Network Administration/System Administration Homework #8

B10202012 劉仲楷

1. 在 Server 安裝 OpenLDAP

   ```
   apt install -y slapd ldap-utils
   ```

   執行

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

   其中 `suffix.ldif`、`rootdn.ldif`、`base.ldif` 都在附件中。執行查詢結果在下一題圖片中。

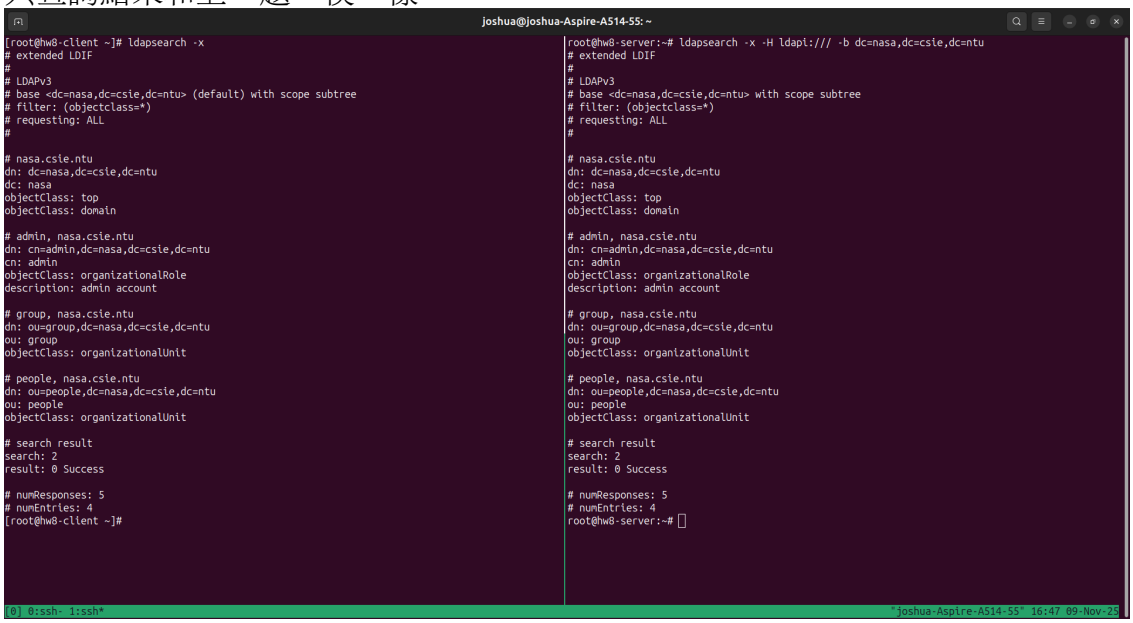
2. ref: OpenLDAP#The Client 安裝 OpenLDAP:

   ```
   pacman -S openldap
   ```

   修改 `/etc/openldap/ldap.conf`

   ```
   BASE    dc=nasa,dc=csie,dc=ntu
   URI     ldap://192.168.8.1
   ```

   只查詢結果和上一題一模一樣：



3. ref: OpenLDAP#OpenLDAP over TLS

   (a) 使用以下指令和附檔 `tls-config.ldif` 用 SSL/TLS。

```
openssl genrsa -out /etc/ldap/sasl2/ldap-server-key.pem 4096

openssl req -new -key /etc/ldap/sasl2/ldap-server-key.pem \
  -out /tmp/ldap-server.csr \
  -subj "/C=TW/ST=Taiwan/L=Taipei/O=NASA CSIE NTU/CN=NASAWS"

openssl x509 -req -days 3650 -in /tmp/ldap-server.csr \
  -out /etc/ssl/certs/ldap-server-cert.pem \
  -signkey /etc/ldap/sasl2/ldap-server-key.pem

cp /etc/ssl/certs/ca-certificates.crt /etc/ldap/sasl2/
chown openldap:openldap /etc/ldap/sasl2
ldapmodify -Y EXTERNAL -H ldapi:/// -f tls.ldif
```

接編輯 `/etc/default/slapd` 修改
`SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"` 再編輯 `/etc/ldap/ldap.conf`
新增

```
TLS_CACERT        /etc/ldap/sasl2/ca-certificates.crt
TLS_REQCERT        allow
```

最後 `systemctl restart slapd`

(b)

```
root@hw8-server:~# 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@hw8-server:~#
```

```
root@hw8-server:~# 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=*)
# 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@hw8-server:~#
```

(c)

(d) 使用以下指令和附檔 `force-tls.ldif` 調整

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

(e) 在 client 端編輯 `/etc/openldap/ldap.conf` 新增

```
TLS_CACERT        /etc/ssl/certs/ca-certificates.crt
TLS_REQCERT        allow
```

```
[root@hw8-client ~]# ldapsearch -x
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> (default) 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@hw8-client ~]#
```

(f)

```
[root@hw8-client ~]# ldapsearch -x -H ldap://192.168.8.1 -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 13 Confidentiality required
text: TLS confidentiality required

# numResponses: 1
[root@hw8-client ~]#
```

4. ref: OpenLDAP#Online and offline authentication with SSSD、sudoer.ldap man page

(a) 在 client 上安裝 sssd: `pacman -Sy sssd nss-pam-ldapd` 將附檔放入 `/etc/sssd/sssd.conf` 並更改權限

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

```
passwd: files systemd sss
group: files [SUCCESS=merge] systemd sss
shadow: files systemd sss
gshadow: files systemd sss
sudoers: files sss
...
```

編輯 `/etc/pam.d/system-auth` 加上

```
auth sufficient pam_sss.so forward_pass
...
account [default=bad success=ok user_unknown=ignore authinfo_unavail=ignore]
...
password sufficient pam_sss.so
...
session     required      pam_mkhomedir.so skel=/etc/skel/ umask=0077
...
session optional pam_sss.so
```

詳細見附檔。最後再

```
systemctl restart sssd sshd
```

(b) 用以下指令和附件在 server 新增群組：

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

在調整權限前，我發現 openldap 沒有內建 sudo schema，於是我到了 sudoer.ldap man page 找到 schema 更改，詳見附檔

```
ldapadd -Y EXTERNAL -H ldapi:/// -f sudo-schema.ldif
```

接用另一個附件和以下指令調整權限：

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

最後在 `/etc/sudoers` 加上

```
\%ta ALL=(ALL:ALL) ALL
```

(c) 用附件（密碼用 slappasswd 生成）和以下指令

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

(d)

```
[root@hw8-client ~]# ssh student001@localhost
student001@localhost's password:
Creating directory '/home/student001'.
[student001@hw8-client ~]$ 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 student001:
sudo: account validation failure, is your account locked?
sudo: a password is required
```

```
[root@hw8-client ~]# ssh ta001@localhost
ta001@localhost's password:
Creating directory '/home/ta001'.
[ta001@hw8-client ~]$ sudo echo "Hello World"
[sudo] password for ta001:
Hello World
[ta001@hw8-client ~]$
```

5. ref: OpenLDAP: 8. Access Control 使用附檔並在 server 下以下指令調整 ACL

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

(a)

```
[root@hw8-client ~]# ldapmodify -x -D "uid=ta001,ou=people,dc=nasa,dc=csie,dc=ntu"
 -W << EOF
dn: uid=student001,ou=people,dc=nasa,dc=csie,dc=ntu
changetype: modify
replace: loginShell
loginShell: /bin/zsh
EOF
Enter LDAP Password:
modifying entry "uid=student001,ou=people,dc=nasa,dc=csie,dc=ntu"
ldap_modify: Insufficient access (50)
```

(b)

```
[root@hw8-client ~]# ldapmodify -x -D "uid=ta001,ou=people,dc=nasa,dc=csie,dc=ntu"
 -W << EOF
dn: uid=ta001,ou=people,dc=nasa,dc=csie,dc=ntu
changetype: modify
replace: cn
cn: ta001
EOF
Enter LDAP Password:
modifying entry "uid=ta001,ou=people,dc=nasa,dc=csie,dc=ntu"
ldap_modify: Insufficient access (50)

[root@hw8-client ~]# ldapmodify -x -D "uid=ta001,ou=people,dc=nasa,dc=csie,dc=ntu"
 -W << EOF
dn: uid=ta001,ou=people,dc=nasa,dc=csie,dc=ntu
changetype: modify
replace: loginShell
loginShell: /bin/zsh
EOF
Enter LDAP Password:
modifying entry "uid=ta001,ou=people,dc=nasa,dc=csie,dc=ntu"
```

(c)

```
[root@hw8-client ~]# ldapsearch -x -D "uid=ta001,ou=people,dc=nasa,dc=csie,dc=ntu" -W \
  -b "uid=student001,ou=people,dc=nasa,dc=csie,dc=ntu" userPassword
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <uid=student001,ou=people,dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: userPassword
#

# student001, people, nasa.csie.ntu
dn: uid=student001,ou=people,dc=nasa,dc=csie,dc=ntu

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
[root@hw8-client ~]# ldapsearch -x -D "uid=ta001,ou=people,dc=nasa,dc=csie,dc=ntu" -W \
  -b "uid=student001,ou=people,dc=nasa,dc=csie,dc=ntu" loginShell
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <uid=student001,ou=people,dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: loginShell
#

# student001, people, nasa.csie.ntu
dn: uid=student001,ou=people,dc=nasa,dc=csie,dc=ntu
loginShell: /bin/bash

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

6. ref: OpenLDAP: 8. Schema Specification 用附檔在 server 執行下列指令

```
ldapadd -Y EXTERNAL -H ldapi:/// -f ntu-schema.ldif
ldapadd -x -ZZ -D "cn=admin,dc=nasa,dc=csie,dc=ntu" -W -f ntu-student.ldif
```

```
root@hw8-server:~# ldapsearch -x -ZZ -b "uid=ntu001,ou=people,dc=nasa,dc=csie
,dc=ntu"# extended LDIF
#
# LDAPv3
# base <uid=ntu001,ou=people,dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# ntu001, people, nasa.csie.ntu
dn: uid=ntu001,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: ntuStudent
uid: ntu001
cn: NTU Student Example
sn: Student
givenName: NTU
mail: ntu001@csie.ntu.edu.tw
uidNumber: 20003
gidNumber: 10002
homeDirectory: /home/ntu001
loginShell: /bin/bash
studentEntryMethod: exam
studentAdvisor: hsinmu

# search result
search: 3
result: 0 Success

# numResponses: 2
# numEntries: 1
```