OpenLDAP installation steps:

Notes: This HOWTO uses somaliren.org to provide this guide with example values.

Please remember to replace all occurrences of the `somaliren.org` domain name with the domain name of your institution.

convert a Domain Name into a Distinguished Name of LDAP, for example, somaliren.org will be:

`dc=somaliren,dc=org`

On your OpenLDAP server, follow the below steps to install and configure OpenLDAP server:

Step 1: Update your server

```
sudo apt-get update
```

Step 2: Install OpenLDAP

```
sudo apt-get install slapd ldap-utils -y
```

Step 3:Reconfiguring OpenLDAP

```
sudo dpkg-reconfigure slapd
```

Answer the following questions:

```
omit OpenLDAP configuration: no
DNS domain name: somaliren.org
Organization name: SomNOG
Administration password: somnog
Cofirm password: somnog
Database backend: MDB
Do you the database to be removed when slapd is purged: yes
Move olda database: yes
Allow LDAP v2 protocol: no
```

Step 3: Start your Openldap Database and ensure It is working with commands as below.

```
sudo systemctl start slapd
sudo ps -ef | grep slapd
```

To test it run:

```
ldapsearch -x
```

Use ldapsearch as follows to query our newly added domain, somaliren.org

```
ldapsearch -x -LLL -H ldap:/// -b dc=somaliren,dc=org dn
```

The following command will query the default content for somaliren.org:

```
ldapsearch -x -LLL -b dc=somaliren,dc=org
```

Step 4: Creating a base Ldif file

Create a file with content below for your base directory structure.

```
nano base.ldif
```

add the following:

```
ou: Groups
objectClass: top
objectClass: organizationalUnit

dn: ou=Users,dc=somaliren,dc=org
ou: Users
objectClass: top
objectClass: organizationalUnit
```

Step 5: Upload your base LDIF file to LDAP

Run the command below to upload your base ldif file into the LDAP server

```
ldapadd -x -W -D "cn=admin,dc=somaliren,dc=org" -f base.ldif
```

Supplied your LDAP password and you should see feedback as below:

```
adding a new entry "ou=Groups,dc=somaliren,dc=org"

adding a new entry "ou=Users,dc=somaliren,dc=org"
```

Step 6: Creating a person Ldif file:

Create a file with content below for your base directory structure.

```
nano person.ldif
```

add the following content:

```
dn: cn=biixi,ou=Groups,dc=somaliren,dc=org
cn: biixi
gidNumber: 4001
objectClass: posixGroup

dn: uid=biixi,ou=Users,dc=somaliren,dc=org
uid: biixi
uidNumber: 4001
gidNumber: 4001
cn: Abdullahi Biixi
sn: Biixi
objectClass: posixAccount
objectClass: organizationalPerson
loginShell: /bin/bash
homeDirectory: /home/biixi
```

Step 7: Upload your person LDIF file to LDAP

Run the command below to upload your base ldif file into the LDAP server

```
ldapadd -x -W -D "cn=admin,dc=somaliren,dc=org" -f person.ldif
```

Supplied your LDAP password and you should see feedback as below, waa in sidaan o kale noqotaa:

```
adding a new entry: "cn=biixi,ou=Groups,dc=somaliren,dc=org"

adding a new entry: "cn=biixi,ou=Groups,dc=somaliren,dc=org"
```

Step 8: Setting up user credentials

Run the command below create a password for the user account created.

```
sudo ldappasswd -s somnog123 -W -D "cn=admin,dc=somaliren,dc=org" -x
"uid=biixi,ou=Users,dc=somaliren,dc=org"
```

Step 9: Check your LDAP directory structure

Run the command below to check your uploaded ldif files forming your LDAP directory structurein your database.

```
sudo slapcat
```

You should see entire OpenLdap database

At this point, the LDAP server is working, and we now focus on configuring the clients.

Go to your client, and follow the below steps:

Step 10: Adding ubuntu server logins with LDAP as a client

10.1: 1. We will need to install the LDAP client-side package on the client system. This package will install all the required tools to authenticate with the remote LDAP server:

```
sudo apt-get update -y &&
sudo apt-get install ldap-auth-client nscd -y
```

10.2. The installation process will ask you some questions regarding your LDAP server and its authentication details. Answer those questions as follows:

LDAP server URI: ldap://you-LDAP-server-IP: Make sure you change the protocol line from ldapi:/// to ldap:// NB: ka dhig ldap://

Distinguished name of search base: Match this to the domain set on the LDAP server in the format dc=somaliren,dc=org

LDAP version to use: 3 Make local root database admin: Yes

Does LDAP database require login: No

LDAP account for root: cn=admin,dc=somaliren,dc=org

LDAP root account password: The password for the LDAP admin account, use your password.

10.3. Next, we need to change the authentication configuration to check with the LDAP server:

```
sudo nano /etc/nsswitch.conf
```

Add ldap after the files, like this:

```
Passwd: files ldap
group: files ldap
shadow: files ldap
```

10.4 Next, add the following line to /etc/pam.d/common-session. This will create a local home directory for LDAP users.

Edit the common-session file:

```
nano /etc/pam.d/common-session
```

and add the following line at the end of the file, to go to the end of the file use this shortcut, ctrl + w then ctrl + w:

session required pam_mkhomedir.so umask=0022 skel=/etc/skel

Now restart the nscd service with the following command:

```
sudo /etc/init.d/nscd restart
```

To test it while logged in on your client machine, we will need to switch your user to the user we created during the OpenLDAP server:

```
First check that this user does not exist in your local machine, in the guide we
create a user called biixi, if you changed it, use your own user:
```

```
cat /etc/passwd | grep biixi
```

```
You should not see any entry for user biixi in the passwd file.
```

Then switch your user to biixi and after running the following, the system should prompt a password for the user to login:

```
su - biixi
```

Congratulations! If you managed to login biixi with your client machine. You have a working centralized identity service.