

NASA HW8 - 金哲安(B12902118)

前置作業

References

- B12902116 (林靖昀)
- B12902066 (宋和峻)
- https://docs.google.com/presentation/d/1QOBSuBnh2F55daXRpcfpHbN-fNiUS3Hz2edsyFqzFQQ/edit#slide=id.g32f3cf8fa06_0_0
- <https://www.youtube.com/watch?v=WSx7-odbd4Y>

1

ssh into Debian

```
ssh -p [port] root@localhost
```

Install OpenLDAP and Utilities and editor

```
apt update  
apt install slapd ldap-utils ldapvi
```

Generate a password hash

```
slappasswd
```

Basic Configuration

```
# basic.ldif
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=nasa,dc=csie,dc=ntu
-
replace: olcRootDN
olcRootDN: cn=admin,dc=nasa,dc=csie,dc=ntu
-
replace: olcRootPW
olcRootPW: {SSHA}8ABxAZ+qNUCbs5pVUmSJMEoYtjBZQQ/J
```

Apply modification

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

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
```

Apply modification

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

Search

```
ldapsearch -x -b dc=nasa,dc=csie,dc=ntu
```

The screenshot shows a terminal window titled "anthony" with the command "ldapsearch -x -b dc=nasa,dc=csie,dc=ntu". The output of the command is displayed in two panes:

```
# numResponses: 1
root@Debian:~# vim base.ldif
root@Debian:~# ldapadd -D cn=admin,dc=nasa,dc=csie,dc=ntu -W -H ldapi:/// -f base.ldif
Enter LDAP Password:
Arch SSH port: 41846, VNC port: 43505
QEMU 9.2.2 monitor - type 'help' for more information
(qemu)

# bash: -H: command not found
root@Debian:~# ldapadd -D cn=admin,dc=nasa,dc=csie,dc=ntu -W -H ldapi:/// -f base.ldif
Enter LDAP Password:
adding new entry "dc=nasa,dc=csie,dc=ntu"
adding new entry "cn=admin,dc=nasa,dc=csie,dc=ntu"
adding new entry "ou=people,dc=nasa,dc=csie,dc=ntu"
adding new entry "ou=group,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# ldapsearch -x -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

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

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

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

# search result
search: 2
result: 0 Success
# numResponses: 5
# numEntries: 4
root@Debian:~#
```

The right pane shows the QEMU monitor interface with Arch SSH port 41846 and VNC port 43505.

2

Lookup the ip on Debian:

```
ip a
```

There is

192.168.163.97

ssh into Arch

```
ssh -p [port] root@localhost
```

Install LDAP tools

```
pacman -Syu
pacman -Syu openldap
```

Search

```
ldapsearch -x -H ldap://192.168.163.97 -b dc=nasa,dc=csie,dc=ntu
```

```
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
    altname enp8s3
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic ens3
        valid_lft 59912sec preferred_lft 59912sec
    inet6 fe80::5054:fff:fe12:3456/64 scope site dynamic mngtmpaddr
        valid_lft 85975sec preferred_lft 13975sec
    inet6 fe80::5054:fff:fe12:3456/64 scope link
        valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:90:21:18:01 brd ff:ff:ff:ff:ff:ff
    altname enp8s4
    inet 192.168.163.97/16 brd 192.168.255.255 scope global dynamic ens4
        valid_lft 3495sec preferred_lft 3495sec
    inet6 fe80::5054:90ff:fe21:1801/64 scope link
        valid_lft forever preferred_lft forever
root@Debian:~# 

[root@Arch ~]# ldapsearch -x -H ldap://192.168.163.97 -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# nasa.csie.ntu

dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

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

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

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

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
[root@Arch ~]# 
[qemu_vnc10:ssh]

```

Task

References

- B12902116 (林靖昀)
 - B12902066 (宋和峻)
 - <https://www.openldap.org/doc/admin26/OpenLDAP-Admin-Guide.pdf>
 - https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
 - <https://www.youtube.com/watch?v=SK8Yw-CiRHk>
 - <https://www.youtube.com/watch?v=Xjpi8xYqPcY&t=97s>
 - <https://www.youtube.com/watch?v=lp5z8HQGAH8>
 - https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/system-level_authentication_guide/configuring_services#Configuring_Services
 - https://wiki.archlinux.org/title/LDAP_authentication#Online_and_offline_authentication_with_SS SD
 - https://drive.google.com/file/d/12kJLmHz_yVKKd1fn_edC9Bu2LNX3xFw7/view?usp=sharing

1

Create a certificate on Debian

```
mkdir /etc/ldap/ssl  
cd /etc/ldap/ssl  
openssl req -new -x509 -nodes -out ldapserver.crt -keyout ldapserver.key -days 365
```

Insert information during prompt:

- Common Name: Debian
- Others: Anything is fine

Set permissions

```
chmod 600 ldapserver.key  
chown openldap:openldap ldapserver.*
```

Tell slapd to use these certificates

```
# certs.ldif  
dn: cn=config  
changetype: modify  
add: olcTLSCertificateFile  
olcTLSCertificateFile: /etc/ldap/ssl/ldapserver.crt  
-  
add: olcTLSCertificateKeyFile  
olcTLSCertificateKeyFile: /etc/ldap/ssl/ldapserver.key
```

Apply modification

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

Modify `/etc/default/slapd` and replace `SLAPD_SERVICES` as

```
SLAPD_SERVICES="ldap:/// ldaps:/// ldapi:///"
```

Restart slapd

```
systemctl restart slapd
```

Allow self-signed certificates

```
echo "TLS_REQCERT allow" >> /etc/ldap/ldap.conf
```

Test

```
ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu
```

```
root@Debian:/etc/ldap# ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

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

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

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

# search result
search: 3
result: 0 Success

# numResponses: 5
# numEntries: 4
root@Debian:/etc/ldap# 

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

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

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
[root@Arch ~]# [qemu: vms]0:sshe#
```

```
ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu
```

```

root@Debian:/etc/ldap/ssl# ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (&(objectClass=*)(objectClass=top))
# requesting: ALL
#
# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

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

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

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

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
root@Debian:/etc/ldap/ssl# 

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

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

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
[root@Arch ~]#
[qemu_vms]0:ssh#
```

Debian SSH port: 39509, VNC port: 35454
QEMU 9.2.2 monitor - type 'help' for more information
(qemu)

Arch SSH port: 41846, VNC port: 43505
QEMU 9.2.2 monitor - type 'help' for more information
(qemu)

"b12902118@nasa-ws3:~/* 14:18 27-Apr-25

Limit connections to StartTLS/LDAPS

```
# tls.ldif
dn: cn=config
changetype: modify
add: olcLocalSSF
olcLocalSSF: 128
-
add: olcSecurity
olcSecurity: ssf=128
```

Apply modification

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

Restart slapd

```
systemctl restart slapd
```

On the client, also allow self-signed certificates

```
echo "TLS_REQCERT allow" >> /etc/openldap/ldap.conf
```

Test on client

```
ldapsearch -x -H ldaps://192.168.163.97 -b dc=nasa,dc=csie,dc=ntu
```

The screenshot shows a terminal window titled 'anthony' with the command 'ldapsearch -x -H ldaps://192.168.163.97 -b dc=nasa,dc=csie,dc=ntu'. The output is as follows:

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

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

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
root@debian:/etc/ldap/ssl# [root@Arch openldap]# ldapsearch -x -H ldaps://192.168.163.97 -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

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

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

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

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
[root@Arch openldap]# [qemu_vms]0:sshd# [root@Arch:/etc/openldap]# 15:40 27-Apr-25
```

2

On the server, use ldapadd to add two groups

```
# ta-group.ldif
dn: cn=ta,ou=group,dc=nasa,dc=csie,dc=ntu
objectClass: posixGroup
cn: ta
gidNumber: 2000
memberUid: tauser
```

```
# student-group.ldif
dn: cn=student,ou=group,dc=nasa,dc=csie,dc=ntu
objectClass: posixGroup
cn: student
gidNumber: 2001
memberUid: studentuser
```

Apply modifications

```
ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f ta-group.ldif
ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f student-group.ldif
```

Create two passwords for two users and copy them using slappasswd

```
slappasswd
```

Create two users

```
# user1.ldif
dn: uid=tauser,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: tauser
sn: User
givenName: TA
cn: TA User
displayName: TA User
uidNumber: 3000
gidNumber: 2000
homeDirectory: /home/tauser
loginShell: /bin/bash
userPassword: {SSHA}8ABxAZ+qNUCbs5pVUmSJMEoYtjBZQQ/J
```

```
# user2.ldif
dn: uid=studentuser,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: studentuser
sn: User
givenName: Student
cn: Student User
displayName: Student User
uidNumber: 3001
gidNumber: 2001
homeDirectory: /home/studentuser
loginShell: /bin/bash
userPassword: {SSHA}8ABxAZ+qNUCbs5pVUmSJMEoYtjBZQQ/J
```

Apply modifications

```
ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user1.ldif
ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user2.ldif
```

On the client, install SSSD

```
pacman -Syu sssd
```

Set up SSSD

```
# /etc/sssd/sssd.conf
[sssd]
config_file_version = 2
services = nss, pam
domains = LDAP

[domain/LDAP]
cache_credentials = true
enumerate = true

id_provider = ldap
auth_provider = ldap

ldap_uri = ldap://192.168.163.97
ldap_search_base = dc=nasa,dc=csie,dc=ntu
ldap_id_use_start_tls = true
ldap_tls_reqcert = allow
chpass_provider = ldap
ldap_chpass_uri = ldap://192.168.163.97
entry_cache_timeout = 600
ldap_network_timeout = 2

# OpenLDAP supports posixGroup, uncomment the following two lines
# to get group membership support (and comment the other conflicting parameters)
ldap_schema = rfc2307
ldap_group_member = memberUid

# Other LDAP servers may support this instead
# ldap_schema = rfc2307bis
# ldap_group_member = uniqueMember
```

Set permissions

```
chmod 600 /etc/sssd/sssd.conf
```

Edit `/etc/nsswitch.conf` as follows

```
# Begin /etc/nsswitch.conf
```

```
passwd: files sss
group: files sss
shadow: files sss
sudoers: files sss
```

```
publickey: files
```

```
hosts: files dns myhostname
networks: files
```

```
protocols: files
services: files
ethers: files
rpc: files
```

```
netgroup: files
```

```
# End /etc/nsswitch.conf
```

Edit `/etc/pam.d/system-auth` as follows

```
#%PAM-1.0
```

```
auth sufficient pam_sss.so forward_pass
auth required pam_unix.so try_first_pass nullok
auth optional pam_permit.so
auth required pam_env.so
```

```
account [default=bad success=ok user_unknown=ignore authinfo_unavail=ignore] pam_sss.so
account required pam_unix.so
account optional pam_permit.so
account required pam_time.so
```

```
password sufficient pam_sss.so
password required pam_unix.so try_first_pass nullok sha512 shadow
password optional pam_permit.so
```

```
session      required      pam_mkhomedir.so skel=/etc/skel/ umask=0077
session required pam_limits.so
session required pam_unix.so
session optional pam_sss.so
session optional pam_permit.so
```

Edit `/etc/pam.d/su` as follows

```
#%PAM-1.0
auth sufficient pam_rootok.so

auth sufficient pam_sss.so      forward_pass
auth required    pam_unix.so

account [default=bad success=ok user_unknown=ignore authinfo_unavail=ignore] pam_sss.so
account required    pam_unix.so

session required    pam_unix.so
session optional pam_sss.so
```

Install sudo

```
pacman -Syu sudo
```

Configure sudoers

```
# /etc/sudoers.d/ta-group
%ta  ALL=(ALL)  ALL
```

Start sssd

```
systemctl enable --now sssd
```

Test

```
ssh tauser@localhost
```

```

  ● ● ● anthony - b12902118@nasa-ws3:~/tmp2/nasa/HW8 - ssh - nws - 180x49
(1/1) checking keys in keyring [#####] 100% Arch SSH port: 27411, VNC port: 18208
(1/1) checking package integrity [#####] 100% QEMU 9.2.2 monitor - type 'help' for more information
(1/1) loading package files [#####] 100% (qemu)
(1/1) checking for file conflicts [#####] 100%
(1/1) checking available disk space [#####] 100%
:: Processing package changes... [#####] 100%
(1/1) installing sudo [#####] 100%
:: Running post-transaction hooks...
(1/3) Reloading system manager configuration...
(2/3) Creating temporary files...
(3/3) Arming ConditionNeedsUpdate...
[root@Arch ~]# vim /etc/sudoers.d/ta-group
[root@Arch ~]# systemctl enable --now sssd
Created symlink '/etc/systemd/system/multi-user.target.wants/sssd.service' → '/usr/lib/systemd/system/sssd.service'
.
[root@Arch ~]# ssh tauser@localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:z6eF2uaakhEQYXuSl+76ChICTBOUv0epU5bXRdywWc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
tauser@localhost's password:
Creating directory '/home/tauser'.
[tauser@Arch ~]$ 

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f ta-group.ldif
Enter LDAP Password:
adding new entry "cn=ta,ou=group,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f student-group.ldif
Enter LDAP Password:
adding new entry "cn=student,ou=group,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# slappasswd
New password:
Re-enter new password:
{SSHA}ZNTXUWyrdNsFHZH+Kw0zhnOII6lyuYF/
root@Debian:~# vim user1.ldif
root@Debian:~# vim user2.ldif
root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user1.ldif
Enter LDAP Password:
adding new entry "uid=tauser,ou=people,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user2.ldif
Enter LDAP Password:
adding new entry "uid=studentuser,ou=people,dc=nasa,dc=csie,dc=ntu"

root@Debian:~#
[qemu_vms]0:ssh*                                     "tauser@Arch:~" 20:15 28-Apr-26

```

sudo echo Hello World

```

  ● ● ● anthony - b12902118@nasa-ws3:~/tmp2/nasa/HW8 - ssh - nws - 180x49
Created symlink '/etc/systemd/system/multi-user.target.wants/sssd.service' → '/usr/lib/systemd/system/sssd.service' | Arch SSH port: 27411, VNC port: 18208
. | QEMU 9.2.2 monitor - type 'help' for more information
[root@Arch ~]# ssh tauser@localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:z6eF2uaakhEQYXuSl+76ChICTBOUv0epU5bXRdywWc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
tauser@localhost's password:
Creating directory '/home/tauser'.
[tauser@Arch ~]$ sudo echo Hello World

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

 #1) Respect the privacy of others.
 #2) Think before you type.
 #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

[sudo] password for tauser:
Hello World
[tauser@Arch ~]$ 

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f ta-group.ldif
Enter LDAP Password:
adding new entry "cn=ta,ou=group,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f student-group.ldif
Enter LDAP Password:
adding new entry "cn=student,ou=group,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# slappasswd
New password:
Re-enter new password:
{SSHA}ZNTXUWyrdNsFHZH+Kw0zhnOII6lyuYF/
root@Debian:~# vim user1.ldif
root@Debian:~# vim user2.ldif
root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user1.ldif
Enter LDAP Password:
adding new entry "uid=tauser,ou=people,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user2.ldif
Enter LDAP Password:
adding new entry "uid=studentuser,ou=people,dc=nasa,dc=csie,dc=ntu"

root@Debian:~#
[qemu_vms]0:ssh*                                     "tauser@Arch:~" 20:15 28-Apr-26

```

Exit out

```
exit
```

Test again

```
ssh studentuser@localhost
```

The screenshot shows a terminal session on a QEMU-hosted Arch Linux system. The session starts with a warning about host key fingerprinting, followed by creating a directory for the user. It then displays a message from the local System Administrator. Below that, three rules of thumb are listed: respect privacy, think before typing, and remember responsibility. A note about password visibility follows. The user then logs out. Subsequent commands show the creation of a new LDAP entry for a 'tauser' account on a Debian host, followed by the creation of 'studentuser' and 'user1' accounts. Finally, the user connects via SSH to the 'studentuser' account on the host system.

```
[anthonysmith@b12902118:nasa-ws3:~/tmp2/nasa/HW8]$ ssh -v studentuser@localhost
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
[tauser@localhost:~]# sudo echo Hello World
[tauser@localhost:~]# exit
Connection to localhost closed.
[studentuser@Arch ~]$ ssh studentuser@localhost
studentuser@localhost's password:
Creating directory '/home/studentuser'.
[studentuser@Arch ~]$ 

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f ta-group.ldif
Enter LDAP Password:
adding new entry "cn=ta,ou=group,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f student-group.ldif
Enter LDAP Password:
adding new entry "cn=student,ou=group,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# slappasswd
New password:
Re-enter new password:
{SSHA}ZNTXUWyrDnSFHZH+Kw0zhnOII6lyuYF/
root@Debian:~# vim user1.ldif
root@Debian:~# vim user2.ldif
root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user1.ldif
Enter LDAP Password:
adding new entry "uid=tauser,ou=people,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user2.ldif
Enter LDAP Password:
adding new entry "uid=studentuser,ou=people,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# 
[studentuser@Arch:~]$
```

```
sudo echo Hello World
```

```

anthony - b12902118@nasa-ws3:~/tmp2/nasa/HW8 - ssh - nws - 180x49
For security reasons, the password you type will not be visible.
[sudo] password for tauser:
Hello World
[tauser@Arch ~]$ exit
logout
Connection to localhost closed.
[root@Arch ~]# ssh studentuser@localhost
studentuser@localhost's password:
Creating directory '/home/studentuser'.
[studentuser@Arch ~]$ sudo echo Hello World

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

 #1) Respect the privacy of others.
 #2) Think before you type.
 #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

[sudo] password for studentuser:
studentuser is not in the sudoers file.
[studentuser@Arch ~]$ 

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f ta-group.ldif
Enter LDAP Password:
adding new entry "cn=ta,ou=group,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f student-group.ldif
Enter LDAP Password:
adding new entry "cn=student,ou=group,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# slappasswd
New password:
Re-enter new password:
{SSHA}ZNTXUWyrdnsFH2H+Kw0zhnOII6lyuYF/
root@Debian:~# vim user1.ldif
root@Debian:~# vim user2.ldif
root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user1.ldif
Enter LDAP Password:
adding new entry "uid=tauser,ou=people,dc=nasa,dc=csie,dc=ntu"

root@Debian:~# ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f user2.ldif
Enter LDAP Password:
adding new entry "uid=studentuser,ou=people,dc=nasa,dc=csie,dc=ntu"

root@Debian:~#

```

studentuser@Arch:~ 20:17 28-Apr-25

3

On the server, create ACL settings

```

# acl.ldif
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to attrs=userPassword
        by self write
        by anonymous auth
        by * none
olcAccess: {1}to attrs=cn,uid,gidNumber,homeDirectory
        by self read
        by * read
olcAccess: {2}to *
        by self write
        by users read
        by anonymous read

```

Apply modifications

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

4

Add two new attributes

```
# attr.ldif
dn: cn=schema,cn=config
changetype: modify
add: olcAttributeTypes
olcAttributeTypes: ( 1.3.6.1.4.1.811.1.1 NAME 'studentName' DESC 'Student Full Name' E

dn: cn=schema,cn=config
changetype: modify
add: olcAttributeTypes
olcAttributeTypes: ( 1.3.6.1.4.1.811.1.2 NAME 'examGroupID' DESC 'Examination Group ID'
```

Apply modifications

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

Add a new objectClass

```
# obj.ldif
dn: cn=schema,cn=config
changetype: modify
add: olcObjectClasses
olcObjectClasses: ( 1.3.6.1.4.1.811.2.1 NAME 'StudentInformation' DESC 'Student Information' E
```

Apply modifications

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

Create a new password for the new student

```
slappasswd
```

Create a new student

```
# newstudent.ldif
dn: uid=b12902118,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: StudentInformation
uid: b12902118
sn: Student
cn: b12902118
uidNumber: 3002
gidNumber: 2001
homeDirectory: /home/b12902118
loginShell: /bin/bash
studentName: Anthony Ching
examGroupID: GRP001
userPassword: {SSHA}8ABxAZ+qNUCbs5pVUmSJMEoYtjBZQQ/J
```

Apply modifications

```
ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f newstudent.ldif
```

Add the new student to the student group

```
# addtogroup.ldif
dn: cn=student,ou=group,dc=nasa,dc=csie,dc=ntu
changetype: modify
add: memberUid
memberUid: b12902118
```

Apply modifications

```
ldapmodify -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f addtogroup.ldif
```

Test

```
ldapsearch -x -H ldaps:/// -b uid=b12902118,ou=people,dc=nasa,dc=csie,dc=ntu
```

```
[sudo] password for studentuser:  
studentuser is not in the sudoers file.  
[studentuser@Arch ~]$  
root@Debian:~# ldapsearch -x -H ldaps:/// -b ou=people,dc=nasa,dc=csie,dc=ntu uid=b12902118  
# extended LDIF  
#  
# LDAPv3  
# base <ou=people,dc=nasa,dc=csie,dc=ntu> with scope subtree  
# filter: uid=b12902118  
# requesting: ALL  
  
# search result  
search: 2  
result: 0 Success  
  
# numResponses: 1  
root@Debian:~# ldapsearch -x -H ldaps:/// -b uid=b12902118,ou=people,dc=nasa,dc=csie,dc=ntu  
# extended LDIF  
#  
# LDAPv3  
# base <uid=b12902118,ou=people,dc=nasa,dc=csie,dc=ntu> with scope subtree  
# filter: (objectclass=*)  
# requesting: ALL  
  
# b12902118, people, nasa.csie.ntu  
dn: uid=b12902118,ou=people,dc=nasa,dc=csie,dc=ntu  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: shadowAccount  
objectClass: StudentInformation  
sn: Ching  
givenName: Anthony  
displayName: Anthony Ching  
uidNumber: 3002  
loginShell: /bin/bash  
studentName: Anthony Ching  
examGroupID: GRP001  
  
# search result  
search: 2  
result: 0 Success  
  
# numResponses: 2  
# numEntries: 1  
root@Debian:~#  
[qemu_uml_0:~]$: ssh*
```

Arch SSH port: 23021, VNC port: 19593
QEMU 9.2.2 monitor - type 'help' for more information
(qemu)

Debian SSH port: 20641, VNC port: 36270
QEMU 9.2.2 monitor - type 'help' for more information
(qemu)

"b12902118@nasa-ws3:~/" 22:48 28-Apr-15