第十單元

Sendmail+POP3 伺服器管理

1.實驗目的

架設郵件伺服器並提供 POP3 服務

2.實驗設備

- 安裝 Linux 系統之電腦
- Webmin(http://www.webmin.com)
- Sendmail(http://www.sendmail.org)
- IMAP(http://www.imap.org/imap)

3.背景資料

Sendmail 對一般的系統管理者而言，往往是個不敢動手的『禁區』，因為絕大多數系統的使用者對 E-Mail 的需求與依賴的程度之高，可說是稍有分毫差錯，系統管理者就要準備接受如雪片般飛來的抗議與抱怨！而 Sendmail 的「內涵」，似乎又有點不太容易理解。

與設定有關的 sendmail.cf 檔，如果不是下過一番死功夫，則讀起來如同讀天書一樣，只知道裡面有英文字與數字！所以一般人總是能不動則不動，只要能用就好。不過，很不幸的，一般跟著機器而來的 sendmail 總是有著令人心驚膽跳的『附加功能』，就是常常都有一些可以讓無聊人士作為侵入路徑的 BUG 或後門，某些 BUG 還可以讓侵入者經由 Sendmail 而取得最高權限的 root！一旦 root 權限被人拿走了，那麼這機器就可被人任意更改，最惡劣的，還可能破壞系統！

Sendmail 8.12.11 是目前 Sendmail 8.12.x 系列的最高版本。系統安全方面是目前評價最好的，目前已知的 BUG 都已經改好了。本軟體是一個 public domain，可以在網路上各 ftp server 上找到其 source code。由於該軟體的發展者把一些必要的設定步驟自動化了，所以，其實安裝這個軟體並不是想像中那麼樣的困難。如果連編譯的時間也算下去，順利的話，不用半個小時就可以安裝完畢。

4.實驗方法

安裝與啟動

預設的 Fedora 就有安裝 sendmail 的套件，不過 pop3/imap 的套件得自行選擇，所以可以用 rpm 的指令來查詢目前有安裝哪些套件：

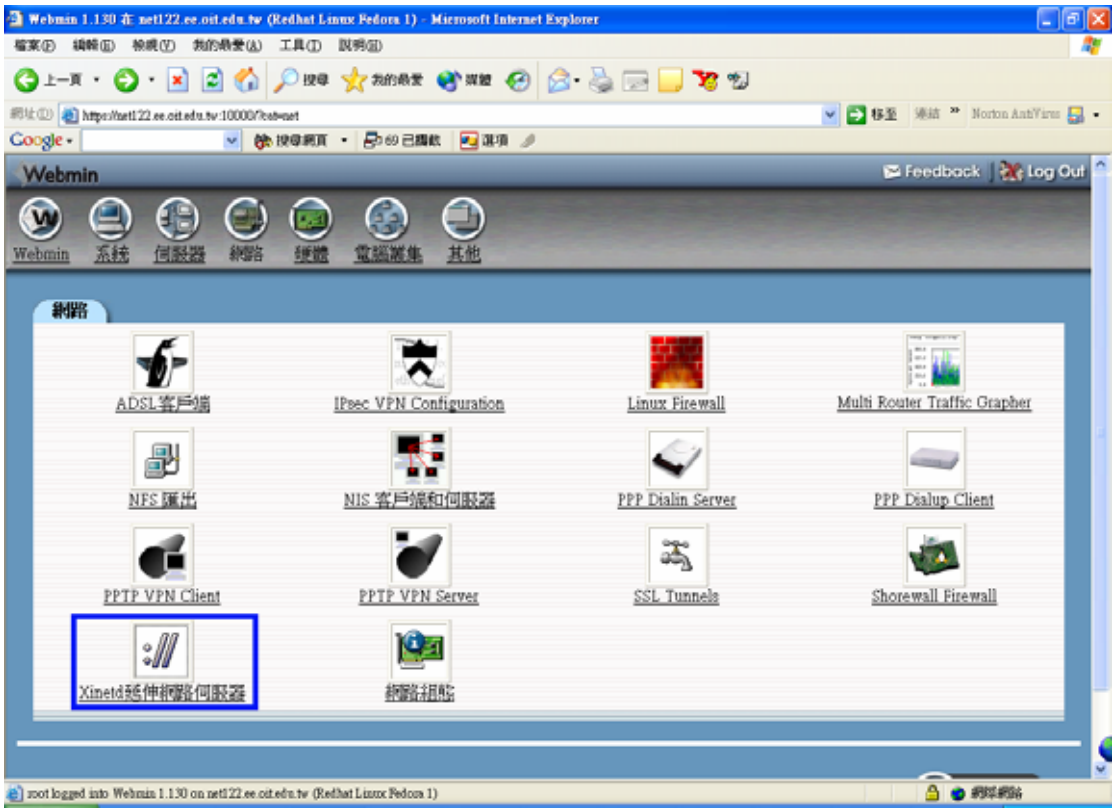
```
[root@net122 root]# rpm -qa|grep sendmail
sendmail-cf-8.12.10-1.1.1
sendmail-8.12.10-1.1.1
```

```
[root@net122 xinetd.d]# rpm -qa|grep imap
imap-2002d-3
php-imap-4.3.3-6
```

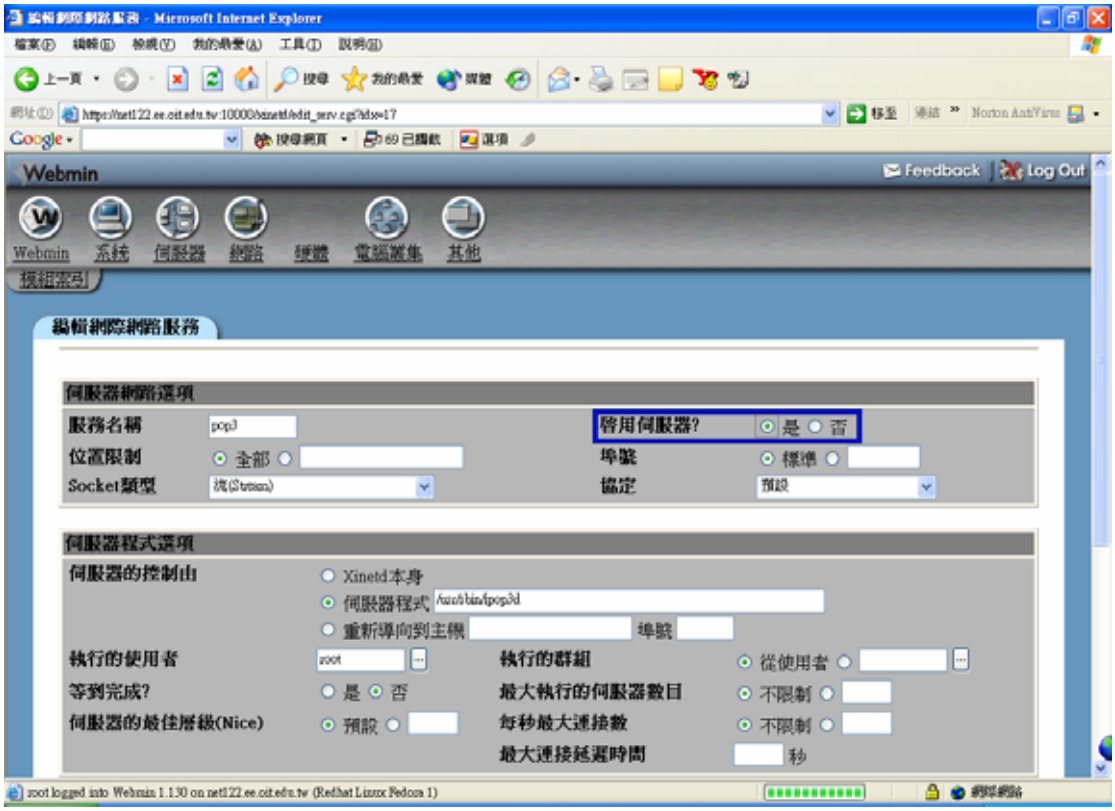
如果沒有 sendmial 和 imap 的套件時，請自行至 http://www.rpmfind.net 下載安裝 rpm 檔安裝即可。

啟動 pop3 服務

選擇【網路】內的『Xinetd 延伸網路伺服器』，出現下列圖示：



選擇『pop3』進入選單後，把『啟用伺服器』選擇『是』。



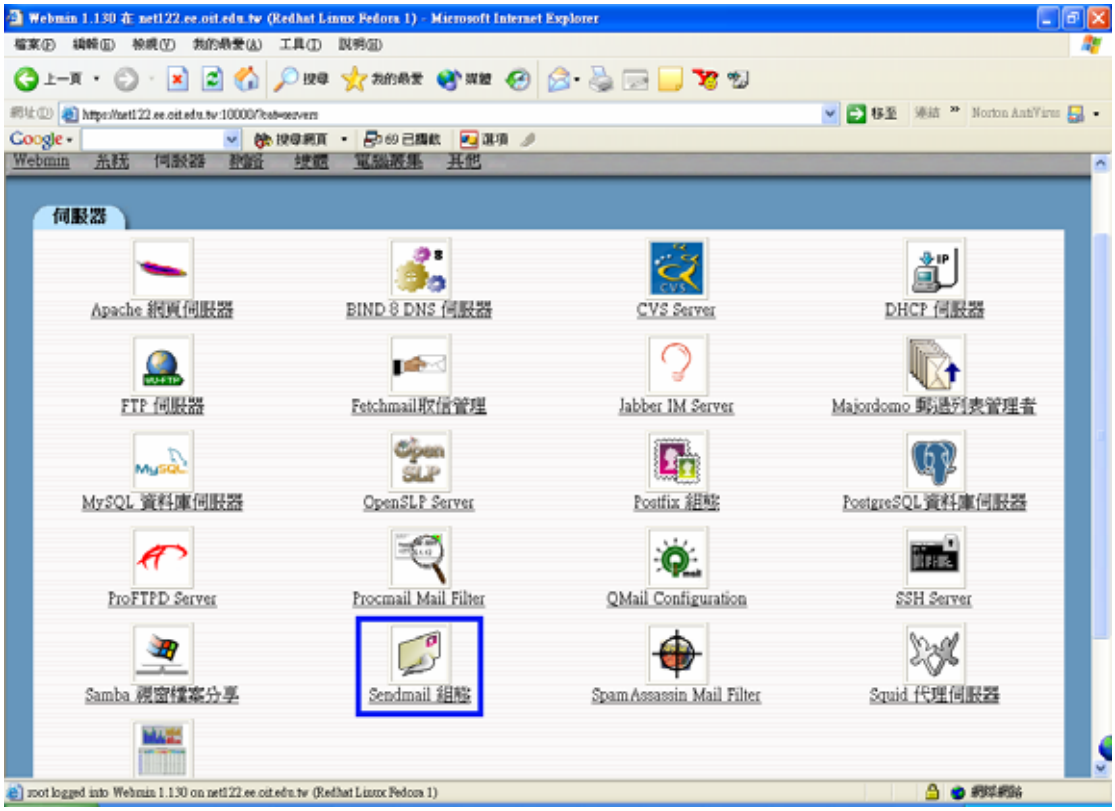
選擇『儲存』後，重新啟動 Xinetd 伺服器後，測試 pop3 的連線。

```
[root@net122 named]# telnet net122.ee.oit.edu.tw 110
Trying 192.192.73.122...
Connected to net122.ee.oit.edu.tw.
Escape character is '^]'.
+OK POP3 net122.ee.oit.edu.tw v2003.83rh server ready
```

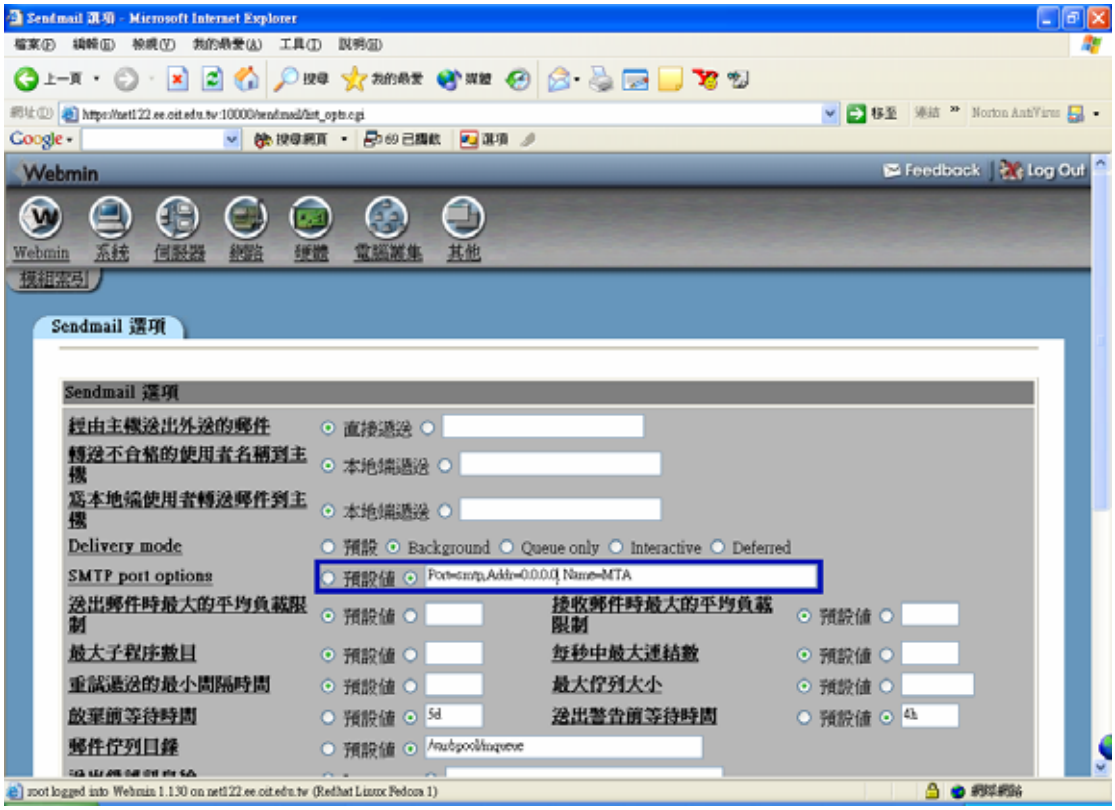
這樣就表示 pop3 已經啟動囉！

啟動 SMTP 服務

在此是使用 Sendmail 的套件來當作 SMTP 伺服器，所點選【伺服器】中的『Sendmail 組態』。



點選進入後，要先打開 Sendmail 的服務，然後點選『Sendmail 選項』進入以下的畫面：



將上面那行原本的 127.0.0.1 改成 0.0.0.0，或者是所有網路卡介面的其中一個 IP 位址。

測試 SMTP 的連結狀態：

```
[root@net122 xinetd.d]# telnet net122.ee.oit.edu.tw 25
Trying 192.192.73.122...
Connected to net122.ee.oit.edu.tw.
Escape character is '^]'.
220 net122.ee.oit.edu.tw ESMTP Sendmail 8.12.10/8.12.10; Wed, 18 Feb 2004
11:27:35 +0800
```

到目前為止已經將 SMTP 伺服器成功啟動。

使用 Webmin 管理

設定主機名稱

當啟動了 sendmail 的服務之後，必需要設定這台 sendmail 伺服器的主機名稱，也就是說是該用哪一個 hostname 來寄信。首先在【Sendmail 組態】中，選擇『本地端網域(Cw)』，進入以下的畫面：

填入後，按下『儲存』並重新啟動，伺服器就只會對 mail.net122.ee.oit.edu.tw 這台 smtp 伺服器作出回應。

設定 relay

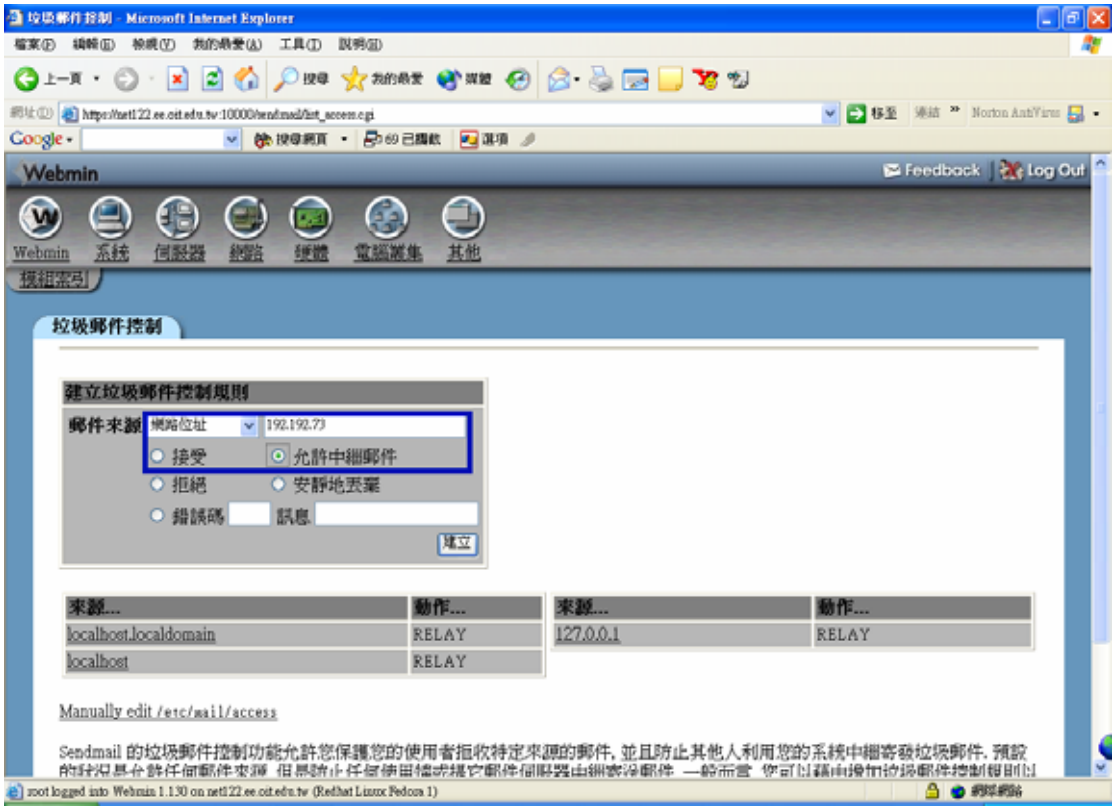
在 Sendmail 的預設值中，除了 localhost 之外，其他的使用者並不能過透過這台 SMTP 伺服器進行寄信。在還未設定 relay 之前，outlook express 可能會出現以下的畫面：

這就是因為尚未設定被允許的 relay 區段，現在開始設定被 relay 的位址。打開

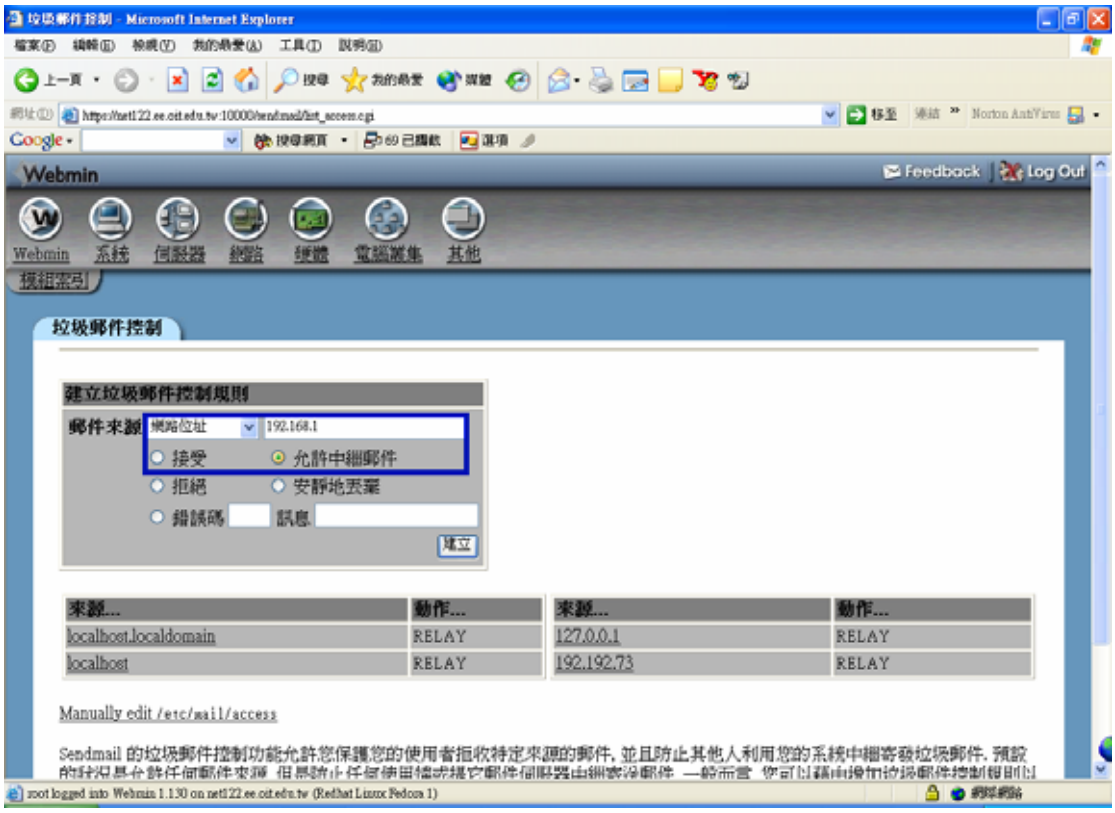
【Sendmail 組態】，選擇『垃圾郵件控制(access)』，進入以下的畫面：

如果有以下的狀況，可以一一將規則放置上去。

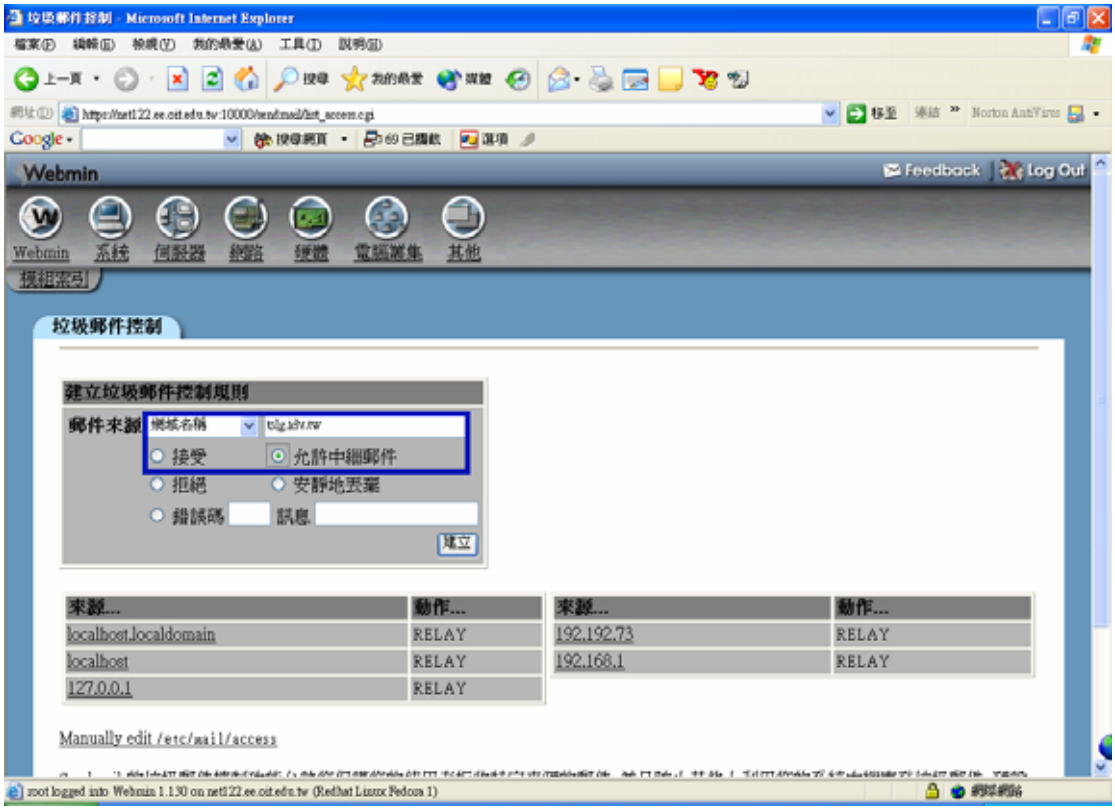
屬於 192.192.73.0/24 這個網段的主機，可以經由此台 SMTP 伺服器寄信。選擇【郵件來源】為『網路位址』，將動作設定為『允許中繼郵件』。



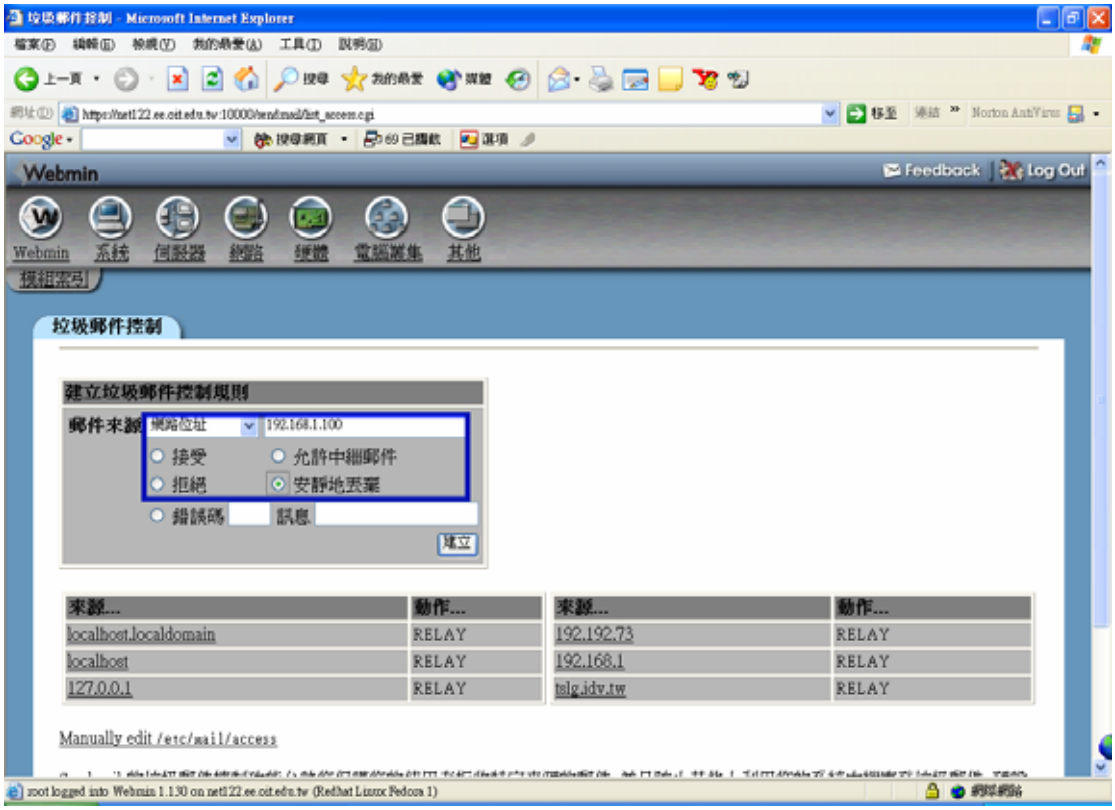
屬於 192.168.1.0/24 這個內部的虛擬主機可以經由此台 SMTP 伺服器寄信，其他設定同上。



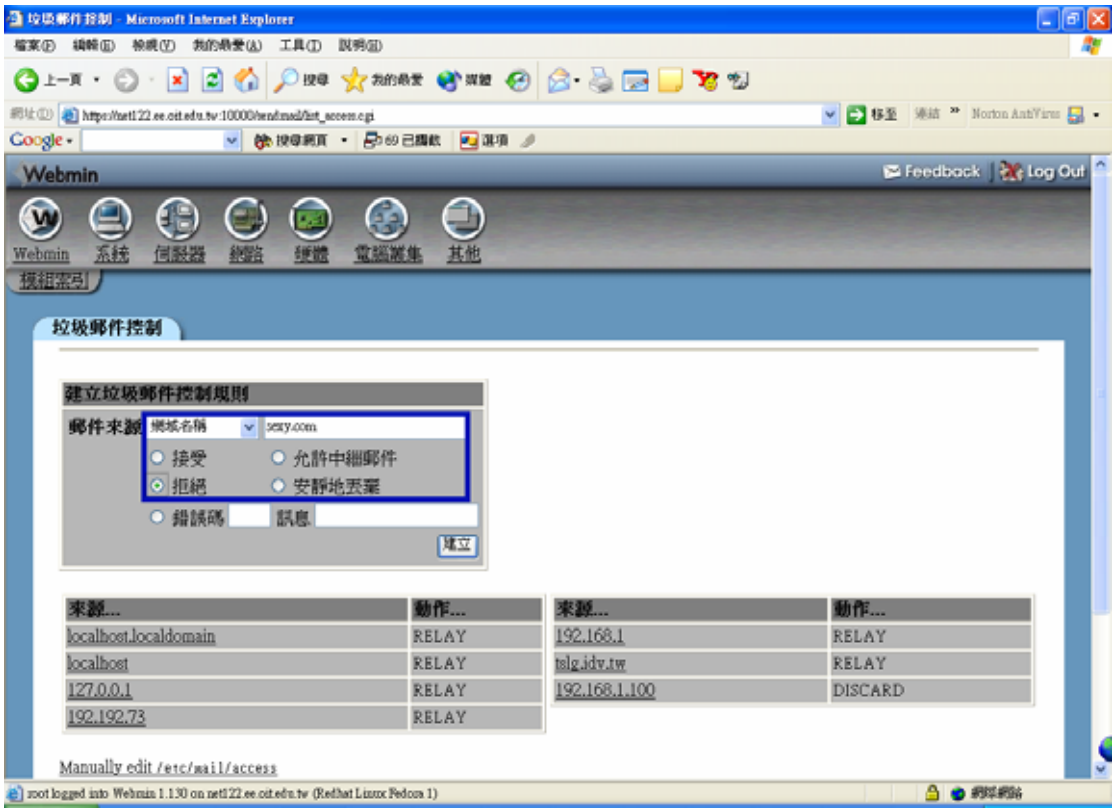
屬於 tslg.idv.tw 網域的主機可以經由此台 SMTP 伺服器寄信。選擇【郵件來源】為『網域名稱』，將動作設定為『允許中繼郵件』。



一台位址為 192.168.1.120 的虛擬主機，會亂發信給這台伺服器將它擋掉。選擇【郵件來源】為『網路位址』，將動作設定為『安靜地丟棄』。



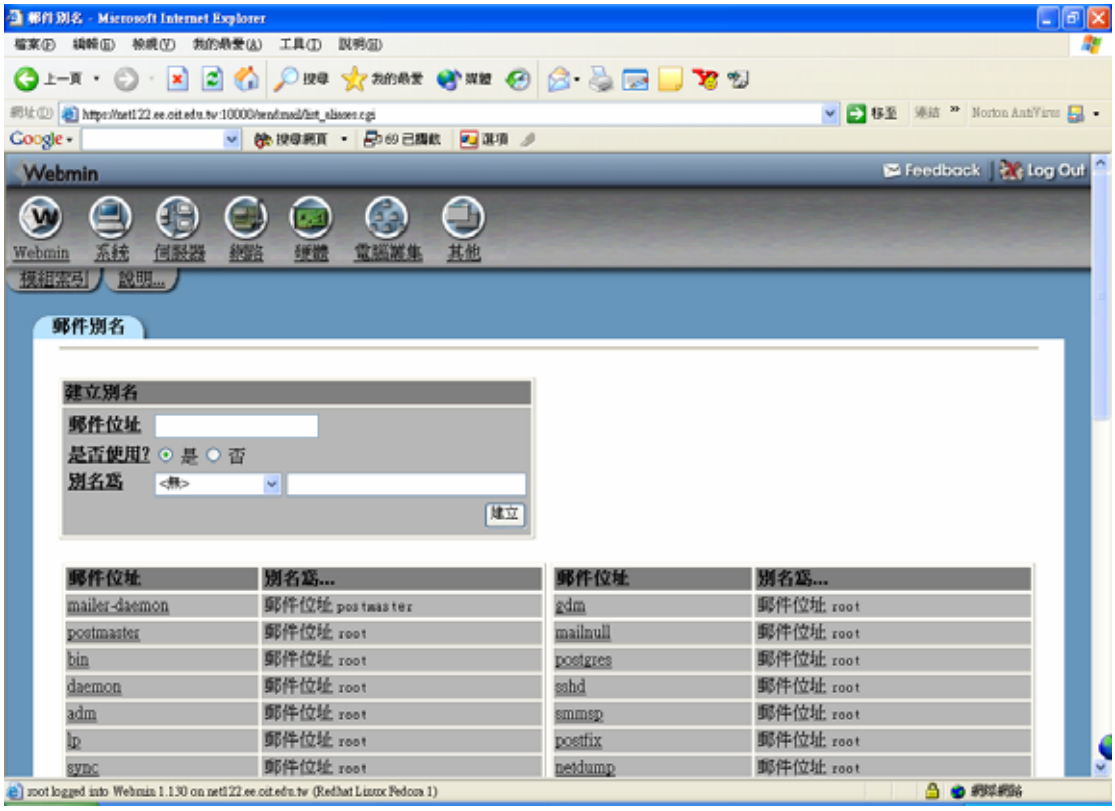
網域 sexy.com 常常用一些奇怪的使用者來寄廣告信，必需將它擋掉。選擇【郵件來源】為『網域名稱』，將動作設定為『拒絕』。



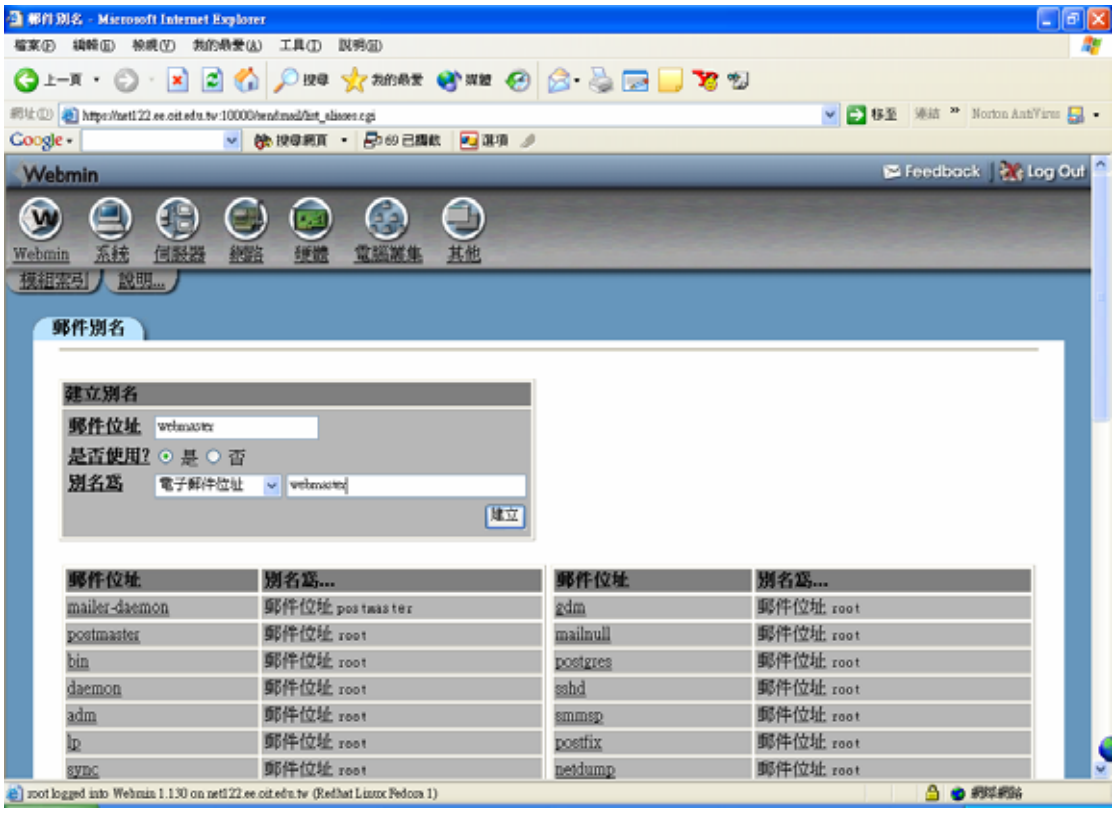
設定郵件別名（aliases）

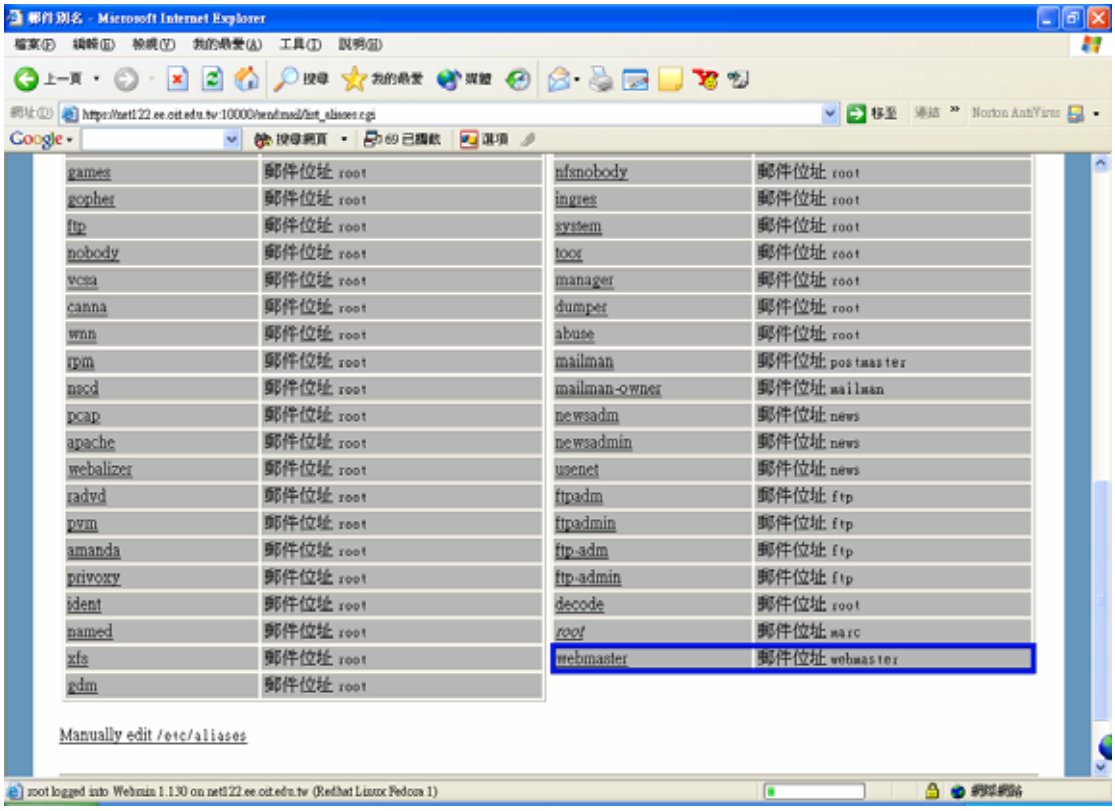
有時候為了工作上的需要，一個人或者一個部門都會有很多的 e-mail 帳號，這個時候如果有很多人都會收到外國寄來的一封信，那麼收到信的那個人一定又要轉寄一次給全部的人，如果是一、兩次那還好，萬一是三天兩頭破百封，那不就很頭痛嗎？所以 sendmail 提供了一個別名的機制，當一個帳號收到信後，系統會直接轉寄一封給其他在別名名單上的使用者，增加了便利性。

首先新增一個叫做 webmaster 的使用者，當要寄信給 webmaster@mail.net122.ee.oit.edu.tw 的時候，系統會自動轉寄給真正的管理者 linul@mail.net122.ee.oit.edu.tw 及 linul@tslg.idv.tw，請至【Sendmail 組態】中點選『郵件別名 (aliases)』，進入以下的畫面：

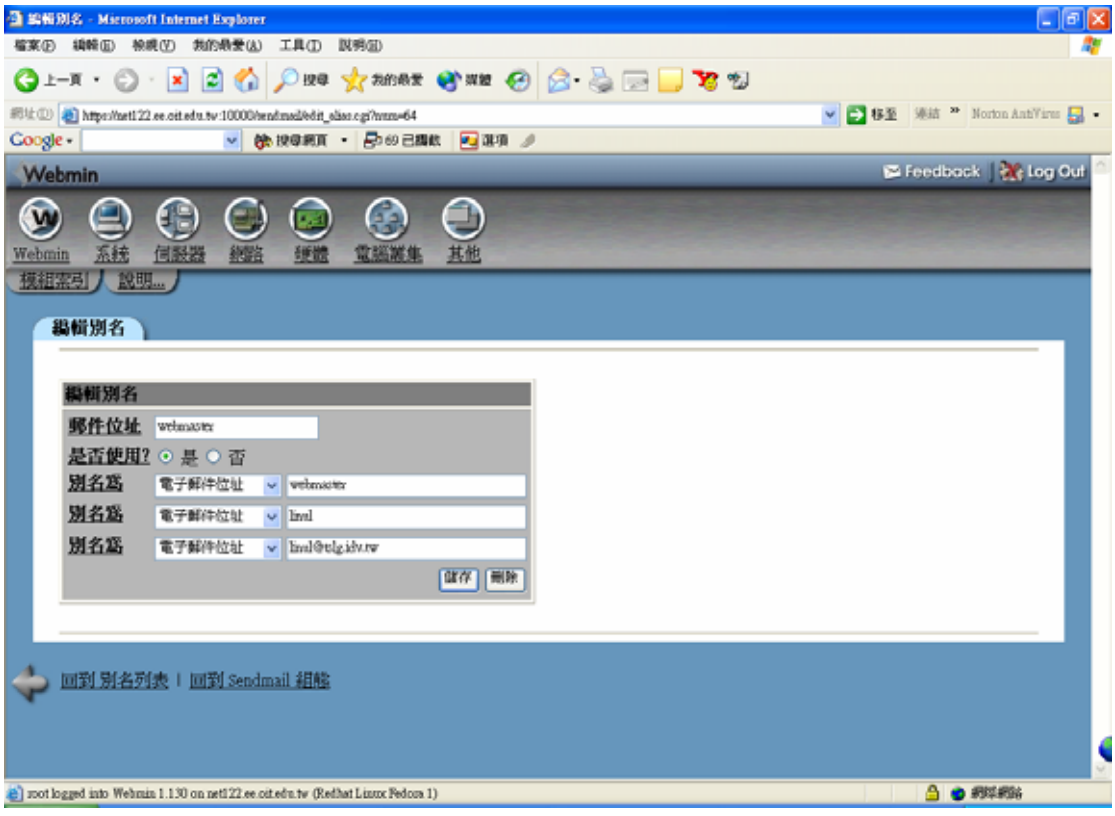


接下來先建立 webmaster 的郵件位址，如下圖所示。別名選擇【電子郵件位址】，設定為 webmaster 先建立一個空的別名。

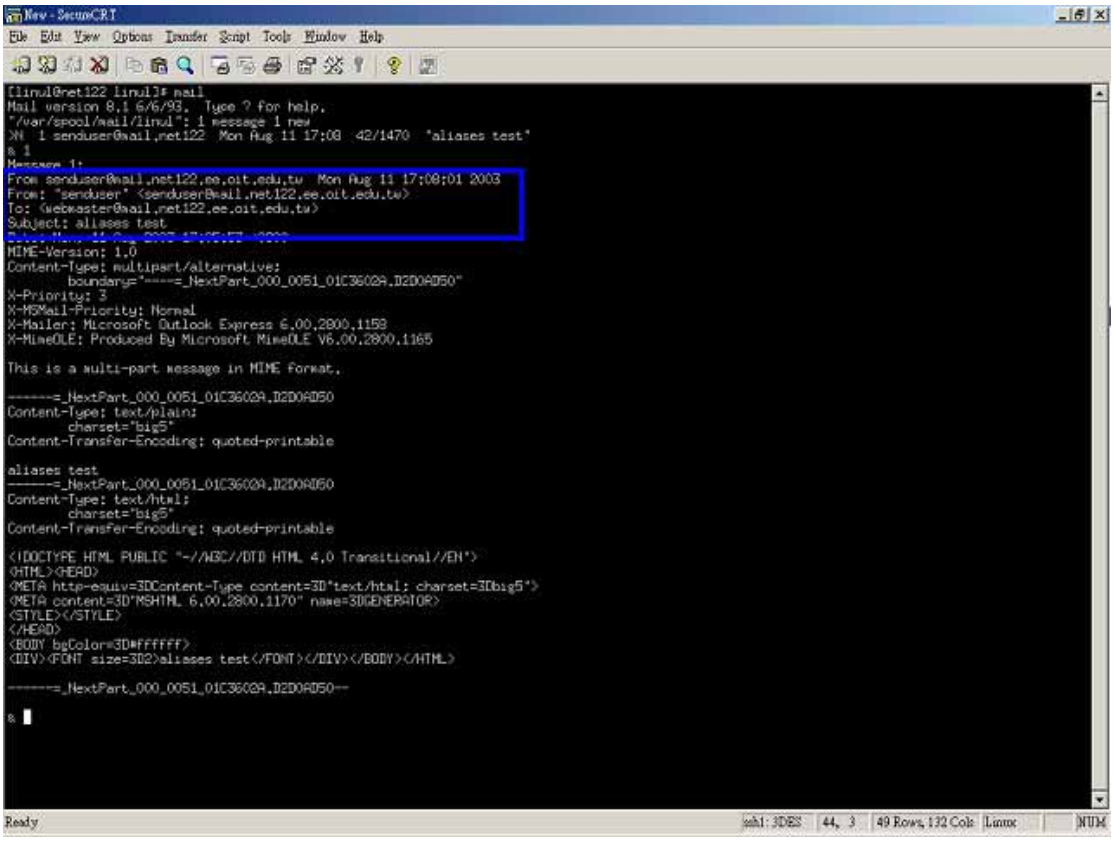




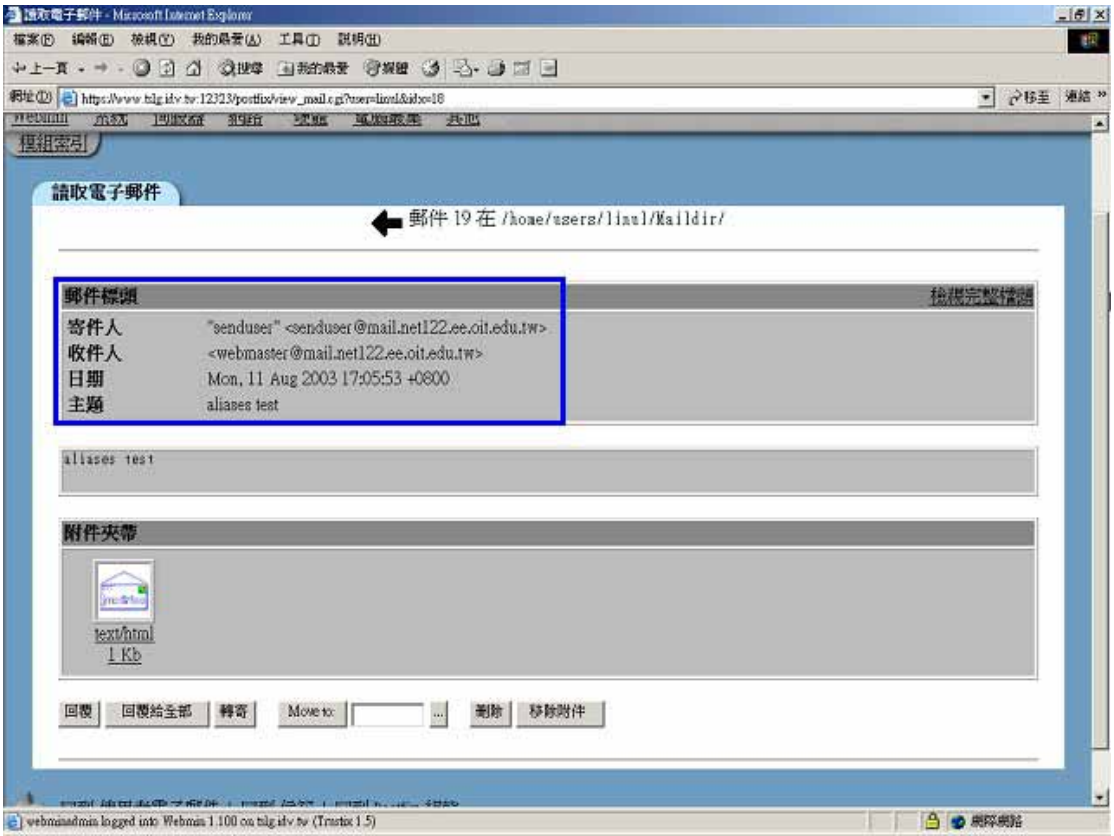
選擇郵件位址 webmaster。再新增兩個別名，分別為本機上的 linul 及 linul@tslg.idv.tw



接下來寄了一封信給 webmaster@mail.net122.ee.oit.edu.tw。



收件者是 webmaster@mail.net122.ee.oit.edu.tw，接來再看看 linul@tslg.idv.tw。



另外當 aliases 變很多的時候，也可以利用檔案的方式來進行匯入，只要再別名的選項選擇【郵件位址在檔案】就行了。而此檔案的格式為以下所示：

linul, linul2, linul@tslg.idv.tw, webmaster@hinetnet（用逗號隔開即可）

以上的設定是專門給系統管理者使用的，如果使用者要自行設定轉寄名單時，也可以使用『.forward』的檔案來設定轉信名單，只要將這個檔案放入使用者的家目錄中，格式與上列檔案格式相同，並把檔案的權限設定成為群組與其他使用者不可以更改、讀取即可。

設定 SMTP 認證功能

前面有提到雖然可以利用 access 表來控制哪些地方可以寄信、哪些地方不可以寄信，但是當出差在外時，所有的位址都是不一定的，如果要經由公司的 SMTP 發信的話，難道還要登入伺服器作修改才能寄信嗎？實在是非常的麻煩，不過 Sendmail 現在可以配合 Cyrus SASL（Cyrus Simple Authentication and Security Layer）這個套件來進行遠端 SMTP 認證的工作，讓使用者可以不經由 access 表就可以直接經由公司的伺服器來發信。

Fedora Linux 已經直接支援 Cyrus SASL 了，只要直接修改 sendmail.cf 檔或者是 mc 檔即可以打開認證機制，將/etc/mail/sendmail.mc 檔打開，找到下面三行：

```
dnl TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
```

將前兩行的 dnl 去掉，最後一行改為 0.0.0.0 或是主機上的網路介面 IP。

```
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
DAEMON_OPTIONS(`Port=smtp,Addr=0.0.0.0, Name=MTA')dnl
```

儲存後離開。

先將原本的 sendmail.cf 檔備份起，以防萬一。

```
[root@net122 mail]# mv sendmail.cf backup
```

重新製作一份 sendmail.cf 檔

```
[root@net122 mail]# m4 sendmail.mc > sendmail.cf
```

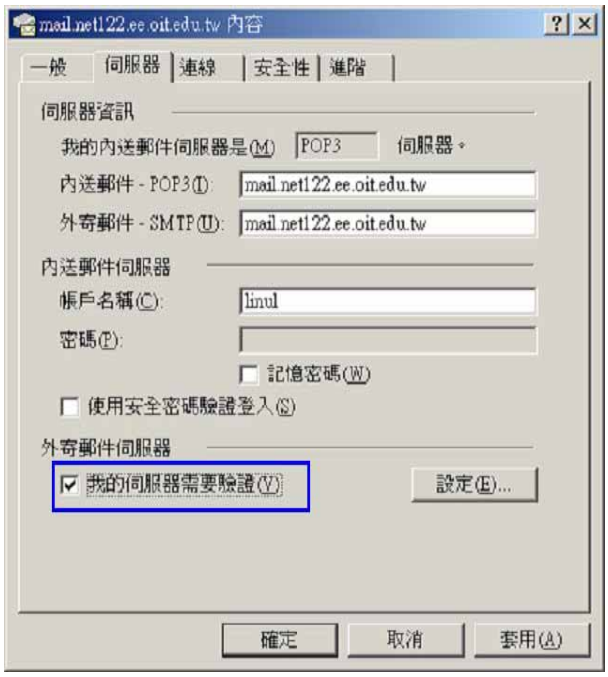
重新啟動 sendmail，再進行測試。

```
[root@net122 mail]# telnet net122.ee.oit.edu.tw 25
Trying 192.192.73.122...
Connected to net122.ee.oit.edu.tw.
Escape character is '^]'.
220 net122.ee.oit.edu.tw ESMTP Sendmail 8.12.10/8.12.10; Wed, 18 Feb 2004
11:47:54 +0800
ehlo net122.ee.oit.edu.tw
250-net122.ee.oit.edu.tw Hello net122.ee.oit.edu.tw [192.192.73.122], pleased to
meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5 LOGIN PLAIN    #出現就代表成功了
250-DELIVERBY
250 HELP
```

最後再啟動 saslauthd：

```
[root@net122 log]# /etc/init.d/saslauthd restart
```

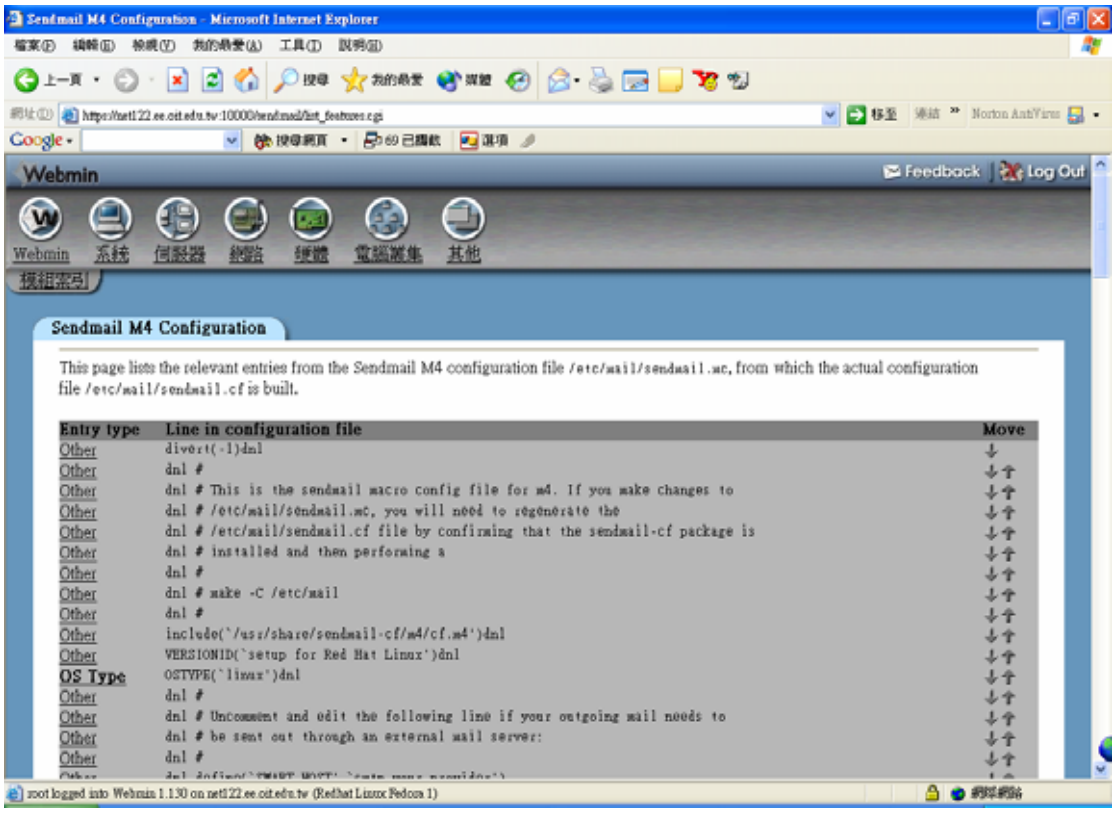
修改成功後，client 也要進行修改，進到 outlook express 中，選擇【工具】->【帳戶】->【郵件】，選擇一個使用者帳號，點選進入【伺服器】，然後勾選『我的伺服器需要驗證』。



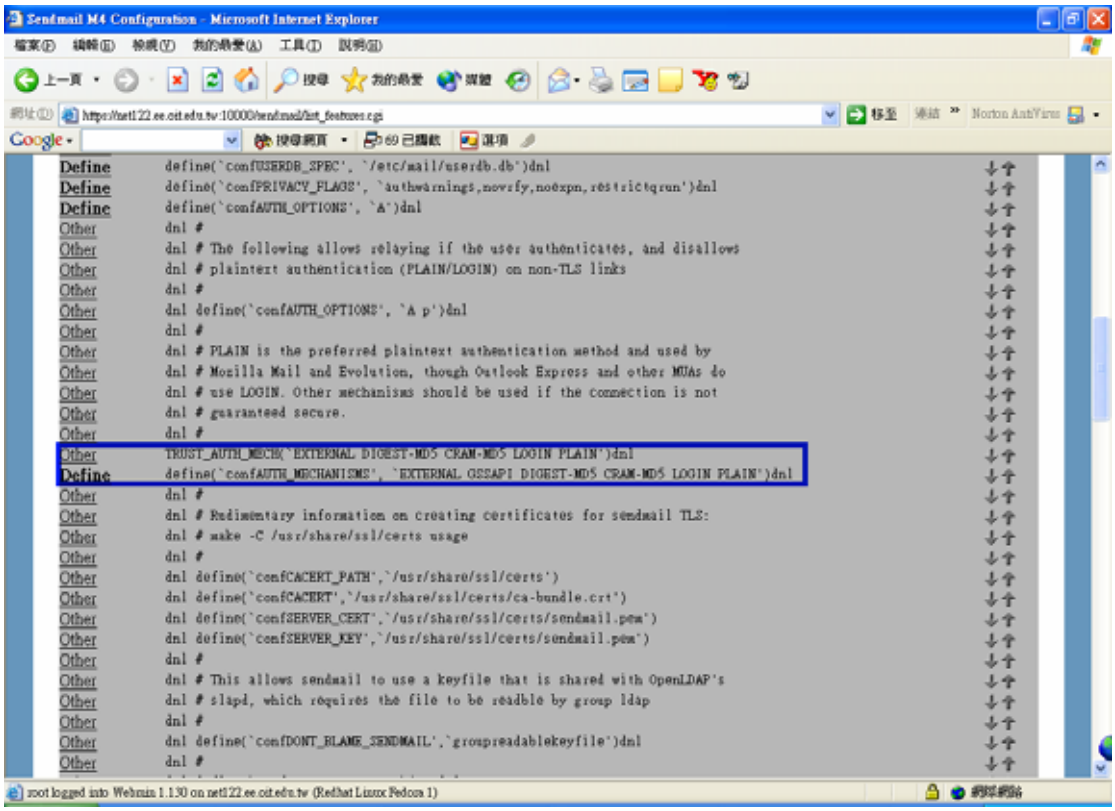
之後，client 端即可遠端進行寄信了。

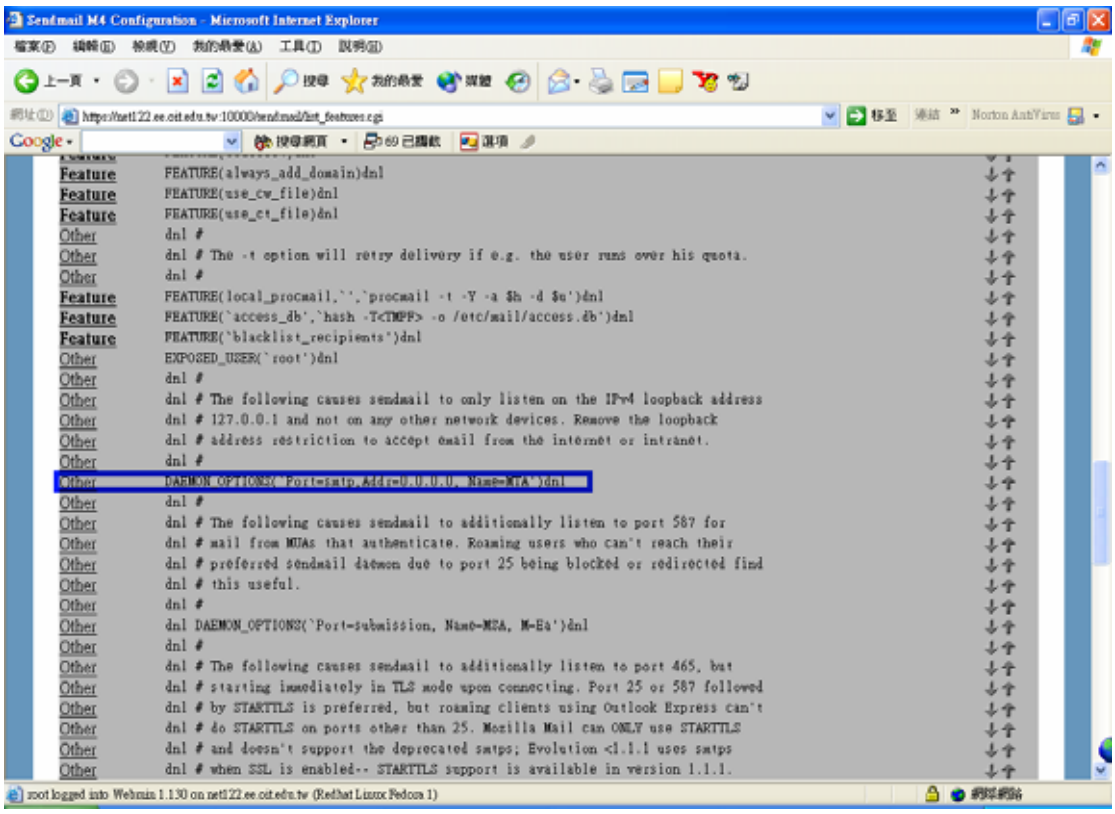
m4 工具的使用

m4 的動作也可利用 Webmin 來進行修改，連到【Sendmail 組態】下的『Sendmail M4 Configuration』，出現以下的畫面：

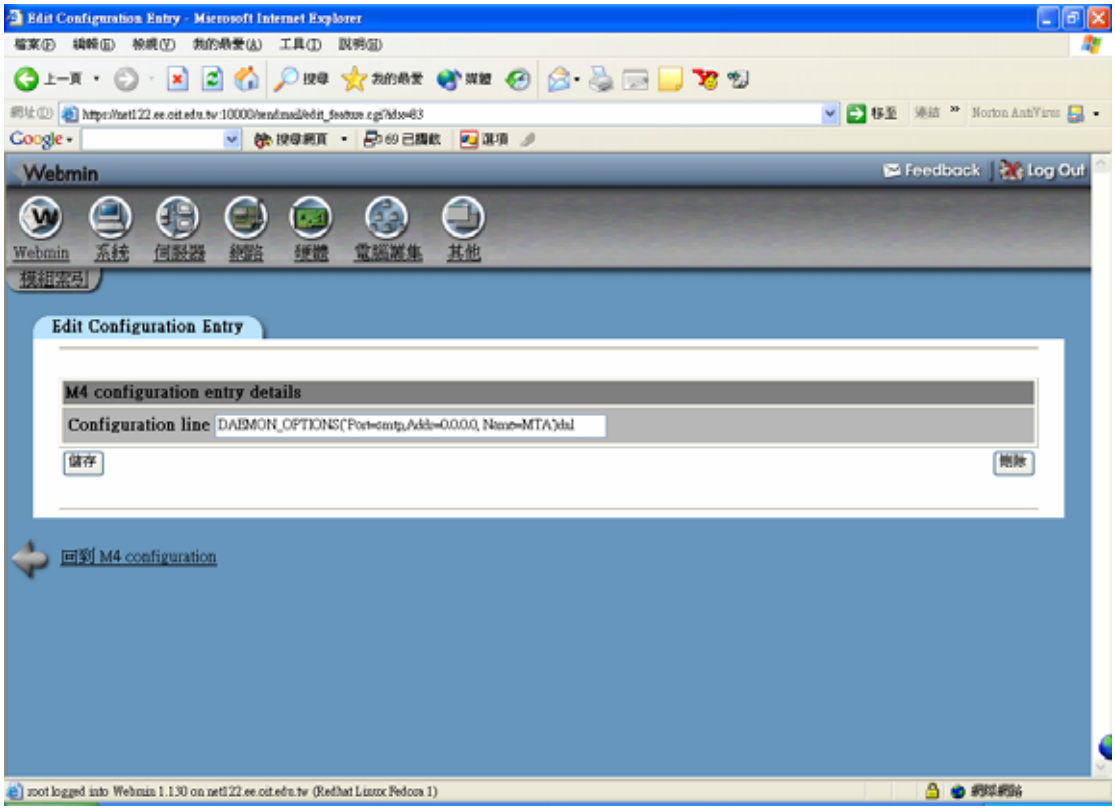


可以找到剛剛修改的那三行：

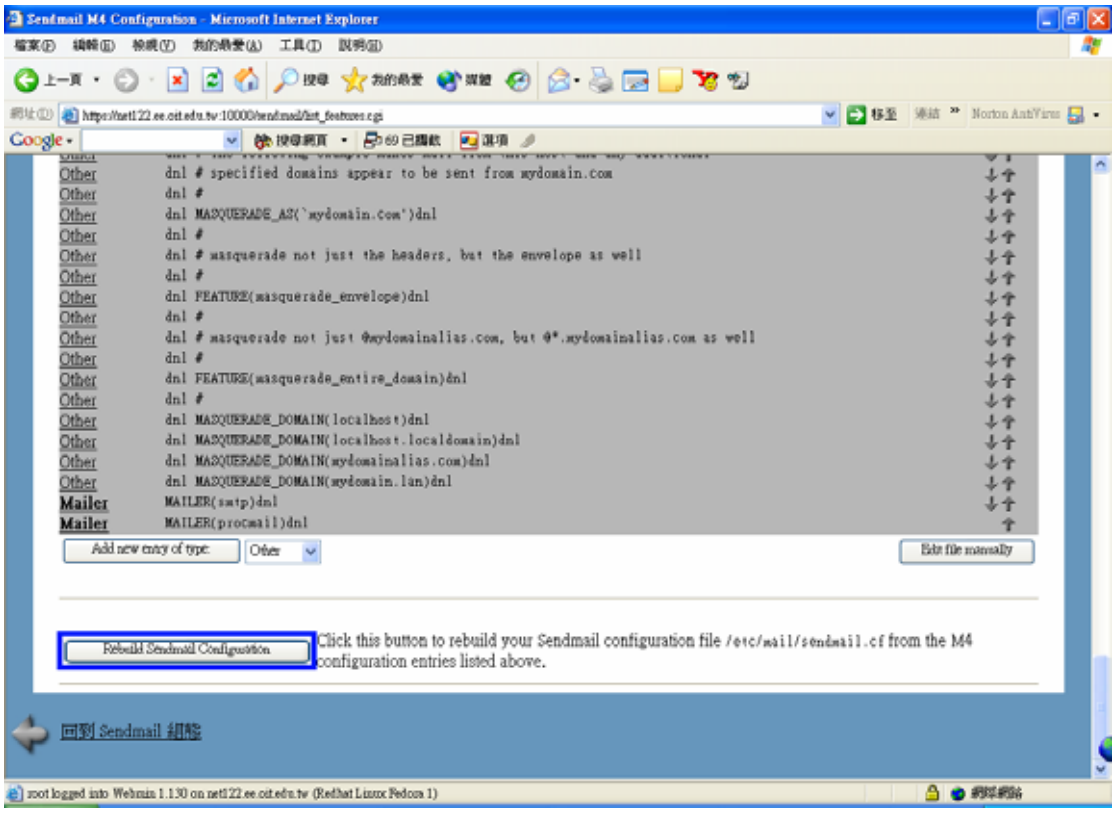




點選旁邊的連結可以進行修改。



修改完成後，按下『Rebuild Sendmail Configuration』並重新啟動 Sendmail，即可完成設定並產生新的 cf 檔。



5.問題與討論

1. 如果可以寄信但不能收信，處理步驟要如何？
2. 如果可以收信但不能寄信，處理步驟要如何？
3. 比較不同 MTA（Mail Transport Agent），如 sendmail、postfix、qmail）的效能及安全性。
4. 比較不同 MUA（Mail User Agent），如 Outlook, pine, elm 的效能及安全性。
5. 如何限制可收發郵件的位址及郵件大小？
6. 如何透過 SMTP 認證的方式寄信？
7. 別名除了轉寄信件還有哪些功能？
8. 如何使帳號含英文大寫字母的使用者能收發信？
9. 郵件的紀錄如何分析？
10. POP 和 IMAP 協定有何不同？