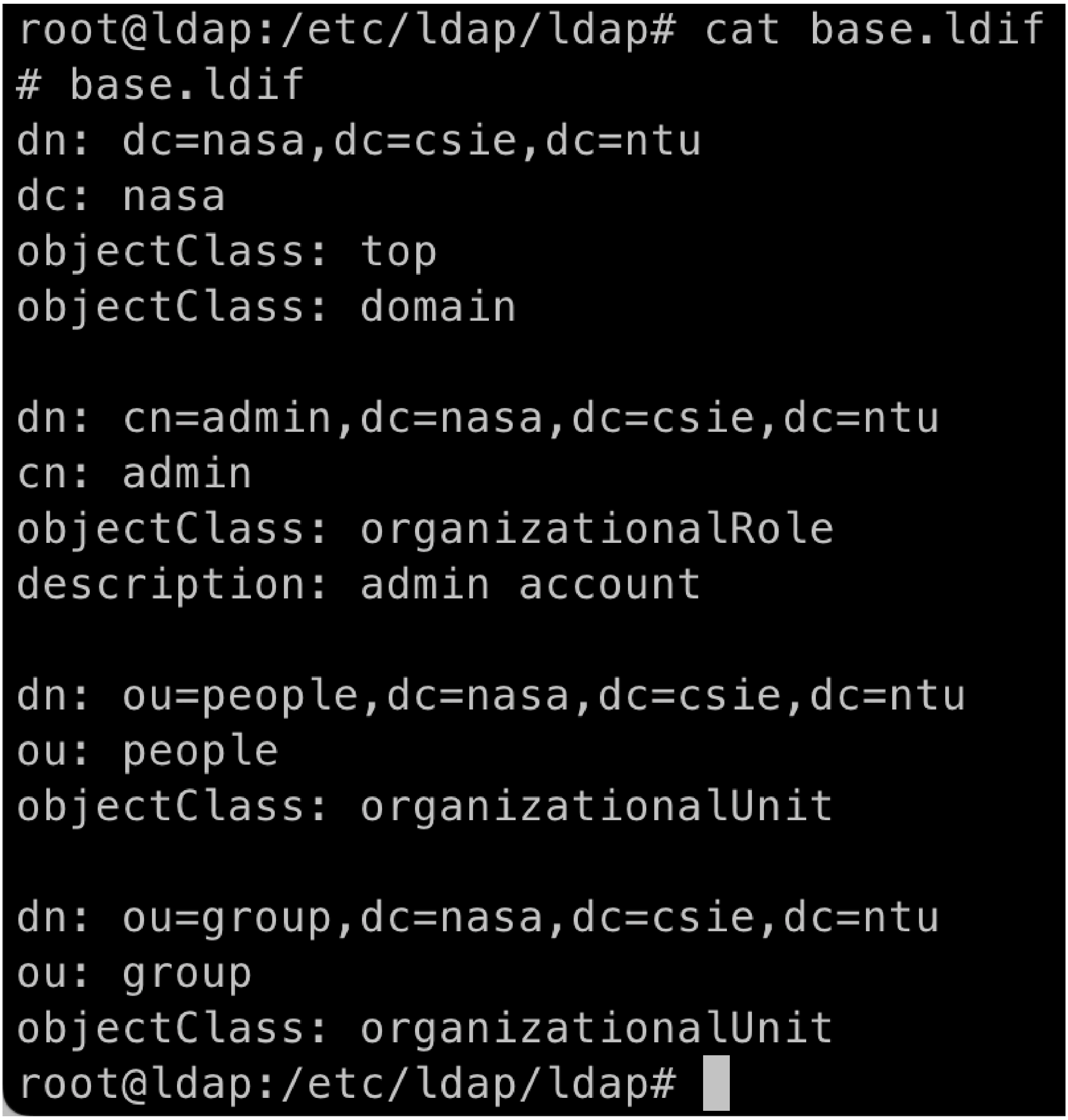
NASA hw8 繳交版

Author: B12705014陳泊華

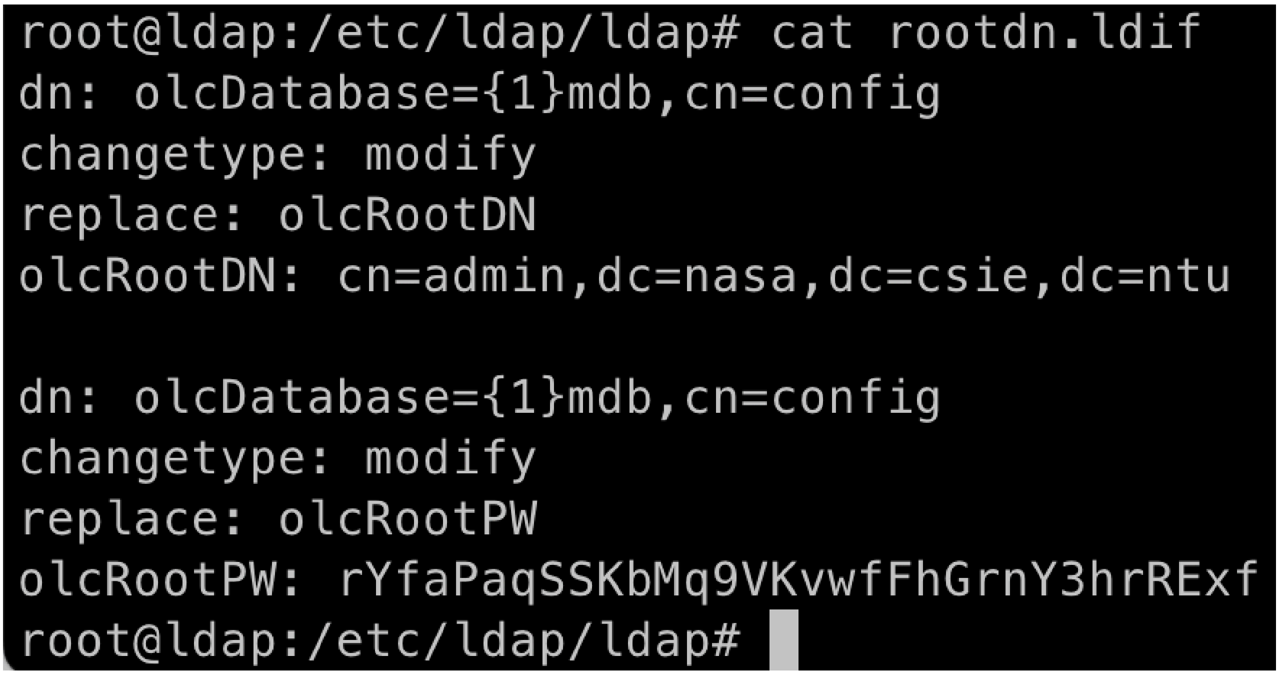
1. Server Setup
   (a)
   在LDAP Server:
   `$ apt install -y slapd ldap-utils`
   password: bowenchenAt16
   `$ apt install ldapvi`

依照Lab所學設定
`$ cat base.ldif`



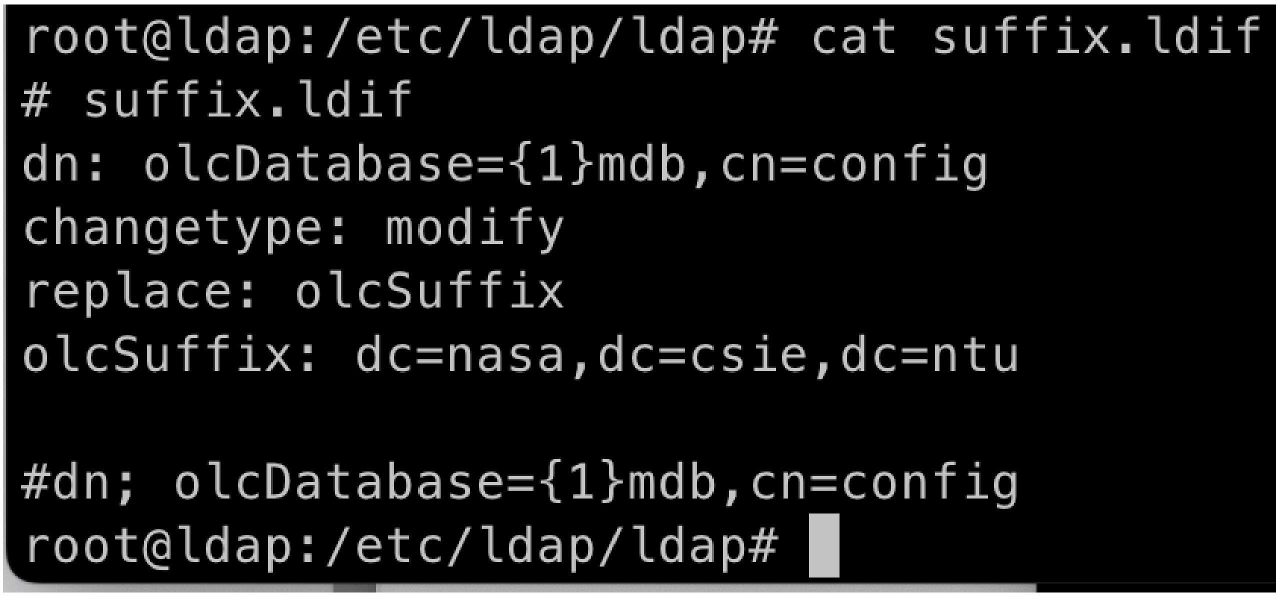
```
root@ldap:/etc/ldap/ldap# cat base.ldif
# base.ldif
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

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
root@ldap:/etc/ldap/ldap# 
```

```
$ cat rootdn.ldif
```



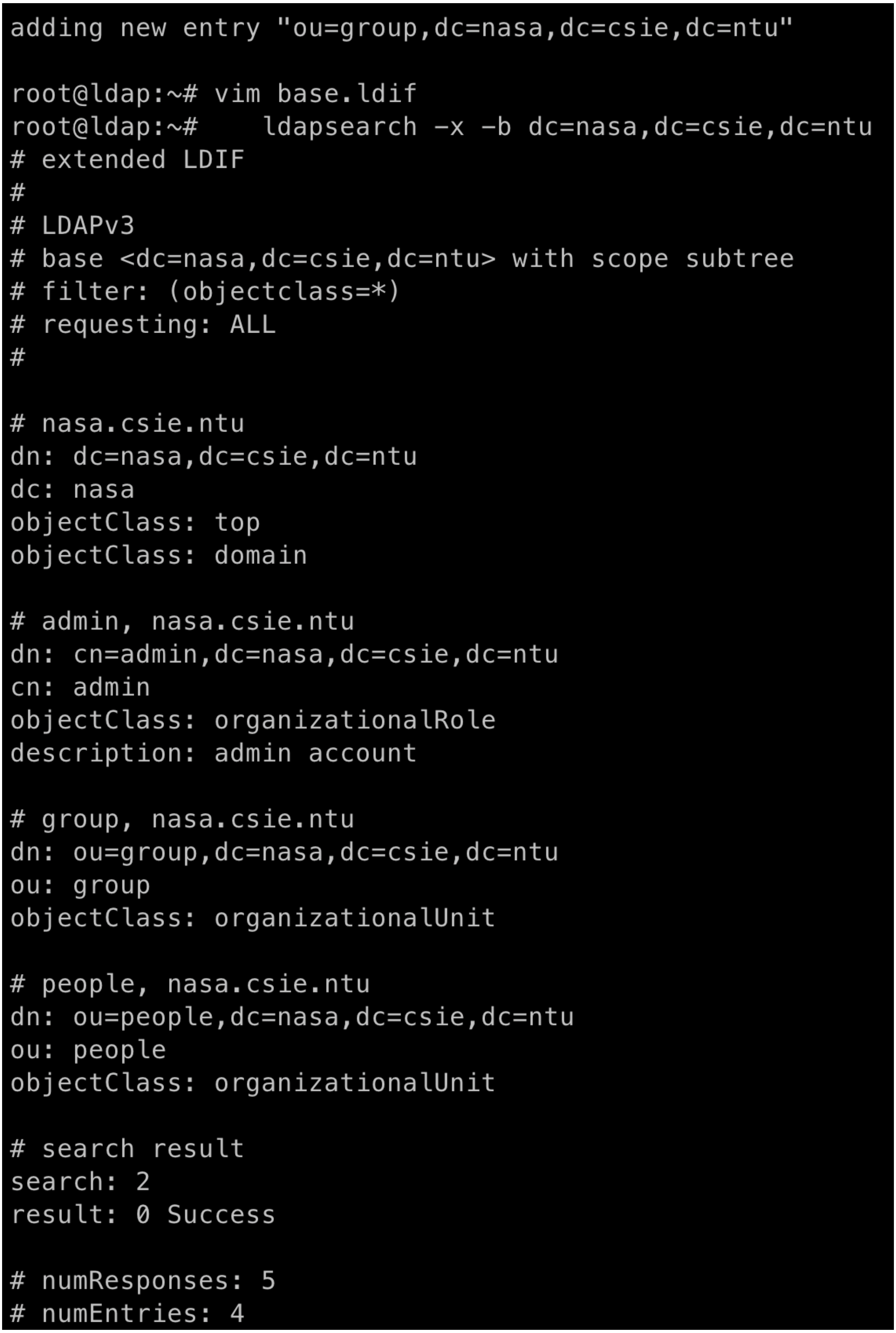
```
root@ldap:/etc/ldap/ldap# cat rootdn.ldif
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=nasa,dc=csie,dc=ntu

dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: rYfaPaqSSKbMq9VKvwfFhGrnY3hrRExf
root@ldap:/etc/ldap/ldap#
```

```
$ cat suffix.ldif
```



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

#dn; olcDatabase={1}mdb,cn=config
root@ldap:/etc/ldap/ldap#
```

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



```
adding new entry "ou=group,dc=nasa,dc=csie,dc=ntu"

root@ldap:~# vim base.ldif
root@ldap:~#    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
```

reference:
TA Lab Slides

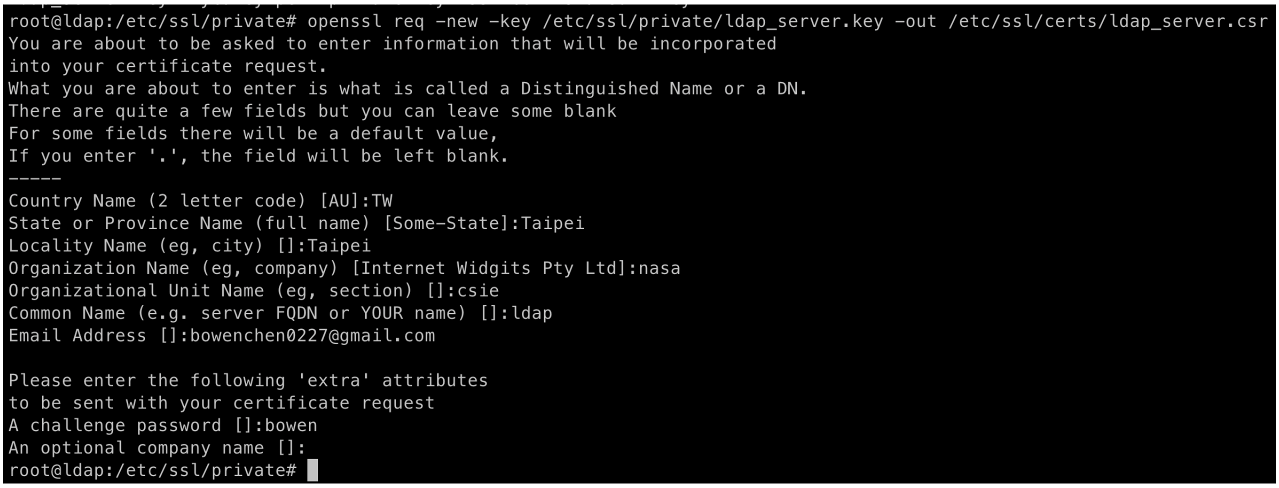
(b)

(1) 創建私鑰

```
$ openssl genrsa -out /etc/ssl/private/ldap_server.key 2048
```

(2) 創建一個證書簽名請求（CSR）

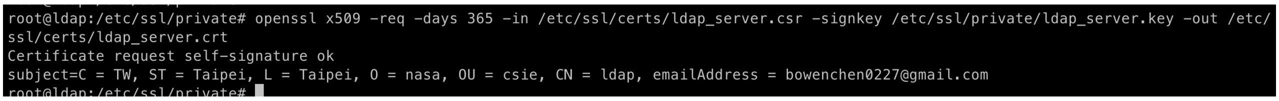
```
$ openssl req -new -key /etc/ssl/private/ldap_server.key -out
/etc/ssl/certs/ldap_server.csr
```



```
root@ldap:/etc/ssl/private# openssl req -new -key /etc/ssl/private/ldap_server.key -out /etc/ssl/certs/ldap_server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taipei
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:nasa
Organizational Unit Name (eg, section) []:csie
Common Name (e.g. server FQDN or YOUR name) []:ldap
Email Address []:bowenchen0227@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:bowen
An optional company name []:
root@ldap:/etc/ssl/private# 
```

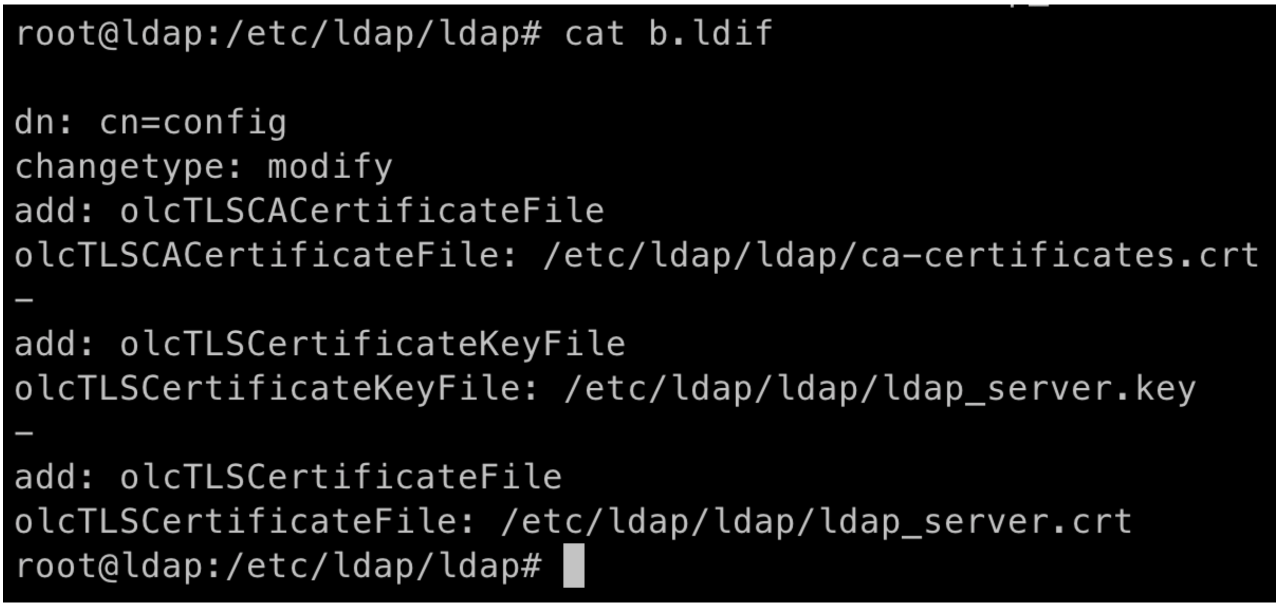
(3) 自己簽署證書

```
$ openssl x509 -req -days 365 -in /etc/ssl/certs/ldap_server.csr -signkey
/etc/ssl/private/ldap_server.key -out /etc/ssl/certs/ldap_server.crt
```



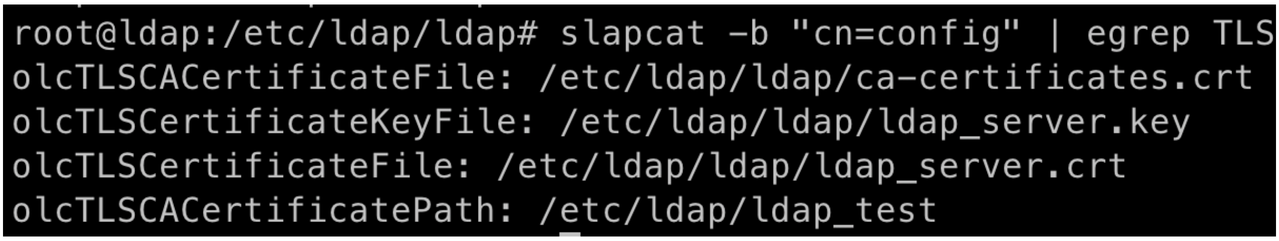
```
root@ldap:/etc/ssl/private# openssl x509 -req -days 365 -in /etc/ssl/certs/ldap_server.csr -signkey /etc/ssl/private/ldap_server.key -out /etc/
ssl/certs/ldap_server.crt
Certificate request self-signature ok
subject=C = TW, ST = Taipei, L = Taipei, O = nasa, OU = csie, CN = ldap, emailAddress = bowenchen0227@gmail.com
root@ldap:/etc/ssl/private# 
```

(4) 編輯ldif檔後執行ldapmodify



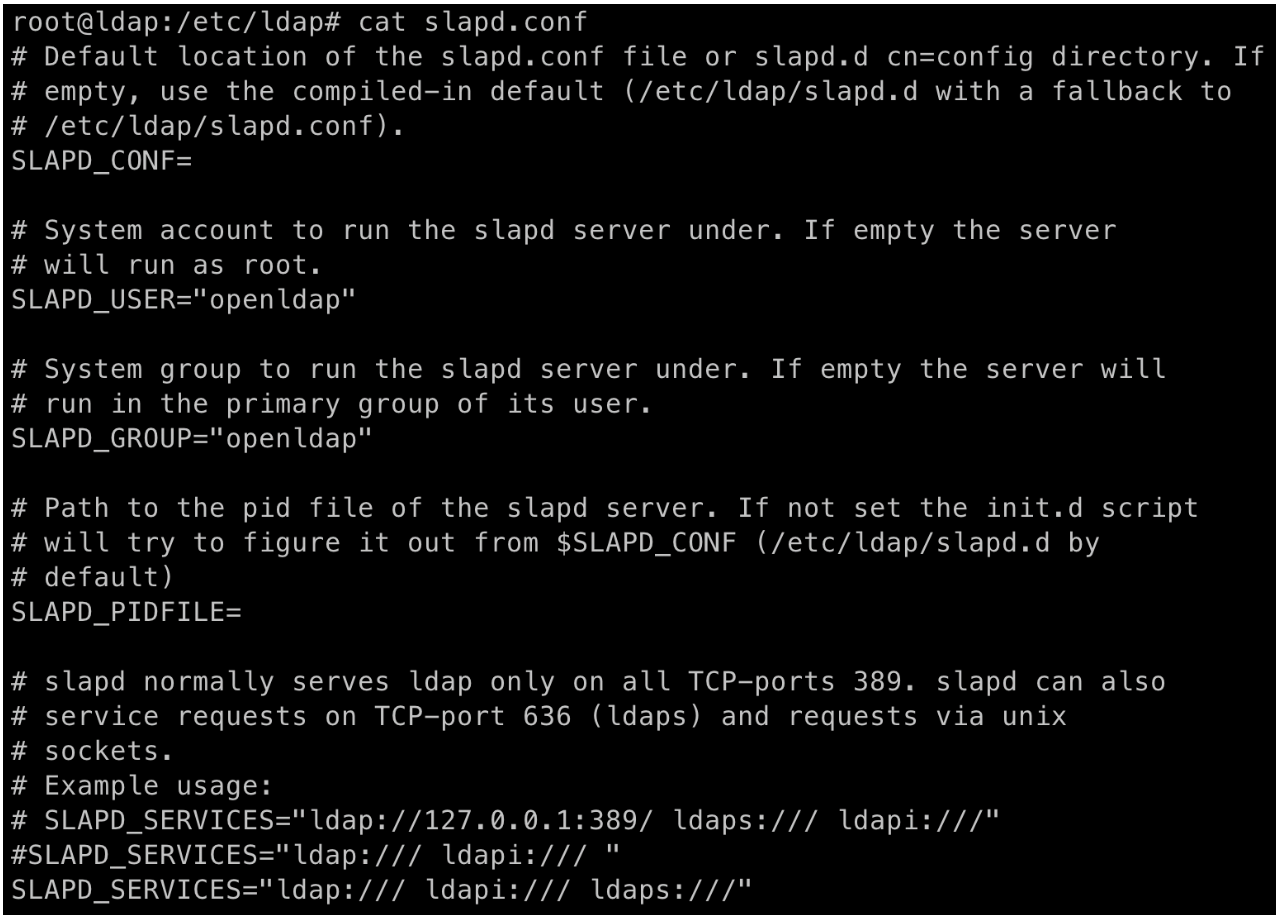
```
root@ldap:/etc/ldap/ldap# cat b.ldif

dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/ldap/ca-certificates.crt
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/ldap/ldap_server.key
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/ldap/ldap_server.crt
root@ldap:/etc/ldap/ldap# 
```

使用 `$ slapcat -b "cn=config" | egrep TLS` 檢查



```
root@ldap:/etc/ldap/ldap# slapcat -b "cn=config" | egrep TLS
olcTLSCACertificateFile: /etc/ldap/ldap/ca-certificates.crt
olcTLSCertificateKeyFile: /etc/ldap/ldap/ldap_server.key
olcTLSCertificateFile: /etc/ldap/ldap/ldap_server.crt
olcTLSCACertificatePath: /etc/ldap/ldap_test
```

(5) 修改/etc/ldap/slapd.conf設定，新增"SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///""進行TLS和SSL設定



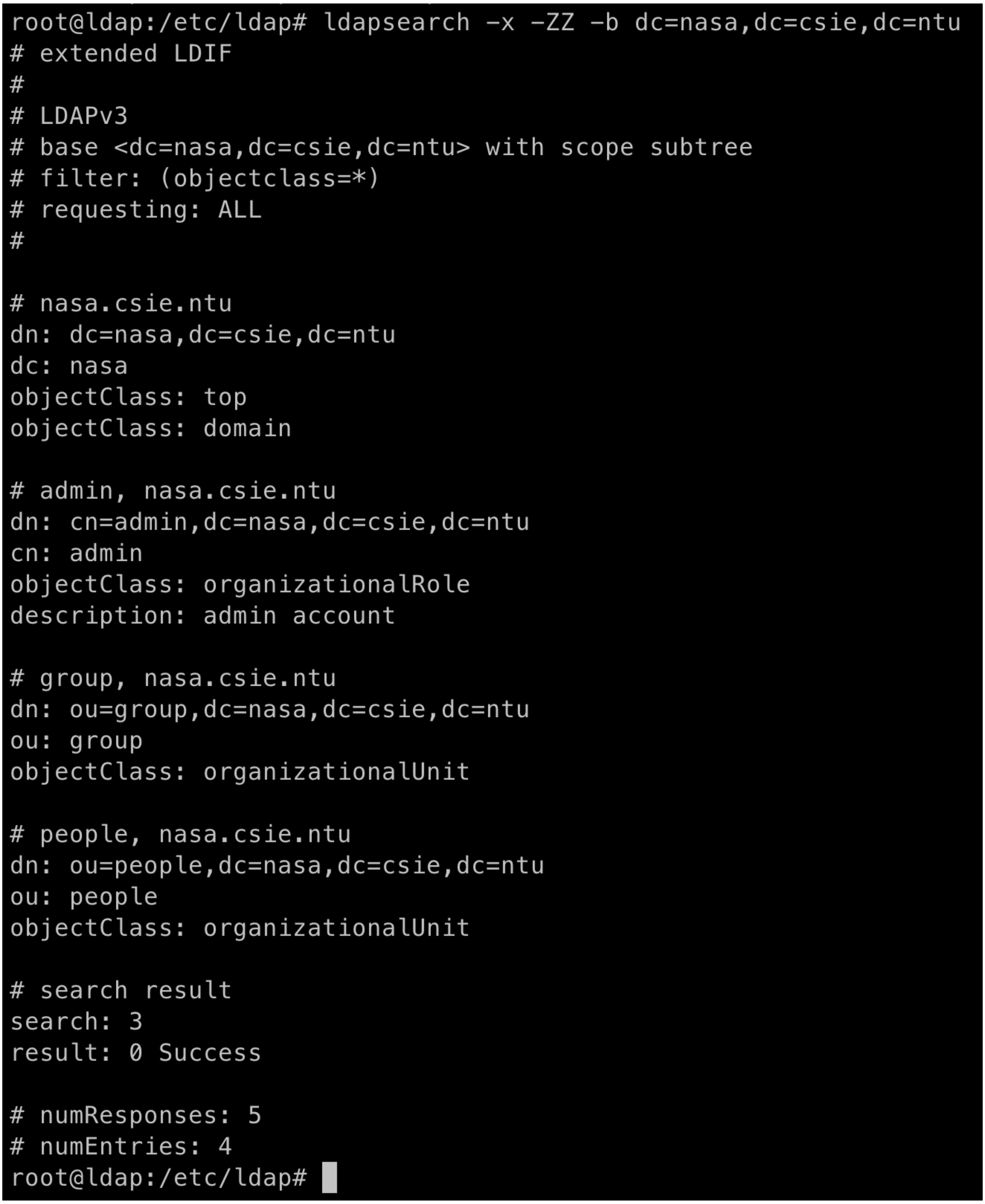
```
root@ldap:/etc/ldap# cat slapd.conf
# Default location of the slapd.conf file or slapd.d cn=config directory. If
# empty, use the compiled-in default (/etc/ldap/slapd.d with a fallback to
# /etc/ldap/slapd.conf).
SLAPD_CONF=

# System account to run the slapd server under. If empty the server
# will run as root.
SLAPD_USER="openldap"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
SLAPD_GROUP="openldap"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.d by
# default)
SLAPD_PIDFILE=

# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
#SLAPD_SERVICES="ldap:/// ldapi:/// "
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

(6) 重啟slapd

```
$ systemctl restart slapd
```

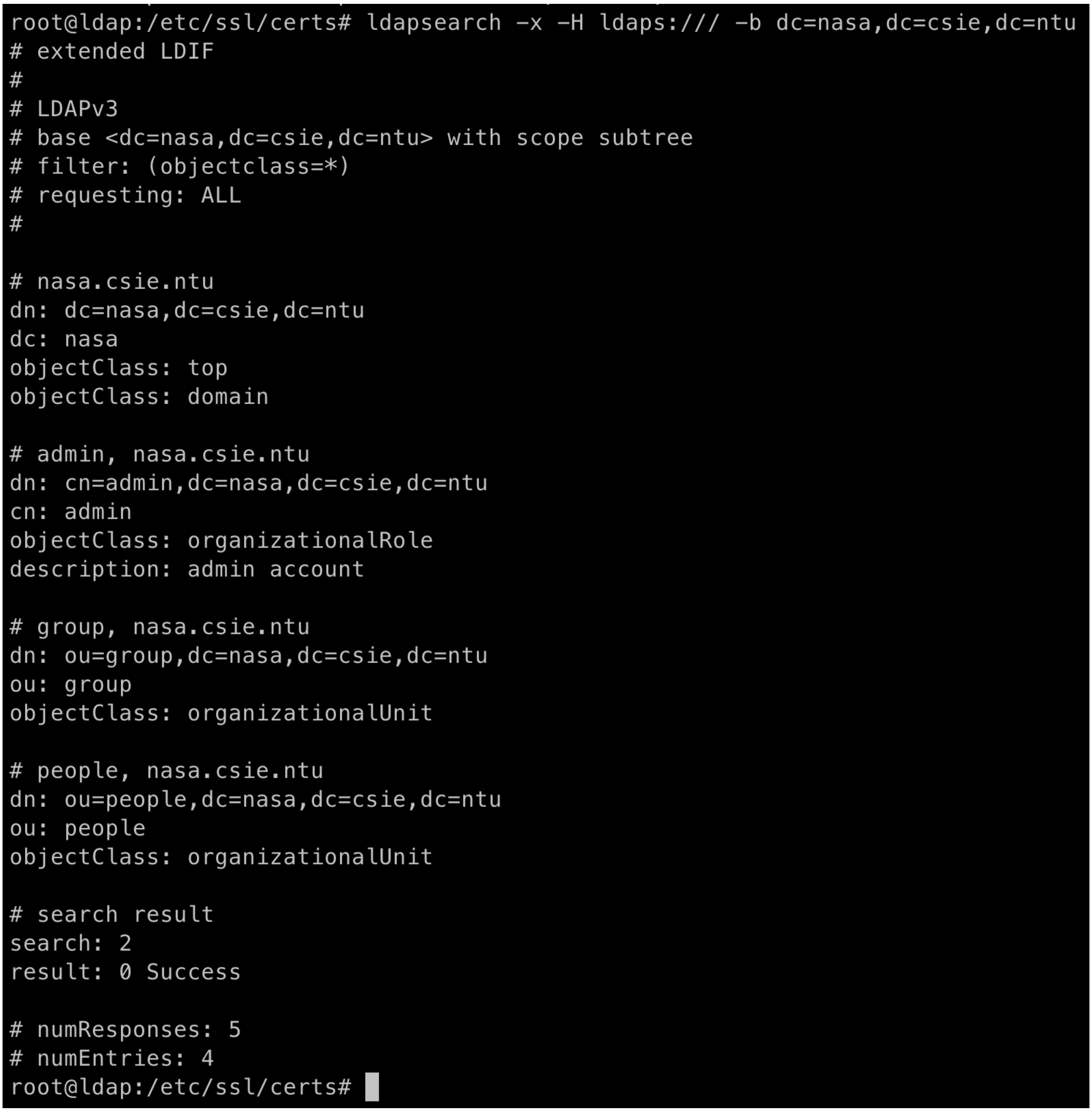
檢查：

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



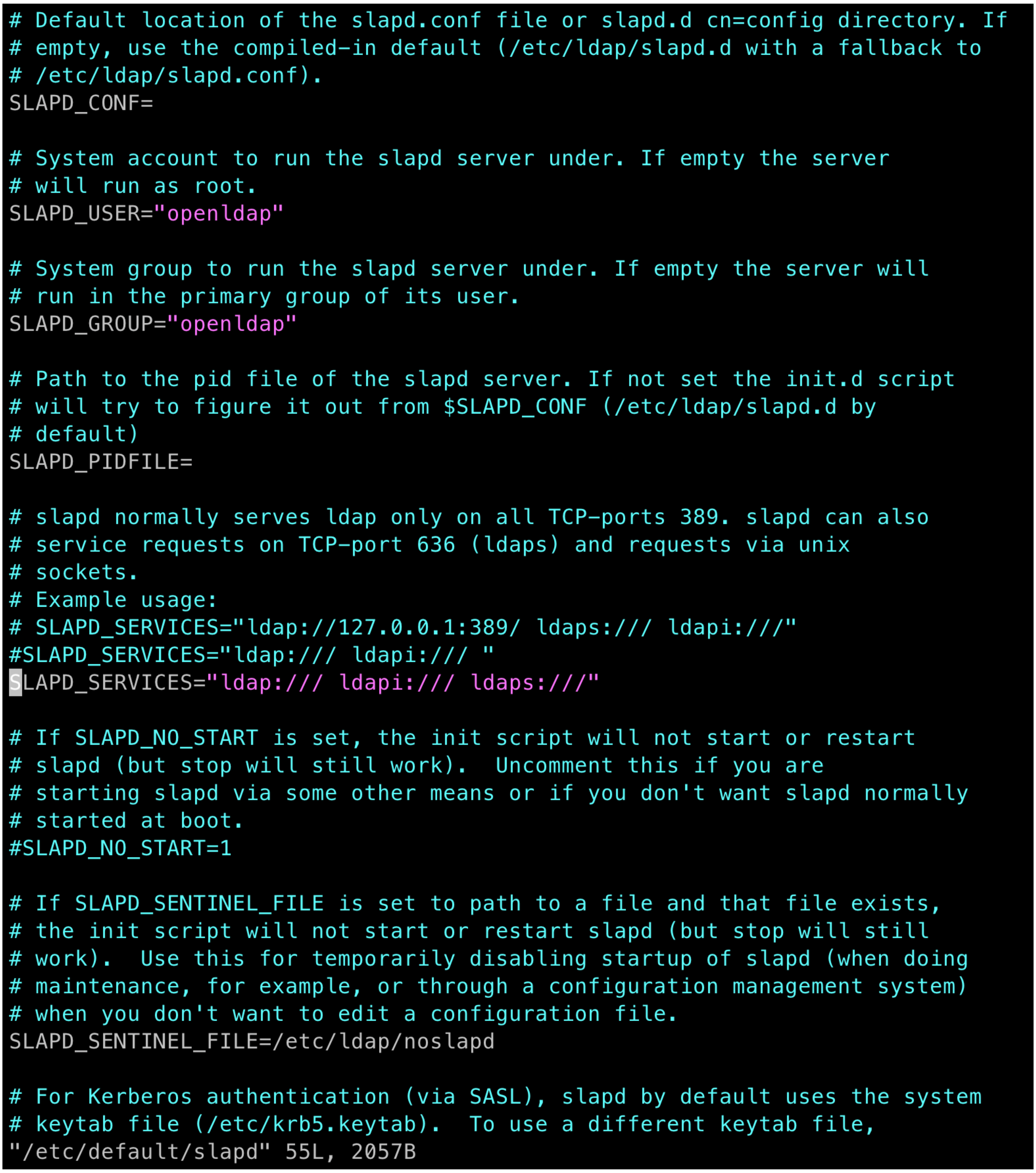
```
root@ldap:/etc/ldap# ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# 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@ldap:/etc/ldap# 
```

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



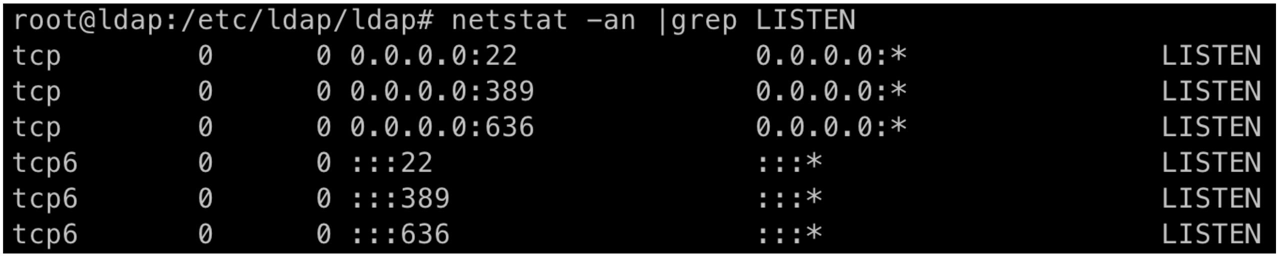
```
root@ldap:/etc/ssl/certs# ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# 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@ldap:/etc/ssl/certs#
```

```
$ vim /etc/default/slapd
```



```
# Default location of the slapd.conf file or slapd.d cn=config directory. If
# empty, use the compiled-in default (/etc/ldap/slapd.d with a fallback to
# /etc/ldap/slapd.conf).
SLAPD_CONF=

# System account to run the slapd server under. If empty the server
# will run as root.
SLAPD_USER="openldap"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
SLAPD_GROUP="openldap"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.d by
# default)
SLAPD_PIDFILE=

# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
#SLAPD_SERVICES="ldap:/// ldapi:/// "
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"

# If SLAPD_NO_START is set, the init script will not start or restart
# slapd (but stop will still work).  Uncomment this if you are
# starting slapd via some other means or if you don't want slapd normally
# started at boot.
#SLAPD_NO_START=1

# If SLAPD_SENTINEL_FILE is set to path to a file and that file exists,
# the init script will not start or restart slapd (but stop will still
# work).  Use this for temporarily disabling startup of slapd (when doing
# maintenance, for example, or through a configuration management system)
# when you don't want to edit a configuration file.
SLAPD_SENTINEL_FILE=/etc/ldap/noslapd

# For Kerberos authentication (via SASL), slapd by default uses the system
# keytab file (/etc/krb5.keytab).  To use a different keytab file,
"/etc/default/slapd" 55L, 2057B
```

```
$ netstat -an |grep LISTEN
```



```
root@ldap:/etc/ldap/ldap# netstat -an |grep LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::389                  :::*                    LISTEN
tcp6       0      0 :::636                  :::*                    LISTEN
```

reference:

(i) TA slides

(ii) https://www.ibm.com/docs/en/zos/2.4.0?topic=hashing-setting-up-ssltls

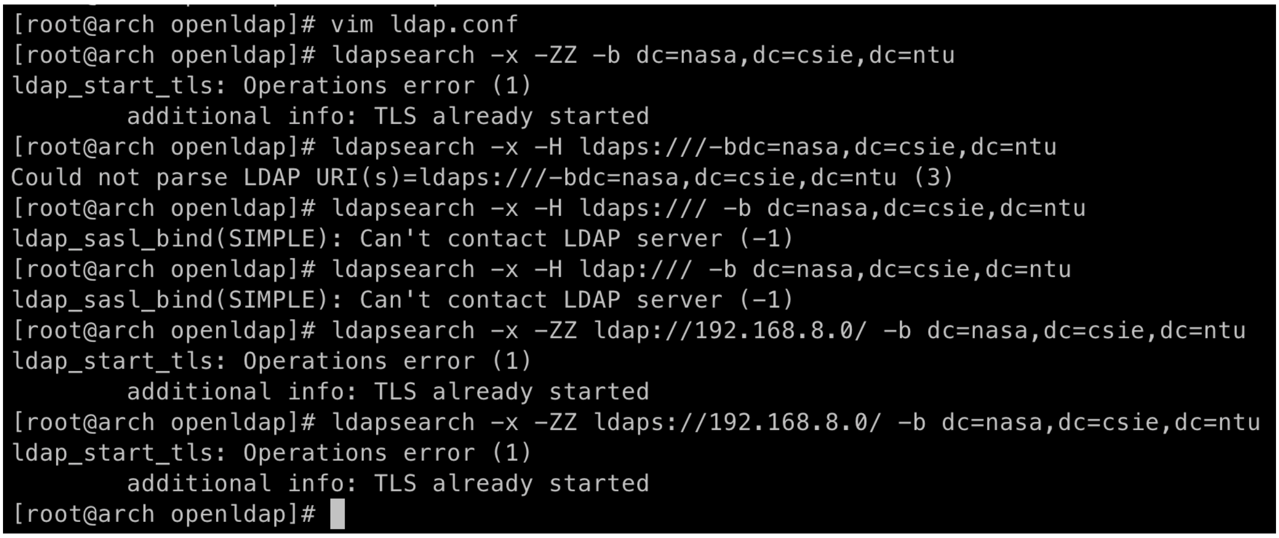
(https://www.ibm.com/docs/en/zos/2.4.0?topic=hashing-setting-up-ssltls)

(iii) https://linux.vbird.org/somepaper/20070222-ldap-5.pdf

(https://linux.vbird.org/somepaper/20070222-ldap-5.pdf)

2. Client Setup

有嘗試在ldap.conf中設定TLS_REQCERT allow，但沒成功



```
[root@arch openldap]# vim ldap.conf
[root@arch openldap]# ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu
ldap_start_tls: Operations error (1)
        additional info: TLS already started
[root@arch openldap]# ldapsearch -x -H ldaps:///-bdc=nasa,dc=csie,dc=ntu
Could not parse LDAP URI(s)=ldaps:///-bdc=nasa,dc=csie,dc=ntu (3)
[root@arch openldap]# ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu
ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1)
[root@arch openldap]# ldapsearch -x -H ldap:/// -b dc=nasa,dc=csie,dc=ntu
ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1)
[root@arch openldap]# ldapsearch -x -ZZ ldap://192.168.8.0/ -b dc=nasa,dc=csie,dc=ntu
ldap_start_tls: Operations error (1)
        additional info: TLS already started
[root@arch openldap]# ldapsearch -x -ZZ ldaps://192.168.8.0/ -b dc=nasa,dc=csie,dc=ntu
ldap_start_tls: Operations error (1)
        additional info: TLS already started
[root@arch openldap]# 
```