**Ldap starting refer**

https://www.certdepot.net/rhel7-configure-ldap-directory-service-user-connection

#rpm -qa | grep openldap\*

#netstat -tunpl | grep 389

#sudo yum info openldap openldap-clients openldap-servers migrationtools

#yum install -y openldap openldap-clients openldap-servers migrationtools

#slappasswd -s redhat -n > /etc/openldap/passwd

\* {SSHA}n2+hi91O8l3QiSuPBF2XsUYNwFSppahn\*

* self-signed certificate for our LDAP server /etc/openldap/certs/

#openssl req -new -x509 -nodes -out /etc/openldap/certs/cert.pem -keyout /etc/openldap/certs/priv.pem -days 365

Secure the content of the /etc/openldap/certs directory:

# cd /etc/openldap/certs

# chown ldap:ldap \*

# chmod 600 priv.pem

**Prepare the LDAP database:**

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

**Generate database files (don’t worry about error messages!):**

# slaptest

**Change LDAP database ownership:**

# chown ldap:ldap /var/lib/ldap/\*

**Activate the slapd service at boot:**

# systemctl enable slapd

**Start the slapd service:**

# systemctl start slapd

**Check the LDAP activity:**

# netstat -lt | grep ldap

**(Alternatively, you can use: # ss -ltap | grep ldap)**

**To start the configuration of the LDAP server, add the cosine & nis LDAP schemas:**

# cd /etc/openldap/schema

# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f cosine.ldif

# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f nis.ldif

**Then, create the /etc/openldap/changes.ldif file and paste the following lines (replace passwd with the previously created password like**

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: dc=example,dc=com

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootDN

olcRootDN: cn=Manager,dc=example,dc=com

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootPW

olcRootPW: {SSHA}9Plty1uKvb+g0v+2sNmZuuZ2Q/F55aIl

dn: cn=config

changetype: modify

replace: olcTLSCertificateFile

olcTLSCertificateFile: /etc/openldap/certs/cert.pem

dn: cn=config

changetype: modify

replace: olcTLSCertificateKeyFile

olcTLSCertificateKeyFile: /etc/openldap/certs/priv.pem

Send the new configuration to the slapd server:

dn: cn=config

changetype: modify

replace: olcLogLevel

olcLogLevel: -1

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=example,dc=com" read by \* none

# **ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/openldap/changes.ldif**

Send the new configuration to the slapd server:

**#Create the /etc/openldap/base.ldif file and paste the following lines:**

dn: dc=example,dc=com

dc: example

objectClass: top

objectClass: domain

dn: ou=People,dc=example,dc=com

ou: People

objectClass: top

objectClass: organizationalUnit

dn: ou=Group,dc=example,dc=com

ou: Group

objectClass: top

objectClass: organizationalUnit

**Build the structure of the directory service:**

# ldapadd -x -w redhat -D cn=Manager,dc=example,dc=com -f /etc/openldap/base.ldif

**Create two users for testing:**

# mkdir /home/guests

# useradd -d /home/guests/ldapuser01 ldapuser01

# passwd ldapuser01

**(passwd is admin)**

# useradd -d /home/guests/ldapuser02 ldapuser02

**(passwd is admin)**

**User Account Migration**

**Go to the directory for the migration of the user accounts:**

# cd /usr/share/migrationtools 71 74

**Edit the migrate\_common.ph file and replace in the following lines:**

$DEFAULT\_MAIL\_DOMAIN = "example.com";

$DEFAULT\_BASE = "dc=example,dc=com";

**Create the current users in the directory service:**

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

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

# ldapadd -x -w redhat -D cn=Manager,dc=example,dc=com -f users.ldif

adding new entry "uid=ldapuser01,ou=People,dc=example,dc=com"

adding new entry "uid=ldapuser02,ou=People,dc=example,dc=com"

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

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

# ldapadd -x -w redhat -D cn=Manager,dc=example,dc=com -f groups.ldif

adding new entry "cn=ldapuser01,ou=Group,dc=example,dc=com"

adding new entry "cn=ldapuser02,ou=Group,dc=example,dc=com"

**1. Ldap Client Configuration to use LDAP Server**

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

# sudo yum install -y pam\_krb5

**2. Tool for testing user config tool it self get further action to integrate with your openldap server**

# authconfig-tui

put \* mark on [\*] Use Ldap in User Information

put \* mark on [\*] Use Ldap Authentication in Authenication section

save it

[]Use TLS /this will be the empty because we dont have configure TLS

Server: ldap://ip-address of Openldap server name

Base DN: dc=example,dc=com make it ok

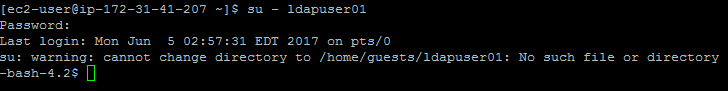
**3**. **Test the Client Configuration.**

**(Search the ldap user using the below command and check the output. If you get output, then our LDAP Configurations are working properly.)**

# **getent passwd ldapuser01**

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

**(if we get this output which shows that our sever and clinet ldap configurations are done)**



**----------------------------------------------------------------------------------------------------------------------**

**From client machine try to login with ldapuser01**

**The above output show that is authenticated by openldap server but there is no local directory on client machine in /home/guests/ldapuser01 so we have to export our home directory from ldapserver to client machine using NFS**

**addprinc –randkey ldapuser01**

**addprinc –randkey ldapuser02**

**ldapuser01@EXAMPLE.COM**

[**ldapuser02@EXAMPLE.COM**](mailto:ldapuser02@EXAMPLE.COM)

**ktadd -k ldapuser01 -norandkey ldapuser01@EXAMPLE.COM**

**ktadd -k ldapuser02 -norandkey** [**ldapuser02@EXAMPLE.COM**](mailto:ldapuser02@EXAMPLE.COM)

**# ktutil**

**ktutil: read\_kt /var/kerberos/myketab/ldapuser01**

**ktutil: list**

**slot KVNO Principal**

**---- ---- ---------------------------------------------------------------------**

**1 3 ldapuser01@EXAMPLE.COM**

**2 3 ldapuser01@EXAMPLE.COM**

**3 3 ldapuser01@EXAMPLE.COM**

**4 3 ldapuser01@EXAMPLE.COM**

**5 3 ldapuser01@EXAMPLE.COM**

**6 3 ldapuser01@EXAMPLE.COM**

**7 3 ldapuser01@EXAMPLE.COM**

**8 3** [**ldapuser01@EXAMPLE.COM**](mailto:ldapuser01@EXAMPLE.COM)

**ON ldap server:**

#rpm –q nfs-utils

#yum –y install nfs-utils

#vi /etc/exports

* /home/ \*(rw,sync)

systemctl start rpcbind

systemctl start nfs-server

systemctl status rpcbind

systemctl status nfs-server

showmount –e

**ON ldap Client**

rpm –qa | grep nfs

yum -y install nfs-utils autofs

vi /etc/auto.master

>> /home/\* /etc/auto.autofs --timeout 600

vi /etc/auto.autofs

>> \* ip-172-31-42-187.ec2.internal:/home/& (ip of ldap server)

systemctl enable autofs

systemctl start autofs

systemctl status autofs

# vi /etc/ssh/ssh\_config

**uncomment and make it yes**

GSSAPIAuthentication yes

GSSAPIDelegateCredentials yes

# vi /etc/ssh/sshd\_config

**make it yes**

GSSAPIAuthentication yes

Permit rootlogin yes

Password authentication yes

#systemctl reload sshd

https://www.youtube.com/watch?v=6SjEhstYR5s#t=69.918977

[‎6/‎9/‎2017 5:40 PM] Rahul Thitame:

1Create base.ldif

#mkdir /root/ldap/

#/usr/share/migrationtools/migrate\_p1 > /root/ldap/base.ldif.

create users,password and groups for LDAP user testing.

#mkdir /home/ldap

#useradd –d /home/ldap/user1 user1;passwd user1

#

#getent shadow |tail –n 3   > /root/ldap/passwords

#getent group |tail –n 3   > /root/ldap/groups

Create LDAP files for users

#./usr/share/migrationtools/migrate\_passwd.p1 /root/ldap/users > /root/ldap/users.ldif

#./usr/share/migrationtools/migrate\_group.p1 /root/ldap/groups > /root/ldap/groups.ldif

[‎6/‎9/‎2017 6:11 PM] Rahul Thitame:

ldapadd –x –W –D “cn=Manager,dc=example,dc=com” –f /root/ldap/base.ldif

#ldapadd –x –W –D “cn=Manager,dc=example,dc=com” –f users.ldif

#ldapadd –x –W –D “cn=Manager,dc=example,dc=com” –f groups.ldif

ldappasswd -H ldap:/// -x -D "cn=Manager,dc=example,dc=com" "uid=rahul,ou=People,dc=example,dc=com" -W -A -S