LDAP - Replication

我在前幾篇的文章裡，有說明了一些 LDAP 的實做與應用，當然你也有可能依照本文 (I hope so :p) 建立了自己的 LDAP 環境。在你越來越依賴 LDAP 的時候，有可能會發現這一台 LDAP 伺服器似乎反應越來越慢，因為大家都一直去查尋或是更新，此時你可能會想要再建立一台 LDAP 的次要伺服器來專門服務查尋，而主要 LDAP 伺服器只要有更改就會同步到次要伺服器。

好了，我不多說，現在我就來示範如何建立一個 (或兩個以上) 的 LDAP Replication Server。

建立 Replication Server

為什麼我要反其道而行先建立好 Replication Server，其實這是個人習慣，因為 Master LDAP Server 是已知的資訊，而 Replication 卻是待產生的，所以我想應該要先把這個東西先生出來才能繼續設定。

當然了你必要安裝套件才行，需要有的套件就如同 LDAP 入門 (new window) 一樣，請參考一下吧。

在下面的示範我會建立 ldap2 和 ldap3 這兩個 Replication Server，也就是有兩個次要 LDAP 的查尋伺服器。

ldap2.l-penguin.idv.tw

為了效能，我們需要把 DB_CONFIG 這個檔建 copy 一份到 LDAP 資料庫的目錄，以便參考。

```
root # cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

設定 slapd.conf

```
root # vi /etc/openldap/slapd.conf
-----------------------------------------------------
# 設定 suffix、rootdn 及 rootpw。
suffix "dc=l-penguin,dc=idv,dc=tw"
rootdn "cn=ldap2,dc=l-penguin,dc=idv,dc=tw"
rootpw password

# 設定 updatedn, 一般和 rootdn 一樣, 不過也可以設定一
# 具有修改權利的帳號。
updatedn  "cn=ldap2,dc=l-penguin,dc=idv,dc=tw"
# 設定主要 Master Server 的主機名稱。
updateref ldap://ldap.l-penguin.idv.tw
-----------------------------------------------------
root #
```

現在，已經設定好 ldap2.l-penguin.idv.tw，再來就是第二部主機。

ldap3.l-penguin.idv.tw

第二部 Replication Server 和第一部 Replication Server 是一樣的設定方法，我就一次做完。

```
root # cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
root # vi /etc/openldap/slapd.conf
-----------------------------------------------------
```

```
# 設定 suffix、rootdn 及 rootpw。
suffix "dc=l-penguin,dc=idv,dc=tw"
rootdn "cn=ldap3,dc=l-penguin,dc=idv,dc=tw"
rootpw password

# 設定 updatedn, 一般和 rootdn 一樣, 不過也可以設定一
# 具有修改權利的帳號。
updatedn  "cn=ldap3,dc=l-penguin,dc=idv,dc=tw"
# 設定主要 Master Server 的主機名稱。
updateref ldap://ldap.l-penguin.idv.tw
-----------------------------------------------------
root #
```

好了，現在第二部 Replication Server 也設定好，也知道了 updatedn 和登入時的密碼，現在就可以一同設定 Master Replication。

建立 Master Server

要讓主要伺服器可以順利同步到 Replication Server，Master Server 的設定很重要，如果設定不完全就會讓同步失效。現在我們就來編輯 slapd.conf。

```
root # vi /etc/openldap/slapd.conf
-----------------------------------------------------------
# 設定資料修改的差異檔。
# 這個設定非常重要，請不要乎略。
replogfile /var/lib/ldap/openldap-master-replog

# 1. 設定第一個 Replication Server，並以 tls 來做傳輸。
# 2. 使用簡易傳輸，使用 cn=ldap2,dc=l-penguin,dc=idv,dc=tw
#    和 password 來做帳號密碼驗證。
replica host=ldap2.l-penguin.idv.tw:389
       suffix="dc=l-penguin,dc=idv,dc=tw"
       binddn="cn=ldap2,dc=l-penguin,dc=idv,dc=tw"
       credentials=password
       bindmethod=simple
       tls=yes

# 1. 設定第二個 Replication Server，並以 tls 來做傳輸。
# 2. 使用簡易傳輸，使用 cn=ldap3,dc=l-penguin,dc=idv,dc=tw
#    和 password 來做帳號密碼驗證。
replica host=ldap3.l-penguin.idv.tw:389
       suffix="dc=l-penguin,dc=idv,dc=tw"
       binddn="cn=ldap3,dc=l-penguin,dc=idv,dc=tw"
       credentials=password
       bindmethod=simple
       tls=yes
-----------------------------------------------------------
root #
```

請注意，你應該要先做好 DNS 的對應 (ldap2.l-penguin.idv.tw 及 ldap3.l-penguin.idv.tw)，否則怎麼樣都會無法同部到。

你可以選擇是否要以 tls 來做資料傳輸，我建議最好使用，因為很難確定資料在同步的時候是否有人有意竊聽。

好了，現在要做一件很重要的事，那就是把 Master Server 的資料全部都複製一份到 Replication Server 才行，請記得這個時候應該要停止任何的更新動作，以免 Master、Replication 的資料不一致。

資料複製

Dump Master Server Data

在此我使用 slapcat 來做資料 dump，並使用 scp 傳送到兩台 Replication Server。

```
root # slapcat -b "dc=l-penguin,dc=idv,dc=tw" -l ldap.l-penguin.idv.tw.ldif
root # scp ldap.l-penguin.idv.tw.ldif steven@ldap2.l-penguin.idv.tw:~/
root # scp ldap.l-penguin.idv.tw.ldif steven@ldap3.l-penguin.idv.tw:~/
```

Restore Data

現在兩台 Replication Server 都有了完整的資料，那麼馬上就來還原。

```
root # slapadd -l ~steven/ldap.l-penguin.idv.tw.ldif
```

現在萬事具備，只欠東風，而這個東風就是要啟動 LDAP Server，現在就馬上來重新啟動吧。

啟動 LDAP 並做驗證

當設定好 LDAP 之後，記得要重新啟動，並且 Master 和 Replication 都要啟動才行。

重新啟動 ldap.l-penguin.idv.tw。

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

請主意，一旦主要伺服器設定了 replica 選項，那麼 ldap 就啟動 slurpd 來做同步更新。

重新啟動 ldap2 及 ldap3。

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

也許你會迫不及待想要看看 Replication Server 的資料是否真的全部匯入。

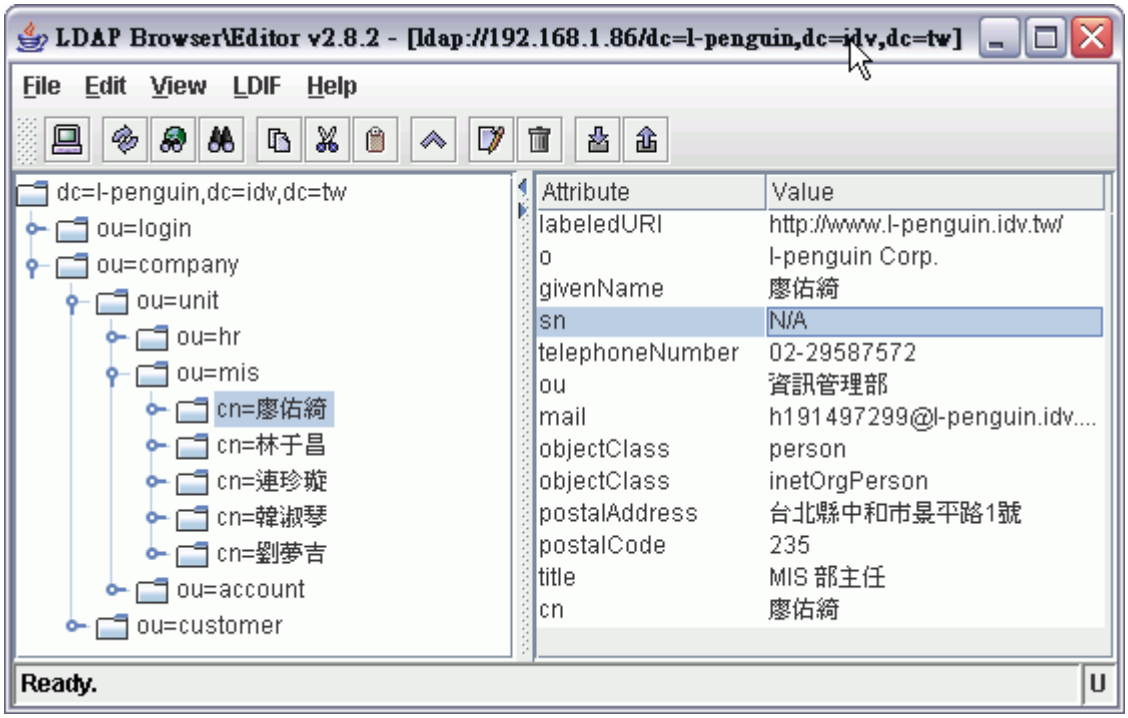
```
root # ldapsearch -x -b "ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
# extended LDIF
#
# LDAPv3
# base <ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
```

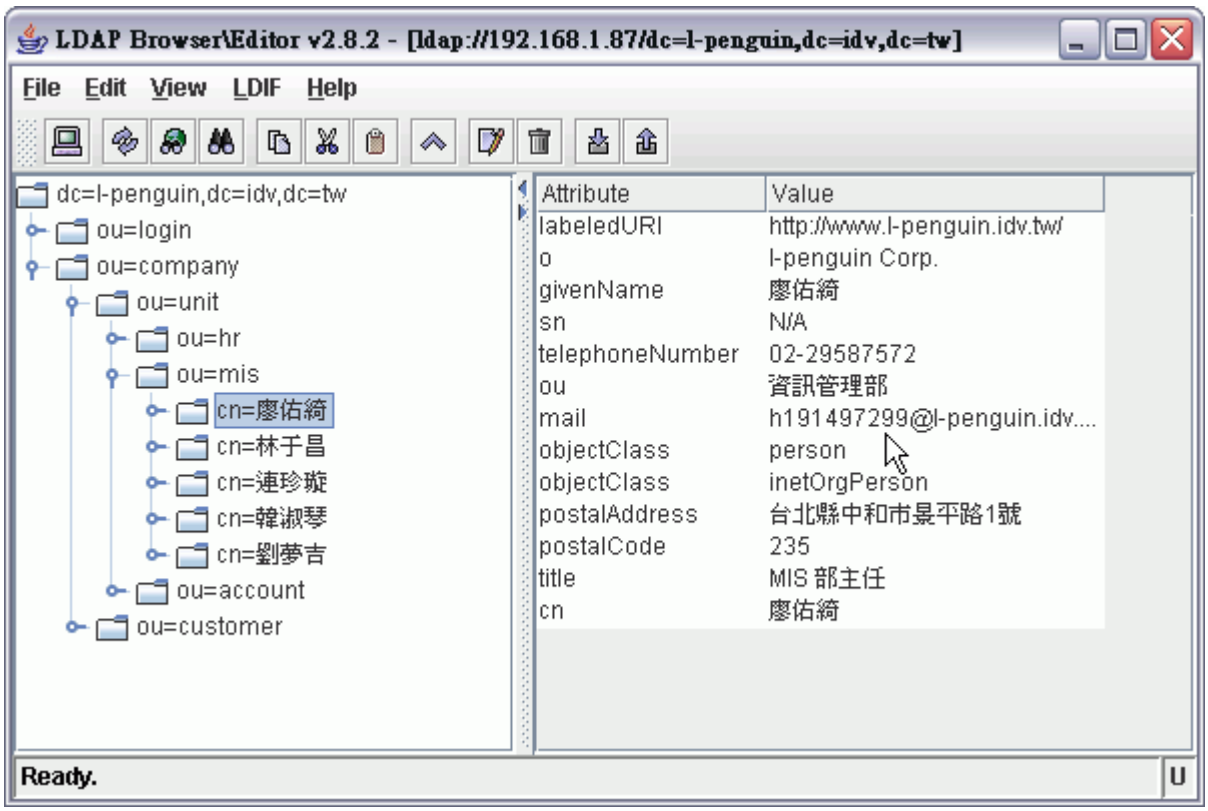
```
# user, login, l-penguin.idv.tw
dn: ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw
ou: user
objectClass: organizationalUnit

# c293831287, user, login, l-penguin.idv.tw
dn: cn=c293831287,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw
uid: c293831287
cn: c293831287
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword:: aHJDMjkzODMxMjg3
shadowLastChange: 11108
shadowMax: 99999
shadowWarning: 7
shadowFlag: 0
loginShell: /bin/bash
uidNumber: 600
gidNumber: 510
homeDirectory: /home/c293831287
gecos: Nicole Coon

# d197700415, user, login, l-penguin.idv.tw
dn: cn=d197700415,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw
uid: d197700415
cn: d197700415
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword:: aHJEMTk3NzAwNDE1
shadowLastChange: 11108
shadowMax: 99999
shadowWarning: 7
shadowFlag: 0
loginShell: /bin/bash
uidNumber: 601
gidNumber: 510
homeDirectory: /home/d197700415
gecos: Sheri Hussey
~ 哇塞! 資料太多了, 以下略過 :D ~
root #
```

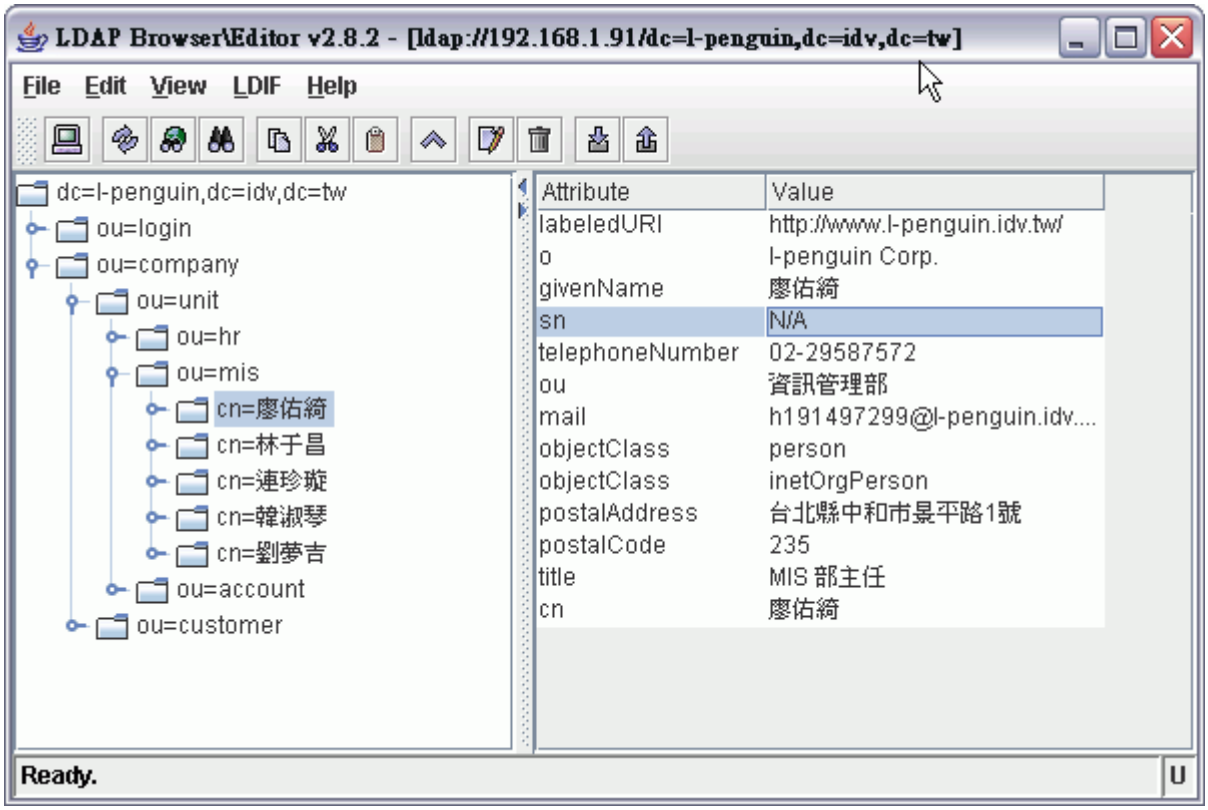
當然你現在可以相信資料已全部匯入。

修改 Master 資料並檢查是否同步

在此我使用在 LDAP 入門 (new window) 時所提的 ldapbrowser 這個工具來做示範。

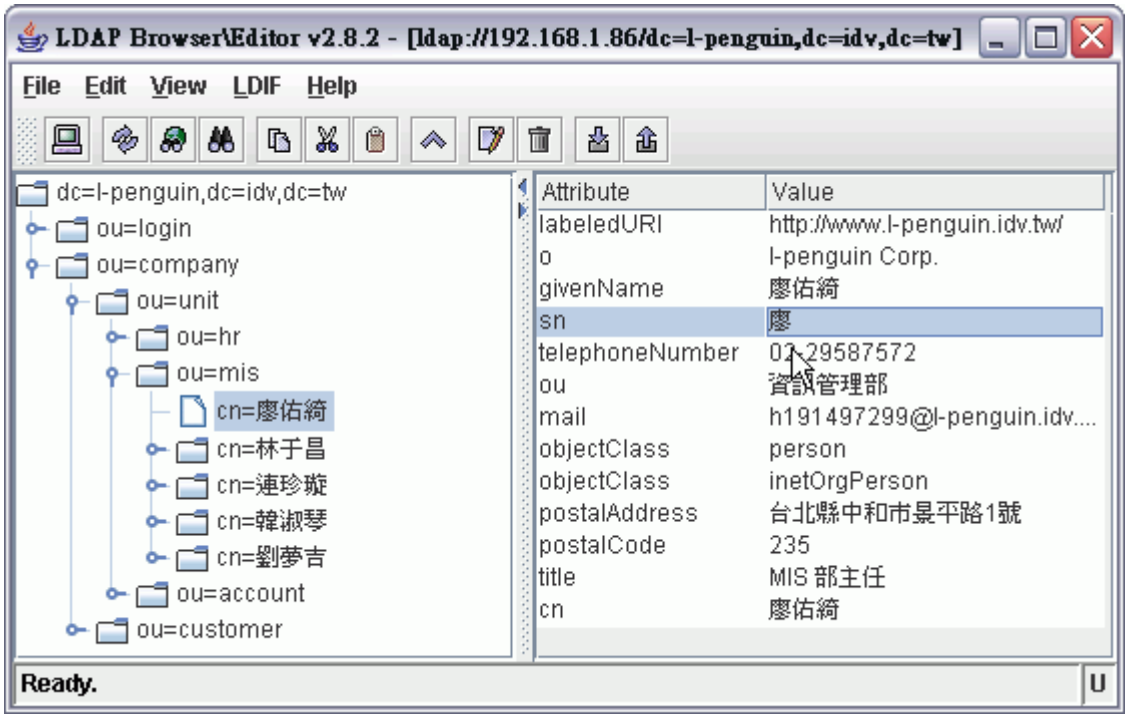

LDAP Browser\Editor v2.8.2 - [ldap://192.168.1.86/dc=l-penguin,dc=idv,dc=tw]
File Edit View LDIF Help
dc=l-penguin,dc=idv,dc=tw
ou=login
ou=company
ou=unit
ou=hr
ou=mis
cn=廖佑綺
cn=林于昌
cn=連珍璇
cn=韓淑琴
cn=劉夢吉
ou=account
ou=customer
Attribute Value
labeledURI http://www.l-penguin.idv.tw/
o l-penguin Corp.
givenName 廖佑綺
sn N/A
telephoneNumber 02-29587572
ou 資訊管理部
mail h191497299@l-penguin.idv....
objectClass person
objectClass inetOrgPerson
postalAddress 台北縣中和市景平路1號
postalCode 235
title MIS 部主任
cn 廖佑綺
Ready.
U

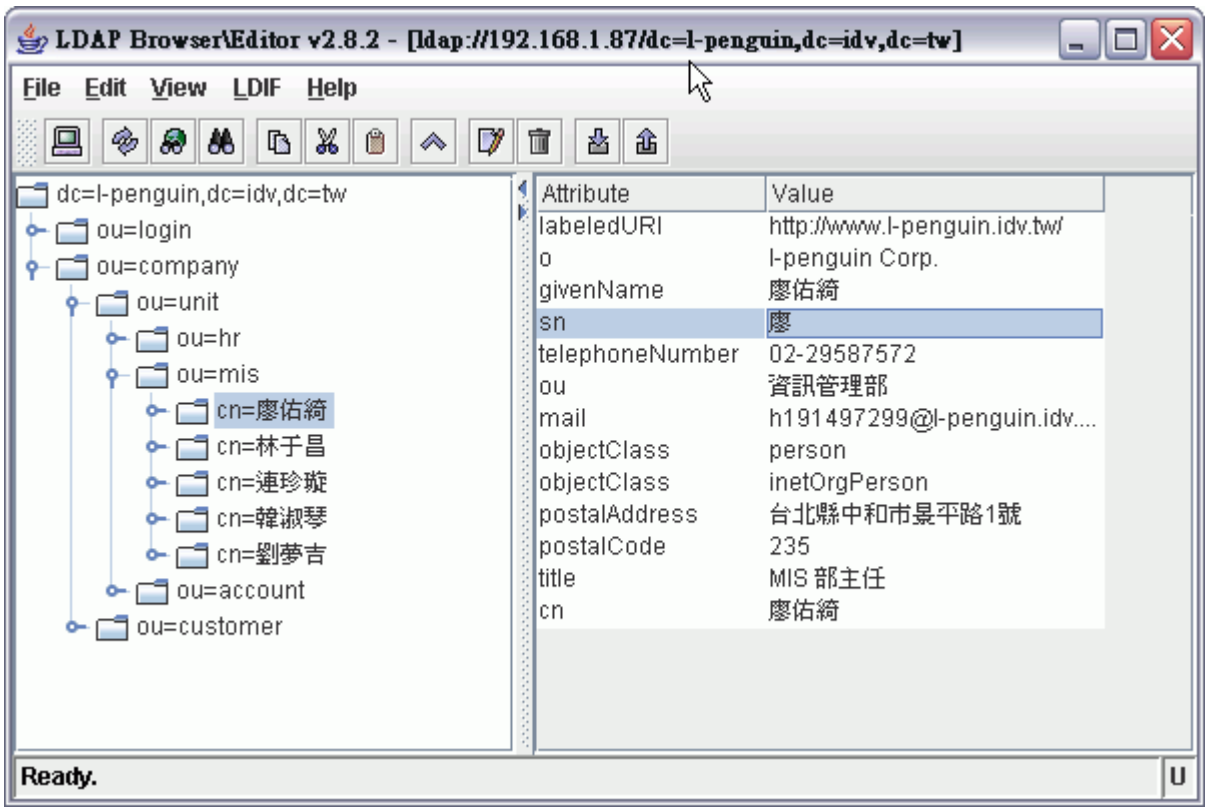

LDAP Browser\Editor v2.8.2 - [ldap://192.168.1.87/dc=l-penguin,dc=idv,dc=tw]
File Edit View LDIF Help
dc=l-penguin,dc=idv,dc=tw
ou=login
ou=company
ou=unit
ou=hr
ou=mis
cn=廖佑綺
cn=林于昌
cn=連珍璇
cn=韓淑琴
cn=劉夢吉
ou=account
ou=customer
Attribute Value
labeledURI http://www.l-penguin.idv.tw/
o l-penguin Corp.
givenName 廖佑綺
sn N/A
telephoneNumber 02-29587572
ou 資訊管理部
mail h191497299@l-penguin.idv....
objectClass person
objectClass inetOrgPerson
postalAddress 台北縣中和市景平路1號
postalCode 235
title MIS 部主任
cn 廖佑綺
Ready.
U

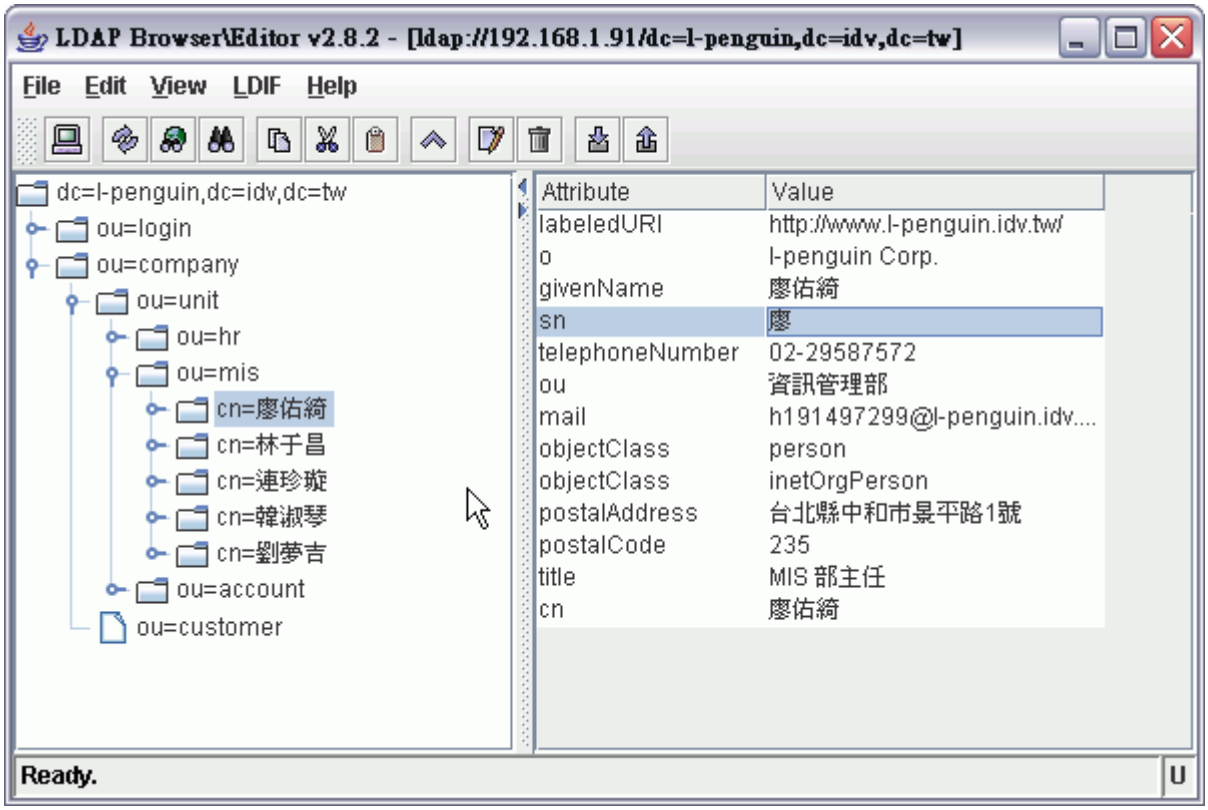


現在這位 廖佑綺 小姐的 sn 值是 N/A，現在我來把她重新設定。

現在馬上來看看另外兩部的變化：


LDAP Browser\Editor v2.8.2 - [ldap://192.168.1.86/dc=l-penguin,dc=idv,dc=tw]
File Edit View LDIF Help
dc=l-penguin,dc=idv,dc=tw
ou=login
ou=company
ou=unit
ou=hr
ou=mis
cn=廖佑綺
cn=林于昌
cn=連珍璇
cn=韓淑琴
cn=劉夢吉
ou=account
ou=customer
Attribute Value
labeledURI http://www.l-penguin.idv.tw/
o l-penguin Corp.
givenName 廖佑綺
sn 廖
telephoneNumber 02-29587572
ou 資訊管理部
mail h191497299@l-penguin.idv....
objectClass person
objectClass inetOrgPerson
postalAddress 台北縣中和市景平路1號
postalCode 235
title MIS 部主任
cn 廖佑綺
Ready.
U


LDAP Browser\Editor v2.8.2 - [ldap://192.168.1.87/dc=l-penguin,dc=idv,dc=tw]
File Edit View LDIF Help
dc=l-penguin,dc=idv,dc=tw
ou=login
ou=company
ou=unit
ou=hr
ou=mis
cn=廖佑綺
cn=林于昌
cn=連珍璇
cn=韓淑琴
cn=劉夢吉
ou=account
ou=customer
Attribute Value
labeledURI http://www.l-penguin.idv.tw/
o l-penguin Corp.
givenName 廖佑綺
sn 廖
telephoneNumber 02-29587572
ou 資訊管理部
mail h191497299@l-penguin.idv....
objectClass person
objectClass inetOrgPerson
postalAddress 台北縣中和市景平路1號
postalCode 235
title MIS 部主任
cn 廖佑綺
Ready.
U



你可以在兩台 Replication Server 上看到是否以 TLS 方式傳輸。

```
root # cat ldap.log | grep 'tls'
Feb 24 03:32:31 ldap2 slapd[1772]: conn=6 fd=14 TLS established tls_ssf=256
ssf=256
Feb 24 03:34:31 ldap2 slapd[1843]: conn=0 fd=14 TLS established tls_ssf=256
ssf=256
Feb 26 23:30:09 ldap2 slapd[1696]: conn=1 fd=22 TLS established tls_ssf=256
ssf=256
Feb 26 23:33:36 ldap2 slapd[1776]: conn=1 fd=16 TLS established tls_ssf=256
ssf=256
root #
```

設定以 SSL 方式傳輸

當然以上在傳輸的時候已經使用 TLS 方式來修改資料，當然你也可以設定使用 SSL 來對整個過程都使用 SSL 的加密方式傳輸。

設定 Master Server：

```
root # vi /etc/openldap/slapd.conf
-----------------------------------------------------------
# 使用 uri 項目來指定傳輸方式。或酗]不再使用 tls 了。
replica uri=ldaps://ldap2.l-penguin.idv.tw:636
        suffix="dc=l-penguin,dc=idv,dc=tw"
        binddn="cn=ldap2,dc=l-penguin,dc=idv,dc=tw"
        credentials=password
        bindmethod=simple

# 使用 uri 項目來指定傳輸方式。或酗]不再使用 tls 了。
replica uri=ldaps://ldap3.l-penguin.idv.tw:389
```

```
       suffix="dc=l-penguin,dc=idv,dc=tw"
       binddn="cn=ldap3,dc=l-penguin,dc=idv,dc=tw"
       credentials=password
       bindmethod=simple
-------------------------------------------------------
root #
```

設定 Replication Server：

```
root # vi /etc/openldap/slapd.conf
-------------------------------------------------------
# 使用 ssl 方式傳輸。
updateref ldaps://ldap.l-penguin.idv.tw
-------------------------------------------------------
root #
```

好了，經過以上設定之後，你就可以全程使用 SSL 來傳輸。

若要使用 ldaps 方式來做完全的加密傳輸，那麼你應該要設定伺服器的 CA 憑證才可以，要設定 CA 憑證可以參考 LDAP - LDAP with TLS/SSL (new window) 的文件。我在這裡就不再說明。

設定平衡負載

當你有兩台以上的次要 LDAP 服務時，可能會想要分散流量到兩台主機，此時你可以使用 DNS 的循環調渡方式來解決流量問題。

若要使用 DNS 的方式，請參考 bind - DNS 設定 (new window)。

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/)