-: OPEN LDAP Configuration :-

ldap.sk.com client.sk.com

#vi /etc/hostname

ldap.zoom.com

:wq

#vi /etc/hosts

192.168.0.80 ldap.zoom.com ldap

:wq ( save & quit )

**Steps To Configure:-**

1. Install the required ldap packages
2. Create a ldap admin passwd
3. Edit the openldap configuration file
4. Provide teh Monitor Privileges
5. Enable and Start slapd service
6. Configure the ldap Database
7. Create the self-signed certicate
8. Create base objects in openldap
9. Generate a base.ldif file for your domain
10. Create local users
11. Import users into the ldap Database
12. Test the configuration

1) Install required LDAP Packages

# yum install openldap\* ldap\* migration\* nss\* -y

2) Create LDAP root password

# slappasswd

New password:123

Re-enter new password:

{SSHA}OJApYJpEEwEeTJlPwfzAB9beMxzcKvDJ ( save this encrypted password )

3) Edit the LDAP configuration file

# cd /etc/openldap/slapd.d/

# ll

drwxr-x---. 3 ldap ldap 4096 Nov 30 14:18 cn=config

-rw-------. 1 ldap ldap 589 Nov 30 14:18 cn=config.ldif

# cd cn=config

# ll

drwxr-x---. 2 ldap ldap 28 Nov 30 14:18 cn=schema

-rw-------. 1 ldap ldap 378 Nov 30 14:18 cn=schema.ldif

-rw-------. 1 ldap ldap 513 Nov 30 14:18 olcDatabase={0}config.ldif

-rw-------. 1 ldap ldap 443 Nov 30 14:18 olcDatabase={-1}frontend.ldif

-rw-------. 1 ldap ldap 562 Nov 30 14:18 olcDatabase={1}monitor.ldif

-rw-------. 1 ldap ldap 609 Nov 30 14:18 olcDatabase={2}hdb.ldif

# vi olcDatabase\=\{2\}hdb.ldif

1 # AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.

2 # CRC32 0b54fdab

3 dn: olcDatabase={2}hdb

4 objectClass: olcDatabaseConfig

5 objectClass: olcHdbConfig

6 olcDatabase: {2}hdb

7 olcDbDirectory: /var/lib/ldap

8 olcSuffix: dc=sk,dc=com

9 olcRootDN: cn=Manager,dc=sk,dc=com

10 olcDbIndex: objectClass eq,pres

11 olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub

12 structuralObjectClass: olcHdbConfig

13 entryUUID: 6f0af94e-88c8-1038-9af6-8ff82b078f63

14 creatorsName: cn=config

15 createTimestamp: 20181130084820Z

16 entryCSN: 20181130084820.862358Z#000000#000#000000

17 modifiersName: cn=config

18 modifyTimestamp: 20181130084820Z

19 olcRootPW: {SSHA}OJApYJpEEwEeTJlPwfzAB9beMxzcKvDJ

20 olcTLSCertificateFile: /etc/pki/tls/certs/skldap.pem

21 olcTLSCertificateKeyFile: /etc/pki/tls/certs/skldapkey.pem

4) Provide the monitoring previliges

# vi olcDatabase\=\{1\}monitor.ldif

1 # AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.

2 # CRC32 943a8fce

3 dn: olcDatabase={1}monitor

4 objectClass: olcDatabaseConfig

5 olcDatabase: {1}monitor

6 olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=extern

al,cn=auth" read by dn.base="cn=Manager,dc=sk,dc=com" read by \* none

7 structuralObjectClass: olcDatabaseConfig

8 entryUUID: 2b38d534-8976-1038-8f28-eb4532db35b8

9 creatorsName: cn=config

10 createTimestamp: 20181201053159Z

11 entryCSN: 20181201053159.508773Z#000000#000#000000

12 modifiersName: cn=config

13 modifyTimestamp: 20181201053159Z

4.1) verify the configuratiion

# slaptest -u

5c01026d ldif\_read\_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif"

5c01026d ldif\_read\_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif"

config file testing succeeded

5) start & enable the service

# systemctl start slapd

# systemctl enable slapd

Created symlink from /etc/systemd/system/multi-user.target.wants/slapd.service to /usr/lib/systemd/system/slapd.service.

6) configure the LDAP database

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

Add the fallowing 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

7) Create self-signed certificates

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

Generating a 2048 bit RSA private key

....+++

..............................................+++

writing new private key to '/etc/pki/tls/certs/skldapkey.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) []:TS

Locality Name (eg, city) [Default City]:HYD

Organization Name (eg, company) [Default Company Ltd]:sk

Organizational Unit Name (eg, section) []:DCOPS

Common Name (eg, your name or your server's hostname) []:ldap.sk.com

Email Address []:root@sk.com

7.1) Verify the created Certificates under the location /etc/pki/tls/certs/

# ll /etc/pki/tls/certs

-rw-r--r--. 1 root root 1704 Nov 30 15:16 /etc/pki/tls/certs/skldapkey.pem

-rw-r--r--. 1 root root 1367 Nov 30 15:16 /etc/pki/tls/certs/skldap.pem

8) Create base objects in openldap

# cd /usr/share/migrationtools

# ll

-rwxr-xr-x. 1 root root 2652 Dec 29 2013 migrate\_aliases.pl

-rwxr-xr-x. 1 root root 2950 Dec 29 2013 migrate\_all\_netinfo\_offline.sh

-rwxr-xr-x. 1 root root 2946 Dec 29 2013 migrate\_all\_netinfo\_online.sh

-rwxr-xr-x. 1 root root 3011 Dec 29 2013 migrate\_all\_nis\_offline.sh

-rwxr-xr-x. 1 root root 3006 Dec 29 2013 migrate\_all\_nis\_online.sh

-rwxr-xr-x. 1 root root 3164 Dec 29 2013 migrate\_all\_nisplus\_offline.sh

-rwxr-xr-x. 1 root root 3146 Dec 29 2013 migrate\_all\_nisplus\_online.sh

-rwxr-xr-x. 1 root root 5267 Dec 29 2013 migrate\_all\_offline.sh

-rwxr-xr-x. 1 root root 7468 Dec 29 2013 migrate\_all\_online.sh

-rwxr-xr-x. 1 root root 3278 Dec 29 2013 migrate\_automount.pl

-rwxr-xr-x. 1 root root 2608 Dec 29 2013 migrate\_base.pl

-rw-r--r--. 1 root root 8880 Dec 29 2013 migrate\_common.ph

-rwxr-xr-x. 1 root root 2952 Dec 29 2013 migrate\_fstab.pl

-rwxr-xr-x. 1 root root 2714 Dec 29 2013 migrate\_group.pl

-rwxr-xr-x. 1 root root 3087 Dec 29 2013 migrate\_hosts.pl

-rwxr-xr-x. 1 root root 2856 Dec 29 2013 migrate\_netgroup\_byhost.pl

-rwxr-xr-x. 1 root root 2856 Dec 29 2013 migrate\_netgroup\_byuser.pl

-rwxr-xr-x. 1 root root 3879 Dec 29 2013 migrate\_netgroup.pl

-rwxr-xr-x. 1 root root 2840 Dec 29 2013 migrate\_networks.pl

-rwxr-xr-x. 1 root root 5635 Dec 29 2013 migrate\_passwd.pl

-rwxr-xr-x. 1 root root 2428 Dec 29 2013 migrate\_profile.pl

-rwxr-xr-x. 1 root root 2873 Dec 29 2013 migrate\_protocols.pl

-rwxr-xr-x. 1 root root 2854 Dec 29 2013 migrate\_rpc.pl

-rwxr-xr-x. 1 root root 11465 Dec 29 2013 migrate\_services.pl

-rwxr-xr-x. 1 root root 3419 Dec 29 2013 migrate\_slapd\_conf.pl

# vi migrate\_common.ph

71 $DEFAULT\_MAIL\_DOMAIN = "sk.com";

74 $DEFAULT\_BASE = "dc=sk,dc=com";

90 $EXTENDED\_SCHEMA = 1;

9) create a base.ldif file for your domain

# vi /root/base.ldif

1 dn: dc=sk,dc=com

2 objectClass: top

3 objectClass: dcobject

4 objectClass: organization

5 o: sk com

6 dc: sk

7

8 dn: cn=Manager,dc=sk,dc=com

9 objectClass: organizationalRole

10 cn: Manager

11 description: Directory Manager

12

13 dn: ou=People,dc=sk,dc=com

14 objectClass: organizationalUnit

15 ou: People

16

17 dn: ou=Group,dc=sk,dc=com

18 objectClass: organizationalUnit

19 ou: Group

20

10) create a local users

# useradd user1

# passwd user1

123

123

# useradd user2

# passwd user2

123

123

10.1) Filter-out these user from /etc/passwd TO another file

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

10.2) Filter out the user-group's from etc/groups TO another file

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

10.3) Now convert the individual users file TO .ldif format

generate a ldif file for users

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

generate a ldif file for groups

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

11) Import users to ldap database

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

Enter LDAP Password: 123

adding new entry "dc=sk,dc=com"

adding new entry "cn=Manager,dc=sk,dc=com"

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

adding new entry "ou=Group,dc=sk,dc=com"

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

Enter LDAP Password: 123

adding new entry "uid=subbu,ou=People,dc=sk,dc=com"

adding new entry "uid=user1,ou=People,dc=sk,dc=com"

adding new entry "uid=user2,ou=People,dc=sk,dc=com"

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

Enter LDAP Password: 123

adding new entry "cn=subbu,ou=Group,dc=sk,dc=com"

adding new entry "cn=user1,ou=Group,dc=sk,dc=com"

adding new entry "cn=user2,ou=Group,dc=sk,dc=com"

12) Test the configuration

# ldapsearch -x cn=user2 -b dc=sk,dc=com

dn: uid=user2,ou=People,dc=sk,dc=com

uid: user2

cn: user2

sn: user2

mail: user2@sk.com

objectClass: person

objectClass: organizationalPerson

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: top

objectClass: shadowAccount

userPassword:: e2NyeXB0fSQ2JGZ0RldrYUdPJDhZMC5XRC8wRTFwbWxwUUdnaVcxTHk2YUI2bXl

vRVVrMEJLLy5JNlJJLkRhd0xDanZSVWNxWE5aRWUyRFRnTS9GeHBab29qRVNpTk81Qmt1TDVPMncx

shadowLastChange: 17865

shadowMin: 0

shadowMax: 99999

shadowWarning: 7

loginShell: /bin/bash

uidNumber: 1002

gidNumber: 1002

homeDirectory: /home/user2