**CSI3670**

**Winter 2021**

**Lab 4: LDAP**

**3/14 at 11:59pm**

**Synopsis:**

In this lab, you will be installing LDAP and playing around with Bash. A nice complement to the last lab (which I know was before break, but still).

Although the final project is for extra credit this semester and therefore optional, pretend that you’re planning to do it anyway with a group of classmates and come up with a fun (class-appropriate) team name. Use that team name for the purposes of this lab.

**LDAP Installation**

1) Login to your GCP Ubuntu partition

LDAP:

$ sudo apt update && sudo apt upgrade

$ sudo apt install slapd ldap-utils

It will ask you for an administrator password. This will be the root credentials of your rootDN of the database (root distinguished name).

The installation set up two directory information trees (DIT). One for slapd-config (config utility for LDAP) and your user-defined information.

Now let’s configure LDAP.

$ sudo dpkg-reconfigure slapd

\* Select **No** for the first option (Omit OpenLDAP server configuration)

\* DNS domain name should be csi3670.local

\* Organization name should be your team name

\* Give it the local Administrator password you created when you first installed (probably temp12345)

\* Select MDB database (if asked)

\* Select Yes for database to be removed when it is purged

\* Yes to Move Old Database

\* No to LDAPv2 if asked

Run the following command to make sure we have the proper config:

$ ldapsearch -x

**Take a screenshot and paste it in your lab report.**

Now let’s create some entries, a node for our users (People), a node for our groups (Groups), and a node for your project team (<your team name>). Create the following file: **csi3670\_content.ldif**

dn: ou=People,dc=csi3670,dc=local

objectClass: organizationalUnit

ou: People

dn: ou=Groups,dc=csi3670,dc=local

objectClass: organizationalUnit

ou: Groups

dn: cn=<teamname>,ou=Groups,dc=csi3670,dc=local

objectClass: posixGroup

cn: <teamname>

gidNumber: 5000

dn: uid=user1,ou=People,dc=csi3670,dc=local

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: shadowAccount

uid: user1

sn: 1

givenName: User

cn: User 1

displayName: User 1

uidNumber: 10000

gidNumber: 5000

userPassword: Temp12345

gecos: User 1

loginShell: /bin/bash

homeDirectory: /home/user1

**Note that the user id and group ids are quite high. Why would this be the case? (Q1)**

Add the file to your LDAP directory:

$ ldapadd -x -D cn=admin,dc=csi3670,dc=local -W -f csi3670\_content.ldif

Check to make sure that the data was appropriately added:

$ ldapsearch -x -b dc=csi3670,dc=local 'uid=user1'

**Take a screenshot of your output and paste it in your lab report. You should be seeing information about the user you created.**

**Run the following command. In Q2, describe what it does.**

$ ldapsearch -x -b dc=csi3670,dc=local subschemaSubentry

Now let’s install a web interface. It used to be phpLDAPAdmin, but that is horribly deprecated. Instead, we're going to install the LDAP Account Manager.

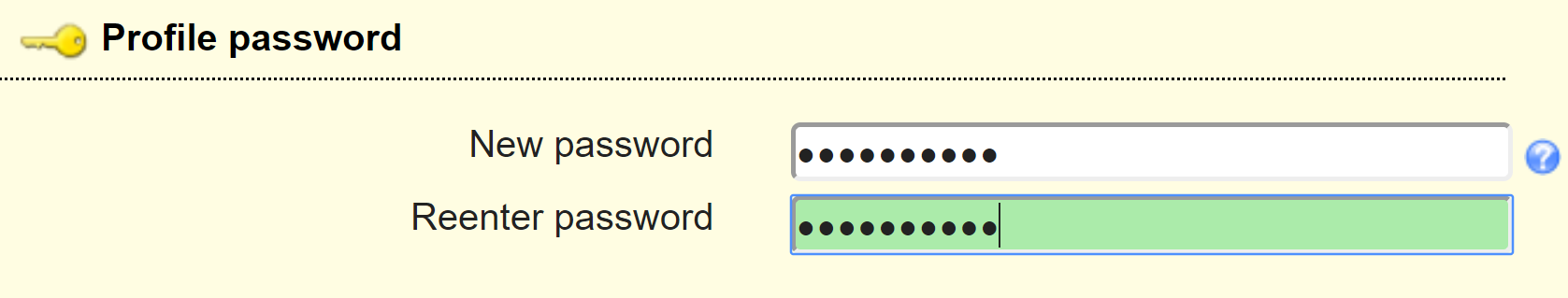
$ sudo apt install ldap-account-manager

That's actually pretty much it for installing! Go to your website: http://<YOUR GCP IP ADDRESS>/lam

Make sure that (1) you use lowercase L for lam, and (2) that it’s http, not https.

**Take a screenshot of LAM in your browser, with your IP address, and paste it into your lab report.**

You will have to setup your admin account. At the top right, click 'LAM configuration' and then 'Edit Server Profiles.' The default password is **lam**. Scroll to the bottom of the page and set a new default password … you don't want anybody breaking into your account!

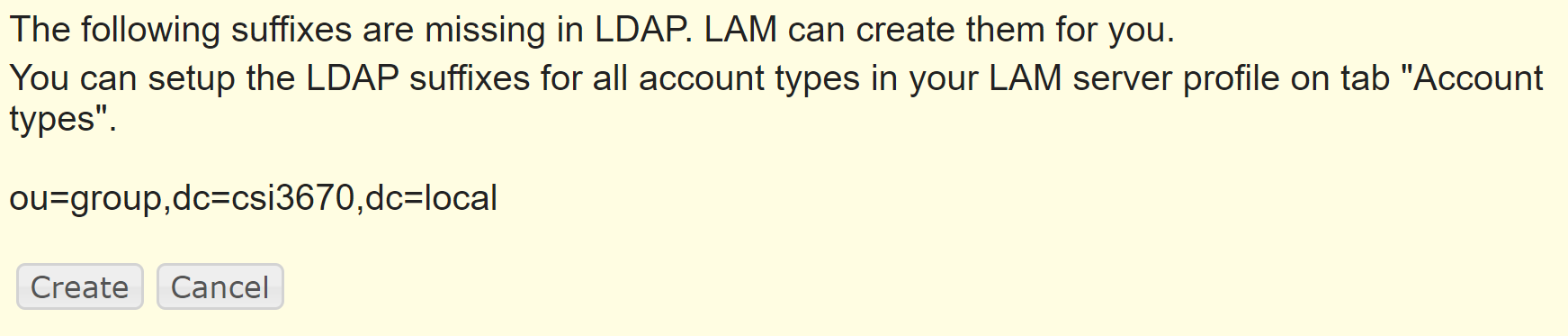


Under the Security Settings section, specify the LDAP admin account. Add cn=admin,dc=csi3670,dc=local to the list of valid users.

Then go to the Account types tab. Update the Users and Groups LDAP suffix to match our domain (dc=csi3670,dc=local)

You can login with your admin credentials (admin should be prepopulated in the login drop down). Login with your LDAP administrator password you setup on the command line (default is temp12345).

You may see something like this. You can click 'Create' and LAM will configure your missing setting(s) for you.



**Create a new user account (in addition to user1 that should already be there) using the web interface. Make sure to navigate to the Unix section (to the left) after filling in the Personal section. Click Save at the top left and navigate back to user list. Take a screenshot of your webpage after you’ve done so and paste it in your lab report (note, there should be 2 users in your screenshot at this point!).**

**2) Bash fun with LDAP!**

Now that we’ve successfully installed LDAP on our Ubuntu VM and used a web interface to add a new user, we’re going to see how we can do this from the command line.

Create a bash script. Call it sample\_user\_add.sh. Copy the following lines and paste it in your editor:

#!/bin/bash

users=( "tempuser1" "tempuser2" "tempuser3" )

userpw="temp12345"

ldif\_file="/tmp/bulk\_user.ldif"

dn="cn=admin,dc=csi3670,dc=local"

adminpw="temp12345" ### REPLACE THIS WITH YOUR ADMIN PASSWORD

i=0

for user in "${users[@]}"; do

touch $ldif\_file

uid=$(( $i + 1000 ))

gid=$(( $i + 1000 ))

echo $uid $gid

echo "Adding $user to LDAP directory with UID [$uid] and GID [$gid]"

echo "dn: uid=$user,ou=People,dc=csi3670,dc=local" >> $ldif\_file

echo "objectClass: inetOrgPerson" >> $ldif\_file

echo "objectClass: posixAccount" >> $ldif\_file

echo "objectClass: shadowAccount" >> $ldif\_file

echo "uid: $user" >> $ldif\_file

echo "sn: 1" >> $ldif\_file

echo "givenName: User" >> $ldif\_file

echo "cn: User $i" >> $ldif\_file

echo "displayName: User $i" >> $ldif\_file

echo "uidNumber: $uid" >> $ldif\_file

echo "gidNumber: $gid" >> $ldif\_file

echo "userPassword: $userpw" >> $ldif\_file

echo "gecos: User $i" >> $ldif\_file

echo "loginShell: /bin/bash" >> $ldif\_file

echo "homeDirectory: /home/$user" >> $ldif\_file

cat $ldif\_file

# Add user

ldapadd -x -D $dn -w $adminpw -a -f $ldif\_file

# Clean up

rm $ldif\_file

i=$(( $i + 1 ))

done

Run it with bash (don’t run it with sh):

$ sudo bash sample\_user\_add.sh

**Take a screenshot of the output and paste it in your lab report.**

**Go back to LAM and refresh your userlist. Take a screenshot showing that tempuser1,tempuser2, and tempuser3 now exist. Paste into your lab report.**

**Lab report (100 points)**

Note that you are allowed to use online sources, as long as you (1) cite your source (no formal formatting required, just copy and paste the website address), and (2) rephrase in your own words.

1. (10 points) Note that the user id and group ids are quite high. Why would this be the case?
2. (10 points) [From lab] (ldapsearch + subSchemaEntry). Describe what the subSchemaEntry is doing to our ldapsearch
3. (10 points) What is LDAP and how does it compare to Active Directory? (you may reuse your exam answer)
4. (10 points) What’s the difference between a DC and an OU in LDAP? What is their purpose?
5. (10 points) What is a Distinguished Name? (you may reuse your exam answer)
6. (20 points) Assume we are running an LDAP server for the class. What changes would need to be made to each *client machine* in order for them to authenticate with the LDAP server over a local login? You don’t need to provide exact details, but describe the technologies needed. This will require Googling, FYI.
7. (10 points extra credit) Modify the script above to create a new user from the command line. Copy the old script and rename your new script to be user\_add.sh. It should accept a single user and password combination as follows (so, no need to loop anymore):

$ sudo bash user\_add.sh username password

Run this and demonstrate that the user has been successfully added (either via LAM or an ldapsearch query).

1. (30 points total, 5 per screenshot) Ensure you’ve taken all six required screenshots and put them at the end of this document.

1. Zip up this report, your script(s) and any other materials and submit to Moodle. You may copy/paste your script inside this Word document as well, just make sure that it copies correctly to avoid losing bonus points.