LDAP

**LDAP server side configuration :**

**1st we to install LDAP packages openldap & migrationtools**

# yum install openldap\*

# yum install migrationtools

**Then we will create ldap root passwd**

# slappasswd

New password: temp  
Re-enter new password: temp

**passwd generated in encrypted format**

{SSHA}bHSiwuPJEypHS6zHSE2Uy7M69sQjmkPL

**Edit the Openldap server configuration**

**configuration file are located in /etc/openldap/slapd.d/**

# cd /etc/openldap/slapd.d/cn=config

# vi olcDatabase={2}hdb.ldif

change the variables of "olcSuffix" and "olcRootDN"

**change ur domain name**

#olcSuffix: dc=server,dc=com

#olcRootDN: cn=Manager,dc=server,dc=com

**Add the three more lines in the same configuring file of the end of line**

#olcRootPW: (your generated encrypt passwd copy here)  
#olcTLSCertificateFile: /etc/pki/tls/certs/server.pem  
#olcTLSCertificateKeyFile: /etc/pki/tls/certs/serverkey.pem

now save & exit

**Provide the monitor privileges**

# cd /etc/openldap/slapd.d/cn=config

# vi olcDatabase={1}monitor.ldif

edit the lines

olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth" read by dn.base="cn=Manager,dc=server,dc=com" read by \* none

**verify the configuration**

# slaptest -u

**show output**

56abba86 ldif\_read\_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif"  
56abba86 ldif\_read\_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif"  
config file testing succeeded

**Configure the LDAP database**

**copy the simple database configuration file, change the file permissions**

# cd /etc/openldap/slapd.d/cn=config

# cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

# chown -R ldap:ldap /var/lib/ldap/

**Add the following LDAP Schemas**

# cd /etc/openldap/slapd.d/cn=config

# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

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

# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

**Create the self-signed certificate**

# openssl req -new -x509 -nodes -out /etc/pki/tls/certs/server.pem -keyout /etc/pki/tls/certs/serverkey.pem -days 365

Country Name (2 letter code) [XX]:IN  
State or Province Name (full name) []:Maharashtra  
Locality Name (eg, city) [Default City]:Nagpur  
Organization Name (eg, company) [Default Company Ltd]:server  
Organizational Unit Name (eg, section) []:DCOPS  
Common Name (eg, your name or your server's hostname) []:linux.server.com  
Email Address []:root@linux.server.com

**Create base objects in Openldap**

**change the migrate\_common.ph**

# cd /usr/share/migrationtools/

# vi migrate\_common.ph

change the line no 71,74 and 91

71 - $DEFAULT\_MAIL\_DOMAIN = "server.com";

74 - $DEFAULT\_BASE = "dc=server,dc=com";

91 -$EXTENDED\_SCHEMA = 1;

now save & exit

**Generate a base.ldif file for your domain**

**create a touch file**

# touch /root/base.ldif

**copy the below line and paste inside the file /root/base/ldif**

dn: dc=server,dc=com  
objectClass: top  
objectClass: dcObject  
objectclass: organization  
o: server com  
dc: server  
  
dn: cn=Manager,dc=server,dc=com  
objectClass: organizationalRole  
cn: Manager  
description: Directory Manager  
  
dn: ou=People,dc=server,dc=com  
objectClass: organizationalUnit  
ou: People  
  
dn: ou=Group,dc=server,dc=com  
objectClass: organizationalUnit  
ou: Group

**Create a User**

# cd/usr/share/migrationtools

# useradd ldapuser1

# passwd ldapuser1

# useradd ldapuser2

# passwd ldapuser2

**Filter out these user from /etc/passwd to another file**

# cd/usr/share/migrationtools

# grep ":10[0-9][0-9]" /etc/passwd > /root/passwd

**Filter out these user from /etc/group to another file**

# grep ":10[0-9][0-9]" /etc/group > /root/group

**Now convert the individual User file to Ldap Data Interchange Format (LDIF)**

**Generate a ldif file for users**

# cd/usr/share/migrationtools

# ./migrate\_passwd.pl /root/passwd /root/users.ldif

**Generate a ldif file for groups**

# ./migrate\_group.pl /root/group /root/groups.ldif

**Import Users in to the LDAP database**

**enter your encrypted passwd**

# ldapadd -x -W -D "cn=Manager,dc=server,dc=com" -f /root/base.ldif

# ldapadd -x -W -D "cn=Manager,dc=server,dc=com" -f /root/users.ldif

# ldapadd -x -W -D "cn=Manager,dc=server,dc=com" -f /root/groups.ldif

**Test the configuration**

# ldapsearch -x cn=ldapuser1 -b dc=server,dc=com

# ldapsearch -x cn=ldapuser2 -b dc=server,dc=com

It prints all the user information:

# ldapsearch -x -b 'dc=server,dc=com' '(objectclass=\*)'

**Stop Firewalld**

# systemctl stop firewalld

**NFS configuration to export the home Directory**

# vi /etc/exports

/home \*(rw,sync)

save & exit

**NFS installation**

# yum -y install rpcbind nfs-utils

**Enables and restart rpcbind and nfs service**

# systemctl start rpcbind

# systemctl start nfs

# systemctl enable rpcbind

# systemctl enable nfs

Test the NFS configuration

# showmount -e 192.168.72.95

to show the export directory

------------------------------------------------------------------------------------------------------------------------------------------

**LDAP client side**

# yum install -y openldap-clients nss-pam-ldapd

# authconfig-tui

1. put '\*' Mark on "Use LDAP"

2. put '\*' Mark on "Use LDAP Authentication''

3.Select "Next" and Enter.

4.Enter the server field as "ldap://linux.server.com/"

5.Enter the base DN Filed as "dc=server,dc=com"

6.Select "ok" and enter

**Ldap configurations are working properly or not to check following cmd**

# getent passwd ldapuser1

output - ldapuser1:x:1000:1000:ldapuser1:/home/ldapuser1:/bin/bash

**Mount the LDAP Users Home Directory.**

add in /etc/fstab

# vi /etc/fstab

/home   /home   auto  defaults 0 0

Then you login the Ldap users

------------------------------------------------------------------------------------------------------------------------------------------

<https://www.itzgeek.com/how-tos/linux/centos-how-tos/step-step-openldap-server-configuration-centos-7-rhel-7.html/2>

<https://www.learnitguide.net/2016/01/configure-openldap-server-on-rhel7.html>

OpenLDAP - Installation and adding objects using phpldapadmin and ldapadd