# LDAP SERVER & CLEINT CONFIGURATION FOR RHEL 6 WITH LTS

**I made this belog to help anyone to install and configuration ldap server and client I hope it will be easy for all.**

## Packages Required

We need to install the following packages for both ldap server and client except **migrationtools-47-7.el6.noarch** it will be on server only.

compat-openldap-2.3.43-2.el6.i686

openldap-servers-2.4.23-15.el6.i686

openldap-clients-2.4.23-15.el6.i686

openldap-2.4.23-15.el6.i686

openldap-devel-2.4.23-15.el6.i686

nss-pam-ldapd-0.7.5-7.el6.i686

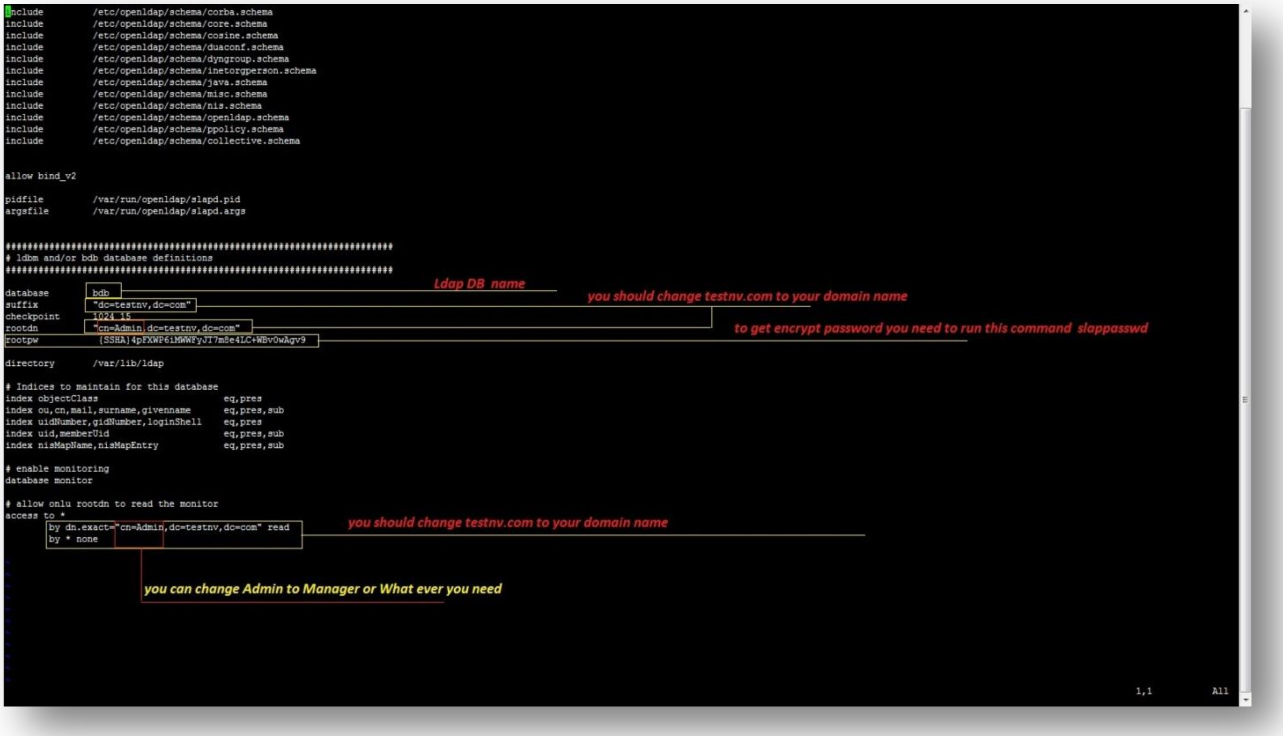
migrationtools-47-7.el6.noarch

# Server side configuration

**<u>We need to run the following command at server side:</u>**

1- # cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf

2- #vim /etc/openldap/slapd.conf you need to change few things based one photo below



```
include         /etc/openldap/schema/corba.schema
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/duaconf.schema
include         /etc/openldap/schema/dyngroup.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/java.schema
include         /etc/openldap/schema/misc.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/ppolicy.schema
include         /etc/openldap/schema/collective.schema


allow bind_v2

pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args


#######################################################################
# ldbm and/or bdb database definitions
#######################################################################

database        bdb
suffix          "dc=testnv,dc=com"
checkpoint      1024 15
rootdn          "cn=Admin,dc=testnv,dc=com"
rootpw           {SSHA}4pFXWP6iMWWFyJT7m8e4LC+WBv0wAgv9

directory       /var/lib/ldap

# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub

# enable monitoring
database monitor

# allow onlu rootdn to read the monitor
access to *
        by dn.exact="cn=Admin,dc=testnv,dc=com" read
        by * none

                                                                  1,1           All
```

Ldap DB name

you should change testnv.com to your domain name

to get encrypt password you need to run this command slappasswd

you should change testnv.com to your domain name

you can change Admin to Manager or What ever you need

3- To enable TLS you should add the following lines in /etc/openldap/slapd.conf

**TLSCipherSuite HIGH:MEDIUM:+SSLv2:+SSLv3:RSA**
**TLSCACertificateFile /etc/openldap/cacerts/server.pem**
**TLSCertificateFile /etc/openldap/cacerts/server.pem**
**TLSCertificateKeyFile /etc/openldap/cacerts/server.pem**
**TLSVerifyClient allow**

4- Under /etc/openldap/slapd.d/ you will see folder called cn=config we need to add few lines at the following file olcDatabase={1}bdb.ldif

5- vim /etc/openldap/slapd.d/cn\=config/olcDatabase\=\{1\}bdb.ldif and the lines below

```
olcRootPW: {SSHA}ccFKiy8ska8IhNwwlaNYxiBNbilWe5M1(output of slappasswd)
olcTLSCertificateFile: /etc/openldap/cacerts/server.pem
olcTLSCertificateKeyFile: /etc/openldap/cacerts/server.pem
```

6- after finished editing file press Esc and press : to be in command mode in vim like the command below

```
:%s/dc=my-domain,dc=com/dc=your_domain,dc=com/g then press :x
```

7- that above command will replace my-domain and com with new domain

8- Copy a default DB_CONFIG file which sets cache and tuning options for the Berkley database backend (this also needs to be writeable by the ldap user). `cp /usr/share/doc/openldap-servers-*/DB_CONFIG.example /var/lib/ldap/DB_CONFIG`

9- Create test user to make test with this user ldapuser1 and ldapuser2 through the following command

```
#useradd -g users ldapuser1
#passwd ldapuser1 and set user password
```

10- Now we need to create ldap db through the following command

```
#vim /usr/share/migrationtools/migrate_common.ph
# in command mode at vim for above file you should write the following
:%s/dc=my-domain,dc=com/dc=your_domain,dc=com/g
```

Then press :x to save your change

```
#cd /usr/share/migrationtools
#./migrate_all_offline.sh this will rebuild ldap DB under /var/lib/ldap
```

11- Now you should change owner ship of ldap DB files to ldap and ldap group too through the following command

```
#chown -R ldap.ldap /var/lib/ldap
#chown -R ldap.ldap /etc/openldap/slapd.d
```

# Enable TLS

12- Now we will create certificate file to enable TLS through openssl command please check commands below:

```
#cd /etc/openldap/cacerts/
#openssl req -newkey rsa:1024 -x509 -nodes -out server.pem -keyout\
server.pem -days 3650
```

Then fill information like country stat.

13- Now you have certificate file for both server and client side at same file we will the following command to create separate certificate file for client side

```
#grep -A 100 CERTIFICATE server.pem > client.pem
#chown -R ldap:ldap /etc/openldap/cacerts/
```

14- `vim /etc/sysconfig/ldap` then change the following like from no to yes

```
SLAPD_LDAPS=yes
```

# Base domain configuration & migration

15- we need to creat ldif file under /etc/openldap/schema/ not must to create it under this path but to collect all config files of ldap under one place this files it will help us to add user in ldap server

```
# cd /etc/openldap/schema/
#vim base.ldif
```

```
dn: dc=your_domain,dc=com
dc: your_domain
objectClass: top
objectClass: domain
dn: ou=People,dc= your_domain,dc= com
ou: People
objectClass: top
objectClass: organizationalUnit
dn: ou=Group,dc= your_domain,dc=com
ou: Group
objectClass: top
objectClass: organizationalUnit
```

```
# /usr/share/migrationtools/migrate_passwd.pl /etc/passwd people.ldif
# /usr/share/migrationtools/migrate_group.pl /etc/group group.ldif
```

16- now you can start sldap service by the following command:

```
# /etc/rc.d/init.d/slapd start
```

# Test server configuration

17- Now we need to verify our config work fine or not first we need to check is ldaps ports by the following commands

```
#netstat -lt | grep ldaps
tcp        0      0 *:ldaps                    *:*
LISTEN
tcp        0      0 *:ldaps                    *:*
LISTEN
```

```
# ldapsearch -x -b '' -s base '(objectclass=*)' namingContexts
The output it should be like the following lines
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: (objectclass=*)
# requesting: namingContexts
#

#
dn:
namingContexts: dc=testnv,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

**18-** Now we will try to add Admin user in ldap by the following command:

```
#ldapadd -x -W -D "cn=Admin,dc=your_domain,dc=com" -f  \
/etc/openldap/schema/base.ldif
```

After that command you should enter the ldap password you had entered by command slappasswd and you should see result like the box below

```
adding new entry "dc= your_domain,dc=com"
adding new entry "ou=People,dc= your_domain,dc=com"
adding new entry "ou=Group,dc= your_domain,dc=com"
```

# Client Configuration

Now that we have a server which is responding correctly, we can configure our clients to authenticate to the LDAP server.

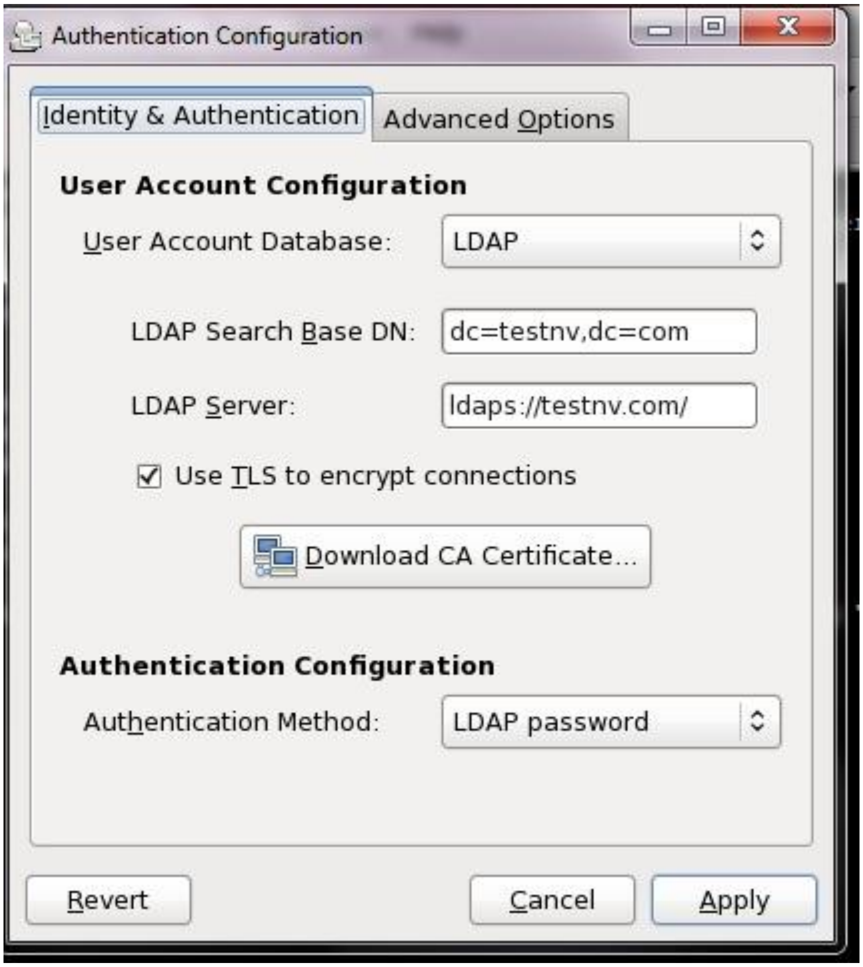
There is easy tool configure the machine as ldap client it called **system-config-authentication**.

We will explain how to use it below

**19-** From command line at client machine run

```
# system-config-authentication &
```

You will get at your screen the following photo


Authentication Configuration
Identity & Authentication
Advanced Options

User Account Configuration

User Account Database: LDAP

LDAP Search Base DN: dc=testnv,dc=com

LDAP Server: ldaps://testnv.com/

☑ Use TLS to encrypt connections

Download CA Certificate...

Authentication Configuration

Authentication Method: LDAP password

**20-** Please note you should replace testnv and come with your domain name.

**21-** You must use ldap password for authentication method

**22-** Check box for use TLS to encrypt connections

**23-** The file called client.pem we had created before you should upload it on http web server or ftp We will use here http server for example [http://xx.xx.xx.xx/rhel6/client.pem](http://xx.xx.xx.xx/rhel6/client.pem) then press apply.

# Client configuration verification

**24-** After filling information at above box you need to check first the certificate file loaded correctly at your system through the following command

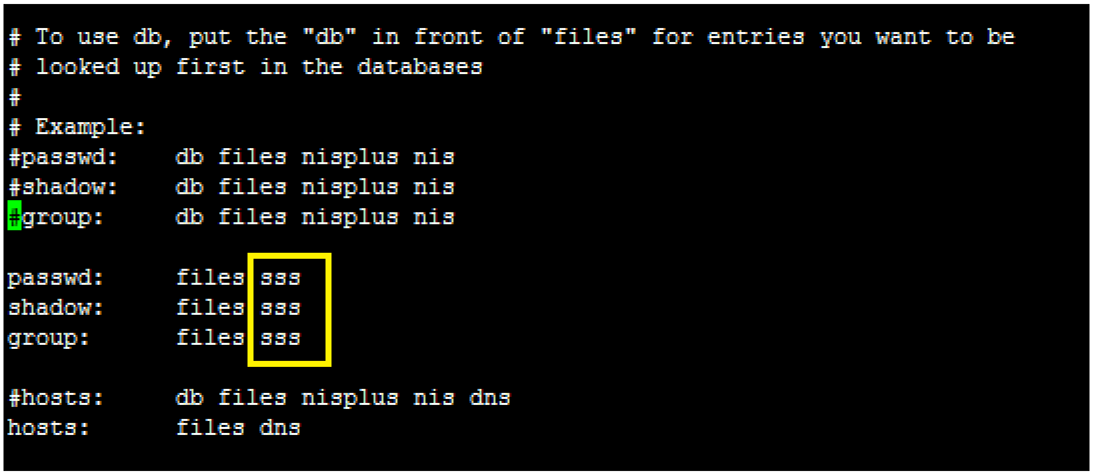
# cd /etc/openldap/cacerts

Run ls with l option you will see the client.pem name converted to authconfig_downloaded.pem as command output showed

```
# ll
total 4
-rw-r--r-- 1 root root 1038 Sep 23 15:42 authconfig_downloaded.pem
lrwxrwxrwx 1 root root   25 Sep 23 18:38 fde58659.0 -> authconfig_downloaded.pem
```

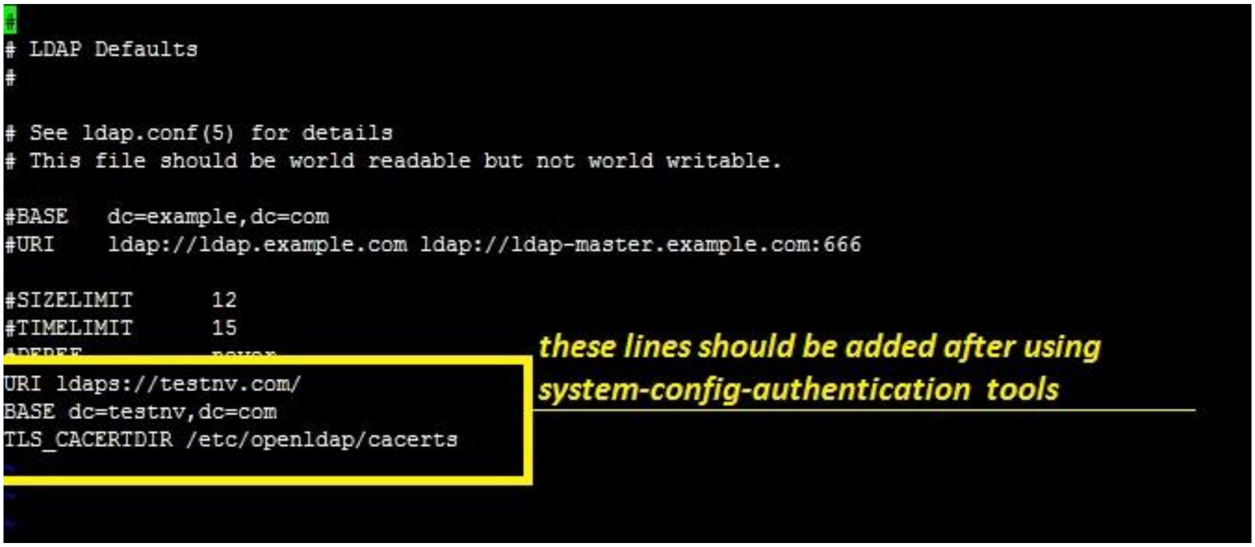
**25-** We need to check network switch by # vi /etc/nsswitch.conf

You will see the tool added **sss** passwd, shadow and group section please check the photo below.



```
# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis

passwd:     files sss
shadow:     files sss
group:      files sss

#hosts:     db files nisplus nis dns
hosts:      files dns
```

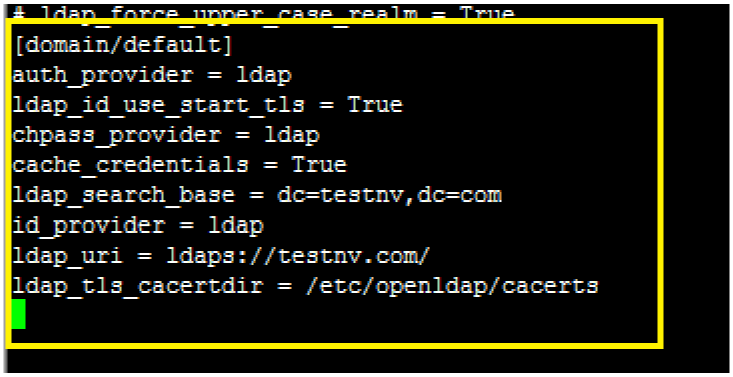
**26-** We need to check now **ldap.conf** under /etc/openldap
The photo below will show what line has added in that file



```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never
URI ldaps://testnv.com/
BASE dc=testnv,dc=com
TLS_CACERTDIR /etc/openldap/cacerts
```

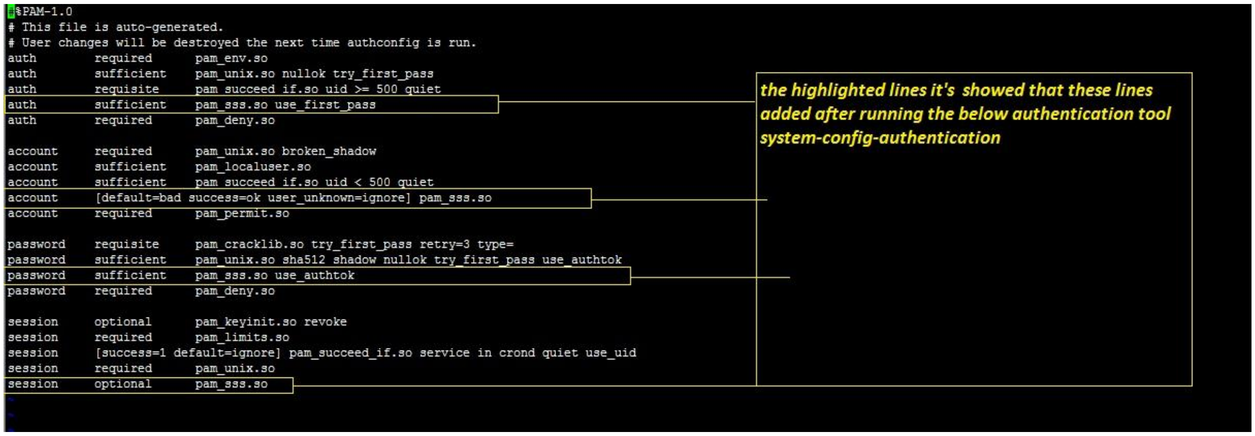
*these lines should be added after using system-config-authentication tools*

**27-** At sssd.conf under /etc/sssd you should see the same like photo above at end of this file under [domain/default] section



```
# ldap_force_upper_case_realm = True
[domain/default]
auth_provider = ldap
ldap_id_use_start_tls = True
chpass_provider = ldap
cache_credentials = True
ldap_search_base = dc=testnv,dc=com
id_provider = ldap
ldap_uri = ldaps://testnv.com/
ldap_tls_cacertdir = /etc/openldap/cacerts
```

**28-** The last file you should check configuration at it password-auth under /etc/pam.d
Please check photo below



```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam succeed if.so uid >= 500 quiet
auth        sufficient    pam_sss.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam succeed if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    sufficient    pam_sss.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_sss.so
```

*the highlighted lines it's showed that these lines added after running the below authentication tool system-config-authentication*

# Add new user at ldap server how to

To add new user at ldap server we need to do the following steps

**29-** Run useradd command at ldap server

- A) #useradd **newuser ;** passwd **newuser**
- B) we need to migrate new user base on the following commands explain
- C) **#cat /etc/passwd | grep newuser > /etc/openldap/schema/newuser**
- D) **# /usr/share/migrationtools/migrate_passwd.pl /etc/openldap/schema/newuser \ /etc/openldap/schema/ newuser.ldif**
- E) **Also we need to update ldap user group by run the following command**

  ```
  # cat /etc/group | grep newuser > newuser.group
  #/usr/share/migrationtools/migrate_group.pl newuser.group newuser.group.ldif
  ```
- F) **Now you can run ldapadd like example below to update ldap with new users**

  ```
  #ldapadd -cxWD cn=Admin,dc=testnv,dc=com -f newuser.ldif
  ```

  **Also we need to update ldap with new users groups by run the following command**

  ```
  #ldapadd -cxWD cn=Admin,dc=testnv,dc=com -f newuser.group.ldif
  ```

**30- Now we need to share /home via nfs service**

**#vim /etc/exports and add the lines below**

```
/home      *(rw,sync)
# service nfs restart
```

**31- At client we need to enable auto mount for ldap server home directory vi the following steps**

- **A) #vi /etc/auto.master ( add the following line)**

  ```
  /home      /etc/auto.home --timeout 60
  ```

  **Then save via :x**
- **B) create new file under /etc called aut.home**

  **#vi /etc/auto.home ( add the following line at this file)**

  ```
  *     -fstype=nfs,rw,intr,rsize=32768,wsize=32768,hard,bg,nosuid,noexec,tcp you_nfs_server_ip:/home/&
  ```
- **C) we need to restart autofs via service command**

  ```
  # service autofs restart
  ```
- **D) at ldap client you can try to run su command followed by newuser as example below showing**

  ```
  [root@localhost ~]# su - newuser
  [newuser@localhost ~]$
  ```

**32- now your ldap server working fine and have a nice day :D**

*Collected and written by Mostafa Galmad*