OpenLDAP 和 Postfix 的整合應用

先前小弟在前三篇文章中提到一些 LDAP 的應用，經過了五、六個月之久，最近終於有機會來實作 Postfix 和 OpenLDAP 的整合，老實說在實作過程中遇到了不少困難，所幸 postfix.org 的豐富文件讓我解開了不少棘手問題。

實作之前，我先說明一下測試環境：

兩台主機分別為 vm-ldap 和 vm-mail，vm-ldap 上面只有跑 OpenLDAP；而 vm-mail 則是負責郵件服務，當然了，郵件系統是使用 postfix。 這次的實作過程，主要是測試如何讓 postfix 去查詢 OpenLDAP 的資料庫資料，也會示範如何編寫 ldap_table 讓 postfix 去做查詢的依據，以下所以的範例，都可以在文章的連結中找得到。

建立 LDAP 環境：

我們沿用先前的環境，先做出 LDAP 的設定檔，再匯入到資料庫中，中間的實作過程，可以參考 LDAP 入門 (New Window)一文，在這裡我就不再贅述。

建立 postfix 環境：

在建立 postfix 環境之前，因為我們是要查詢 LDAP 資料錄，所以要先讓 postfix 支援 LDAP 才行，在你的系統之中，以 Redhat 系為例的話，最少需要裝有 openldap 套件才可以。

```
root # yum install openldap
```

安裝完成之後，就可以開始編釋 postfix 了。

```
root # cd /misc
root # wget
ftp://postfix.cdpa.nsysu.edu.tw/Unix/Mail/Postfix/official/postfix-2.
3.0.tar.gz
root # cd postfix-2.3.0
root # make tidy
root # make makefiles CCARGS="-I/usr/local/include -DHAS_LDAP"
AUXLIBS="-L/usr/local/lib -R/usr/local/lib -lldap -L/usr/local/lib
-R/usr/local/lib -llber"
```

上面的過程，會重新建立 mailfile 檔案，並且把 LDAP 的支援也加進去。設定好 Makefile 之後，接下來的安裝設定，都跟一般過程一樣，你可以參考 Mail Server - Postfix 安裝 (New Window) 一文。

安裝完成之後，請使用 postconf 工具看看你的 postfix 對 ldap 是否支援。

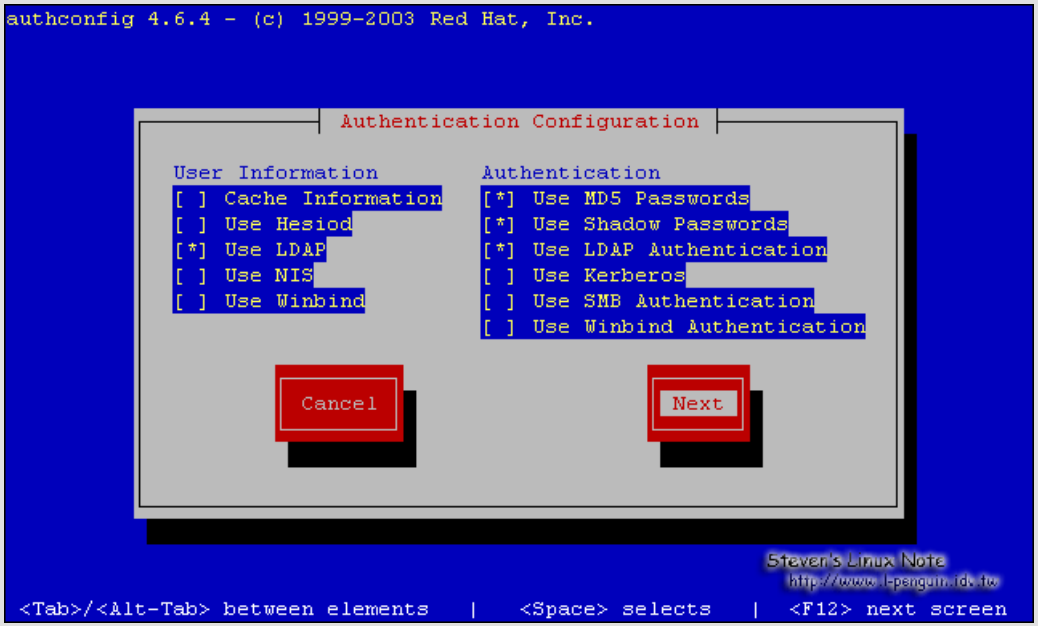
```
root # postconf -m
btree
cidr
environ
hash
ldap
nis
proxy
regexp
static
unix
root #
```

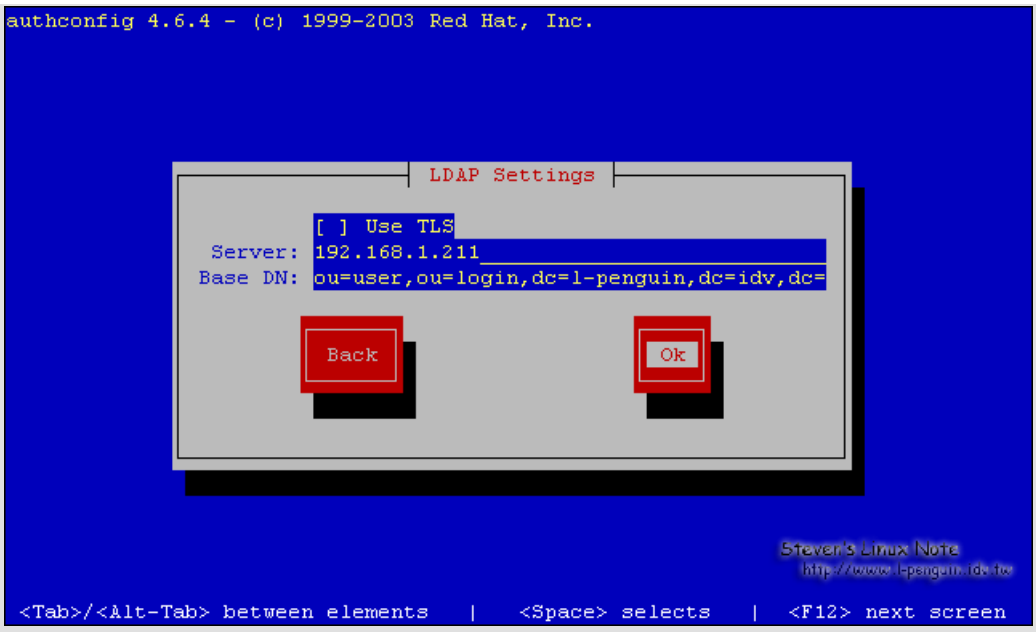
若有看到 ldap 就表示你的 postfix 支援 ldap 儲存格式。

設定 PAM

Linux 有一項管理登入的機制稱為 PAM，只要應用程式都支援 PAM 管理，那麼對於帳號的操就可以得到統一的整合而不用再去設定應用程式。所以，在開始之前，我要使 Linux 支援 LDAP 登入的話，可以使用 pam_ldap 這個模組，這其中會有很多設定，當然也有很快速的方法，在此我介紹使用 authconfig 這個工具，就可以很輕易的設定好 ldap 的相關設定。

```
root # authconfig
```






```
root #
```

這個方法，我在 LDAP - 整合 Linux user login (New Window) 裡面也有提過，我建議你再參考一次，因為有一些細節的地方，像是 group 如何對應到 LDAP，在該篇文寫得很清楚。

測試系統是否經由 LDAP 認證

這個時候，你只要隨便打個 id 就可以知道了。

```
root # id c293831287
uid=600(c293831287) gid=510(hr) groups=510(hr)
root #
```

建立使用者的 mail 檔案

postfix 會把使用者的 mail 放到 /var/spool/mail/{USER} 的檔案裡，若是使用 LDAP 建立帳號的話，就必需再建立 user 的 mail 檔案才可以收到信，比方說，現在要寄一封信給 f296974826 這個帳號的使用者，但是因為 postfix 在 /var/spool/mail 找不到 f296974826 這個檔案，所以我們必需手動建立 /var/spool/mail/f296974826 這個檔案，並設定權限。

```
root # cd /var/spool/mail
root # touch f296974826
root # chown f296974826.mail f296974826
root # chmod 660 f296974826
```

經過以上設定，就算設定好了，下一節再來看看如何測試 postfix。

測試 postfix

設定完 postfix 和 user 郵件檔案之後，現在來看看是否可以寄信。

```
root # mail f296974826
Subject: Welcome to vm-mail
Hi, f296974826:
Welcome to l-penguin.
Have a good day.
.
Cc:
root #
```

再來，登入為 f296974826 的帳號，看看是否有收到信件。

```
root # su - f296974826
su: warning: cannot change directory to /home/f296974826: No such file
or directory <- 不要理會這條訊息。
-bash-3.00$ mail
Mail version 8.1 6/6/93. Type ? for help.
"/var/spool/mail/f296974826": 2 messages 2 new
>N 1 root@vm-mail.l-pengu Sun Jul 23 20:02 15/520 "Welcome to vm-mail"
& 1
Message 1:
From root@vm-mail.l-penguin.idv.tw Sun Jul 23 20:19:26 2006
X-Original-To: f296974826
Delivered-To: f296974826@vm-mail.l-penguin.idv.tw
To: f296974826@vm-mail.l-penguin.idv.tw
Subject: Welcome to vm-mail
Date: Sun, 23 Jul 2006 20:19:26 +0800 (CST)
From: root@vm-mail.l-penguin.idv.tw (root)
Hi, f296974826:
Welcome to l-penguin.
Have a good day.
& q
/home/f296974826/mbox: No such file or directory
f296974826 $
```

其實只要看到有剛剛由 root 寄過來的歡迎信那就表示 OK 了。

重點討論：

其實到現在 postfix 還是沒有使用 LDAP ...

為什麼要多出這個章節呢？很簡單，可能有很多人認為到目前為止 postfix 是去詢找 ldap 的資料，然後再送信的，其實這是不對的，我用下面簡單的圖來說明：

一般想法（錯誤）：

```
postfix -- ldap -- user
```

實際流程：

```
postfix -- linux pam_ldap -- ldap -- user
```

由上面可以知道，其實正確流程是 postfix 使用 pam 系統去找 user 的資訊，而中間關於 ldap 的部份 postfix 根本就不管，而是由 pam_ldap 這個模組去做連結，再傳回使用者資訊給 postfix。

手續這麼多，我要怎麼一次建立 user mail 檔案？

其實建立 user mail 檔案可以使用 shell script 來做，這樣就可以很快速的達到想要的設定。下面是我寫的一個 shell 程式。

```
#!/bin/bash
user=""
cd /var/spool/mail
# 以下黑體字為同一行
for user in `ldapsearch -x -b
"ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw" | egrep 'uid\:' | awk
'{print $2}'`
do
      if !([ -f ${user} ]); then
            touch ${user}
            chown ${user}.mail ${user}
            chmod 660 ${user}
      fi
done
```

你也可以在此 下載。

真正讓 postfix 尋找 ldap 資料！

其實 ldap 能放的資訊很多，像是存放 user alias 資料、hostnames、body_checks 或 header_checks 等資訊都可以存放，這也就是說你連垃圾信的分析都可以放到裡面，端看你怎麼應用！

我在這裡，示範如何使用 postmap 去查詢 LDAP 資訊。我以 alias 來做說明。

編輯 /etc/postfix/main.cf

```
root # vi /etc/postfix/main.cf
-----------------------------------------------------
#加入 alias
alias_maps = ldap:/misc/ldap/alias
-----------------------------------------------------
root #
```

而 /misc/ldap/alias 的內容如下。

```
root # vi /mis/ldap/alias
-----------------------------------------------------
# server 的位置
server_host = 192.168.1.61
#資料的查詢位置
search_base = ou=user,ou=login,dc=l-penguin,dc=idv,dc=tw
#資料過濾條件
query_filter = (&(uid=%s))
#要回傳的值
result_attribute = gecos
-----------------------------------------------------
root #
```

在設定 server_host 時，請注意使用 IP 而不要使用 FQDN、Simple name，不知道什麼原因，小弟只有在 IP 的表示下才正確連線，其它設定都會連到 localhost :(

使用 postmap 工具測試

設定好之後，請使用 postmap 來做測試，查詢 d295380453 這個帳號的 gecos 值。

```
root # postmap -q 'd295380453' ldap:/misc/ldap/alias
Edward Mcelhaney
root #
```

對於 postfix 來說，有回傳值表示有效的條件，若沒有的話就代表無效，你可以使用 $? 參數來看。

```
root # postmap -q 'd295380453' ldap:/misc/ldap/alias; echo $?
Edward Mcelhaney
0
root #
```

回傳一個 0 的有效值，postfix 如果遇到這種情況的話，因為是由 alias_maps 來使用 /misc/ldap/alias 這個檔案的設定，所以當 postfix 得到

LDAP 的回應時，就會把這封送到 d295380453 的信件轉送到 edward mcelhaney 這兩個帳號。

現在我們再看另一個示範，是找出 c293831287。

```
root # postmap -q 'c293831287' ldap:/misc/ldap/alias; echo $?
1
root #
```

它回傳一個 1 值，對於 postfix 來說，這個表示 c293831287 這個帳號沒有別名因為將會直接寄到 c293831287 這個帳號的信箱(如果真有其帳號的話)。以一個程式設計師來說，return 0 表示正常的或成功的離開，而回傳一個非 0 的值表示有其它的錯誤或不正常的結束。

postfix 2.0.x (含 2.0.x) 以前版本的使用者請注意

上述使用 ldap:/path/to/file 的方式只適合用在 postfix 2.1.x 或以後版本上，對於 2.0.x 或以前的版本並不適用，你可以在 Postfix manual - ldap_table(5) 找到相關說明。

附註：

小弟在寫這一篇文件時參考了一些大大小小的文件，postfix 和 LDAP 整合涉及到了 PAM 的設定、LDAP 模組安裝和 postfix 本身對 LDAP 的編釋，我儘量去除理論部份並加強註明在實作時的細節，若有問題的話請不吝指教。
若要深入了解有關 postfix 和 LDAP 的理論，請參考其官方網站，有更多的資訊可查。

參考資訊：

- Postfix LDAP Howto：http://www.postfix.org/LDAP_README.html
- LDAP 系統管理 (O'Reilly, ISBN：986-7794-21-4)：http://www.oreilly.com.tw/product_network.php?id=a130
- Postfix 技術手冊 (O'Reilly, ISBN：986-7794-29-X)：http://www.oreilly.com.tw/product_network.php?id=a141

本篇文章以 PDF 方式散播，有關原始網頁和檔案下載的部份請參閱 http://www.l-penguin.idv.tw/~steven/article/ldap-4.htm。

作者：廖子儀 (Tzu-Yi Liao)
Certified：LPIC Level I、LPIC Level II、RHCE
E-mail：steven@l-penguin.idv.tw
Web site：http://www.l-penguin.idv.tw/