Mail Server安裝設定

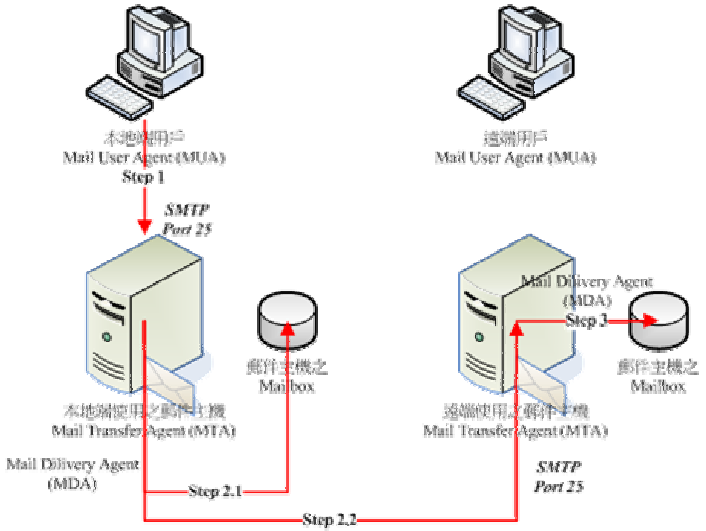
E-Mail簡介

陳柏愷

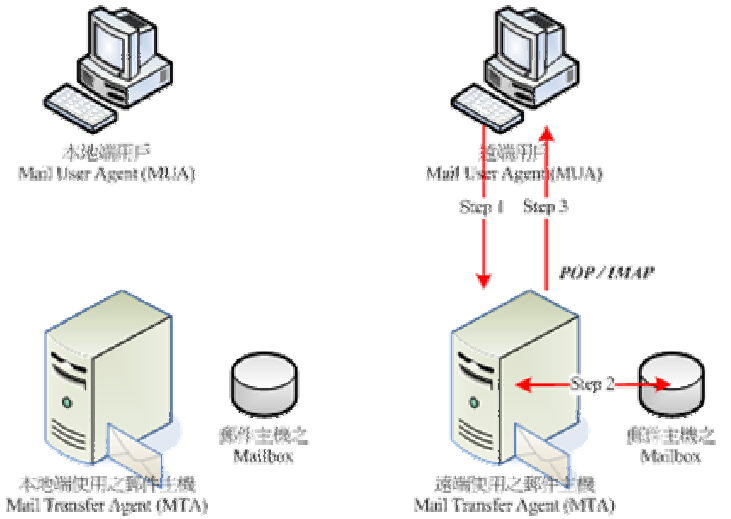
Mail是最複雜的網路服務

- 送信協定
  - SMTP
- 收信協定
  - POP3, IMAP
- DNS
  - MX record
- Web Mail
- 垃圾信過濾
- 病毒信過濾
- 信件備份
- 帳號與容量管理
- 高可用性
  - RAID
  - 多台主機備援
- 郵件簽章與加密

寄信流程



收信流程



名詞解釋

- MUA (Mail User Agent)
  - 郵件使用者代理人，負責在**使用者端**電腦收發信件
  - 如Outlook、Thunderbird等都是著名的MUA程式
- MTA (Mail Transfer Agent)
  - 郵件傳輸代理人，負責在**Mail Server端**收發信件
  - 負責收信、轉遞信件、回應MUA收信的功能
  - Sendmail、postfix、exim等都是著名的MTA程式
  - cyrus、dovecot通常負責MTA上，回應MUA收信的功能
- MDA (Mail Deliver Agent)
  - 郵件遞送代理人，基本上是MTA上的一個軟體元件，負責轉遞郵件
  - 負責分析郵件去向、過濾郵件、自動回覆等
  - MTA本身通常都具有基本MDA功能，procmail、spamassassion等是著名的MDA程式。procmail負責信件過濾、轉向等功能。spamassassion能分析處理垃圾郵件。
- Mailbox
  - 信件實際存放的所在地，通常是MTA主機上的/var/spool/mail/*username*，以檔案的形式存在

郵件相關協定

- SMTP (Simple Mail Transfer Protocol)
  - 送信的過程中，Mail Server端會開啟**port 25**，跑SMTP協定等待信送過來，**SMTP是一種『推』的協定，由送信端發起**。
  - Mail Client端連接Server端的port 25，使用SMTP協定與其溝通，達成**送信**的功能
  - Mail Server A要轉送信件到Mail Server B時，也是連線到Mail Server B的port 25
  - **SMTP協定只能傳輸ASCII文字**，因此如中文字、多媒體資料等等，必須經過MIME (Multipurpose Internet Mail Extensions)標準來做編碼轉換，以達到傳輸Binary的目的
  - SMTPs是架構在TLS/SSL的SMTP加密型協定，使用port 465 ，避免信件傳輸過程中被竊聽

郵件相關協定

- POP3(Protocol Of Post version 3)
  - 當信已經送達目標Mail Server端，使用者可使用MUA，連接Mail Server的**port 110**，使用POP3協定**將信取回使用者電腦**
  - **POP3是一種『拉』的協定**，由收信端發起
  - POP3s是架構在TLS/SSL的POP3加密型協定，使用port 995 ，避免信件傳輸過程中被竊聽
- IMAP(Internet Message Access Protocol)
  - 跟POP3一樣是**將信取回使用者電腦**的協定，然而IMAP具有一些比較進階的功能，如在**伺服器保留訊息狀態資訊**、自訂信件目錄、收信後仍在Server上保留原信件等。當使用者有多台電腦時，利用IMAP協定來收信，**可以讓不同電腦看到相同的信件狀態**
  - 因為IMAP具有以上特性，一般架設WebMail都使用IMAP協定
  - IMAP使用port 143，是一種『拉』的協定，由收信端發起
  - IMAPs是架構在TLS/SSL的IMAP加密型協定，使用port 993，避免信件傳輸過程中被竊聽

轉送信件的問題

- 如果任意來源的信件，Mail Server都協助其轉送的話，那此Mail Server很可能被當成**垃圾信件的中繼站**，此稱之為open relay的問題
- 一般Mail Server只提供**同一網域**底下的機器轉寄，如學校或公司
- 若不在同一個網域底下，則需經過**認證程序**才會轉寄
- 常見的認證是採用cyrus-sasl來處理

DNS與Mail的關係

- 為了提高信件遞送的成功性，DNS定義**MX record**來對應**同一網域**負責的**多台Mail Server**，並定義其**權重**，當高權重(數字較小)的Mail Server無法連線時，送信方會依序往下找尋可連線的目標。以下面的例子來說，除非5台機器都故障，才會無法送信到gmail.com

```
C:\Documents and Settings\user>nslookup -qt=mx gmail.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
```


使用SMTP協定來傳輸郵件

```
S: 220 www.example.com ESMTP Postfix
C: HELO mydomain.com
S: 250 Hello mydomain.com
C: MAIL FROM: <sender@mydomain.com>
S: 250 Ok
C: RCPT TO: <friend@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: test message
C: From: sender@mydomain.com
C: To: friend@example.com
C:
C: Hello,
C: This is a test.
C: Goodbye.
C: .
S: 250 Ok: queued as 12345
C: quit
S: 221 Bye
```

HELO *sendinghostname*	打招呼
EHLO *sendinghostname*	打招呼說要使用ESMTP
MAIL From: <*source email address*>	宣告寄件者
RCPT To:<destination email address>	宣告收件者
SIZE=*numberofbytes*	宣告信件大小，可不使用
DATA	宣告信件本體，以『.』來結束
QUIT	結束連線
VRFY *username*	確認username存在，建議不使用
EXPN *aliasname*	要求aliasname的列表，建議不使用
Subject: From: To: Cc: Reply-To:	信件的header

sendmail安裝設定

sendmail簡介

- sendmail是世界上最早，也是目前市占率最高的MTA程式
- sendmail具有效能低、安全性低、設定檔太艱澀的缺點
- 如果可以的話，盡量使用postfix或exim等新一代的MTA來取代sendmail
- 考試還是考sendmail為主

安裝sendmail與相關程式

- yum install sendmail sendmail-cf dovecot cyrus-sasl thunderbird

sendmail主要的設定檔

- **/etc/mail/sendmail.cf**
  - sendmail程式的主要設定檔，一般建議不要手動修改
  - 請手動修改/etc/mail/sendmail.mc 再以m4程式轉成 sendmail.cf
- **/etc/mail/local-host-names**
  - 設定本主機同時擁有多個主機名稱時候的收發信件主機名稱
- **/etc/mail/access.db**
  - 控制外來主機存取權限的檔案，不可手動編輯
  - 請手動修改/etc/mail/access.db，再以makemap程式轉換
- **/etc/mail/aliases.db**
  - 定義信箱別名，一般用來群組寄信，不可手動編輯
  - 請手動修改/etc/aliases ，再以newaliases程式轉換

sendmail主要的程式檔

- **/usr/sbin/sendmail**
  - sendmail 的主要執行檔，在發送信件時，就是使用這支程式。它會讀取 sendmail.cf 這個檔案的設定內容 ，預設的啓用的 port 是 25 。
- **/usr/sbin/makemap**
  - 將 access 轉成 access.db資料庫的執行檔
- **/usr/sbin/mailstats**
  - 查看到目前爲止sendmail 工作共傳送、接收多少郵件
- **/usr/bin/newaliases**
  - 將 /etc/aliases 轉成 /etc/mail/aliases.db 的執行檔
- **/usr/bin/mailq**
  - 用來觀察 /var/spool/mqueue 這個郵件暫存目錄的資料情況，如果太多信件在裡面，表示送信效能有問題，或有什麼地方卡住
- **/usr/bin/m4**
  - 將 *.mc 檔案轉成 *.cf 檔案的主要執行檔

sendmail相關目錄

- **/var/spool/mail**
  - 郵件『收受下來之後，每個使用者信件放置的目錄』，一個帳號會使用掉一個檔案，例如你的帳號 爲 test ，那麼你的信在 Server 中時，就是 /var/spool/mail/test 這個檔案
- **/var/spool/mqueue**
  - 當郵件由於對方主機的問題，或者是網路的問題，而無法送出去時，那麼該封郵件將會暫時的存放在這個目錄下，然後主機會每隔大約 30 ~ 60 分鐘重新嘗試傳送一遍，通常設定在五天內該封信件還寄不出去，那就會退給原發信者
- **/var/spool/clientmqueue**
  - 當你在郵件主機上，直接用sendmail寄信時，信件會被丟到這個目錄， 之後再被MTA發送出去，通常是被放到/var/spool/mqueue再傳送出去。如果你的機器上MTA沒有被啓動，這個目錄很容易被塞爆

m4設定

- 設定元件(`設定項目', `參數一', `參數二')
  - **左邊的是 quod ，也就是鍵盤上面數字鍵 1 的左邊那個按鍵『`』**
  - **右邊的是單引號『'』**
- **註解符號可以是 # 也可以是 “dnl” 這個字串**
- **divert** :是否要將說明資料(或者是註解資料)寫入輸出的檔案中 ，divert (-1) 爲不要，divert(0)是要
- OSTYPE(`linux')
- **define**：可以定義 sendmail 需要的參數，更多的define說明，可以參考 /usr/share/sendmail-cf/README
  - define(`ALIAS_FILE', `/etc/aliases')
- **undefine :** 與 define 相反，sendmail 預設會支援定義很多的項目，而如果您不需要定義該項目，則可以使用 undefine 來將他移除掉喔
- **FEATURE**：這個元件裡面會規定出 sendmail 所額外新增的一些任務，這些任務的支援必需要 sendmail 有提供才可以。可以在 /usr/share/sendmail-cf/feature 這個目錄當中找到 sendmail 所提供的各個功能
- **MAILER :** 設定所使用的郵件主機傳送郵件代理人(MDA)
  - MAILER(smtp)
  - MAILER(procmail)

更改郵件主機名稱

- /etc/hosts
  - *IP　　yourhost.yourdomain　(your-id.cyu.edu.tw)*
- /etc/mail/local-host-names
  - *yourhost.yourdomain　(your-id.cyu.edu.tw)*

允許連線相關設定

- /etc/mail/sendmail.mc
  - 將DAEMON_OPTIONS(`Port=smtp,Addr=**127.0.0.1**, Name=MTA')dnl
  - 改成 DAEMON_OPTIONS(`Port=smtp,Addr=**0.0.0.0**, Name=MTA')dnl
  - 執行m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
- /etc/mail/access
  - 加入一行Connect:192.168.1　　RELAY
  - 執行makemap hash /etc/mail/access.db < /etc/mail/access
- /etc/dovecote.conf
  - 將mail_location = mbox:~/mail:INBOX=/var/mail/%u ，前面的『#』拿掉，使其生效

設定防火牆、服務、及重新開機

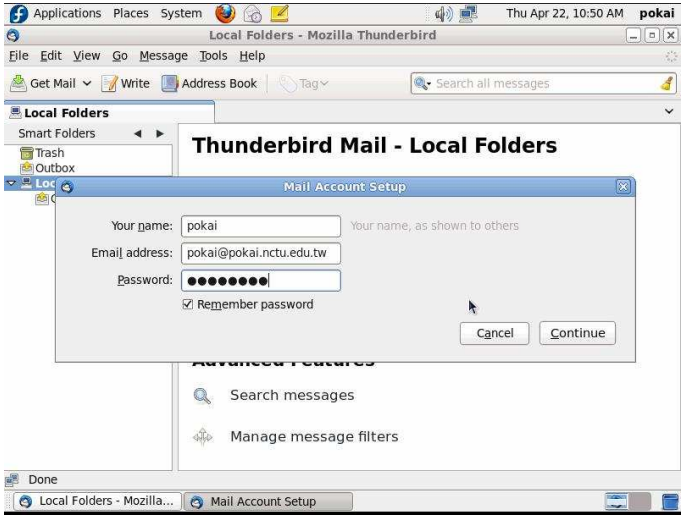
- ntsysv
  - 開sendmail, dovecot, saslauthd
- 開Firewall
  - IMAP over SSL(993)
  - Mail(SMTP)
  - POP-3 over SSL(995)
  - 在『Other Ports』的地方開pop3(110)跟imap(143)
- reboot

使用SMTP協定來傳輸郵件

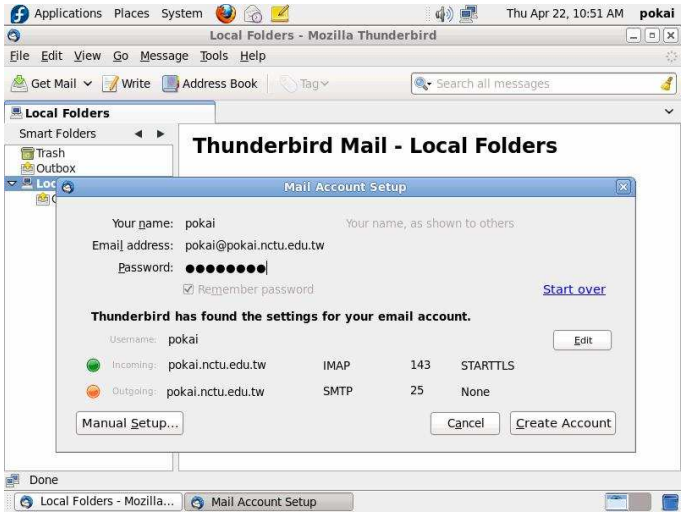
S: 220 www.example.com ESMTP Postfix
C: HELO mydomain.com
S: 250 Hello mydomain.com
C: MAIL FROM: <sender@mydomain.com>
S: 250 Ok
C: RCPT TO: <friend@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: test message
C: From: sender@mydomain.com
C: To: friend@example.com
C:
C: Hello,
C: This is a test.
C: Goodbye.
C: .
S: 250 Ok: queued as 12345
C: quit
S: 221 Bye

HELO *sendinghostname*	打招呼
EHLO *sendinghostname*	打招呼說要使用ESMTP
MAIL From: <*source email address*>	宣告寄件者
RCPT To:<destination email address>	宣告收件者
SIZE=*numberofbytes*	宣告信件大小，可不使用
DATA	宣告信件本體，以『.』來結束
QUIT	結束連線
VRFY *username*	確認username存在，建議不使用
EXPN *aliasname*	要求aliasname的列表，建議不使用
Subject: From: To: Cc: Reply-To:	信件的header

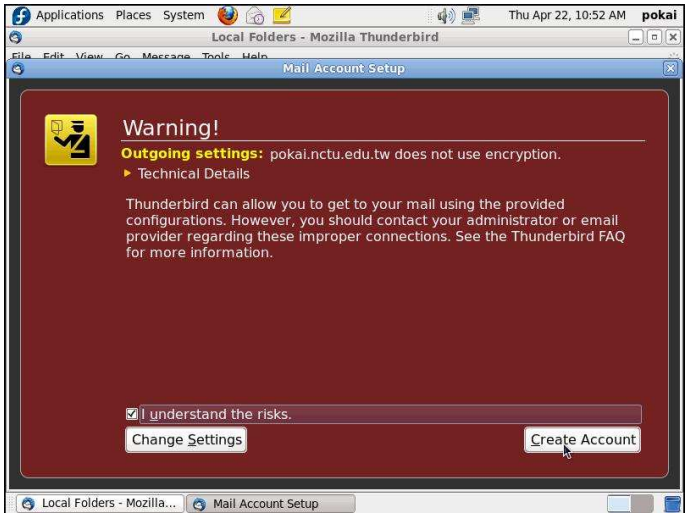
本機thunderbird設定(1/3)



本機thunderbird設定(2/3)



本機thunderbird設定(3/3)



練習

- 練習一
  - 從Mail主機上，開啓thunderbird，寄信給內部的自己(如user@your-id.cyu.edu.tw)
  - 看看信有沒有收到
- 練習二
  - 從Mail主機上，開啓thunderbird，寄信到外部信箱(如user@gmail.com)
  - 看看信有沒有收到

設定外來寄信權限(Relay)

- /etc/mail/sendmail.mc
  - 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
  - **以上兩行把『dnl #』拿掉**
  - 執行m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
- /etc/sysconfig/saslauthd
  - 把MECH=pam前面加上一個『#』，使其失效
- /etc/selinux/config
  - 把SELINUX=enforcing改成SELINUX=disabled
- 重開機

PC端outlook express設定(1/2)

PC端outlook express設定(2/2)

練習

- 練習三
  - 從PC上，開啓outlook express，寄信給內部的自己(如user@your-id.cyu.edu.tw)
  - 看看信有沒有收到
- 練習四
  - 從PC上，開啓outlook express ，寄信到外部信箱(如user@gmail.com)
  - 看看信有沒有收到

PC端outlook express設定-SMTP驗證

練習

- 練習五
  - 從PC上，開啓outlook express ，寄信到外部信箱(如user@gmail.com)
  - 看看信有沒有收到

aliases

- 別名:通常用來做群組，或有代表性的e-mail address
- 只有管理者可用，一般使用者不可用
- /etc/aliases
  - student:　　std01,std02,std03,std04
- 修改後須執行newaliases才會生效

forward

- 用來做個人的信件轉寄
- ~/.forward

```
localuser2
localuser3
remoteuser@gmail.com
```

- .forward所在使用者家目錄權限，其 group、other 不可以有寫入權限
- .forward 檔案權限，其 group、other 不可以有寫入權限

procmail

- procmail是一個著名的MDA，主要用來做信件過濾
- ~/.procmailrc

```
## 把中國大陸編碼的信直接丟掉
:0
* .*GB18030
/dev/null

##把已被標註為SPAM的信丟到垃圾信夾
:0
* ^Subject:.*SPAM
spam-mail
```