LDAP 入門

參考書籍

- LDAP 系統管理 (O'Reilly, ISBN: 986-7794-21-4)
- http://www.openldap.org/doc/admin23/index.html

現今網路常用的服務，以 HTTP、Mail 和 File System (Samba) 爲最常用的服務，然而在這些常用的服務裡，會有使用者帳號的問題，每當要使用 Mail 時要輸入 Mail 的帳號密碼，存取 File System 要有 File System 帳號密碼，再更多的服務就要記更多的帳號密碼，小弟曾看過某機關，一位承辦人居要要背五組以上的的帳號密碼，而每兩個月又要修改一次，想想看這是多麼恐怖 的一件事。LDAP 是一種目錄服務，可使用 LDAP 記錄各種的人員資訊，就像是通訊錄一樣，又更進階一點，他也可以拿來做帳號整合，若是在 AP 上都有所支援，那麼要使用同一組帳號秘碼就不再是難以搞定的事了。

在小弟等當兵的這一段日子裡，打算使用 LDAP 來做 Linux login、Postfix、Samba、HTTP 等帳號密碼整合。所以，我將會寫一系列的 LDAP 整合文章，當然，太深入、難以說明或是太過於理論的地方我都不會講，因爲這只是筆記，我會儘量說明清楚。爲了要讓閱讀本文章的讀者們可以更容易的找到相關書籍，我在文章裡也會提供參考圖書或網頁的資料。

無論如何，小弟只對 Redhat Linux 的部份較爲熟悉，所以在以下文章裡所提到的 LDAP，其實是指 OpenLDAP 套件，跟 Microsoft 的 Active Directory 沒有關係，因爲小弟對 AD 也不熟。

在這個章節裡，我將要介紹基本的 LDAP 觀念和如何使者用 ldap command 來新增、查尋資料。而在實作的環境裡，我是使用 CentOS 4.0，也就是說若您的系統是使用 CentOS 4、Redhat Enterprise Linux 4、Fedora Core 3 或 Fedora Core 4 的話應該都可以照著本文章實作，當然，CentOS 4.0 裡附的 OpenLDAP 版本是 openldap-2.2。

安裝

要實作 LDAP 的話，當然一定要安裝 LDAP 套件了，包含了 server 及 devel 相關的套件，你可以查看系統有無 LDAP Server 套件。

```
root # rpm -qa | grep openldap
openldap-2.2.13-2
openldap-devel-2.2.13-2
openldap-servers-2.2.13-2
openldap-clients-2.2.13-2
root #
```

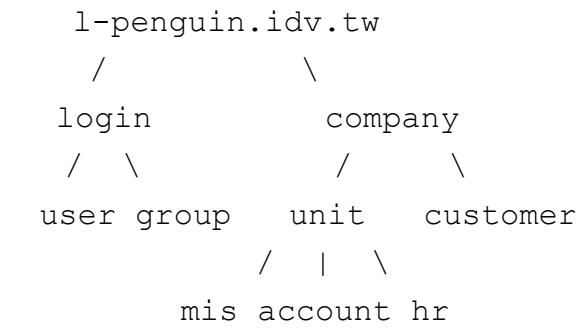
若沒有的話，可使用 CentOS 4 光碟所附的 RPM 來安裝就可以了。

```
root # rpm -ivh openldap*
```

```
~ 中間略 ~
root #
```

規劃

其實 LDAP 也不用想得太難，把他想成資料庫的一種就對了，對於有資料庫設計經驗的人應該不成問題，但是若你之前都沒有碰過，那就把 LDAP 想成組織圖一樣就可以了，只是這個組織圖是在你腦海裡浮現，所以你最好要再準備一張紙，把你的架構畫出來才行。就我這次提供的組織來看，大約是以下這樣：



爲了這次的實做，我把這個 l-penguin.idv.tw 分成主要兩個部份，login 部份是用來做有關 login 的資料，所有有關 login 的機制都是放在這裡。而 company 裡面，就只單純提供通訊錄的查尋而已。而這個架構圖，在之後的 LDAP 系列文件裡，還會出現，我現在的實做，是以 l-penguin.idv.tw -> company -> unit 這個路線走，在最後的結果，可以查到在每個部份下的人員。

Note: 這個部份，我還沒有講到 LDAP 的表示法，主要是要讓各位讀者明白，在使用 LDAP 之前要先有一個架構，畫出來再依圖實做就會很好理解。這個部份，可以參考 LDAP 系統管理 第二章 LDAPv3 概論。

LDAP 表示法

若要表示一筆人員記錄，可使用：

```
cn=user name,ou=gourp,dc=your,dc=domain
```

若是以本例來說，在 mis 部門下有一位 steven，那麼對於這位 steven 的表示法爲：

```
cn=steven,ou=mis,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
```

這一長串，我們稱之爲一個 dn 值，在 LDAP 的表示方法都是由小到大，也就是人名先表示、再表示部門、單位（這和老外的門牌表示法是一樣的意思）。

當然，經過這麼一說你就可以知道 cn 值在同一個 ou 下是不可以重複的，就是說在 ou=mis 下不可以有兩位 steven，不然就照成資料重複。當然，在同一公司裡叫 steven 的人可能到處跑，但是同一部門下同時叫 steven 的機率就就會降低了。

LDAP 也可以使用中文，比方說小弟是在 mis 部門下的，若依名字設定 dn 的話，

就會變成：

```
cn=廖子儀,ou=mis,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
```

相信，有了中文的支援下，大家對 LDAP 應該不會太排斥才對。

主要設定檔

在使用 LDAP 之前，一定要先設定好主要設定檔，如此才能讓你的 LDAP 正常使用。OpenLDAP 主要設定檔在 /etc/openldap/slapd.conf，這個 slapd.conf 若要各位用手打出來可能會讓大家反彈，所幸裡面已經有最主要的設定了，這些設定可以符合大部份的需求，剩下來的只需要一些微調而已。

Note: 主要設定檔, 在 **LDAP** 系統管理 第三章 **OpenLDAP** 裡可得到詳細資訊。

```
root # vi /etc/openldap/slapd.conf
==========================================
suffix "dc=l-penguin,dc=idv,dc=tw"
rootdn "cn=Manager,dc=l-penguin,dc=idv,dc=tw"
rootpw secret
==========================================
```

好了，三行，三行就符合本篇的主要設定，現在我就來解釋一下這三行的意思：

- suffix "dc=l-penguin,dc=idv,dc=tw"
  suffix 就是用來定義你 LDAP 的根尾碼
- rootdn "cn=Manager,dc=l-penguin,dc=idv,dc=tw"
  Unix/Linux root 裡有至高無尚的地位，可以打破任何規定，而在這裡，這個 rootdn 就是指 LDAP 的 root，設定了之後就可以對整個 LDAP 系統資料做新增、刪除、修改等動作。一般 cn 值會是 Manager。
- rootpw secret
  故名思意就是指定剛剛那個 Manager 的密碼，而在這個範例中，我們是使用 secret 這個明碼的文字，當然是爲了解說方便，真正在管理時還是以加密過的文字較爲安全。

設定完之後，你應該可以體會到這個 slapd.conf 有多重要，因爲裡面包含了最大權限管理者的帳號密碼，所以除了相關帳號之外，應該不允許有其它人修改和閱讀。

設計機關檔 / 啓動 **ldap**

當完成最主要的設定之後，系統內不會有任何資料，所以我們必需逐步建立，當然最重要的是機關設定吧！

記錄資訊的格式我們一般取爲 *.ldif 檔，一般第一次接觸會顯得很陌生，在這裡我將設計一個符合我規劃的 LDIF 檔案，並存在 /etc/openldap/data/root-unit.ldif 檔裡：

```
# root node
dn: dc=l-penguin,dc=idv,dc=tw
dc: l-penguin
objectClass: dcObject
objectClass: organizationalUnit
ou: l-penguin Dot idv Dot tw
#login top
dn: ou=login,dc=l-penguin,dc=idv,dc=tw
ou: login
objectClass: organizationalUnit
#user, uid, password
dn: ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw
ou: user
objectClass: organizationalUnit
#group
dn: ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw
ou: group
objectClass: organizationalUnit
##for company organization top
dn: ou=company,dc=l-penguin,dc=idv,dc=tw
ou: company
objectClass: organizationalUnit
#for company organization (unit)
dn: ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: unit
objectClass: organizationalUnit
#human resource (under unit)
dn: ou=hr,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: hr
objectClass: organizationalUnit
#MIS (under unit)
dn: ou=mis,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: mis
objectClass: organizationalUnit
#Account (under unit)
dn: ou=account,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: account
```

```
objectClass: organizationalUnit
# for customers information
dn: ou=customer,ou=company,dc=l-penguin,dc=idv,dc=tw
ou: customer
objectClass: organizationalUnit
```

好的，以上我們是一層一層的規劃下來，每一筆新的記錄和前一筆新記錄要使用一行空白行來隔開表示示別；而每一筆一開頭就要表示這筆資料的完整 dn 值，就像是絕對路徑一樣；在每一筆資料的參數裡，可以自行選用要使用那些 objectClass。

當然，各位若不想用手慢慢 key 這些無聊的文字，可以由此下載 root-unit.ldif 檔案。現在設定完了之後，我們要這些機關新增到 LDAP 裡，可以使用 slapadd 來新增：

```
root # slapadd -v -l /etc/openldap/data/root-unit.ldif
added: "ou=login,dc=l-penguin,dc=idv,dc=tw" (00000005)
added: "ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw" (00000006)
added: "ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw" (00000007)
added: "ou=company,dc=l-penguin,dc=idv,dc=tw" (00000008)
added: "ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw" (00000009)
added: "ou=hr,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw"
(0000000a)
added: "ou=mis,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw"
(0000000b)
added: "ou=account,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw"
(0000000c)
added: "ou=customer,ou=company,dc=l-penguin,dc=idv,dc=tw" (0000000d)
root #
```

現在你可以很清楚的看到，你的機關名錄都被新增進去了！

若確定了之後，再來就啓動 DLAP 吧，若你和我一樣是由 RPM 安裝的，就很簡單了：

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

這樣就完成了！

Note: 在使用 slap* 工具之前，並不可以啓動 LDAP。

再來，查看 LDAP 資料錄，下面的指令可以查看所有項目：

```
root # ldapsearch -x -b "dc=l-penguin,dc=idv,dc=tw"
# extended LDIF
```

```
#
# LDAPv3
# base <dc=l-penguin,dc=idv,dc=tw> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#
# l-penguin.idv.tw
dn: dc=l-penguin,dc=idv,dc=tw
dc: l-penguin
ou: l-penguin Dot idv Dot tw
objectClass: dcObject
objectClass: organizationalUnit
# login, l-penguin.idv.tw
dn: ou=login,dc=l-penguin,dc=idv,dc=tw
ou: login
objectClass: organizationalUnit
# user, login, l-penguin.idv.tw
dn: ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw
ou: user
objectClass: organizationalUnit
# group, login, l-penguin.idv.tw
dn: ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw
ou: group
objectClass: organizationalUnit
~ 其它略 ~
# search result
search: 2
result: 0 Success
# numResponses: 11
# numEntries: 10
root #
```

你得到的結果會是一長串的項目，雖然有可能會看不懂，但你最少可以確定剛剛新增的資料都有成功的進去。對於一開始接觸 LDAP 的各位讀者，一長串總比“什麼都沒有”來得好吧 :)

設計人員名錄

人員名錄和機關設計原理一樣，也是使用文字檔的 ldif 來做設計。在這裡我準備新增幾個人員加入到各不同的單位裡，當然所示範的資料裡人員或身份證都是

瞎掰杜撰的 ^^
我把設定檔存成 /etc/openldap/data/users.ldif

```
#設定 吳怡君 通訊錄
dn: cn=吳怡君,ou=hr,ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw
cn: 吳怡君
sn: N/A
objectclass: person
objectclass: inetOrgPerson
givenName: 吳怡君
mail: c293831287@l-penguin.idv.tw
telephoneNumber: 02-29587572
mobile: 0939689593
postalAddress: 台北縣中和市景平路 1 號
postalCode: 235
ou: 人力資源部
o: l-penguin Corp.
labeledURI: http://www.l-penguin.idv.tw/
title: 辦事員
```

礙於篇幅上面這只是一個人員的資料而已，這位隸屬於人事資源部的吳小姐 (?!) ，我使用了 inetOrgPerson 和 person 這兩個 objectclass。其它的請望文生意吧，尤其是你不應該再問那個 dn: 值是什麼意思。有一點值得題的是，上面 sn: 這個參數，其實是“姓”啦！
對於開始規劃使用 LDAP 的公司來說，要手動 key 這些名錄可能會死人，你可以請工讀生幫忙做這些鎖事，或是略施小計，使用 Shell Script 或 Perl 來產生吧這樣就可以很快的建立這些名錄了。
好吧，我還是知道有人先抱著玩玩的心態來做實驗，但是又沒有現成的人名資料可以參考，那麼我就把本次的 users.ldif 給各位下載了。

Note: 關於 inetOrgPerson 和 person 這兩個 objectClass 可以查閱 *LDAP 系統管理* 第四章 *4.2* 定義綱要。

新增人員名錄
建立好人員名錄之後，請得要注意下列幾項：

- 轉換到 unix 格式
- 中文字元和 UTF-8

我相信，很多人一定是在 Windows 編好 ldif 檔之後再傳到主機上，但是在 Windows 編好的文件，有經驗的使用者會發現用 vi 一打開之後每一行的最後面會多一種 ^M 的字元，這種字元在 Linux 可是不被認得的，若沒有消除就會造成新增錯誤。你可以使用 vi 取代掉，或是使用更簡單的方法，讓 dos2unix 來幫

你做：

```
root # dos2unix /etc/openldap/data/users.ldif
root #
```

中文字元的問題，因爲在 Windows 編完之後，會使用 Big5 編碼，所以，我們要把他轉成 UTF-8 字元，爲什麼？因爲 LDAP 就規定了 ldif 文件需要使用 UTF-8 格式，這樣子明白了吧！要讓 Big5 變成 UTF-8 可以使用 iconv 這個程式來轉換：

```
root # iconv -f big5 -t UTF-8 -o users.ldif.utf8 users.ldif
root # file users.ldif.utf8
users.ldif.utf8: UTF-8 Unicode text
root #
```

好了，經過一翻煩雜的設定之後就可以開始來新增資料了，新增資料可使用 ldapmodify 來完成任務：

```
root # ldapmodify -D "cn=Manager,dc=l-penguin,dc=idv,dc=tw" -w secret -x -a -f /etc/openldap/data/users.ldif.utf8
~ 中間略 ~
root #
```

好了，若中間沒有發生任何的問題，就表示新增成功，一樣我們使用 ldapsearch 來查看吧：

```
root # ldapsearch -x -b "ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw"
# extended LDIF
#
# LDAPv3
# base <ou=unit,ou=company,dc=l-penguin,dc=idv,dc=tw> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#
~ 略 ~
# \E9\BB\83\E6\80\A1\E9\9A\86, hr, unit, company, l-penguin.idv.tw
dn::
Y2496buD5oCh6ZqGLG91PWhyLG91PXVuaXQsb3U9Y29tcGFueSxkYz1sLXBlbmd1aW4sZ
GM9a
WR2LGRjPXR3
cn:: 6buD5oCh6ZqG
sn: N/A
objectClass: top
objectClass: person
```

```
objectClass: inetOrgPerson
givenName:: 6buD5oCh6ZqG
mail: d197700415@l-penguin.idv.tw
telephoneNumber: 02-29587572
mobile: 0939689593
postalAddress:: 5Y+w5YyX57ij5Lit5ZKM5biC5pmv5bmz6LevMeiZnw==
postalCode: 235
ou:: 5Lq65Yqb6LOH5rqQ
o: l-penguin Corp.
labeledURI: http://www.l-penguin.idv.tw/
title:: 5Lq65LqL6LOH5rqQ6YOo5Li75Lu7
# \E5\90\B3\E5\AE\B6\E8\87\BB, hr, unit, company, l-penguin.idv.tw
dn::
Y2495ZCz5a626Ie7LG91PWhyLG91PXVuaXQsb3U9Y29tcGFueSxkYz1sLXBlbmd1aW4sZ
GM9a
WR2LGRjPXR3
cn:: 5ZCz5a626Ie7
sn: N/A
objectClass: top
objectClass: person
objectClass: inetOrgPerson
givenName:: 5ZCz5a626Ie7
mail: d295723341@l-penguin.idv.tw
telephoneNumber: 02-29587572
mobile: 0939689593
postalAddress:: 5Y+w5YyX57ij5Lit5ZKM5biC5pmv5bmz6LevMeiZnw==
postalCode: 235
ou:: 5Lq65Yqb6LOH5rqQ
o: l-penguin Corp.
labeledURI: http://www.l-penguin.idv.tw/
title:: 6L6m5LqL5ZOh
~ 略 ~
# search result
search: 2
result: 0 Success
# numResponses: 22
# numEntries: 21
root #
```

GUI 工具

哎呀，人客呀，大家一看到這個小單元，可能會認爲自己又誤上賊船了，千辛萬苦努力看完前面的廢話之後居然又出現一個 GUI 工具，但是，大家千萬不要認爲小弟誘拐大家上賊船，明明有很方便的 GUI 工具還不放在第一個介紹～

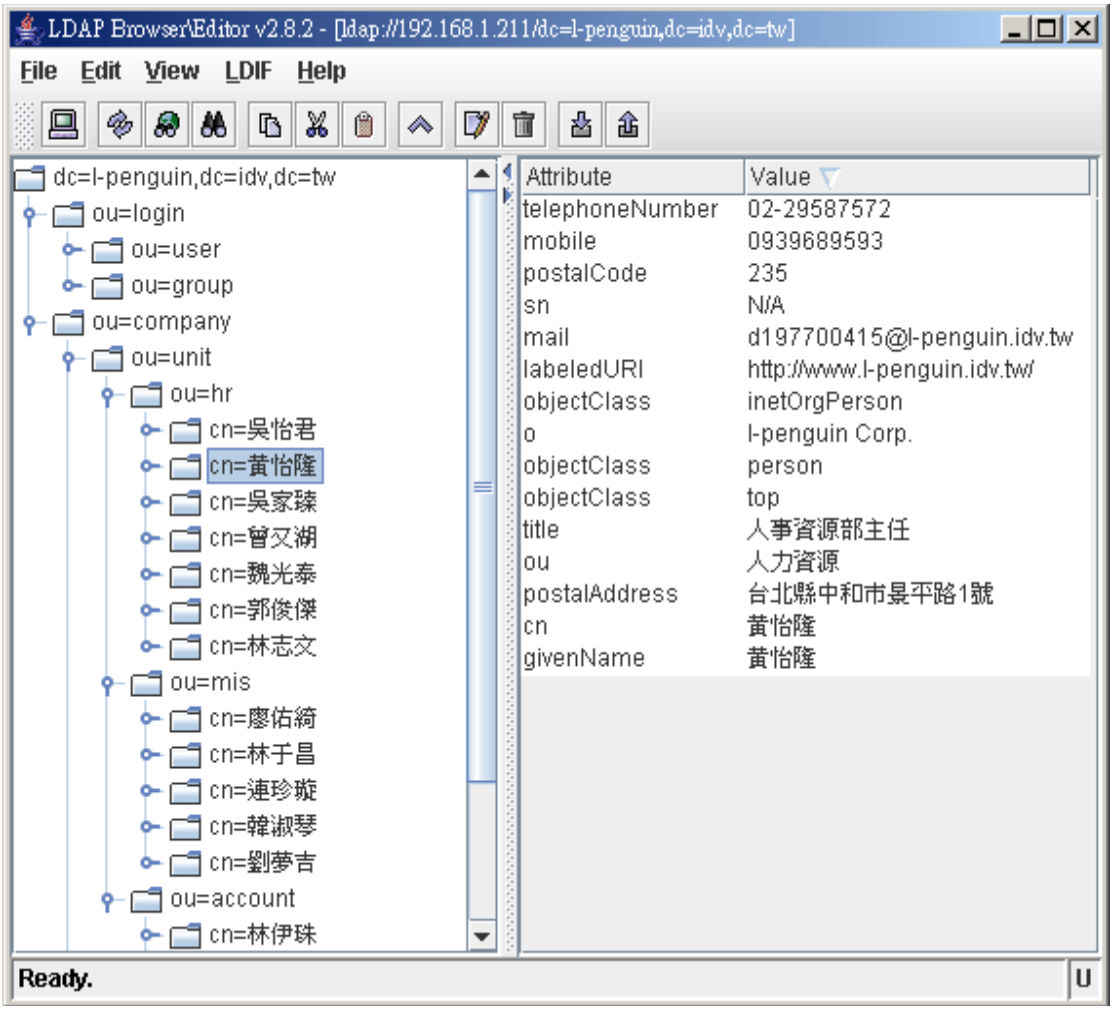
可別誤會呀，若各位是從頭開始看的話，那麼已經可以開始使用文字模式來新增了，GUI 只是一種輔助而已，若是不了解其原理，那麼就算有 GUI 工具還是無法使用順手。

在這裡我介紹的 GUI 工具是 ldapbrowser，這工具可用來新增、移除、修改你的資料。使用方法就由各位去發現吧！

名稱：ldapbrowser

首頁：http://www-unix.mcs.anl.gov/~gawor/ldap/

下載：http://www-unix.mcs.anl.gov/~gawor/ldap/download.html



後記：

套一句 LDAP 系統管理 作者講的話，學習 LDAP 就像跳傘一樣，當越接近地面時，事物會變得越來越清晰。在此小弟實在是非常強力的推薦 LDAP 系統管理這本書，它在理論上解釋的非常清楚，如果有時間的話這本書應該要好好讀一次

以了解 LDAP 其中的原理。
當然最新最快更新的文件還是 OpenLDAP 官方的文件，但因爲是英文版的我想一開始會讓很多人打退堂鼓，其實這是不必要的，當你閱讀了官方線上文件之後，很多問題都會發現其實都有解決方案。

本文原始網頁：
http://ms.ntcb.edu.tw/~steven/article/ldap-1.htm