joe@ldap2:~$ sudo apt-get install slapd ldap-utils
Configuring slapd

Please enter the password for the admin entry in your LDAP directory.

Administrator password:

<ok>
Please enter the admin password for your LDAP directory again to verify that you have typed it correctly.

Confirm password:

**********

<ok>
joe@ldap2:~$ sudo dpkg-reconfigure slapd
If you enable this option, no initial configuration or database will be created for you.

Omit OpenLDAP server configuration?

<Yes>  <No>
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:

zero.cs.dixie.edu

<ok>
Configuring slapd

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

Organization name:

joezero

<ok>
Package configuration

Configuring slapd

Please enter the password for the admin entry in your LDAP directory.

Administrator password:

***********

<ok>
Configuring slapd

Please enter the admin password for your LDAP directory again to verify that you have typed it correctly.

Confirm password:

******

<ok>
Configuring slapd

The HDB backend is recommended. HDB and BDB use similar storage formats, but HDB adds support for subtree renames. Both support the same configuration options.

In either case, you should review the resulting database configuration for your needs. See /usr/share/doc/slapd/README.DB_CONFIG.gz for more details.

Database backend to use:

```text
BDB
HDB
```

<ok>
Configuring slapd

Do you want the database to be removed when slapd is purged?

<Yes>  <No>
Package configuration

Configuring slapd

There are still files in /var/lib/ldap which will probably break the configuration process. If you enable this option, the maintainer scripts will move the old database files out of the way before creating a new database.

Move old database?

<Yes>  <No>
The obsolete LDAPv2 protocol is disabled by default in slapd. Programs and users should upgrade to LDAPv3. If you have old programs which can't use LDAPv3, you should select this option and 'allow bind_v2' will be added to your slapd.conf file.

Allow LDAPv2 protocol?
joe@ldap2:~$ sudo slapcat | grep ^dn
dn: dc=zero,dc=cs,dc=dixie,dc=edu
dn: cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu
joe@ldap2:~$ echo "Looks like my dit has begun"
Looks like my dit has begun
joe@ldap2:~$
sudo slapcat -b 'cn=config' | grep '^olcAccess'

olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external
olcAccess: {1}to dn.exact="" by * read
olcAccess: {2}to dn.base="cn=Subschema" by * read
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymous
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu" write by * read

echo "We will be modifying some of these access controls"
We will be modifying some of these access controls

joe@ldap2:~$
cat ou-People.ldif

dn: ou=People,dc=zero,dc=cs,dc=dixie,dc=edu
ou: People
objectClass: top
objectClass: organizationalUnit

echo "I created the above file"

ldapadd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu'
-W -H ldap:/// -f ou-People.ldif

Enter LDAP Password:
adding new entry "ou=People,dc=zero,dc=cs,dc=dixie,dc=edu"
cat ou-Groups.ldif

dn: ou=Groups,dc=zero,dc=cs,dc=dixie,dc=edu
ou: Groups
objectClass: top
objectClass: organizationalUnit

ldapadd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu'
-W -H ldap:/// -f ou-Groups.ldif

Enter LDAP Password:
adding new entry "ou=Groups,dc=zero,dc=cs,dc=dixie,dc=edu"
joe@ldap2:~/ldap-files-security$ cat ou-Etc.ldif
dn: ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu
ou: Etc
objectClass: top
objectClass: organizationalUnit

joe@ldap2:~/ldap-files-security$ ldapadd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu'
-W -H ldap:// -f ou-Etc.ldif
Enter LDAP Password:
adding new entry "ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu"
joe@ldap2:~/ldap-files-security$ cat cn-nonpriv.ldif
dn: cn=nonpriv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: nonpriv
description: User-level LDAP read-only administrator
userPassword: nonprivsecret

joe@ldap2:~/ldap-files-security$ ldapadd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu'
-W -H ldap:/// -f cn-nonpriv.ldif
Enter LDAP Password:
adding new entry "cn=nonpriv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu"
ldap_add: Invalid syntax (21)
    additional info: objectClass: value #1 invalid per syntax

joe@ldap2:~/ldap-files-security$ vi cn-nonpriv.ldif
joe@ldap2:~/ldap-files-security$ ldapadd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu'
-W -H ldap:/// -f cn-nonpriv.ldif
Enter LDAP Password:
adding new entry "cn=nonpriv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu"

joe@ldap2:~/ldap-files-security$ echo "Note what happens when you have an error above"
Note what happens when you have an error above
joe@ldap2:~/ldap-files-security$
cat cn-priv.ldif

dn: cn=priv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: priv
description: Root-level LDAP read-only administrator
userPassword: privsecret

ldapadd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu'
-W -H ldap:/// -f cn-priv.ldif

Enter LDAP Password:
adding new entry "cn=priv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu"
cat cn-eskeleto.ldif

ldapadd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu'
-W -H ldap:/// -f cn-eskeleto.ldif

Enter LDAP Password:
adding new entry "cn=eskeleto,ou=Groups,dc=zero,dc=cs,dc=dixie,dc=edu"
cat uid-eskeleto.ldif

dn: uid=eskeleto,ou=People,dc=zero,dc=cs,dc=dixie,dc=edu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: Foo Eskeleto
uid: eskeleto
uidNumber: 11000
gidNumber: 11000
homeDirectory: /home/eskeleto
loginShell: /bin/bash
gecos: F. Eskeleto,,
shadowLastChange: 14000
shadowMax: 99999
shadowWarning: 7

ldapadd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu'
-W -H ldap:// -f uid-eskeleto.ldif

Enter LDAP Password:
adding new entry "uid=eskeleto,ou=People,dc=zero,dc=cs,dc=dixie,dc=edu"
ldappasswd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu' -W -H ldap:// -S 'uid=eskeleto,ou=People,dc=zero,dc=cs,dc=dixie,dc=edu'
New password:
Re-enter new password:
passwords do not match
ldappasswd -x -D 'cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu' -W -H ldap:// -S 'uid=eskeleto,ou=People,dc=zero,dc=cs,dc=dixie,dc=edu'
New password:
Re-enter new password:
Enter LDAP Password:
"Just set his password"
dn: olcDatabase={1}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=zero,dc=cs,dc=dixie,dc=edu

access: {0} to attr=userPassword,shadowLastChange by self write by anonymous
auth by dn="cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu" write by * none
access: {1} to dn.base="" by * read
access: {2} to * by dn="cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu" write by * read
olcLastMod: TRUE
olcRootDN: cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu
olcRootPW:: e1NTSEF90DDqMkdmnpxbi9TL3Qva0Y1L0lUVDil3MHpJOW5EaG0=
olcDbCheckpoint: 512 30
olcDbConfig: {0}set_cachesize 0 2097152 0
olcDbConfig: {1}set_lk_max_objects 1500
olcDbConfig: {2}set_lk_max_locks 1500
olcDbConfig: {3}set_lk_max_lockers 1500
olcDbIndex: objectClass eq
structuralObjectClass: olcHdbConfig
entryUUID: 6437eb4a-5a21-1035-8861-4500a8d7f3b6
creatorsName: cn=config
createTimestamp: 20160128154150Z
entryCSN: 20160128154150.247164Z#00000000#000#00000000
modifiersName: cn=config
modifyTimestamp: 20160128154150Z

(END)
Those are the access privileges that we are going to change
Updated Database Settings
dn: olcDatabase={1}hdb,cn=config
changelog: modify
replace: olcAccess
# access to password information
olcAccess: to attrs=userPassword,shadowLastChange
  by dn="cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu" write
  by dn="cn=priv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu" read
  by anonymous auth
  by self write
  by * none
# for client/server hand-shaking in the LDAP protocol
olcAccess: to dn.base="" by * read
# access to rest of the information
olcAccess: to *
  by dn="cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu" write
  by dn="cn=priv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu" read
  by dn="cn=nonpriv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu" read
  by * none
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0, cn=peercred, cn=external, cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}hdb, cn=config"
joe@ldap2:~/ldap-files-security$ echo "Lets look at those privileges again"
Lets look at those privileges again
joe@ldap2:~/ldap-files-security$ sudo slapcat -b 'cn=config' | less
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=zero,dc=cs,dc=dixie,dc=edu
olcLastMod: TRUE
olcRootDN: cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu
olcRootPW:: e1NTSEF90DDqMkdmanpXbi9TL3Qva0Y1L0lUVDL3MHpJOW5EaG0=
olcDbCheckpoint: 512 30
olcDbConfig: [0]set_cachesize 0 2097152 0
olcDbConfig: [1]set lk_max_objects 1500
olcDbConfig: [2]set lk_max_locks 1500
olcDbConfig: [3]set lk_max_lockers 1500
olcDbIndex: objectClass eq
structuralObjectClass: olcHdbConfig
entryUUID: 6437eb4a-5a21-1035-8861-4500a8d7f3b6
creatorsName: cn=config
createTimestamp: 20160128154150Z
olcAccess: [0]to attrs=userPassword,shadowLastChange by dn="cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu" write by dn="cn=priv,ou=Etc,dc=dsctux,dc=net" read by * nonymous auth by self write by * none
olcAccess: [1]to dn.base="" by * read
olcAccess: [2]to * by dn="cn=admin,dc=zero,dc=cs,dc=dixie,dc=edu" write by dn="cn=priv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu" read by dn="cn=nonpriv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu" read by * none

entryCSN: 20160128160716.383718Z#000000#000#0000000
modifiersName: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
modifyTimestamp: 20160128160716Z

~
PORT80

(END)
Here I am on potential LDAP client

```
 joe@ubuntu:~$ echo "Here I am on potential LDAP client"
Here I am on potential LDAP client
```

```
 joe@ubuntu:~$ sudo apt-get install libnss-ldap libpam-ldap ldap-utils
[sudo] password for joe:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  auth-client-config ldap-auth-client ldap-auth-config libldap-2.4-2
Suggested packages:
  libpam-cracklib nscl
The following NEW packages will be installed:
  auth-client-config ldap-auth-client ldap-auth-config libldap-2.4-2
  libpam-ldap
The following packages will be upgraded:
  libldap-2.4-2
1 upgraded, 6 newly installed, 0 to remove and 172 not upgraded.
Need to get 406 kB of archives.
After this operation, 1,280 kB of additional disk space will be used.
Do you want to continue? [Y/n] 
```
Package configuration

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:

ldap://144.38.220.202/
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=zero,dc=cs,dc=dixie,dc=edu

<ok>
Package configuration

Configuring ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

3
2

<Ok>
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 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>
Package configuration

Configuring ldap-auth-config

This account will be used when root changes a password.

Note: This account has to be a privileged account.

LDAP account for root:

\texttt{cn=priv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu}

<0k>
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 ldap-auth-config

Please enter the name of the account that will be used to log in to the LDAP database.

Warning: DO NOT use privileged accounts for logging in, the configuration file has to be world readable.

Unprivileged database user:

cn=nonpriv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu

<ok>
Configuring ldap-auth-config

Please enter the password that will be used to log in to the LDAP database.

Password for database login account:

***************

<ok>
sudo dpkg-reconfigure ldap-auth-config

```
If you have problems during client setup, you can re-run the above command
```

joe@ubuntu:~$ ls -l /etc/ldap.*
-rw-r--r-- 1 root root  8928 Jan 28 09:20 /etc/ldap.conf
-rw------- 1 root root   11 Jan 28 09:20 /etc/ldap.secret
joe@ubuntu:~$ sudo cat /etc/ldap.secret
privsecret
joe@ubuntu:~$ echo "Note that the configuration wizard just run put the values in here"
Note that the configuration wizard just run put the values in here
joe@ubuntu:~$
 joe@ubuntu:~$ egrep '^\(base|uri|bind|root\)' /etc/ldap.conf
base dc=zero,dc=cs,dc=dixie,dc=edu
uri ldap://144.38.220.202/
bind dn cn=nonpriv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu
bind pw nonprivsecret
root bind dn cn=priv,ou=Etc,dc=zero,dc=cs,dc=dixie,dc=edu
joe@ubuntu:~$
joe@ubuntu:~$ sudo vi /etc/nsswitch.conf
/etc/nsswitch.conf

# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:   compat ldap
group:    compat ldap
shadow:   compat ldap

hosts:    files dns
networks: files

protocols: db files
services:  db files
ethers:   db files
rpc:      db files

netgroup: nis
```
$ sudo id eskeleto
uid=11000(eskeleto) gid=11000(eskeleto) groups=11000(eskeleto)

$ sudo apt-get install finger
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  finger
0 upgraded, 1 newly installed, 0 to remove and 172 not upgraded.
Need to get 17.3 kB of archives.
After this operation, 68.6 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/trusty/universe/finger amd64 0.17-15 [17.3 kB]
Fetched 17.3 kB in 0s (50.0 kB/s)
Selecting previously unselected package finger.
(Reading database ... 55225 files and directories currently installed.)
Preparing to unpack .../finger_0.17-15_amd64.deb ...
Unpacking finger (0.17-15) ...
Processing triggers for man-db (2.6.7.1-1) ...
Setting up finger (0.17-15) ...

$ finger eskeleto
Login: eskeleto                      Name: F. Eskeleto
Directory: /home/eskeleto           Shell: /bin/bash
Never logged in.
No mail.
No Plan.

$ echo "YAY!"
YAY!
```
joe@ubuntu:~$ sudo mkdir /home/eskeleto
joe@ubuntu:~$ sudo chown eskeleto:eskeleto /home/eskeleto/
joe@ubuntu:~$
joe@ubuntu:~$ su - eskeleto
Password:
eskeleto@ubuntu:~$ pwd
/home/eskeleto
eskeleto@ubuntu:~$ ls -la
total 12
drwxr-xr-x 2 eskeleto eskeleto 4096 Jan 28 09:25 .
drwxr-xr-x 5 root root 4096 Jan 28 09:24 ..
-rw------- 1 eskeleto eskeleto 11 Jan 28 09:25 .bash_history
eskeleto@ubuntu:~$