Ecole Supérieure Privée
d'Ingénierie et de Technologies

Install and configure OpenLDAP on CentOS 7

Services and Networks Administration

ESPRIT 2021/2022

Introduction

LDAP stands for Lightweight Directory Access Protocol. LDAP is a solution to access centrally stored information over network. This centrally stored information is organized in a directory that follows X.500 standard.

The information is stored and organized in a hierarchical manner and the advantage of this approach is that the information can be grouped into containers and clients can access these containers whenever needed. The OpenLDAP hierarchy is almost similar to the DNS hierarchy. The following are the two most commonly used objects in OpenLDAP:

1. **cn (common name)** – This refers to the leaf entries, which are end objects (for example: users and groups)
2. **dc (domain component)** – This refers to one of the container entries in the LDAP hierarchy. If in a setup the LDAP hierarchy is mapped to a DNS hierarchy, typically all DNS domains are referred to as DC objects

   What is LDIF

   A LDIF(LDAP Interchange Format) file is Known as a standard text file which can be used for configuring and storing information in LDAP directory. This file is usually used for the addition or modification of data inside the LDAP Directory Server based on Schema rules accepted by the Directory.

   What is an Attribute

   An attribute is like a variable which holds the value. It can be different types based on the different values it holds just like the variable in Programming Paradigms where it could be of type int, char, float, double etc.

Step 1: Install and configure OpenLDAP

```
# yum -y install openldap openldap-servers openldap-clients

#cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB-CONFIG

# systemctl start slapd

# systemctl enable slapd
```

Generate a password hash to be used as the admin password. This password hash will be used when you create the root user for your LDAP installation. For example

```
#slappasswd

New password :

Re-enter new password :

{SSHA}XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Take the hash output of the above command and add it to the oclRootPW parameter in the conf file as shown below.

```
# vi chrootpw.ldif
# specify the password generated above for "olcRootPW" section
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}xxxxxxxxxxxxxxxx
# ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.ldif
SASL/EXTERNAL authentication started
SASL username:
gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config
```

While editing this file, change the distinguished name (DN) of the olcSuffix to something appropriate. The suffix typically corresponds to your DNS domain name, and it will be appended to the DN of every other LDAP entry in your LDAP tree.

For example, let's say your University is called ESPRIT, and that your domain name is "esprit.com."

```
# generate directory manager's password
[root@dlp ~]# slappasswd
New password:
Re-enter new password:
{SSHA}xxxxxxxxxxxxxxxxxxxxxxx
[root@dlp ~]# vi chdomain.ldif
# replace to your own domain name for "dc=***,dc=***" section
# specify the password generated above for "olcRootPW" section
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
  read by dn.base="cn=Manager,dc=esprit,dc=com" read by * none

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=esprit,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
```

```
olcRootDN: cn=Manager,dc=esprit,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxx

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by
  dn="cn=Manager,dc=esprit,dc=com" write by anonymous auth by
self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=Manager,dc=esprit,dc=com" write by
* read

[root@dlp ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f
chdomain.ldif
SASL/EXTERNAL authentication started
SASL username:
gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}monitor,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"
```

Import basic shemas

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/cosine.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/nis.ldif
#ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/inetorgperson.ldif
[root@dlp ~]# vi basedomain.ldif
# replace to your own domain name for "dc=***,dc=***" section
dn: dc=esprit,dc=com
objectClass: top
objectClass: dcObject
objectclass: organization
o: ESPRIT
dc: esprit
dn: cn=Manager,dc=esprit,dc=com
objectClass: organizationalRole
```

```
cn: Manager
description: Directory Manager
dn: ou=People,dc=esprit,dc=com
objectClass: organizationalUnit
ou: People
dn: ou=Group,dc=esprit,dc=com
objectClass: organizationalUnit
ou: Group
[root@dlp ~]# ldapadd -x -D cn=Manager,dc=esprit,dc=com -W -f
basedomain.ldif
Enter LDAP Password:     # directory manager's password
adding new entry "dc=esprit,dc=com"

adding new entry "cn=Manager,dc=esprit,dc=com"

adding new entry "ou=People,dc=esprit,dc=com"
```

Now we need to start the service

```
# systemctl restart slapd
```

Verify that your entry was added correctly: `# ldapsearch -x -LLL -b dc=esprit,dc=com`

By default, the CentOS 7firewall will block external requests to OpenLDAP, you will have to configure your firewall to allow connections on port 389. (Port 389 is the default LDAP port.)

```
#firewall-cmd --add-service=ldap --permanent
#firewall-cmd --reload
```

Step 2: Add a user to the LDAP tree

In this example, we will add a user named "Ahmed Mejeri" to LDAP inside the "Users" OU. Create a file called ldapuser.ldif

```
# generate encrypted password
[root@dlp ~]# slappasswd
New password:
Re-enter new password:
{SSHA}xxxxxxxxxxxxxxxx
[root@dlp ~]# vi ldapuser.ldif
# create new
# replace to your own domain name for "dc=***,dc=***" section
dn: uid=Ahmed,ou=People,dc=esprit,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Ahmed
sn: Mejeri
userPassword: {SSHA}xxxxxxxxxxxxxxxx
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/ahmed

dn: cn=ahmed,ou=Group,dc=esprit,dc=com
objectClass: posixGroup
cn: Ahmed
gidNumber: 1000
memberUid: ahmed

[root@dlp ~]# ldapadd -x -D cn=Manager,dc=esprit,dc=com -W -f ldapuser.ldif
Enter LDAP Password:
adding new entry "uid=ahmed,ou=People,dc=esprit,dc=com"

adding new entry "cn=Ahmed,ou=Group,dc=esprit,dc=com"
```

Verify that your entry was added correctly:

```
# ldapsearch -x -LLL -b dc=esprit,dc=com
```

Step 3: Configure LDAP client

Now, we will configure the client part

```
[root@www ~]# yum install -y openldap-clients nss-pam-ldapd nscd
 # ldapserver=(LDAP server's hostname or IP address)
 # ldapbasedn="dc=(your own domain name)"
 [root@www ~]# authconfig --enableldap \
 --enableldapauth \
 --ldapserver=192.168.145.131\
 --ldapbasedn="dc=esprit,dc=com" \
 --enablemkhomedir \
 --update
 [root@www ~]# exit
 logout
 CentOS Linux 7 (Core)
 Kernel 3.10.0-123.20.1.el7.x86_64 on an x86_64
 www login: ahmed      # LDAP user
 Password:      # password
 Creating directory '/home/ahmed'.
 [ahmed@www ~]$      # logined normally
```

Or you can test with your windows host ;

Install jxplorer Application and try to connect to the ldap server: http://jxplorer.org/downloads/users.html