esprit

Ecole Supérieure Privée
d'Ingénierie et de Technologies

Install and configure OpenLDAP on Ubuntu

Services and Networks administration

Esprit 23-24

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.

Step1: Update and Upgrade

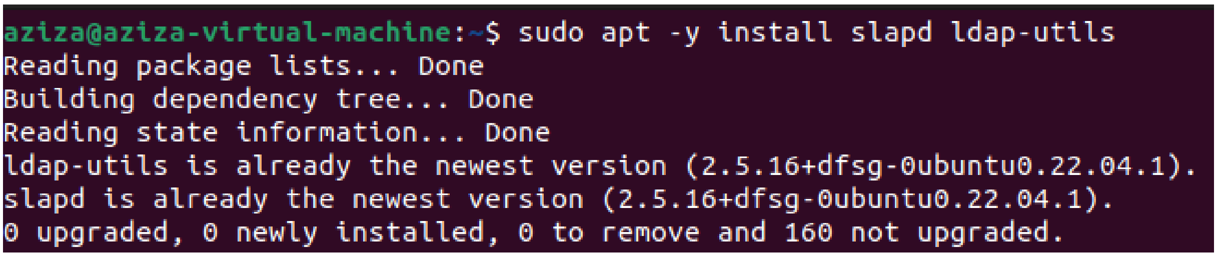
The first step is to ensure that your system is up to date. Open a terminal and run the following commands:

```
sudo apt-get update
```

Step2: Install OpenLDAP packages

Execute the command below to OpenLDAP on Ubuntu 22.04. In order to continue the installation process, you should enter your system password (you will be prompted to enter the pwd)

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



```
aziza@aziza-virtual-machine:~$ sudo apt -y install slapd ldap-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ldap-utils is already the newest version (2.5.16+dfsg-0ubuntu0.22.04.1).
slapd is already the newest version (2.5.16+dfsg-0ubuntu0.22.04.1).
0 upgraded, 0 newly installed, 0 to remove and 160 not upgraded.
```

Step3: Configuration of OpenLDAP

Configuring OpenLDAP involves several steps, including setting up the basic configuration, defining the directory structure, and configuring access control.

Step 3.1: Stop the LDAP Service

Before making changes to the configuration, stop the OpenLDAP service:

```
Sudo service slapd stop
```

Step 3.2: Configure OpenLDAP Server

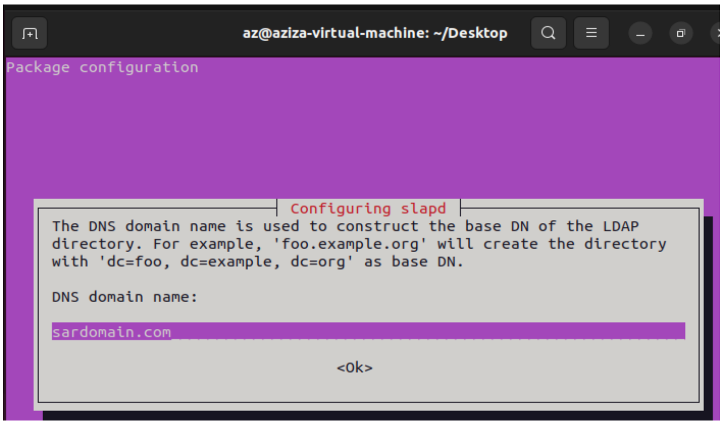
To start configuring the OpenLDAP server, run the following command.

```
sudo dpkg-reconfigure slapd
```

This command will reconfigure the main OpenLDAP package \slapd\ and you will be asked for some of the basic OpenLDAP configurations

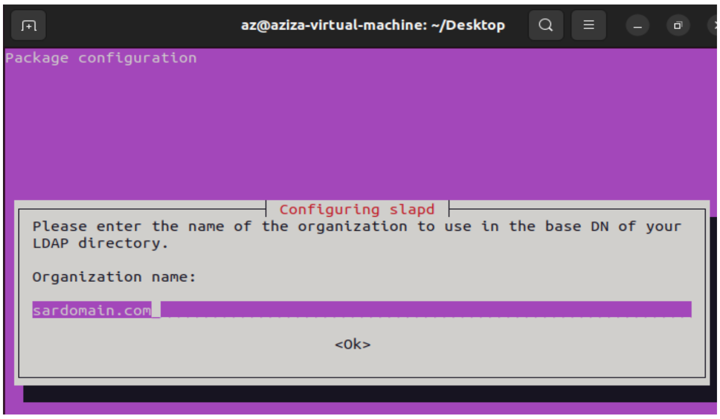
When you are prompted to Omit OpenLDAP server configuration, select **No**, in order to configure the OpenLDAP server with a new configuration file and database.

Enter the domain name of your OpenLDAP installation and select **Ok**. This domain name will be used as the DN (Distinguished Name) of your OpenLDAP server. In our case, the domain name is **sardomain.com**, and the DN is **dc=sardomain,dc=com**.



```
Package configuration

Configuring slapd
The DNS domain name is used to construct the base DN of the LDAP
directory. For example, 'foo.example.org' will create the directory
with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

sardomain.com

<Ok>
```

Enter the organization name that will be used in the DN.We will keep it **sardomain.com**, in our case.

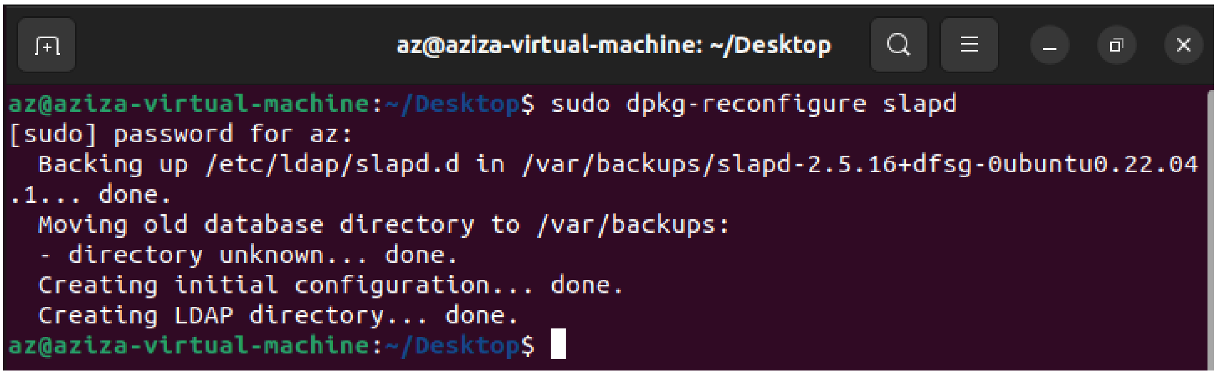


```
Package configuration

Configuring slapd
Please enter the name of the organization to use in the base DN of your
LDAP directory.

Organization name:

sardomain.com

<Ok>
```

Then, you will be asked to introduce the admin of your LDAP system.

Select **Yes twice** when you are prompted to remove database when slapd is purged and to move old database before creating a new one.

Finally, the configuration is done.



```
az@aziza-virtual-machine:~/Desktop$ sudo dpkg-reconfigure slapd
[sudo] password for az:
  Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.16+dfsg-0ubuntu0.22.04
.1... done.
  Moving old database directory to /var/backups:
  - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
az@aziza-virtual-machine:~/Desktop$
```

After reconfiguring the **slapd** package, modify the configuration file **/etc/ldap/ldap.conf** using the command below

```
sudo nano /etc/ldap/ldap.conf
```

Uncomment the two lines **Base** and **URI** and enter our domain name of our OpenLDAP server, as follows:

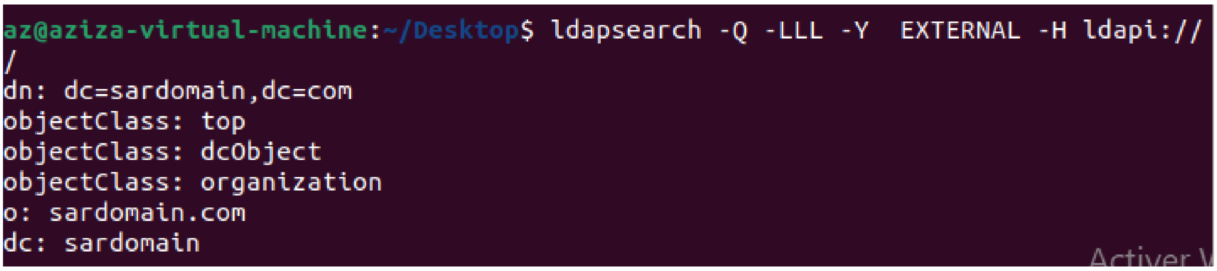
```
BASE dc=sardomain,dc=com
URI  ldap://localhost:389
```

After saving the modifications, restart the LDAP service and be sure that it is active.

```
Systemctl restart slapd
Systemctl status slapd
```

In order to check the basic configuration of OpenLDAP, execute the following command line. The DN should be like /dn: dc= sardomain,dc=com/

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:///
```

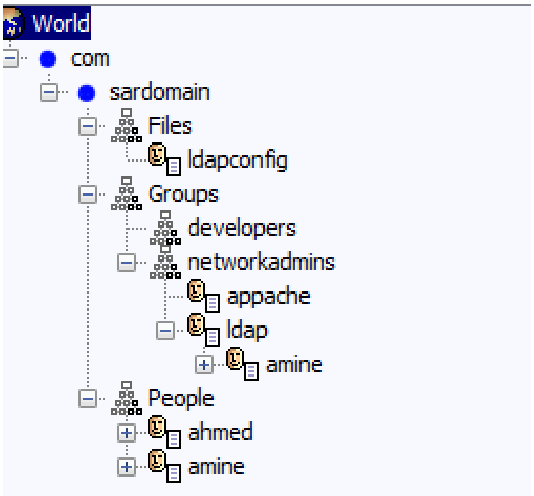


```
az@aziza-virtual-machine:~/Desktop$ ldapsearch -Q -LLL -Y  EXTERNAL -H ldapi://
/
dn: dc=sardomain,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: sardomain.com
dc: sardomain
```

Step4: Creation of the directory structure

After configuring the base DN of the OpenLDAP server, we will now create a new penLDAP user base group.

In this Lab we will create the following DIT:



We will create three organizational units **Groups**,**Files** and **People** to store the groups, the files and the users, respectively, of our OpenLDAP server.

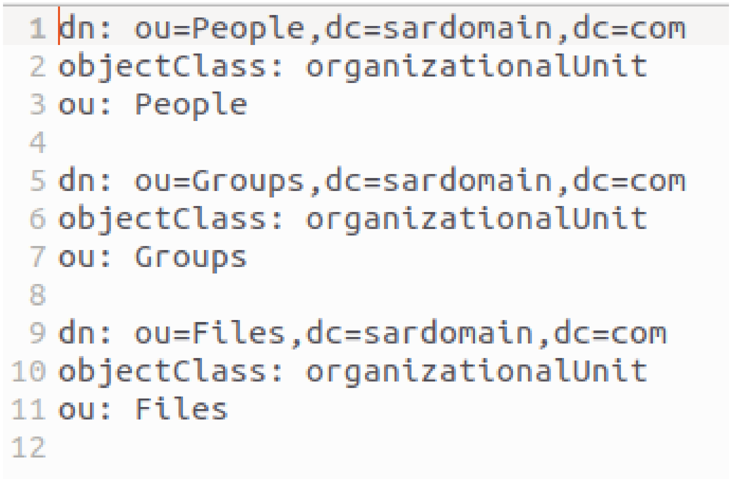
To create new LDAP content, we will use the LDIF file and the LDAP tool ldapadd.

Step 4.1: Creation of Goups,Files and People

1. Create a file named **base-groups.ldif** using this command:

```
sudo nano base-groups.ldif
```

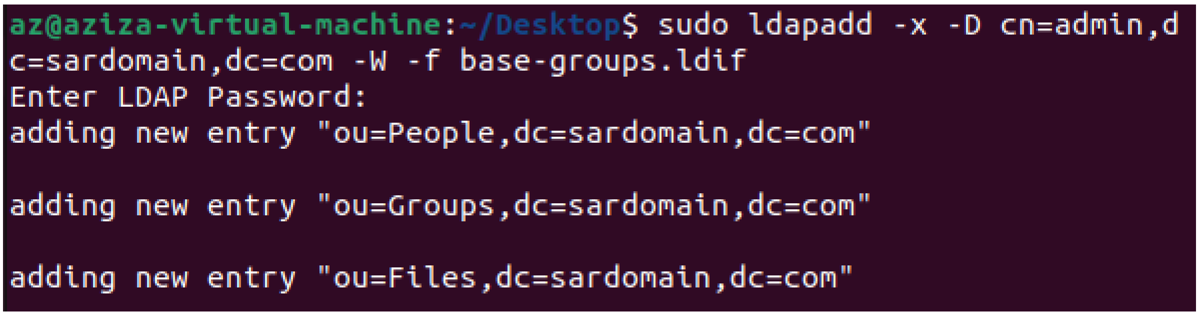
2. Add the following content



```
dn: ou=People,dc=sardomain,dc=com
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=sardomain,dc=com
objectClass: organizationalUnit
ou: Groups

dn: ou=Files,dc=sardomain,dc=com
objectClass: organizationalUnit
ou: Files

```

3. Execute the command line **ldapadd**, and enter the password of the LDAP admin in order to add new entries.

```
sudo ldapadd -x -D cn=admin,dc=sardomain,dc=com -W -f base-groups.ldif
```



```
az@aziza-virtual-machine:~/Desktop$ sudo ldapadd -x -D cn=admin,d
c=sardomain,dc=com -W -f base-groups.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=sardomain,dc=com"

adding new entry "ou=Groups,dc=sardomain,dc=com"

adding new entry "ou=Files,dc=sardomain,dc=com"
```

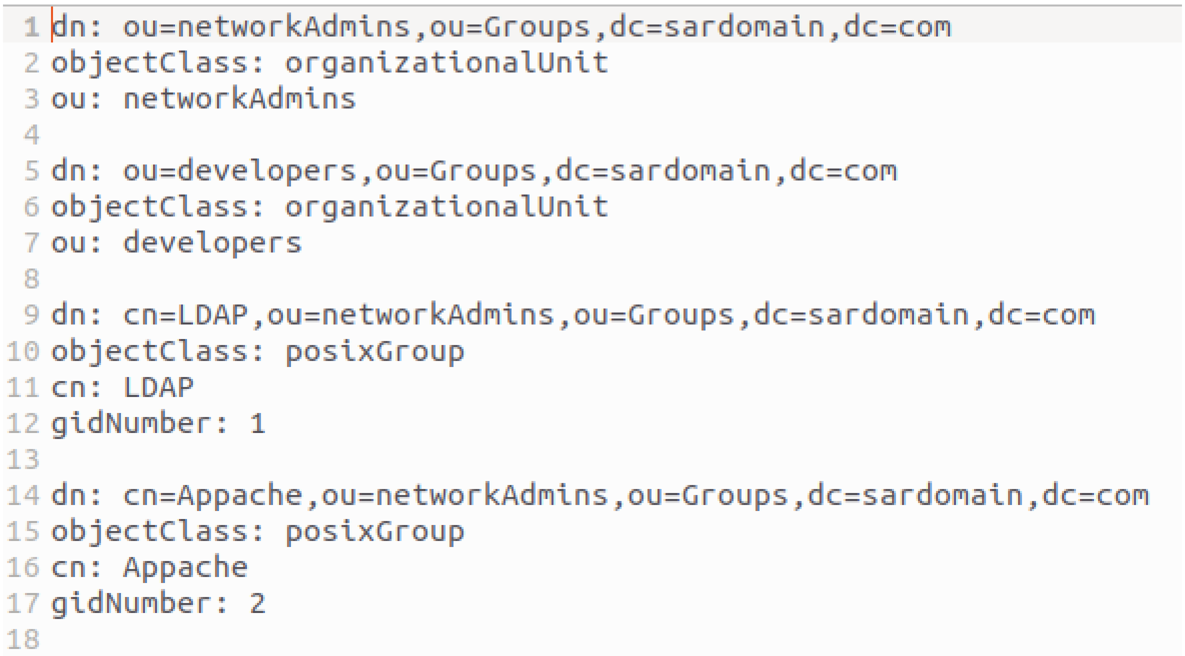
Step 4.2: Creation of Groups

In our base, we will create two main groups “**developers**” and “**networkadmins**” that contains two other groups “**LDAP**” and “**apache**”.

1. Create a file named **add-groups.ldif** using this command:

```
sudo nano add-groups.ldif
```

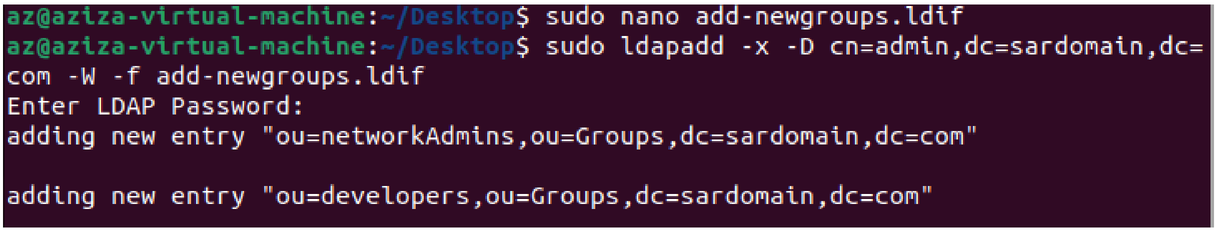
2. Add the following content:



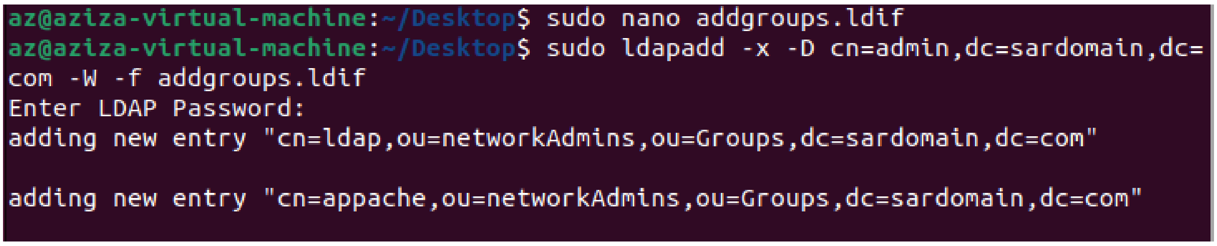
```
dn: ou=networkAdmins,ou=Groups,dc=sardomain,dc=com
objectClass: organizationalUnit
ou: networkAdmins

dn: ou=developers,ou=Groups,dc=sardomain,dc=com
objectClass: organizationalUnit
ou: developers

dn: cn=LDAP,ou=networkAdmins,ou=Groups,dc=sardomain,dc=com
objectClass: posixGroup
cn: LDAP
gidNumber: 1

dn: cn=Appache,ou=networkAdmins,ou=Groups,dc=sardomain,dc=com
objectClass: posixGroup
cn: Appache
gidNumber: 2

```

3. Execute the command line **ldapadd**, and enter the password of the LDAP admin in order to add new entries.

```
sudo ldapadd -x -D cn=admin,dc=sardomain,dc=com -W -f add-groups.ldif
```



```
az@aziza-virtual-machine:~/Desktop$ sudo nano add-newgroups.ldif
az@aziza-virtual-machine:~/Desktop$ sudo ldapadd -x -D cn=admin,dc=sardomain,dc=
com -W -f add-newgroups.ldif
Enter LDAP Password:
adding new entry "ou=networkAdmins,ou=Groups,dc=sardomain,dc=com"

adding new entry "ou=developers,ou=Groups,dc=sardomain,dc=com"
```



```
az@aziza-virtual-machine:~/Desktop$ sudo nano addgroups.ldif
az@aziza-virtual-machine:~/Desktop$ sudo ldapadd -x -D cn=admin,dc=sardomain,dc=
com -W -f addgroups.ldif
Enter LDAP Password:
adding new entry "cn=ldap,ou=networkAdmins,ou=Groups,dc=sardomain,dc=com"

adding new entry "cn=appache,ou=networkAdmins,ou=Groups,dc=sardomain,dc=com"
```

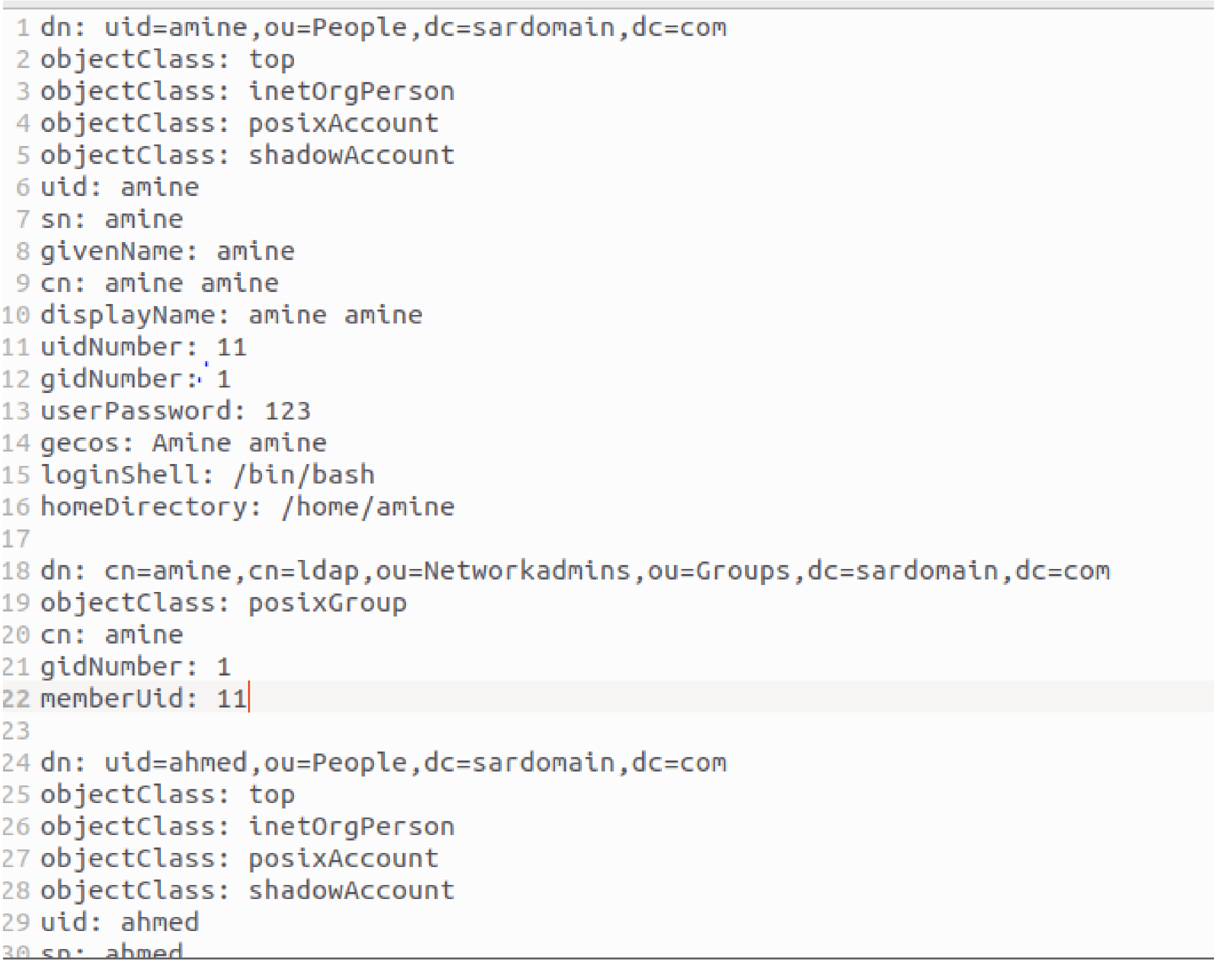
Step 4.1: Creation of users

We will add two users “Ahmed” et “Amine”. The user “Amine” is a member of the group “NetworkAdmins”.

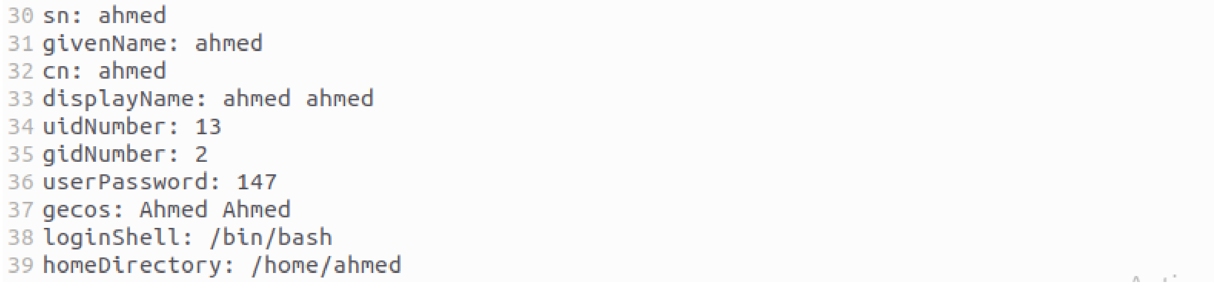
1. Create a file named **add-users.ldif** using this command:

```
sudo nano add-users.ldif
```

2. Add the following content



```
dn: uid=amine,ou=People,dc=sardomain,dc=com
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: amine
sn: amine
givenName: amine
cn: amine amine
displayName: amine amine
uidNumber: 11
gidNumber: 1
userPassword: 123
gecos: Amine amine
loginShell: /bin/bash
homeDirectory: /home/amine

dn: cn=amine,cn=ldap,ou=Networkadmins,ou=Groups,dc=sardomain,dc=com
objectClass: posixGroup
cn: amine
gidNumber: 1
memberUid: 11

dn: uid=ahmed,ou=People,dc=sardomain,dc=com
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: ahmed
```

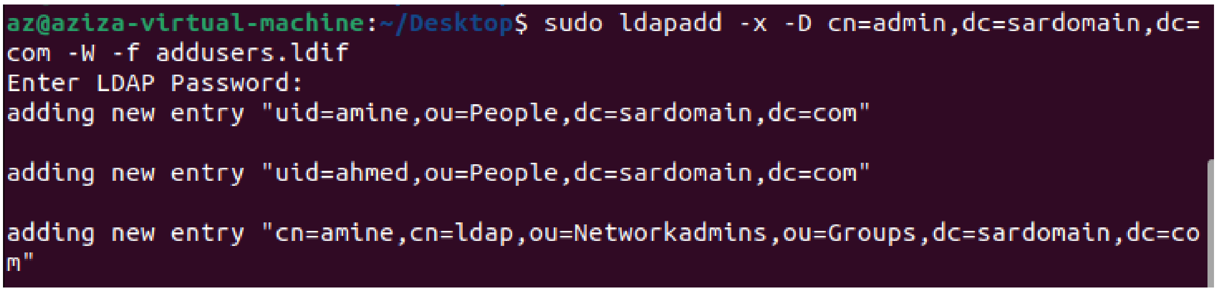


```
sn: ahmed
givenName: ahmed
cn: ahmed
displayName: ahmed ahmed
uidNumber: 13
gidNumber: 2
userPassword: 147
gecos: Ahmed Ahmed
loginShell: /bin/bash
homeDirectory: /home/ahmed
```

PS: You ca generate a password hash to be used as a user password using the following command `sudo slappasswd`

3. Execute the command line **ldapadd**, and enter the password of the LDAP admin in order to add new entries.

```
sudo ldapadd -x -D cn=admin,dc=sardomain,dc=com -W –f add-users.ldif
```



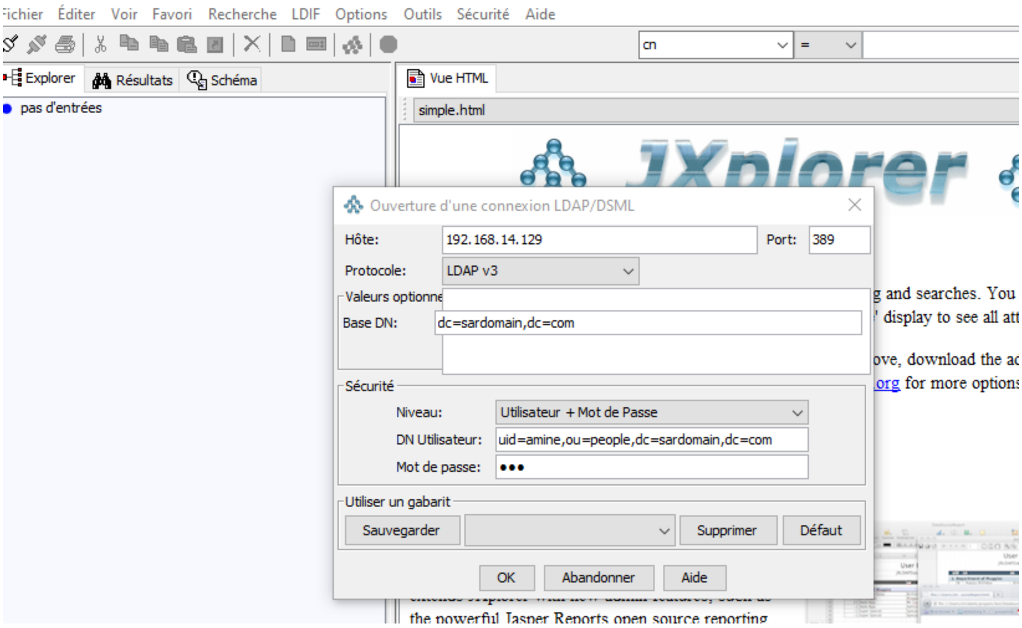
```
az@aziza-virtual-machine:~/Desktop$ sudo ldapadd -x -D cn=admin,dc=sardomain,dc=
com -W -f addusers.ldif
Enter LDAP Password:
adding new entry "uid=amine,ou=People,dc=sardomain,dc=com"

adding new entry "uid=ahmed,ou=People,dc=sardomain,dc=com"

adding new entry "cn=amine,cn=ldap,ou=Networkadmins,ou=Groups,dc=sardomain,dc=co
m"
```

Step5: Test

To test the server with your VM and show the DIT of our LDAP server, execute this command

```
ldapsearch -x -LLL -b dc=sardomain,dc=com
```

To test with your windows host, install jxplorer Application and try to connect to the ldap server: http://jxplorer.org/downloads/users.html .



Ouverture d'une connexion LDAP/DSML

Hôte: 192.168.14.129 Port: 389

Protocole: LDAP v3

Valeurs optionne

Base DN: dc=sardomain,dc=com

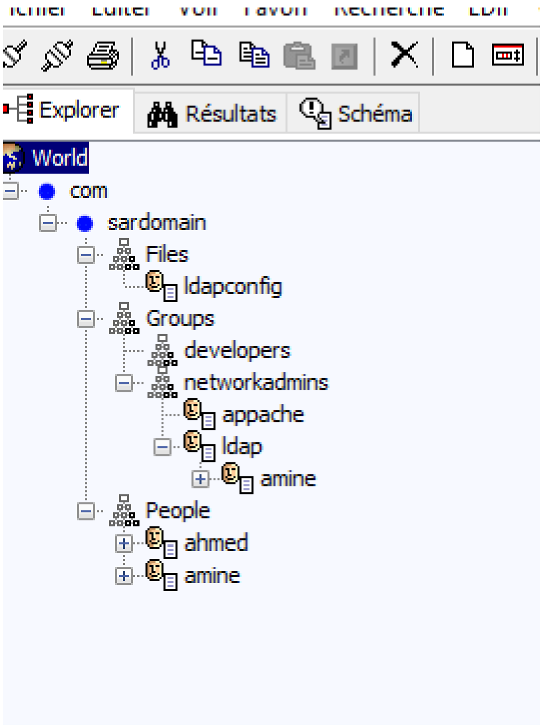
Sécurité

Niveau: Utilisateur + Mot de Passe

DN Utilisateur: uid=amine,ou=people,dc=sardomain,dc=com

Mot de passe: •••

Utiliser un gabarit



```
World
⊟ com
    ⊟ sardomain
        ⊟ Files
            ldapconfig
        ⊟ Groups
            developers
            ⊟ networkadmins
                appache
                ⊟ ldap
                    ⊞ amine
        ⊟ People
            ⊞ ahmed
            ⊞ amine
```