IAM Assignment

OpenLDAP

Done by

Aravind Kumar (MSc. Computer Security)

OpenLDAP

It is a free, open-source implementation of the Lightweight Directory Access Protocol (LDAP) developed by the OpenLDAP Project. It is released under its own BSD-Style license called OpenLDAP Public License.

LDAP is a platform-independent protocol. Several common Linux distributions include OpenLDAP software for LDAP support.

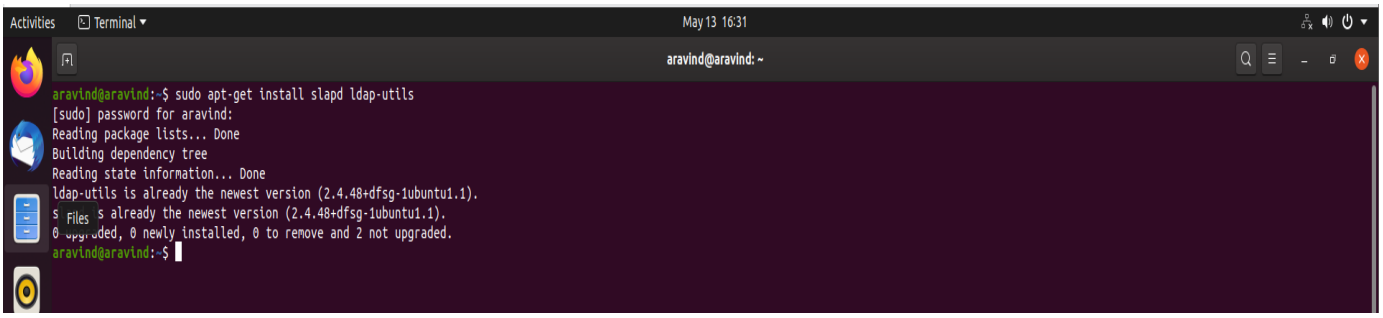
The following are the steps which we are going to follow for installing the OpenLDAP in Ubuntu OS and configure it.

Steps for installation

Step 1

Install LADP using the following command

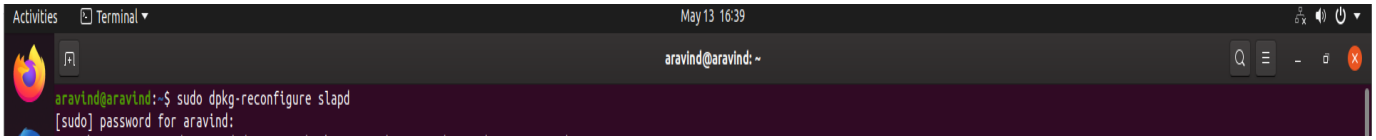
Command - sudo apt-get install slapd ldap-utils



Step 2

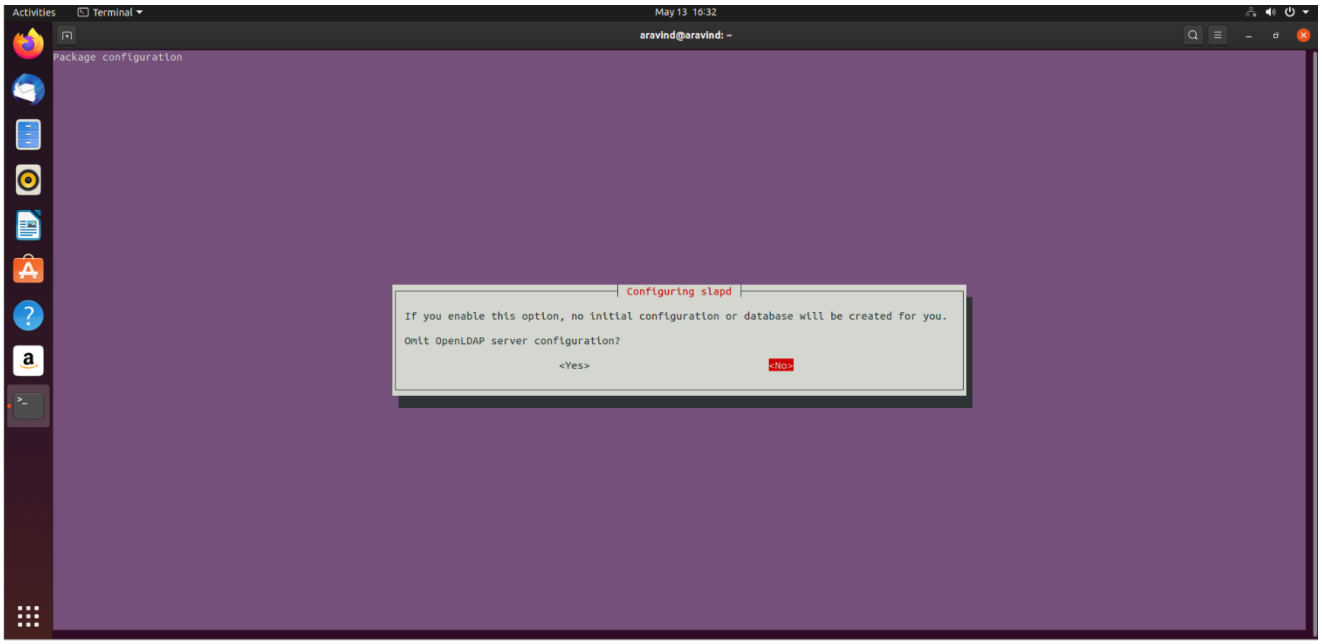
- Now we are going to reconfigure the package even though we just installed it.
- The slapd package has the ability to ask a lot of important configuration questions, but by default they are skipped over in the installation process.

Command - sudo dpkg-reconfigure slapd

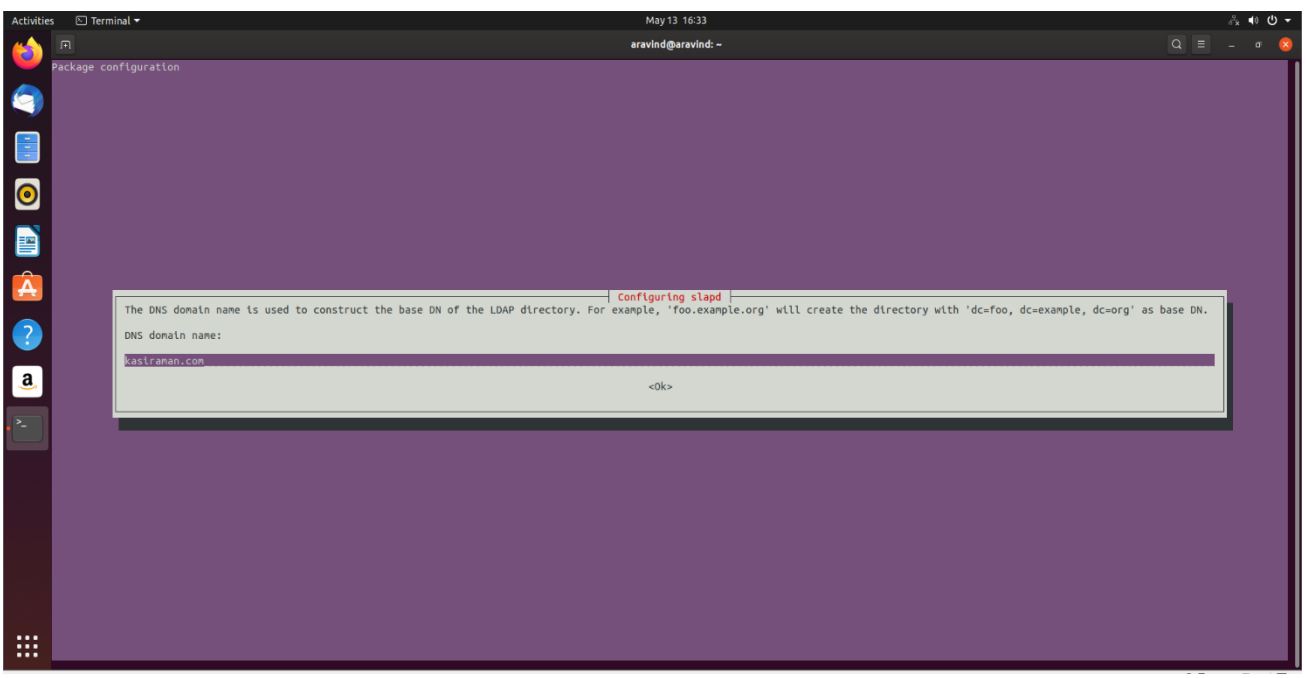


There will be new screen with questions we need to answer for this process.

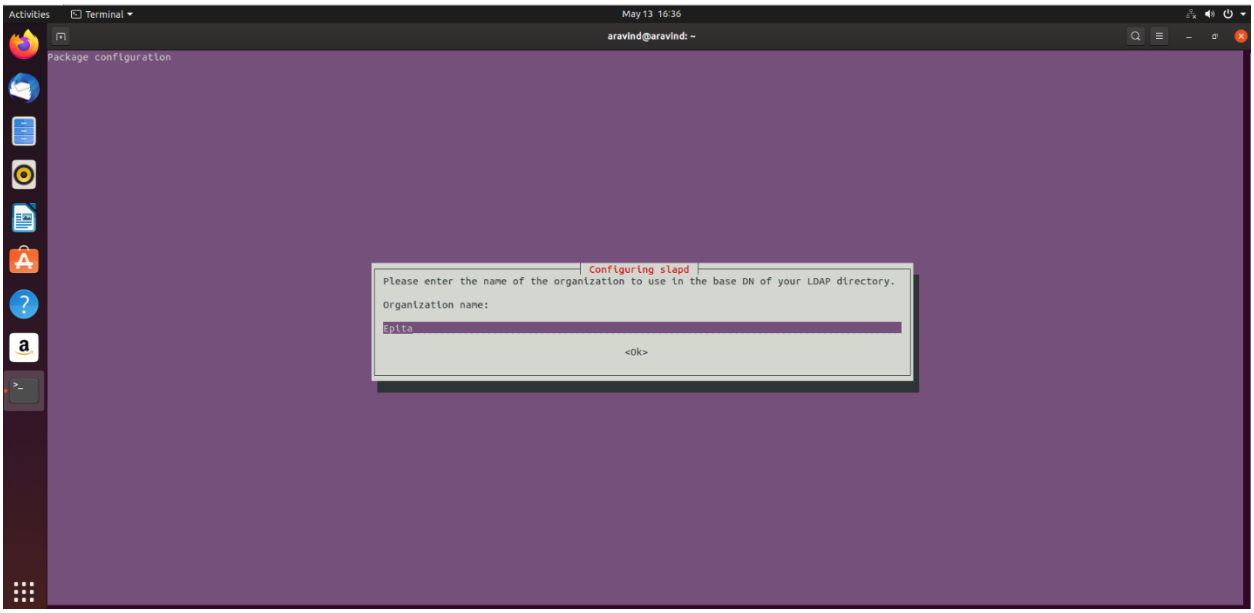
- **Omit OpenLDAP server configuration?** – No



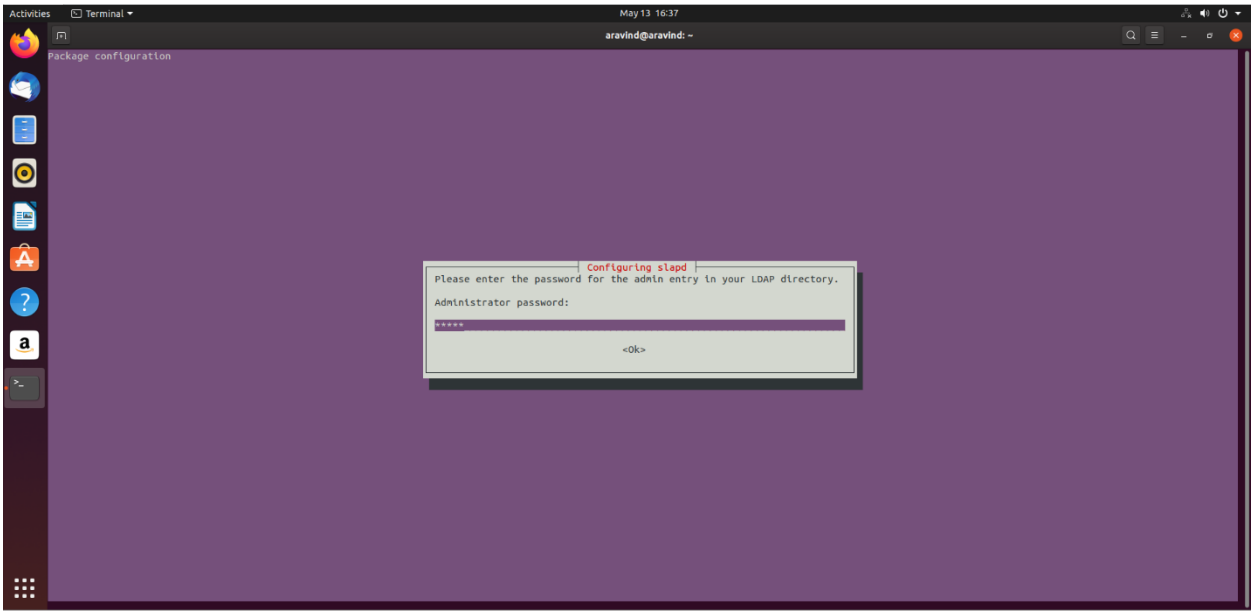
- **DNS domain name** – give your last_name (as per my project) or any name of your choice

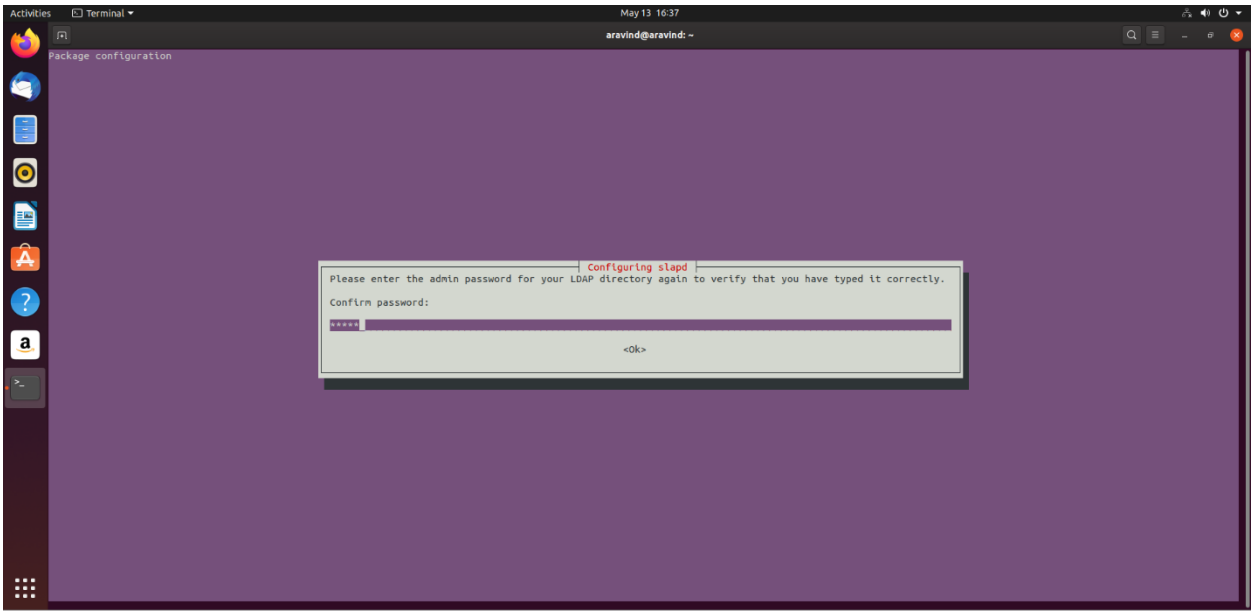


- **Organization name** – Epita (as per my project) you can give any name

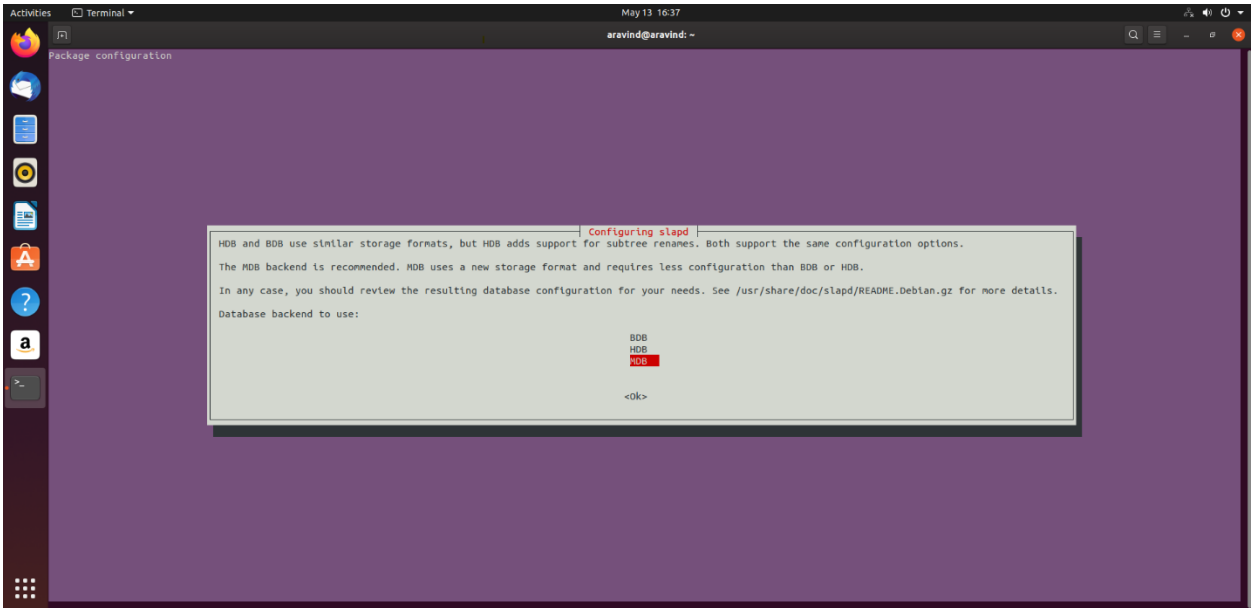


- **Administrator password –** give a password and confirm it again

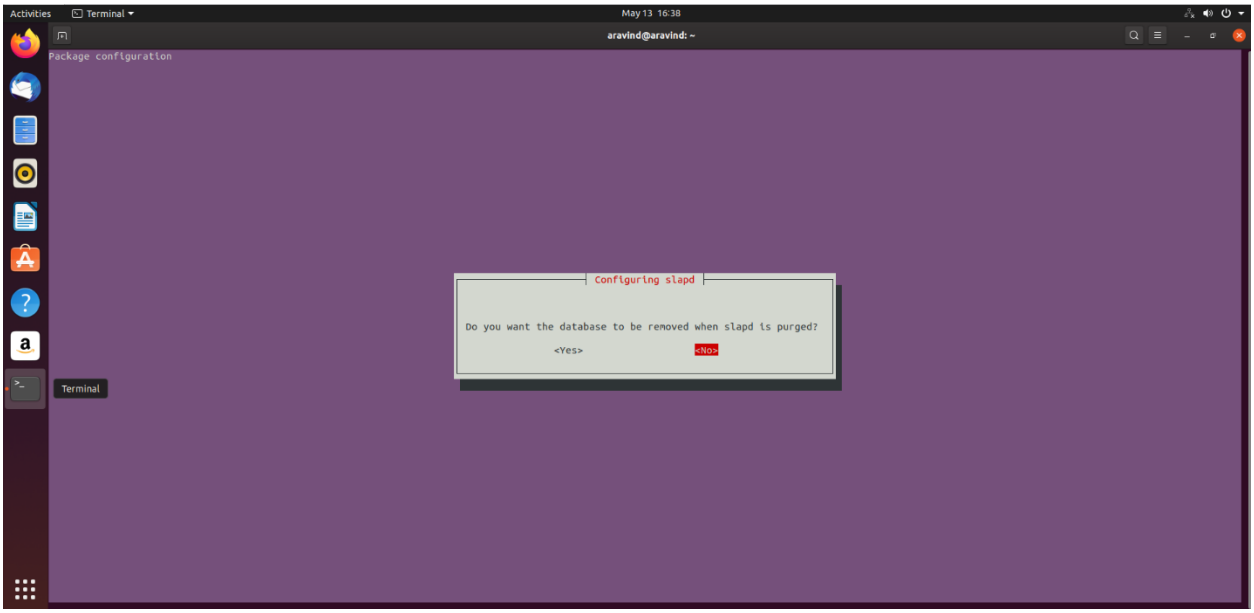




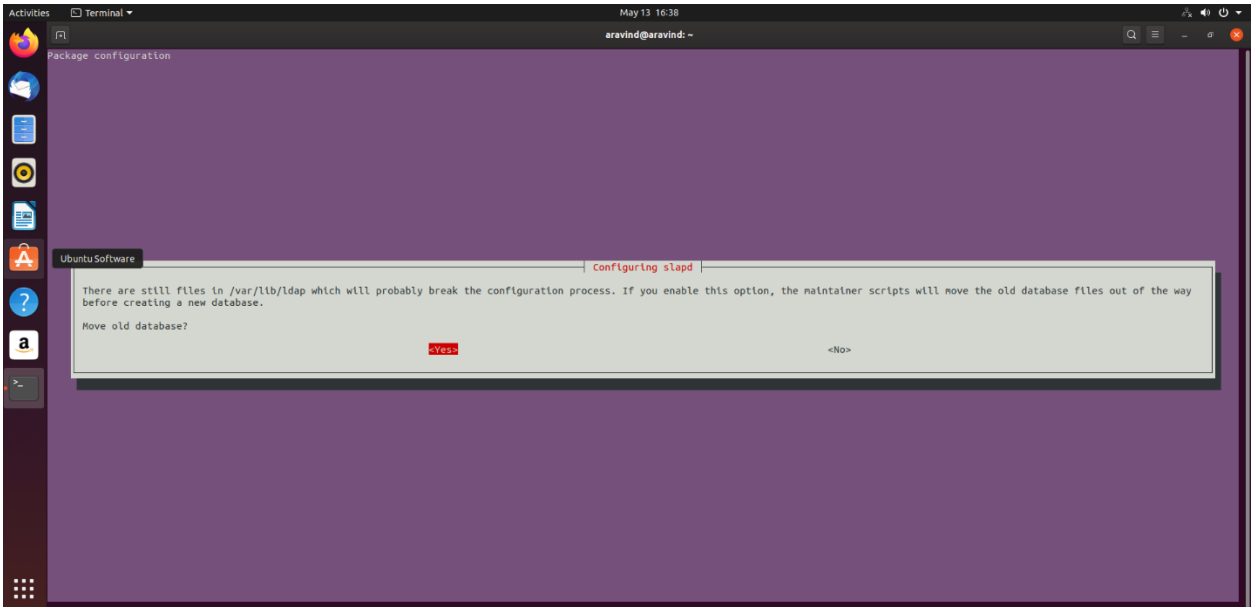
- **Database backend-** MDB



- **Remove the database when slapd is purged? –** No



- **Move old database? –** Yes



Step 3

Once all the steps are done, we now are going to perform the configuration verification checks

Command - sudo slapcat

```
aravind@aravind:~$ sudo slapcat
dn: dc=kasiraman,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: Epita
d
s                                  lass: organization
entryUUID: 36c7e162-2973-103a-8051-d1801aff8744
creatorsName: cn=admin,dc=kasiraman,dc=com
createTimestamp: 20200513143854Z
entryCSN: 20200513143854.126416Z#000000#000#000000
modifiersName: cn=admin,dc=kasiraman,dc=com
modifyTimestamp: 20200513143854Z

dn: cn=admin,dc=kasiraman,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9NStKYjBYQWZKaDRQbDNFL01LR1V5ZDRvb0lrSyt2cHg=
structuralObjectClass: organizationalRole
entryUUID: 36c8396e-2973-103a-8052-d1801aff8744
creatorsName: cn=admin,dc=kasiraman,dc=com
createTimestamp: 20200513143854Z
entryCSN: 20200513143854.128739Z#000000#000#000000
modifiersName: cn=admin,dc=kasiraman,dc=com
modifyTimestamp: 20200513143854Z
```

The above command will print all the directory entries.

Step 4

Now we are going to check the config DIT

Command - sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn

-Q: enable silent mode for SASL authentication

-Y: pick the SASL mode chosen for authentication. Normally, EXTERNAL implies an authentication by client certificate but in this case, it means that the authentication will be done by the UID and the GID of the system account. This is why you have to launch the command with “sudo”.

-L: choose to display the result in LDIF format. We could have said -LLL to have the same thing without all the lines commented.

-H: indicates the URI we want to use to connect. Here ldapi:/// says to connect to the Unix socket locally (communication goes through a local file rather than over the network).

-b: indicates the node from which you want to search. Here "dc= kasiraman,dc=com" is the root so you search throughout the DIT.

```
aravind@aravind:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn
dn: cn=config

dn: cn=module{0},cn=config

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: olcBackend={0}mdb,cn=config

dn: olcDatabase={-1}frontend,cn=config

dn: olcDatabase={0}config,cn=config

dn: olcDatabase={1}mdb,cn=config

aravind@aravind:~$
```

Step 5

In this step we are going to start the logging of slapd. But first we need to check the existing log level of slapd.

Command - sudo ldapsearch -Q -L -Y EXTERNAL -H ldapi:/// -s base -b cn=config olcLogLevel

```
aravind@aravind:~$ sudo ldapsearch -Q -L -Y EXTERNAL -H ldapi:/// -s base -b cn=config olcLogLevel
version: 1

#
# LDAPv3
# base <cn=config> with scope baseObject
# filter: (objectclass=*)
# requesting: olcLogLevel
#

# config
dn: cn=config
olcLogLevel: none

# search result

# numResponses: 2
# numEntries: 1
aravind@aravind:~$
```

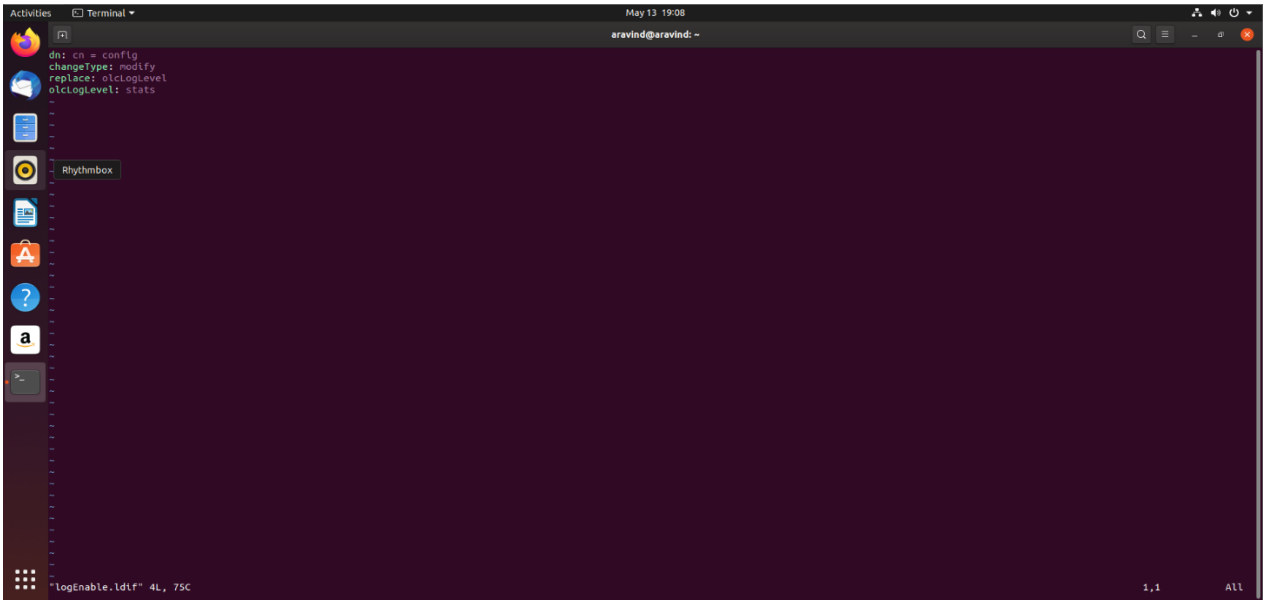
Once we check the existing level of the slapd we are going to start the logging of slapd and enable them

Command – nano/vim logEnable.ldif

Once we created the file, we need to manually enter the following commands lines listed below

Command -

dn: cn = config
changeType: modify
replace: olcLogLevel
olcLogLevel: stats



Step 6

Now we are going to apply the changes in the logEnable.ldif file

Command - sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f logEnable.ldif

Once we have enabled, the server will start generating logs, but it will be generated to the path **"/var/log/syslog"**.

In order to create a separate log file, we need to create a rsyslog daemon

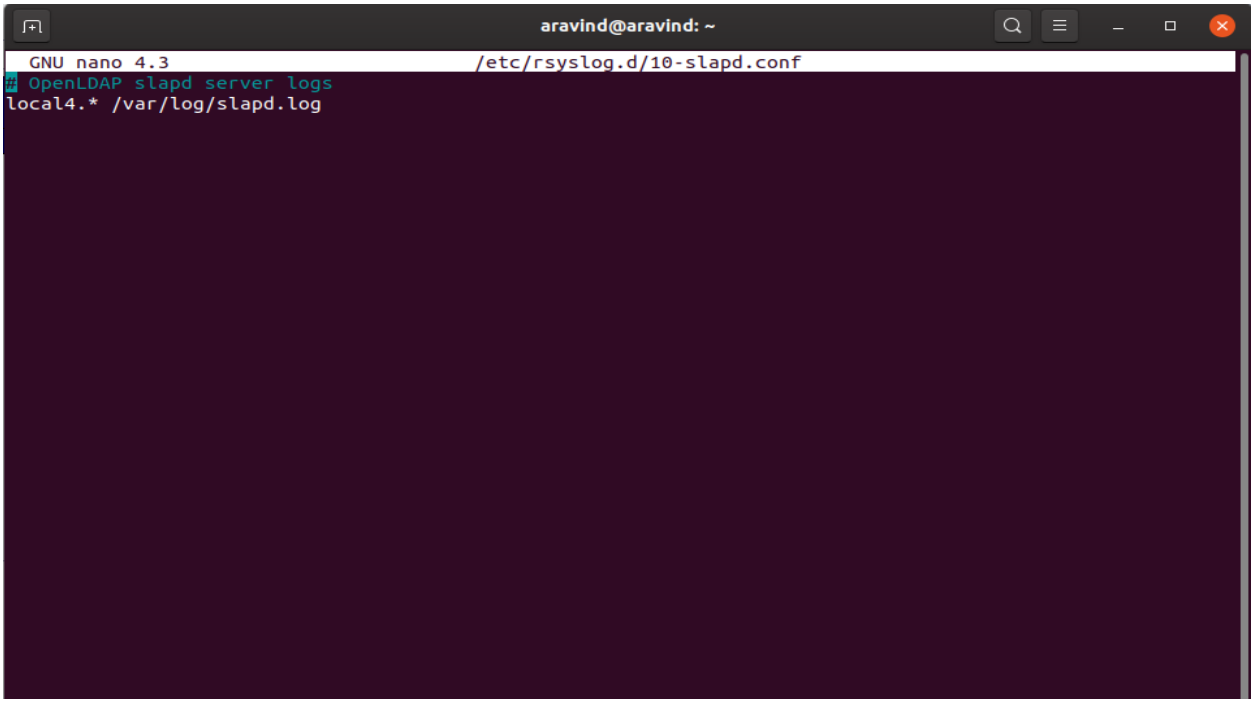
Command – sudo nano /etc/rsyslog.d/10-slapd.conf

Once created and entered into the file we need to enter the following lines as listed below

Command -

OpenLDAP slapd server logs

local4.* /var/log/slapd.log



Once done save the file. The above file will now create a separate log for the slapd server logs instead of saving in **"/var/log/syslog".**

Now we need to restart the rsyslog

Command - sudo systemctl restart rsyslog

Step 7

Once done with the logging we need to create new entries for the ldap. For that we need to create a file called as treekasiraman.ldif (as per my project)

Command – nano treekasiraman.ldif

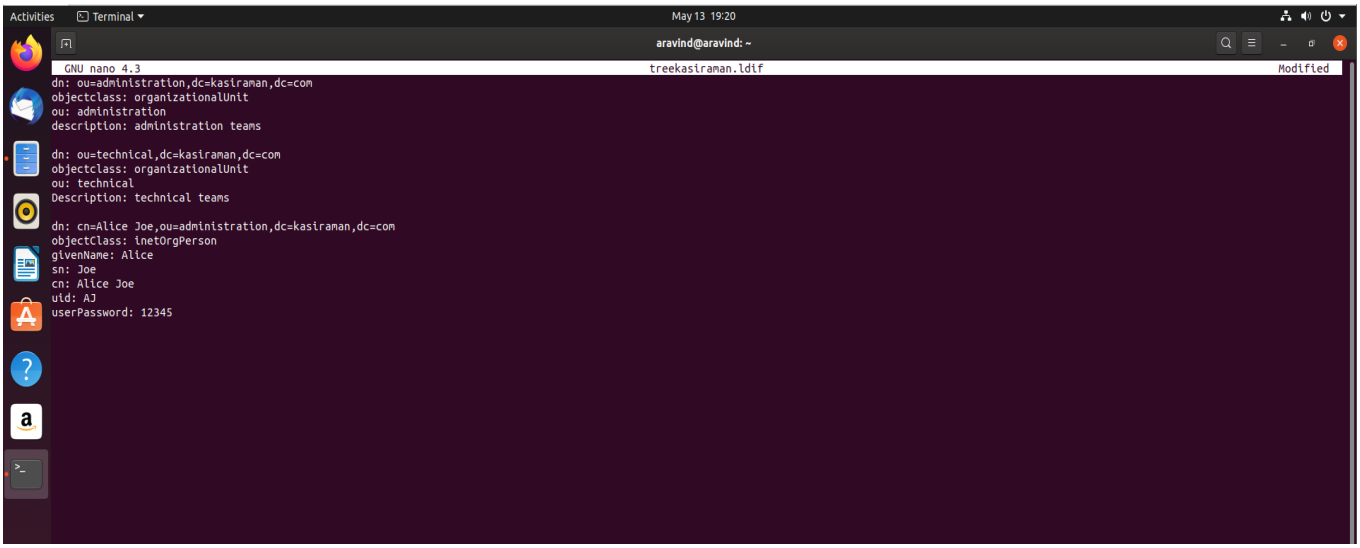
Once done, copy the following command from below and paste it inside the file

Command –

dn: ou=administration,dc=kasiraman,dc=com
objectclass: organizationalUnit
ou: administration
description: administration teams

dn: ou=technical,dc=kasiraman,dc=com
objectclass: organizationalUnit
ou: technical
Description: technical teams

dn: cn=Alice Joe,ou=administration,dc= kasiraman,dc=com
objectClass: inetOrgPerson
givenName: Alice
sn: Joe
cn: Alice Joe
uid: AJ
userPassword: 12345



Save the file once done. Now we need to apply the changes to the treekasiraman.ldif file

Command - sudo ldapadd -x -W -D "cn=admin,dc= kasiraman,dc=com" -H ldap://localhost -f treekasiraman.ldif

-x: pick 'simple authentication' by password
-W: displays an interactive prompt for admin account credentials submission
-D: to indicate the Distinguished Name binding of the respective account to connect
-H: choose the connection method: ldap://localhost initiates a connection using the network on TCP port 389

Note: In case if you plan to re-run this command then make sure you include the -c (switch) to continue execution if any of the entry (in passed ldif file) already exists.

Delete an entry (optional): sudo ldap -v -D "cn=admin,dc= kasiraman,dc=com" -W "cn=Alice Joe,ou=administration,dc= kasiraman,dc=com"

Step 8

In this step we are going to setup a web-based front-end using the PHPLDAPADMIN client.

We are going to install PHPLDAPADMIN

Command - sudo apt-get install phpldapadmin

You can also use other frontal clients.

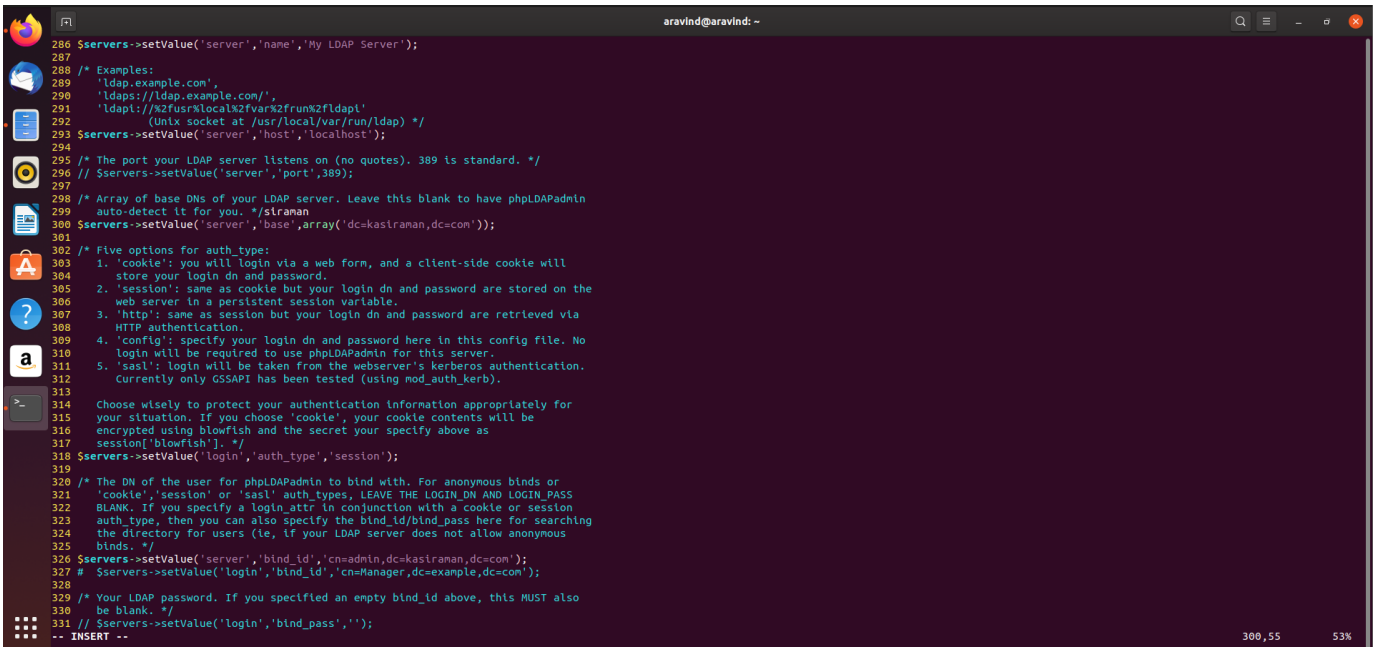
```
aravind@aravind:~$ sudo apt-get install phpldapadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
phpldapadmin is already the newest version (1.2.2-6.1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
aravind@aravind:~$
```

Once installed phpldapadmin we are going to configure it by modifying the config.php file in the phpldapadmin folder (Path – **"/etc/phpldapadmin/config.php"**)

Command – sudo nano /etc/phpldapadmin/config.php

Modify the following lines in the config.php file

- servers->SetValue('server','host','localhost') //line ~293
- servers->SetValue('server','base',array('dc=epita,dc=com') //line ~300
- servers->SetValue('server','bind_id',array('cn=admin,dc=epita,dc=com')) //line ~326
- config->custom->appearance['hide_template_warning'] = true; //line ~161: uncomment first



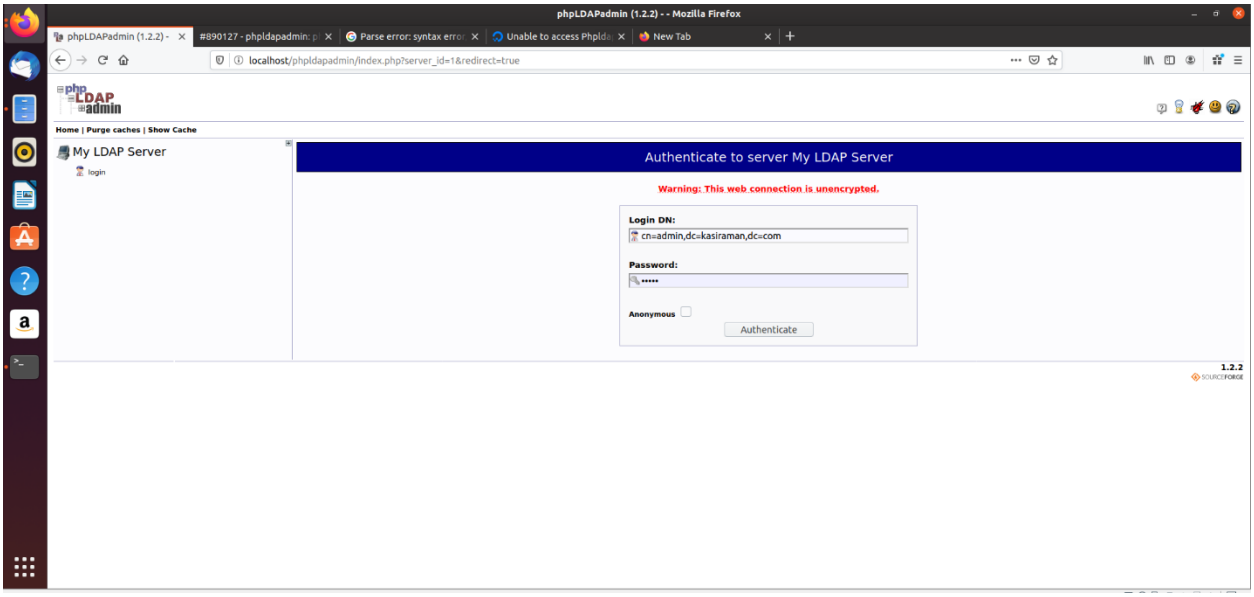
Once we modified the following, we need to restart the apache service.

Command - systemctl restart apache2.service

Step 9

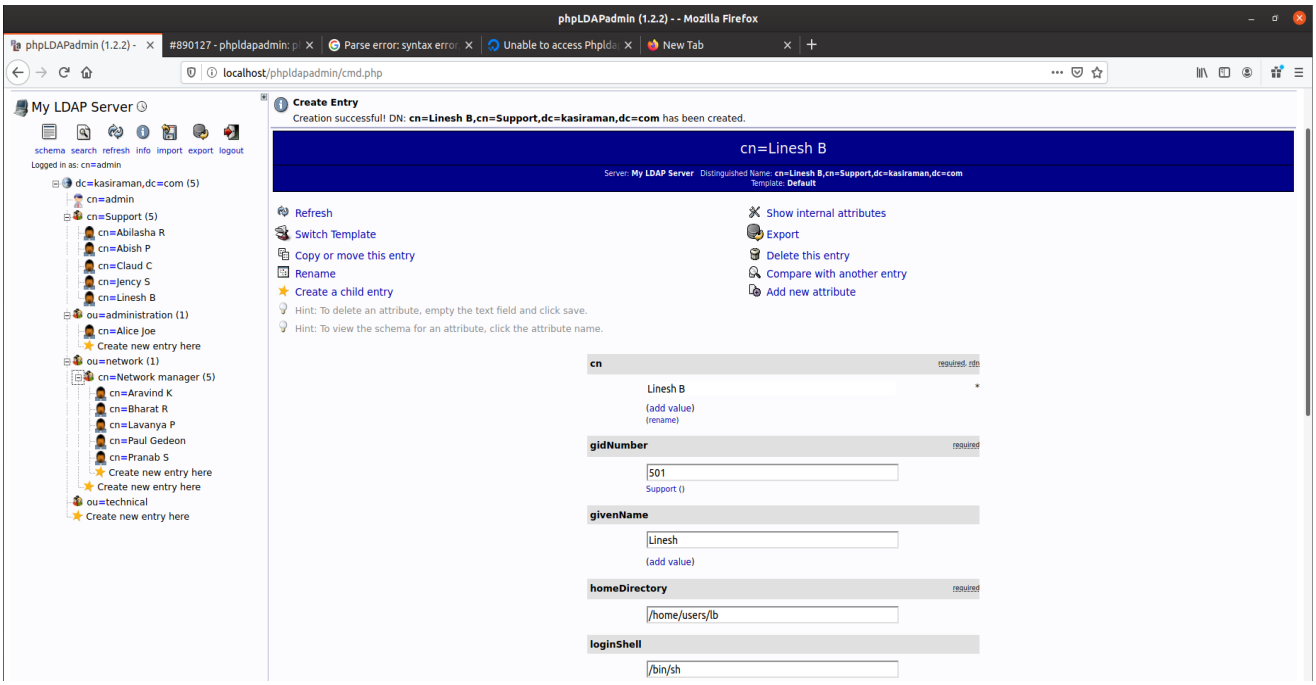
Open the browser and type the following

Command – localhost/phpldapadmin/



Once opened login with the LDAP password which we created in step 2.

After that we need to create a group and add the users in each group



NOTE

If faced any error which accessing the site localhost/phpldapadmin/, we need to do the following in order to access the site

Open nano usr/share/phpldapadmin/lib/functions.php

change line 54 to "function my_autoload($className) {"
Add this code "spl_autoload_register("my_autoload");" **on line 777**

On line 1083

change line 1083 to "$CACHE[$sortby] = __create_function('$a, $b',$code);"
add the code below from the
http://php.net/manual/pt_BR/function.create-function.php page **on line 1091**

```
function __create_function($arg, $body) {
   static $cache = array();
   static $maxCacheSize = 64;
   static $sorter;

   if ($sorter === NULL) {
```

```
        $sorter = function($a, $b) {
            if ($a->hits == $b->hits) {
                return 0;
            }

            return ($a->hits < $b->hits) ? 1 : -1;
        };
    }

    $crc = crc32($arg . "\\x00" . $body);

    if (isset($cache[$crc])) {
        ++$cache[$crc][1];
        return $cache[$crc][0];
    }

    if (sizeof($cache) >= $maxCacheSize) {
        uasort($cache, $sorter);
        array_pop($cache);
    }

    $cache[$crc] = array($cb = eval('return
function('.$arg.'){'.$body.'};'), 0);
    return $cb;
}
```

By doing the changes we will be able to access the site.