Workshop: Configure LDAP Server and migrating the users

Step 1: Install the required LDAP Packages and the migration tools:
yum -y install openldap* migrationtools
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown ldap. /var/lib/ldap/DB_CONFIG
systemctl start slapd
systemctl enable slapd

Step 2: Set OpenLDAP admin password
Generate encrypted password
slappasswd
New password:
Re-enter new password:
{SSHA}R4NrD5Y3JmeU0UBwzrk+tPrIZF/n2h/w

vi chrootpw.ldif
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}R4NrD5Y3JmeU0UBwzrk+tPrIZF/n2h/w

ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.ldif

Step 3: Import basic 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

Step 4: Set your domain name on LDAP DB
slappasswd
New password:
Re-enter new password:
{SSHA}xxxxxxxxxxxxxxxxxxxxxxxx

Step 5: vi chdomain.ldif
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=lpi,dc=org" read by * none

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=lpi,dc=org

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=lpi,dc=org

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}RAc0UwkKHKUJhSv2v9sHUGxIWnF4m28K

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by
  dn="cn=Manager,dc=lpi,dc=org" write by anonymous auth by self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=Manager,dc=lpi,dc=org" write by * read
```

Step 6:

```
# ldapmodify -Y EXTERNAL -H ldapi:/// -f chdomain.ldif
```

Step 7: create base objects in OpenLDAP

Generate a basedomain.ldif file for your Domain

```
# vim basedomain.ldif
dn: dc=lpi,dc=org
objectClass: top
objectClass: dcObject
objectclass: organization
o: anisa

dn: cn=Manager,dc=lpi,dc=org
objectClass: organizationalRole
cn: Manager
description: Directory Manager

dn: ou=People,dc=lpi,dc=org
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=lpi,dc=org
objectClass: organizationalUnit
ou: Group
```

Step 8: configure and use migration scripts

```
# cd /usr/share/migrationtools/
# vim migrate_common.ph

....
Change line 71 to below:
$DEFAULT_MAIL_DOMAIN = "lpi.org";
```

Change line 74 to below:
$DEFAULT_BASE = "dc=lpi,dc=org";

Change line 90 to below:
$EXTENDED_SCHEMA = 1;

Step 9: Create local users
useradd ldapuser1
useradd ldapuser2
passwd ldapuser1
passwd ldapuser2
grep ldapuser /etc/passwd > /root/passwd
grep ldapuser /etc/group > /root/group
export ETC_SHADOW=/etc/shadow # This is an important variable
./migrate_passwd.pl /root/passwd /root/passwd.ldif
./migrate_group.pl /root/group /root/group.ldif

Step 10: Import Users in to the LDAP Database
ldapadd -x -W -D "cn=Manager,dc=lpi,dc=org" -f /root/basedomain.ldif
ldapadd -x -W -D "cn=Manager,dc=lpi,dc=org" -f /root/users.ldif
ldapadd -x -W -D "cn=Manager,dc=lpi,dc=org" -f /root/groups.ldif

Step 11:
vim /etc/openldap/ldap.conf
URI ldap://localhost
BASE dc=lpi,dc=org

Step 12:
To test:
ldapsearch -x -D "cn=Manager, dc=lpi,dc=org " -W

Step 13:
Remove the local ldapuser1 user:
userdel -r ldapuser1

Step 14:
Configure PAM & system authentication:
in CLI (shell) do:

yum install -y openldap-clients nss-pam-ldapd
authconfig --enableldap --enableldapauth --ldapserver "127.0.0.1" --ldapbasedn " dc=lpi,dc=org" --update --enablemkhomedir

Step 15:
Test the PAM service with sshd service: ssh ldapuser1@localhost

Good Luck
Fanavaran Anisa - 2017