Operating System Security #3 Centralized Auth.

Herman Kabetta, M.T.

Centralized Auth. Service or Directory Services

- A central repository for storing and managing information. Almost any kind of information can be stored, from identity profiles and access privileges to information about application and network resources, printers, network devices and manufactured parts.

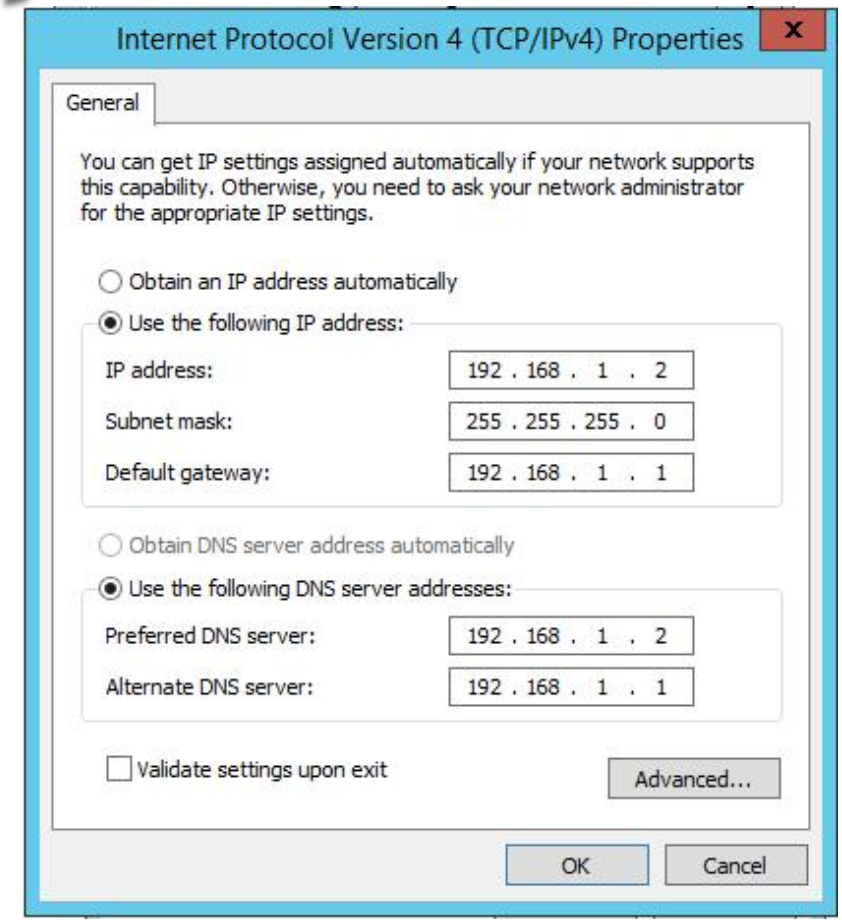
Centralized Auth. Service or Directory Services

- Information stored in Directory server can be used for the authentication and authorization of users to enable secure access to enterprise and internet services and applications
- It is also referred to single sign-on

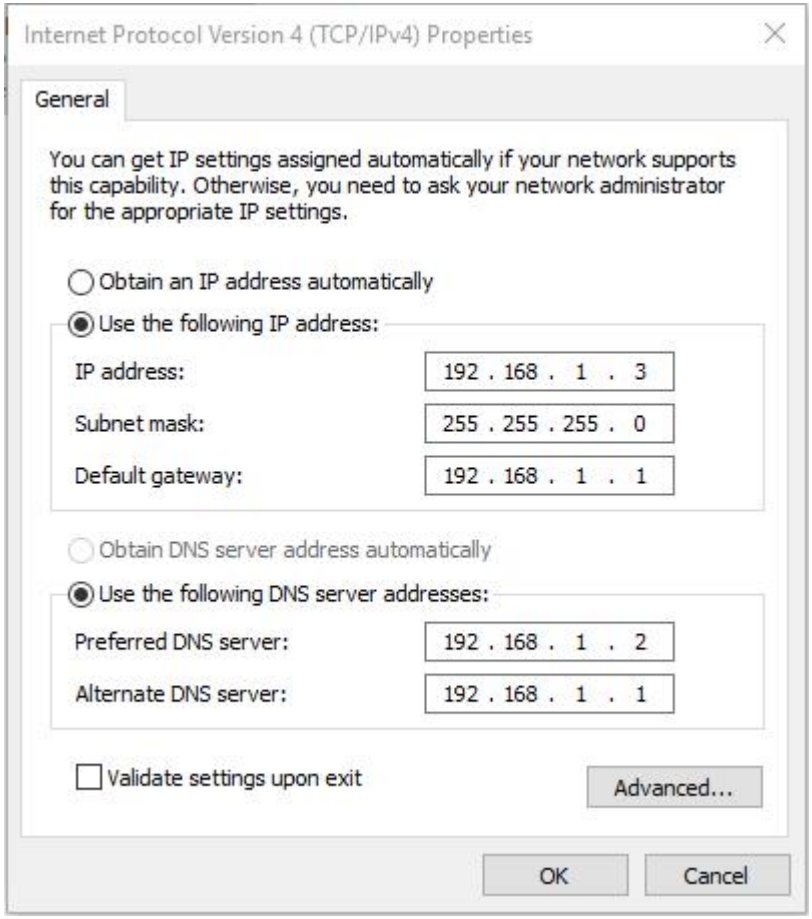
Examples of Directory Services :

- OpenLDAP
- RedHat IDM
- WinBind
- Microsoft Active Directory

Lab Prep. : VM Connection



Server IP



Client IP

```
C:\Users\herma>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
```

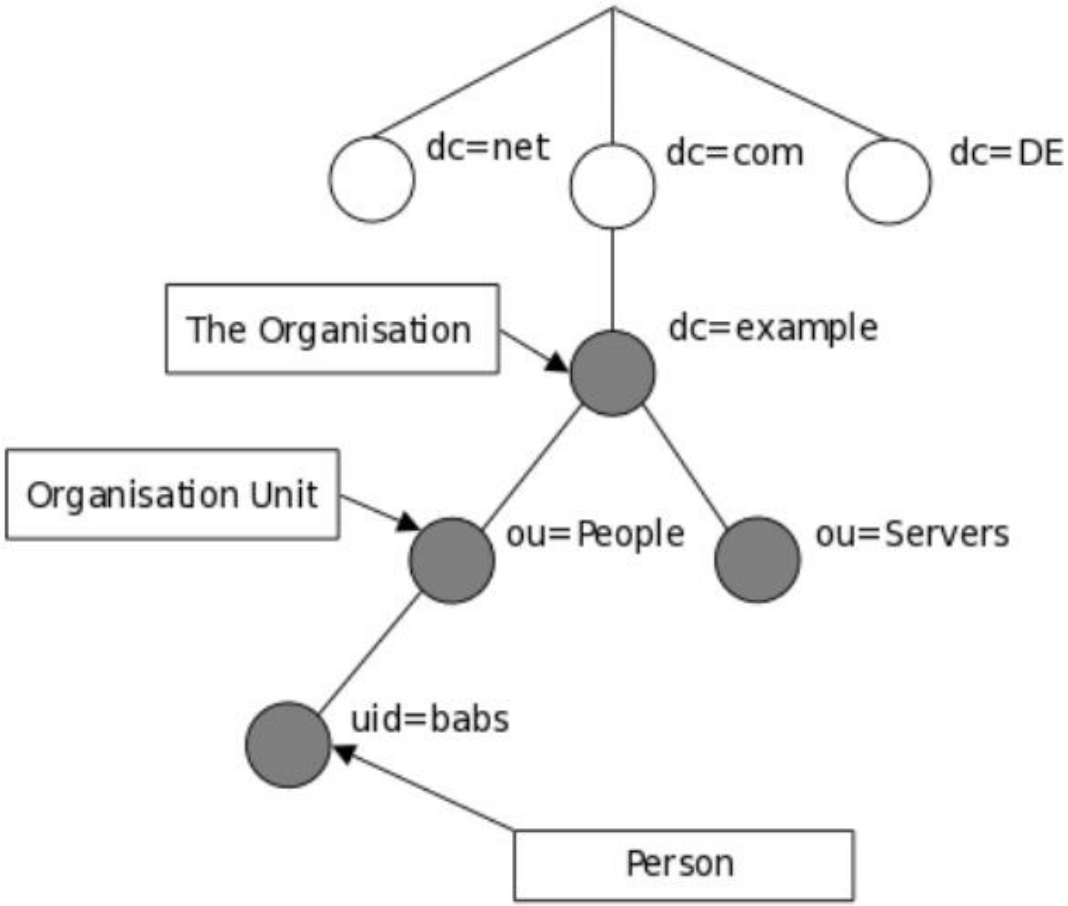
Lab Prep. : VM Connection

```
vi /etc/sysconfig/network-scripts/ifcfg-enp0s3
```

How to change adapter in CentOS 7

```
TYPE=Ethernet
# Static IP Address #
BOOTPROTO=none
# Server IP #
IPADDR=192.168.1.2
# Netmask #
NETMASK=255.255.255.0
# Default Gateway IP #
GATEWAY=192.168.1.1
# DNS Servers #
DNS1=192.168.1.2
DNS2=192.168.1.1
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
# Disable ipv6 #
IPV6INIT=no
# Device Name #
NAME=enp0s3
DEVICE=enp0s3
```

Terms


dc=net
dc=com
dc=DE
The Organisation
dc=example
Organisation Unit
ou=People
ou=Servers
uid=babs
Person

LDAP Server Installation (OpenLDAP)

```
$ yum install openldap openldap-server
```

LDAP Server Start

```
$ sudo systemctl start slapd
$ sudo systemctl enable slapd
$ sudo systemctl status slapd
```

```
[root@rkss ~]# systemctl status slapd
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset
: disabled)
   Active: active (running) since Wed 2019-10-30 10:46:58 WIB; 17s ago
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
 Main PID: 5927 (slapd)
   CGroup: /system.slice/slapd.service
           └─5927 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///

Oct 30 10:46:53 rkss systemd[1]: Starting OpenLDAP Server Daemon...
Oct 30 10:46:53 rkss runuser[5911]: pam_unix(runuser:session): session open...0)
Oct 30 10:46:53 rkss slapcat[5916]: DIGEST-MD5 common mech free
Oct 30 10:46:53 rkss slapd[5926]: @(#) $OpenLDAP: slapd 2.4.44 (Jan 29 2019... $
                                          mockbuild@x86-01.bsys.centos.org:...pd
```

Firewall & Password Hash

Allow requests to the LDAP server daemon through the firewall

```
$ firewall-cmd --add-service=ldap
```

Generate password that used on next step

```
$ slappasswd
```

```
[root@rkss ~]# slappasswd
New password:
Re-enter new password:
{SSHA}oBYuDcH8hrW2uRNZ7pGP69gRmkNHtBPN
```

Create LDIF File

Create an LDIF file (ldapadmin.ldif) which is used to add an entry to the LDAP directory.

```
$ sudo nano ldapadmin.ldif
```

```
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}PASSWORD_CREATED
```

Add the corresponding LDAP entry by specifying the URI referring to the ldap server and the file above

```
$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f ldapadmin.ldif
```

Configuring LDAP Database (cp & chown)

Copy the sample database configuration file for slapd into the /var/lib/ldap directory, and set the correct permissions on the file.

```
$ sudo cp /usr/share/openldap
  servers/DB_CONFIG.example
  /var/lib/ldap/DB_CONFIG

$ sudo chown -R ldap:ldap
  /var/lib/ldap/DB_CONFIG

$ sudo systemctl restart slapd
```

Configuring LDAP Database (import basic LDAP)

Import some basic LDAP schemas from the /etc/openldap/schema directory

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

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

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

Configuring LDAP Database (add domain)

Add your domain in the LDAP database and create a file called ldapdomain.ldif

```
$ sudo nano ldapdomain.ldif
$ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f
  ldapdomain.ldif
```

```
$ sudo nano baseldapdomain.ldif
$ sudo ldapadd -x -D cn=Manager,dc=myserver,
  dc=local -W -f baseldapdomain.ldif
```

Both files downloadable on lecture web page

Configuring LDAP Database (create user)

Create a LDAP user for and set a password for this user as follows

```
$ sudo useradd subzero
$ sudo passwd subzero
```

Configuring LDAP Database (create group LDIF)

Create the definitions for a LDAP group

```
$ sudo nano ldapgroup.ldif
```

```
dn: cn=Manager,ou=Group,dc=myserver,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 1005
```

```
$ sudo ldapadd -x -W -D
  "cn=Manager,dc=myserver,dc=local" -f
  ldapgroup.ldif
```

Configuring LDAP Database (create user LDIF)

Create another LDIF file called ldapuser.ldif and add the definitions for user subzero

```
$ sudo nano ldapuser.ldif
```

```
$ sudo ldapadd -x -D
  cn=Manager,dc=myserver,dc=local -W
  -f  ldapuser.ldif
```

ldapuser.ldif can be downloaded on lecture web page

Configuring Client (Windows)

pGina

pGina is a pluggable, open source credential provider (and GINA) replacement. It allows for alternate methods of interactive user authentication and access management on machines running the Windows operating system.

Download pGina

General | Plugin Selection | Plugin Order | Simulation | Credential Provider Options

Search Directories

Directory

C:\Program Files\pGina\Plugins\Core

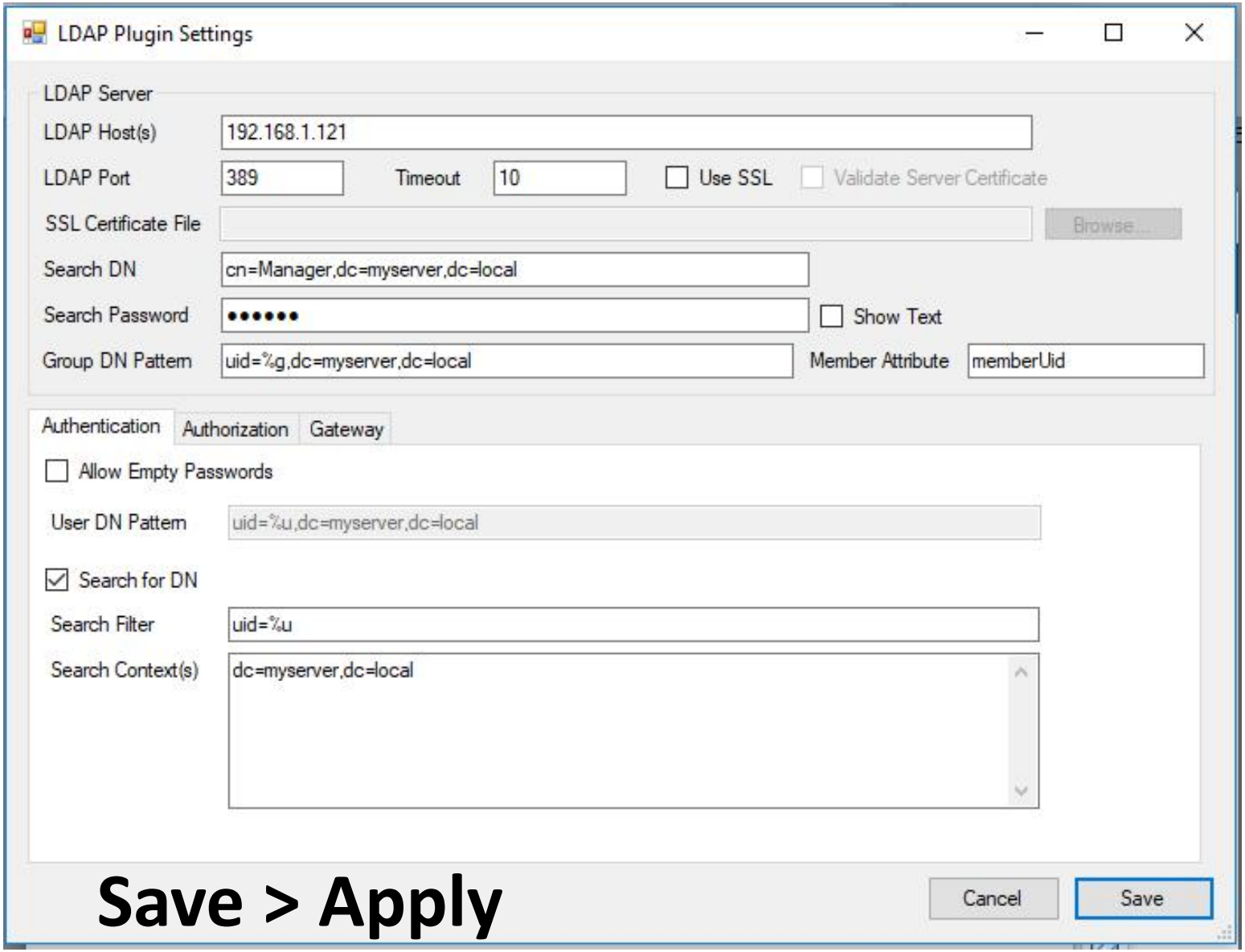
C:\Program Files\pGina\Plugins\Contrib

Add | Remove

Current Plugins

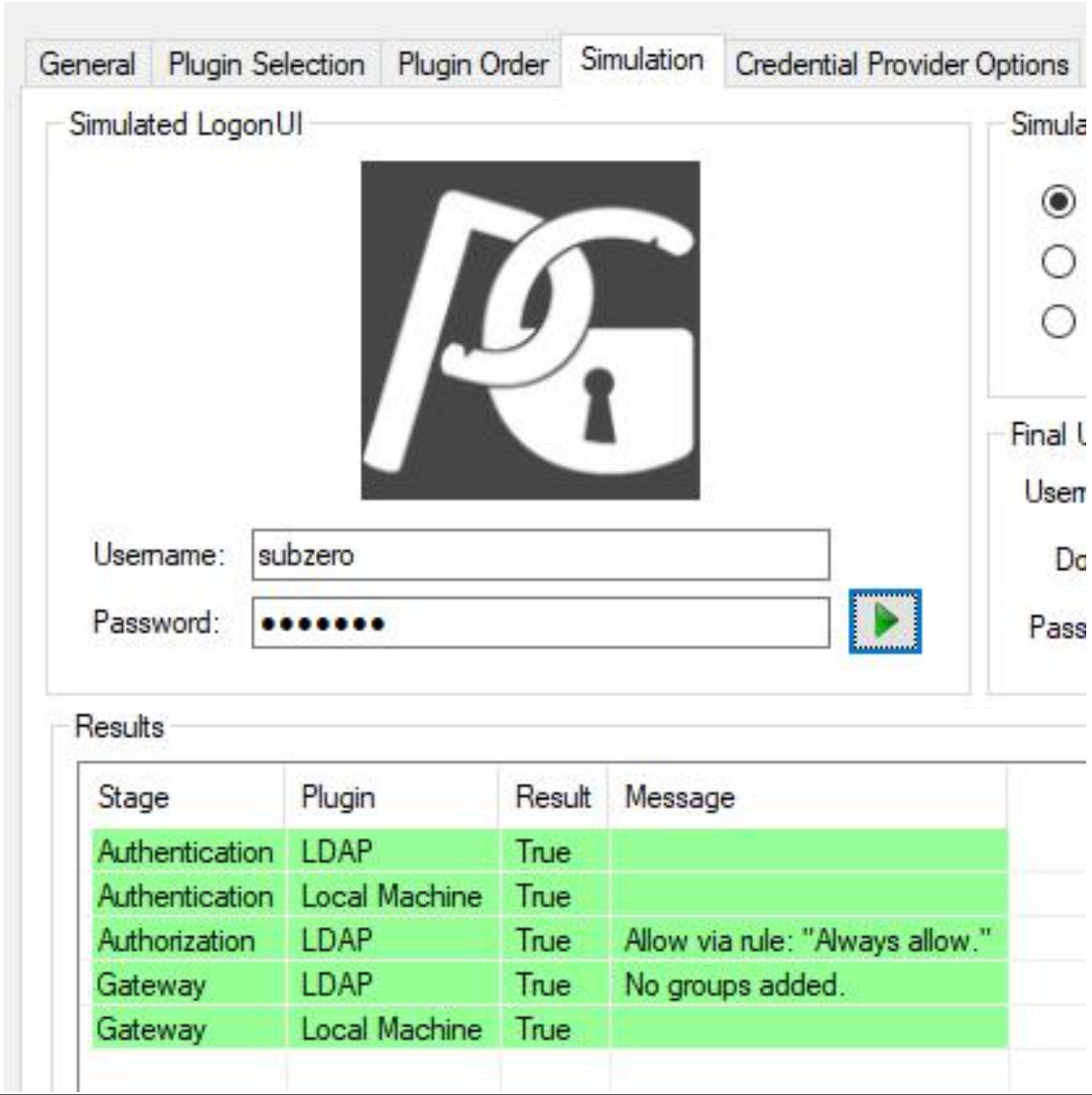
Plugin Name	Authentication	Authorization	Gateway	Notification	Description
LDAP	☑	☑	☑		Uses a LDAP serv
Local Machine	☑	☐	☑		Manages local mac
MySQL	☐	☐	☐		Uses a MySQL ser

Configuring Client (Windows)



Save > Apply

Configuring Client (Windows)



Configuring Client (Ubuntu)

```
sudo apt update
sudo apt install libnss-ldap libpam-ldap ldap-utils nscd
```

Configuring Client (Ubuntu)

```
Configuring ldap-auth-config
Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>:<port>/.
ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name
service problems.

LDAP server Uniform Resource Identifier:

ldapi:///192.168.1.121

<Ok>
```

Configuring Client (Ubuntu)

```
Configuring ldap-auth-config
Please enter the distinguished name of the LDAP search base. Many sites
use the components of their domain names for this purpose. For example,
the domain "example.net" would use "dc=example,dc=net" as the
distinguished name of the search base.

Distinguished name of the search base:

dc=myserver,dc=local

<Ok>
```

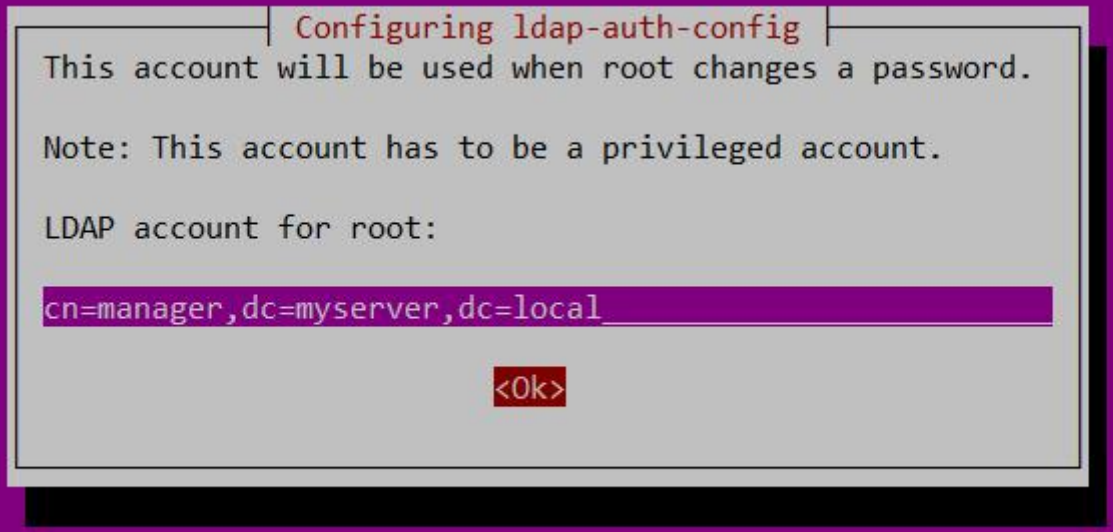
Configuring Client (Ubuntu)

```
Configuring ldap-auth-config

This option will allow you to make password utilities that use pam to
behave like you would be changing local passwords.

The password will be stored in a separate file which will be made
readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should
disable this.

Make local root Database admin:

                <Yes>                    <No>
```

Configuring Client (Ubuntu)

```
Configuring ldap-auth-config

Choose this option if you are required to login to the database to
retrieve entries.

Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

                <Yes>                    <No>
```

Configuring Client (Ubuntu)



Configuring Client (Ubuntu)

```
Configuring ldap-auth-config
Please enter the password to use when ldap-auth-config tries to login to
the LDAP directory using the LDAP account for root.

The password will be stored in a separate file /etc/ldap.secret which
will be made readable to root only.

Entering an empty password will re-use the old password.

LDAP root account password:

******

<Ok>
```

Configuring Client (Ubuntu)

```
┤ PAM configuration ├
Pluggable Authentication Modules (PAM) determine how authentication, authorization, and password changing are
handled on the system, as well as allowing configuration of additional actions to take when starting user
sessions.

Some PAM module packages provide profiles that can be used to automatically adjust the behavior of all PAM-using
applications on the system.  Please indicate which of these behaviors you wish to enable.

PAM profiles to enable:

  [*] Unix authentication
  [*] LDAP Authentication
  [*] Register user sessions in the systemd control group hierarchy
  [*] Create home directory on login
  [*] Inheritable Capabilities Management

                    <Ok>                    <Cancel>
```