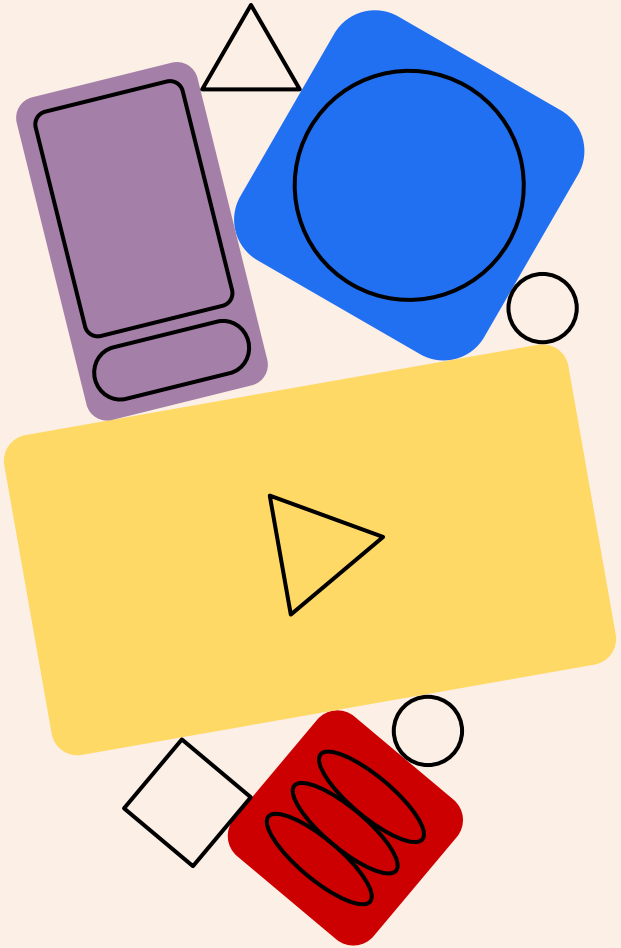
LAB 9: LDAP

NASA 1! 2025/04/21



Introduction

Directory service

- A directory is a specialized database designed for searching and browsing

LDAP

- Lightweight Directory Access Protocol
- a lightweight protocol for accessing directory service

Introduction

OpenLDAP

- Open-source implementation of LDAP
- Non-relational database management system

slapd

- Standalone LDAP Daemon
- An LDAP server process in OpenLDAP
- Make OpenLDAP be powerful

Introduction

In NTU CSIE

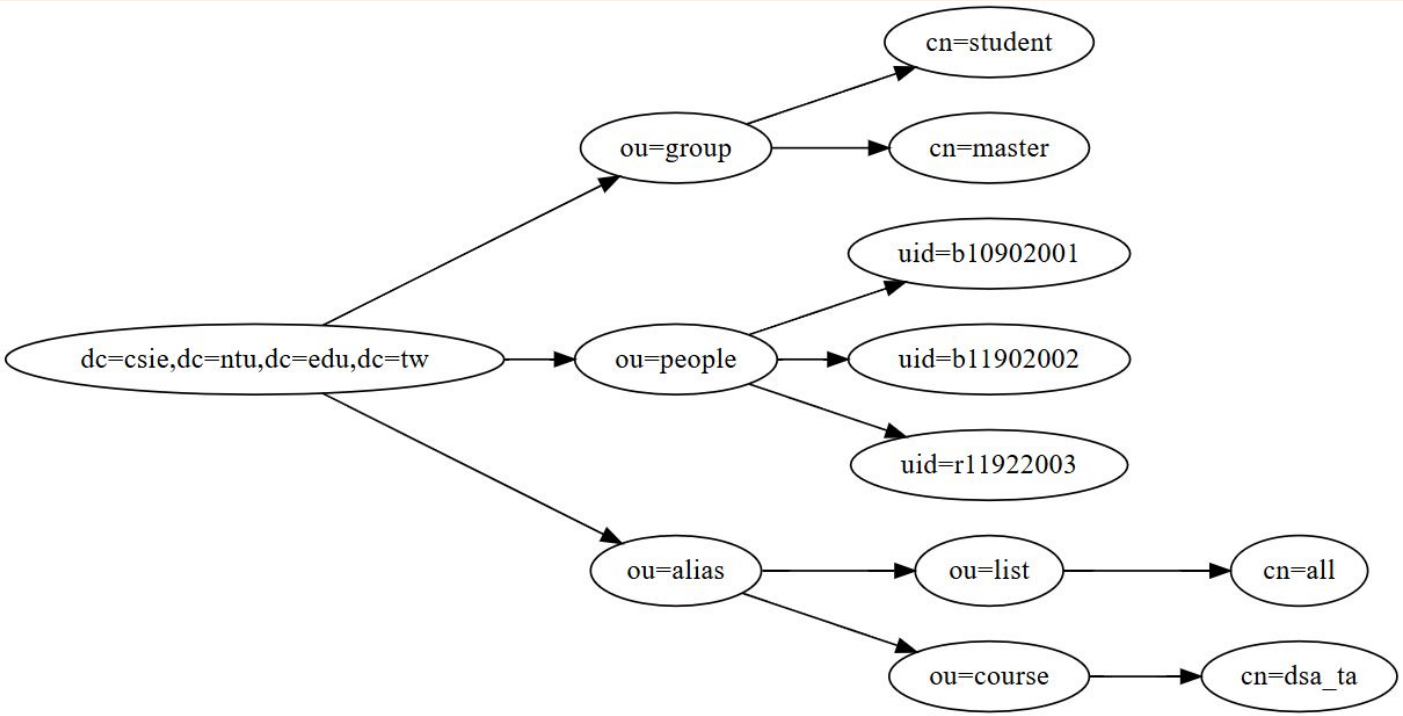
- Used to manage user accounts and mail aliases
- CSIE Wi-Fi, SMTP, Printing, Workstation, …
  all use LDAP to authenticate users
- SMTP uses LDAP to resolve aliases
  (e.g. vegetable@csie, all@csie)
- Workstations use LDAP to configure user accounts

LDAP

- Information is based on ***entry***, a collection of attributes that has unique **DN (Distinguished Name)**
- Each of the entry's **attributes** has
  - ***type***
    - *"cn"* for common name, "*mail*" for email address
  - ***value***
    - attribute *"mail"* might contain value "vegetable@csie"
- Special attribute ***"objectClass"***
  - Determine the schema rules the entry must obey
  - Also form a tree hierarchy – they can be inherited

LDAP

Entries are in hierarchical tree-like structure



LDAP Example

Use ldapsearch -x "uid=`whoami`" on workstations:

```
b11902167@ws1 [~] ldapsearch -x "uid=`whoami`"
# extended LDIF
#
# LDAPv3
# base <dc=csie,dc=ntu,dc=edu,dc=tw> (default) with scope subtree
# filter: uid=b11902167
# requesting: ALL
#

# b11902167, people, csie.ntu.edu.tw
dn: uid=b11902167,ou=people,dc=csie,dc=ntu,dc=edu,dc=tw
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
objectClass: shadowAccount
objectClass: sambaSamAccount
objectClass: GAppUser
objectClass: csieEsystem
objectClass: posixAccount
objectClass: csieAccount
uid: b11902167
cn: b11902167
givenName:: 5paH6ae/
sn:: 6ZCY
mail: b11902167@ntu.edu.tw
uidNumber: 71091
gidNumber: 450
loginShell: /bin/bash
loginShellFreeBSD: /usr/local/bin/bash
homeDirectory: /home/student/11/b11902167
```

LDIF

- LDAP Data Interchange Format
- Text-based format used to represent LDAP contents and update requests
- Update requests can be add, delete, modify…
- LDIF (.ldif) can be consumed by *ldapadd*, *ldapmodify* …

VM Installation

```
# Download qcow2 file (Debian GNU/Linux 12)
    cp /tmp2/lab9/Debian.qcow2 .

# Start the VM, replace <port> to a digit
    qemu-system-x86_64 -enable-kvm -cpu host -m 8G \
        -drive file=Debian.qcow2,format=qcow2 \
        -monitor stdio \
        -nic user,hostfwd=tcp::<port>-:22 \
        -vnc :0

# SSH to VM in a new terminal
    ssh -p <port> root@localhost
# Then, login as root with password nasa2025
Please modify the password immediately, or you may
be hacked by others!!!
```

OpenLDAP Installation

```
# Install OpenLDAP and Utilities
   apt install -y slapd ldap-utils

# Install ldapvi (Optional, LDAP editor)
   apt install ldapvi
```

Configure Database

- Configure LDAP DC Suffix

```
# suffix.ldif
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=nasa,dc=csie,dc=ntu
```

- Apply modification

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f suffix.ldif
```

- What is “`-Y EXTERNAL -H ldapi:///`”? See this

Configure Database

- Configure LDAP Root DN

```
# rootdn.ldif
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=nasa,dc=csie,dc=ntu
```

- Apply modification

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f rootdn.ldif
```

Configure Database

- Configure LDAP Base Records

```
# base.ldif
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

dn: cn=admin,dc=nasa,dc=csie,dc=ntu
cn: admin
objectClass: organizationalRole
description: admin account

dn: ou=people,dc=nasa,dc=csie,dc=ntu
ou: people
objectClass: organizationalUnit

dn: ou=group,dc=nasa,dc=csie,dc=ntu
ou: group
objectClass: organizationalUnit
```

Configure Database

- Apply modification

```
ldapadd -D cn=admin,dc=nasa,dc=csie,dc=ntu -W
-H ldapi:/// -f base.ldif
```

- `ldapadd`: `ldapmodify` for adding new entry (hence `changetype` is omitted)
- `-D`: Tell server who you are
- `-H`: Use prompt for password

LDAP LAB - Add User

1. Hash the password

   ```
   slappasswd
   ```

   copy the hash result for the next step

LDAP LAB - Add User

2. Change the cn, uid, and homeDirectory according to your student ID

```
#user.ldif
dn: uid=<b13902000>,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: <b13902000>
uid: <b13902000>
uidNumber: 1234
gidNumber: 123
homeDirectory: /home/<b13902000>
loginShell: /bin/bash
userPassword: <password hash>
```

LDAP LAB - Add User

3. Add this user to the server

```
ldapadd -D cn=admin,dc=nasa,dc=csie,dc=ntu -W
-H ldapi:/// -f user.ldif
```

LDAP LAB - Add User

4. Search user

```
ldapsearch -x -b dc=nasa,dc=csie,dc=ntu cn=<b13902000>
```

5. Edit /etc/ldap/ldap.conf to make this works:

```
ldapsearch -x cn=<b13902000>
```

6. Take screenshot of the above command

Submission form

Your submission should include:

- Command “`ldapsearch -x cn=<b13902000>`”
- Result of the command
- You should replace `<b13902000>` with your student ID
- Submission Form

Submission form

Example:

```
root@nasa2025:~# ldapsearch -x cn=b11902167
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> (default) with scope subtree
# filter: cn=b11902167
# requesting: ALL
#

# b11902167, people, nasa.csie.ntu
dn: uid=b11902167,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: b11902167
uid: b11902167
uidNumber: 1234
gidNumber: 123
homeDirectory: /home/b11902167
loginShell: /bin/bash
```

Reference

- OpenLDAP
- Arch Wiki