LDAP Part 2

# LAM Installation

We are going to install a web-based administration tool to administer and maintain or LDAP database. Of course, we don’t need a web-based admin tool to maintain, we can use the shell. But since we’re just adding users and groups to an existing install, we will install something called LDAP Account Manager (LAM).

1. Since it’s web-based, let’s generate a certificate as we’ll want to access it over HTTPS.

First, let’s create a directory for our certificates. We’ll copy them after they’ve been generated to a different location. We have a working directory of /var/ldap where we’ve putting out ldif files.

* 1. Let’s create a certs directory there: **sudo mkdir /var/ldap/certs**

Text

Description automatically generated

* 1. Next, let’s use a utility called **setfacl.** This utility will help us set ACLs (Access Control List) for files and directories.
     1. Execute the following command to give the account “openldap” read and execute access to the new certs directory: **sudo setfacl -m u:openldap:rx /var/ldap/certs**.

We can verify with: **sudo getfacl /var/ldap/certs/**

Text

Description automatically generated

Note the “+”indicates that additional permissions have been applied through an ACL.

* 1. Next, let’s generate a self-signed certificate for our ldap server:

**sudo openssl req -new -x509 -nodes -out /var/ldap/certs/saskpoly.pem -keyout /var/ldap/certs/saskpolykey.pem\** Background pattern

Description automatically generated

Text

Description automatically generated

Note: Ensure the Common Name property to matches your hostname. This cert will be moved to an Apache server.

* 1. Take a look in the certs directory, this is what you should see: ll /var/ldap/certs

Text

Description automatically generated

* 1. Let’s change the ownership of those certs to openldap:

**sudo chown openldap:openldap /var/ldap/certs/\*.pem**

Text

Description automatically generated

Recall: The ***saskpolykey.pem*** file is the private key and needs to be kept secure. The ***saskpoly.pem*** file is the public key (or certificate) that we will add to our server shortly after installing Apache2.

* 1. Let’s tell slapd about these certificates.
     1. Create a file called certmodify.ldif: **sudo vi /var/ldap/certmodify.ldif**

And add the following lines:

dn: cn=config

changetype: modify

add: olcTLSCertificateKeyFile

olcTLSCertificateKeyFile: /var/ldap/certs/saskpolykey.pem

-

add: olcTLSCertificateFile

olcTLSCertificateFile: /var/ldap/certs/saskpoly.pem

Text

Description automatically generated

Text

Description automatically generated

* + 1. The LDAP config is stored in LDAP and is not a file we can change directly. We can however, modify our database with the **ldapmodify** command:

**sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f certmodify.ldif**

* + - * This command modifies an LDAP entry based on the certmodify.ldif file (“cn=config”), with authentication for this change being set to external, ie a Linux user, not an LDAP user (-Y EXTERNAL), and connects to the local LDAP server to make the change (-H ldapi:///).

Text

Description automatically generated

Note: The **ldapmodify** command is very useful. For example, you can add and remove attributes for users. Check it out **man ldapmodify** for more information.

* + 1. Next, restart: **sudo systemctl restart slapd** and that’s it for the server!

1. Now we’re ready to add and configure a web-app called LDAP Account Manager (LAM). It has a few dependencies, namely: slapd, apache, php

Reference: <https://computingforgeeks.com/install-and-configure-ldap-account-manager-on-ubuntu/>

* 1. Since we don’t have DNS setup here: do **hostname -I** to get your *ipaddress* then **vi /etc/hosts** and add this line: ***ipaddress* ldap.saskpoly.edu**

Text

Description automatically generated

* 1. Let’s install php since we don’t have that yet. Run the following:

**sudo apt -y install php php-cgi libapache2-mod-php php-mbstring php-common php-pear**

*Adding the libapache2-mod-php should automatically install apache2 as a dependency, if not run sudo apt install apache2. Check the Apache2 status: sudo systemctl status apache2.*

* 1. Now we can copy our public key file to our webserver so that it’s hosted on the default site for ldap.saskpoly.edu. (Recall that /var/www/html is the default site location.):

**sudo cp /var/ldap/certs/saskpoly.pem /var/www/html**

Text

Description automatically generated

* 1. Next, install and configure LDAP Account Manager: **sudo apt -y install ldap-account-manager** Text

     Description automatically generated
  2. After successful installation, let’s take a look at the LDAP account manager (LAM). Open Firefox and go to the following url: **ldap.saskpoly.edu/lam**

Graphical user interface

Description automatically generated

* 1. Initially, go to LAM configuration in the top-right. Once there, you’ll be given this screen:  
     Graphical user interface, text, application

     Description automatically generated
  2. Click on Edit server profiles. It will ask you for a password for the ldap admin “lam”. The default password is “lam”. It takes you to this screen, where we’ll have to edit some properties to reflect our DIT Adjust the Tool settings Tree Suffix to be dc=saskpoly,dc-eduGraphical user interface, text, application

     Description automatically generated
  3. Adjust the security settings: Graphical user interface, text, application

     Description automatically generated
  4. Change your password at the bottom if you so wish: (This is the “lam” password.)A picture containing diagram

     Description automatically generated
  5. Switch to the “Account Types” tab, and make the following changes:

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

* 1. So, logging in with admin/password will open up our web-based ldap manager.Graphical user interface, application

     Description automatically generated
  2. We’re provided with the list of LDAP Users and Groups:

Graphical user interface, application, table

Description automatically generated

* 1. Here, we can create a new user, delete users that we select, and edit/delete/generate account PDFs for any of the users listed, as well as groups.

1. Creating a new LDAP User via LAM:

Graphical user interface, text, application, chat or text message

Description automatically generated

* 1. Click on “New user.

Graphical user interface, application

Description automatically generated

* 1. On the Personal page, enter a First and Last name.

Graphical user interface, text, application

Description automatically generated

* 1. On the Linux page, enter the desired User name.

Graphical user interface, application

Description automatically generated

* 1. Click on Set Password.

Graphical user interface, application

Description automatically generated

* 1. Enter the same password twice and click ok.

Graphical user interface, text, application, email

Description automatically generated

* 1. Save the changes.

Text

Description automatically generated

* 1. Log on as the new user.

# Install the LDAP Client

Reference: <https://computingforgeeks.com/how-to-configure-ubuntu-as-ldap-client/>

This allows logging in as users that are defined in LDAP

1. Install the LDAP client utilities. Namely, we’ll install the packages libnss-ldap, libpam-ldap, ldap-utils

**Libnss-ldap** allows X.500 and ldap directory servers to be used as a name service, maps usernames to UIDs and the information in /etc/passwd

**Libpam-ldap** installs PAM (Pluggable Authentication Module), this provides authentication from LDAP

To install, run the following command: **sudo apt -y install libnss-ldap libpam-ldap ldap-utils**

1. During installation, we’ll have to configure pam:

Graphical user interface, text, application

Description automatically generated

* 1. Here, enter **ldapi:///** (if we were doing this on another machine we would enter ldap://ldap.saskpoly.edu and make sure the other machine has an entry in the hosts file for this.)

Text

Description automatically generated

* 1. Enter your top-level DCs. **dc=saskpoly,dc=edu**

Graphical user interface, text, application

Description automatically generated

* 1. Next, we’ll be asked the following. Selection V3

Graphical user interface, text, application

Description automatically generated

* 1. Next, we’ll be asked if we want to make local root a database admin. Let’s choose **Yes**.

Graphical user interface, text

Description automatically generated

* 1. Next, we’ll be asked whether the LDAP database requires login in order retrieve entries. For now, let’s turn that off. Select **No**.

Graphical user interface, text, application

Description automatically generated

* 1. Next, what account should PAM use if the root wants to change a password? Let’s use the admin cn that we created: **cn=admin,dc=saskpoly,dc=edu**

Graphical user interface, text, application

Description automatically generated

* 1. Choose a password. Preferably something you’ll remember. I’m using “**password**”
  2. After this, it will continue installing our packages.

1. Let’s enable ldap authentication on our nsswitch.conf located here: **sudo** **vi /etc/nsswitch.conf**. We’ll edit the following two lines:
   1. passwd: files systemd ldap 🡨 add the word ldap
   2. group: files systemd ldap 🡨 same here, add ldap

Text

Description automatically generated

Now let’s compare the output of cat /etc/passwd and getent passwd, they’re no longer the same!

1. The LDAP accounts we have set up right now don’t have home directories. Let’s configure PAM to create one when a user first logs in.
   1. To do this: **sudo vi /etc/pam.d/common-session** and add the following line at the bottom:

**session optional pam\_mkhomedir.so skel=/etc/skel umask=077**

Text

Description automatically generated Text

Description automatically generated

**And we’re done!**

Let’s test it out. Try logging as “timmy” with the Welc0me! password.

Text

Description automatically generated

**Exercise**: Create 2 additional users “jill” and “ted” through LAM and confirm you can log in.