

LDAP Authentication

(CISS – 150 William Jojo)
(20081015)

Authenticated Remote LDAP Users (10-points)

Install software for LDAP support in the Ubuntu GUEST. Using Synaptic or the command line install:

libnss-ldap

slapd

ldap-utils

Other packages will be installed in addition to these.

Choose a password you will remember when installing slapd. This password will be changed later for administrative access to any LDAP databases controlled by **slapd** you will create on this guest.

When configuring **ldap-auth-config**, you will need to know the following:

LDAP Version is 3

rootdn is **cn=admin,dc=ciiss150,dc=net**

ldap URI is **ldap://acedev2.hvcc.edu**

Search base DN is **dc=ciiss150,dc=net**

We will not make root the database admin.

The database does not require login.

When modifying configuration files or running privileged commands, consider opening a root shell with **sudo bash**.

Local users are defined in **/etc/passwd**. The command **getent passwd** should display the local users. If you do not have users displayed, STOP and get assistance.

The file **/etc/ldap.conf** allows LDAP tools to use a default mechanism. This file was created with **ldap-auth-config** processing. Confirm the file has the following lines uncommented:

```
BASE dc=ciiss150,dc=net
URI ldap://acedev2.hvcc.edu
host acedev2.hvcc.edu
rootbinddn cn=admin,dc=ciiss150,dc=net
bind_policy soft
```

Add to **/etc/ldap/ldap.conf** (may not exist):

```
BASE dc=ciiss150,dc=net
URI ldap://acedev2.hvcc.edu
```

Contact the LDAP server using the following command:

```
ldapsearch -x -LLL dn
```

You should receive about 35 distinguished names.

Now modify/create `/etc/libnss-ldap.conf` whose line must minimally be:

```
host acedev2.hvcc.edu
base dc=ciss150,dc=net
ldap_version 3
rootbinddn cn=admin,dc=ciss150,dc=net
```

Also modify/create `/etc/pam_ldap.conf` to include the text below. You may just need to uncomment and/or enhance some lines.

```
host acedev2.hvcc.edu
base dc=ciss150,dc=net
ldap_version 3
rootbinddn cn=admin,dc=ciss150,dc=net
pam_password md5
nss_base_passwd ou=people,dc=ciss150,dc=net?one
nss_base_shadow ou=people,dc=ciss150,dc=net?one
nss_base_group ou=groups,dc=ciss150,dc=net?one
```

Now set the password for the `rootdn` in `/etc/ldap.secret`, `/etc/libnss-ldap.secret` and `/etc/pam_ldap.secret`

Edit `/etc/nsswitch.conf` and add `ldap` to the `passwd`, `shadow` and `group` lines like so:

```
passwd:      compat ldap
group:       compat ldap
shadow:      compat ldap
```

The `getent passwd` (and `getent group`) command should now return your LDAP users at this point. If you do not have users from LDAP displayed, STOP and get assistance.

Now we will configure Ubuntu to allow these newly discovered users to login to this guest.

Edit the following files. These configurations guarantee that you can still login with local credentials in case the LDAP server is unavailable.

/etc/pam.d/common-account:

```
account sufficient pam_ldap.so
account required pam_unix.so
```

/etc/pam.d/common-auth:

```
auth sufficient pam_ldap.so
auth required pam_unix.so nullok_secure use_first_pass
```

/etc/pam.d/common-password:

```
password sufficient pam_ldap.so
password required pam_unix.so nullok obscure min=4 max=8 md5
```

/etc/pam.d/common-session:

```
session required pam_unix.so
session required pam_mkhomedir.so skel=/etc/skel
session optional pam_ldap.so
```

The following commands should return the ldap users and groups:

```
getent passwd
getent group
```

Select a user based on your team number. Be sure to create a home directory based on the LDAP information for that user. For example:

```
sudo mkdir /home/remuser##
sudo chown remuser##:remgroup## /home/remuser##
```

You should be able to logout and log back in as the LDAP user at this point.

You must demonstrate to your instructor that you can successfully login to GNOME using your LDAP user account.

Authenticated Local LDAP users (10 points)

Install **ldapscripts**.

Run the following commands to stop LDAP and remove the current database:

```
sudo /etc/init.d/slaped stop
sudo rm /var/lib/ldap/*
```

```
sudo dpkg-reconfigure slapd
```

1. Select the default of **NO** for Omit server configuration.
2. Enter the domain name **newdomain.local**
3. Enter whatever you like for the organization name.
4. Choose a new admin password and confirm.
5. Press the **TAB** key and then press the **Enter** key for **Ok** regarding the use of HDB.
6. Press **Enter** for the default of keeping the database if **slaped** is purged.
7. If asked, select **Yes** and press **Enter** to move the old database.
8. Press **Enter** to accept the default of **NO** for LDAPv2 support.

```
sudo gedit /etc/ldap/ldap.conf
and
sudo gedit /etc/ldap.conf
```

Be sure that the following are set and uncommented:

```
BASE dc=newdomain,dc=local
host 127.0.0.1
URI ldap://127.0.0.1
```

At this point an `ldapsearch` should return some results.

Create a file `ou.ldif` with the following information:

```
dn: ou=people,dc=newdomain,dc=local
ou: people
objectclass: organizationalunit

dn: ou=groups,dc=newdomain,dc=local
ou: groups
objectclass: organizationalunit
```

Then run the command:

```
ldapadd -x -D cn=admin,dc=newdomain,dc=local -w secret -f ou.ldif
```

Modify the `/etc/ldapscripts/ldapscripts.conf` file so that there are uncommented, modified entries like so:

```
SERVER=127.0.0.1
BINDDN='cn=admin,dc=newdomain,dc=local'
BINDPWD='secret'
SUFFIX='dc=newdomain,dc=local'
GSUFFIX='ou=groups'
USUFFIX='ou=people'
GIDSTART=10000
UIDSTART=20000
MIDSTART=20000
PASSWORDGEN="echo %u"
```

Now you must re-modify `/etc/libnss-ldap.conf` and `/etc/pam_ldap.conf`

Now set the password for the rootdn in `/etc/ldap.secret`, `/etc/libnss-ldap.secret` and `/etc/pam_ldap.secret` if they have changed.

Run the following commands to create a new group (called `newldapgrp`) and user (called `newldapuser`):

```
sudo ldapaddgroup newldapgrp
```

Make sure `getent group` returns your new group. If not check `/var/log/ldapscripts.log` for hints about the problem.

```
sudo ldapadduser newldapuser newldapgrp
```

Make sure you can see the user with `getent passwd`. Check the log if the new user is not present.

```
sudo passwd newldapuser
```

You should be able to logout and log back in as the LDAP user at this point. If you receive a message “cannot set your user group” you will need to reboot and then the login should succeed.

You must demonstrate to your instructor that you can successfully login to GNOME using your LDAP user account.