Install OpenLDAP

Step 1: Install OpenLDAP
#sudo apt-get install slapd ldap-utils

step 2: Login as root
#sudo su

Step3: Configure OpenLDAP
#nano /etc/ldap/ldap.conf

Make sure the file looks as follows:
#
LDAP Defaults
#

see ldap.config(5) for details
This file should be world readable but not world writable.

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

#SIZELIMIT   12
#TIMELIMIT   15
#DEREF   NeVER

TLS certificates (needed for GnuTLS)
TLS_CACERT   /etc/ssl/certs/ca-certificates.crt

Save the file and exit

Step 4: Reconfigure the slapd with the updated values
#dpkg-reconfigure slapd

select "No" and Press Enter

Enter the DNS Domain Name
ldap.com

Enter the Organization Name: Enter any name
e.g IT610

Enter the LDAP admin Password

Select the backend Database
Choose “HDB”

On the next screen select "No"
click Yes to Move the Old Database
Select "No" under LDAPv2 Protocol

PART -B LDAP Server Administration
Install phpldapadmin Package
#apt-get install phpldapadmin
#nano /etc/phpldapadmin/config.php

#get IP address of your machine (For AWS, use the private IP)
#ipaddress

1. Edit the following value
Set your LDAP server name
$server->setValue('server','name', Anand LDAP Server');

Set your LDAP server IP address
$server->setValue('server','host','IP-Address');

set Server domain name
$server->setValue('server','base',array('dc=ldap,dc=com'));

Set Server domain name again
$server->setValue('login','bind_id','cn-admin,dc-ldap,dc-com')

$config->custom->appearance['hide_template_warning'] = true;

Exit the file

#systemctl restart apache2

Open Web browser
http://IP-Address/phpldapadmin

Login into OpenLdap and set up organizations, groups and users

2. Then set up a few more packages to connect to ldap server.
#sudo apt-get install libpam-ldap nscd

- in the prompt, remove one forward slash and set the ip address

- Enter your ldap server name
- Ldap server version to use, select 3
- Make local root database admin: Yes
- Require login? No
- Set you ldap account for root (cn=admin,dc=ldap,dc=com)
- Enter ldap root account password

Edit the following file
#sudo nano /etc/nsswitch.conf

Add ldap word on from of compat as the fallowing:

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

Edit the following file
#sudo nano /etc/pam.d/common-session
add this line at the end:

```
session required        pam_mkhomedir.so skel=/etc/skel umask=0022
```

Restart the service:
#sudo /etc/init.d/nscd restart

download ssh if needed
#sudo apt-get install ssh

In order for openldap users to login to AWS the public key has to be saved in the ldap user directory.
In the console login in AWS using the Ubuntu username
#mkdir .ssh
#chmod 700 .ssh
#touch .ssh/authorized_keys
#chmod 600 .ssh/authorized_keys
Generate public key for the user. Open a second terminal find the directory of your private key.
#ssh-keygen –y
Copy the generated publick key and in the previous terminal
#nano .ssh/authorized_keys
Paste the public key and save and exit.
This openldap user now will be able to log into AWS now.

Then test your ldap user by try to log:
#ssh ajohn@IPaddress

--add user to sudo
#sudo adduser username sudo

--change user password
#sudo passwd username

Set up quota

```
apt-get install quota quotatool
touch quota.user quota.group
chmod 600 quota.user
chmod 600 quota.group
mount -o remount /
sudo quotacheck -mavug
edquota -u ajohn
repquota -u /
```