```
             Openldap server and client Configration in rhel6 with tls

          KISHOR RAMDAS AHIRE (RHCSS)    Fri 01 Mar 2013 12:44:05 PM IST
=======================================================================================
                   LDAP server
            Lightweitht Directory Access Protocol
                   Port No:- 389

LDAP is an internet protocol that email and other programs use to look up information from a server LDAP
is mostly used by medium-to-large organization.
- Centralized User login
- Network User Login
==============================================================================
SSSD = single sign-on Services Deamon
===============================================================
lets see the openldap server setup configuration on rhel 6:-

In my setup:-

1. server name is:- server.example.com
2. address is :- 192.168.0.20/24
3. domain name is:- example.com
4. openldap-server version is:- openldap-servers-2.4.23-20
5. my server os is:- RedHat Enterprise Linux

=======================================================================================
Step 1: first we need to install the required packages:

# yum install openldap-servers openldap-clients -y

Step2: As the configuration for LDAP is stored inside the LDAP server itself the configuration is in
this /etc/openldap/slapd.d/ directory.

(First of all we need set the password for administrator(we called it Manager)by using this command.)

# slappasswd
password: 12345678
retype-password: 12345678

(you'll get something like this "{SSHA}r2or9f2vYlvieCu0LP6wTnSdYfrddsuV" as a result. This is the string
we will have to add into config file. So we need to copy it.)

Now time to open configuration file..

# vim /etc/openldap/slapd.d/cn\=config/olcDatabase\=\{2\}bdb.ldif

(here we need to change domain name)

substitute "my-domain.com" with "example.com" replace.

We can use this command to change this

:%s/dc=my-domain,dc=com/dc=example,dc=com/g

(We now set the administrator(Manager) password..)
and if you want make that encrypt then we need to add those line's over there

add these 3 lines at the end of the file "bdb.ldif" file:

olcRootPW: {SSHA}r2or9f2vYlvieCu0LP6wTnSdYfrddsuV
olcTLSCertificateFile: /etc/pki/tls/certs/example.pem
olcTLSCertificateKeyFile: /etc/pki/tls/certs/examplekey.pem

Step 4: Now we have to specify the monitoring privileges
if you want to monitoring then we need to specify those lines in this file..
```

```
# vim /etc/openldap/slapd.d/cn\=config/olcDatabase\=\{1\}monitor.ldif
```

again, we have to replace the default domain name with our domain name

now can replace the default domain name manualy.

```
:%s/cn=manager,dc=my-domain,dc=com/cn=Manager,dc=example,dc=com/g
```

Step 5: Now its time for the Database Cache

```
# updatedb
```

otherewise automatic calculation of cache we need to copy that file in this location

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

now set the permission for ldap user also.

```
# chown -Rf ldap:ldap /var/lib/ldap/
```

Step 6: Now we will need to set up a certificate for TLS. First we need to edit /etc/sysconfig/ldap and change SLAPD_LDAPS= options in this manner

```
# vim /etc/sysconfig/ldap
```

```
SLAPD_LDAPS=yes -----(default is no)
```

Now we need to create certificate.

There is lots of options for gen rate the certificate we can use any method.
I am going with this command.

```
# openssl req -new -x509 -nodes -out /etc/pki/tls/certs/example.pem -keyout /etc/pki/tls/certs/examplekey.pem -days 365
```

fill the required information of command

This will create the two required keys in the /etc/pki/tls/certs/ directory. We need to make them readable for the ldap user.

```
# chown -Rf root:ldap /etc/pki/tls/certs/example.pem
# chown -Rf root:ldap /etc/pki/tls/certs/examplekey.pem
```

check the read permission for ldap user........

```
# cp -iv /etc/pki/tls/certs/example.pem /var/ftp/pub/ca.crt
```

Step 7: Time to test our configuration

Now time to check the ldap configuration

```
# slaptest -u
```

"config file testing succeeded" answer should we come..

Step 8: Start the ldap server

```
# service slapd start
# chkconfig slap on
```

```
# yum install migrationtools -y
# cd /usr/share/migrationtools
# ls
# vim migrate_common.ph
```

on the line number 61. change "ou=Groups"

```
on the line number 71. change your domain name

"example.com";

on the line number 74. change your base name
"dc=example,dc=com";

on the line number 90. change schema value

$EXTENDED_SCHEMA=1;
:wq

# ./migrate_base.pl > /root/base.ldif

# mkdir /rhome
# useradd -u 5000 -d /rhome/ldapuser1 ldapuser1
# useradd -u 5001 -d /rhome/ldapuser2 ldapuser2
# passwd ldapuser1
# passwd ldapuser2   [password is redhat]

Step 9: Configure the base domain

# vim /etc/exports

/rhome   *(rw)
:wq

# service nfs restart

# chkconfig nfs on

# getent passwd | tail -n 2 > /root/users
# getent shadow | tail -n 2 > /root/passwds
# getent group | tail -n 2 > /root/groups

# vim migrate_passwd.pl

inside this file search /etc/shadow and change it to /root/passwds and then save & exit
line no. 188

:wq

#./migrate_passwd.pl /root/users > /root/users.ldif

#./migrate_passwd.pl /root/groups > /root/groups.ldif

now we import our base information to the ldap directory:

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

redhat

Step 10: add the users in ldap

(now time to add the users into ldap database. Do that only we need to create a .ldif file and we can add
it into ldap.)

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

redhat

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

Now test this user's List.

# ldapsearch -x -b "dc=example,dc=com"
```

it should be receive success result.

#################### Ldap Client Configuration #####################

there is only few steps for connect the client with ldap server.

First pf all we need to install the required package's on client side.

Step first:-

```
# yum install openldap-clients -y
```

Step Two:-

simple run the authentication command.

```
# authconfig-gtk or authconfig-tui or system-config-authentication
```

put the url of certificate. which is already shared from your ftp server...

Now should be able to find the users in the ldap database..

```
# ldapsearch -x -ZZ        [to check]
```

Auto Mounting...

```
# vim /etc/auto.master
# vim /etc/auto.misc
```

DONE