Mail Server Log 查詢技巧-從郵件紀錄器下手

說明:

常常都會發現有些使用者會說,客戶寄來的信我都沒有收到,我們的 MailServer 會漏信,這時候就必須查詢 Log 以釐清原因,否則可能會錯怪到某一方,就冤枉好人了 ~

所以遇到這類的問題,查 Log 是最直接的方法.

一封信從 A 寄出到 B 收件者收到 簡單的路徑是:

1. A 寄件者寫信軟體(outlook / thunderbir 或 webmail)上寫信
2. 寄到自己的 A mail server 上
3. A mail server 寄到 對方的 B mail server
4. 對方的 B mail server 收下信
5. 等待 B 收件者過 pop/imap 連線收信,或直接用 webmail 收看信

但是現在的 Mail Server 大都因為垃圾郵件猖獗,所以都會有自己的防禦手段,來阻擋垃圾信,所以上面的路徑可能在任何一點都可能會被阻止,甚至信就被『吃』掉 ~~

在 UMail 上如果沒有被 『郵件條件過濾器』 所捕捉到的信,都會出現在『郵件紀錄器』上,除非你把這個功能關閉,或是設定某些人的的信不紀錄.

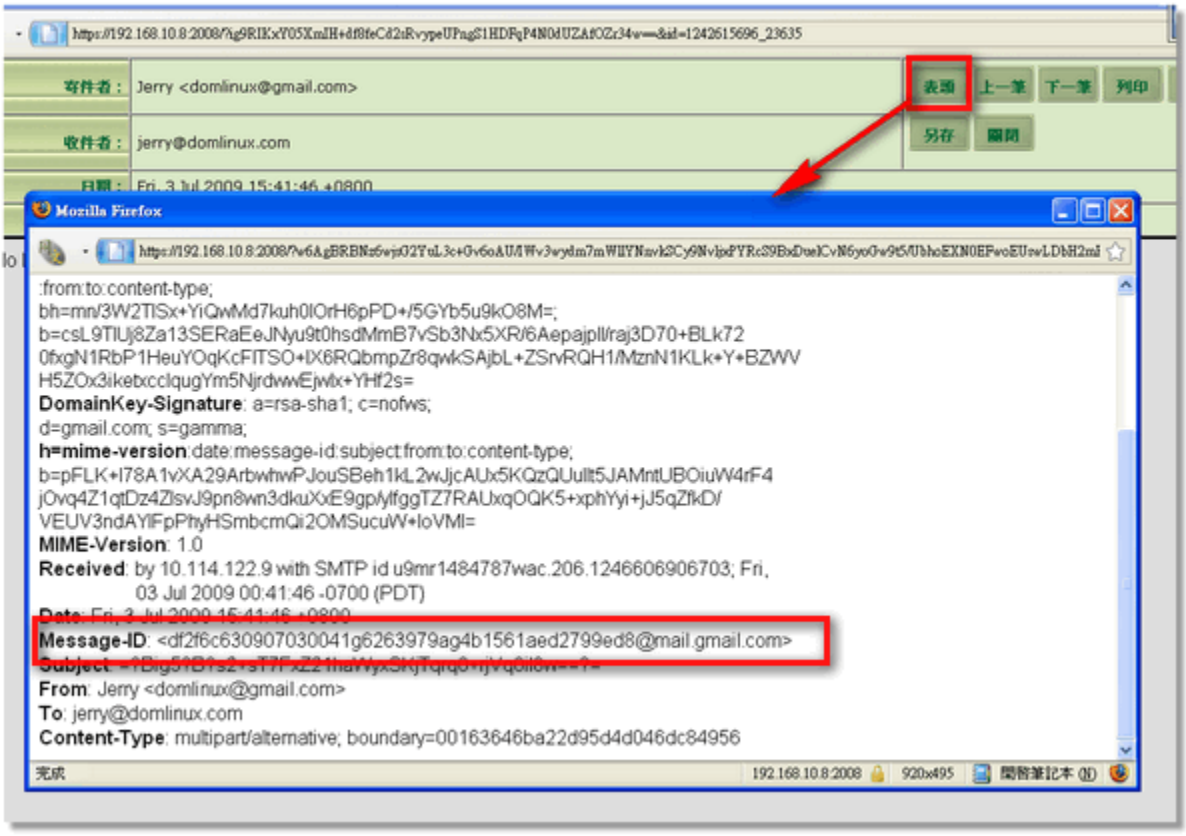
從 『郵件紀錄器』下手,先知道信件有沒有確定寄到我們的伺服器,正常應該是先查詢 SMTP Log ,但是因為 SMTP Log 比較屬於 『分解動作』, 一般人不容易快速查詢到你想查詢的資料, 所以建議先看郵件紀錄器.

首先在郵件紀錄器先查詢到你要找的信件, 你可以用 『時間』 ,』寄件者』 , 『主旨』 , 『收件者』 搜尋到該信 , 如果在郵件記錄器找不到你想找的信,可能 :

1. 如果有開啟 『灰名單』 機制,查看看是不是被擋在紀錄區
2. 當成有病毒的信,被隔離在病毒郵件隔離區
3. 被你所設定的過濾器阻檔,請檢查條件過濾器的隔離區
4. 對方的伺服器沒有正確把信遞送過來,或寄件者把地址寫錯

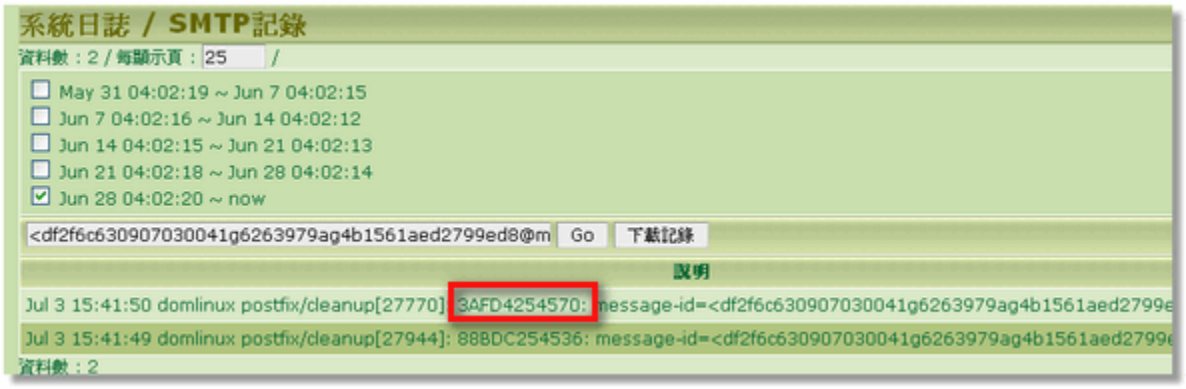
找到該信後,記下該信的時間

打開該信,查閱表頭,並找到信件的 **Message-ID**



複製這個 **Message-ID**；貼到系統日誌->SMTP Log 查詢

注意 ：Log 看的時間順序是 **從下往上看**,越上面的 Log 越接近現在的時間

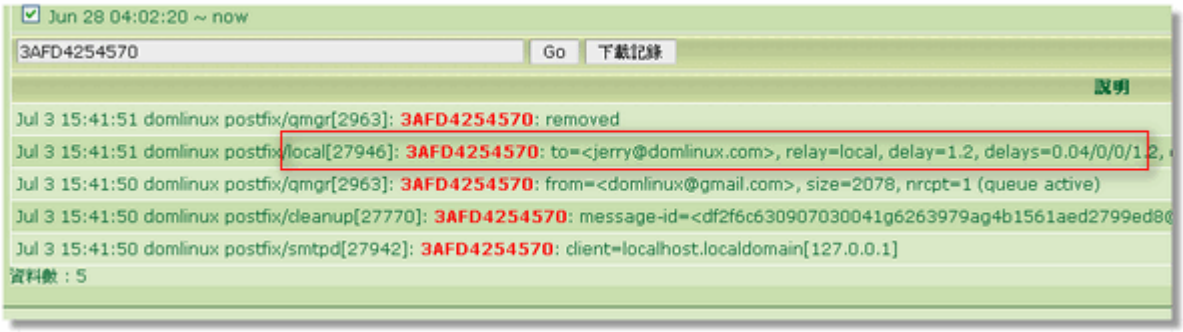


一般會查詢到至少 2 筆紀錄,如果你只有查詢到 1 筆,就表示信件沒有到達收件者的信箱.

第一筆 (下面那筆) Log，是對方伺服器寄到我方的伺服器所產生的 Log，其中 88BDC254536 這個序號是 QueueID (儲列 ID)，你可以用這個 ID 查詢 Log

可以查詢到當時 Server 對 Server 的交談內容

再來查詢 另一個 QueueID : 3AFD4254570 ,正常狀況下這封信遞送給本地的帳號



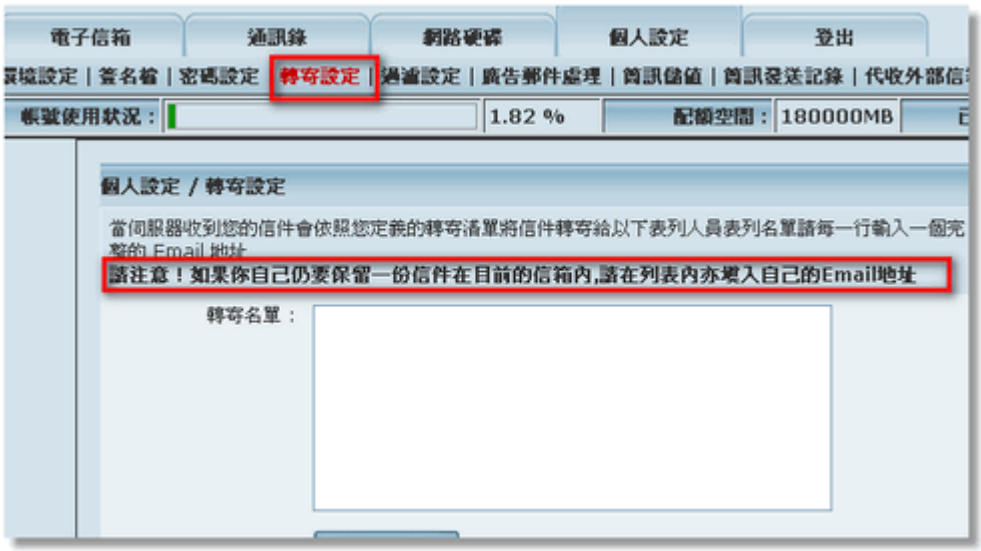
確定有遞送給本地的使用者

如果有這筆紀錄,而收件者表示沒有收到信,這時需找看看

- 是不是信件被判斷為 SPAM 信件,查查看 垃圾郵件處理器 / 垃圾郵件隔離區
- 是不是收件者設定了某些過濾條件將信件過濾,請登入 User 的 Webmail 查詢

- 或查詢過濾器設定紀錄

- 或是使用者設定的轉寄,也可能會把信件給轉走了, 注意: 如果有設定轉寄而沒有在轉寄名單上設定自己,則不會保留信給自己



- 最後 查看看是不是使用者自己把信收走了,或已經刪除

上面的 Log 顯示 Jerry 已經在 7/3 16:39 25 秒 透過 IMAP 方式,把信件從收件匣移到垃圾桶 ,所以信件已經不在收件匣,如果要更細的 Log ,也許你想知道是從哪個 IP 連線執行這個動作,你可以用時間 『Jul 03 16,jerry』 把當時 jerry 全部的 Log 調閱,你也許會查出類似的 Log