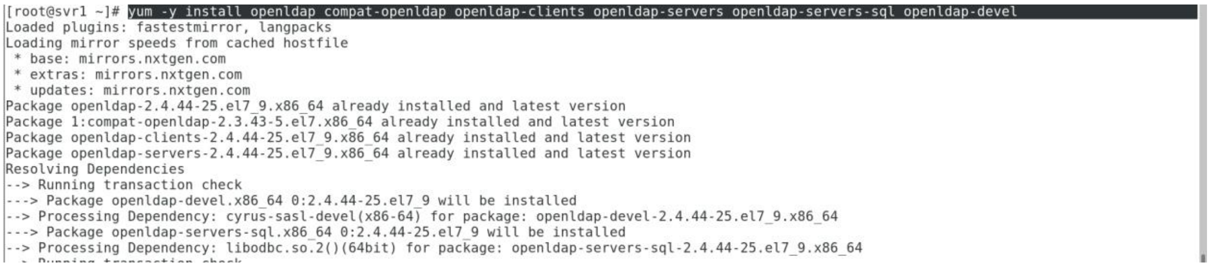
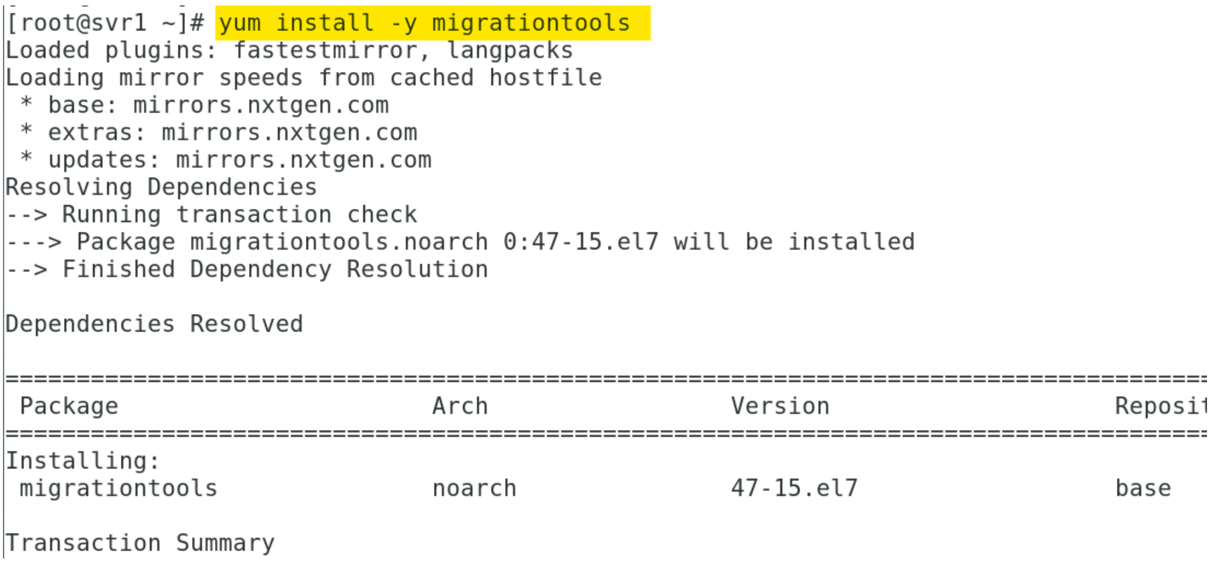
Install the required LDAP Packages "Openldap"

yum -y install openldap* migrationtools



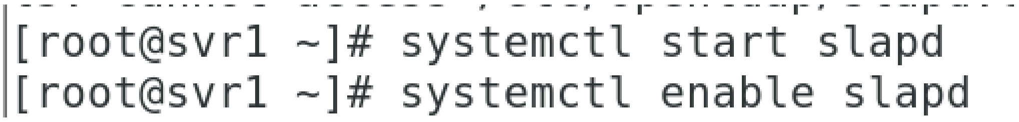
```
[root@svr1 ~]# yum -y install openldap compat-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.nxtgen.com
 * extras: mirrors.nxtgen.com
 * updates: mirrors.nxtgen.com
Package openldap-2.4.44-25.el7_9.x86_64 already installed and latest version
Package 1:compat-openldap-2.3.43-5.el7.x86_64 already installed and latest version
Package openldap-clients-2.4.44-25.el7_9.x86_64 already installed and latest version
Package openldap-servers-2.4.44-25.el7_9.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
---> Package openldap-devel.x86_64 0:2.4.44-25.el7_9 will be installed
--> Processing Dependency: cyrus-sasl-devel(x86-64) for package: openldap-devel-2.4.44-25.el7_9.x86_64
---> Package openldap-servers-sql.x86_64 0:2.4.44-25.el7_9 will be installed
--> Processing Dependency: libodbc.so.2()(64bit) for package: openldap-servers-sql-2.4.44-25.el7_9.x86_64
--> Running transaction check
```

yum install -y migrationtools



```
[root@svr1 ~]# yum install -y migrationtools
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.nxtgen.com
 * extras: mirrors.nxtgen.com
 * updates: mirrors.nxtgen.com
Resolving Dependencies
--> Running transaction check
---> Package migrationtools.noarch 0:47-15.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====================================================================================
 Package                      Arch                 Version                    Reposit
=====================================================================================
Installing:
 migrationtools               noarch               47-15.el7                  base

Transaction Summary
```

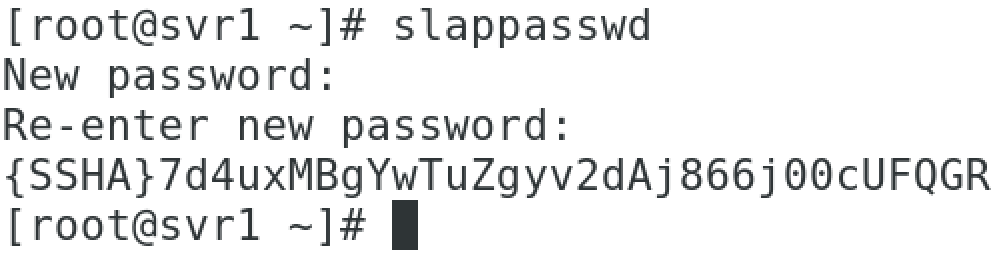
Start & enable ldap service:



```
[root@svr1 ~]# systemctl start slapd
[root@svr1 ~]# systemctl enable slapd
```

Create a LDAP root passwd for administration purpose

# slappasswd (& copy this password)

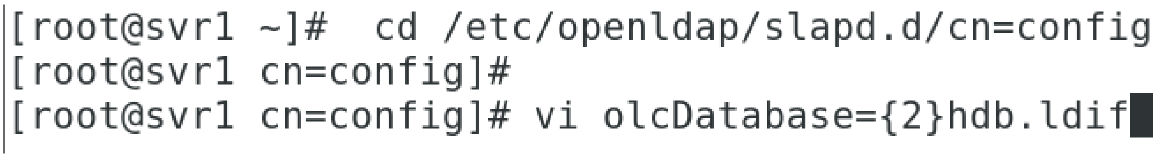


```
[root@svr1 ~]# slappasswd
New password:
Re-enter new password:
{SSHA}7d4uxMBgYwTuZgyv2dAj866j00cUFQGR
[root@svr1 ~]# █
```

Edit OpenLDAP Server Configuration

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

ls

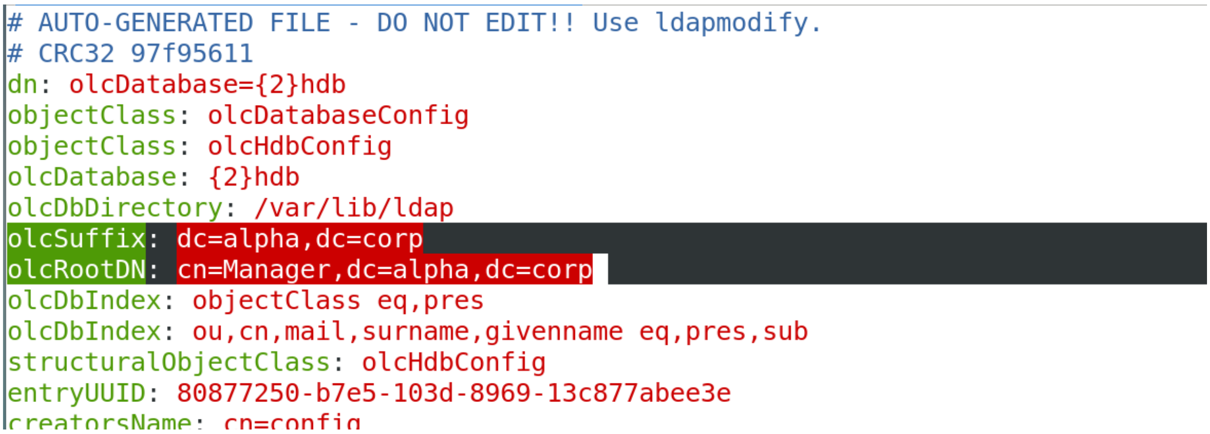


```
[root@svr1 ~]#  cd /etc/openldap/slapd.d/cn=config
[root@svr1 cn=config]#
[root@svr1 cn=config]# vi olcDatabase={2}hdb.ldif
```

Edit below lines:

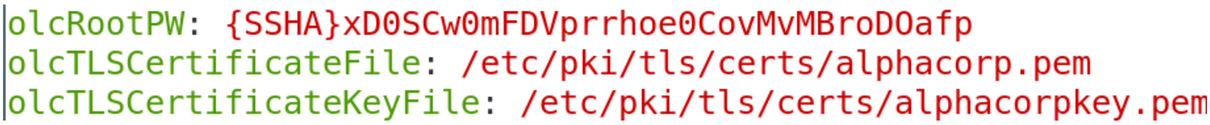
olcSuffix: dc=alpha,dc=corp

olcRootDN: cn=Manager, dc=alpha,dc=corp



```
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 97f95611
dn: olcDatabase={2}hdb
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=alpha,dc=corp
olcRootDN: cn=Manager,dc=alpha,dc=corp
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub
structuralObjectClass: olcHdbConfig
entryUUID: 80877250-b7e5-103d-8969-13c877abee3e
creatorsName: cn=config
```

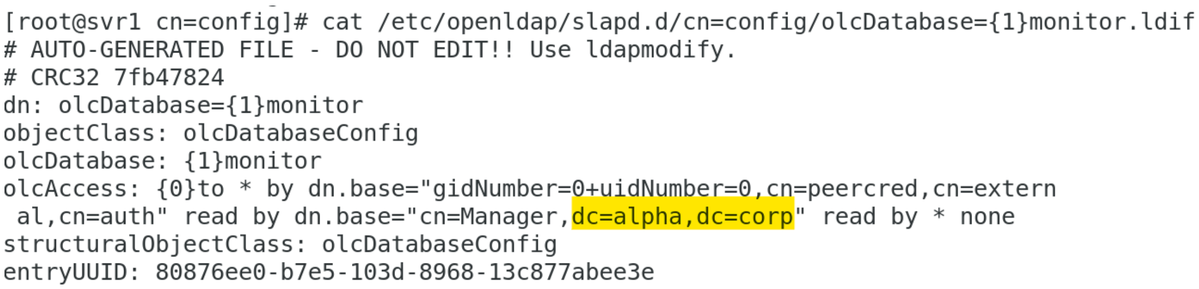
Add these lines to the bottom lines to the same config file:



```
olcRootPW: {SSHA}xD0SCw0mFDVprrhoe0CovMvMBroDOafp
olcTLSCertificateFile: /etc/pki/tls/certs/alphacorp.pem
olcTLSCertificateKeyFile: /etc/pki/tls/certs/alphacorpkey.pem
```

:wq!

Provide the Monitor privileges

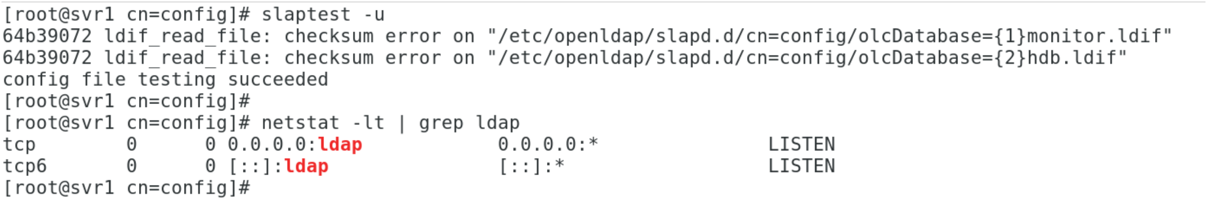


```
[root@svr1 cn=config]# cat /etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 7fb47824
dn: olcDatabase={1}monitor
objectClass: olcDatabaseConfig
olcDatabase: {1}monitor
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=extern
 al,cn=auth" read by dn.base="cn=Manager,dc=alpha,dc=corp" read by * none
structuralObjectClass: olcDatabaseConfig
entryUUID: 80876ee0-b7e5-103d-8968-13c877abee3e
```

:wq!

Verify the configuration:

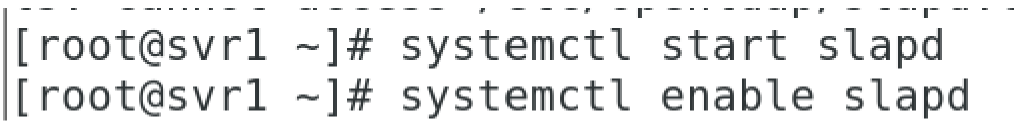
# slaptest -u



```
[root@svr1 cn=config]# slaptest -u
64b39072 ldif_read_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif"
64b39072 ldif_read_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif"
config file testing succeeded
[root@svr1 cn=config]#
[root@svr1 cn=config]# netstat -lt | grep ldap
tcp        0      0 0.0.0.0:ldap            0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ldap               [::]:*                  LISTEN
[root@svr1 cn=config]#
```

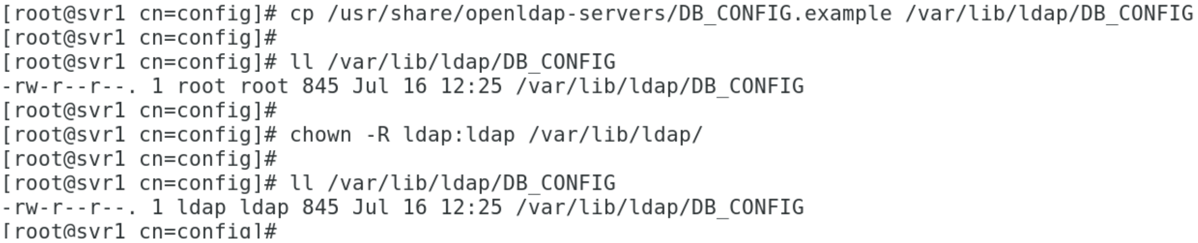
Note: ignore the checksum error as of now.

Enable and Start SLAPD service:



```
[root@svr1 ~]# systemctl start slapd
[root@svr1 ~]# systemctl enable slapd
```

Configure the LDAP Database



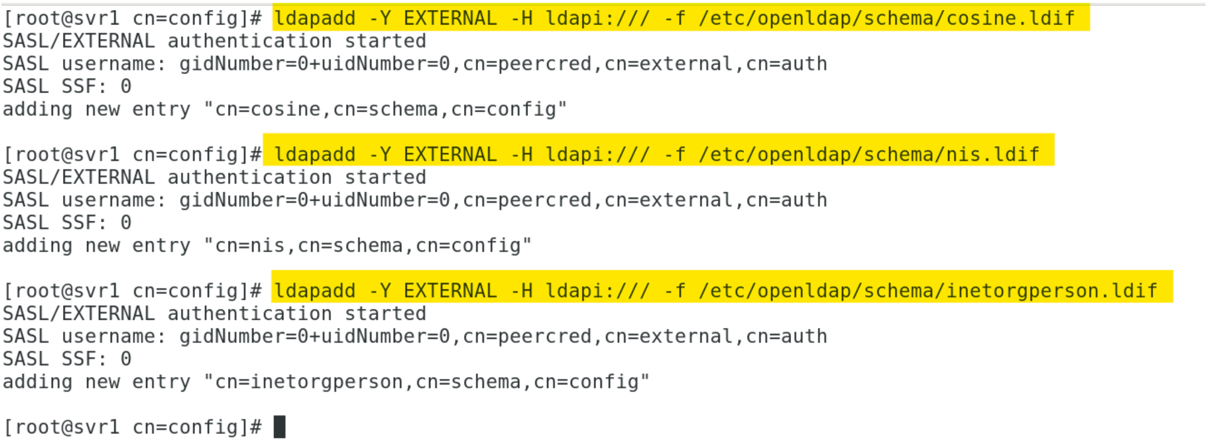
```
[root@svr1 cn=config]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
[root@svr1 cn=config]#
[root@svr1 cn=config]# ll /var/lib/ldap/DB_CONFIG
-rw-r--r--. 1 root root 845 Jul 16 12:25 /var/lib/ldap/DB_CONFIG
[root@svr1 cn=config]#
[root@svr1 cn=config]# chown -R ldap:ldap /var/lib/ldap/
[root@svr1 cn=config]#
[root@svr1 cn=config]# ll /var/lib/ldap/DB_CONFIG
-rw-r--r--. 1 ldap ldap 845 Jul 16 12:25 /var/lib/ldap/DB_CONFIG
[root@svr1 cn=config]#
```

Add the following LDAP Schemas

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

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

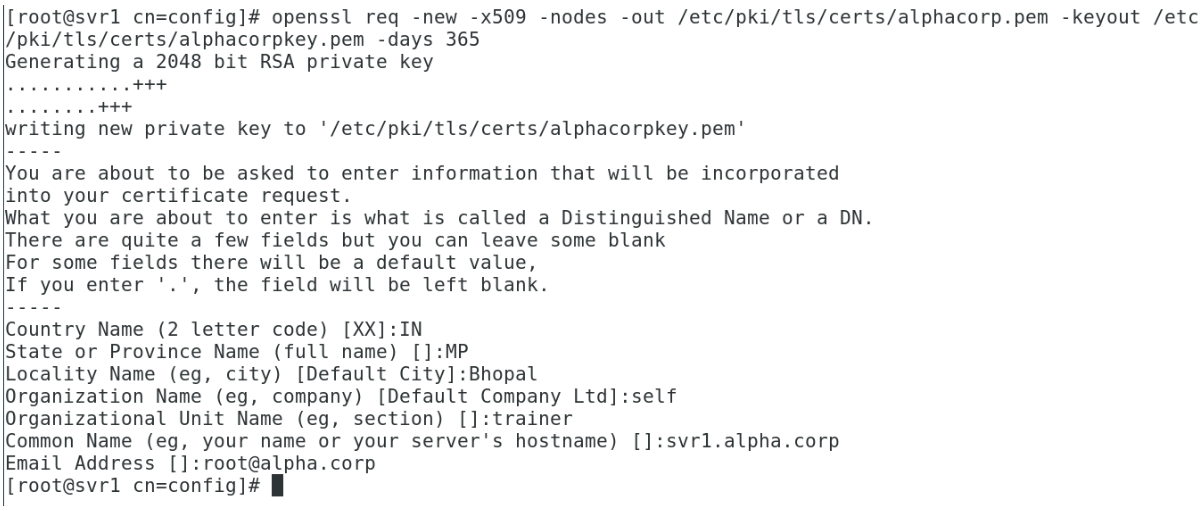
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif



```
[root@svr1 cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/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@svr1 cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/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"

[root@svr1 cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"

[root@svr1 cn=config]# █
```

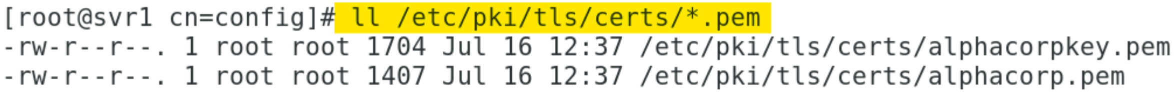
Create the self-signed certificate

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



```
[root@svr1 cn=config]# openssl req -new -x509 -nodes -out /etc/pki/tls/certs/alphacorp.pem -keyout /etc
/pki/tls/certs/alphacorpkey.pem -days 365
Generating a 2048 bit RSA private key
...........+++
........+++
writing new private key to '/etc/pki/tls/certs/alphacorpkey.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) []:MP
Locality Name (eg, city) [Default City]:Bhopal
Organization Name (eg, company) [Default Company Ltd]:self
Organizational Unit Name (eg, section) []:trainer
Common Name (eg, your name or your server's hostname) []:svr1.alpha.corp
Email Address []:root@alpha.corp
[root@svr1 cn=config]# 
```

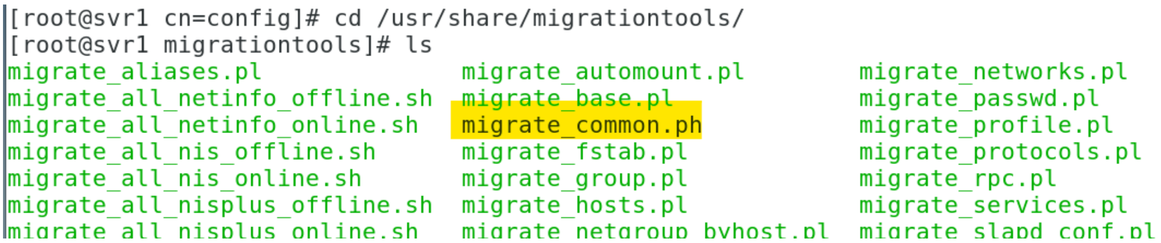
ll /etc/pki/tls/certs/*.pem



```
[root@svr1 cn=config]# ll /etc/pki/tls/certs/*.pem
-rw-r--r--. 1 root root 1704 Jul 16 12:37 /etc/pki/tls/certs/alphacorpkey.pem
-rw-r--r--. 1 root root 1407 Jul 16 12:37 /etc/pki/tls/certs/alphacorp.pem
```

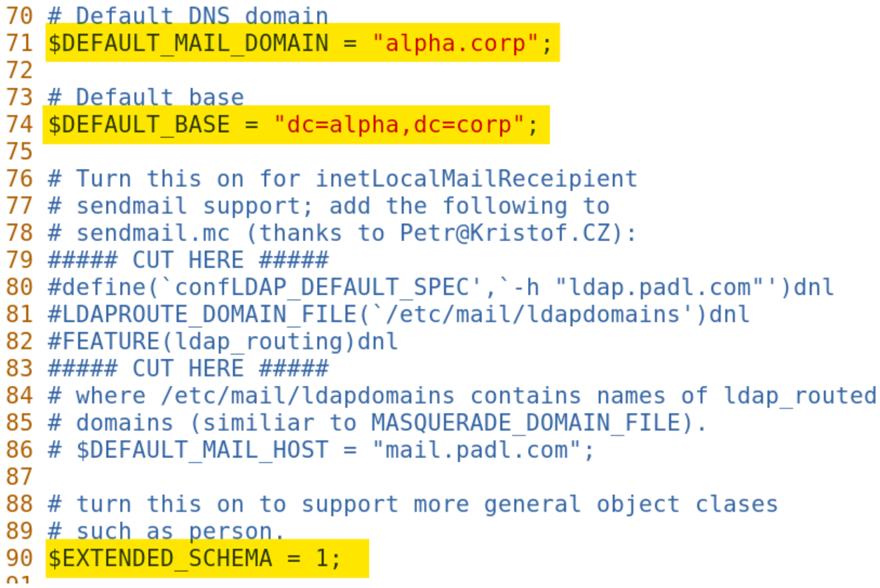
Create base objects in OpenLDAP:

cd /usr/share/migrationtools/



```
[root@svr1 cn=config]# cd /usr/share/migrationtools/
[root@svr1 migrationtools]# ls
migrate_aliases.pl                migrate_automount.pl          migrate_networks.pl
migrate_all_netinfo_offline.sh    migrate_base.pl               migrate_passwd.pl
migrate_all_netinfo_online.sh     migrate_common.ph             migrate_profile.pl
migrate_all_nis_offline.sh        migrate_fstab.pl              migrate_protocols.pl
migrate_all_nis_online.sh         migrate_group.pl              migrate_rpc.pl
migrate_all_nisplus_offline.sh    migrate_hosts.pl              migrate_services.pl
migrate_all_nisplus_online.sh     migrate_netgroup_byhost.pl    migrate_slapd_conf.pl
```

Edit **"migrate_common.ph" file**:

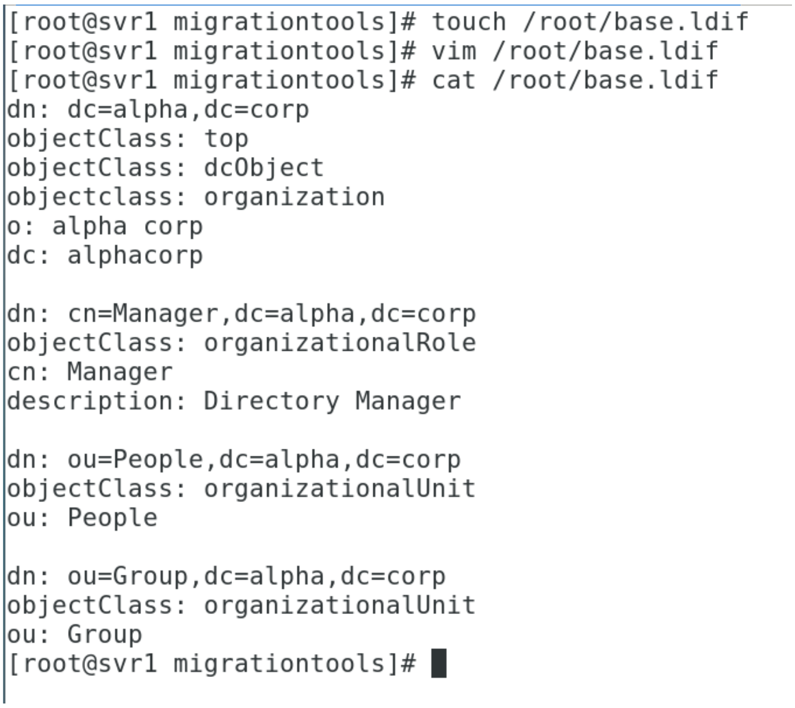


```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "alpha.corp";

# Default base
$DEFAULT_BASE = "dc=alpha,dc=corp";

# Turn this on for inetLocalMailReceipient
# sendmail support; add the following to
# sendmail.mc (thanks to Petr@Kristof.CZ):
##### CUT HERE #####
#define(`confLDAP_DEFAULT_SPEC',`-h "ldap.padl.com"')dnl
#LDAPROUTE_DOMAIN_FILE(`/etc/mail/ldapdomains')dnl
#FEATURE(ldap_routing)dnl
##### CUT HERE #####
# where /etc/mail/ldapdomains contains names of ldap_routed
# domains (similiar to MASQUERADE_DOMAIN_FILE).
# $DEFAULT_MAIL_HOST = "mail.padl.com";

# turn this on to support more general object clases
# such as person.
$EXTENDED_SCHEMA = 1;
```

:wq!

Generate a base.ldif file for your Domain:

# touch /root/base.ldif



```
[root@svr1 migrationtools]# touch /root/base.ldif
[root@svr1 migrationtools]# vim /root/base.ldif
[root@svr1 migrationtools]# cat /root/base.ldif
dn: dc=alpha,dc=corp
objectClass: top
objectClass: dcObject
objectclass: organization
o: alpha corp
dc: alphacorp

dn: cn=Manager,dc=alpha,dc=corp
objectClass: organizationalRole
cn: Manager
description: Directory Manager

dn: ou=People,dc=alpha,dc=corp
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=alpha,dc=corp
objectClass: organizationalUnit
ou: Group
[root@svr1 migrationtools]# 
```

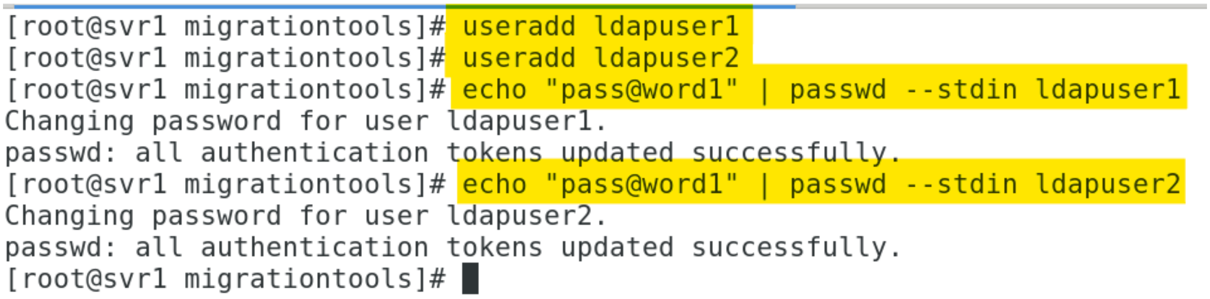
Create Local Users:

useradd ldapuser1

useradd ldapuser2

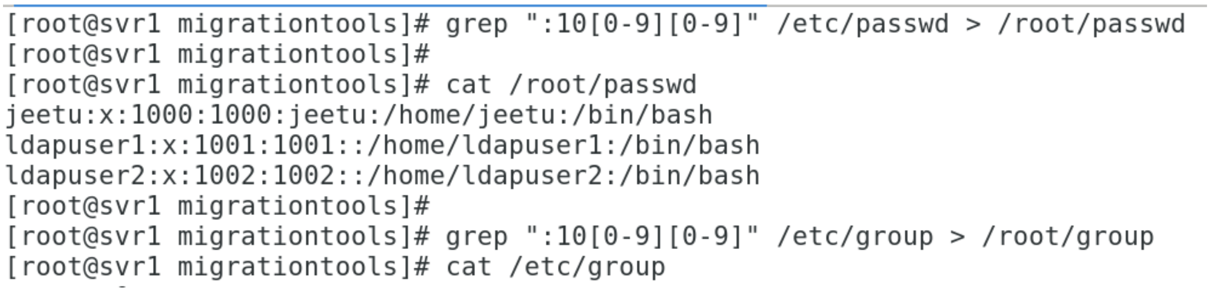
echo "pass@word1" | passwd --stdin ldapuser1

echo "pass@word1" | passwd --stdin ldapuser2



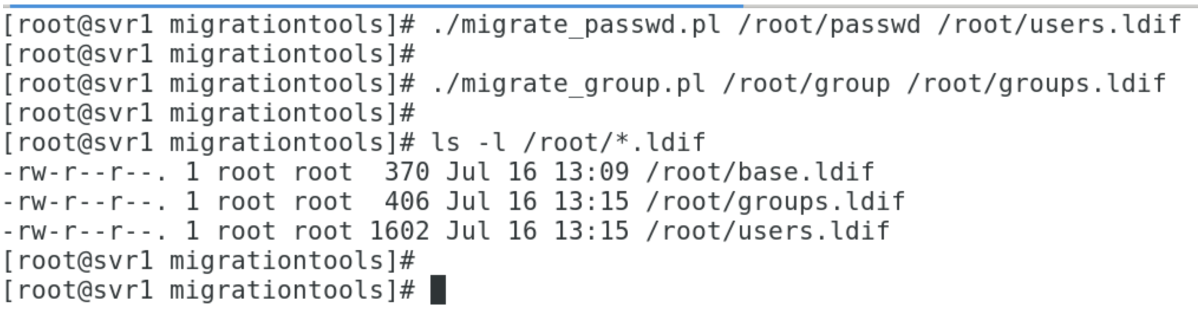
```
[root@svr1 migrationtools]# useradd ldapuser1
[root@svr1 migrationtools]# useradd ldapuser2
[root@svr1 migrationtools]# echo "pass@word1" | passwd --stdin ldapuser1
Changing password for user ldapuser1.
passwd: all authentication tokens updated successfully.
[root@svr1 migrationtools]# echo "pass@word1" | passwd --stdin ldapuser2
Changing password for user ldapuser2.
passwd: all authentication tokens updated successfully.
[root@svr1 migrationtools]# 
```

Filter out these user from /etc/passwd & /etc/group to another file:



```
[root@svr1 migrationtools]# grep ":10[0-9][0-9]" /etc/passwd > /root/passwd
[root@svr1 migrationtools]#
[root@svr1 migrationtools]# cat /root/passwd
jeetu:x:1000:1000:jeetu:/home/jeetu:/bin/bash
ldapuser1:x:1001:1001::/home/ldapuser1:/bin/bash
ldapuser2:x:1002:1002::/home/ldapuser2:/bin/bash
[root@svr1 migrationtools]#
[root@svr1 migrationtools]# grep ":10[0-9][0-9]" /etc/group > /root/group
[root@svr1 migrationtools]# cat /etc/group
```

Now Convert the Individual Users file to LDAP Data Interchange Format (LDIF)



```
[root@svr1 migrationtools]# ./migrate_passwd.pl /root/passwd /root/users.ldif
[root@svr1 migrationtools]#
[root@svr1 migrationtools]# ./migrate_group.pl /root/group /root/groups.ldif
[root@svr1 migrationtools]#
[root@svr1 migrationtools]# ls -l /root/*.ldif
-rw-r--r--. 1 root root  370 Jul 16 13:09 /root/base.ldif
-rw-r--r--. 1 root root  406 Jul 16 13:15 /root/groups.ldif
-rw-r--r--. 1 root root 1602 Jul 16 13:15 /root/users.ldif
[root@svr1 migrationtools]#
[root@svr1 migrationtools]#
```

Import Users in to the LDAP Database.

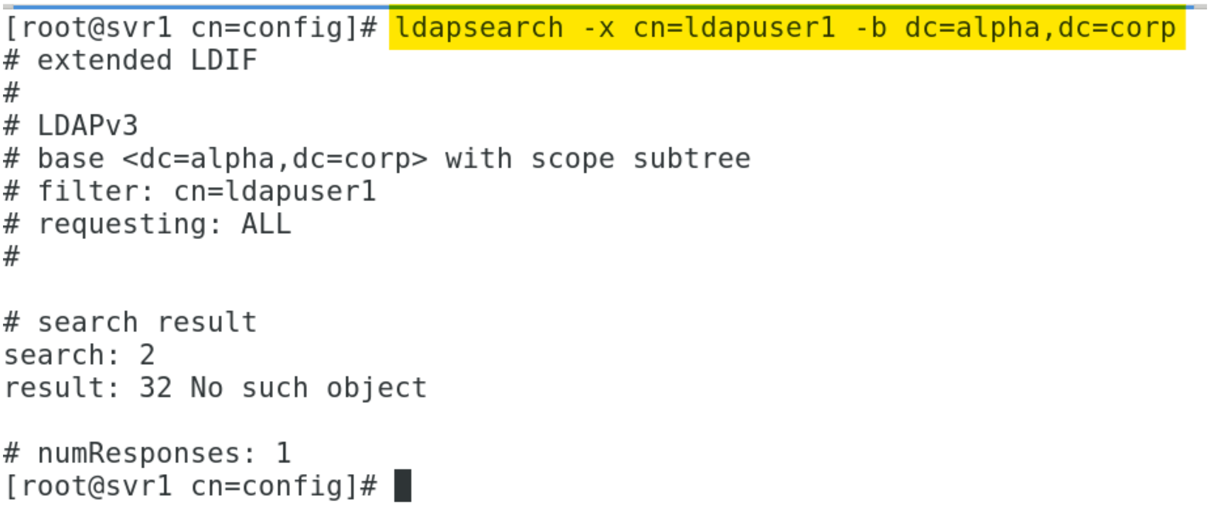
ldapadd -x -W -D "cn=Manager,dc=alpha,dc=corp" -f /root/base.ldif

ldapadd -x -W -D "cn=Manager,dc=alpha,dc=corp" -f /root/users.ldif

ldapadd -x -W -D "cn=Manager,dc=alpha,dc=corp" -f /root/groups.ldif

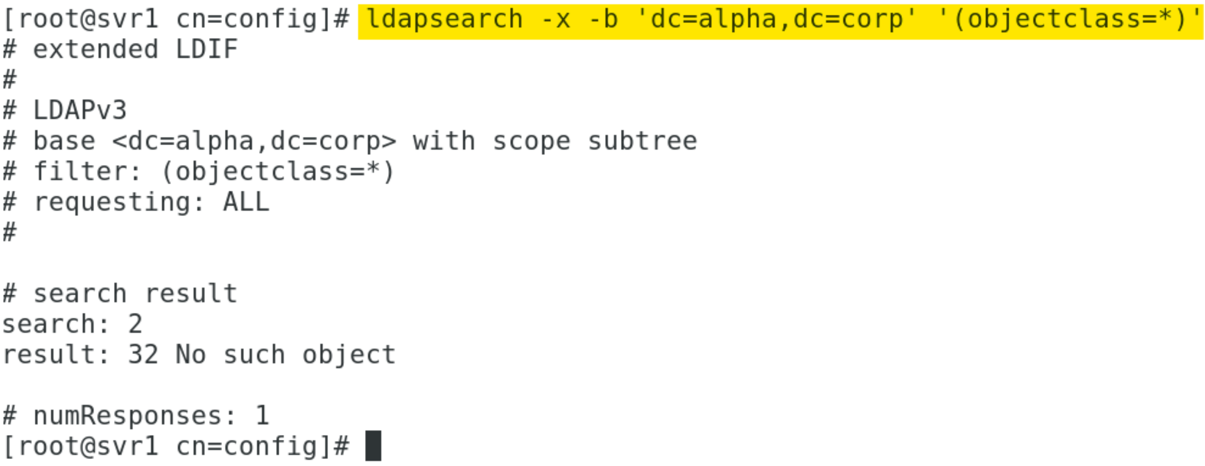
Test the configuration.

ldapsearch -x cn=ldapuser1 -b dc=alpha,dc=corp



```
[root@svr1 cn=config]# ldapsearch -x cn=ldapuser1 -b dc=alpha,dc=corp
# extended LDIF
#
# LDAPv3
# base <dc=alpha,dc=corp> with scope subtree
# filter: cn=ldapuser1
# requesting: ALL
#

# search result
search: 2
result: 32 No such object

# numResponses: 1
[root@svr1 cn=config]#
```

ldapsearch -x -b 'dc=alpha,dc=corp' '(objectclass=*)'



```
[root@svr1 cn=config]# ldapsearch -x -b 'dc=alpha,dc=corp' '(objectclass=*)'
# extended LDIF
#
# LDAPv3
# base <dc=alpha,dc=corp> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 32 No such object

# numResponses: 1
[root@svr1 cn=config]#
```