Lab 9 Assignment

Lightweight Directory Access Protocol

Harsh Tomar
B21AI049

Question 1

Part a)

What is LDAP, and what is its primary purpose in the context of computer networks and directory services?

Directory information is made available through Web interfaces, as many organizations and phone companies do. Such interfaces are understandable for humans. However, computer programs too need to access directory information.
Directories can be used for storing other types of information, much life `file system directories`. For instance, Web browsers can store personal bookmarks and other browser settings in a directory system. (Example from Korth). A user can thus access the same settings from multiple locations, such as home and at work, without having to share a file system.

LDAP stands for Lightweight Directory Access Protocol. It is a protocol used to access and manage directory information over a `network`.
In LDAP, directories store entries, which are similar to objects. Each entry must have a distinguished name (DN), which uniquely identifies the entry. A DN is in turn made up of a sequence of `relative distinguished names (RDN's)`.

Directory Services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services and applications throughout the network.

The primary purpose of LDAP is to provide a means for accessing and managing directory information in a distributed and hierarchical manner. It allows clients to query and update information in a directory, which could include user accounts, network devices, services, and more.

LDAP is commonly used for authentication, authorization, and directory-related services in various network environments.

- Standardized protocol for accessing ad managing directory information in Computer Networks
- Central Repo for storing and organizing user data, authentication, authorization and efficient retrieval of information through the hierarchical directory structure (as a service).

Part b)

Explain the key components of an LDAP directory entry. Provide examples of attributes commonly found in LDAP entries.
An LDAP Directory Entry is a record or (set of information) in the DIT that represents an object or entity such as a

user, group or device. Each entry has a **Distinguished Name (DN)** and further attributes (cn, sn, givenName, etc.) that identifies it's position in the DIT. ObjectClass also helps define the type of the Entry and specifies attributes that represent the entry.

Commonly Found Attributes are

- **ObjectClass, dc, o, ou, cn, sn, givenName, mail, uniqueMember, etc**

example:

- objectClass: person
- cn : bob
- sn : conway
- mail : bob@example.com

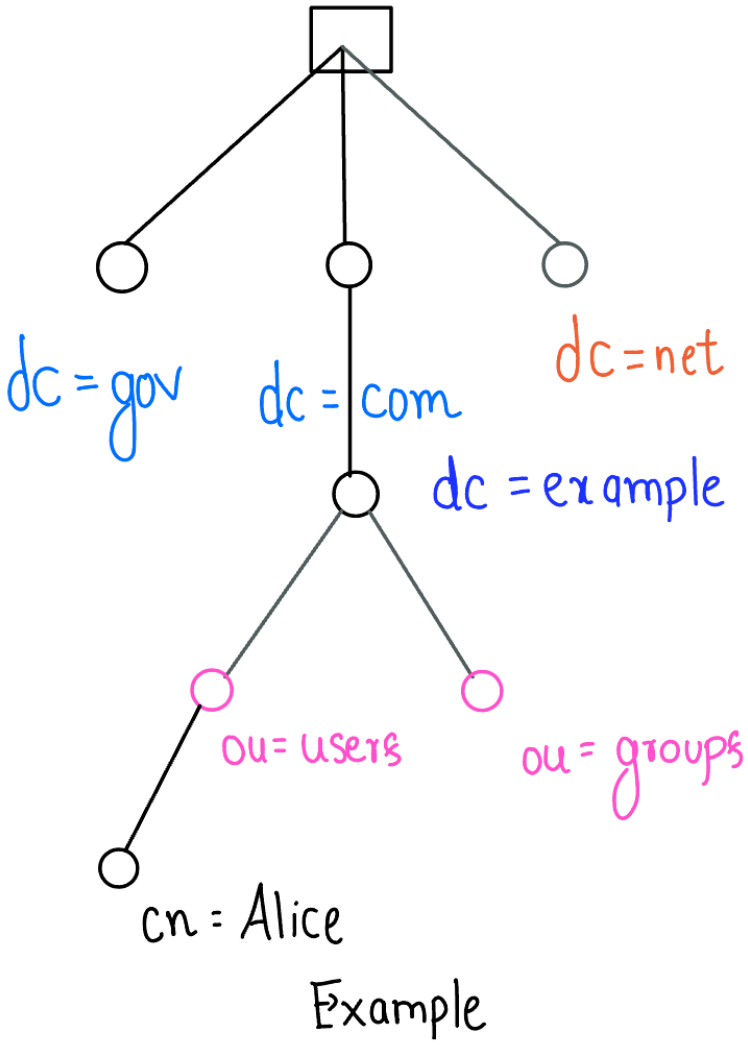
Part c)

Describe the LDAP directory tree structure and its significance in organizing directory information. Use a simple diagram to illustrate a directory tree.

Structure organizes directory information in a Hierarchical Fashion -> DIT.

- Entries in the tree are objects like users/groups / locations, etc (Components like DN, OU, etc.)

The Hierarchical Structure helps in organizing directory information in such a way that aids use cases such as **User Management**, **Geographical Organization**, and **Device Organizations**.



Part d)

In the context of LDAP, what is LDIF (LDAP Data Interchange Format), and how is it used for data import/export operations? Provide a sample LDIF entry for adding a user to an LDAP directory.

LDIF (LDAP Data Interchange Format) is a inter-exchange format that is designed to represent LDAP directory entries and modifications. It provides a simple and human-readable way to describe LDAP data.

It is used for data import / export operations

- We can create a `.ldif` file and use it to import (Add / Modify / Drop Entries)
- and Export (an `ldif` file representing the directory's entries and attributes)

These actions are used to migrate, backup / restore and bulk loading of data.

An example of an LDIF entry for adding a user to an LDAP directory is

```
# alice.ldif

dn: uid=alice,ou=users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: alice
cn: Alice
sn: Doe
givenName: Alice
mail: alice@example.com
userPassword: aliceisthebest
```

Question 2

Answer the following:

LDAP User Account Creation

Part a)

You need to create a new user account in an LDAP directory for a user named "Alice." The user should belong to the "ou=users,dc=example,dc=com" organizational unit (OU). Explain the steps and LDAP commands you would use to accomplish this task.

First we download and install the Apache Directory Studio and slapd services
To download Apache DS 2.0

```
wget https://dlcdn.apache.org/directory/studio/2.0.0.v20210717-M17/ApacheDirectoryStudio-
2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz

cd ApacheDirectoryStudio
./ApacheDirectoryStudio
```

`sudo apt install slapd ldap-utils`
`sudo dpkt-reconfigure slapd`
and we enter Admin details for our directory.

Steps for Method 1 (Using slapd service)

1. Check if slapd service is running

```
sudo systemctl status slapd
```

2. Create the `.ldif` file to add `ou : users` to the Directory

```
# users_ou.ldif

dn: ou=users,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: users
```

3. Add the entry using the command :

```
ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f users_ou.ldif
```

4. Create `alice.ldif` file and add to the Directory

```
# alice.ldif

dn: uid=alice,ou=users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: alice
cn: Alice
sn: Doe
givenName: Alice
mail: alice@example.com
userPassword: {SSHA}hashed_password
```

```
ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f alice.ldif
```

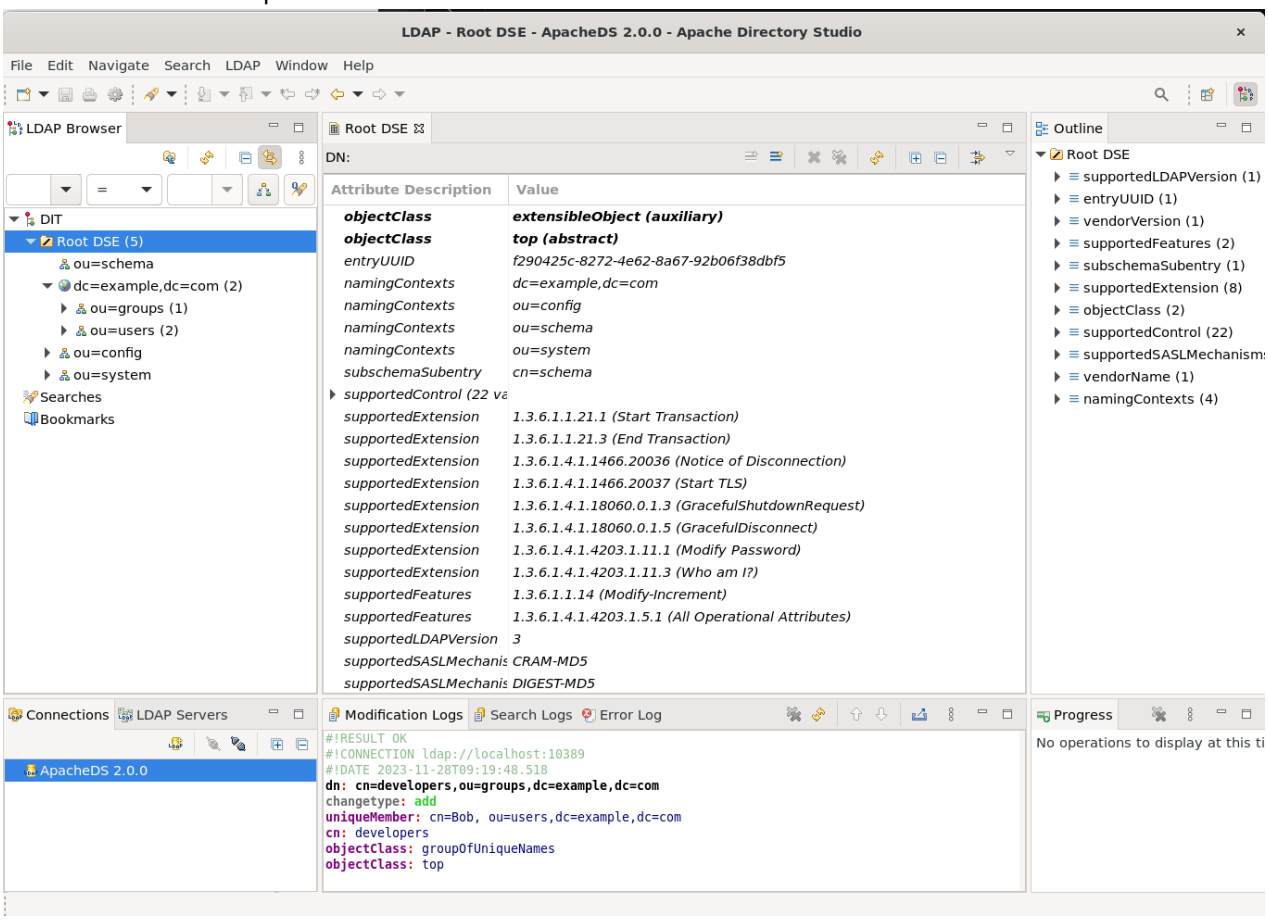
5. Verify the Entries using `ldapsearch -x -b "ou=users,dc=example,dc=com" -D "cn=admin,dc=example,dc=com" -W`

Output

```
hush@LAPTOP-G6QAR288  ~ 〉 de2 〉 Data-Engineering-Lab-Assignments 〉 Lab_9 ⎇master ≡ +0 ~0 -0  code
hush@LAPTOP-G6QAR288  ~ 〉 de2 〉 Data-Engineering-Lab-Assignments 〉 Lab_9 ⎇master ≡ +0 ~0 -0  ldapsearch -x -b "ou=users,dc=example,dc=com" -D "cn=admin,dc=example,dc=com" -W
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <ou=users,dc=example,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# users, example.com
dn: ou=users,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: users

# bob, users, example.com
dn: uid=bob,ou=users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: bob
cn: Bob
sn: Smith
givenName: Bob
mail: bob@example.com
userPassword:: Ym9iaXN0aGViZXN0

# alice, users, example.com
dn: uid=alice,ou=users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: alice
cn: Alice
sn: Doe
givenName: Alice
mail: alice@example.com
userPassword:: YWxpY2Vpc3RoZWJlc3Q=

# search result
search: 2
result: 0 Success

# numResponses: 4
# numEntries: 3
hush@LAPTOP-G6QAR288  ~ 〉 de2 〉 Data-Engineering-Lab-Assignments 〉 Lab_9 ⎇master ≡ +0 ~0 -0
```

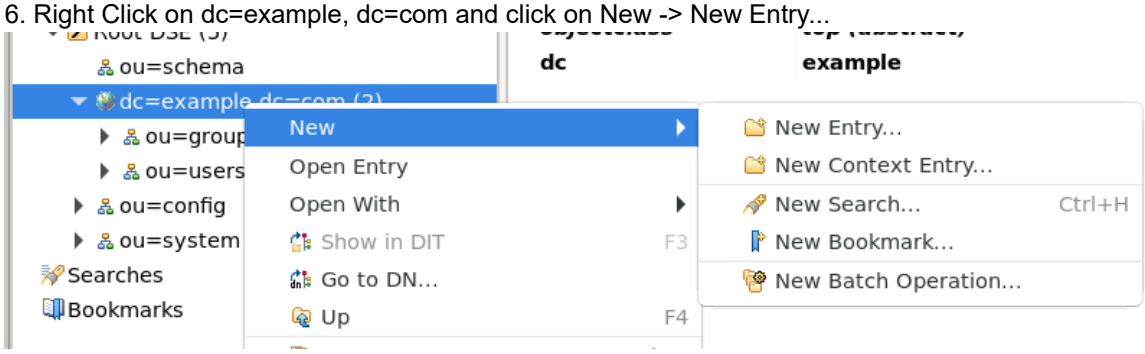
Steps for Method 2 (Using Apache Directory Studio)

1. Open the ApacheDirectoryStudio `./ApacheDirectoryStudio`
2. Start the Server `Aoache DS 2.0.0` and after starting, right click on it and `create connection`.
3. Click on the Connection Tab and select the ApacheDS 2.0.0 Connection
4. On the LDAP Browser Section click on DIT and expand the DropDown options
5. Select the Root DSE option

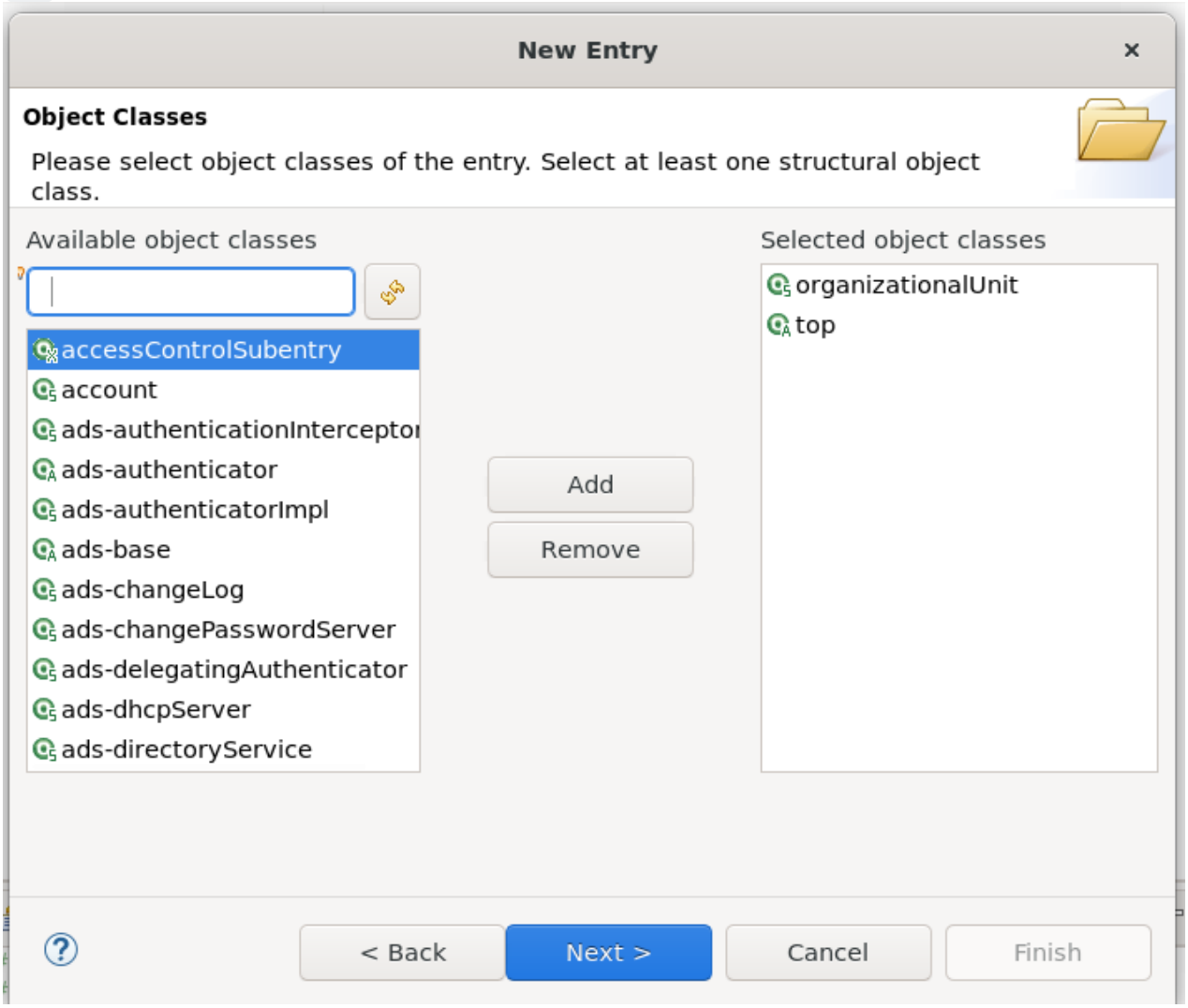


Now,

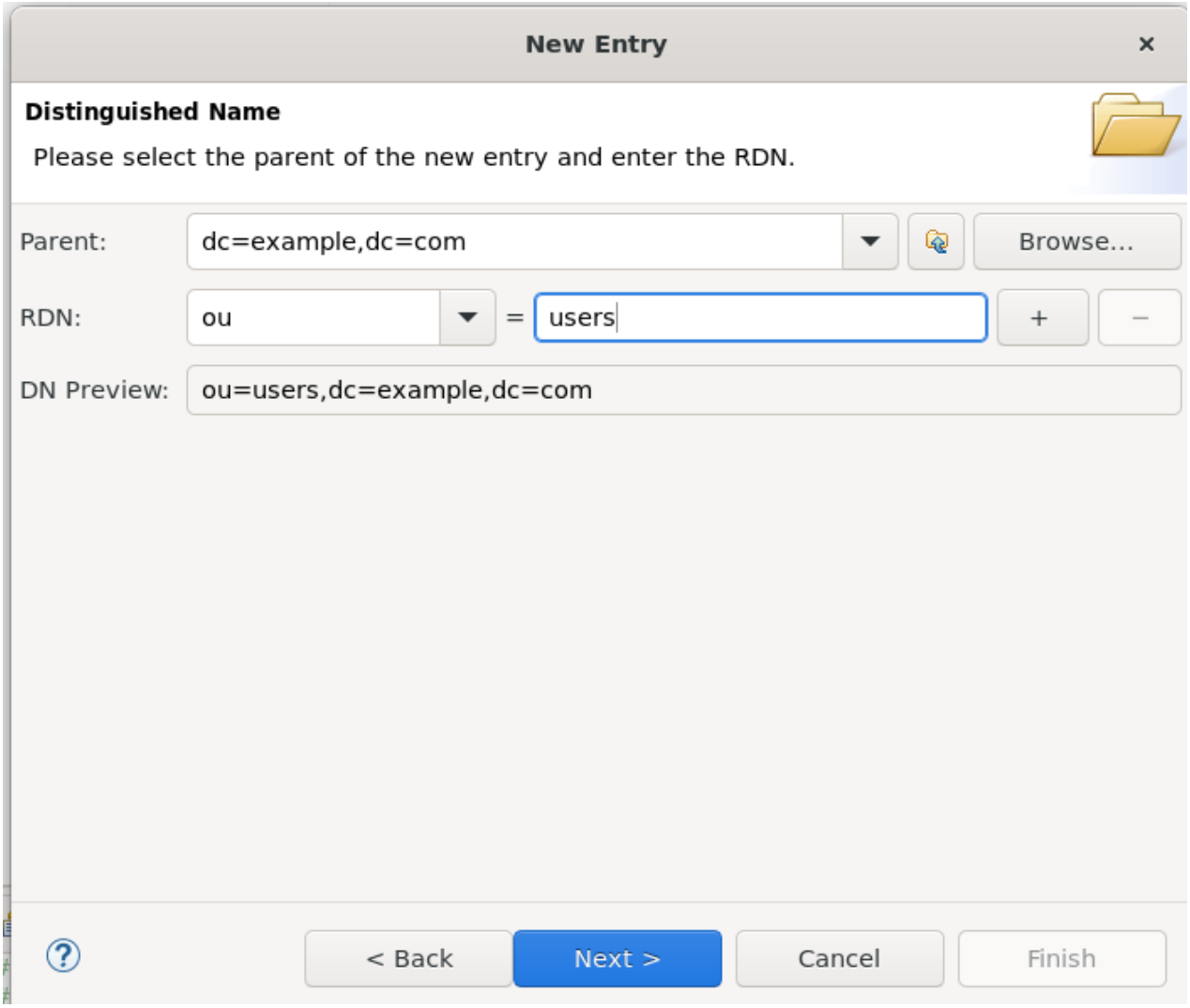
6. Right Click on dc=example, dc=com and click on New -> New Entry...



7. Select `Create Entry from Scratch` and Next > Select the Object Class "organizationalUnit" and click on `Add` and then click on Next



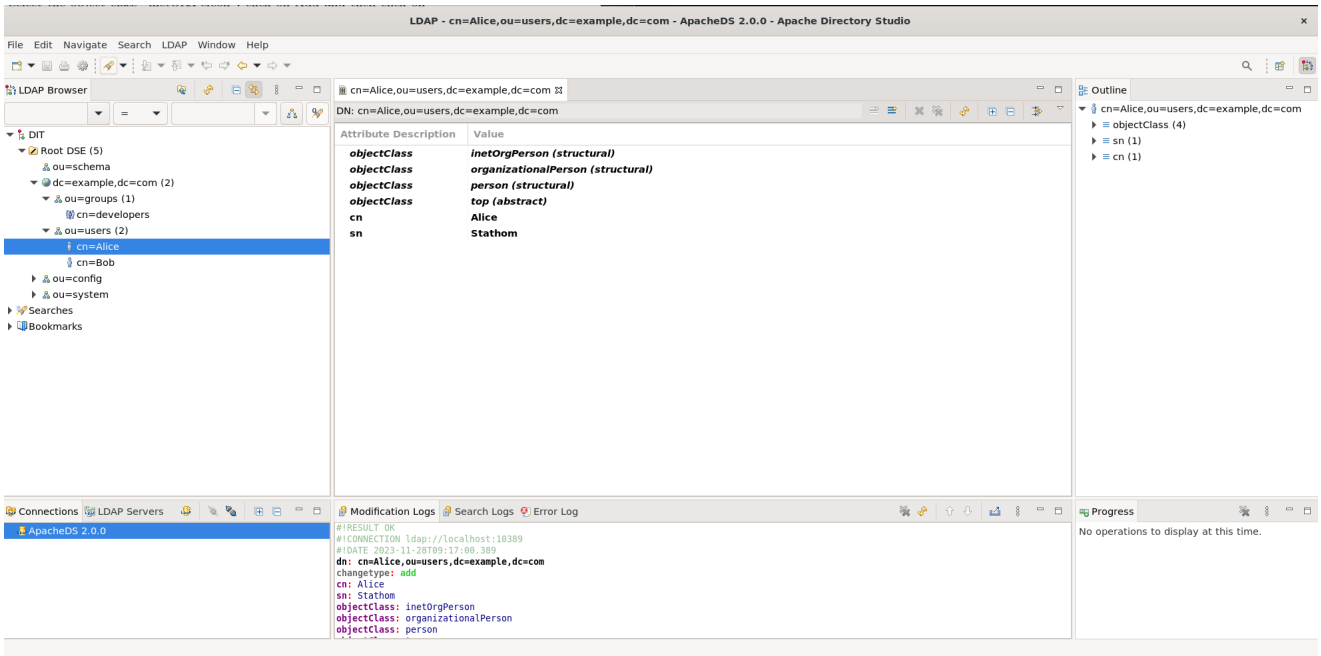
8. In the RDN section, type ou = users and click on Next >



9. Now we Click on Finish

Repeating the same but for Object Class = `inetOrgPerson` and in the RDN Section we choose `cn = Alice` when asked for `sn` we can put the sir_name as `stathom` and then we finish.

Final Screen would look something like



Part b)

LDAP Group Membership
You are tasked with adding a user named "Bob" to an LDAP group named "developers." The group "developers" is located under the "ou=groups,dc=example,dc=com" OU. Provide a step-by-step guide on how to add the user "Bob" to the "developers" group.

Steps for Method 1 (Using slapd service)

1. Check if slapd service is running

```
sudo systemctl status slapd
```

2. `.ldif file for Bob`

```
# bob_user.ldif

dn: uid=bob,ou=users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: bob
cn: Bob
sn: Smith
givenName: Bob
mail: bob@example.com
userPassword: bobisthebest
```

```
ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f bob_user.ldif
```

3. We create LDIF for "developers" group and "ou = groups":

```
# developers_group_with_ou.ldif

dn: ou=groups,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: groups

dn: cn=developers,ou=groups,dc=example,dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: developers
uniqueMember: uid=bob,ou=users,dc=example,dc=com
```

```
ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f developers_group_with_ou.ldif
```

4. Verify

```
ldapsearch -x -b "ou=groups,dc=example,dc=com" -D "cn=admin,dc=example,dc=com" -W
```

```
ps,dc=example,dc=com" -D "cn=admin,dc=example,dc=com" -W
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <ou=groups,dc=example,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# groups, example.com
dn: ou=groups,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: groups

# developers, groups, example.com
dn: cn=developers,ou=groups,dc=example,dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: developers
uniqueMember: uid=bob,ou=users,dc=example,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
hush@LAPTOP-G6QAR288 ~ > de2 > Data-Engineering-Lab-Assignments > Lab_9 master ≡ +0 ~0 -0
```

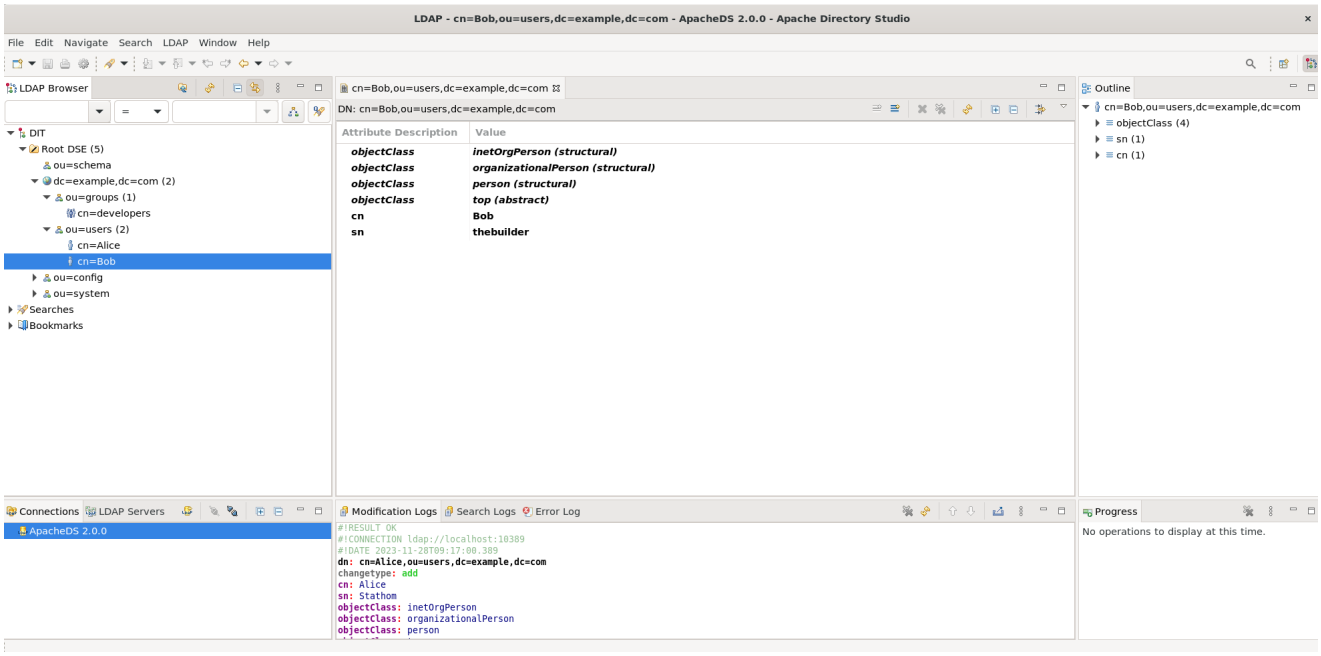
5. Final Directory Structure

```
hush@LAPTOP-G6QAR288 ~ > de2 > Data-Engineering-Lab-Assignments > Lab_9 master ≡ +0 ~0 -0 ldapsearch -x -b "ou=users,dc=example,dc=com" -s sub -D "cn=admin,dc=example,dc=com" -W
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <ou=users,dc=example,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# users, example.com
dn: ou=users,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: users

# bob, users, example.com
dn: uid=bob,ou=users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: bob
cn: Bob
sn: Smith
givenName: Bob
mail: bob@example.com
userPassword:: Ym9iaXN0aGViZXN0

# alice, users, example.com
dn: uid=alice,ou=users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: alice
cn: Alice
sn: Doe
givenName: Alice
mail: alice@example.com
userPassword:: YWxpY2Vpc3RoZWJlc3Q=

# search result
search: 2
result: 0 Success

# numResponses: 4
# numEntries: 3
hush@LAPTOP-G6QAR288 ~ > de2 > Data-Engineering-Lab-Assignments > Lab_9 master ≡ +0 ~0 -0
```

Steps for Method 2 (Using Apache Directory Studio)

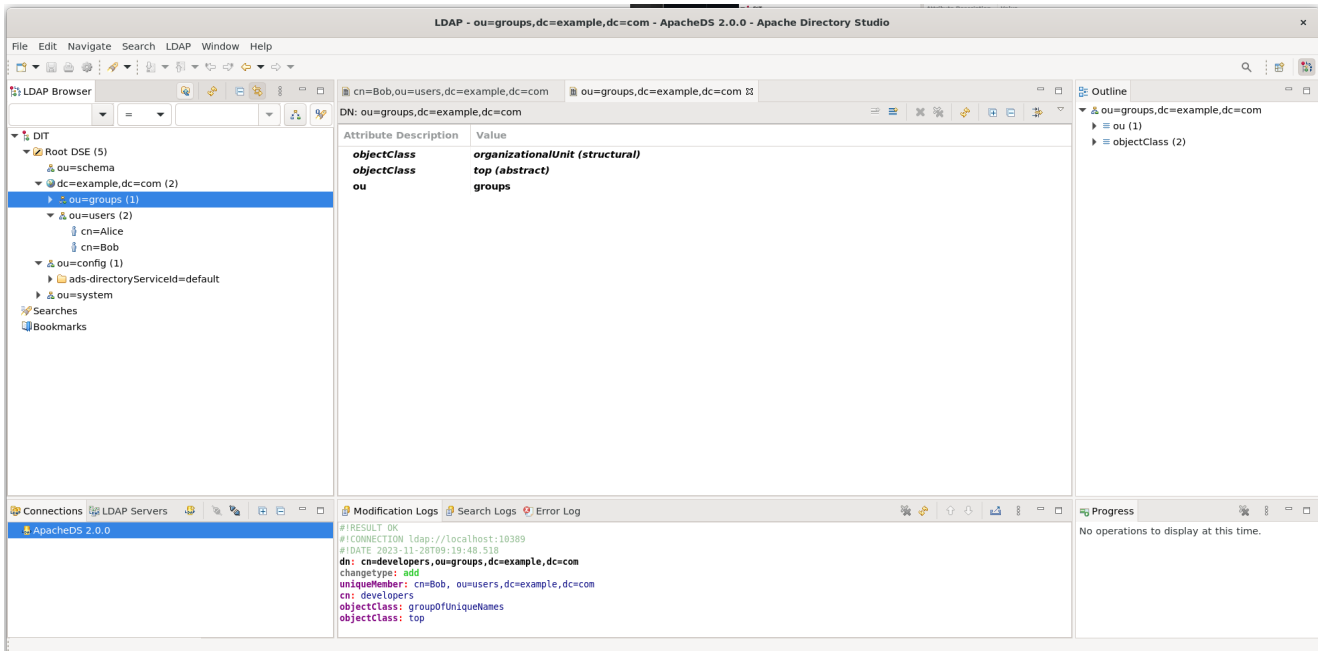
1. We repeat the initial steps in Part (a) to add Bob as a user
2. Root DSE -> `ou=users` -> New -> New Entry
3. `Create entry from scratch` -> Next >
4. objectClass = inetOrgPerson and click on `Add` and then Next >

5. Enter `RDN: cn = Bob` and click on Next
   When asked for `sn` we can enter `thebuilder`.
   Click on Finish



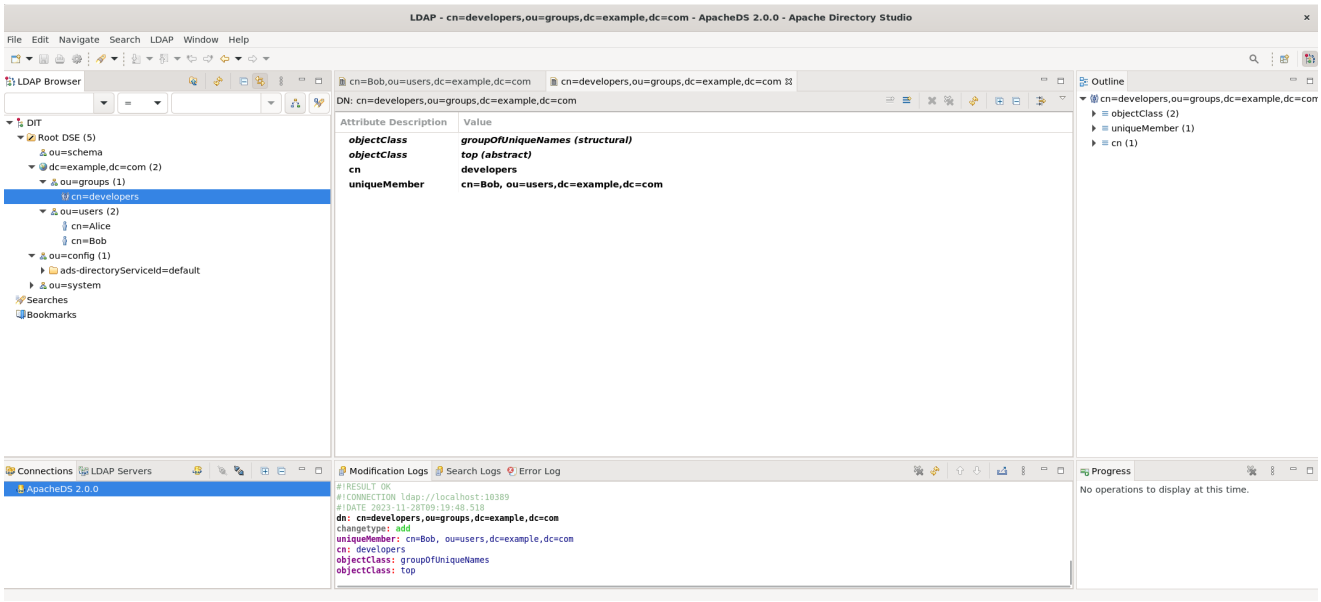
Now we add the organizationUnit of groups

6. Right Clicking `dc=example, dc=com` -> Click on New -> New Entry
7. `Create entry from Scratch` -> Next
8. Select objectClass = `organizationUnit` -> Add -> Next
9. under the RDN `ou=groups` -> Next
10. Finish



11. Right Clicking `ou = groups` -> Click on New -> New Entry
12. `Create entry from Scratch` -> Next
13. Select objectClass = `groupOfUniqueNames` -> Add -> Next
14. under the RDN `cn=developers` -> Next
15. And then we Add `cn = Bob, ou=users, dc=example, dc=com` value to the `uniqueMember` attribute
16. We click on Finish

Output



ThankYou 😊