LDAP - 整合 Linux user login

參考資料

- LDAP 系統管理 (O'Reilly, ISBN: 986-7794-21-4)

Server 的設定與資料新增

自從 Sun 推出了 Sun Yellow Pages (就是現在在 Unix/Linux 常聽到的 Network Information Service，NIS) 之後，Unix/Linux 的帳號管理就有了完整的統一方案，在此，我在這裡介紹如何使用 LDAP 統一帳帳號密碼的管理。

schema 與 **Attribute** 設定

LDAP 裡，只要引入 nis.schema 就可以使用和 Linux 登入相關的 attribute。要引用這個 nis.schema 可在 /etc/openldap/slapd.conf 設定：

```
root # vi /etc/openldap/slapd.conf
====================================
include /etc/openldap/schema/nis.schema
====================================
```

加入這一行之後，再重新啓動 ldap 服務：

```
root # service ldap restart
root #
```

/etc/passwd、**/etc/shadow** 和 **/etc/group**

大家都知道，/etc/passwd 是存放個人的帳號資料，而 /etc/shadow 是存放著個人的密碼資訊，而 /etc/passwd 格式應該像下面這樣：

```
steven:x:500:500::/home/steven:/bin/bash
```

也就是：

```
id:password:uid:gid:full_name:Home Directory:Login shell
```

這樣的格式，然而，在 Linux login 時，對於 LDAP 也要引用相關的 atrribute 才可以正確對應登入，下表爲 posix /etc/passwd 和 LDAP 的對應：

objectClass: posixAccount	
id	uid
password	userPassword
uid	uidNumber
gid	gidNumber
full_name	gecos
Home Directory	homeDirectory
Login shell	loginShell

上表可以很清楚的看到，若是要讓設計 ldif 檔的話，最少需要引用 posixAccount 這個 objectClass，並且設定必要的 attribute。

介紹完了 /etc/passwd 之後，另一個很重要的檔案，也就是記錄整個 Linux 主機的 user password 的檔案就是 /etc/shadow 這個檔，那麼他的格式是：

```
steven:$1$xGQPf1Cs$Y/kQw5TmUXvWY/1z3QgNZ/:13001:0:99999:7:::
```

他們的意義依序爲：

username:passwd:last:may:must:warn:expire:disable:reserved

好的，那麼和剛剛一樣，我來解釋一下要引用的 objectclass 和 attribute 對應：

objectClass: shadowAccount	
username	uid
password	userPassword
last	shadowLastChange
may	shadowMin
must	shadowMax
warn	shadowWarning
expire	shadowExpire
disable	shadowInactive
reserved	shadowFlag

上面也可以得知，在設計 ldif 時，除了要引用剛剛的 posixAccount，還有 shadowAccount 才行。

介紹完了兩個重要的 passwd 和 shadow 檔之後，再來就是群組檔 (/etc/group) 的問題啦！一樣的，也有對應的 attribute，但我還是先列出格式出來：

```
steven:x:500:
```

也就是：

```
group name:password:group id:other account
```

下面是 objectclass 和 attribute 的對應：

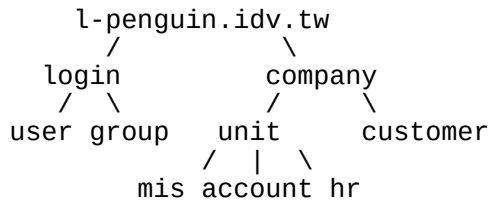
objectClass: posixGroup	
group name	cn
password	userPassword
group id	gidNumber
other account	memberUid

聰明的你一定之道我最後爲什麼要講 group 這個檔案，因爲 gorup 對系統管理也是很重要的一環，記得不要忘了 /etc/group。

註: 關於 /etc/passwd 和 /etc/shadow 的格式可參考 http://www.linux.org.tw/CLDP/HOWTO/admin/Shadow-Password-HOWTO/Shadow-Password -HOWTO-2.html，而 LDAP 和 login 的項目，可參考 **LDAP** 系統管理 第六章 取代 **NIS**。

LDIF 設編寫

現在我們再來看一次原本我們的目錄架構樹：



原本的計劃，就是要把 ou=login,dc=l-penguin,dc=idv,dc=tw 這條存放 user 的 login 資料，包含了帳號密碼，這個檔案我們放在 /etc/openldap/data/user-login.ldif，現在我們來看一下一個簡單的範列：

```
#設定 吳怡君 login
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: hrC293831287
shadowLastChange: 11108
shadowMax: 99999
shadowWarning: 7
shadowFlag: 0
loginShell: /bin/bash
uidNumber: 600
gidNumber: 510
homeDirectory: /home/c293831287
gecos: Nicole Coon
```

上面爲一位 吳怡君小姐 (?) 的 user-login 記錄，在這裡使用了 account、posixAccount 和 shadowAccount 等三個 objectclass，剩下的在前面已都有說明，在此就不再贅述。

當然，照例我還是請各位下載完整的 user-login.ldif 讓大家玩玩。

新增到 **LDAP** 資料庫

當 ldif 檔編較好了之後，我們需要把這些資料加入到 ldap 才可以使用，而 ldapmodify 就可以幫我們完成這個工作：

```
root # ldapmodify -D "cn=Manager,dc=l-penguin,dc=idv,dc=tw" -w secret -x -a -f /
etc/openldap/data/users-login.ldif.utf8
adding new entry "cn=c293831287,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=d197700415,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=d295723341,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=c297303122,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=d191627793,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=b192927969,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=c293190610,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=h191497299,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=b299479351,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=c291677874,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=b297933030,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=f296974826,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=b299136575,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
```

```
adding new entry "cn=e295689078,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=a293893990,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=f192426229,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
adding new entry "cn=d295380453,ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw"
root #
```

好了，若你有看過 LDAP 入門 (new window) 的話，應該知道可以使用 ldapsearch 這個指令來幫忙印出資料：

```
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 sub
# 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
shadowLastChange: 11108
shadowMax: 99999
shadowWarning: 7
shadowFlag: 0
loginShell: /bin/bash
uidNumber: 600
gidNumber: 510
homeDirectory: /home/c293831287
gecos: Nicole Coon
~ 以下略 ~
root #
```

建立 **Group** 資料並新增

現在我們來建立 Group 資料，如此才能正確查到 Group 的對應，而這個檔存放在 /etc/openldap/data/group.ldif：

```
#Human Resource
dn: cn=hr,ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw
objectClass: posixGroup
cn: hr
gidNumber: 510

#MIS
dn: cn=mis,ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw
objectClass: posixGroup
cn: mis
gidNumber: 511

#Account
dn: cn=account,ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw
objectClass: posixGroup
cn: account
```

```
gidNumber: 512
```

以上的三個 Group 分別爲 Human Resource、MIS 和 Account 群組，使用 posixGroup 這個 objectClass，記得，這次是要新在 ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw 這個 dn 下，而 group.ldif 請點這裡下載。

完成之後，一樣我們需要使用 ldapmodify 指令來幫我們做新增動作：

```
root # ldapmodify -D "cn=Manager,dc=l-penguin,dc=idv,dc=tw" -w secret -x -a -f /etc/openldap/data/group.ldif
adding new entry "cn=hr,ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw"

adding new entry "cn=mis,ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw"

adding new entry "cn=account,ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw"

root #
```

修改 **/etc/openldap/slapd.conf ACLs**

爲什麼還需要修改 slapd.conf 呢？看看上面的範例，裡面是否包含了一個很重要的項目就是 password，如果不加一限制的話，那麼不就每個人都可以查到別人的 password 了呢！那麼這麼的存取控制，就是要讓 userPassword 這個 attribute 只能用來做認證，並且只有 user 自己可以修改密碼：

```
root # vi /etc/openldap/slapd.conf
=========================================
# userPassword 只能用來做認證用，只有 user 自己才能修改密碼。
access to * attr=userPassword
by self write
by * auth

# 預設 ACL，大家只能讀取。
access to *
by * read
=========================================
```

修改完之後，記得重新啓動 ldap。

如此就完成了 LDAP Server 端的資料匯整了。

Note: slapd.conf ACLs 的相關說明，可以參考 **LDAP** 系統管理 第三章 **3.6** 存取控制清單 **(ACL)**。

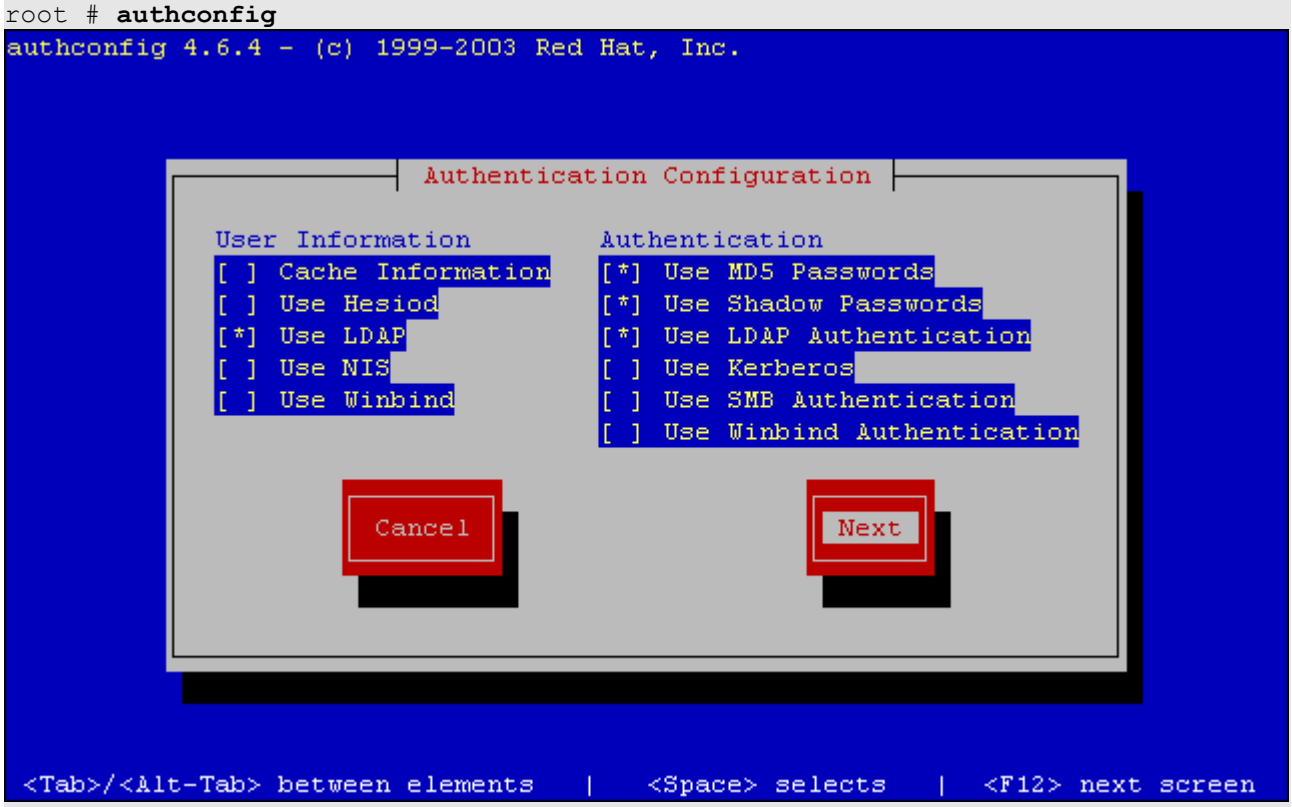
Linux Client 調整

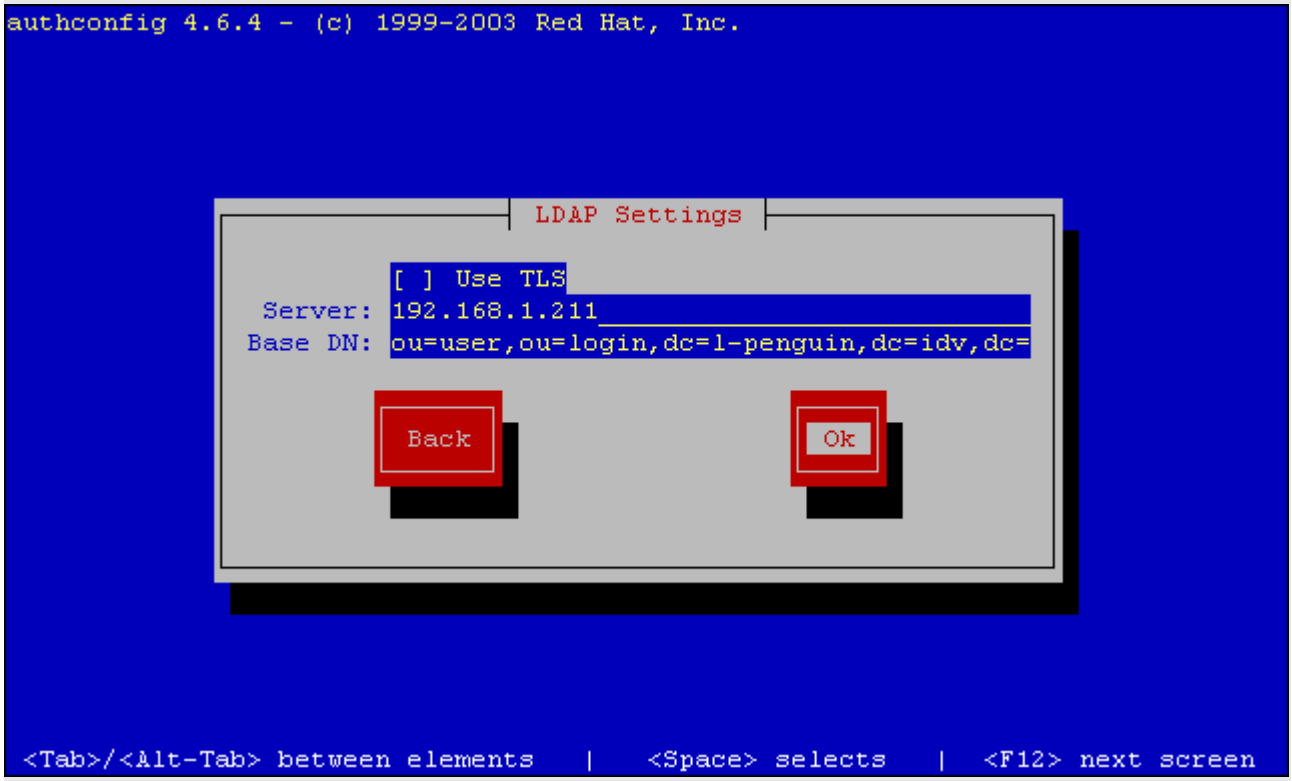
因爲我們現在所有的 Linux Login 都是使用 LDAP 來做帳號統整，所以在 Client 必需調整一下才行。Linux Client 如何做調整呢，記得在做 NIS 時，是使用 PAM 模組來做認證，若使用 LDAP 怎麼辦呢，沒關係，我們還是有相關的 LDAP PAM 模組可以使用，你可能在網路上看到很多說明文件，PAM 要調整一堆又不能打錯字，否則會造成系統無法進入等問題。

若是使用 Redhat 系的 Linux，那麼這些調整 PAM 的事就可以請 authconfig 來代勞了！

首先，我們這台 Client IP 爲 192.168.1.212，LDAP Server 是 192.168.1.211，所以在登入 192.168.1.212 之後，馬上就可以使用 authconfig 來做調整了：

```
root # authconfig
```





上面的那個 Base DN 就輸入的就是 ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw 這個 dn 值，當然 Server 就不用說了吧！

做好之後，我們還有一個小地方需要修改，因爲我們的 user account 和 group 是分別在不同的 dn 之下，所以要修改一下 /etc/ldap.conf 才可以找正確的 group：

```
root # vi /etc/openldap.conf
====================================
nss_base_group ou=group,ou=login,dc=l-penguin,dc=idv,dc=tw
====================================
```

好了，修改好之後就請隨便找一個使用者登入吧！

```
login as: b299136575
b299136575@192.168.1.212's password: your-password
Could not chdir to home directory /home/b299136575: No such file or directory
-bash-3.00$ passwd
Changing password for user b299136575.
Enter login(LDAP) password: your-password
New UNIX password: your-new-password
Retype new UNIX password: your-new-password
LDAP password information changed for b299136575
passwd: all authentication tokens updated successfully.
-bash-3.00$
```

可以修改密碼，那麼來看看 group 是否對應正確（是向 LDAP 所要求的資料而來）：

```
-bash-3.00$ id
uid=612(b299136575) gid=512(account) groups=512(account)
-bash-3.00$
```

Note: 在使用 LDAP 帳號登入時，會出現 "Could not chdir to home directory /home/b299136575: No such file or directory" 這個錯誤訊息是很正常的，因爲你並沒有建立 User Home Directory 怎麼會找得到家目錄呢！所以您可以再建立該使用者的 Home Directory 就可以了。當然如果你的單位有提供 File Server，我非常建議使用 NFS 的方法並搭配 automount 來掛載使用者家目錄。

NFS 的方法：man 5 exports
automount 的方法：man 5 auto.master

本文原始網頁：
http://ms.ntcb.edu.tw/~steven/article/ldap-3.htm