard** guides you through a series of steps to install Active Directory. The following procedure illustrates the same:

1. Click Next in the Welcome to the Active Directory Installation Wizard dialog box to display the Operating System Compatibility dialog box. Click Next to get the Domain Controller Type dialog box.

Active Directory Installation	n Wizard	×
	Welcome to the Active Directory Installation Wizard This wizard helps you install Active Directory services on this server, making the server a domain controller.	
	If this is the first time you have installed Active Directory, it is recommended that you first read the overview in <u>Active</u> <u>Directory Help</u> . To continue, click Next.	
	< Back Next > Cance	

2. Select the required option in the **Domain Controller Type** dialog box based on whether you want to create a new domain or an additional domain. Note that if you select **Additional domain controller for an existing domain**, all local accounts and cryptographic keys will be deleted. The caution is provided in the wizard dialog box. In this example, the option **Domain controller for a new domain** is selected.

Click **Next** to display the **Create New Domain** dialog box.

Active Directory Installation Wizard	×
Domain Controller Type Specify the role you want this server to have.	A.
Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?	
Domain controller for a new domain	
Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.	
Additional domain controller for an existing domain	
Proceeding with this option will delete all local accounts on this server.	
All cryptographic keys will be deleted and should be exported before continuing.	
All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.	
< <u>B</u> ack <u>N</u> ext > Cance	

3. Select the required option in the **Create New Domain** dialog box and click **Next**. In this example, the option **Domain in a new forest** is selected.

	e New Domain elect which type of domain to create.
Cre	eate a new:
•	Domain in a new forest
	Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
C	Child domain in an existing domain tree
	If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
С	Domain tree in an existing forest
	If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
	< Back Next > Cancel

4. Enter the DNS name in the **Full DNS name for new domain:** field and click **Next** to display the **NetBIOS Domain Name** dialog box.

Active Directory Installation Wizard	×
New Domain Name Specify a name for the new domain.	A
Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).	
Eull DNS name for new domain:	
testdomain.hp.com	
< Back Kext>	Cancel

5. Enter the **Domain NetBIOS name:** or click **Next** if you do not want to change the displayed name. Click **Next** to display the **Database and Log Folders** dialog box.

Directory Installation Wiz	aru	
etBIOS Domain Name Specify a NetBIOS name for t	he new domain.	
	earlier versions of Windows wil the name shown, or type a new	
Domain NetBIOS name:	TESTDOMAIN	
	< <u>B</u> ack	<u>N</u> ext> Ca

6. Browse and select the **Database folder** and **Log folder** or retain the default folder names and click **Next**.

Active Directory Installation Wizard	×
Database and Log Folders Specify the folders to contain the Active Directory database and lo	ng files.
For best performance and recoverability, store the database and th hard disks.	ne log on separate
Where do you want to store the Active Directory database?	
Database folder:	
C:\WINDOWS\NTDS	B <u>r</u> owse
Where do you want to store the Active Directory log? Log folder:	
C:\WINDOWS\NTDS	Browse
< <u>B</u> ack <u>N</u>	lext > Cancel

7. If DNS is not installed, the DNS registration diagnostics will fail and an option is provided to configure the DNS. Use the appropriate option and click **Next**.

NS Registration Diagnostics Verify DNS support, or install DNS on this computer.	S.
Diagnostic Failed	•
The registration diagnostic has been run 1 time.	
Warning: Domain Controller functions like joining a domain, logging onto a domain, and Active Directory replication will not be available until the DNS infrastructure for Active Directory is correctly configured.	
None of the DNS servers used by this computer responded within the timeout interval.	
For more information, including steps to correct this problem, see Help.	-
C I have corrected the problem. Perform the DNS diagnostic test again.	
Install and configure the DNS server on this computer, and set this computer to this DNS server as its preferred DNS server.	use
I will correct the problem later by configuring DNS manually. (Advanced)	
< Back Next> 0	Cance
	 Verify DNS support, or install DNS on this computer. Diagnostic Failed The registration diagnostic has been run 1 time. Warning: Domain Controller functions like joining a domain, logging onto a domain, and Active Directory replication will not be available until the DNS infrastructure for Active Directory is correctly configured. None of the DNS servers used by this computer responded within the timeout interval. For more information, including steps to correct this problem, see Help. I have corrected the problem. Perform the DNS diagnostic test again. Install and configure the DNS server on this computer, and set this computer to this DNS server as its preferred DNS server. I will correct the problem later by configuring DNS manually. (Advanced)

8. Select the required option and click **Next** to display the **Directory Services Restore Mode Administrator Password** dialog box.

Active Directory Installation Wizard	×
Permissions Select default permissions for user and group objects.	
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.	
Permissions compatible with pre-Windows 2000 server operating systems Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are	
members of pre-Windows 2000 domains.	
 Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems 	
Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.	
< <u>B</u> ack Next > Cance	

9. Enter the password for the administrator account and confirm the same in the respective fields and click **Next** to display the **Summary** dialog box.

This password is used when y Mode.	you start the computer in Directory Services Restore
	rd you want to assign to the Administrator account used Directory Services Restore Mode.
	or account is different from the domain Administrator he accounts might be different, so be sure to remember
Restore Mode Password:	•••••
Confirm password:	••••••
For more information about Di	rectory Services Restore Mode, see <u>Active Directory Help</u> .
	N
	<back next=""> Can</back>

10. Click **Next** or **Finish** as required, in the next series of wizards after **Summary** dialog box to complete the Active directory installation.

Active Directory Installation Wizard	×
Summary Review and confirm the options you selected.	S.
You chose to:	
Configure this server as the first domain controller in a new forest of domain trees.	<u> </u>
The new domain name is testdomain.hp.com. This is also the name of the new forest.	
The NetBIOS name of the domain is TESTDOMAIN	
Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL	
The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.	•
To change an option, click Back. To begin the operation, click Next.	
< <u>B</u> ack Next>	Cancel

11. **Restart** the system for the Active directory configuration to take effect.

Creating accounts on Active directory

Create two accounts on the directory server, one a binding account, for example, "query_account" and the second, a test user account, for example, , "jdoe" on the directory server. The "query_account" will be used by the ACME LDAP to connect to the Active directory server. The following sections provide information on how to get the distinguished name of the "query_account" and use in the ACME LDAP configuration file. You can use any account name of your choice here. "query_account" is an example. The account "jdoe" is a sample user account.

To create the accounts, perform the following steps:

1. Select the Manage users and computers in Active Directory option in the Domain Controller (Active Directory) panel. The Active Directory Users and Computers window is displayed.

Manage Your Server	Search Help and Suppo	rt Center
File servers provide and manage access to files.	 Manage this file server Add shared folders Review the next steps for this role 	See Also Help and Support Microsoft TechNet Deployment and Resource Kits List of Common Administrative Tasks
Application servers provide the core technologies required to build, deploy and operate XML Web Services, Web applications, and distributed applications. Application server technologies include ASP.NET, COM+, and Internet Information Services (IIS).	 Manage this application server Read about application servers Read about Web Interface for Remote Administration of Web servers Review the next steps for this role 	Windows Server Communities What's New Strategic Technology Protectic Program
Domain Controller (Active Directory) Domain controllers use Active Directory to manage network resources such as users, computers, and applications.	 Manage users and jonguiters in Active jorguiters in Active jorguiters of the second sec	
DNS Server		
DNS (Domain Name System) servers translate domain and	Managa this DNIS corver	

2. Select testdomain.hp.com under **Active Directory Users and Computers** tree to display the subtree **Users**.

Right-click and select **New > User** from the pop-up menu in the **Active Directory Users and Computers** window. The **New Object-User** dialog box is displayed.

4 Active Directory Users and Comp	uters				_ 6 >
Sile Action Yew Window H					<u>_18</u>]>
⇔ → 🗈 📧 🃾 🗗 🖓 🖳		is			
Active Directory Users and Computer					
Saved Queries Saved Queries Saved Queries	Name Administrator	Type User	Description J Bulk-in account for administering the computer/domain		
🖲 🧰 Bultin	Cert Publishers	Security Group - Domei			
Computers Domain Controllers	DonsAdmins	Security Group - Domai	DNS Administrators Group		
GoreignSecurityPrincipals	DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).		
Users	Domain Admins	Security Group - Global Security Group - Global	Designated administrators of the domain All workstations and servers joined to the domain		
	Domain Controlers	Security Group - Global	All domain controllers in the domain		
	Domain Guests	Security Group - Global	All domain guests		
	Domain Users	Security Group - Global	All domain users Designated administrators of the enterprise		
	Contempose Admins	Security Group - Global Security Group - Global	Designated administrators of the enterprise. Members in this group can modify group policy for the domain		
	Group Policy Creator Owners	User	Built-in account for guest access to the computer/domain		
	HelpServicesGroup	Security Group - Domai			
	RAS and IAS Servers Schema Admins	Security Group - Domai Security Group - Global	Servers in this group can access remote access properties of users Designated administrators of the schema		
	SUPPORT 38894540	User	This is a vendor's account for the Help and Support Service		
	TeinetClients		Members of this group have access to Telnet Server on this system.		
	Delegate Contro	. I			
	Find				
	New	Computer			
	AI Tasks	+ Contact			
	Refresh	Group			
	Export List	InetOrgPerson MSMQ Queue Al			
	Yew	Printer	b.		
	Arrange [cons	User			
	Ling up loons	Shared Folder			
	Properties				
	Help				
<u>. </u>	J.			 	
Create a new object					
🐮 Start 🛛 😥 🙍 🔄 🗐 Manag	e Your Server	Directory User			🛃 3:47 PM

Enter the required details for the account and click Next. The following figures show the 3. details entered for the "query_account" and for the user account.

Create the binding account, "query_account":

Last name:		ials:	
Last name:	Įnit	ials:	
Full name: query_account			
User logon name:			
query_account @testo	lomain.hp.c	om	
User logon name (pre- <u>W</u> indows 2000):			
TESTDOMAIN\ query_	account		
< <u>B</u> ac	с. <mark>Г</mark> N	ext >	Cance

Enter the password for the user in the specific domain and click **Next**. 4.

New Object - User	×
Create in: testdomain.hp.com/Users	
Password:	
Confirm password:	
User must change password at next logon	
✓ User cannot change password	
Password never expires	
Account is disabled	
< <u>B</u> ack <u>N</u> ext> Cancel	

 The New Object-User dialog box displays the details for the user and selected password settings. Click Finish to create the user profile.
 Details of "query_account":

i Object - User	
Create in: testdomain.hp.com/Users	
When you click Finish, the following object will be created:	
Full name: query_account	<u>^</u>
User logon name: query_account@testdomain.hp.com	
The user cannot change the password. The password never expires.	
	<u>ت</u> ــــــــــــــــــــــــــــــــــــ
< <u>B</u> ack Finish	Cancel

6. Create the test user account "jdoe", similar to the "query_account".

Extracting ACME LDAP configuration parameter values

You require the following information from the Active directory to populate the LDAP INI configuration file.

- LDAP port (This is usually 389 the non-secure port and 636 the secure port). For detailed steps on how to obtain this information, see "Querying LDAP port" (page 41).
- Base Distinguished Name (DN) under which all users are present.
- Distinguished Name and password of the "query_account".
- Login attribute (usually "samaccountname").

The base distinguished name (base_dn directive), the distinguished name of the query_account (bind_dn directive), and the samaccountname (login_attribute directive) are obtained from the database log file, .ldf file. For more information on how to obtain the specific attribute value, see "Extracting base_dn, bind_dn, and login_attribute" (page 41).

Querying LDAP port

To query LDAP ports, you can install the PortQryUI tool provided by Microsoft. This tool is available for download from:<u>http://www.microsoft.com/downloads/en/</u> confirmation.aspx?familyId=8355e537-1ea6-4569-aabb-f248f4bd91d0=en

You can use any other query tool of your choice.

Extracting base_dn, bind_dn, and login_attribute

You can extract the values for *base_dn*, *bind_dn*, and *login_attribute* directives (in the ACME LDAP configuration file) from the .ldf file.

To extract the .ldf file, at the command prompt, enter the following command on your Windows system:

Command Prompt Microsoft Windows [Version 5.2.3790] (C) Copyright 1985-2003 Microsoft Corp. C:\Documents and Settings\Administrator.CSSN-DDRS.000>ldifde -f output.ldf Connecting to "cssn-ddrs.testdomain.hp.com" Logging in as current user using SSPI Exporting directory to file output.ldf Searching for entries... Writing out entries... 204 entries exported The command has completed successfully C:\Documents and Settings\Administrator.CSSN-DDRS.000>_

After the .ldf file is extracted, copy the *base_dn* and *bind_dn* value. For more information on the *base_dn* and *bind_dn* directives, see Table 2-1.

Figure 4-2 shows a sample .ldf file. Here, the account, "query_account" is identified as the binding account. The "base_dn" and "bind_dn" values are highlighted.

ldifde -f <filename>.ldf

Figure 4-2 Sample LDF file

output_new.ldf - Notepad File Edit Format Vew Help
· · · · · · · · · · · · · · · · · · ·
in: DC=testdomain, DC=hp, DC=com "base_dn=DC=testdoamin,DC=hp, DC=com"
Changerype: add
obječtClass: top
objectClass: domain objectClass: domainDNS
distinguishedName: Dc=testdomain, DC=hp, DC=com
instanceType: 5
when created: 20091204100612.0Z
whenchanged: 20091210034419.0Z
subrefs: DC=ForestDnsZones, DC=testdomain, DC=hp, DC=com
subrefs: DC=DomainDnszOnes, DC=testdomain, DC=hp, DC=com
subrefs: CN=Configuration, DC=testdomain, DC=hp, DC=com
uSNCreated: 4098
uSNChanged: 16717
name: testdomain
objectGUID:: R1CJZmqGHU+9oq12GGOFXQ==
créationTime: 129043928120468750
forceLogoff: -9223372036854775808
lockoutDuration: -1800000000
lockoutobservationwindow: -1800000000
lockoutThreshold: 0
maxPwdAge: -37108517437440
minPwdAge: -86400000000
dn: CN=query_account,CN=Users,DC=testdomain,DC=hp,DC=com
changetype: add
objectClass: top
objectClass: preson objectClass: organizationalPerson
objectClass: user
givenName: guery_account
Instance/uppe: 4 "bind_ch= CN=query_account,CN=Users, the control of the control of the cN=query_account,CN=Users,DC=testdomain,DC=hp,DC=com"
whencreated: 20091204101609.0Z
whenChanged: 20091204101609.0Z
displayName: query_account
uSNCreated: 13913
uSNChanged: 13919
name: query_account
objectGUID:: f6634xgfgUygjoEPOKnZ5w==
userAccountControl: 66048 badPwdcount: 0
coderace: 0
courtrycode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 129043953697031250
primaryGroupID: 513
objectsid:: AQUAAAAAAAUVAAAA/pKYOHKiWJNbkqRqTWQAAA==
accountExpires: 9223372036854775807
logonCount: 0
\$AMAccountName: query_account "SAMAccountName: query_account"
SAMACCOUNTTYPE: 805306368
userPrincipalName: query_account@testdomain.hp.com
objectCategory:
CN=Person, CN=Schema, CN=Configuration, DC=testdomain, DC=hp, DC=com

Configuring ACME LDAP agent for non-secure port

To configure an ACME LDAP agent on a non-secure port, do the following:

- 1. Install the ACMELOGIN and ACMELDAP_STD kit as explained in "Installing the ACMELOGIN and ACMELDAP_STD kits" (page 13).
- 2. Check whether the images are loaded correctly:

```
ANALYZE/IMAGE/INTER SYS$COMMON:[SYSEXE]LOGINOUT.EXE
$ ANALYZE/IMAGE/INTER SYS$COMMON:[SYSEXE]LOGINOUT.EXE
This is an OpenVMS IA64 (Elf format) executable image file
```

Image Identification Information, in section 3.

```
Image name:"LOGINOUT"Global Symbol Table name:"LOGINOUT"Image file identification:"LOGIN98 X-1"Image build identification:"XC7Q-BL4-000000"Link identification:"Linker I02-37"Link Date/Time:8-FEB-2010 15:23:06.56
```

ANALYZE/IMAGE/INTER SYS\$COMMON: [SYSEXE] SETPO.EXE

\$ ANALYZE/IMAGE/INTER SYS\$COMMON:[SYSEXE]SETPO.EXE This is an OpenVMS IA64 (Elf format) executable image file

Image Identification Information, in section 3.

Image name:	"SETPO"
Global Symbol Table name:	"SETPO"
Image file identification:	"LOGIN98 X-1"
Image build identification:	"XC7Q-BL4-000000"
Link identification:	"Linker I02-37"
Link Date/Time:	8-FEB-2010 15:25:05.14

- 3. Set up the LDAP persona extension. For more information on how to set the persona extension, see "Setting up LDAP persona extension" (page 15).
- 4. Restart the OpenVMS system after setting the persona extension.
- 5. For a non-secure port, enter the following values for the attributes in the LDAP configuration file, SYS\$STARTUP:LDAPACME\$CONFIG-STD.INI:

```
server = cssn-ddrs.testdomain.hp.com. Ensure that you are able to make a $
TCPIP PING cssn-ddrs.testdomain.hp.com to the Active directory system.
```

port = 389. This is the default value for a non-secure port.

bind_dn = CN=query_account, CN=Users, DC=testdomain, DC=hp, DC=com. This value can be obtained from the .ldf file. For information on how to extract the value, see "Extracting base_dn, bind_dn, and login_attribute" (page 41).

bind_password = welcome@123. This is the password given for the query_account in the Active directory. See "Creating accounts on Active directory" (page 38).

base_dn = DC=testdomain, DC=hp, DC=com. This is the base account under which all other accounts reside. See "Creating accounts on Active directory" (page 38).

login_attribute = samaccountname. See "Creating accounts on Active directory"
(page 38).

scope = sub. Retain the default value "sub".

port_security = none. Since this is a non-secure port, replace the default value with "none".

```
password_type = active-directory. Replace the default value with active-directory
since the configuration is done with an Active directory.
```

The populated configuration file will be as shown:

```
server = cssn-ddrs.testdomain.hp.com
port = 389
bind_dn = CN=query_account,CN=Users,DC=testdomain,DC=hp,DC=com
bind_password = welcome@123
base_dn = DC=testdomain,DC=hp,DC=com
login_attribute = samaccountname
scope = sub
port_security = none
password type = active-directory
```

6. Add the following logical to the SYS\$MANAGER : ACME\$START . COM:

```
$ DEFINE/SYSTEM/EXECUTIVE LDAPACME$INIT
SYS$STARTUP:LDAPACME$CONFIG-STD.INI and uncomment the
@SYS$STARTUP:LDAPACME$STARTUP-STD.
```

7. Restart the ACME server.

8.

```
$ SET SERVER ACME/EXIT/WAIT
$ SET SERVER ACME/START=AUTO
Execute SHOW SERVER ACME/FULL to check if the ACME LDAP agent has been loaded.
```

```
$ SHOW SERVER ACME/FULL
    ACME Information on node EARWIG 18-FEB-2010 06:03:42.00 Uptime 0 00:15:24
    ACME Server id: 2 State: Processing New Requests
       Agents Loaded: 2 Active: 2

Thread Maximum: 1 Count: 1

Request Maximum: 826 Count: 0

Requests awaiting service: 0
                                                 0
       Requests awaiting dialogue:
       Requests awaiting AST:
                                                 0
       Requests awaiting resource:
                                                 0
       Logging status: Active
       Tracing status: Inactive
       Log file: "SYS$SYSROOT: [SYSMGR] ACME$SERVER.LOG;19"
    ACME Agent id: 1 State: Active
       Name: "VMS"
       Image: "DISK$164SYS:[VMS$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
Credentials Type: 1 Name: "VMS"
       Resource wait count:
                                                  0
    ACME Agent id: 2 State: Active
       Name: "LDAP-STD"
       Image: "DISK$164SYS:[VMS$COMMON.SYSLIB]LDAPACME$LDAP-STD ACMESHR.EXE;1"
       Identification: "ACME LDAP Standard V1.5"
       Information: "ACME LDAP DOI Agent is initialized"
       Domain of Interpretation: Yes
       Execution Order: 2
Credentials Type: 3 Name: "LDAP"
       Resource wait count:
                                                 0
9. Add the user jdoe to the SYSUAF. DAT file.
```

```
Password (password is not echoed to terminal) [JDOE]:
     UIC Group number [200]:
     UIC Member number: 201
     Account name: TEST
     Privileges [TMPMBX,NETMBX]:
     Login directory [JDOE]:
     Login device [SYS$SYSDEVICE:]:
     %CREATE-I-EXISTS, SYS$SYSDEVICE: [JDOE] already exists
     %UAF-I-PWDLESSMIN, new password is shorter than minimum password length
     %UAF-E-UAEERR, invalid user name, user name already exists
     %UAF-I-NOMODS, no modifications made to system authorization file
     %UAF-I-RDBNOMODS, no modifications made to rights database
     Check newly created account:
     Username: JDOE
                                                           Owner:
     Account: TEST
                                                           UIC: [201,2011] ([JDOE])
     CLI:
                 DCL
                                                           Tables: DCLTABLES
     Default: SYS$SYSDEVICE: [JDOE]
     LGTCMD:
     Flags: VMSAuth
     Primary days: Mon Tue Wed Thu Fri
    No access restrictions
Expiration
                                                  Sat Sun
    No access restrictions

Expiration: (none) Pwdminimum: 6 Login Fails: 1

Pwdlifetime: 90 00:00 Pwdchange: (pre-expired)

Last Login: (none) (interactive), (none) (non-interactive)

Maxjobs: 0 Fillm: 128 Bytlm: 128000

Maxacctjobs: 0 Shrfillm: 0 Pbytlm: 0

Maxdetach: 0 BIOlm: 150 JTquota: 4096

Prclm: 8 DIOlm: 150 WSdef: 4096

Prio: 4 ASTIm: 300 WSquo: 8192

Queprio: 4 TQElm: 100 WSextent: 16384

CPU: (none) Enqlm: 4000 Pgflquo: 256000

Authorized Privileges:
     Authorized Privileges:
      NETMBX TMPMBX
     Default Privileges:
       NETMBX TMPMBX
     %UAF-I-NOMODS, no modifications made to system authorization file
     &UAF-I-RDBNOMODS, no modifications made to rights database
     Is everything satisfactory with the account [YES]:
10. Set ExtAuth and VMSAuth flag for the user jdoe. For information about adding a SYSUAF
     account, see "Specifying EXTAUTH and VMSAUTH flags on OpenVMS" (page 19).
     $ SET DEF SYS$SYSTEM
     $ MC AUTHORIZE
     UAF> modify jdoe/flags=(EXTAUTH,VMSAUTH)
     %UAF-I-MDFYMSG, user record(s) updated
     UAF> SHOW jdoe
```

```
Username: JDOE
                                                                     Owner:
Account: TEST
                                                                     UIC:
                                                                                  [201,2011] ([JDOE])
              DCL
                                                                    Tables: DCLTABLES
CLT:
Default: SYS$SYSDEVICE: [JDOE]
LGICMD:
Flags: ExtAuth VMSAuth
Primary days: Mon Tue Wed Thu Fri
Secondary days:
                                                          Sat Sun
No access restrictions
No access restrictionsExpiration:(none)Pwdminimum: 6Login Fails: 1Pwdlifetime:90 00:00Pwdchange:(pre-expired)Last Login:(none)(interactive),(none)(non-interactive)Maxjobs:0Fillm:128Bytlm:128000Maxacctjobs:0Shrfillm:0Pbytlm:0Maxdetach:0BIOlm:150JTquota:4096Prclm:8DIOlm:150WSdef:4096
```

Prio:	4	ASTlm:	300	WSquo:	8192
Queprio:	4	TQElm:	100	WSextent:	16384
CPU:	(none)	Enqlm:	4000	Pgflquo:	256000
Authorized	Privileg	es:			
NETMBX	TMPM	BX			
Default Pr	ivileges:				
NETMBX	TMPM	BX			
UAF>					

11. Login to the system as user "jdoe".

Enabling ACME LDAP for secure ports

This section includes the following:

- 1. "Creating Active directory certificates" (page 46)
- 2. "Configuring ACME LDAP for secure port" (page 51)

Creating Active directory certificates

To create a certificate file to enable secure authentication, you can install the Microsoft certification service and create the root CA as explained in the following procedure. Optionally, you can install third-party certificates. Refer to the knowledge brief provided by Microsoft: <u>How to enable LDAP over SSL with a third-party certification authority</u>"

1. Go to Start > All Programs > Control Panel>Add or Remove Programs to open Add or Remove Programs window.



2. Click Add or Remove Windows Components option in the Add or Remove Programs window. The Windows Components Wizard dialog box is displayed.

ndows Components You can add or remove co	omponents of Windows.	Ì
part of the component will Details.	onent, click the checkbox. A sh be installed, To see what's inclu	
Components:		22 (140)
Application Server		33.4 MB
Certificate Service	\$	1.4 MB
E-mail Services		
Eax Services		7.9 MB
Devine Service		0.0 MB 土
Description: Installs a cer	tification authority (CA) to issue c acuity programs	ertificates for use with
public key se	sound programs.	
	en 192 en el 197 en general de la Señera de la composition de la composition de la composition de la compositi	Details

3. Select **Certificate Services**. You get the following warning message. Click **Yes** in the message box and **Next** in the **Windows Components Wizard** to continue installing the certificates.

Microsoft	Lettilicate services	l
	After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would available the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?	
	Ves No	and and a state of the state of

4. Select the required CA type from the options provided. The default is **Enterprise root CA**. Click **Next** to display the **CA Identifying Information** window.

Windows Components Wizard	1			×
CA Type Select the type of CA you	want to set up	×.		Ċ
 Enterprise root CA Enterprise subordinate Stand-alone root CA Stand-alone subordinate Description of CA type – The most trusted CA in a 	ite CA	hould be installed	f before any other	CA.
Use custom settings to) generate the l < <u>B</u> ack	(ey pair and CA o	certificate.	Help

5. Enter the **Common name for this CA:** in the **CA Identifying Information** dialog box. Also, select the **Validity period**. Click **Next** to display the **Certificate Database Settings** dialog box.

Common name for this CA:		
testdomain-rootca		
Distinguished name suffix:		
DC=testdomain,DC=hp,DC=com		
<u> </u>		
Preview of distinguished name:		
CN=testdomain-rootca,DC=testdo	main,DC=hp,DC=com	
Validity period:	Expiration date:	
5 Years 💌	11/30/2014 3:07 PM	

6. Browse and select the **Certificate database** and **Certificate database log:** folders or retain the default location and click **Next** to display the **Configuring Components** dialog box..

Window	rs Components Wizard	×
	tificate Database Settings Enter locations for the certificate database, database log, and confi information.	guration
1	<u>C</u> ertificate database:	
ļ	C:\WINDOWS\system32\CertLog	Browse
i	Certificate database log:	
	C:\WINDOWS\system32\CertLog	Bro <u>w</u> se
1	Store configuration information in a shared folder Shared folder: Preserve existing certificate database	Browse
	< <u>B</u> ack <u>N</u> ext > Ca	ncel Help

7. Wait while the certificate components are being configured. When the configuration is complete, click **Next**.

	g Component making the cor	s nfiguration change	es you requested	L	ĺ
Ö	Please wait w several minut	vhile Setup configues, depending on	ures the compor the component:	nents. This may t s selected.	ake
Status:	Building file list.				
[

8. You may get the following message:

"Internet Information Services (IIS) is not installed on this computer. Certificate Services Web Enrollment Support will be unavailable until IIS is installed."

Click OK . The Completing the Windows Components Wizard dialog box is displayed.

nge or	Currently installed programs:	≦ort by;	Name	
move grams	Windows Components Wizard Configuring Components Setup is making the configuration changes you requested.		Size Used Used On 1 Change	<u>0.23M</u> rarel 1/27/200 e/Remove
l <u>N</u> ew grams	Please wait while Setup configures the components. This may take several minutes, depending on the components selected.		Size	78.28M
	e Services formation Services (IIS) is not installed on this computer. Certificate Services Web Enrollment	Support will I) pe unavailab	le until IIS
		Support will I	- pe unavailab	le until IIS
	formation Services (IIS) is not installed on this computer. Certificate Services Web Enrollment	Support will I	pe unavailab	le until II:

9. Click **Finish** to complete installing certificates.

Windows Components Wizard		×
	Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard.	
	To close this wizard, click Finish.	
	< Back Finish	Help

10. Restart the Windows system.

Configuring ACME LDAP for secure port

1. Update the LDAP configuration file, SYS\$STARTUP:LDAPACME\$CONFIG-STD.INI similar to how the file was updated in section "Configuring ACME LDAP for non-secure port". The only difference is the values provided to the *port* and *port_security* directives.

See the following sample configuration file:

```
server = cssn-ddrs.testdomain.hp.com
port = 636
bind dn = CN=query account, CN=Users, DC=testdomain, DC=hp, DC=com
bind password = welcome@123
base dn = DC=testdomain,DC=hp,DC=com
scope = sub
port security = ssl
password type = active-directory
or
server = cssn-ddrs.testdomain.hp.com
port = 389
bind dn = CN=query account, CN=Users, DC=testdomain, DC=hp, DC=com
bind_password = welcome@123
base_dn = DC=testdomain,DC=hp,DC=com
scope = sub
port_security = starttls
password type = active-directory
```

2. Restart ACME_SERVER and check the login as explained in section "Configuring ACME LDAP agent for non-secure port" (page 43).

Providing Active directory certificates to ACME LDAP

This is an optional step, where you can export the public root certificate of the Active directory and provide it to the ACME LDAP agent. The ACME LDAP agent checks if it is connecting to the correct active directory server by validating the certificate.

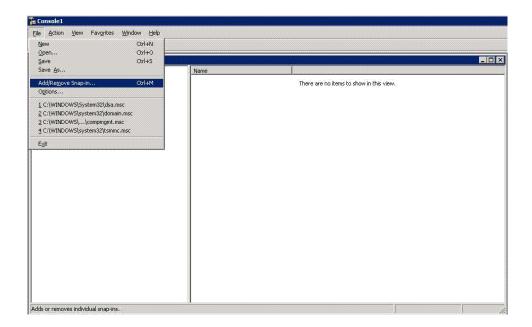
Viewing the certificate on Active directory

To view the certificate generated, perform the following steps:

1. Go to **Run** and open **mmc** to open a console.

Run Type the name of a program, Internet resource, and Windo	folder, document, or
Open: mmc	
ОК	Cancel Browse
🛃 Start 🛛 😰 🙇 👘 🧾 Manag	je Your Server
Ele Action yiew Favgrites Window Help ← → III IB IS Console Root	
Console Root	Name There are no items to show in this view.

2. Go to File > Add/Remove Snap-in to open the Add/Remove Snap-in dialog box.



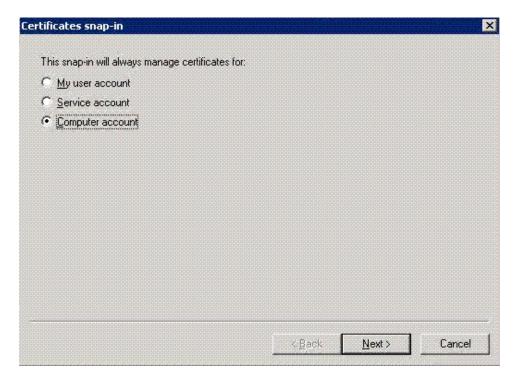
3. Click Add in the Standalone tab in the Add/Remove Snap-in dialog box. The Add Standalone Snap-in dialog box is displayed.

tandalone Extensi	ons d or remove a standalone Snap-in I	rom the console.
	Console Root	ľ
- Description		
Description	<u>R</u> emove A <u>b</u> out	

4. Select **Certificates** and click **Add** to display the **Certificates snap-in** dialog box. You will be required to enter details of the certificate in the next few dialog boxes.

Snap-in	Vendor	
🍓 .NET Framework 1:1 Configuration	Microsoft Corporation	
Retive Directory Domains and Trusts	Microsoft Corporation	
🚮 Active Directory Sites and Services 🚽	Microsoft Corporation	
Active Directory Users and Comput	Microsoft Corporation	
🗯 ActiveX Control	Microsoft Corporation	
🛺 Authorization Manager	Microsoft Corporation	
🙀 Certificate Templates	Microsoft Corporation	
Certificates	Microsoft Corporation	
📴 Certification Authority	Microsoft Corporation	
Component Services	Microsoft Corporation	
Description The Certificates snap-in allows you to brov certificate stores for yourself, a service, or		

5. Select the **Computer account** option and click **Next** to display the **Select Computer** dialog box.



6. Select Local computer (the computer this console is running on) option and click Finish to complete the process of adding the certificate. You will be taken back to the Add Standalone Snap-in dialog box.

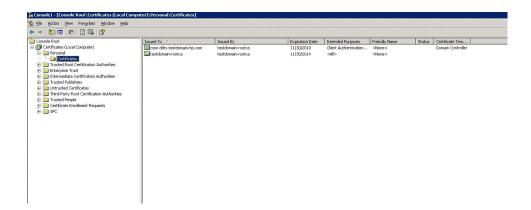
lect the computer you w	ant this snap-in to manage			
his snap-in will always n	nanage:			
• Local computer: (th	e computer this console is	running on)		
C Another computer:				Browse
	computer to be obspreed w	hen launching f	rom the comma	nd line. This
Allow the selected of				
Allow the selected of only applies if you selected of the s				

7. Click **Close** on the **Add Standalone Snap-in** dialog box. The **Add/Remove Snap-in** dialog box displays the certificates added to the snap-in.

Click **OK** to close the **Add/Remove Snap-in** dialog box.

d/Remove Snap-in	? ×	_	
Standalone Extensions			
Use this page to add or remove a standalone Snap-in from the console.			
Snap-ins added to: 🔄 Console Root			
Certificates (Local Computer)	Add Standalone Snap-in		? ×
En Ceruicates (Eucar computer)	Available Standalone Snap-ins:		
	Snap-in	Vendor	
Description	 NET Framework 1.1 Configuration Active Directory Domains and Trusts Active Directory Sites and Services Active Directory Users and Comput ActiveX Control Authorization Manager Certificate Templates Certificates Certification Authority Component Services 	Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
Agd <u>Hemove</u> <u>About</u> OK Ca	Description The Cettificates snap-in allows you to brov cettificate stores for yourself, a service, or		056

8. Go to **Console Root** > **Certificates** > **Personal** > **Certificates**. The available certificates are displayed in the right-hand side panel of the **Console Root** window.



9. Right-click on the certificate and select **All Tasks** > **Export** to export the certificate. The **Certificate Export Wizard** dialog box is displayed.



10. Click **Next** in the **Welcome** dialog box to start exporting the certificate. The **Export Private Key** dialog box is displayed.



11. Select **No**, **do not export the private key** and click **Next** to display the **Export File Format** dialog box.

Certificate Export Wizard	×
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
Do you want to export the private key with the certificate?	
\bigcirc Yes, export the private key	
No, do not export the private key	
< <u>B</u> ack <u>N</u> ext > Cance	:i

12. Export the **certificate in Base-64 encoded X.509 format** only. Click **Next**. The **File to Export** dialog box is displayed.

port File Format Certificates can be exported in a variety of file formats.		
Select the format y	ou want to use:	
C DER encode	d binary X.509 (.CER)	
Base-64 end	oded X.509 (.CER)	
	nic Message Syntax Standard - PKCS #7 Certificates (.P7B) all certificates in the certification path if possible.	
	ormation Exchange - PKCS #12 (PPX) all certificates in the certification path if possible	
📕 Enable s	trong protection (requires IE 5.0, NT 4.0 SP4 or above)	
📕 Delete t	he private key if the export is successful	

13. Browse and select the **File name:** or click **Next** with the default file name. The **Completing the Certificate Export Wizard** dialog box is displayed.

Certificate Export Wizard			×
File to Export Specify the name of the file you want to e:	xport		
<u>File name:</u>			
c:\base64_testdomain_rootca.cer		Browse	<u>. </u>
	< <u>B</u> ack	Next >	Cancel
	<u> </u>	<u>N</u> ext >	Cancel

14. Click **Finish** to complete exporting the certificate. You get the following message if the export is successful.

The export was successful.

Certificate Export Wizard		×
	Completing the Certificate Export Wizard	
	You have successfully completed the Certificate Export wizard.	
Contract States	You have specified the following settings:	
	File Name c:\base Export Keys No Include all certificates in the certification path No File Format Base64	
	▲	
	< <u>B</u> ack Finish Cancel	

Wizard You have successfully completed the Certificate wizard.	Export
You have specified the following settings:	
File Name Export Keys Include all certificates in the certification path File Format	c:\base No No Base64
Certificate Export Wizard 🛛 🗙	
 The export was successful.	
	Ċano

To view the certificate, open the certificate file with Notepad

🔇 Back 🔹 🏐 🕣 🧊 🔎 Search	🜔 Folders 🛛 🔯 🌛 🗙 🍫	·				
Address 🖙 C:\						
Folders ×	Name A		Size	Туре	Date Modified	Attributes
 Desktop Desktop My Documents My Computer My Computer My Computer Documents and Settings Install Program Files WINDOWS Control Program Files WINDOWS Control Program Files My Network Places Recycle Bin 	broadcom, 5/52, driver Documents and Settings install Materials Portcy/UI Portgy/UI WINDow/S WINDOW/S WINDOWS WINDOW/S WIN	Open Install Certificate Copen W/bl ▶ Send To ▶ Cut Copy Copy Create Shortcut Delete Renage Properties ■	2 KB		11/26/2009 10:34 AM 11/27/2009 3:10 PM 11/27/2009 3:10 PM 11/27/2009 3:10 PM 11/27/2009 3:10 PM 11/27/2009 3:19 PM 11/25/2009 4:07 PM 11/26/2009 3:09 PM 11/27/2009 10:17 AM 11/30/2009 3:20 PM	

The certificate generated on the system is shown in the following figure:



Adding the certificate to OpenVMS

To add the certificate for LDAP authentication, perform the following steps:

- 1. Create a file SYS\$SYSROOT: [SYSMGR] <certificate name>. For example, SYS\$SYSROOT: [SYSMGR] BASE64_TESTDOMAIN_ROOTCA.CER, where BASE64_TESTDOMAIN_ROOTCA.CER is the name of the certificate.
- 2. Copy the certificate from the Active directory server and paste it on to the BASE64_TESTDOMAIN_ROOTCA.CER file.
- **3.** Save the file.

NOTE: If you FTP this file, use ASCII mode.

4. Ensure that this file is protected.

```
SET SECURITY/PROTECTION = (SYSTEM: "RWED", OWNER: "", GROUP: "", WORLD: "")
```

5. Open the SYS\$STARTUP:LDAPACME\$CONFIG-STD.INI file and edit the *ca_file* attribute with the exact directory location of the certificate file.

For example, ca_file = SYS\$SYSROOT: [SYSMGR] :BASE64_TESTDOMAIN_ROOTCA.CER
and save the configuration file

- 6. Restart ACME server:
 - \$ SET SERVER ACME/EXIT/WAIT
 - \$ SET SERVER ACME/START=AUTO

5 Troubleshooting

Problem

System displays the following error when @SYS\$STARTUP:ACME\$START.COM is executed:

```
$ @sys$startup:acme$start.com
```

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

Solution

```
The LDAPACME$INIT logical is not defined before the
@SYS$STARTUP:LDAPACME$STARTUP-STD command in
SYS$COMMON: [SYSMGR] ACME$START.COM. For more information, see the steps in "Editing
LDAP configuration file" (page 15).
```

Problem

When @SYS\$STARTUP: ACME\$START. COM is executed, the system displays the following error, all ACME agent are in stopped state when using the SHOW SERVER ACME/FULL command and new logins are not permitted:

```
$ @sys$startup:acme$start.com
%ACME-E-INVPARAMETER, parameter selector or descriptor is invalid
```

Solution

The LDAPACME\$INIT logical is defined to a wrong INI file name. Perform the following steps:

- 1. Deassign the LDAPACME\$INIT logical
 - \$ deassign /system/exec LDAPACME\$INIT
- 2. Stop the ACME Server process
 - \$ set server acme/exit/wait
- **3.** Correct the LDAPACME\$INIT logical to point to the right path inside SYS\$STARTUP:ACME\$START.COM
- 4. Start the ACME server in auto mode so that it starts the ACME LDAP agent during startup.

```
$ set server acme/start=auto
```

Problem

The SHOW SERVER ACME/FULL command does not display the LDAP agent.

```
$ sh server acme/full
ACME Information on node EARWIG 18-FEB-2010 05:50:06.40 Uptime 0 00:01:48
ACME Server id: 2 State: Processing New Requests
  Agents Loaded: 1 Active:
Thread Maximum: 1 Count:
                                           1
   Thread Maximum:
                                           1
  Request Maximum: 1
                            Count:
                                           0
   Requests awaiting service:
                                           0
   Requests awaiting dialogue:
                                           0
   Requests awaiting AST:
                                           0
   Requests awaiting resource:
                                           0
   Logging status: Active
   Tracing status: Inactive
   Log file: "SYS$SYSROOT: [SYSMGR] ACME$SERVER.LOG;17"
ACME Agent id: 1 State: Active
   Name: "VMS"
```

```
Image: "DISK$I64SYS:[VMS$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
Credentials Type: 1 Name: "VMS"
Resource wait count: 0
```

```
$
```

Solution

Check if the SYS\$STARTUP: ACME\$START. COM has been updated with the LDAP logical names and @SYS\$STARTUP: LDAPACME\$STARTUP-STD ! LDAP command is uncommented in the file. For more information on updating the SYS\$STARTUP: ACME\$START. COM, see "Editing LDAP configuration file" (page 15).

```
ACME Server id: 2 State: Processing New Requests
  Agents Loaded: 2 Active:
Thread Maximum: 1 Count:
Request Maximum: 826 Count:
                                            2
                                           1
                                           0
   Requests awaiting service:
                                           0
   Requests awaiting dialogue:
                                           0
   Requests awaiting AST:
                                           0
   Requests awaiting resource:
                                            0
   Logging status: Active
   Tracing status: Inactive
   Log file: "SYS$SYSROOT: [SYSMGR] ACME$SERVER.LOG; 19"
ACME Agent id: 1 State: Active
   Name: "VMS"
   Image: "DISK$I64SYS:[VMS$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
Credentials Type: 1
                            Name: "VMS"
   Resource wait count:
                                            0
ACME Agent id: 2 State: Active
   Name: "LDAP-STD"
   Image: "DISK$164SYS:[VMS$COMMON.SYSLIB]LDAPACME$LDAP-STD ACMESHR.EXE;1"
   Identification: "LDAP ACME Standard V1.5"
   Information: "ACME LDAP DOI Agent is initialized"
   Domain of Interpretation: Yes
   Execution Order: 2
Credentials Type: 3
                        3 Name: "LDAP"
   Resource wait count:
                                            0
$
```

Problem

All the ACME LDAP configuration is correct, but the user is unable to log in.

Solution 1

Use the Ping command to check whether the LDAP server provided in the server directive of the LDAP INI file is reachable:

```
$ tcpip ping
PING earwig (15.146.235.235): 56 data bytes
64 bytes from 15.146.235.235: icmp_seq=0 ttl=64 time=0 ms
64 bytes from 15.146.235.235: icmp_seq=1 ttl=64 time=0 ms
64 bytes from 15.146.235.235: icmp_seq=2 ttl=64 time=0 ms
64 bytes from 15.146.235.235: icmp_seq=3 ttl=64 time=0 ms
```

```
----earwig PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0 ms
```

Solution 2

Ensure that the ExtAuth flag is provided for the user in SYSUAF. DAT file.

Solution 3

Use TCPDUMP to check whether data is flowing on the configured LDAP port.

```
$ tcpdump -w tcpdump.enc tcp port 389
tcpdump: Filtering in user process
tcpdump: listening on WE1, link-type EN10MB (Ethernet), capture size 96 bytes
*CANCEL*
24 packets captured
24 packets received by filter
0 packets dropped by kernel
$ dir .enc
Directory SYS$SYSROOT: [SYSMGR]
TCPDUMP.ENC;1
Total of 1 file.
$ tcpdump -r TCPDUMP.ENC
reading from file tcpdump.enc, link-type EN10MB (Ethernet)
05:39:16.726000 IP opnvms.ind.hp.com.49160 > CSSN-DDRS.TESTDOMAIN.HP.COM.389: S 1252791091:1252791091(0) win
61440 <mss 1460,nop,wscale 0>
05:39:16.726000 IP CSSN-DDRS.TESTDOMAIN.HP.COM.389 > opnvms.ind.hp.com.49160: S 1725693481:1725693481(0) ack
1252791092 win 16384 <mss 1460,nop,wscale 0>
05:39:16.726000 IP opnvms.ind.hp.com.49160 > CSSN-DDRS.TESTDOMAIN.HP.COM.389: . ack 1 win 62780
05:39:16.726000 IP opnvms.ind.hp.com.49160 > CSSN-DDRS.TESTDOMAIN.HP.COM.389: P 1:78(77) ack 1 win 62780
05:39:16.728000 IP CSSN-DDRS.TESTDOMAIN.HP.COM.389 > opnvms.ind.hp.com.49160: P 1:23(22) ack 78 win 65458
05:39:16.729000 IP opnvms.ind.hp.com.49160 > CSSN-DDRS.TESTDOMAIN.HP.COM.389: P 78:154(76) ack 23 win 62780
```

Solution 4 (for Programmers)

To troubleshoot issues with the LDAP configuration, use a compiled version of SYS\$EXAMPLES:LDAP_EXAMPLES.C

Note that the LDAP_EXAMPLE. C can currently only connect to the directory server on the standard (non-secure) port 389.

ld = ldap_init(argv[1], LDAP_PORT);

The LDAP_EXAMPLE.C assumes anonymous binding to the directory server. You can provide a DN (parameter 2) and password (parameter 3) to modify this behavior. If this is not the case, you can change the following code:

```
stat = ldap simple bind s(ld,NULL,NULL); to
```

```
stat =
```

ldap simple bind s(ld, "ON-query account, ON-Users, DC-testdomain, DC-yourdomain, dc-com", "yourpassword");

Where, CN=query_account, CN=Users, DC=testdomain, DC=yourdomain, dc=com is the value provided to the *bind_dn* directive of the ACME LDAP configuration file and **yourpassword** is the value provided to the *bind_password* directive of the ACME LDAP configuration file.

A sample compilation and execution is shown as follows. In the following sample, the **cssn-ddrs.testdomain.yourdomain.com** is the value of the *server*directive,

CN=Users, DC=testdomain, DC=yourdomain, dc=com is the value for the *base_dn* directive of the ACME LDAP configuration file.

```
$ set def sys$examples
```

```
$ cc LDAP_EXAMPLE
```

^{\$} link LDAP_EXAMPLE

^{\$} ldap_example:=="\$sys\$examples:LDAP_EXAMPLE.EXE"

^{\$} ldap_example

Usage : opnvms\$dka0:[sys0.][syshlp.examples]ldap_example.exe;6 [server] [base] [filter] <
attributes>

Program terminating \$ ldap_example cssn-ddrs.testdomain.yourdomain.com "CN=Users,DC=testdomain,DC=yourdomain, dc=com" "" sAMAccountName Number of entries returned : 34

dn = CN=Users,DC=testdomain,DC=yourdomain,dc=com
<Noattributes returned>
dn = CN=VMSUsers,CN=Users,DC=testdomain,DC=yourdomain,dc=com
sAMAccountName : VMSUsers
-

dn = CN=John Doe,CN=Users,DC=testdomain,DC=yourdomain,dc=com sAMAccountName : John Doe

Program terminating

FAQ

What events can be traced using the "\$ SET SERVER ACME/TRACE=<value>" command and how do we interpret the traces?

You can view critical errors logged by the agent in ACME\$SERVER.LOG without setting the SET SERVER ACME/TRACE=<value>. See Table 5-1 (page 65) for setting the appropriate values.

For example:

When ACME LDAP agent is configured to a Directory server, which is not reachable, the following error messages are displayed:

%ACME-I-LOGAGENT, agent initiated log event on 25-FEB-2010 10:41:06.43 ==> Time of Log -ACME-I-THREAD, thread: id = 4, type = EXECUTION ==> Thread ID of the ACME Server causing this error -ACME-I-REQUEST, request information, id = 1, function = AUTHENTICATE_PRINCIPAL ==> Function code passed to SYS\$ACM -ACME-I-CLIENT, client information, PID = 2020044C ==> Process ID of the client talking to ACME Server -ACME-I-AGENT, agent information, ACME id = 2, name = LDAP-STD ==> Agent handling this request -ACME-I-CALLOUT, active callout routine = acme\$co_accept_principal ==> Authentication routine handling the request -ACME-I-CALLBACK, active callback routine = acme\$cb_send_logfile ==> Callback routine.

-ACME_-I-TRACE, message from LDAP ACME agent: Internal error. LDAP search operation failed ==> Status returned by the ACME agent

Another example on giving port_security = nonenone instead of port_security = none in the configuration file:

%ACME-I-LOGAGENT, agent initiated log event on 25-FEB-2010 10:42:39.41 -ACME-I-THREAD, thread: id = 1, type = CONTROL -ACME-I-CONTROL, control information, operation = STARTUP -ACME-I-AGENT, agent information, ACME id = 2, name = LDAP-STD -ACME-I-CALLOUT, active callout routine = acme\$co_agent_startup -ACME-I-CALLBACK, active callback routine = acme\$cb_send_logfile -ACME_I-TRACE, MESSAGE FROM LDAP ACME agent: Reading the config file (LDAPACME\$INIT) failed ===> Error message

The information starting from "%ACME-I-" to the next "%ACME-I-" marks one trace.

When you execute \$ SET SERVER ACME/TRACE=<value>, tracing is enabled and logged to SYS\$MANAGER:ACME\$SERVER.LOG file.

You must look for the "MESSAGE FROM LDAP ACME agent" line in the ACME\$SERVER.LOG to locate status messages returned by the LDAP ACME agent

For details about the various flags that can be enabled for tracing execute \$ HELP SET SERVER ACME/TRACEON a OpenVMS system

The following table provides details about the trace flags:

Table 5-1 Bitmask

Bitmask	Event Description	
0	agent	Enable agent tracing.
1	general	General (non-specific) tracing.

Bitmask	Event	Description
2	vm	Virtual memory operations. That is, trace the memory allocation and de-allocation of both the ACME_SERVER and the agent (if the agent uses the memory services provided by ACME_SERVER process).
		NOTE: Tracing is not enabled if the agent uses is own or standard (malloc, calloc, free) memory management routines.
3	ast	AST processing.
		Traces ASTs that are triggered by agents to the ACME_SERVER.
4	wqe	WQE parameter that flows between the ACME_SERVER process and agent.
5	report	Agent status or attribute operations.
6	message	Messaging operations.
7	dialog	Dialogue operations.
8	resource	Agent resource operations. Agents can request for some specific resource locks from the ACME_SERVER process.
9	callout	Agent callout routine. Routines that are implemented by individual agents such as ACME LDAP, that are called by the ACME_SERVER.
10	callout_status	Agent callout return status.

Table 5-1 Bitmask (continued)

For example:

If you want tracing of "agent", "general", "report", "message", "dialog", "callout", and "callout_status", use:

\$ SET SERVER ACME/TRACE=1763

6 Restrictions

This section lists the restrictions associated with ACME LDAP agent.

Username and password restrictions

Password modifications are made to the standard userPassword attribute or Active directory's unicodePwd attribute. The details of the configuration attributes are described in "Installing and configuring ACME LDAP agent" (page 13). 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 the 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 user names 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 is that Active Directory expects UTF-8 character strings when updating the unicodePwd attribute.
- SET PASSWORD command will not work for SSH logins.

Mapping restrictions

- SSH login will not work for mapped users.
- While executing DECnet operations, such as DECnet copy, you must use the user name and password that is present in the SYSUAF.DAT file.
- The "SYSTEM" account is not mapped.

That is, if a user enters "SYSTEM" at the user name prompt, that user is mapped only to the "SYSTEM" account in SYSUAF.DAT.

The reverse is also true. That is, if the mapping is done for any user, for example, "johnd" to map to "SYSTEM" account in SYSUAF.DAT, this mapping will not happen and user gets a "Operation failure" error at login prompt.

7 References

The following resources can be referred for more information:

- SYS\$HELP:ACME_DEV_README.TXT
- "Enabling External Authentication" and "Authentication and Credentials Management Extensions (ACME) Subsystem" sections in the *HP OpenVMS Guide to System Security* manual.
- HP OpenVMS System Services Reference Manual

Index

A

adding certificate, 60 attribute unicodePwd, 67 userPassword, 67

В

base_dn, 16 bind_dn, 17 bind_password, 17

С

ca file, 17 certificate adding, 60 generating, 59 ovms, 60 viewing, 59 configuration file, 15 configuration files example, 21 configuring, 13 ACME LDAP non-secure port, 43 secure port, 51 ACME LDAP agent, 15 active directory, 28 global mapping, 25 local mapping, 25 creating accounts, 38 certificate, 46

D

DECnet restriction, 67 define logical, 61 defining logical, 44 directive base dn, 16 bind_dn, 17 bind_password, 17 ca file, 17 filter, 16 login_attribute, 16 mapping, 17 mapping_attribute, 17 mapping_file, 18 mapping_target, 18 password_type, 16 password_update, 16 port, 16

port_security, 17 scope, 16 server, 16 domain controller active directory, 28

Е

editing configuration file, 15 enabling ACME LDAP, 46 extracting base_dn, 41 bind_dn, 41 login_attribute, 41 parameter values, 41

F

faq, 65 filter, 16

G

generating certificates, 59 global mapping, 23

L

Installing ACMELDAP_STD, 13 ACMELOGIN, 13 installing, 13 active directory, 32 kits, 13

К

kits ACMELDAP_STD, 13 ACMELOGIN, 13 installing, 13

L

LDAP configuration attributes, 18 LDAP persona extension, 15 local mapping, 23 logical defining, 18 login_attribute, 16 LOGINOUT, 14

Μ

mapping, 17 global, 23 mapping, 17 mapping_attribute, 17 mapping_target, 18 local, 23 mapping, 17 mapping_file, 18 mapping_attribute, 17 mapping_file, 18 mapping_target, 18

Ρ

password_type, 16 password_update, 16 port, 16 port_security, 17 prerequisites, 13

Q

querying LDAP port, 41

R

reboot, 15 restarting ACME LDAP agent, 19 ACME server, 25, 26, 44 restoring kits, 14 restrictions active directory, 67 DECnet operation, 67 SSH, 67 username and password, 67

S

scope, 16 secure port configure, 51 server, 16 SETP0, 14 setting active directory domain controller, 28 LDAP persona extension, 15 specifying EXTAUTH, 19 VMSAUTH, 19 SSH restriction, 67

Т

tcpdump, 63 tracing, 66 troubleshooting configuration file, 62 define logical, 61 ExtAuth flag, 63 for programmers, 63 logical, 61 ping command, 62 tcpdump, 63 tracing errors, 65

U

user scenario, 27 configuring, 28 configuring ACME LDAP, 43 creating accounts, 38 creating certificate, 46 domain controller, 28 extracting attributes, 41 extracting parameter values, 41 global mapping, 25 installing acitve directory, 32 local mapping, 25 querying LDAP, 41 viewing certificate, 52 username and password restrictions SSH, 67

V

viewing certificate, 59 viewing certificate user scenario, 52