**LDAP CONFIGURATION**

**What is LDAP:**

LDAP stands for Lightweight Directory Access Protocol. It is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an IP network. LDAP is often used as a centralized authentication and authorization system in Linux servers and other networked environments.

In Linux servers, LDAP is commonly used in conjunction with other services such as OpenLDAP or Microsoft's Active Directory to provide a centralized directory service for managing user accounts, groups, and other network resources. Here are some key aspects of LDAP in Linux servers:

**Directory Structure**:

LDAP organizes directory information into a hierarchical structure similar to a tree. Entries in the LDAP directory represent objects such as users, groups, and organizational units (OUs). Each entry has attributes that define its characteristics.

**Authentication**:

LDAP can be used to authenticate users attempting to access resources on Linux servers. Instead of authenticating users locally on each server, Linux servers can be configured to authenticate users against an LDAP directory. This enables centralized management of user accounts and credentials.

**Authorization**: LDAP can also be used for authorization purposes. Once users are authenticated, LDAP can determine their access rights and permissions based on their group memberships or other attributes stored in the directory.

**Single Sign-On (SSO):** LDAP can facilitate single sign-on solutions, allowing users to authenticate once and access multiple services or resources without having to re-enter their credentials.

Integration with Applications: Many applications and services in Linux environments support LDAP authentication and can be configured to use LDAP for user authentication and authorization. This includes web servers, email servers, file servers, and more.

**OpenLDAP**: OpenLDAP is an open-source implementation of the LDAP protocol. It provides a server-side solution for managing LDAP directories on Linux servers. OpenLDAP can be used to deploy and manage LDAP directory services, configure access controls, and replicate directory data for fault tolerance and scalability.

Overall, LDAP plays a crucial role in Linux server environments by providing a centralized directory service for managing user accounts, authentication, and authorization. It simplifies administration, enhances security, and enables interoperability across various applications and services.

**LDAP CONFIGURATION IN UBUNTU:**

## Prerequisites

Before you begin with this guide, you must have the following prerequisites:

* An Ubuntu 22.04 server
* A non-root user with root/administrator privileges.

## Setting Up FQDN (Fully Qualified Domain Name)

Before you begin the installation of the OpenLDAP server, you need to ensure the FQDN (Fully Qualified Domain Name) configuration for the OpenLDAP server is correct. In this demo, we will set up an OpenLDAP server with the server hostname "**ldap**" and the domain "**localdomain.com**", and with the IP address "**192.168.5.25**".

Run the below command to set up the FQDN to "ldap.localdomain.com".

*sudo hostnamectl set-hostname ldap.localdomain.com*

Edit the config file "/etc/hosts" using the following command.

*sudo nano /etc/hosts*

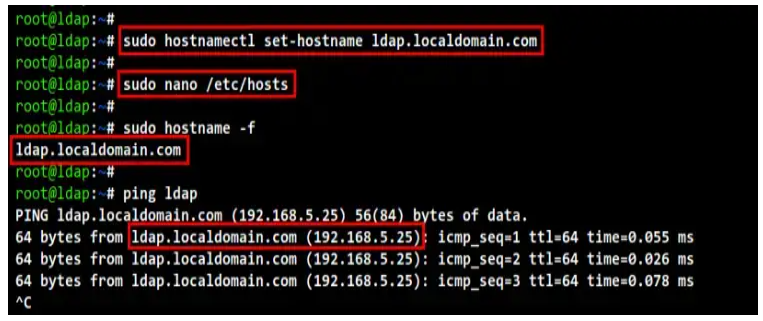
Add the below configuration to the file. The format of the "/etc/hosts" file here is "server-IP  fqdn  hostname".

192.168.5.25 ldap.localdomain.com ldap

Save and close the file when you are done.

Lastly, run the command below to check and verify the FQDN of your LDAP server. In this demo, you should get the output such as "ldap.localdomain.com". Also, if you try to ping the hostname "ldap", you should get the response from the server IP address "192.168.5.25" instead of localhost.

*sudo hostname -f  
ping ldap*



**Installing OpenLDAP Packages**

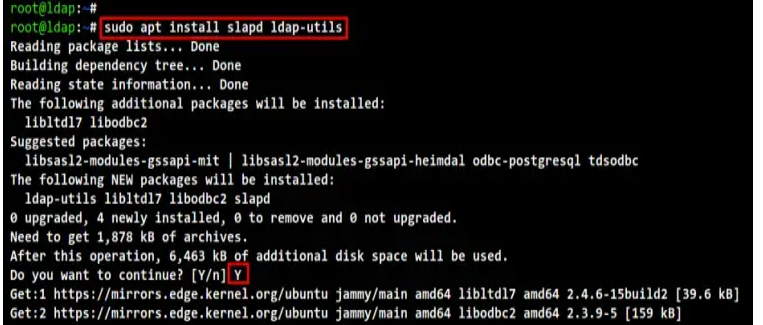
After you have the correct FQDN, it's time to install OpenLDAP packages which are available by default on the Ubuntu repository.

Before start installing packages, run the apt command below to update and refresh your Ubuntu system repository.

*sudo apt update*

Now install OpenLDAP packages using the following command. Input **Y** to confirm the installation and press **ENTER**, and the installation will begin.

*sudo apt install slapd ldap-utils*

****

During the OpenLDAP packages installation, you will be asked to set up the admin password for OpenLDAP. Input the strong password for the OpenLDAP admin user and select "**OK**", then repeat your password. And the OpenLDAP installation will be complete.

****

****

## Configuring OpenLDAP Server

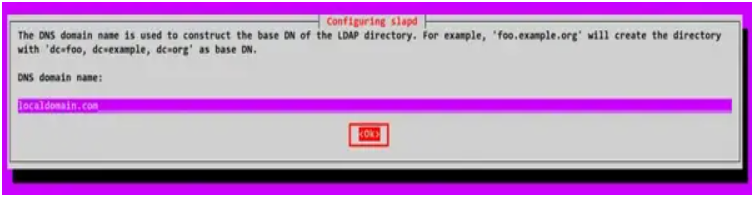
To start configuring the OpenLDAP server, run the following command. This command will re-configure the main OpenLDAP package "slapd" and you will be asked for some of the basic OpenLDAP configurations.

*sudo dpkg-reconfigure slapd*

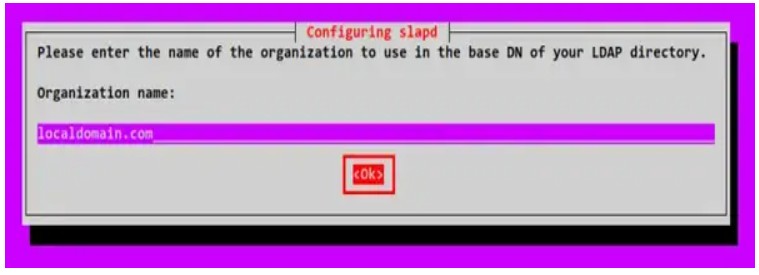
When asked to "Omit OpenLDAP server configuration?", select "**No**". This will set up the OpenLDAP server with a new configuration file and a new database.



Input the domain name for your OpenLDAP installation and select "**Ok**". This domain name will be used as the DN (Distinguished Name) of your OpenLDAP server. In this demo, the domain name is "**localdomain.com**", so the DN will come "**dc=localdomain,dc=com**".

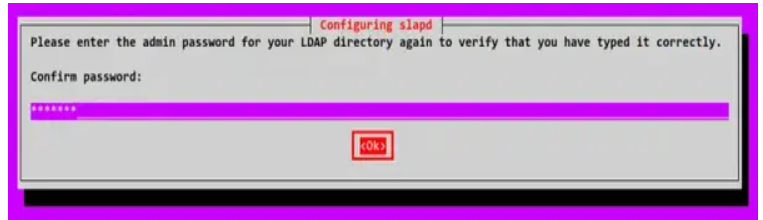
****

Input the organization name that will be used inside the **DN**. You can use the domain for this, but also you can use another name.

****

Now input the admin password for your OpenLDAP server and repeat the password. Also, be sure the password is correct.

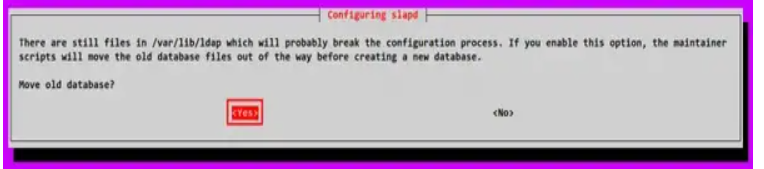
****

****

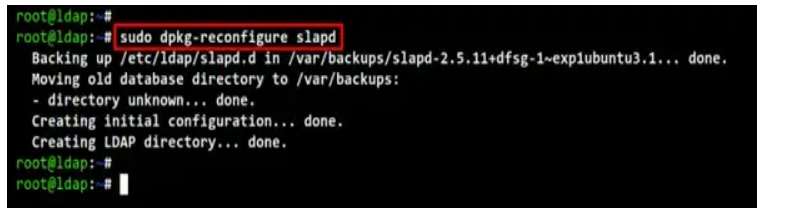
When asked to remove the old database, select "**No**".

****

Now select "**Yes**" to move the old OpenLDAP database, and the OpenLDAP configuration is finished.

****

Below is the output when the OpenLDAP configuration is completed.

****

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

*sudo nano /etc/ldap/ldap.conf*

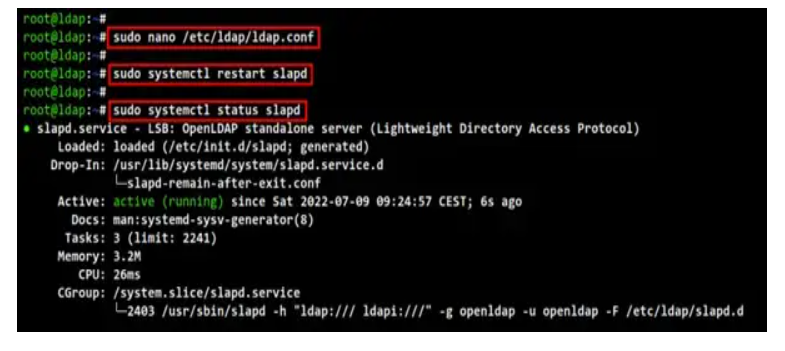
Uncomment the line "BASE" and "URI" and input the domain name for your OpenLDAP server. In this demo, the "**BASE**" here is "*dc=localdomain,dc=com*" and the "**URI**" for the OpenLDAP server is "*ldap://ldap.localdomain.com*".

BASE dc=localdomain,dc=com  
URI  ldap://ldap.localdomain.com

Save and close the file are you are done.

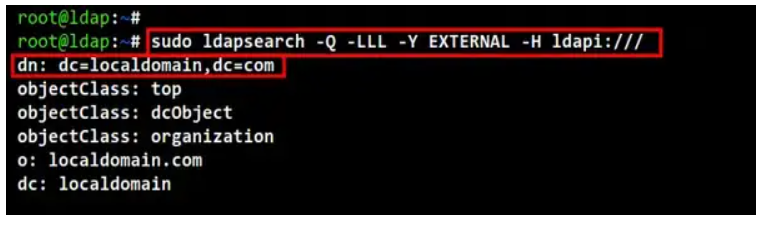
Now run the command below to restart the "slapd" OpenLDAP service and apply new changes on the OpenLDAP server. The OpenLDAP server is now running with the base DN "**dc=localdomain,dc=com**".

*sudo systemctl restart slapd  
sudo systemctl status slapd*

****

Lastly, run the following command to check and verify the OpenLDAP basic configuration. You should get the base DN for the OpenLDAP server as "**dc=localdomain,dc=com**".

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

****

## Setting Up Base Group

After configuring the base DN (Distinguished Name) of the OpenLDAP server, now you will be creating a new base group of OpenLDAP users. In this demo, you will create two different base groups, the group named "People" for storing users, and then the group named "Groups" for storing groups on your OpenLDAP server.

To create new LDAP contents such as user and group, you can use the LDIF file (LDAP Data Interchange Format) and the LDAP tool "ldapadd".

Create a new LDIF file "base-groups.ldif" using the command below.

*sudo nano base-groups.ldif*

Add the following configuration to the file.

dn: ou=People,dc=localdomain,dc=com  
objectClass: organizationalUnit  
ou: People  
  
dn: ou=Groups,dc=localdomain,dc=com  
objectClass: organizationalUnit  
ou: Groups

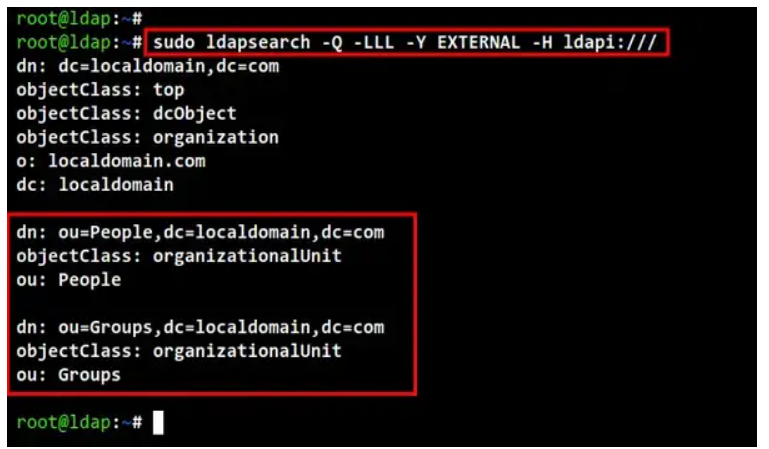
Now run the "ldapadd" command below to new base groups through the file "base-groups.ldif". You will be prompted for the OpenLDAP admin password, so be sure to input the correct password.

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

****

Lastly, run the following command to check and verify the base groups of your OpenLDAP server. You should see two base groups available now, the group named  "**People**" and "**Groups**".

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

****

## Adding New Group

After creating base groups on the LDAP server, now you can create a new LDAP group and user. In this section, you will be creating a new group through the LDIF file.

Create a new LDIF file "group.ldif" using the following command.

*sudo nano group.ldif*

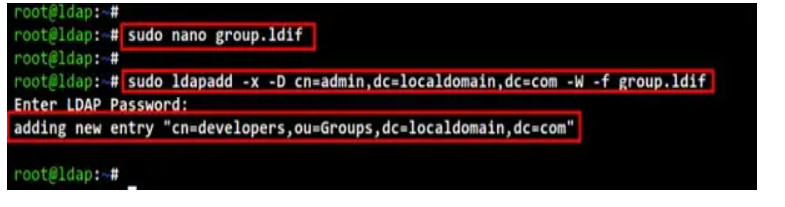
Add the following configuration to the file. In this example, we will create a new group with the name "developers", store it on the base group "Groups" and define the gidNumber "**5000**".

dn: cn=developers,ou=Groups,dc=localdomain,dc=com  
objectClass: posixGroup  
cn: developers  
gidNumber: 5000

Save and close the file when you are done.

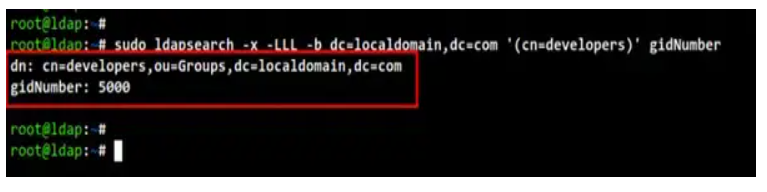
Next, run the "ldapadd" command below to add the new group of "**developers**". And be sure to input the admin password for your OpenLDAP server.

*sudo ldapadd -x -D cn=admin,dc=localdomain,dc=com -W -f group.ldif*

****

Lastly, run the following command to check and verify the group "**developers**". You should get the output of the group "**developers**" which is part of "**Groups**" and with the gidNumber "**5000**".

*sudo ldapsearch -x -LLL -b dc=localdomain,dc=com '(cn=developers)' gidNumber*



## Adding OpenLDAP Users

After you have created a group on the OpenLDAP server, it's time to create an LDAP user through the LDIF file.

Before creating a new user, run the following command to generate an encrypted password for the new LDAP user. Input the new password and repeat, then copy the encrypted password "{SSHA}ZdNAB+uH/zbK1mdS9JWlfOwRDf0mrsla".

*sudo slappasswd*

Now create a new LDIF file "user.ldif" using the following command.

*sudo nano user.ldif*

Add the following configuration to the file. In this demo, we will create a new user "**john**" with the default home directory "/home/john" and the default shell "/bin/bash". Also, you can see on top of the config file, that this user is part of the group "**People**" and using the gidNumber "**5000**".

dn: uid=john,ou=People,dc=localdomain,dc=com  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: shadowAccount  
uid: john  
sn: Doe  
givenName: John  
cn: John Doe  
displayName: John Doe  
uidNumber: 10000  
gidNumber: 5000  
userPassword: {SSHA}ZdNAB+uH/zbK1mdS9JWlfOwRDf0mrsla  
gecos: John Doe  
loginShell: /bin/bash  
homeDirectory: /home/john

Save and close the file when you are done.

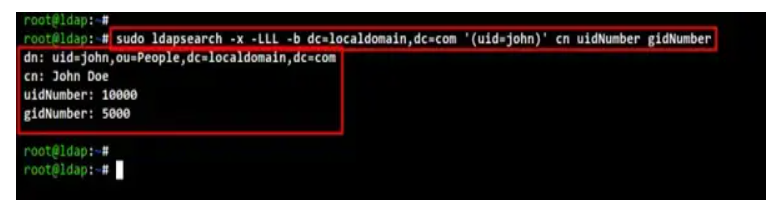
Next, run the "ldapadd" command below to add a new user within the file "user.ldif". Now input the admin password for the OpenLDAP server.

*sudo ldapadd -x -D cn=admin,dc=localdomain,dc=com -W -f user.ldif*



Lastly, run the "*ldapsearch*" command below to check and verify the new LDAP user. And you should get the user "**john**" created and available on the OpenLDAP server.

*sudo ldapsearch -x -LLL -b dc=localdomain,dc=com '(uid=john)' cn uidNumber gidNumber*

****

## Installing LDAP Account Manager

At this point, you have finished the basic OpenLDAP installation. Now you will be installing the LDAP Account Manager on the same server as the OpenLDAP server. The LDAP Account Manager (LAM) is a web application that can be used as the front-end for the OpenLDAP server. It allows you to manage the OpenLDAP server from the web browser, you can set up new users, groups, etc from the web browser.

The LAM is available by default on the Ubuntu repository. You can install it using the apt command below. This will install some other packages including PHP and Apache2 web server.

Input **Y** to confirm the installation and press **ENTER** to continue. And the LAM installation will begin.

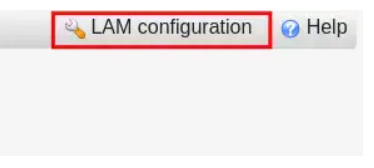
*sudo apt install ldap-account-manager*

After installation is completed, open up the web browser and visit the server IP address followed by the URL path "/lam (i.e <http://192.168.5.25/lam>). And you should get the login page of the LDAP Account Manager (LAM).

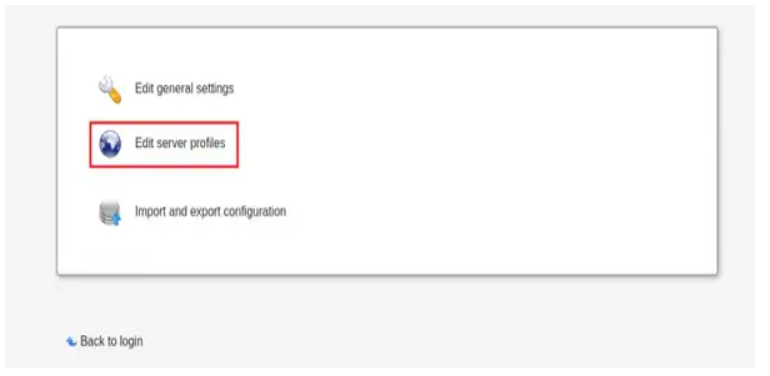
## Configuring LDAP Account Manager

Before you start managing your OpenLDAP server from the LAM application, you will be setting up the LAM profile for your OpenLDAP server.

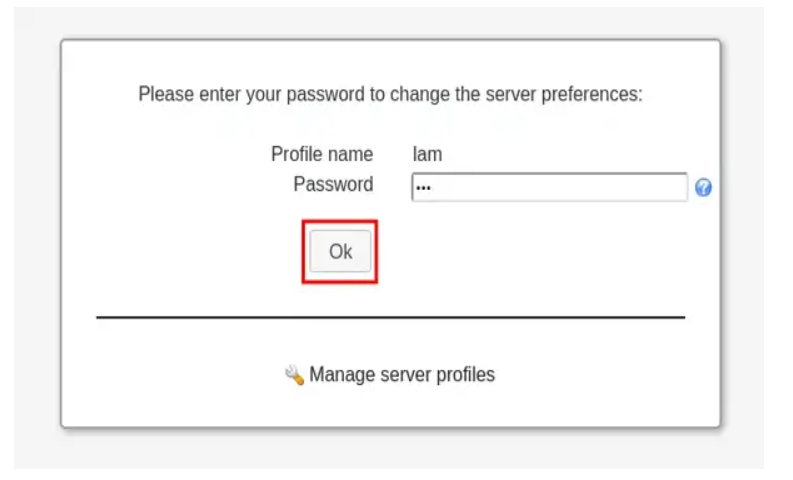
On the LAM login page, click the menu "**LAM configuration**" on the top left.

****

Now click "**Edit server profiles**" to set up the LAM profile for your OpenLDAP server.

****

When asked for the password, input the default password "**lam**" and click "**Login**". The default profile on the LDAP Account Manager is "**lam**". You will be editing this default profile for your OpenLDAP server.

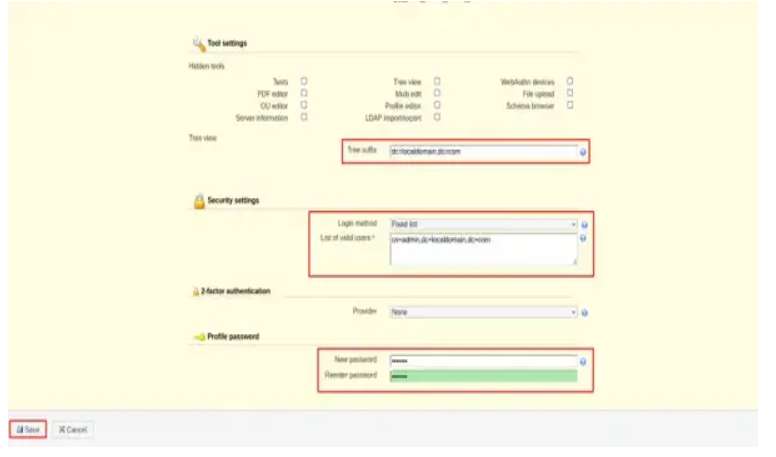
****

On the "**General settings**" page, you will see some of the different settings.

On the "**Tools settings**", input the main DN (*Distinguished Name*) of the OpenLDAP server. In this demo, the DN is "*dc=localdomain,dc=com*".

On the "**Security settings**" section, select the "login method" as "Fixed list". Then, input details login for the OpenLDAP server. The default user for OpenLDAP is "admin", so the filed should be like this "*cn=admin,dc=localdomain,dc=com*".

Lastly, input a new password on the "Password profile" section. This will change the default password for the profile "lam". Then, click the "Save" button to apply new changes.



Now you will be redirected to the LDAP Account Manager login page. Click the "LAM configuration" menu again and edit the default profile "**lam**".

Now move to the "Account types" page to set up the default group of the OpenLDAP server.

On the "**Users**" section, input the LDAP suffix as "*ou=People,dc=localdomain,dc=com*". In this example, all users should be available on the "**People**".

On the "**Groups**" section, input the LDAP suffix as "*ou=Groups,dc=localdomain,dc=com*". In this example, all groups should be available at the base group "**Groups**".

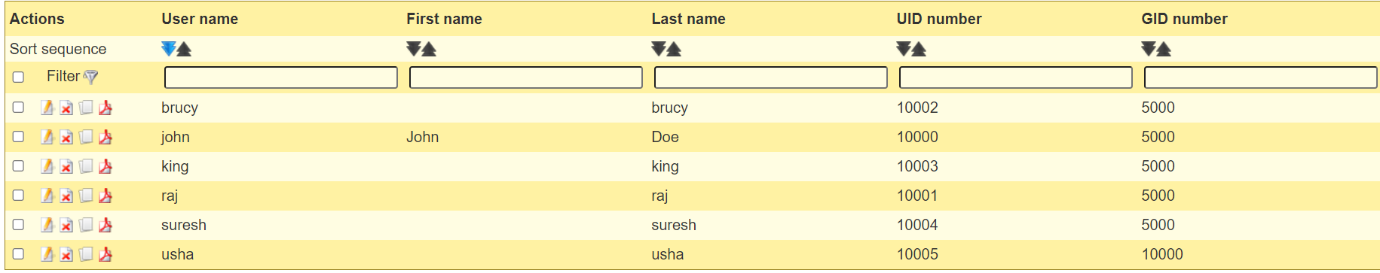
Now click the "**Save**" button to save the changes on the default profile "**lam**".



At this point, you will be redirected again to the LDAP Account Manager login page. As you can see the default user login is now changed to "**admin**". Input the admin password for your OpenLDAP password and click "**Login**". And you should get the LAM dashboard.

****

On the "**Users**" menu, you should see the user "**john**" that you just created.



While on the "**Groups**" menu, you should see the group "**developers**".



## Conclusion

Congratulation! You have now successfully installed the OpenLDAP server with the LDAP Account Manager (LAM) on the Ubuntu 22.04 server. You have also learned how to set up an OpenLDAP group and user. Lastly, you have also learned how to set up an LDAP Account Manager profile to add the OpenLDAP server to the LAM web application.

**LDAP CLIENT SERVER SET-UP AND VALIDATION**

**Prerequisites:**

**LDAP Server**

Hostname: Idap

FQDN: Idap.localdomain.com

IP: 192.168.1.8(your private IP of LDAP server)

**LDAP Client**

Hostname: Idap2

FQDN: Idap2.localdomain.com

IP: 192.168.1.9(your private IP of LDAP server)

OpenLDAP & LAM Server have been installed on Idap.localdomain.com

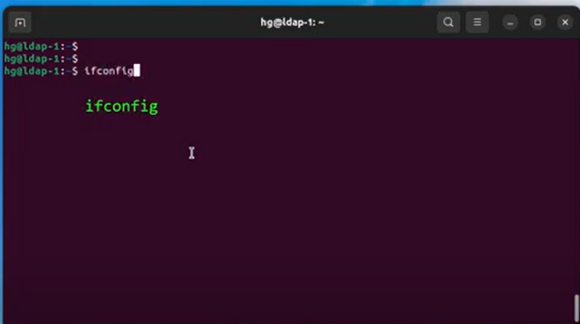
User accounts such as john,suresh have been created on the LDAP Server

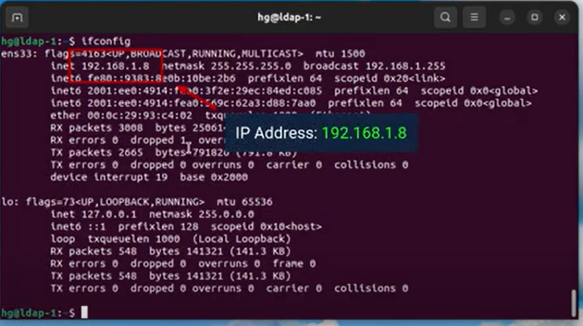
Root LDAP account: cn=admin,dc=local,dc=com

Check the Hostname & FQDN/Fullname on the LDAP server

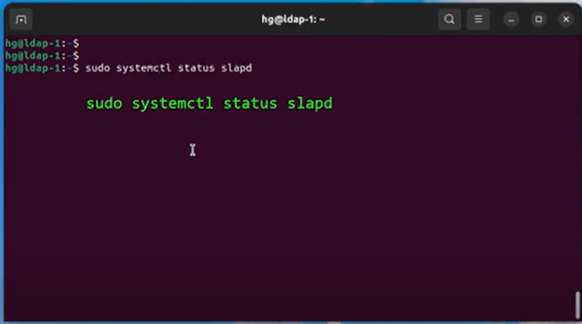


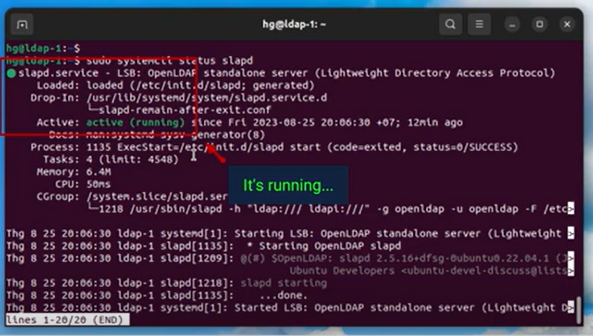
. Check IP address of the LDAP server





Ensure that the OpenLDAP service are running on the system

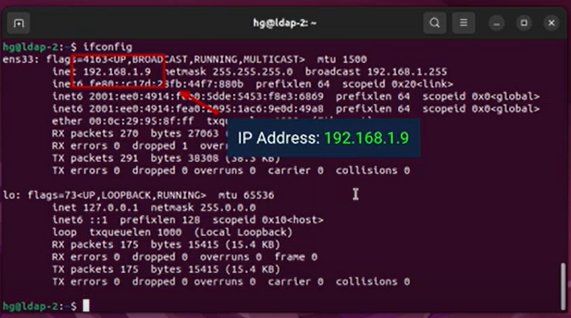




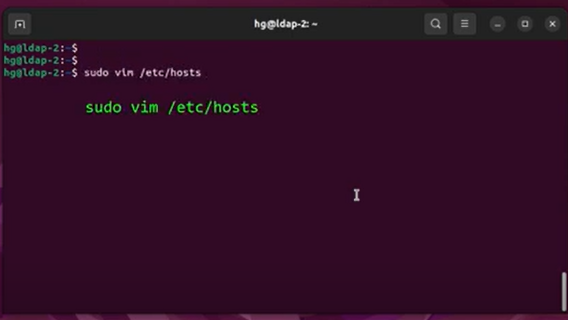
* **Step 1**- Check the Prerequisites

1. On the LDAP Client [ ldap2.localdomain.com]
2. Check the Hostname & FQDN/Fullname on the LDAP client

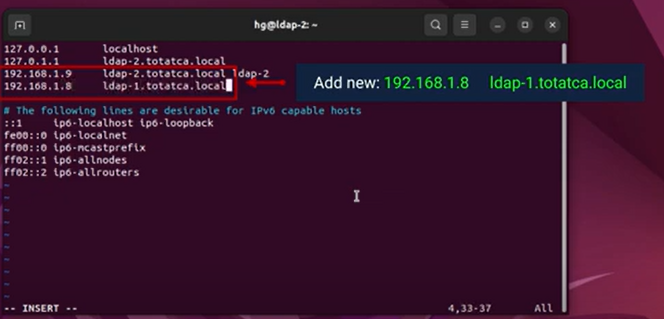
Check the IP address of the LDAP client using **ifconfig** command.



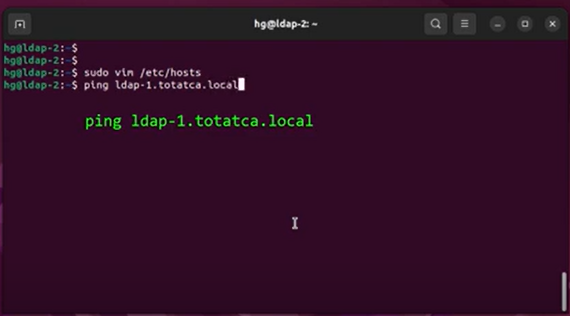
Edit the configuration using $**sudo vim /etc/hosts command**



Add the IP and FQDN of the LDAP server to the /etc/hosts file of LDAP Client

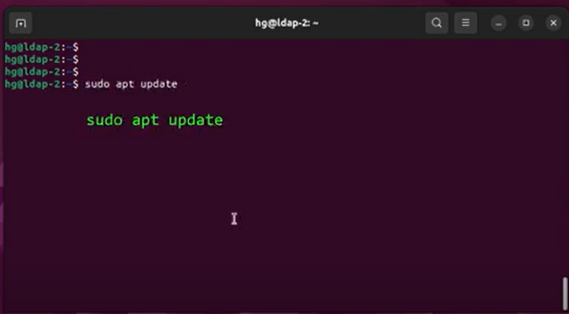


Ensure that the LDAP Client can successfully ping the LDAP Server via its FQDN



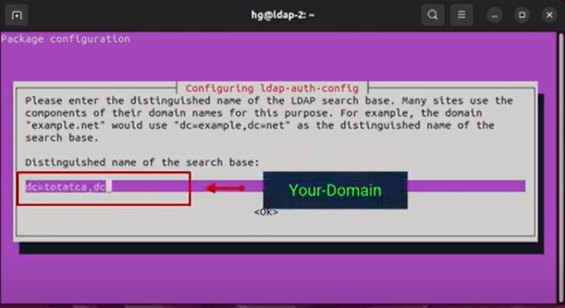
**Step 2** - Install Idap2.localdomain.com as an LDAP client

* Update system using $ **sudo apt update**

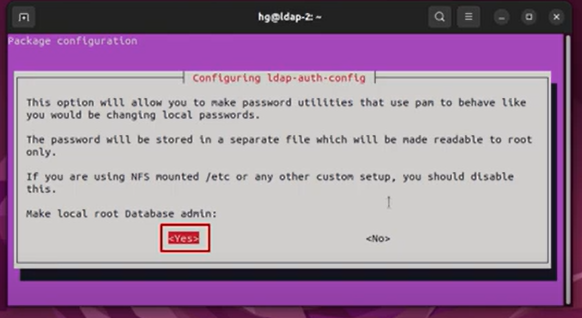
****

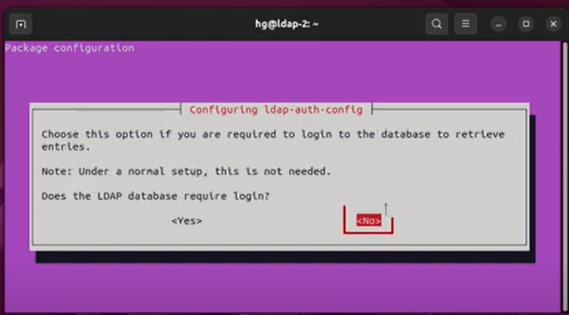
Install LDAP Client using sudo apt install libnss-ldap libpam-ldap ldap-utils nscd -y

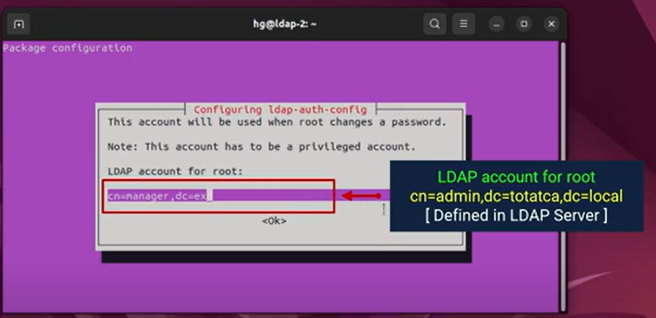


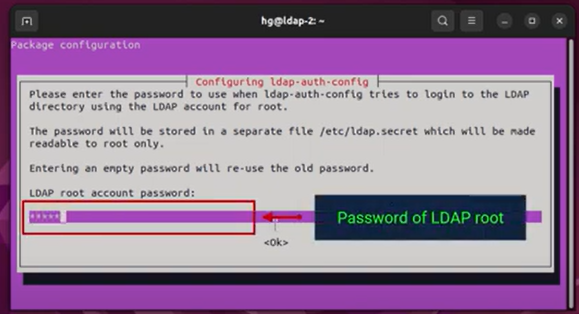






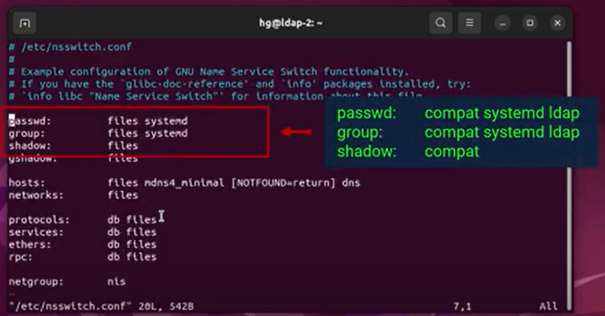




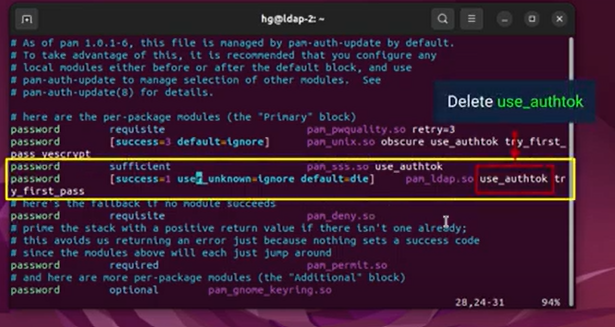


**Step 3** - Configure LDAP Client

Edit /etc/nsswitch.conf file using **$ sudo vim /etc/nsswitch.conf** command

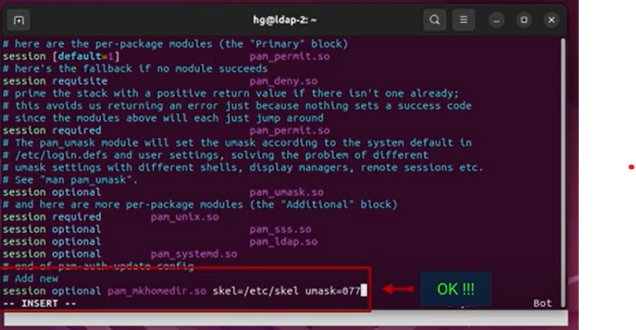


Edit /etc/pam.d/common- password file using **$ sudo vim /etc/pam.d/common-password** command



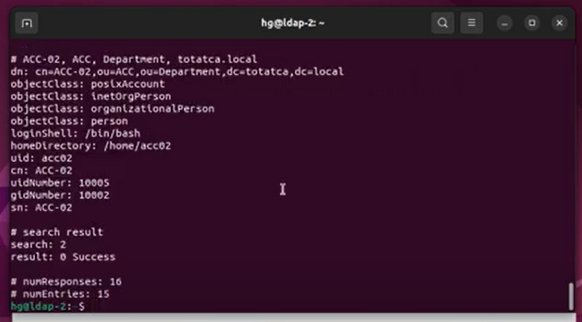
Now Edit /etc/ pam.d/common- session file using **$ sudo vim /etc/pam.d/common-session** command

**~ session optional pam\_mkhomedir.so skel=/etc/skel umask=077** Add this content to the end of the page



Restart and Enable NSCD service using $ **sudo systemctl restart nscd** and $ sudo **systemctl enable nscd** commands

Ensure that the LDAP Client can query the LDAP Server using the Idapsearch command i.e **$ ldapsearch -x -H ldap://192.168.1.8 -b "dc=localdomain,dc=com".**

****

**Step-4 -**Testing

We have created user accounts (john,suresh...) on the LDAP Serrver.Now, let's try logging in with these accounts on the LDAP Client

Testing by command line

Use command **$ sudo login**



**Advantages of LDAP**

LDAP (Lightweight Directory Access Protocol) offers several advantages for managing and accessing distributed directories. Let’s explore them:

1. Global Naming Model:
   * LDAP ensures unique entries by providing a global naming model.
   * Each entry has a unique distinguished name (DN), making it easy to locate and manage.
2. Multiple Independent Directories:
   * LDAP allows the use of multiple independent directories within an organization.
   * Different departments or services can maintain their own directory structures.
3. Extensibility:
   * LDAP is extensible, allowing you to meet future or local requirements.
   * You can add custom attributes or object classes as needed.
4. TCP/IP and SSL Support:
   * LDAP runs directly over TCP/IP, making it compatible with standard networking protocols.
   * It also supports SSL for secure communication (LDAPS).
5. Industry Support:
   * LDAP has wider support across various industries and applications.
   * It is used by services like TCP and DNS.
6. Open Source and Flexible:
   * LDAP is an open-source protocol with a flexible architecture.
   * It can be customized to fit specific organizational needs.

**PROJECT DONE BY :-**

* **G.Suresh Kiran**
* **D.Usha Sravani**
* **CH.Sravani**
* **P.Raju**
* **D.Pavan Kalyan**
* **E.Simhadri**
* B.**Sai Kumar.**

**-----------THE END-------------**