OpenLDAP
Server and Client Configuration
Rocky Linux 10

This lab requires 2 virtual machines with rocky 10 installed. The installation may be minimal or Server with GUI. Both the virtual machines should be connected to NAT mode. In production environment the OpenLDAP server should have a manually assigned IP address. But for this lab you can keep both the virtual machines in the DHCP mode. Make sure the VMWare NAT DHCP server is running. Decide which machine will work as a client and which will work as client. Keep the server virtual machine RAM to 4GB and client may have 2GB/3GB RAM.

It is recommended to use **putty** to configure OpenLDAP as some of the commands are long and some configuration invloves typing multiple lines in a file. Thus instead of typing you can copy paste the configuration from this file. Putty will help you do this easily.
The domain name for OpenLDAP used is demo.lab.

OpenLDAP Server Configuration

Login with a user having sudo permissions.

1. Update the system.

sudo dnf update -y

2. Set the hostname for the server. Domain name in the hostname is compulsory.

sudo hostnamectl set-hostname ldapsrv.demo.lab

```
[admin@ldapsrv ~]$ sudo hostnamectl set-hostname ldapsrv.demo.lab
```

Verify with the **hostname** command.

```
[admin@ldapsrv ~]$ hostname
ldapsrv.demo.lab
[admin@ldapsrv ~]$
```

3. Map the server IP address and hostname in the /etc/hosts file.

sudo vi /etc/hosts

Add following line. But replace your server IP address.

192.168.65.131 ldapsrv.demo.lab ldapsrv

Save the file. The file looks like as shown below.

```
[admin@ldapsrv ~]$ cat /etc/hosts
# Loopback entries; do not change.
# For historical reasons, localhost precedes localhost.localdomain:
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
# See hosts(5) for proper format and other examples:
# 192.168.1.10 foo.example.org foo
# 192.168.1.13 bar.example.org bar
192.168.65.131   ldapsrv.demo.lab  ldapsrv
```

4. verify with following commands

hostname -f
ping -c3 ldapsrv.demo.lab

5. Install the EPEL repository.

sudo dnf install epel-release -y

Once the package is installed, run following command.

sudo dnf update -y

6. Now install the LDAP packages

sudo dnf install openldap-servers openldap-clients -y

7. Now start and enable the OpenLDAP service. Also check the status of the service to confirm that it is started and running. Use following commands.

sudo systemctl start slapd

sudo systemctl enable slapd

sudo systemctl status slapd

8. Open ports/Service for LDAP in the firewall and make it permanent.

sudo firewall-cmd --add-service={ldap,ldaps}

sudo firewall-cmd --add-service={ldap,ldaps} --permanent

verify with

sudo firewall-cmd --list-all

```
[admin@ldapsrv ~]$ sudo firewall-cmd --list-all
[sudo] password for admin:
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client ldap ldaps ssh
```

9. Generate a password for the LDAP manager user (Admin user)

slappasswd

Type your password at the prompt. **Copy the encrypted password starting with {SSHA} and paste it in a file**. You will require it later.

```
[admin@ldapsrv ~]$ slappasswd
New password:
Re-enter new password:
{SSHA}coDc4P611PVkdXxKbTJ+Mq8FyYC4yH7b
[admin@ldapsrv ~]$
```

10. Crate following file and put the given contents. The filename can be aything but the extension should be ldif.

vi changerootpass.ldif

Type following in this file. Copy and paste will be a better option

```
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: <Here Put the above copied password starting with {SSHA}>
```

save the file.

Run the following command.

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f changerootpass.ldif

11. Now run the following commands to import some basic schema .

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

```
[admin@ldapsrv ~]$ sudo  ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
[sudo] password for admin:
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=cosine,cn=schema,cn=config"
```

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

```
[admin@ldapsrv ~]$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=nis,cn=schema,cn=config"
```

sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

```
[admin@ldapsrv ~]$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"
```

12. Restart the OpenLDAP service.

sudo systemctl restart slapd

13. Now create a ldif file to create a base domain in LDAP.

vi setdomain.ldif

Add following content.

```
#setdomain.ldif

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=demo,dc=lab" read by * none
```

```
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=demo,dc=lab

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=demo,dc=lab

dn: olcDatabase={2}mdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: <Put here the copied password starting with {SSHA}>

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

save the file.

The file looks like as shown below.

```
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=demo,dc=lab" read by * none

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=demo,dc=lab

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=demo,dc=lab

dn: olcDatabase={2}mdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW:{SSHA}OuEwcTIIFovG+Q5yLXDg6rrMu5xJT+UY

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

Run following command.

sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f setdomain.ldif

Verify with the following command.

sudo ldapsearch -H ldap:// -x -s base -b "" -LLL "namingContexts"

The output of this command should be as shown below.

```
[admin@ldapsrv ~]$ sudo ldapsearch -H ldap:// -x -s base -b "" -LLL "namingContexts"
[sudo] password for admin:
dn:
namingContexts: dc=demo,dc=lab
```

14. Now create a ldif file to create 2 OU's by name people and group in the LDAP database.

vi addou.ldif

```
# addou.ldif

dn: dc=demo,dc=lab
objectClass: top
objectClass: dcObject
objectclass: organization
o: My ditiss Organisation
dc: ditiss

dn: cn=Manager,dc=demo,dc=lab
objectClass: organizationalRole
cn: Manager
description: OpenLDAP Manager

dn: ou=People,dc=demo,dc=lab
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=demo,dc=lab
objectClass: organizationalUnit
ou: Group
```

save the file.
The file should look like as below.

```
dn: dc=demo,dc=lab
objectClass: top
objectClass: dcObject
objectclass: organization
o: My demo Organisation
dc: demo

dn: cn=Manager,dc=demo,dc=lab
objectClass: organizationalRole
cn: Manager
description: OpenLDAP Manager

dn: ou=People,dc=demo,dc=lab
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=demo,dc=lab
objectClass: organizationalUnit
ou: Group
```

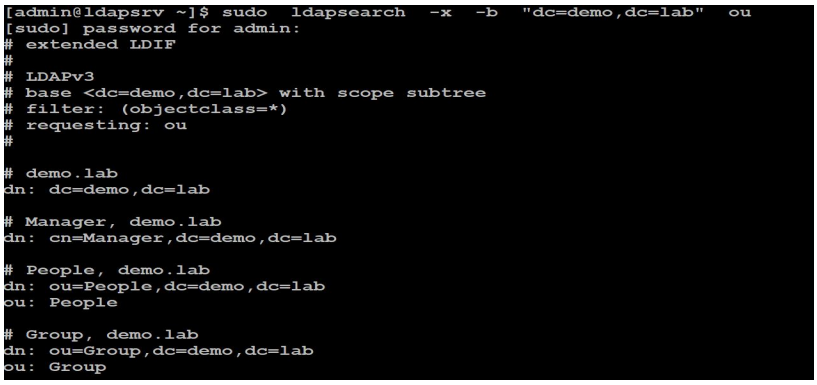
Run following command.

sudo ldapadd -x -D cn=Manager,dc=demo,dc=lab -W -f addou.ldif

Verify using following command.

sudo ldapsearch -x -b "dc=demo,dc=lab" ou

The output should look like



15. Now we will add a user in the LDAP database.

Create a password for the user.

slappasswd

Give the required password and save the encrypted password starting with {SSHA} in a file.

Now create a ldif file to add user.

vi adduser.ldif

```
# adduser.ldif

dn: uid=ldap1,ou=People,dc=demo,dc=lab
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: ldap1
sn: temp
userPassword: {SSHA}m+2H3BPqMSRWqe9Q8nIYCsFERVBDJChn
loginShell: /bin/bash
uidNumber: 2001
gidNumber: 2001
homeDirectory: /home/ldap1
shadowLastChange: 0
shadowMax: 0
shadowWarning: 0

dn: cn=ldap1,ou=Group,dc=demo,dc=lab
objectClass: posixGroup
cn: ldap1
gidNumber: 2001
memberUid: ldap1
```

save the file.

Run the following command to create the user.

sudo ldapadd -x -D cn=Manager,dc=demo,dc=lab -W -f adduser.ldif

Verify with the following command.

sudo ldapsearch -x -b "ou=People,dc=demo,dc=lab"

```
[admin@ldapsrv ~]$ sudo ldapsearch -x -b "ou=People,dc=demo,dc=lab"
[sudo] password for admin:
# extended LDIF
#
# LDAPv3
# base <ou=People,dc=demo,dc=lab> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# People, demo.lab
dn: ou=People,dc=demo,dc=lab
objectClass: organizationalUnit
ou: People

# ldap1, People, demo.lab
dn: uid=ldap1,ou=People,dc=demo,dc=lab
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: ldap1
sn: temp
loginShell: /bin/bash
uidNumber: 2001
gidNumber: 2001
homeDirectory: /home/ldap1
shadowMax: 0
shadowWarning: 0
uid: ldap1
```

The OpenLDAP server configuration is done .
Now you can create OU's and users on this server using the respective ldif files.

############################## Assignment ##############################
Try to create a script to add an OU in the LDAP database.
Try to create a script to add a user in the LDAP database inside a specific OU.
##

OpenLDAP Client Configuration

Login with a user having sudo permissions on the client virtual machine.

1. Update the system.

sudo dnf update -y

2. Set the hostname for the server. Domain name in the hostname is compulsory.

sudo hostnamectl set-hostname ldapcli1.demo.lab

3. Install the EPEL repository.

sudo dnf install epel-release -y

Once the package is installed, run following command.

sudo dnf update -y

4. Now install the LDAP packages. Please follow the sequence of installing the packages as sometimes it may create a problem.

sudo dnf install openldap -y

sudo dnf install openldap-clients -y

sudo dnf install oddjob-mkhomedir -y

sudo dnf install nss-pam-ldapd -y

5. Edit the following file.

sudo vi /etc/nslcd.conf

Modify following lines.

uri ldap://192.168.16.130 **# make sure you type your server IP address here**.
base dc=demo,dc=lab

save the file. The file will look as shown in the below image.

```
17 # Note: %2f encodes the '/' used as directory separator
18 uri ldap://192.168.65.131/
19
20 # The LDAP version to use (defaults to 3
21 # if supported by client library)
22 #ldap_version 3
23
24 # The distinguished name of the search base.
25 base dc=demo,dc=lab
26
27 # The distinguished name to bind to the server with.
28 # Optional: default is to bind anonymously.
29 #binddn cn=proxyuser,dc=example,dc=com
```

6. Edit the following file to enable LDAP authentication on the system.

sudo vi /etc/nsswitch.conf

change the following lines and add ldap as shown below.

passwd: files ldap
group: files ldap

save the file. This is as shown in the following image.

```
# In order of likelihood of use to accelerate lookup.
passwd:     files  systemd ldap
shadow:     files
group:      files [SUCCESS=merge] systemd ldap
hosts:      files  dns myhostname
services:   files
```

7. Start the nslcd service and enable it.

sudo systemctl start nslcd

sudo systemctl enable nslcd

Test the connection with the LDAP server with

sudo getent passwd

the output should display the users and it should contain the ldap1 user at the end as shown in the following image.

```
gnome-initial-setup:x:985:985::/run/gnome-initial-setup/:/s
tcpdump:x:72:72:tcpdump:/:/usr/sbin/nologin
dnsmasq:x:984:984:Dnsmasq DHCP and DNS server:/var/lib/dnsm
n
gnome-remote-desktop:x:982:982:GNOME Remote Desktop:/var/li
op:/usr/sbin/nologin
nslcd:x:65:55:LDAP Client User:/:/sbin/nologin
ldap1:*:2001:2001:ldap1:/home/ldap1:/bin/bash
```

Also verify using following command.

id ldap1

The output will be as shown in the following image.

```
admin@srv2:~$ id ldap1
uid=2001(admin) gid=2001(admin) groups=2001(admin)
```

8. Configure PAM module.

sudo vi /etc/pam_ldap.conf

Type following

uri ldap://192.168.16.130 # type your server IP address
base dc=ditiss,dc=lab
binddn cn=manager,dc=demo,dc=lab
bindpw password **# type your manager password created first in plain text**

Save the file. The file will look as shown below.

```
uri   ldap://192.168.65.131
base dc=demo,dc=lab
binddn cn=manager,dc=demo,dc=lab
bindpw password
```

Restart the nslcd service.

sudo systemctl restart nslcd

Again verify using

id ldap1

sudo getent passwd

9. Now edit the /etc/pam.d/su file. This will configure su utility to use ldap authentication also.

sudo vi /etc/pam.d/su

add following

auth sufficient pam_ldap.so
account sufficient pam_permit.so

Save the file. The file will look like as in the below image.

```
#%PAM-1.0
auth            required        pam_env.so
auth            sufficient      pam_rootok.so
auth            sufficient      pam_ldap.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth           sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth           required        pam_wheel.so use_uid
auth            substack        system-auth
auth            include         postlogin
account         sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account         sufficient      pam_permit.so
account         include         system-auth
password        include         system-auth
session         include         system-auth
session         include         postlogin
session         optional        pam_xauth.so
~
```

Now try with

su - ldap1

User should be able to login but you should get an error about the user home directory not present.

10. Now we will configure oddjob to create home directory for the LDAP users when they login.

Edit the file /etc/pam.d/system-auth

sudo vi /etc/pam.d/system-auth

add following line at the end

session optional pam_oddjob_mkhomedir.so skel=/etc/skel umask=0077

save the file.

The file looks as below.

```
-session    optional                                    pam_systemd.so
session     [success=1 default=ignore]                  pam_succeed_if.so service in crond quiet use_uid
session     required                                    pam_unix.so
session     optional                                    pam_oddjob_mkhomedir.so  skel=/etc/skel umask=0077
~
```

Now add the same line to /etc/pam.d/password-auth

sudo vi /etc/pam.d/password-auth

add following line at the end

session optional pam_oddjob_mkhomedir.so skel=/etc/skel umask=0077
save the file.

Start the oddjobd service.

sudo systemctl start oddjobd

sudo systemctl enable oddjobd

Sudo systemctl status oddjobd

Now again verify using

getent passwd

id ldap1

Now try to login using

su - ldap1

the home directory should be created.

```
admin@srv2:~$ su - ldap1
Password:
Last login: Sun Oct 19 04:30:52 EDT 2025 on tty2
admin@srv2:~$ pwd
/home/ldap1
admin@srv2:~$ whoami
admin
admin@srv2:~$ echo $uid

admin@srv2:~$ ls /home
admin  dbda1  ldap1  sunbeam
admin@srv2:~$ cat /etc/passwd | grep admin
admin:x:2001:2001::/home/admin:/bin/bash
```

As on this client machine there was an admin user with the same uid as ldap1 user, thus it is showing username as admin instead of ldap1.

This is how the LDAP client is also configured.

############################ Assignment ##
A. Add one more client to the LDAP domain.
B. Configure SSH access between clients for LDAP users by modifying /etc/pam.d/sshd file similar to the su file as above.
C. Create a new user on the LDAP server by name ssh1 and confirm
###