OpenLDAP Server and Client Setup

Introduction

This is a guide to setup OpenLDAP server and client in CentOS 7. The server is configured to use NFS for home directories. The client is configured to use LDAP for authentication and NFS for home directories.

Contents

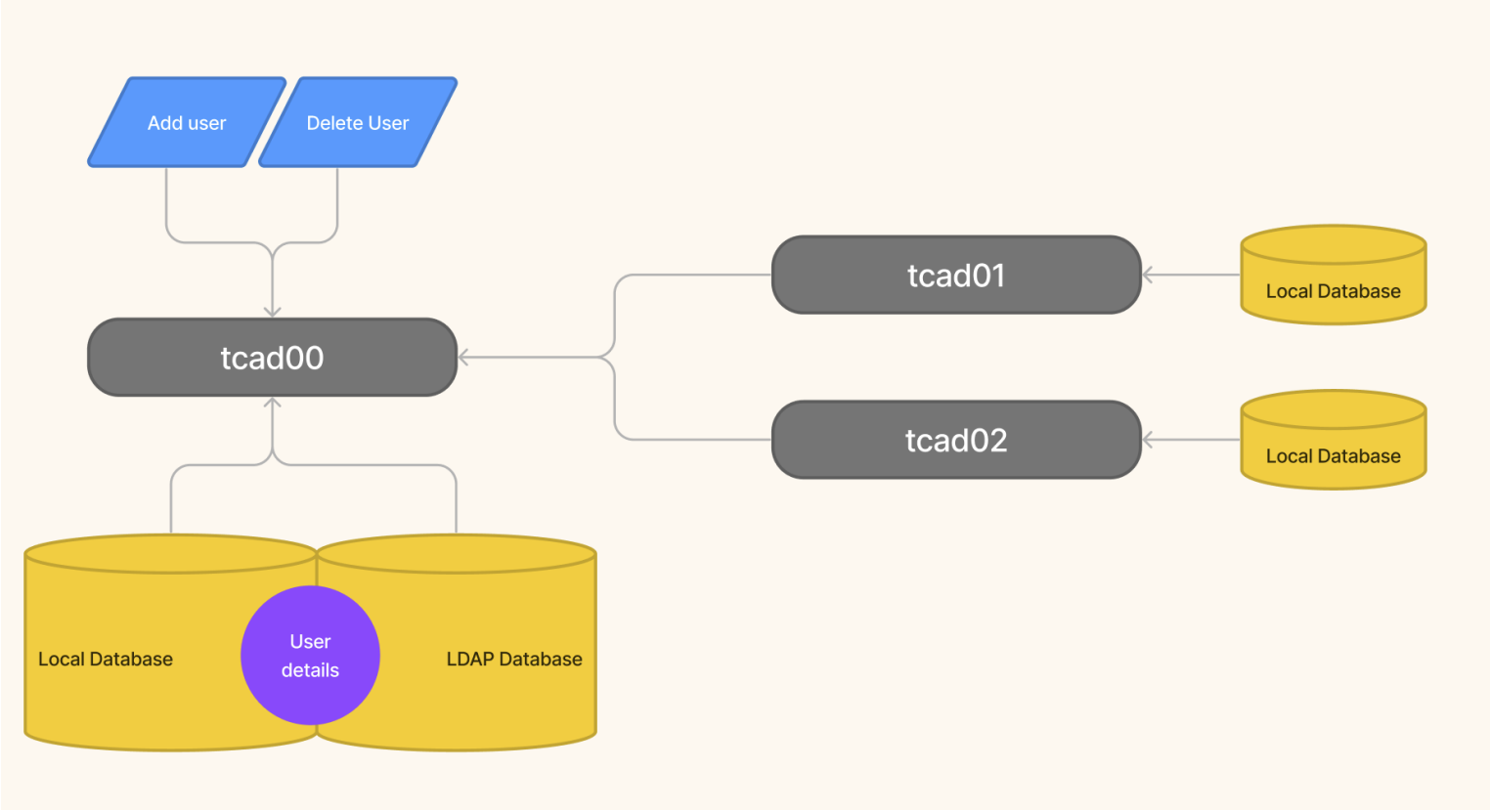
TODO

- [ ] Setup PPOLICY(Password Policy) to expire default password on first login

Configuration

Description	Server	Client
Host Name	tcad00	tcad01
IP Address	192.168.122.62	192.168.122.70

▼ Config Diagram



VM Setup

1. Install CentOS
2. run the following commands

```
# To setup graphical interface: https://www.cyberithub.com/how-to-install-gnome-deskto
[root@tcadxx ~] sudo yum update
[root@tcadxx ~] sudo yum groupinstall "GNOME Desktop" "Graphical Administration Tools"
[root@tcadxx ~] sudo systemctl set-default graphical
[root@tcadxx ~] reboot
# After reboot, you'll get gnome signin
```

3. Disable SELinux(Because it is disabled in other tcad devices)

```
[root@tcadxx ~] sudo vim /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled # <------------------------------------------------------ this line
# SELINUXTYPE= can take one of three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

4. Your device should be ready with to add OpenLDAP and NFS now.

Note: While installing CentOS in VM, make sure to enable network and set hostname in the setup itself. Otherwise, you'll have to do it manually.

Server

1. Install libraries

```
yum  -y install openldap-servers openldap-clients
```

2. Copy LDAP DB config and change ownership

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown ldap. /var/lib/ldap/DB_CONFIG
```

3. Start and enable the LDAP service

```
systemctl start slapd
systemctl enable slapd
```

4. Create OpenLDAP admin password

```
# generate encrypted password
[root@tcad00] slappasswd
New password:
Re-enter new password:
{SSHA}BImora09h57dbDn7R9J0RXdnwB8cjshz

[root@tcad00] cat chrootpw.ldif
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}BImora09h57dbDn7R9J0RXdnwB8cjshz

[root@tcad00] ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

5. Import basic 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
```

6. Set your domain name on LDAP DB.

```
[root@tcad00] cat chdomain.ldif
# domain is "ncl" and "in"
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=ncl,dc=in" read by * none

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

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

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}BImora09h57dbDn7R9J0RXdnwB8cjshz     #<==============Directory Manager

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

[root@tcad00] ldapmodify -Y EXTERNAL -H ldapi:/// -f chdomain.ldif
```

7. Set your base domain for LDAP DB

```
[root@tcad00 ldap] cat basedomain.ldif
# replace to your own domain name for "dc=***,dc=***" section
dn: dc=ncl,dc=in
objectClass: top
objectClass: dcObject
objectclass: organization
o: ncl in
dc: ncl

dn: cn=Manager,dc=ncl,dc=in
objectClass: organizationalRole
cn: Manager
description: Directory Manager

dn: ou=People,dc=ncl,dc=in
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=ncl,dc=in
```

```
objectClass: organizationalUnit
ou: Group

dn: ou=Policies,dc=ncl,dc=in
objectClass: organizationalUnit
objectClass: top
ou: Policies

[root@tcad00] ldapadd -x -D cn=Manager,dc=ncl,dc=in -W -f basedomain.ldif
```

8. Configure firewall

```
firewall-cmd --add-service=ldap --permanent
firewall-cmd --reload
```

Client

1. Install libraries

```
yum -y install openldap-clients nss-pam-ldapd authconfig
```

2. Use `authconfig` to configure ldap client

```
# 192.168.122.62 is the server IP
# dc should match with all the server configurations
[root@tcad01 ~] authconfig --enableforcelegacy --update
[root@tcad01 ~] authconfig --enableldap --enableldapauth --ldapserver="ldap://192.168.

dc=ncl,dc=in" --enablemkhomedir --update
```

3. Add these lines in `/etc/sssd/sssd.conf` file

```
[nss]
homedir_substring = /nclnfs            # <= Important to change the default home direc
fallback_homedir = /home/%u        # <= Incase NFS isn't working, there should be a fa
```

4. Restart sssd service

```
[root@tcad01 ~]# systemctl restart sssd
```

Add user and delete user

1. Using `addUser.sh`, add a new user in server
2. Verify if the user is added to LDAP

```
ldapsearch -x cn=rb875 -b dc=ncl,dc=in #where rb875 is the username
```

3. To delete user, use `delUser.sh`

Now, you can only ssh into the ldap user but linux cannot mount the user because there's no home directory in client machine since home directory is in a NFS mount.

Setup NFS for home directories

Server

```
yum install nfs-utils
systemctl start rpcbind
systemctl enable rpcbind
systemctl start nfs
systemctl enable nfs

mkdir /nclnfs

echo "/nclnfs *(rw,sync,no_root_squash)" >> "/etc/exports"
systemctl restart nfs
systemctl restart rpcbind

firewall-cmd --add-service={nfs,rpc-bind,mountd} --permanent
firewall-cmd --reload
```

Client

```
yum install nfs-utils
systemctl start rpcbind
systemctl enable rpcbind

# 192.168.122.62 is the server IP
showmount -e 192.168.122.62

echo "192.168.122.62:/nclnfs /nclnfs                  nfs     defaults        0 0" >>
mount -a
```

Now client can see the exported `/nclnfs` directory and all the home directories in it.