Open LDAP Lab 10

Unfortunately, LDAP doesn't play well with the underlying SELinux (Security Enhanced Linux) system on Centos, so we'll need to disable that before proceeding. It's nothing to worry over much about -- SELinux is usually more trouble than it's worth anyway. So, on your centos-server VM:

1. Edit (with `sudo`) `/etc/sysconfig/selinux`.
2. Change the line that says "`SELINUX=enforcing`" to be: `SELINUX=disabled`
3. Save the file and exit.
4. Reboot the VM.

OK, now we can get on with installing our LDAP server.

Use Yum to download the following five packages:

- openldap-clients
- openldap-servers
- openldap
- nss-pam-ldapd
- pam_krb5

Set up your admin password with `slappasswd`

a. It will ask you to repeat the password and give you a SHA hash.
b. **Save the line with the hash**. Mine was {SSHA}Qc2w7vayLQkVBVqdmxsnKt8OfQ45r7oo

Edit the configuration file.

edit `/etc/openldap/slapd.d/cn=config/olcDatabase={2}bdb.ldif`

Make the following changes:

```
suffix "dc=comp150,dc=com
rootdn "cn=Manager,dc=comp150,dc=com"
rootpw <{SHA}yourhash>
```

If your domain contained additional components, such as `eng.uni.edu.eu`, you would use:

```
database bdb
suffix "dc=eng,dc=uni,dc=edu,dc=eu"
rootdn "cn=Manager,dc=eng,dc=uni,dc=edu,dc=eu"
rootpw secret
directory /usr/local/var/openldap-data
```

Details regarding configuring *slapd*(8) can be found in the *slapd.conf*(5) manual page and the The slapd Configuration File chapter of this document.

Add this information `ldap.conf` by going to System/Administration/Authentication

a. User Account Database LDAP
b. LDAP Search Base DN: ou=people,dc=comp150
c. LDAP Server: ldaps://centos-server.comp150
d. Don't select TLS
e. Authentication Method: LDAP password

2. You will need to add the line below to /etc/openldap/ldap.conf

```
HOST    127.0.0.1
```

Start SLAPD.

You are now ready to start the Standalone LDAP Daemon, *slapd*(8), by running the commands:

```
sudo chkconfig slapd on
sudo service slapd start
```

To check to see if the server is running and configured correctly, you can run a search against it with *ldapsearch*(1). By default, *ldapsearch* is installed as `/usr/local/bin/ldapsearch`:

Test the base configuration:

```
ldapsearch -x -s base -b "" "objectclass=*"
```

TAKE A SCREENSHOT of the output of the command showing the above line.

Details regarding running *slapd*(8) can be found in the *slapd*(8) manual page and the Running slapd chapter of this document.

Add initial entries to your directory.
You can use *ldapadd*(1) to add entries to your LDAP directory. *ldapadd* expects input in LDIF form. We'll do it in two steps:

1. create an LDIF file
2. run ldapadd

Use your favorite editor and create an .ldif file that contains:

```
dn: dc=comp150,dc=com
objectclass: dcObject
objectclass: organization
o: <MY ORGANIZATION>
dc: <MY-DOMAIN>

dn: cn=Manager,dc=<MY-DOMAIN>,dc=<COM>
objectclass: organizationalRole
cn: Manager
```

Be sure to replace `<MY-DOMAIN>` and `<COM>` with the appropriate domain components of your domain name. `<MY ORGANIZATION>` should be replaced with the name of your organization. When you cut and paste, be sure to trim any leading and trailing whitespace from the example.

```
dn: dc=example,dc=com
objectclass: dcObject
objectclass: organization
o: Example Company
dc: example

dn: cn=Manager,dc=example,dc=com
objectclass: organizationalRole
cn: Manager
```

Now, you may run *ldapadd*(1) to insert these entries into your directory.

```
ldapadd -x -D "cn=Manager,dc=comp150,dc=com" -W -f example.ldif
```

where `example.ldif` is the file you created above.

You will be prompted for the "`secret`" specified in `slapd.conf`.

Additional information regarding directory creation can be found in the Database Creation and Maintenance Tools chapter of this document.

See if it works.
Now we're ready to verify the added entries are in your directory. You can use any LDAP client to do this, but our example uses the *ldapsearch*(1) tool. Remember to replace `dc=example,dc=com` with the correct values for your site:

```
ldapsearch -x -b 'dc=example,dc=com' '(objectclass=*)'
```

This command will search for and retrieve every entry in the database.

TAKE A SCREENSHOT of the output of the command showing the above line.