LDAP Server & Client Configuration

First check server & clients hostname & IP address-

```
[root@ldap-server ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.78.151  netmask 255.255.255.0  broadcast 192.168.78.255
        inet6 fe80::2b78:2a99:23fd:73b1  prefixlen 64  scopeid 0x20<link>
```

```
[root@ldap-server ~]# hostname
ldap-server.cricbuzz.com
```

```
[root@client1 ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.78.152  netmask 255.255.255.0  broadcast 192.168.78.255
        inet6 fe80::8f97:7078:1751:8e7f  prefixlen 64  scopeid 0x20<link>
```

```
[root@client1 ~]# hostname
client1.cricbuzz.com
[root@client1 ~]#
```

Server Configuration: -

Domain: cricbuzz.com

1. At server, hostname & IP in /etc/hosts file as we don't have DNS configured-

```
[root@ldap-server ~]# vim /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.78.151 ldap-server.cricbuzz.com
192.168.78.152 client1.cricbuzz.com
```

2. Install required packages to setup LDAP-

```
[root@ldap-server ~]#
[root@ldap-server ~]# yum install -y openldap openldap-clients openldap-servers migrationtools
```

3. Set password for LDAP & store it in encrypted form-

```
[root@ldap-server ~]# slappasswd -s redhat -n > /etc/openldap/passwd
[root@ldap-server ~]# cat /etc/openldap/passwd
{SSHA}NhugkFCPdBvUWJDRWVYx6i28P1NSUa4b[root@ldap-server ~]#
```

4. Now we will generate a certificate for 365 days-

```
[root@ldap-server ~]# openssl req -new -x509 -nodes -out /etc/openldap/certs/cert.pem -keyout /etc/openldap/certs/priv.pem -days 365
Generating a 2048 bit RSA private key
.....................................................................................................................+++
........+++
writing new private key to '/etc/openldap/certs/priv.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:Bihar
Locality Name (eg, city) [Default City]:Gaya
Organization Name (eg, company) [Default Company Ltd]:Cricket
Organizational Unit Name (eg, section) []:HO
Common Name (eg, your name or your server's hostname) []:ldap-server.cricbuzz.com
Email Address []:root@ldap-server.cricbuzz.com
[root@ldap-server ~]#
```

5. Go to certs directory & change files ownership to ldap-

```
[root@ldap-server ~]# cd /etc/openldap/certs/
[root@ldap-server certs]# ls -ll
total 92
-rw-r--r--. 1 root root 65536 Dec  8 09:07 cert8.db
-rw-r--r--. 1 root root  1464 Dec  8 09:14 cert.pem
-rw-r--r--. 1 root root 16384 Dec  8 09:07 key3.db
-r--r-----. 1 root ldap    45 Nov 21 18:57 password
-rw-r--r--. 1 root root  1704 Dec  8 09:14 priv.pem
-rw-r--r--. 1 root root 16384 Nov 21 18:57 secmod.db
```

```
[root@ldap-server certs]# chown ldap:ldap *
[root@ldap-server certs]# ls -ll
total 92
-rw-r--r--. 1 ldap ldap 65536 Dec  8 09:07 cert8.db
-rw-r--r--. 1 ldap ldap  1464 Dec  8 09:14 cert.pem
-rw-r--r--. 1 ldap ldap 16384 Dec  8 09:07 key3.db
-r--r-----. 1 ldap ldap    45 Nov 21 18:57 password
-rw-r--r--. 1 ldap ldap  1704 Dec  8 09:14 priv.pem
-rw-r--r--. 1 ldap ldap 16384 Nov 21 18:57 secmod.db
```

6. Change permission of file priv.pem to give read, write access to file owner only-

```
[root@ldap-server certs]# chmod 600 priv.pem
[root@ldap-server certs]#
[root@ldap-server certs]# ls -ll
total 92
-rw-r--r--. 1 ldap ldap 65536 Dec  8 09:07 cert8.db
-rw-r--r--. 1 ldap ldap  1464 Dec  8 09:14 cert.pem
-rw-r--r--. 1 ldap ldap 16384 Dec  8 09:07 key3.db
-r--r-----. 1 ldap ldap    45 Nov 21 18:57 password
-rw-------. 1 ldap ldap  1704 Dec  8 09:14 priv.pem
-rw-r--r--. 1 ldap ldap 16384 Nov 21 18:57 secmod.db
[root@ldap-server certs]#
```

7. Now we will prepare LDAP database & for that copy the DB_CONFIG.example as shown-

```
[root@ldap-server certs]#
[root@ldap-server certs]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
[root@ldap-server certs]#
```

8. Now to generate database, we will use command as shown below-

```
[root@ldap-server certs]#
[root@ldap-server certs]# slaptest
6391f1dd hdb_db_open: database "dc=my-domain,dc=com": db_open(/var/lib/ldap/id2entry.bdb) failed: No such file or directory (2).
6391f1dd backend_startup_one (type=hdb, suffix="dc=my-domain,dc=com"): bi_db_open failed! (2)
slap_startup failed (test would succeed using the -u switch)
[root@ldap-server certs]#
```

It is giving error, because we need to sync parameters in this file. We will modify it later.

9. We will change file ownership of all the files inside ldap directory to ldap-

```
[root@ldap-server certs]# chown ldap:ldap /var/lib/ldap/*
[root@ldap-server certs]#
```

10. Start & enable slapd service-

```
[root@ldap-server ~]# systemctl enable slapd.service --now
Created symlink from /etc/systemd/system/multi-user.target.wants/slapd.service to /usr/lib/systemd/system/slapd.service.
[root@ldap-server ~]#
```

11. Verify whether it is listening on ldap port or not-

```
[root@ldap-server ~]# netstat -lt | grep ldap
tcp        0      0 ldap-server.cric:domain 0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ldap            0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ldap               [::]:*                  LISTEN
```

12. Now we go to schema directory for adding schema for ldap & will put configuration from cosine.ldif & nis.ldif file into ldap directory-

```
[root@ldap-server ~]# cd /etc/openldap/schema/
[root@ldap-server schema]#
```

```
[root@ldap-server schema]# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f cosine.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=cosine,cn=schema,cn=config"
```

```
[root@ldap-server schema]# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f nis.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=nis,cn=schema,cn=config"
```

13. We will create one ldif file where we will specify all the parameters-

```
[root@ldap-server ~]# vim /etc/openldap/changes.ldif
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=cricbuzz,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=cricbuzz,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SSHA}NhugkFCPdBvUWJDRWVYx6i28P1NSUa4b

dn: cn=config
changetype: modify
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/openldap/certs/cert.pem

dn: cn=config
changetype: modify
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/openldap/certs/priv.pem

dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: -1

dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=Manager,dc=cricbuzz,dc=com" read by * none

dn: cn=config
changetype: modify
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/openldap/certs/cert.pem
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/openldap/certs/priv.pem
```

Here we will add that encrypted password for ldap in olcRootPw, generated earlier.

14. Now we will have to add all these entries in ldap using command as shown-

```
[root@ldap-server ~]#
[root@ldap-server ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/openldap/changes.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "cn=config"
ldap_modify: Other (e.g., implementation specific) error (80)
```

Ignore the last error.

15. Now create base.ldif file inside same directory where we will define few more parameters-

```
[root@ldap-server ~]# vim /etc/openldap/base.ldif
dn: dc=cricbuzz,dc=com
dc: cricbuzz
objectClass: top
objectClass: domain

dn: ou=People,dc=cricbuzz,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit

dn: ou=Group,dc=cricbuzz,dc=com
ou: Group
objectClass: top
objectClass: organizationalUnit
```

16. To build directory structure, we will add this newly created base.ldif file in ldap-

```
[root@ldap-server ~]# ldapadd -x -w redhat -D cn=Manager,dc=cricbuzz,dc=com -f /etc/openldap/base.ldif
adding new entry "dc=cricbuzz,dc=com"

adding new entry "ou=People,dc=cricbuzz,dc=com"

adding new entry "ou=Group,dc=cricbuzz,dc=com"
```

17. We will create home directory for ldap users, create ldap users & set their password-

```
[root@ldap-server ~]# mkdir /home/guests
[root@ldap-server ~]#
[root@ldap-server ~]# useradd -d /home/guests/ldapuser01 ldapuser01
[root@ldap-server ~]#
[root@ldap-server ~]# passwd ldapuser01
Changing password for user ldapuser01.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ldap-server ~]#
[root@ldap-server ~]# useradd -d /home/guests/ldapuser02 ldapuser02
[root@ldap-server ~]# passwd ldapuser02
Changing password for user ldapuser02.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

18. Now we will migrate these user accounts. For this we will have to make their entry in ldap directory for authentication to be completed-

```
[root@ldap-server ~]# cd /usr/share/migrationtools
[root@ldap-server migrationtools]#
```

19. Next, we will add our domain in shown file-

```
[root@ldap-server migrationtools]# vim migrate_common.ph
        $NAMINGCONTEXT{'networks'}          = "cn=networks";
        $NAMINGCONTEXT{'protocols'}         = "cn=protocols";
        $NAMINGCONTEXT{'rpc'}               = "cn=rpcs";
        $NAMINGCONTEXT{'services'}          = "cn=services";
} else {
        $NAMINGCONTEXT{'aliases'}           = "ou=Aliases";
        $NAMINGCONTEXT{'fstab'}             = "ou=Mounts";
        $NAMINGCONTEXT{'passwd'}            = "ou=People";
        $NAMINGCONTEXT{'netgroup_byuser'}   = "nisMapName=netgroup.byuser";
        $NAMINGCONTEXT{'netgroup_byhost'}   = "nisMapName=netgroup.byhost";
        $NAMINGCONTEXT{'group'}             = "ou=Group";
        $NAMINGCONTEXT{'netgroup'}          = "ou=Netgroup";
        $NAMINGCONTEXT{'hosts'}             = "ou=Hosts";
        $NAMINGCONTEXT{'networks'}          = "ou=Networks";
        $NAMINGCONTEXT{'protocols'}         = "ou=Protocols";
        $NAMINGCONTEXT{'rpc'}               = "ou=Rpc";
        $NAMINGCONTEXT{'services'}          = "ou=Services";
}

# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "cricbuzz.com";

# Default base
$DEFAULT_BASE = "dc=cricbuzz,dc=com";
```

20. Verify the ldap users created locally-

```
[root@ldap-server migrationtools]# tail -2 /etc/passwd
ldapuser01:x:1001:1001::/home/guests/ldapuser01:/bin/bash
ldapuser02:x:1002:1002::/home/guests/ldapuser02:/bin/bash
[root@ldap-server migrationtools]#
```

21. Now we will add users whose id equal to or greater than 1000 in same directory inside passwd file & verify the same-

```
[root@ldap-server migrationtools]# grep ":10[0-9][0-9]" /etc/passwd > passwd
[root@ldap-server migrationtools]#
[root@ldap-server migrationtools]# cat passwd
abhay:x:1000:1000:abhay singh:/home/abhay:/bin/bash
ldapuser01:x:1001:1001::/home/guests/ldapuser01:/bin/bash
ldapuser02:x:1002:1002::/home/guests/ldapuser02:/bin/bash
[root@ldap-server migrationtools]#
```

22. We will create users.ldif using one of script file inside migrationtools directory & will verify the same-

```
[root@ldap-server migrationtools]# ./migrate_passwd.pl passwd users.ldif
[root@ldap-server migrationtools]#
[root@ldap-server migrationtools]# ll
total 136
-rwxr-xr-x. 1 root root  2652 Dec 28  2013 migrate_aliases.pl
-rwxr-xr-x. 1 root root  2950 Dec 28  2013 migrate_all_netinfo_offline.sh
-rwxr-xr-x. 1 root root  2946 Dec 28  2013 migrate_all_netinfo_online.sh
-rwxr-xr-x. 1 root root  3011 Dec 28  2013 migrate_all_nis_offline.sh
-rwxr-xr-x. 1 root root  3006 Dec 28  2013 migrate_all_nis_online.sh
-rwxr-xr-x. 1 root root  3164 Dec 28  2013 migrate_all_nisplus_offline.sh
-rwxr-xr-x. 1 root root  3146 Dec 28  2013 migrate_all_nisplus_online.sh
-rwxr-xr-x. 1 root root  5267 Dec 28  2013 migrate_all_offline.sh
-rwxr-xr-x. 1 root root  7468 Dec 28  2013 migrate_all_online.sh
-rwxr-xr-x. 1 root root  3278 Dec 28  2013 migrate_automount.pl
-rwxr-xr-x. 1 root root  2608 Dec 28  2013 migrate_base.pl
-rw-r--r--. 1 root root  8888 Dec  8 09:54 migrate_common.ph
-rwxr-xr-x. 1 root root  2952 Dec 28  2013 migrate_fstab.pl
-rwxr-xr-x. 1 root root  2714 Dec 28  2013 migrate_group.pl
-rwxr-xr-x. 1 root root  3087 Dec 28  2013 migrate_hosts.pl
-rwxr-xr-x. 1 root root  2856 Dec 28  2013 migrate_netgroup_byhost.pl
-rwxr-xr-x. 1 root root  2856 Dec 28  2013 migrate_netgroup_byuser.pl
-rwxr-xr-x. 1 root root  3879 Dec 28  2013 migrate_netgroup.pl
-rwxr-xr-x. 1 root root  2840 Dec 28  2013 migrate_networks.pl
-rwxr-xr-x. 1 root root  5635 Dec 28  2013 migrate_passwd.pl
-rwxr-xr-x. 1 root root  2428 Dec 28  2013 migrate_profile.pl
-rwxr-xr-x. 1 root root  2873 Dec 28  2013 migrate_protocols.pl
-rwxr-xr-x. 1 root root  2854 Dec 28  2013 migrate_rpc.pl
-rwxr-xr-x. 1 root root 11465 Dec 28  2013 migrate_services.pl
-rwxr-xr-x. 1 root root  3419 Dec 28  2013 migrate_slapd_conf.pl
-rw-r--r--. 1 root root   168 Dec  8 09:55 passwd
-rw-r--r--. 1 root root  1347 Dec  8 09:56 users.ldif
[root@ldap-server migrationtools]#
```

```
[root@ldap-server migrationtools]#
[root@ldap-server migrationtools]# cat users.ldif
```

23. Using this file, we will add the users entry in ldap-

```
[root@ldap-server migrationtools]# ldapadd -x -w redhat -D cn=Manager,dc=cricbuzz,dc=com -f users.ldif
adding new entry "uid=abhay,ou=People,dc=cricbuzz,dc=com"

adding new entry "uid=ldapuser01,ou=People,dc=cricbuzz,dc=com"

adding new entry "uid=ldapuser02,ou=People,dc=cricbuzz,dc=com"

[root@ldap-server migrationtools]#
```

24. We will do the same thing for groups-

```
[root@ldap-server migrationtools]# grep ":10[0-9][0-9]" /etc/group > group
[root@ldap-server migrationtools]#
[root@ldap-server migrationtools]# ./migrate_group.pl group groups.ldif
[root@ldap-server migrationtools]#
[root@ldap-server migrationtools]# ll
total 144
-rw-r--r--. 1 root root    57 Dec  8 09:58 group
-rw-r--r--. 1 root root   416 Dec  8 09:58 groups.ldif
```

```
[root@ldap-server migrationtools]# cat groups.ldif
```

```
[root@ldap-server migrationtools]# ldapadd -x -w redhat -D cn=Manager,dc=cricbuzz,dc=com -f groups.ldif
adding new entry "cn=abhay,ou=Group,dc=cricbuzz,dc=com"

adding new entry "cn=ldapuser01,ou=Group,dc=cricbuzz,dc=com"

adding new entry "cn=ldapuser02,ou=Group,dc=cricbuzz,dc=com"

[root@ldap-server migrationtools]#
```

25. Now we will check whether we are able to see ldap user's entry or not-

```
[root@ldap-server migrationtools]#
[root@ldap-server migrationtools]# ldapsearch -x cn=ldapuser01 -b dc=cricbuzz,dc=com
```

We will see success message at last.

26. We will allow ldap service from firewall (It works on tcp port 389)-

```
[root@ldap-server migrationtools]# firewall-cmd --permanent --add-service=ldap
success
[root@ldap-server migrationtools]# firewall-cmd --reload
success
[root@ldap-server migrationtools]#
```

27. Define which file we will use for for ldap logs-

```
[root@ldap-server migrationtools]# vim /etc/rsyslog.conf

# File to store the position in the journal
$IMJournalStateFile imjournal.state


#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog


# Log cron stuff
cron.*                                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log

local4.* /var/log/ldap.log
```

28. Restart syslog service-

```
[root@ldap-server migrationtools]# systemctl restart rsyslog.service
[root@ldap-server migrationtools]#
```

29. Next, we will setup nfs in order to mount ldap user's home directory on client. Install packages for it-

```
[root@ldap-server migrationtools]#
[root@ldap-server migrationtools]# yum install -y nfs* rpcbind mountd
```

30. Now we will export home directory-

```
[root@ldap-server migrationtools]#
[root@ldap-server migrationtools]# vim /etc/exports
/home *(rw,sync)
```

31. We will start & enable nfs, rpcbind services-

```
[root@ldap-server migrationtools]# systemctl start rpcbind
[root@ldap-server migrationtools]# systemctl start nfs
[root@ldap-server migrationtools]# systemctl enable rpcbind
[root@ldap-server migrationtools]# systemctl enable nfs
Created symlink from /etc/systemd/system/multi-user.target.wants/nfs-server.service to /usr/lib/systemd/system/nfs-server.service.
[root@ldap-server migrationtools]#
```

32. To check whether nfs configuration is done properly or not-

```
[root@ldap-server migrationtools]# showmount -e
Export list for ldap-server.cricbuzz.com:
/home *
[root@ldap-server migrationtools]#
```

33. Next, we will add nfs, rpcbind & mountd services in firewall-

```
[root@ldap-server ~]# firewall-cmd --add-service={nfs3,mountd,rpc-bind} --permanent
success
[root@ldap-server ~]#
[root@ldap-server ~]# firewall-cmd --reload
success
[root@ldap-server ~]#
```

34. We will restart slapd service & get ldap user detail-

```
[root@ldap-server ~]# systemctl restart slapd.service
[root@ldap-server ~]# getent passwd ldapuser01
ldapuser01:x:1001:1001::/home/guests/ldapuser01:/bin/bash
[root@ldap-server ~]#
```

LDAP server configuration are done now. Next, we will configure LDAP client.

Client Configuration: -

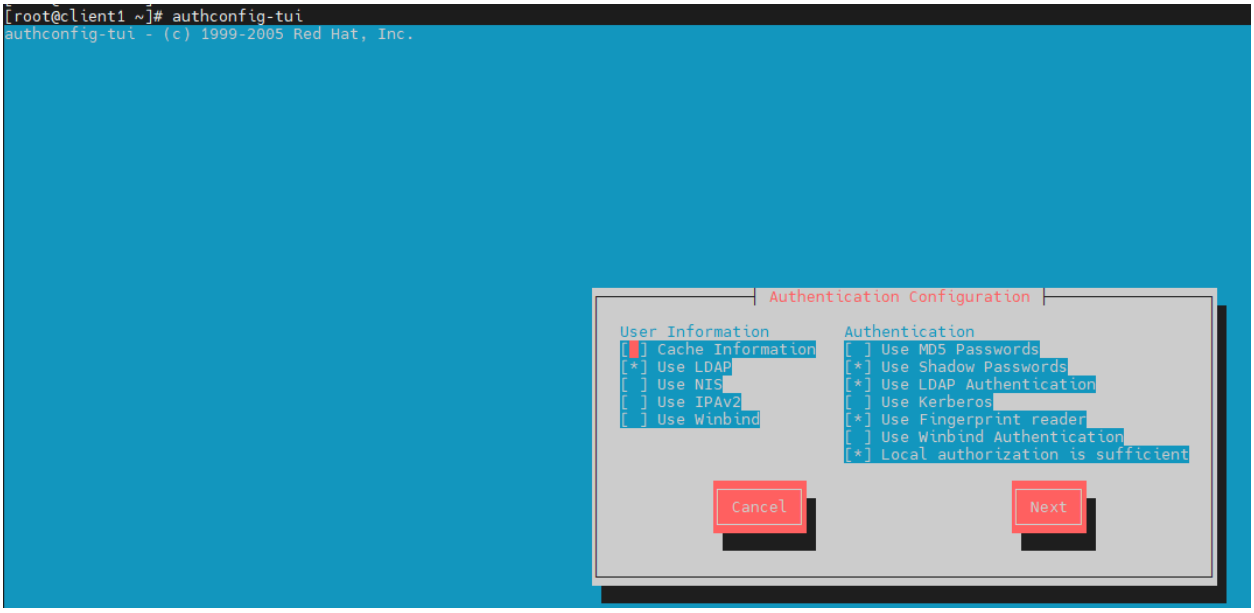
1. At server, hostname & IP in /etc/hosts file as we don't have DNS configured-

```
[root@client1 ~]# vim /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.78.151 ldap-server.cricbuzz.com
192.168.78.152 client1.cricbuzz.com
```

2. We will install few packages as shown-

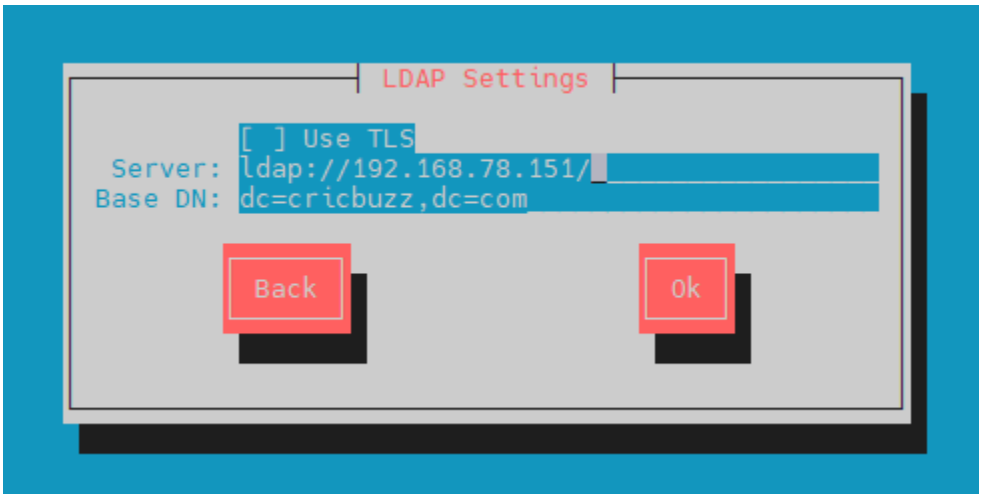
```
[root@client1 ~]#
[root@client1 ~]# yum install -y openldap-clients nss-pam-ldapd autofs
```

3. Configure LDAP client using authconfig-tui-



Make sure to select (i) Use LDAP (ii) Use LDAP Authentication.

4. Next, uncheck “Use TLS” option & specify LDAP server IP or hostname-



5. Get LDAP user detail-

```
[root@client1 ~]# getent passwd ldapuser01
ldapuser01:*:1001:1001:ldapuser01:/home/guests/ldapuser01:/bin/bash
[root@client1 ~]#
[root@client1 ~]# getent passwd ldapuser02
ldapuser02:*:1002:1002:ldapuser02:/home/guests/ldapuser02:/bin/bash
[root@client1 ~]#
```

This user is not available this on client. It is available on server.

6. Now we will auto mount these LDAP user's home directory using autofs. We will create one file for this-

```
[root@client1 ~]#
[root@client1 ~]# vim /etc/auto.master.d/home.autofs
/home/guests /etc/auto.home
```

Here, /home/guests is exported path from server & auto.home we will create in next step.

7. Create auto.home file & define which directories are there in /home/guests, permissions on them & from where they are exported-

```
[root@client1 ~]#
[root@client1 ~]# vim /etc/auto.home
ldapuser01 -rw,sync 192.168.78.151:/home/guests/&
ldapuser02 -rw,sync 192.168.78.151:/home/guests/&
~
```

8. We will restart autofs service. These mounts will not reflect if we check using df -h -

```
[root@client1 ~]# systemctl restart autofs.service
[root@client1 ~]# df -h
Filesystem             Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root   36G  7.9G   28G  22% /
devtmpfs               3.8G     0  3.8G   0% /dev
tmpfs                  3.9G     0  3.9G   0% /dev/shm
tmpfs                  3.9G   13M  3.8G   1% /run
tmpfs                  3.9G     0  3.9G   0% /sys/fs/cgroup
/dev/sda1             1014M  178M  837M  18% /boot
tmpfs                  781M  4.0K  781M   1% /run/user/42
tmpfs                  781M   24K  781M   1% /run/user/0
/dev/sr0               4.2G  4.2G     0 100% /run/media/root/RHEL-7.6 Server.x86_64
[root@client1 ~]#
```

9. Next, we will try to login using ldap users-

```
[root@client1 ~]#
[root@client1 ~]# su - ldapuser01
Last login: Sun Nov 27 11:07:17 EST 2022 on pts/0
[ldapuser01@client1 ~]$
[ldapuser01@client1 ~]$ logout
[root@client1 ~]#
[root@client1 ~]# su - ldapuser02
Last login: Sun Nov 27 10:56:27 EST 2022 on pts/1
[ldapuser02@client1 ~]$
[ldapuser02@client1 ~]$
[ldapuser02@client1 ~]$ whoami
ldapuser02
[ldapuser02@client1 ~]$
[ldapuser02@client1 ~]$ exit
logout
[root@client1 ~]#
```

Note: As soon as we login with LDAP user, their home directory gets created on server.

This is all about LDAP server & client configuration.