LDAP - Referral

當您點開這一篇文件之後，想必您對 LDAP 的運作流程都是有一定的程度的了解了，如果您還不知道或是不清楚 LDAP 到底是什麼或是如何應用的話，小弟在此建議看觀從 LDAP 入門開始看起會比較好。

這篇文章介紹了如何實做 LDAP v3 的 Referral 功能，請記得，是 LDAP v3，因為 LDAP v2 未支援 Referral 的功能。

假如在您的環境中，想要授權一個子單位下去，而您希望這個子單位自己維護自己的 LDAP，比方說台北總公司授權到高雄的子公司，當然這就很像 DNS 裡的授權子網域一樣，那麼當總公司要查高雄子公司的名錄時，就會直接連線到高雄的 LDAP 做查詢，現在我們就來看看如何實做。

如果您不知道如何開始，或是要從頭建立一個跟我一樣的範例，可以參考以下資料：

- LDAP 入門 (new window)
- LDAP - 使用 Thunderbird / Outlook 查尋通訊錄 (new window)
- LDAP - 整合 Linux user login (new window)
- LDAP - OpenLDAP 和 Postfix 的整合應用 (new window)
- LDAP - LDAP with TLS/SSL (new window)
- LDAP - Replication (new window)

LDAP 架構

如果您是依照之前文章的架構來實做，那麼您應該有一個主要的 LDAP Server，現在我們就為 l-penguin Corp. 公司再建立一個高雄子公司的 LDAP，當要查詢高雄的資料時，就會直接依 LDAP 的參照查下去。

也就是說，我們加了一條：

l-penguin.idv.tw -> company -> branch -> ldap-kh

是的，就如您所想的一樣，必需還要再加入一個 branch 的 ou，並且還要為 kh 做一個指定的參照。

設定總公司 LDAP

當然了，小弟會把新增一個 ou 的技巧視為您已經必需有的知識，所以在此只列出 ldap-kh 的做法。

```
dn: ou=kh,ou=branch,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: kh
objectClass: extensibleObject
objectClass: referral
ref: ldap://ldap-kh.l-penguin.idv.tw/ou=ldap-kh,dc=l-penguin,dc=idv,dc=tw
```

上序所指示的，需要使用到 extensibleObject 及 referral 這兩個 objectClass。另外 ref 項目就是指定要向那一台 LDAP Server 做查詢。

好吧好吧！小弟真的不是有意要猜中，此時的你應該會想說如果有一個現成的檔案下載就好了，我已經聽到您的聲音，所以就請點 這裡 來下載為您準備好的 branch ldif 檔囉！

新增 LDIF

不知您是否還記得如何新增一個 ldif 檔案的命令，您可以使用下列方法來新增。

```
root # ldapadd -H ldap://ldap.l-penguin.idv.tw/ -D "cn=Manager,dc=l-
penguin,dc=idv,dc=tw" -w secret -x -f /etc/openldap/data/branch.ldif
root #
```

新建完成之後，也許您會想要看看是否已成功建立。

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

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

# search reference
ref: ldap://ldap-kh.l-penguin.idv.tw/ou=ldap-kh,dc=l-penguin,dc=idv,dc=tw??sub

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 1
# numReferences: 1
root #
```

設定 ldap-kh.l-penguin.idv.tw

設定 slap.conf

當然了，您需要先設定好 slapd.conf 檔案之後才可以匯入 LDIF 檔案。

```
root # vi /etc/openldap/slapd.conf
-----------------------------------------------------------------
# 直接設定 ou 的 root suffix。
suffix "ou=ldap-kh,dc=l-penguin,dc=idv,dc=tw"
rootdn "cn=Manager,ou=ldap-kh,dc=l-penguin,dc=idv,dc=tw"
rootpw secret

# 若找不到名錄，則向上尋找指定的名錄伺服器。
referral ldap://ldap.l-penguin.idv.tw:389/
-----------------------------------------------------------------
root #
```

嗯，建立 ldap-kh.l-penguin.idv.tw 的方法就如同建立一個總公司名錄的方法是一樣的，只不過他的 parent 是 l-penguin.idv.tw。

對於 ldap-kh 而言，首先就是要先建立 ou=ldap-kh,dc=l-penguin,dc=idv,dc=tw 這個 dn，因為你的 ldap.l-penguin.idv.tw 已指向他了，所以必需要如此做才行，否則在查尋時會對應不到。以下是 ldap-kh 的 ou LDIF。

```
#kh branch top

dn: ou=ldap-kh,dc=l-penguin,dc=idv,dc=tw
ou: ldap-kh
objectClass: organizationalUnit
```

以上就是要建立的 ou 項目。一樣的，小弟還是知道您在尋找到底那裡可以下載這個 LDIF，請按 這裡 吧！

匯入 LDIF 檔

使用以下方式就可以簡單的匯入

```
root # slapadd -v -l /etc/openldap/data/kh-root.ldif
added: "ou=ldap-kh,dc=l-penguin,dc=idv,dc=tw" (00000002)
root #
```

好了，當您使用 slapadd 之後，您應該要知道需要啟動 ldap。

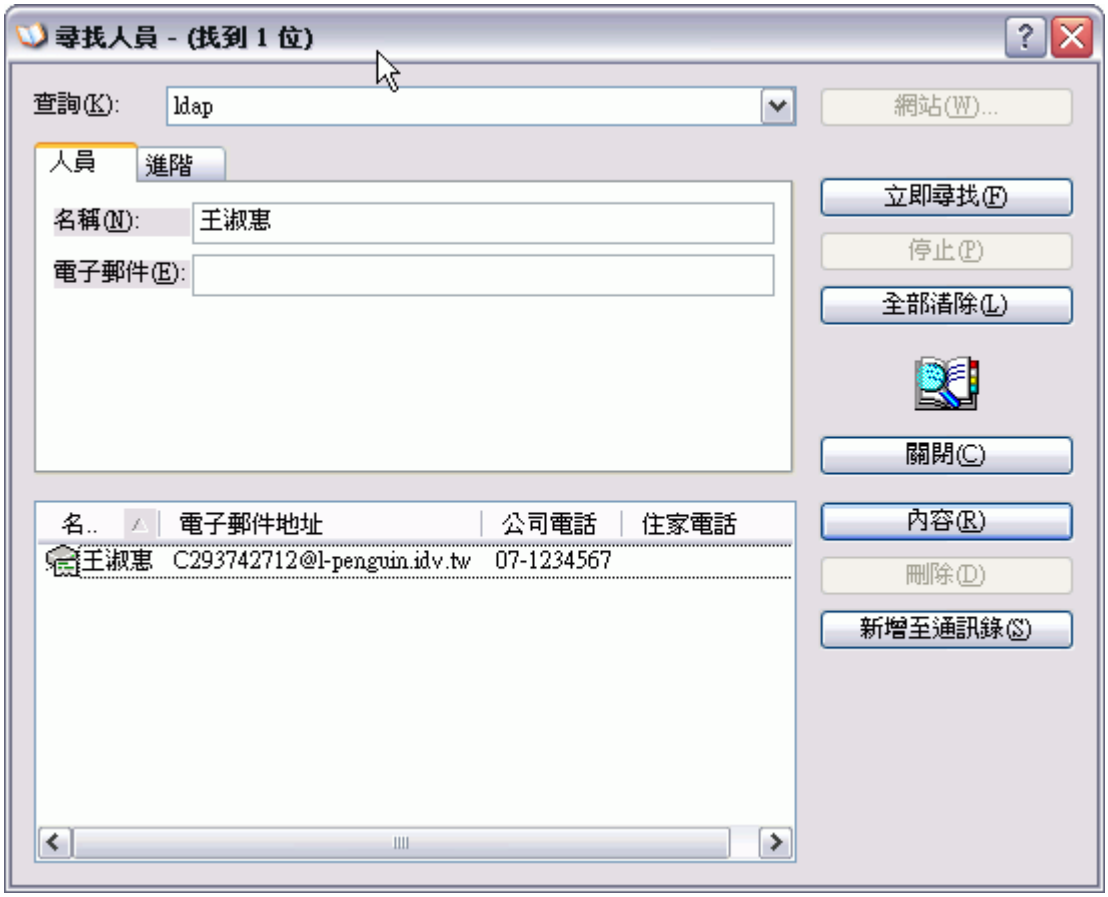
建立單位人員通訊錄

有了單位的 ou，那麼應該可以馬上想到需要有人員名錄，沒關係，在您努力的嘗試建立測試用名錄時，小弟又貼心的幫您貼上這個人員名錄 LDIF 檔了，請點選 這裡 下載。

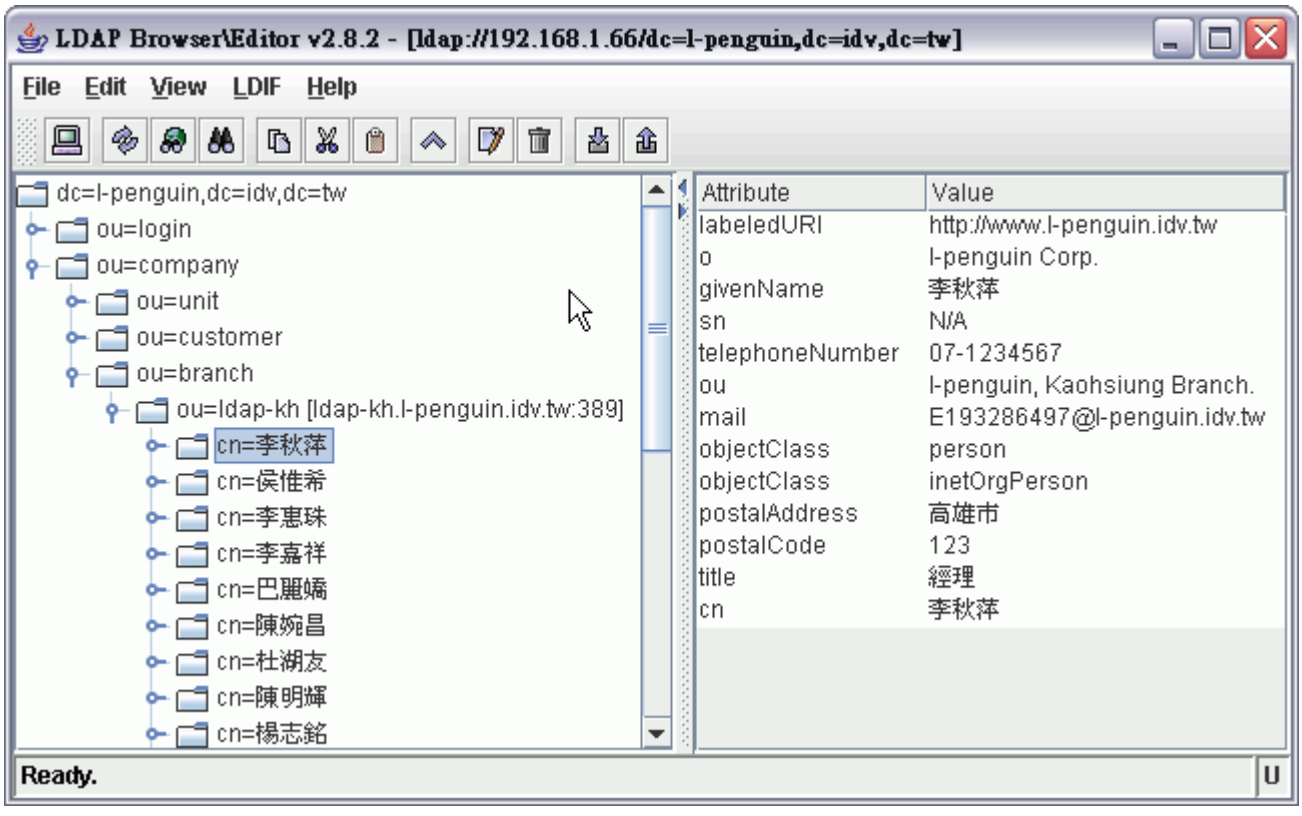
當然了，你所下載好的名錄是已轉存成 UTF8 格式檔案，所以就不需要再使用 iconv 轉一次囉。

```
root # ldapadd -H ldap://ldap-kh.l-penguin.idv.tw -D "cn=Manager,ou=ldap-
kh,dc=l-penguin,dc=idv,dc=tw" -w secret -x -f kh-usr.ldif.utf8
root #
```

使用 Outlook 測試



使用 LDAP Browser 測試



使用 ldapsearch 測試

也許聰明的你已經知道可以使 ldapsearch 來測試看看是否正確，但預設 ldapsearch 並不會依參照去詢找 ldap-kh.l-penguin.idv.tw 的名錄，就像如下所示：

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

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

# search reference
ref: ldap://ldap-kh.l-penguin.idv.tw/ou=ldap-kh,dc=l-penguin,dc=idv,dc=tw??sub

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 1
# numReferences: 1
root #
```

這真是糟糕，怎麼找不到 ou=branch,ou=company,dc=l-penguin,dc=idv,dc=tw 之下的名錄呢，現在，請您再加上一個 -C 參數，就可以讓 ldapsearch 依參照指示繼續搜尋。

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

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

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

# E69D8EE7A78BE8908D, ldap-kh, l-penguin.idv.tw
dn:: Y2495p2O56eL6JCNLG91PWxkYXAta2gsZGM9bC1wZW5ndWluLGRjPWlkdixkYz10dw==
cn:: 5p2O56eL6JCN
sn: N/A
objectClass: person
~ 以下略 ~
root #
```

後記：

小弟到目前為止，一共寫了七篇有關 OpenLDAP 的實例與應用，在一次偶然的情況之下，發現大家對 LDAP 入門 (new window) 有很多的閱讀次數，而在 Google 的查尋之下也發現 LDAP 入門 有很多人連結，小弟在此跟各位說聲感謝。

LDAP 應用無限寬廣，很多應用需要有環境配合才有辦法做出實例，希望小弟這幾篇的文章能帶動更多 LDAP 的先進們一同寫出 LDAP 的實例應用，達到拋磚引玉的效果。

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/)