使用 FreeBSD 建立安全的郵件系統 – imap/pop 篇

中央研究院 計算中心 張毓麟 ylchang@sinica.edu
(本文刊載於 中央研究院 計算中心通訊 17 卷 14 期)

前言

電子郵件根據使用者的動作而言，基本上可分爲送信與收信兩方面。發信通常使用郵件軟體(例如 MS-OutLook 或是 Netscape-Messenger)使用 SMTP 協定經由郵件伺服器的 Sendmail 程式發送。收信則有較多的選擇，常見的是操作郵件軟體透過 POP-3 或是 IMAP-4 協定到郵件伺服器上抓取信件。(前文所提到的 3 與 4 指的是目前通行的協定版本)

上一期的中心通訊中，爲大家介紹了具有身分認證以及保密連線功能的 Sendmail 程式，可用於安全的發送電子郵件。在本期的通訊中，我們將繼續探討使用者收信時的安全機制。以期建立一個安全的郵件收發系統。

IMAP 與 POP 有何不同?

以使用者的角度來看，POP 與 IMAP 最明顯的差異在於郵件存放的方法，以及郵件軟體抓取郵件以及保存郵件的行爲。

郵件軟體透過 POP 抓取郵件的時候，通常會把郵件全部下載到使用者的 PC 上，然後把伺服器上的信箱清空，以便釋放空間。如果使用者建立了不同的郵件夾作郵件分類，這些郵件夾會存放在使用者的 PC 上，不會佔用到郵件伺服器的空間。這種做法適合在伺服器上只擁有少量儲存空間的使用者。

使用 IMAP 協定抓取郵件的時候，一開始只會列出郵件的標題，不會真正的下載郵件。直到使用者確定要讀取該郵件的時候，才會將該封內容抓取到 PC 上顯示，而且並不會將伺服器上的郵件刪除。如果使用者建立了不同的郵件夾作郵件分類的動作，這些郵件夾會建立在伺服器上，而不是建立在使用者的 PC 上。在郵件伺服器上擁有大量儲存空間且方便長時間連線在網路上的使用者，很適合使用 IMAP 協定來收取郵件。

在 FreeBSD 的軟體庫中，已經包含有數種 IMAP 與 POP 的伺服器端軟體，其中以卡內基美隆大學發展的 Cyrus-IMAP(提供 IMAP4/POP3 協定)、華盛頓大學發展的 IMAP-UW(提供 IMAP4/POP3 協定)，以及 QualComm 通訊公司發展的 Qpopper(只提供 POP3 協定)最爲有名。本文中將以華盛頓大學的 IMAP-UW 作爲範例，示範架設 IMAP 與 POP 的伺服器端軟體。

軟體與程式庫安裝

以下所有的操作程序，請依照順序執行，並請留意大小寫的不同。大小寫與空白的混淆，將造成操作上的失敗。

安裝 cclient 程式庫

cclient 是由華盛頓大學所發展的一個泛用型信箱(mailbox)處理程式庫。華盛頓大學所發展的一系列郵件相關軟體都需要這個程式庫。下列指令，可以安裝具備保密連線功能的 cclient 程式庫。

```
# cd /usr/ports/mail/cclient
# make WITH_SSL=YES install
```

安裝 IMAP-UW 伺服器軟體

IMAP-UW 被收錄在軟體庫的電子郵件分類中，安裝的指令如下

```
# cd /usr/ports/mail/imap-uw
# make WITH_SSL=YES install
```

以上會將 imapd ipop3d ipop2d 三支伺服器程式以及 mlock 這個輔助程式安裝到 /usr/local/libexec/ 目錄中。因爲目前 POP-2 協定幾乎已經不再使用，而由 POP-3 取代，因此在後文的設定中，將不討論 POP-2 的相關設定。

製作並安裝保密連線金鑰(key-pair)

IMAP/POP 與上一期所提到的 Sendmail 相同，在進行保密連線的時候都需要一把連線金鑰，我們可以利用下列指令來製作金鑰

```
# cd /usr/ports/mail/imap-uw
# make cert
```

這時候，螢幕上會陸續出現一些關於伺服器狀態的相關問題，請用英文依序

回答即可，切勿使用中文或是其他語言，以免造成某些郵件軟體運作不常。

這邊需要特別留心的是，當出現 Common Name (FQDN of your server)這一道問題的時候，必須回答伺服器在網路上所登錄的全名，例如後文圖片範例中出現的 beta.wsl.sinica.edu.tw，否則日後使用者操作保密連線時，郵件軟體會不斷跳出警告訊息，造成使用者的困擾。

回答完所有問題之後，連線金鑰會被安裝到 /usr/local/certs/ 目錄中，檔案名稱爲 imapd.pem，也會自動產生一個符號連結檔(symbolic link) ipop3d.pem 連結到 imapd.pem。

調整系統設定

IMAP-UW 伺服器軟體安裝完之後，並不能直接運作，還需要調整系統部分設定項目。包括啓動 IMAP/POP 服務的 /etc/inetd.conf 檔案、管理 client 連線範圍的 /etc/hosts.allow 檔案，以及管理使用者認證的 /etc/pam.conf 檔案。

/etc/inetd.conf 設定

IMAP 與 POP 服務可以由 /etc/inetd.conf 內設定執行，請用 vi 或是 joe 等文字編輯器，編輯 /etc/inetd.conf 檔案，並加入下列四行設定

```
pop3 stream tcp nowait root /usr/local/libexec/ipop3d ipop3d
imap4 stream tcp nowait root /usr/local/libexec/imapd imapd
pop3s stream tcp nowait root /usr/local/libexec/ipop3d ipop3d
imaps stream tcp nowait root /usr/local/libexec/imapd imapd
```

/etc/hosts.allow 設定

編輯 /etc/hosts.allow 可以對 client 端的連線 ip 作限制。一般來說，爲了方便使用者連線使用，會允許 client 端於任何地方連線。在 /etc/hosts.allow 檔案中加入下列兩行設定，可以達成此功能

```
imapd : ALL : allow
ipop3d : ALL : allow
```

/etc/pam.conf 檔案

IMAP-UW 伺服器軟體會參考 /etc/pam.conf 的設定，作爲對使用者認證方法的順序。請在 /etc/pam.conf 檔案中加入下列六行設定，以便 IMAP-UW 伺服器

軟體參照系統帳號來認證使用者

```
imap auth required pam_unix.so
imap account required pam_unix.so try_first_pass
imap session required pam_deny.so
pop3 auth required pam_unix.so
pop3 account required pam_unix.so try_first_pass
pop3 session required pam_deny.so
```

檢查 IMAP/POP 功能是否已經啓動

首先，以下列指令重新啓動 inetd 以便提供 IMAP/POP 服務

```
# killall -HUP inetd
```

以下列指令檢查 IMAP/POP 是否在正確的 port 上準備提供服務

```
# sockstat -l
```

若螢幕上出現的訊息包含以下四行，則表示 IMAP/POP 已經在預定的 port 準備提供服務。

```
root inetd 123 6 tcp4 *:110 *:*
root inetd 123 7 tcp4 *:995 *:*
root inetd 123 8 tcp4 *:143 *:*
root inetd 123 9 tcp4 *:993 *:*
```

請注意上面的訊息中，第三與第四欄的值可能會有所變化，每台機器都有可能不相同。若沒有出現這四個訊息，表示前述的操做發生了錯誤，請檢查系統記錄檔 /var/log/messages 內的訊息，了解錯誤發生的詳細狀況。

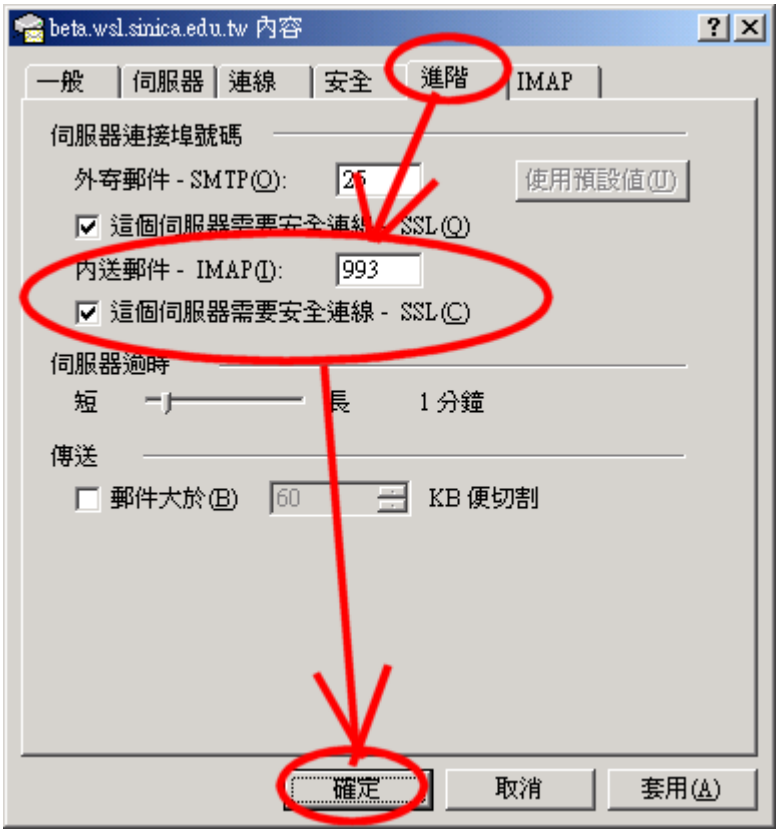
設定使用者的郵件程式使用保密連線

本段落以 Microsoft OutLook Express 以及 Netscape Messenger 爲範例，以圖例說如何設定明使用者抓取郵件時，受到保密連線的保護。

Microsoft OutLook Express 設定步驟

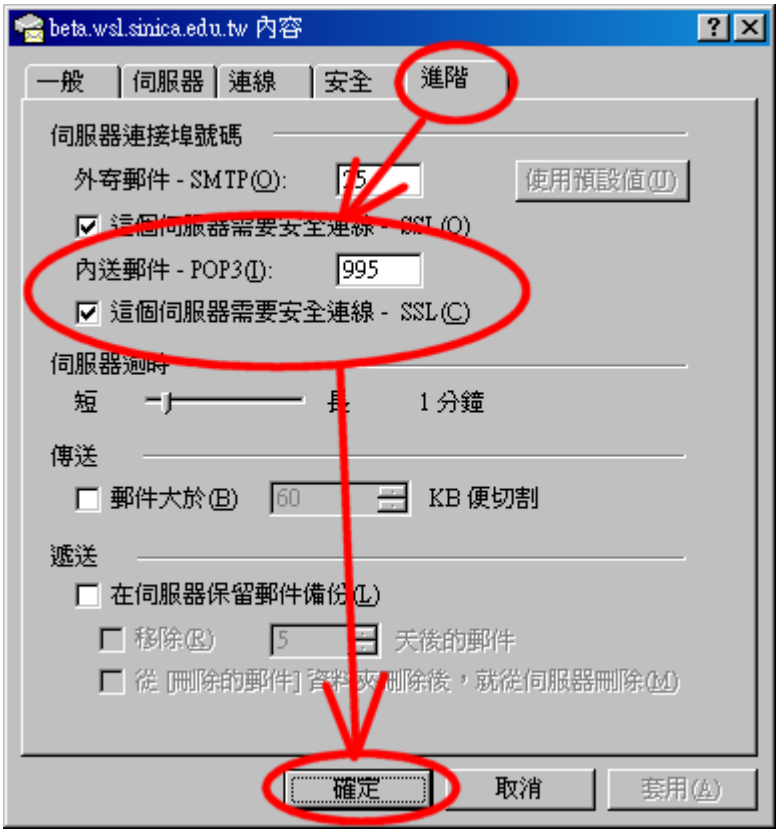
IMAP 範例(如圖一):

[OutLookExpress]-->[工具]-->[帳號]-->[郵件]-->[內容]-->[進階]-->[內送郵件-IMAP:993]-->[這個伺服器需要安全連線-SSL] (打勾)



POP 範例(如圖二):

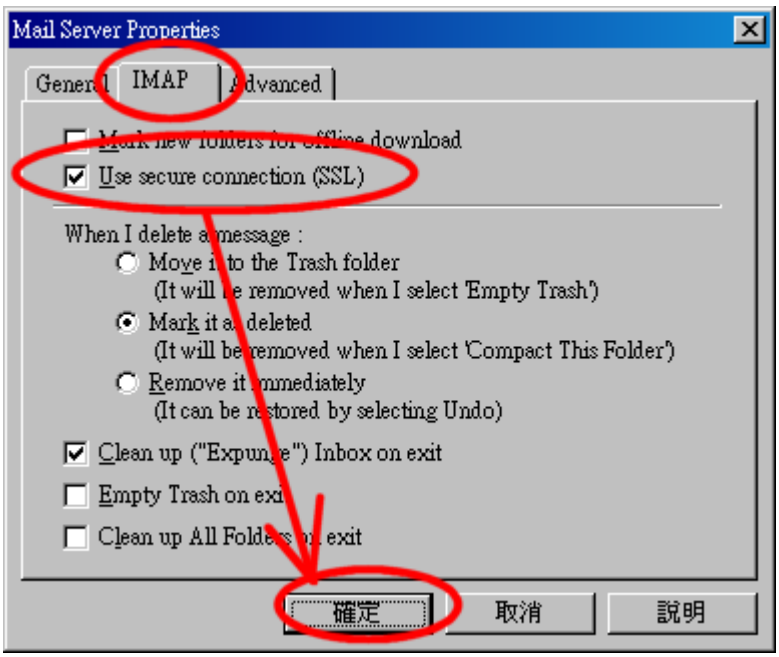
[OutLookExpress]-->[工具]-->[帳號]-->[郵件]-->[內容]-->[進階]-->[內送郵件-POP3:995]-->[這個伺服器需要安全連線-SSL] (打勾)



Netscape Messenger 設定步驟

IMAP 部分(如圖三):

[NetscapeMessenger]-->[Edit]-->[Preference]-->[Mail&Newsgroups]
-->[Mail Servers]-->[Incoming Mail Servers]-->[Edit]-->[IMAP]
-->[Use secure connection (SSL)] (打勾)



POP 部分:

由於 Netscape Messenger 不支援具有保密連線功能的 POP3 協定，因此無法在此位讀者示範。

結語

在此對於 Netscape Messenger 的使用者，筆者必須特別提出一點叮嚀。雖然 Netscape Messenger 使用 IMAP 抓取郵件的時候有支援保密連線功能，但是其內所附的『新進郵件檢查』功能，卻不支援保密連線。如果使用 Netscape Messenger 的『新進郵件檢查』功能，則您的通行碼將以明文(clear text)的方式在網路上傳送，造成潛在的洩密危機。不幸的是，該功能在軟體安裝後是預設爲啓用的。

因此筆者建議，在 Netscape 未修正此一問題之前，不要使用 Netscape Messenger 作爲您閱讀郵件的工具。

以上，就是在 FreeBSD 4.3-STABLE 版作業系統上，以華盛頓大學所發展的 IMAP-UW 伺服器軟體，搭配系統內建的 OpenSSL 功能建構具備保密連線的郵件伺服器的建構程序。使用合適的用戶端郵件軟體，可以在使用者收取郵件及閱讀的過程中，保護郵件的安全。