LDAP

# VM Prep

Roll back to a snapshot of your VM from the beginning of February, we want a nice clean VM.

We want one Network Adapter that is set to NAT.

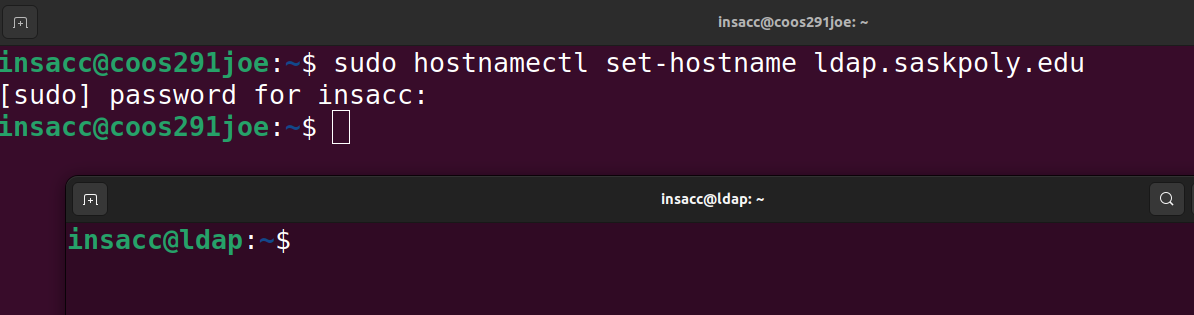
# Install LDAP

Reference Link: <https://computingforgeeks.com/install-and-configure-openldap-server-ubuntu/>

The first thing we want to realize, is that LDAP in Ubuntu will be implemented through OpenLDAP. OpenLDAP is open source of course, and it’s very popular for this type of implementation.

1. Change the hostname: **sudo hostnamectl set-hostname ldap.saskpoly.edu**

Close the terminal and reopen it to see the change in the prompt.



1. Let’s have a look at the output of a couple of commands:
   1. cat /etc/passwd
   2. getent passwd 🡨 gets all of the entries in the passwd database

Note that currently they look the same, this will change after we set up LDAP.

Let’s also ensure our package repositories are up to date: **sudo apt update**

1. Next, let’s install slapd and ldap-utils. Again, slapd is our implementation of ldap, specifically openldap.
   1. Run the following command: **sudo apt -y install slapd ldap-utils**

It will prompt you for an Administrator Password:

Graphical user interface, application

Description automatically generated

This password will correspond to the admin account used to maintain and service slapd. For now, use “password”, but in a real organization, use something more secure.

Confirm it:

Graphical user interface, timeline

Description automatically generated

When we install slapd, it uses a default database entry for our DIT.

1. We can view our current database by executing the following command:
   1. Output the current SLAPD database contents: **sudo slapcat**

Text

Description automatically generated



When we installed slapd, it detected our hostname that we set, and created our top-level **d**omain **c**omponents automatically (dc=saskpoly, dc=edu).

1. Next, we need to edit this “database”. We’ll be adding other distinguished names and organizational units.
   1. First, let’s create a directory to put some files in. When we edit our DIT, we’ll be creating .lidf files and then importing them into ldap.

Create a directory /var/ldap: **sudo mkdir /var/ldap** and browse to it.

Text

Description automatically generated

* 1. Let’s create our Base. This base will be at the top level underneath our domain components (edu->saskpoly). We’ll make two OU’s: people & groups.

**sudo vi basedn.ldif**

**dn: ou=people,dc=saskpoly,dc=edu**

**objectClass: organizationalUnit**

**ou: people**

**dn: ou=groups,dc=saskpoly,dc=edu**

**objectClass: organizationalUnit**

**ou: groups**

Text

Description automatically generated



“dn” stands for distinguished name. Like it implies, it’s a unique name for our new entry.

Note that the two “entries” are separated by the blank line.



* 1. It’s just a file right now, we have to import it into our database (DIT). To do this, add it to our database via the **ldapadd** command that is now available after installing slapd and ldap-utils.

Run the following command to import our ldif file into our database:

**sudo ldapadd -x -D cn=admin,dc=saskpoly,dc=edu -W -f basedn.ldif**

Text

Description automatically generated

* 1. Let’s check out our database after these changes by slapping the cat: **sudo slapcat**

Text

Description automatically generated



* 1. **Working with Users and Groups:**

**User Creation:** There’s multiple ways to do this. First, user ldifs (ldif files that add users) have an option to provide a password hash for that user.

* + 1. This is great if you have a default org password you use for new employees etc. Let’s use Welc0me!
    2. To generate a hash for a new user Bob, execute the following command:

**sudo slappasswd**

Text

Description automatically generated

This is a password hash. They’re used everywhere, think of all your online user accounts. COPY IT!! **{SSHA}CI0tiIAr7Lk/JqhNT/PsHVLDkKCpL9/z**

* + 1. From here, lets’ create a new ldif file called ldapusers.ldif: **sudo vi ldapusers.ldif**

**dn: uid=Bob,ou=people,dc=saskpoly,dc=edu**

**objectClass: top**

**objectClass: account**

**objectClass: PosixAccount**

**objectClass: shadowAccount**

**cn: bob**

**uid: bob**

**uidNumber: 3001**

**gidNumber: 3101**

**homeDirectory: /home/bob**

**loginShell: /bin/bash**

**userPassword: {SSHA}ySUWpLeRr1gH4nEJ8FdhXqV9BzfHJpSj**

Text

Description automatically generated

Note the pretty colours! (Sorry Connor)

Text

Description automatically generated

* + 1. And add it to our database via the ldapadd command:

**sudo ldapadd -x -D cn=admin,dc=saskpoly,dc=edu -W -f ldapusers.ldif**

Text

Description automatically generated

Let’s slap our cat: **sudo slapcat**

Text

Description automatically generated

Our user has been added!

Let’s add another user: Just edit the previous file and run the ldapadd command again.

Text

Description automatically generated

**sudo slapcat** to see Timmy in our database:

Text

Description automatically generated

* + 1. Group Creation: Let’s create a group ou for Bob to be a member of with a file called ldapgroups.ldif:

**sudo vi ldapgroups.ldif**

**dn: cn=students,ou=groups,dc=saskpoly,dc=edu**

**objectClass: posixGroup**

**cn: students**

**gidNumber: 3101**

**memberUid: bob**

**memberUid: timmy**

^repeat this line for multiple users to be added to the group

Text

Description automatically generated

**sudo slapcat** to see our new group in our database:

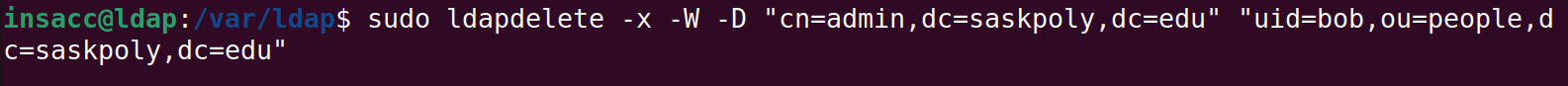
Text

Description automatically generated



To **delete** an entry, we can use ldapdelete:

**sudo ldapdelete -x -W -D "cn=admin,dc=saskpoly,dc=edu" "uid=bob,ou=people,dc=saskpoly,dc=edu"**



And if we **sudo slapcat**, we will see that Bob no longer exists:

* 1. Let’s add some logging to slapd. Let’s configure Rsyslog to log LDAP events to the log file /var/log/ldap.log
     1. **sudo vi /etc/rsyslog.conf**
     2. add the following line: **local4.\* /var/log/ldap.log**
     3. And then restart rsyslog: **sudo systemctl restart rsyslog**

Text

Description automatically generated