LDAP - LDAP with TLS/SSL

我在前幾篇 LDAP 文件中，介紹與實作了 LDAP 的簡單應用，但是 LDAP 傳送時是使用明碼的方式，也就是說在傳送資訊的時間是沒有任何的加密，如果在資訊傳送的過程中封包被側錄，那麼側錄者不用花費任何的力氣就可以得知訊息。

在這篇文章中，我會實做如何讓 OpenLDAP 使用 SSL 來做傳輸時的資訊加密，讓資訊在傳送中加了一層安全防護。

系統需求

- OpenSSL
- OpenLDAP
- OpenLDAP Client

建立 LDAP 憑證

你可以參考 更安全的連線 Apache + SSL (new window) 做出一個 LDAP 的憑證，下面的範例中我會建立一個 ldap.l-penguin.ivd.tw.key 的私有金鑰。

```
root # openssl genrsa -out ldap.l-penguin.idv.tw.key 1024
Generating RSA private key, 1024 bit long modulus
.....................................................................++++++
.....................++++++
e is 65537 (0x10001)
```

建立一個 csr 待簽證檔

```
root # openssl req -new -key ldap.l-penguin.idv.tw.key -out ldap.l-
penguin.idv.tw.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) [GB]:TW
State or Province Name (full name) [Berkshire]:Taiwan
Locality Name (eg, city) [Newbury]:Taipei County
Organization Name (eg, company) [My Company Ltd]:l-penguin Corp.
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:ldap.l-penguin.idv.tw
Email Address []:steven@l-penguin.idv.tw

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root #
```

簽證 csr 檔案

如果你的單位沒有憑證中心，那麼可以使用 更安全的連線 Apache + SSL (new window) 的方式來做自我簽證，但如果你的環境中已經有憑證中心（本例中為 ca.l-penguin.idv.tw）那麼你可以使用 ca.l-penguin.idv.tw 來幫 ldap.l-penguin.idv.tw 做簽證。

若你想建立一個 CA 認證中心，則可以參考 建立一個可信任的單位根簽證 (Root CA) (new window)。

```
root # openssl x509 -req -days 365 -in ldap.l-penguin.idv.tw.csr -CA ca.l-
penguin.idv.tw.crt -CAkey ca.l-penguin.idv.tw.key -CAcreateserial -out ldap.l-
penguin.idv.tw.crt
Signature ok
subject=/C=TW/ST=Taiwan/L=Taipei County/O=l-penguin Corp./OU=IT/CN=ldap.l-
penguin.idv.tw/emailAddress=steven@l-penguin.idv.tw
Getting CA Private Key
Enter pass phrase for ca.l-penguin.idv.tw.key:your_password
root #
```

當做好簽證之後，在 ldap.l-penguin.idv.tw 上應該要有兩個重要的憑證檔案。

```
root # ls -l
total 12
-rw-r--r-- 1 root root 1017 Feb 21 01:12 ldap.l-penguin.idv.tw.crt
-rw-r--r-- 1 root root  737 Feb 21 00:55 ldap.l-penguin.idv.tw.csr
-rw-r--r-- 1 root root  887 Feb 21 00:54 ldap.l-penguin.idv.tw.key
root #
```

設定 slapd.conf

做好憑證之後，應該要設定 OpenLDAP 的 slapd.conf 讓 OpenLDAP 知道以那些憑證來做 TLS/SSL 的傳輸。

```
root # vi /etc/openldap/slapd.conf
-----------------------------------------------------------
TLSCipherSuite HIGH::MEDIUM:LOW
# 設定憑證檔案
TLSCertificateFile /CA/ldap.l-penguin.idv.tw.crt
# 設定私有憑證金鑰檔案
TLSCertificateKeyFile /CA/ldap.l-penguin.idv.tw.key
-----------------------------------------------------------
```

重新啟動 OpenLDAP

```
root # service ldap restart
Stopping slapd:                                            [  OK  ]
Checking configuration files for slapd:  config file testing succeeded
                                                           [  OK  ]
Starting slapd:                                            [  OK  ]
root #
```

確認 OpenLDAP 是否有聆聽 636 埠

```
root # netstat -ntulp | grep slapd
tcp        0      0 0.0.0.0:389         0.0.0.0:*       LISTEN      1737/slapd
tcp        0      0 0.0.0.0:636         0.0.0.0:*       LISTEN      1737/slapd
tcp        0      0 :::389                    :::*       LISTEN      1737/slapd
tcp        0      0 :::636                    :::*       LISTEN      1737/slapd
```

```
root #
```

以上，就完成了伺服器端的設定。

Client 設定

Linux/Unix ldapsearch

如果要讓 ldapsearch 可以使用 TLS/SSL 來做傳輸的話，就必需修改 ldap.conf 檔案。

```
root # vi /etc/openldap/ldap.conf
-------------------------------------
# 加入設定
TLS_REQCERT never
-------------------------------------
```

使用 TLS 方式傳輸

```
root # ldapsearch -x -ZZ -b "ou=company,dc=l-penguin,dc=idv,dc=tw" -h
ldap.l-penguin.idv.tw
# extended LDIF
#
# LDAPv3
# base <ou=company,dc=l-penguin,dc=idv,dc=tw> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# company, l-penguin.idv.tw
dn: ou=company,dc=l-penguin,dc=idv,dc=tw
ou: company
objectClass: organizationalUnit

# unit, company, l-penguin.idv.tw
dn: ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: unit
objectClass: organizationalUnit

# hr, unit, company, l-penguin.idv.tw
dn: ou=hr,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: hr
objectClass: organizationalUnit
~ 以下略 ~
root #
```

使用 SSL 方式傳輸

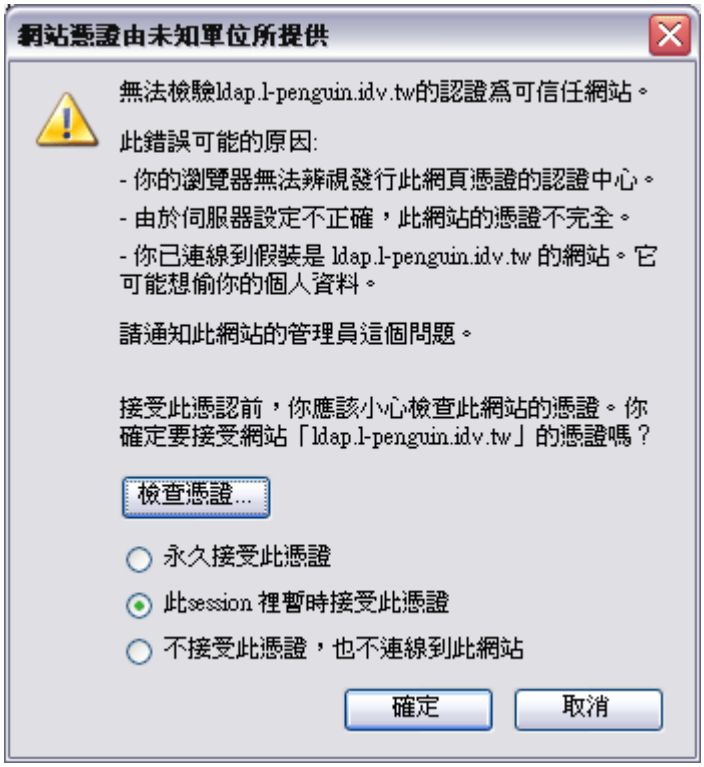
```
root # ldapsearch -x -b "ou=company,dc=l-penguin,dc=idv,dc=tw" -H
ldaps://ldap.l-penguin.idv.tw
# extended LDIF
#
# LDAPv3
# base <ou=company,dc=l-penguin,dc=idv,dc=tw> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# company, l-penguin.idv.tw
dn: ou=company,dc=l-penguin,dc=idv,dc=tw
ou: company
```

```
objectClass: organizationalUnit

# unit, company, l-penguin.idv.tw
dn: ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: unit
objectClass: organizationalUnit

# hr, unit, company, l-penguin.idv.tw
dn: ou=hr,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: hr
objectClass: organizationalUnit
~ 以下略 ~
root #
```

Thunderbird 設定

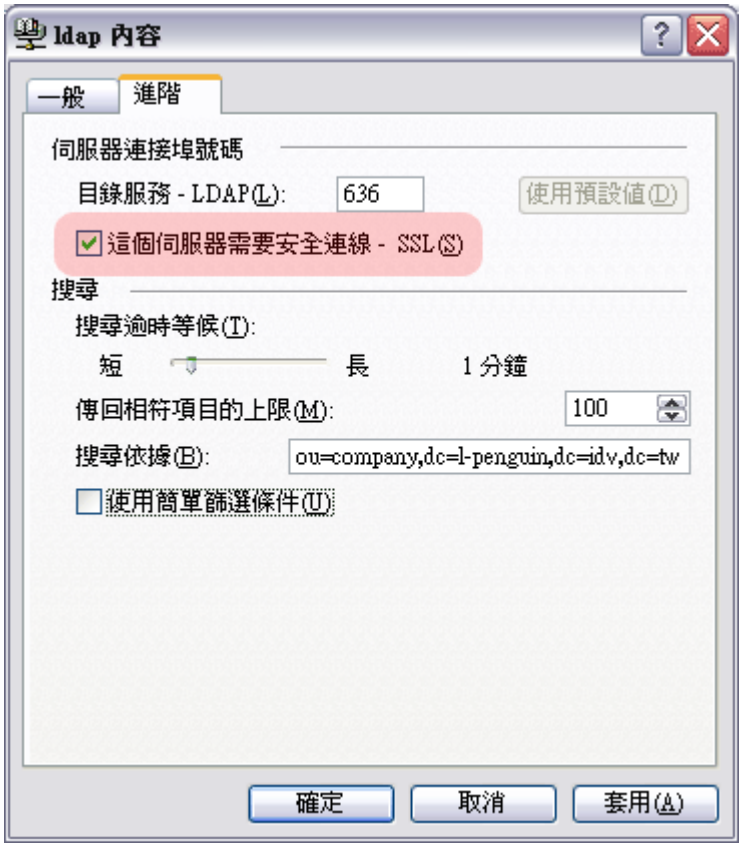
如果你已經把 Root CA 設定為 認證中心，那麼就只要做以下設定即可。

若你的憑證是由自己所檢發的，那麼就會需要同意傳輸時的憑證才行。

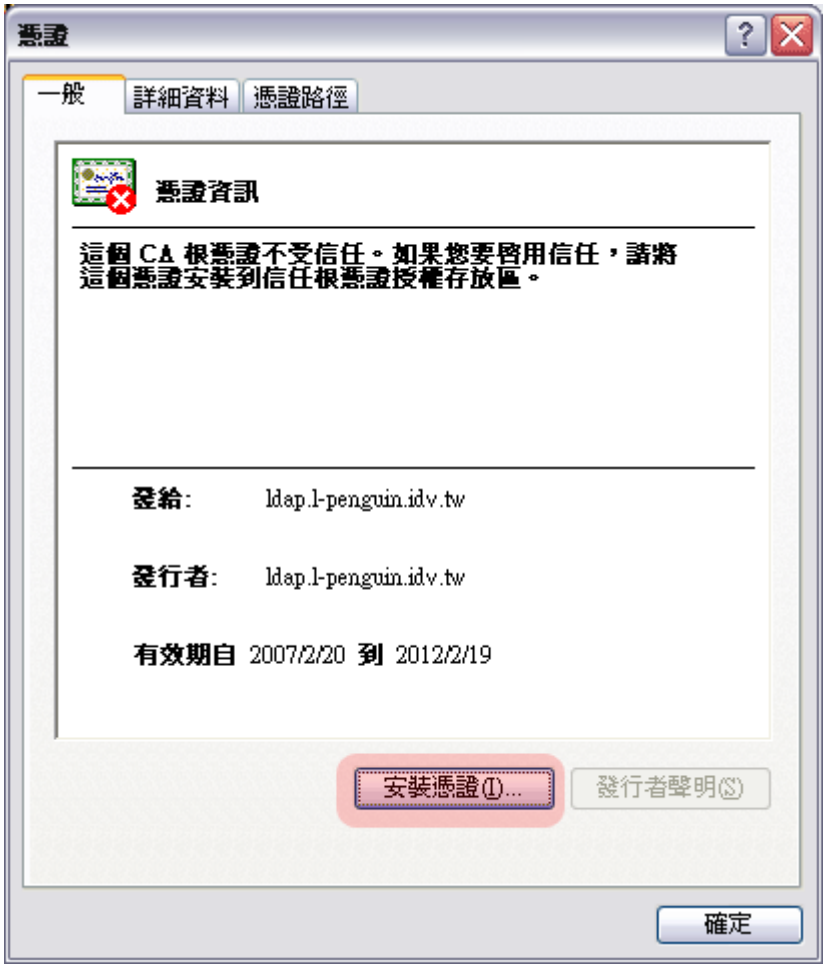


Outlook 設定

如果你已經把 Root CA 設定匯入到 Windows 的憑證管理，那麼就只要做以下設定即可。



若你的憑證是由自己所檢發的，那麼就會需要匯入憑證才行。



For more articles, please visit http://www.l-penguin.idv.tw/

作者：廖子儀 (Tzu-Yi Liao)
Certified：LPIC Level I、LPIC Level II、RHCE
E-mail：steven@ms.ntcb.edu.tw
Web site：Steven's Linux Note (http://www.l-penguin.idv.tw/)