Please use a Screen or Video Capture software to save your works!

OBJECTIVE & PREPARATION

- Learn some fundamental concepts and terminology used with LDAP.
- Practice creating users in OpenLDAP.
- Set up Linux machines to authenticate against an OpenLDAP server.
- Learn to update LDAP information with ldif files.

Online Resources

We'll use OpenLDAP in this course.

The purpose of LDAP the way it's used most of the time is relatively intuitive, but the implementation details will take longer to understand.

LDAP is a generic directory access protocol, but we'll look at it specifically as a server containing user credentials that can be used for authorization on multiple machines.

You should read as much of the OpenLDAP Administration Guide as you can handle. You'll find that parts of it make no sense at first, but as you get more practice with the software and the concepts they become easier to understand. As a minimum, read:

- The introduction.
- The quick start guides.
- The configuration layout part of "Configuring slapd".
- There is a glossary at the end of the guide. It's not complete and it doesn't have any details, but it's a good place to look when you get confused by weird looking shorthands like dc, dn, or cn.

Case 1: Binding a Client Machine to an LDAP server (ops345.com)

You won't be asked to set up an OpenLDAP server from scratch, we don't have time for that. So, you can start with a VM I made for you.

- The ldap server is "ops345.com"
- The ldap password (if asked) is "Password1234"

OpenLDAP has been set up on it using this itzgeek guide. You should read that guide even though you don't need to perform all those steps yourself.

This OpenLDAP server (ops345.com) has been set up with:

- The Domain Components dc=ops345,dc=com.
- An Organisation Unit named People, for regular users.

The rest of your tasks for this section of the lab are to set up your Server or Client VM to authenticate using the LDAP service hosted on ops345.com.

Perform the Following steps on any of your VM(s):
LDAP client configuration to use LDAP Server, use "Password1234" when asked.

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

authconfig --enableldap --enableldapauth --ldapserver=ops345.com --ldapbasedn="dc=ops345,dc=com" --enablemkhomedir --update

systemctl restart nslcd
```

Case 2: Adding Users to LDAP

Perform the Following steps on the same VM from Case 1. Replace ldapuser to your first name.

```
vi ldapuser.ldif
```

Add the following contents to the file, replace the highlighted part with your own value (e.g. your Seneca username) and the **uidNumber** should be unique.

Better to put your Seneca Student number for the **uidNumber** to make sure it is unique. (This field could have max of 10 characters).

```
dn: uid=ldapuser,ou=People,dc=ops345,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: ldapuser
uid: ldapuser
uidNumber: 99999999
gidNumber: 100
homeDirectory: /home/ldapuser
loginShell: /bin/bash
gecos: LDAP user [User (at) ops345.com]
userPassword: {crypt}x
shadowLastChange: 17058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
```

Run the following command to create the user from the ldif file:

```
ldapadd -x -w Password1234 -D "cn=ldapadm,dc=ops345,dc=com" -f ldapuser.ldif
```

Change the password for the newly created "ldapuser":

```
ldappasswd -s Password1234 -W -D "cn=ldapadm,dc=ops345,dc=com" -x "uid=ldapuser,ou=People,dc=ops345,dc=com"
```

Check if the account created successfully:

```
ldapsearch -x cn=ldapuser -b dc=ops345,dc=com
```

Delete the ldapuser account:

```
ldapdelete -W -D "cn=ldapadm,dc=ops345,dc=com" "uid=ldapuser,ou=People,dc=ops345,dc=com"
```

Case 3: Authenticating against LDAP

Perform the Following steps on the same VM from Case 2.

1. Verify LDAP Login

   ```
   getent passwd ladpuser
   ```

   or simply "getent passwd" to see all users.

2. Login to the same VM from Case 2 with the newly created username and password to make sure you can login.
   Note you are login with the ldap user, not the local user on the OS.

Save the captured file(s) or video file(s) as OPS345_Lab10_yourusername and upload to Blackboard.