郵件歸檔伺服器

MArchive 全系列

管理者共用手冊

V 7.0.4.0

製作手冊: HERHSIANG FREEDY

出版日期：2023 / 06 / 10 修改日期: 2024 / 4 / 19

www.herhsiang.com / www.herhsiang.com.tw

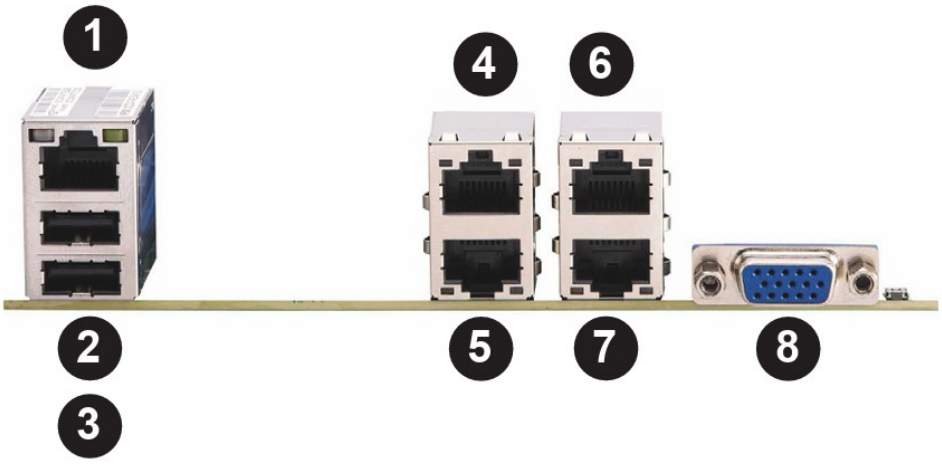
目　　錄

第 1 章 第一次安裝

1-1、郵件歸檔伺服器硬體及介面說明

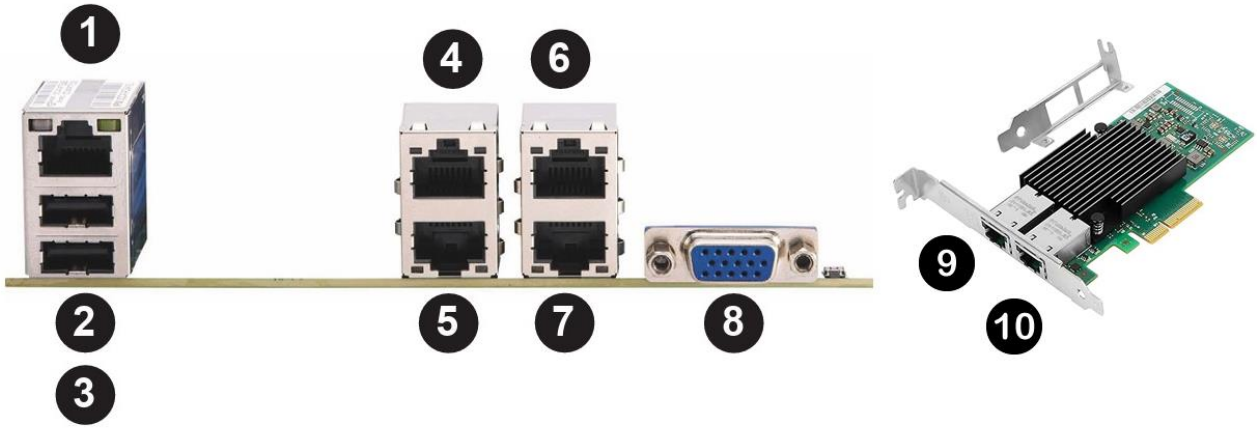
郵件歸檔伺服器機器圖，以 MArchive H368 / H57TA / H91X 為範例。

圖 1-0-1、郵件歸檔伺服器的外觀 MArchive H57TA 主機



1. RJ45 IPMI網路連接埠 (可用, IP KVM)
2. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
3. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
4. RJ45 乙太網路連接埠3 (可用, iSCSI)
5. RJ45 乙太網路連接埠1 (可用, LAN)
6. RJ45 乙太網路連接埠4 (無功能)
7. RJ45 乙太網路連接埠2 (可用, HA)
8. VGA連接埠6 (可用, Console)

圖 1-0-2、MArchive H368 1G 標準配備後端 I/O 配置



1. RJ45 IPMI網路連接埠 (可用, IP KVM)
2.USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
3.USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
4. RJ45 乙太網路連接埠3 (可用, iSCSI)
5. RJ45 乙太網路連接埠1 (停用, LAN)
6. RJ45 乙太網路連接埠4 (無功能)
7. RJ45 乙太網路連接埠2 (停用, HA)
8. VGA連接埠6 (可用, Console)
9. 雙埠10G RJ45 乙太網路連接埠 (可用, LAN)
10. 雙埠10G RJ45 乙太網路連接埠 (可用, HA)

圖 1-0-3、MArchive H368 10G 選購配備後端 I/O 配置

1、RJ45 IPMI 連接埠

可當 IP KVM, 遠端遙控開關機，及觀看螢幕鍵盤當 Colsone 使用)。

2、USB 2.0 (可接鍵盤或外接碟，Console)

3、USB 2.0 (可接鍵盤或外接碟，Console)

4 & 6、網路接口 1-2

10 / 100 / 1000Mbps 自動選取乙太網路介面，由管理者配置在閘道器模式下，哪一個是對內/對外的網卡，管理者可以配置 2 個不同區段的橋接。

5、RJ45 網路連接埠(LAN)

郵件歸檔伺服器的 LAN 是 10 / 100 / 1000Mbps 自動選取乙太網路介面，將內部的網路連結在此網路介面，讓管理者可以進入系統的管理介面，授權的使用者也是利用這個介面進入使用者介面。

7、HA

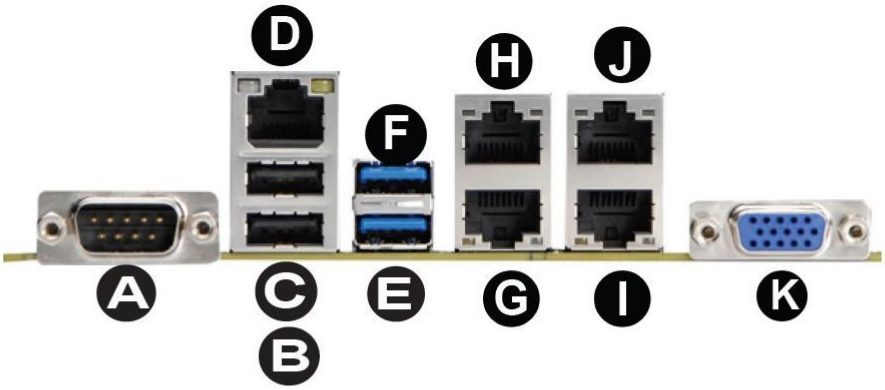
10 / 100 / 1000Mbps 自動選取乙太網路介面，啟用 HA 功能後將 2 台的郵件歸檔伺服器 HA 對接在一起，執行 HA 的任務。

8、VGA 顯示連接埠（接螢幕）(Console)

9 & 10、10G 光纖網路連接埠，網路接口 3 - 4 （擴充模組選購）

1000M / 10000Mbps 自動選取乙太網路介面，由管理者配置在閘道器模式下，哪一個是對內/對外的網卡，管理者可以配置 2 個不同區段的橋接。

圖 1-1-1、郵件歸檔伺服器的外觀 MArchive H57TA 主機



A. RS232 COM1序列連接埠 (無功能)

B. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)

C. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)

D. RJ45 IPMI連接埠 (可用, IP KVM)

E. USB (3.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)

F. USB (3.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)

G. RJ45 乙太網路連接埠1 (可用, LAN)

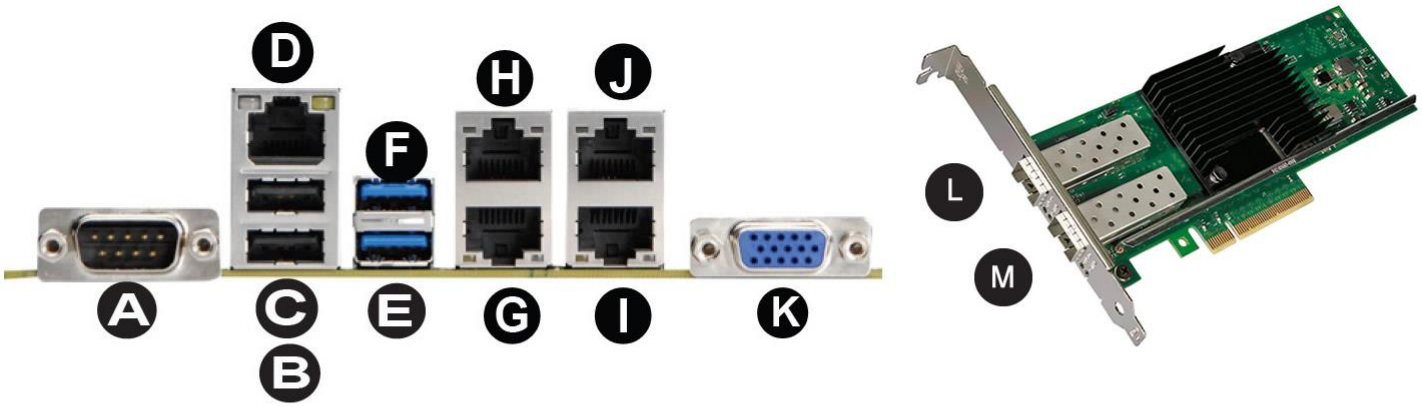
H. RJ45 乙太網路連接埠3 (可用, Port 1)

I. RJ45 乙太網路連接埠2 (可用, HA)

J. RJ45 乙太網路連接埠4 (可用, Port 2)

K. VGA 顯示連接埠 (可用, Console)

圖 1-1-2、MArchive H57TA 1G 標準配備後端 I/O 配置



A. RS232 COM1序列連接埠 (無功能)
B. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
C. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
D. RJ45 IPMI連接埠 (可用, IP KVM)
E. USB (3.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
F. USB (3.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
G. RJ45 乙太網路連接埠1 (可用, LAN)
H. RJ45 乙太網路連接埠3 (可用, Port 1)
I. RJ45 乙太網路連接埠2 (可用, HA)
J. RJ45 乙太網路連接埠4 (可用, Port 2)
K. VGA 顯示連接埠 (可用, Console)
L. 10G介面卡光纖GBIC連接埠 (可用, Port 3)
M. 10G介面卡光纖GBIC連接埠 (可用, Port 4)

圖 1-1-3、MArchive H57TA 10G 選購配備後端 I/O 配置

A、RS-232 Port

無功能作用

B、USB 2.0 (可接鍵盤或外接碟，Console)

C、USB 2.0 (可接鍵盤或外接碟，Console)

D、RJ45 IPMI 連接埠

可當 IP KVM, 遠端遙控開關機，及觀看螢幕鍵盤當 Colsone 使用)。

E、USB 3.0HDD (可接鍵盤或外接碟，Console)

F、USB 3.0HDD (可接鍵盤或外接碟，Console)

G、RJ45 網路連接埠(LAN)

郵件歸檔伺服器的 LAN 是 10 / 100 / 1000Mbps 自動選取乙太網路介面，將內部的網路連結在此網路介面，讓管理者可以進入系統的管理介面，授權的使用者也是利用這個介面進入使用者介面。

H & J、網路接口 1-2

10 / 100 / 1000Mbps 自動選取乙太網路介面，由管理者配置在閘道器模式下，哪一個是對內/對外的網卡，管理者可以配置 2 個不同區段的橋接。

I、HA

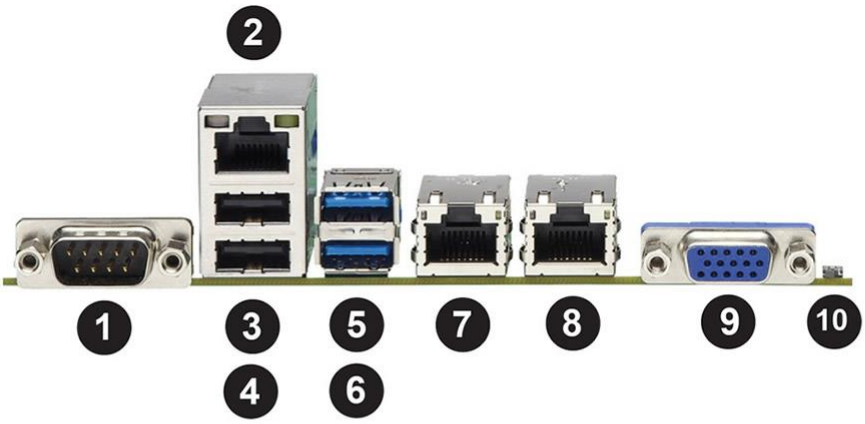
10 / 100 / 1000Mbps 自動選取乙太網路介面，啟用 HA 功能後將 2 台的郵件歸檔伺服器 HA 對接在一起，執行 HA 的任務。

K、VGA 顯示連接埠（接螢幕）(Console)

L & M、10G 光纖網路連接埠，網路接口 3 - 4 （擴充模組選購）

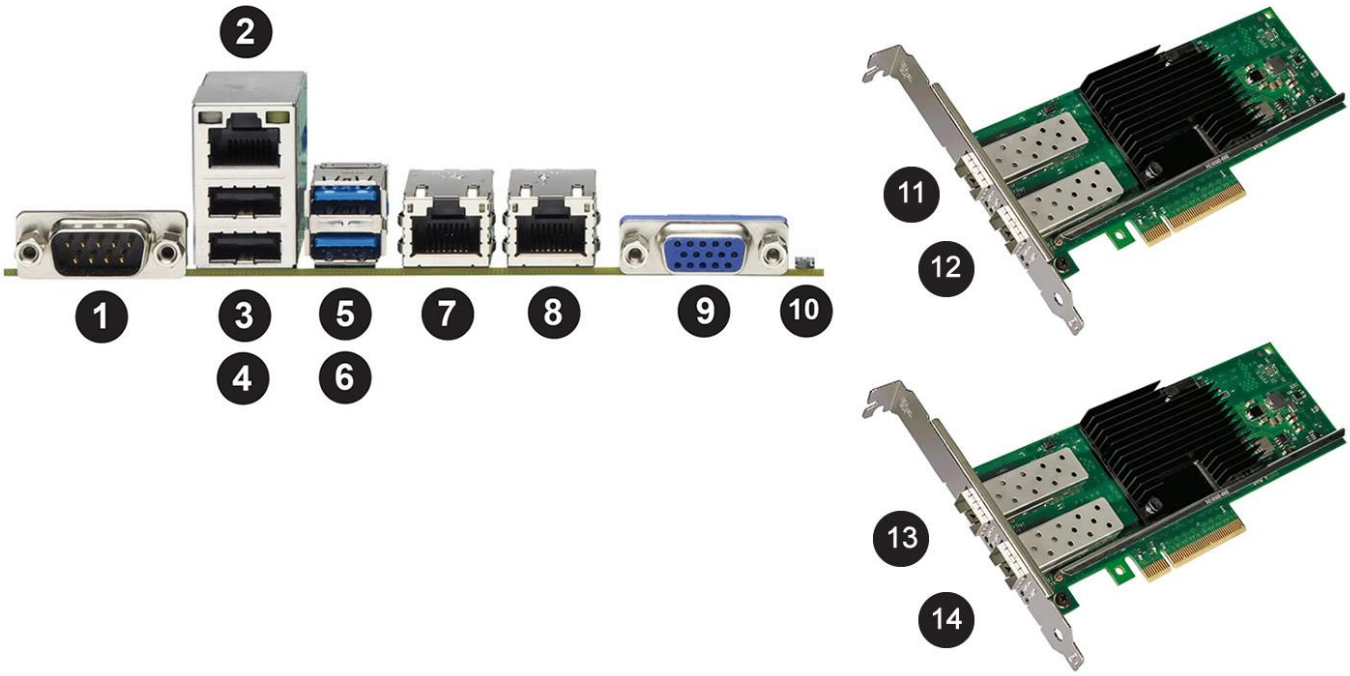
1000M / 10000Mbps 自動選取乙太網路介面，由管理者配置在閘道器模式下，哪一個是對內/對外的網卡，管理者可以配置 2 個不同區段的橋接。

圖 1-1-4、郵件歸檔伺服器的外觀 MArchive H91XT 主機



1. RS232 COM1序列連接埠 (無功能)
2. RJ45 IPMI連接埠 (可用, IP KVM)
3. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
4. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
5. USB (3.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
6. USB (3.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
7. RJ45 乙太網路連接埠1 (可用, LAN)
8. RJ45 乙太網路連接埠2 (可用, HA)
9. VGA 顯示連接埠 (可用, Console)
10. UID Switch (無功能)
11. 10G介面卡光纖GBIC連接埠 (定義1)
12. 10G介面卡光纖GBIC連接埠 (定義2)

圖 1-1-5、MArchive H91XT 10G 標準配備後端 I/O 配置



1. RS232 COM1序列連接埠 (無功能)
2. RJ45 IPMI連接埠 (可用, IP KVM)
3. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
4. USB (2.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
5. USB (3.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
6. USB (3.0) 連接埠 (可用, 鍵盤滑鼠/外接碟)
7. RJ45 乙太網路連接埠1 (可用, LAN)
8. RJ45 乙太網路連接埠2 (可用, HA)
9. VGA 顯示連接埠 (可用, Console)
10. UID Switch (無功能)
11. 10G介面卡光纖GBIC連接埠 (可用, 定義1)
12. 10G介面卡光纖GBIC連接埠 (可用, 定義2)
13. 10G介面卡光纖GBIC連接埠 (可用, 定義3)
14. 10G介面卡光纖GBIC連接埠 (可用, 定義4)

圖 1-1-6、MArchive H91XT 追加第 2 組 10G 選購配備後端 I/O 配置

1、RS-232 Port

無功能作用

2、RJ45 IPMI 連接埠

可當 IP KVM, 遠端遙控開關機，及觀看螢幕鍵盤當 Colsone 使用)。

3、USB 2.0 (可接鍵盤或外接碟，Console)

4、USB 2.0 (可接鍵盤或外接碟，Console)

5、USB 3.0 (可接鍵盤或外接碟，Console)

6、USB 3.0 (可接鍵盤或外接碟，Console)

7、RJ45 網路連接埠(LAN)

郵件歸檔伺服器的 LAN 是 10 / 100 / 1000Mbps 自動選取乙太網路介面，將內部的網路連結在此網路介面，讓管理者可以進入系統的管理介面，授權的使用者也是利用這個介面進入使用者介面。

8、HA

10 / 100 / 1000Mbps 自動選取乙太網路介面，啟用 HA 功能後將 2 台的郵件歸檔伺服器 HA 對接在一起，執行 HA 的任務。

9、VGA 顯示連接埠（接螢幕）(Console)

10、UID Switch（無功能）

11 & 12、網路接口 1-2

1000 / 10000Mbps 自動選取乙太網路介面，由管理者配置在閘道器模式下，哪一個是對內/對外的網卡，管理者可以配置 2 個不同區段的橋接。

13 & 14、10G 光纖網路連接埠，網路接口 3 - 4 （擴充模組選購）

1000M / 10000Mbps 自動選取乙太網路介面，由管理者配置在閘道器模式下，哪一個是對內/對外的網卡，管理者可以配置 2 個不同區段的橋接。

1-2、第一次進入管理介面

步驟 1：

插入電源及開啟設備電源後，在第一次開機的狀況下，郵件歸檔伺服器會自動格式化內建的硬碟機，約 2-3 分鐘整個開機動作就會完成，可進行下一步的設定動作。

步驟 2：

將管理者的電腦和郵件歸檔伺服器的 LAN 介面接到同一個 Switch 或者將管理者電腦直接跟郵件歸檔伺服器的 LAN 連線，設備的所有網路接口都支援 Auto-MDI/MDI-X，所以用普通的網路線直接對接就可以。

步驟 3：

更改管理者的 IP 位址跟郵件歸檔伺服器 LAN 的預設 IP 位址相同的網段，郵件歸檔伺服器的預設 IPV4 位址是 192.168.2.1 / 255.255.255.0，將管理者的 IP 位址設定成 192.168.2.X 區段內除了 1 以外的任何 IPV4 位址，讓管理者可進入系統的管理介面。

以 Windows 10 的作業系統為例，在管理者電腦的 設定 ➔ 網路及網際網路 ➔ 變更介面卡選項 ➔ 網路連線 ➔ 乙太連線 ➔ 內容 ➔ 網際網路通訊協定第 4 版(TCP/IPV4) ➔ 內容中將電腦的 IP 位址設為 192.168.2.66 /255.255.255.0，預設閘道不需要設定。(圖 1-2)

圖 1-2、更改管理者的 IP 位址

步驟 4：

執行瀏覽器(IE，FireFox，Chrome)，並在瀏覽器的網址列上填入 https://192.168.2.1:88 ，就會出現郵件歸檔伺服器的管理介面，管理介面是使用 https 加密的 SSL 連線，預設通訊埠是 88。

輸入預設的管理者帳號與密碼，預設的管理者帳號及密碼如下。(圖 1-3)

帳號：admin

密碼：adminpw

圖 1-3、進入管理介面

郵件歸檔伺服器的管理介面會自動偵測管理者的使用語系並且自動切換，例如，管理者的電腦使用英文語系，進入管理登入介面時就會自動切換成英文介面。目前支援英文、繁體中文跟簡體中文等 3 種語系，預設的語系是英文，進入管理介面前，也可以從右上方的語系切換紐直接切換適當的語系。(圖 1-4)

圖 1-4、語系切換鈕

登入成功後會出現首頁區，系統的首頁區分成 4 個區域，分別是 (1)選單區、(2)系統資訊區、(3)個人帳號及登出區、(4)管理介面說明區。(圖 1-5)

圖 1-5、管理介面首頁

(1)、選單區

在選單的管理上，郵件歸檔伺服器採取 2 階層的選單，分別是主選單跟次(子)選單，主選單是依照提供的主功能分類，例如，運作架構管理的相關設定通通歸在架構管理主選單中，至於他的次選單則用橫列的方式展示。(圖 1-6)

圖 1-6、主選單跟次選單

(2)、系統資訊區

顯示系統的即時訊息跟狀態，例如，版本、系統資源及連線資訊等，讓管理者在第一個時間內就能了解整台設備的資訊。

(3)、個人帳號及登出區

這個區域會顯示登入者的帳號及登出的按鈕，如果需要即時的切換語系，也可以在這個地方切換。

(4)、管理介面說明區

這個區域有 2 個部份，最左的部分是首頁標題，另一個是主選單顯示。首頁標題部分管理者可以在系統管理的系統設定中輸入代表這台設備的文字，方便管理者在操作多台設備下辨識，在主選單路徑的顯示部分，顯示管理者當下的主選單名稱。

1-3、首頁的系統資訊

在首頁的系統資訊區共分成 5 大塊，分別是系統時間、伺服器系統資源、軟體訊息、伺服器服務及重要信息。介紹如下：

(一)、系統時間

顯示目前系統的日期/時間、時區與開機時間。(圖 1-7)

圖 1-7、系統時間資訊

- 【伺服器日期 / 時間】：顯示郵件歸檔伺服器的系統日期及時間。例如，2023-06-04 : 15:55:31，2023-06-04 是日期，15:55:31 就是當下的時間，系統具有網路時間伺服器校正時間的功能，詳細的設定在系統管理中的系統設定。
- 【現在時區】：顯示目前設備設定的時區，例如，Asia/Taipei，就是目前的時區是以亞洲的台北時區。
- 【伺服器開機時間】：顯示郵件歸檔伺服器從開機到現在的運作時間，每次重新開機後，數字會被歸零。

(二)、伺服器系統資源：

顯示郵件歸檔伺服器硬體資源及使用狀況，如 CPU(型號/系統負載)、記憶體、硬碟、虛擬記憶體、域名/全部郵件帳號數量等。(圖 1-8)

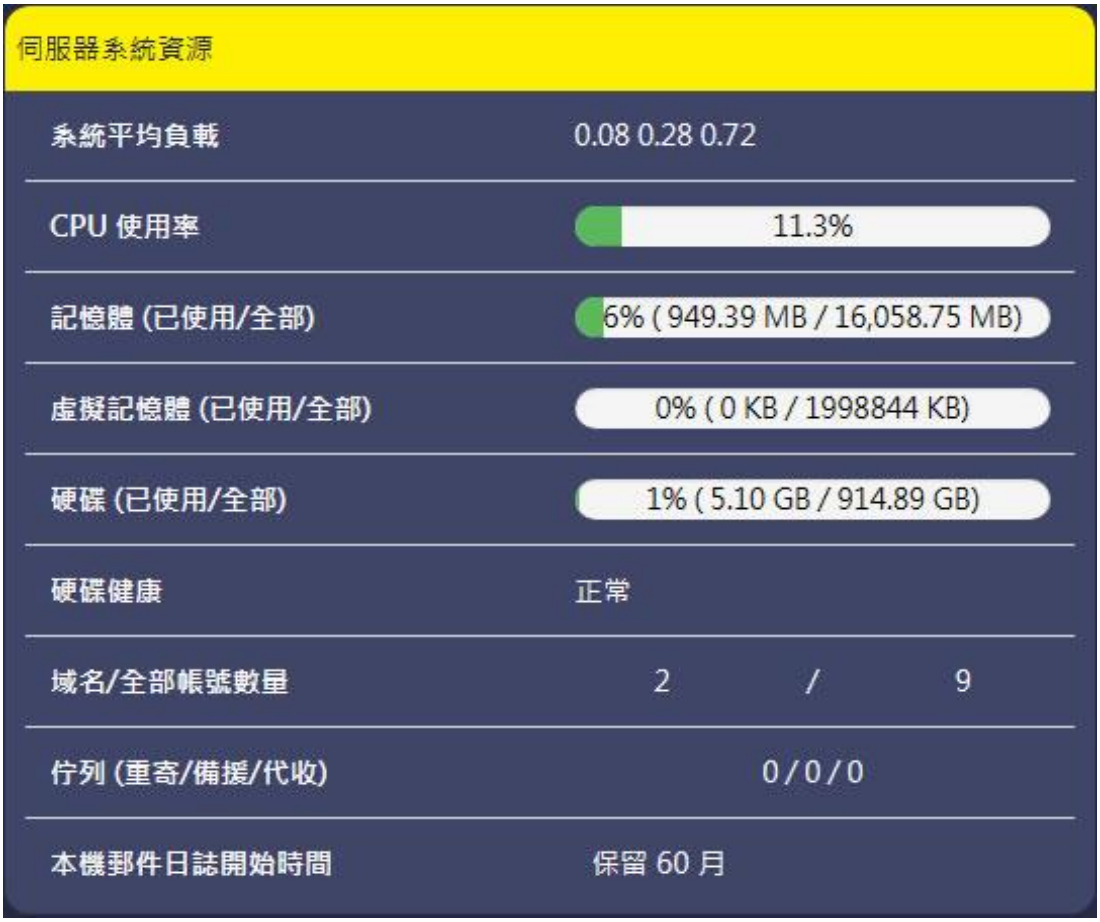


圖 1-8、系統資源

- 【系統平均負載】：系統負載的資訊，一般來說，系統負載超過 10，硬碟的讀寫幾乎是滿載的狀況，資料每 3 秒鐘會自動更新一次。
- 【CPU 使用率】：目前 CPU 使用量，每 3 秒鐘會自動更新。
- 【記憶體 (已使用/全部)】：伺服器配置的全部記憶體數量跟目前已使用的數量及比例，例如，6%(949.39MB / 16058.75MB)，代表系統配置 16GB 的記憶體，在當下郵件歸檔伺服器已經使用 949.39MB，佔全部的 6%，每 10 秒鐘會自動更新一次。
- 【虛擬記憶體 (已使用/全部)】：伺服器配置的虛擬記憶體量跟目前已使用的數量及比例，在正常運作下，系統會自動回收目前沒在使用的記憶體，儘量不用到用硬碟模擬的虛擬記憶體。例如，0%(0 KB / 11998844KB MB)，代表系統配置 11998844KB 用硬碟模擬的虛擬記憶體，在當下郵件歸檔伺服器已經使用 0KMB，佔全部的 0%，每 10 秒鐘會自動更新一次。

- 【硬碟 (已使用/全部)】：伺服器配置的硬碟容量跟目前已使用的數量及比例，例如，1%(5.10 GB / 914.88 GB)，代表硬碟容量是 914.88GB(約是 1TB 的硬碟)，已經使用 5.10GB ，佔全部的 1 %，每 1 小時會自動更新一次。
- 【硬碟健康】：郵件歸檔伺服器會自動偵測硬碟的磁區狀況，如果出現錯誤時，會主動通知管理者，進行處置。
- 【網域/全部帳號數量】：郵件歸檔伺服器目前設定的網域數量及可登入系統使用者介面查詢被記錄郵件的帳號數量。

(三)、軟體訊息

顯示設備型號、機器序號等軟體訊息。(圖 1-9)

圖 1-9、軟體訊息

- 【伺服器型號】：郵件歸檔伺服器的型號，共有 2 種，分別是 MArchive H57TA & Marchive H91XT。
- 【伺服器軟體版本】：目前系統運作的軟體，HERHSIANG 會不定期的更新運作版本，管理者可以隨時注意 HERHSIANG 官網的**最新消息 - > 線上版更說明**所發佈更新消息。
- 【機器序號】：機器的身分證，根據這個號碼提供保固維修等資訊。

(四)、伺服器服務

目前在系統上運作的各項服務啟動與否，其中病毒信過濾 –Kaspersky 需要上傳授權碼才啟用，SQL 服務如果顯示停用，則系統將無法紀錄郵件。(圖 1-10)

圖 1-10、伺服器服務訊息

- 【垃圾信過濾】：系統上的垃圾信過濾功能是否啟動？這個功能的啟用與否，管理者可以自行決定。
- 【病毒信過濾 - ClamAV】：內建的病毒信過濾引擎 ClamAV 是否啟用？ClamAV 的病毒碼更新並不需要收取年費。
- 【病毒信過濾 - Kaspersky】：郵件歸檔伺服器有另一個病毒信過濾引擎，Kaspersky，他需要上傳授權碼才能啟用，**且每年都需要病毒碼的更新費用**。
- 【垃圾信過濾-AI】：7.0.4.0 開始支援，郵件歸檔伺服器有另一個自動化垃圾&釣魚信過濾引擎，AI Spam，他需要上傳授權碼才能啟用，且**每年都需要特徵碼的更新費用**。
- 【SQL 服務】：系統的 SQL 服務是否正常運作，當 SQL 服務不是正常運作時，系統無法紀錄郵件。
- 【透通模式 – 外對內服務】：在透通模式下，從外面寄到郵件伺服器主機的郵件會被記錄。

- 【透通模式 – 內對外服務】：在透通模式下，從郵件伺服器主機寄到外面的郵件會被記錄。【透通模式 – 代收重送服務】：在透通模式下，當後端的郵件伺服器故障，無法收送郵件時，有這項功能，郵件稽核過濾伺服器會把郵件代收下來，因為郵件伺服器已經故障，無法正常提供寄送服務，此時具有登入使用者介面權限的使用者登入後，可以看到被代收的郵件內容，利用系統提供的轉寄功能，將郵件轉寄出去，轉寄的對象不能是原本已經故障的郵件伺服器內的帳號，必須是可以正常運作的郵件主機中的帳號。

  這一個功能輔助後端的郵件主機，萬一發生故障無法提供郵件收送服務時，讓使用者可以看到郵件內容並緊急的處理重要的郵件，當郵件主機恢復正常後，所有被代收的郵件，就會傳送回去。

(五)、重要信息

系統的登入信息，哪一位管理者在何時登入？用哪一個帳號登入，成功或是失敗，在這裡都會顯示。(圖 1-11)

圖 1-11、伺服器重要訊息

(六)、登出

結束管理介面的運作時，可以點選右上方  圖示登出。

第 2 章 運作架構說明

管理者第一次進入郵件歸檔伺服器的管理介面後，有幾個重要的設定需要處理，分成 2 個部分，分別如下：

一、 更改 LAN IPV4 位址及管理者密碼

二、 決定運作架構是 POP3 代收還是透通模式

郵件歸檔伺服器 LAN 預設 IPV4 位址跟實際的網路環境不一定一樣，所以管理者就要將它改成符合當地環境的 IPV4 位址，方便日後管理，使用者登入使用者介面也是利用這個 IP 位址，同時因為安全因素，建議管理者把預設的密碼改掉。

2-1、更改 LAN IPV4 位址及管理者密碼

(一)、更改 LAN IPV4 位址

進入【系統管理】的【網路設定】中，這個地方就是設定 LAN 接口的地方。(圖 2-1)

圖 2-1、更改 LAN IPV4 位址

郵件歸檔伺服器支援 IPV4/IPV6 位址模式，目前內部網路環境大都以 IPV4 為主，所以先設定 IPV4 的位址、子網路遮罩及閘道器位址，設定的範例：

IPV4 的位址：192.168.168.167

IPV4 子網路遮罩：255.255.255.0

IPV4 閘道器位址：192.168.168.254

DNS 伺服器：192.168.188.5

POP3 代收郵件、使用者認證、垃圾郵件特徵值更新、病毒碼更新及軟體自動下載更新等功能都需要跟外面的網路連線，如果上述的功能都不需要，則 IPV4 閘道器就可以不設定。萬一郵件歸檔伺服器對外的網路不通，可能會導致上述的功能失效。

設定 IPV4 位址就可以讓郵件歸檔伺服器正常運作，所以 IPV6 不一定要設定，更改 IPV4 位址後，管理者就需要用新的 IPV4 位址再次的登入管理介面。

(二)、更改管理者密碼

系統預設的管理者帳號是 admin，預設密碼是 adminpw，因為安全的因素，建議在設備連上網際網路後，立刻把管理者的密碼改掉，修改密碼是在【認證與權限管理】中【使用者管理】列表中，找到 admin 的帳號，點選修改圖示後重新輸入密碼跟確認密碼這 2 個欄位。(圖 2-2)

圖 2-2、更改管理者密碼

系統預設的管理者帳號是 admin 是屬於本機帳號，在建立其他具有管理者權限的帳號後，可以將它刪除或限縮管理權限，系統會自動檢查具有管理者權限的帳號，最後一個具有管理者權限的帳號將具有防呆裝置，不會被刪除。

2-2、運作架構說明

郵件歸檔伺服器有 2 種模式紀錄郵件，一種是 POP3 代收，另一種是閘道器模式，同一台設備可以讓 2 種模式同時運作，詳細說明如下：

(一)、POP3 代收

郵件主機適用在雲端代管、承租郵件主機空間或是原本郵件主機沒有郵件紀錄器功能，希望利用郵件歸檔伺服器的郵件歸檔功能將所有的郵件備份，這個模式適用 GMAIL、Office365 或是自己架設的 Exchange Server 上。

POP3 代收的運作原理是在郵件伺服器上建立一個帳號，例如，archive.yourdomain.com，並在郵件伺服器上設定一個規則，將所有進出的郵件都複製一份給 archive.yourdomain.com，郵件歸檔伺服器再依照設定的時間內用 POP3/POP3S 的方式將郵件收到系統中，收到的郵件就會依照網域名稱跟郵件帳號分類，方便管理者、查詢者或是使用者查詢使用。(圖 2-3)

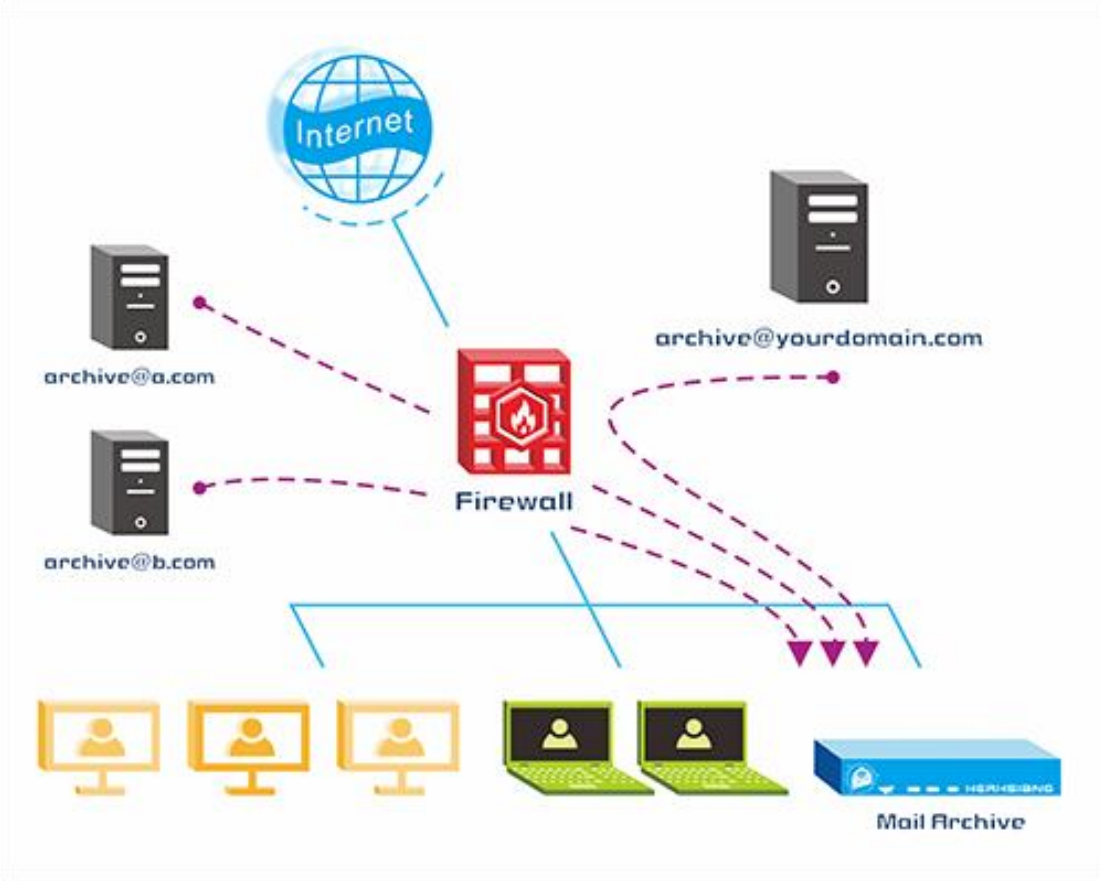


圖 2-3、POP3 代收示意圖

在代收郵件後，為了避免原本郵件伺服器上代收帳號空間爆掉，管理者需要選擇代收後就刪除郵件還是保留數天後刪除郵件，郵件歸檔伺服器支援多網域，因此管理者可以建立多筆代收帳號分別指向不同的郵件主機，系統會根據網域名稱自動分類，考慮到效能因素，當設定的代收會依照數量分批執行。

在【架構管理】的【POP3 代收】中，填入代收帳號及網域名稱就可以，比較需要注意的是代收的通訊協定，一般來說 POP3 是用 TCP 110 用非加密的協定傳輸郵件，在安全上有很大的顧慮，所以雲端主機業者通常會再提供 POP3S 加密的協定，在【功能狀態】啟用擷取郵件使用安全連線(SSL)就是 POP3S，點選後埠號就會自動更新為 TCP 995。(圖 2-4)

圖 2-4、POP3 代收設定

(二)、閘道器模式

郵件歸檔伺服器在閘道器模式下，可以指定對外跟對內的網卡，MArchive H57TA & H91XT（需追加擴充雙埠 10G 光纖網路卡定義 Port 3 & 4），還可以配置 2 組對內及對外的橋接模式，系統會自動給予 br0 跟 br1 這 2 個橋接器的名稱，記錄同網段的郵件。

一種配置模式是設定一個為對外接口，另外 3 個為對內接口，在這個配置下

，這 3 個接口就像是一個 Switch。

在透通模式下，郵件歸檔伺服器會把所有進出設備的 SMTP 跟 SMTPS 的連線通通攔截下來，經過內部代理程序後再把這些通訊協定送到目的端。

對於自己架設郵件伺服器的環境來說，郵件歸檔伺服器擺放的位置有 2 個地方，如下圖中 A、B 2 個圖示：：（圖 2-5）

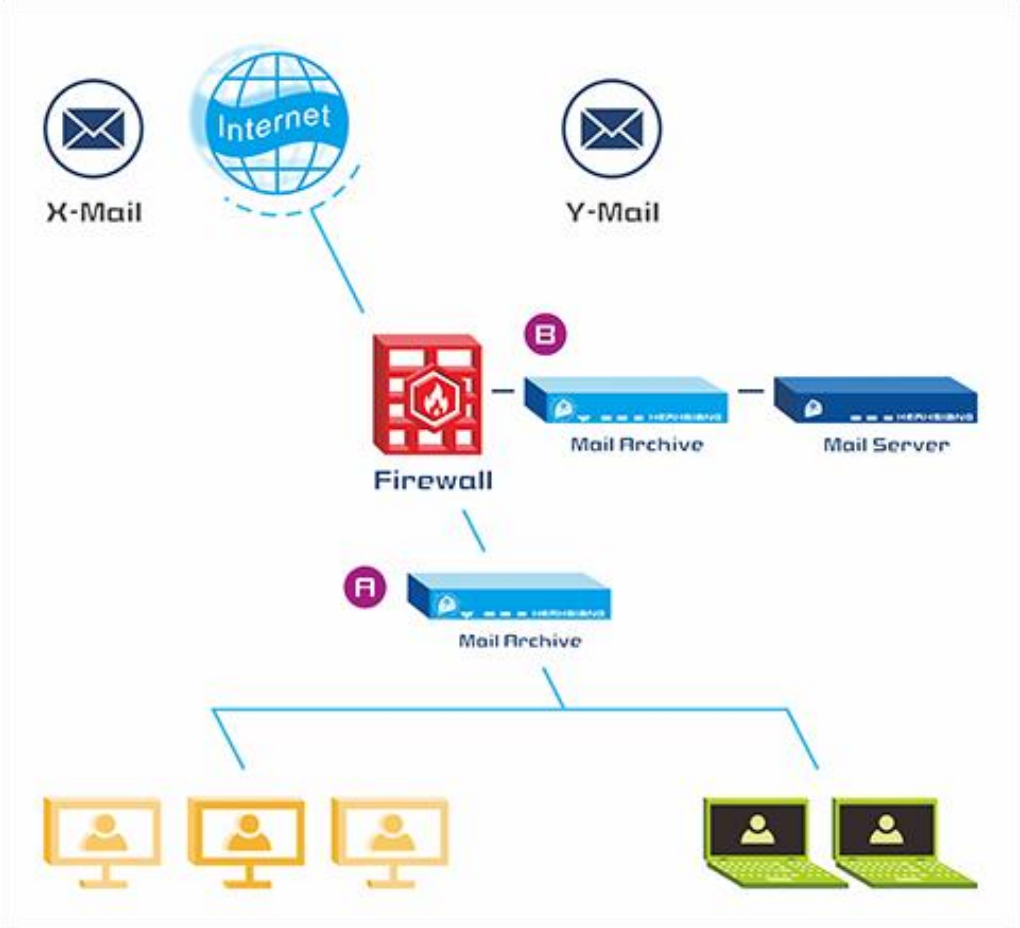


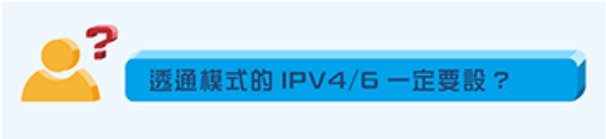
圖 2-5、透通模式設備配置示意圖 FOR MArchive H57TA & H91XT（需追加擴充 10G 網路卡）

位置 A ：除了記錄自己的郵件伺服器的通聯記錄之外，如果內部使用者有用外部的郵件伺服器 X-Mail Server / Y-Mail Server ，他的郵件也會被記錄下來。這個位置也適用於將郵件伺服器託管在 ISP 機房或是跟 ISP 業者承租郵件空間等環境。

位置 B ：單純記錄自己的郵件伺服器的通聯記錄。

在【架構管理】的【透通模式】中新增一筆資料，在埠號綁定的示意圖上，除了 LAN 跟 HA 是不可以更改點選外，指定哪個 Port 網卡是對內還是對外，點選圖示就可以切換。(圖 2-6)

圖 2-6、透通模式的 Port 及 IPV4 位址設定



在透通模式下的郵件歸檔伺服器需要寄出各式通知信及後端的郵件伺服器故障時能夠代收郵件，這 2 項功能都靠閘道器的 IPV4/IPV6 才能達到，為了系統運作順利，建議設定 IPV4 位址，否則會造成郵件寄送上的問題，這位址不一定要跟 LAN 的 IP 位址同一個網段。

第 3 章 系統管理

屬於整台郵件歸檔伺服器系統的設定，都是在系統管理中處理，具備有【管理者】權限的管理人員才可以進入這一個選單中進行設定。

在本單元中分成為網路設定、時間設定、系統設定、SMTP 伺服器設定、備份管理及系統更新等子功能，每一項的子功能都會在這個章節中詳細介紹，這一些設定牽涉到整台設備運作正常與否的關鍵，管理人員應該特別注意。

3-1、網路設定

郵件歸檔伺服器本身支援 IPV4 及 IPV6 2 種定址模式，管理者只需要設定其中一種，就可以讓設備正常運作，在這裡【網路設定】設定的接口就是 LAN，LAN 接口的 IP 位址是讓管理者、查詢者或是使用者進入設備，管理者也可以在自己的 DNS 伺服器上設定一筆 A/AAAA 紀錄，操作人員就不需要記住 IP 位址。

系統也會利用 LAN 接口進行垃圾信特徵值更新、病毒碼更新、軟體自動下載更新及 POP3 代收等動作。

★ A/AAAA 記錄小技巧

郵件歸檔伺服器設定的 IPV4 位址為 192.168.168.167 或是 IPV6 位址為 2001:b030:8102:1::1000，為了方便操作人員進入設備，管理者在自己的 DNS 伺服器上設定一筆 IPV4 的 A 紀錄或是 IPV6 的 AAAA 紀錄，範例如下：

ma.yourdomain.com　　192.168.168.167

ma.yourdomain.com　　2001:b030:c201:ff00:0192:0168:0168:0167

操作人員要進入郵件歸檔伺服器時，只要用 ma.yourdomain.com 這個網域，透過 DNS 伺服器的名稱解析後，就可以進入設備中。

網路設定

網路設定的設定頁面如下：(圖 3-1)

圖 3-1、網路介面設定

- 【IPV4 的位址】：設定 IPV4 的 IP 位址，例如，192.168.168.167。
- 【IPV4 子網路遮罩】：設定 IPV4 的子網路遮罩，例如，255.255.255.0。
- 【IPV4 閘道器位址】：設定 IPV4 的閘道器位址，設上正確的閘道器位址讓郵件歸檔伺服器能夠正常地從網際網路上更新病毒碼特徵值、垃圾郵件特徵值或是設備的更新檔，例如，192.168.168.254。

  前端如果有防火牆保護設備，也要注意要能夠讓郵件歸檔伺服器能夠正常地到網際網路上。

- 【IPV6 的位址】：設定 IPV6 的 IP 位址，如果不知道該如何設定 IPV6 的 IP 位址，可以先設定【IPV6 閘道器位址】，再按旁邊的『MAC 轉 IP』按鈕，系統會用機器的 MAC 位

址，自動轉換成 IPV6 的位址，例如，2001:b030:c201:ff00:0192:0168:0168:999，後面的 2250:efee:6666:2751 就是機器的 MAC 位址。

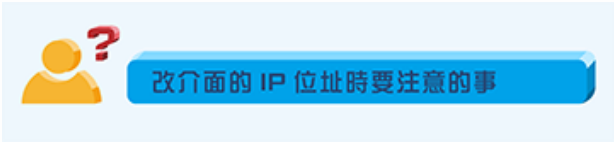
- 【IPV6 子網路遮罩】：設定 IPV6 的子網路遮罩，範圍可以是 0 ~ 128，一般預設是 64，例如，64。

  【IPV6 閘道器位址】：設定 IPV6 的閘道器位址，設上正確的閘道器位址讓郵件歸檔伺服器能夠正常地從網際網路上更新病毒碼特徵值、垃圾郵件特徵值或是設備的更新檔，例如，2001:b030:c201:ff00::0254。

在 IPV6 的定址模式下，每一個子網路所包含的 IP 位址範圍都相當大，大到管理者不知道如何設，在這個狀況下，可以用這一個簡單的『MAC 轉 IP』按鈕，讓系統利用機器的 MAC 位址，自動轉換成一個 IPV6 的位址，並把這一個位址自動填入【IPV6 的位址】的位置上。

- 【DNS 伺服器】：設一筆以上的 DNS 伺服器 IP 位址給郵件歸檔伺服器查詢網域使用，每一行為一筆 DNS 伺服器的 IP 位址，例如，168.95.1.1　8.8.8.8。

當設定完成後按下『確定』按鈕，新的 IP 位址就會生效，此時要再進入管理介面，則需要使用新的 IP 位址才能進入管理介面。



1、新的 IP 位址沒有別的設備占用，否則會產生 IP 位址衝突，無法進入管理介面。

2、記住自己設定的新 IP 位址，否則無法進入管理介面。

3、不要忘了將設定電腦的 IP 位址改回正常可以上網的 IP 位址。

閘道器的位址跟 DNS 伺服器是否正確，如果讓設備無法連上網際網路，則病毒碼更新、垃圾郵件特徵值更新等都會失效。

3-2、時間設定

郵件歸檔伺服器紀錄所有郵件伺服器進出的郵件，所以何時紀錄下來這個時間就非常重要，通常郵件本身也會標註收發信的時間，但是哪個時間是可以更改，拿來當作時間排序依據時，顯示的資訊就不準確，所以預設在顯示時間排序是以系統收到郵件的時間為主，系統的查詢郵件介面就可以讓查詢者自行選擇是以郵件本身的時間還是以收到郵件的時間為準。系統本身可以跟網際網路的時間伺服器校正準確的時間。（圖 3-2）

圖 3-2、時間設定

- 【伺服器時間】：顯示目前系統的時間，如果想要手動更改時間，只要點選顯示的時間或是後面的圖示就可以更改，例如，2023-06-04　18:34:52。
- 【伺服器時區】：郵件歸檔伺服器所在的時區，例如，Asia/Taipei。
- 【目前使用的時間伺服器】：顯示系統目前使用那一個時間伺服器，例如，time.stdtime.gov.tw。
- 【最後的校正資訊】：顯示郵件歸檔伺服器跟時間伺服器最後更新的紀錄，由紀錄可以看出時間差多少或是校正不成功，例如，4 Jun 18:20:36 ntpdate[16763]: adjust time server 118.163.81.61 offset -0.009085 sec，代表校正成功且有 0.009085 秒的差距。

- 【時間伺服器】：選擇一個符合當地時區的時間伺服器或是自行輸入一個時間伺服器的 Domain/IP 位址，例如，選擇 Taipei 的時間伺服器。
- 【校正時間伺服器間隔】：系統每隔多長時間跟時間伺服器校正時間，預設是 1h，也就是 1 個小時，管理者可以自行更改時間間隔，例如，1h。

設定完成後按下『確定』按鈕，新的時間就會開始運作，此時紀錄下來的郵件，就會以新的時間為紀錄標的。

3-3、系統設定

管理者對於整台郵件歸檔伺服器關機、重新開機甚至定時重新開關機等命令，都可以在這裡設定，也可以設定管理者、查詢者或是使用者要進入這一台系統的主機網域名稱及瀏覽器上顯示的標題等資訊。（圖 3-3）

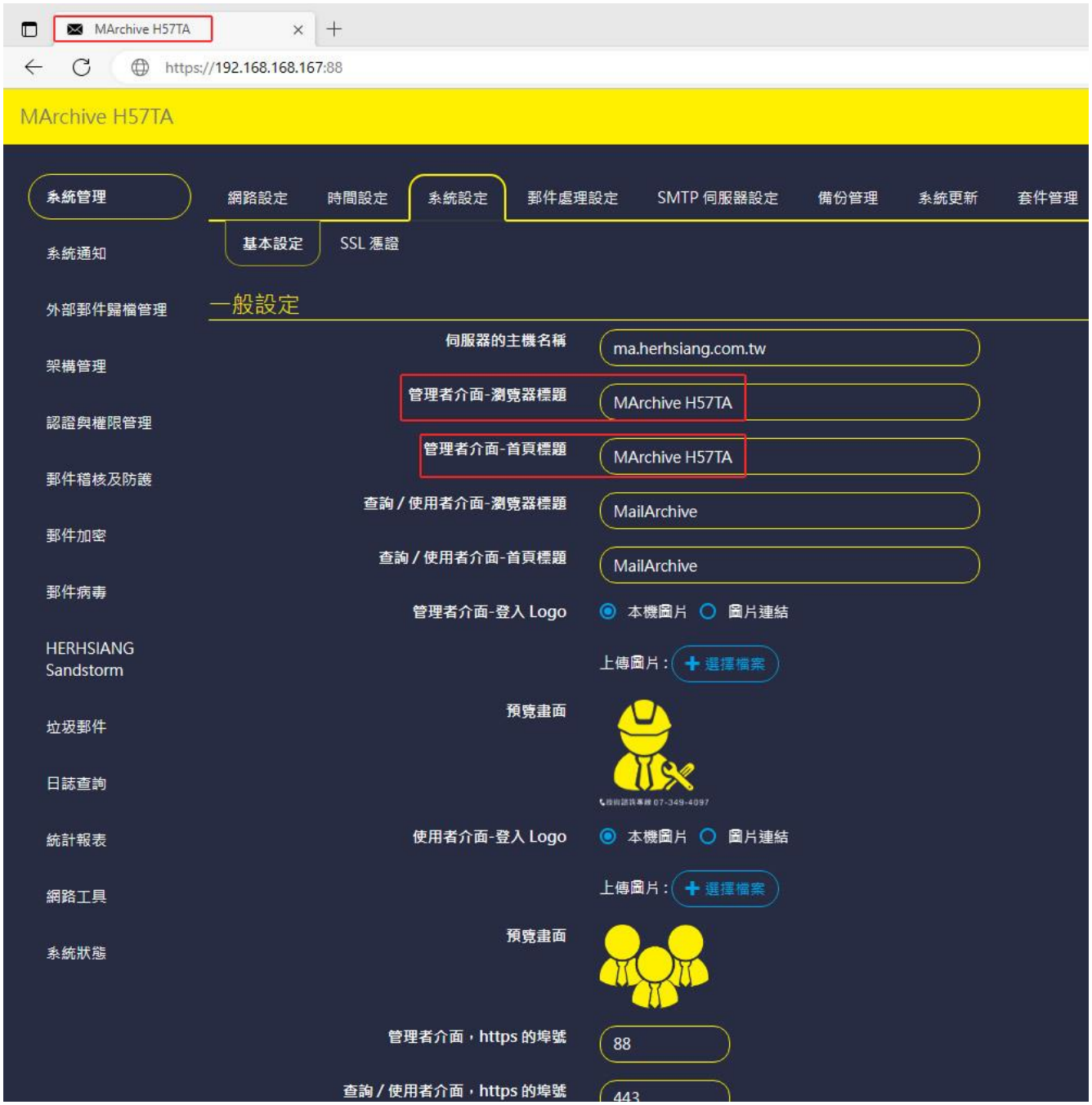


圖 3-3、系統設定

(一)、基本設定

- 【伺服器主機名稱】：設定郵件歸檔伺服器的主機名稱，方便管理者或是使用者進入系統使用，在 DNS 伺服器上必須要有相對應的 A 或是 AAAA 紀錄，例如，ma.yourdomain.com，如果都是用 IP 位址登入，則這個地方可以不用設定。

管理者可以根據公司規定，設定瀏覽器要顯示的標題跟登入郵件歸檔伺服器後在首頁要顯示的文字，系統提供 2 種管理介面分別是管理者使用的管理介面跟查詢者或使用者操作的使用者介面，所以這個地方需要分別設定。

- 【管理介面 - 瀏覽器標題】: 顯示在管理介面的瀏覽器上的分頁標題，方便操作者辨識，例如，MArchive H57TA。
- 【管理介面 -首頁標題】：在管理介面左上角顯示的文字，可以是任何文字組合，例如，This is a Brand Name。
- 【查詢 / 使用介面 - 瀏覽器標題】: 在查詢者跟使用者登入的使用介面的瀏覽器上的分頁標題，方便操作者辨識，例如，User Page。
- 【查詢 / 使用介面 -首頁標題】：在查詢者跟使用者登入的使用介面左上角顯示的文字，可以是任何文字組合，例如，MailAchive。
- 【管理者介面 –https 的埠號】：進入管理介面的埠號，預設使 88。
- 【查詢 / 使用介面 –https 的埠號】：進入使用者介面面的埠號，預設使 443。
- 【管理者介面 –閒置自動登出】：當管理者沒操作管理介面，系統會自動登出。

(二)、本機硬碟空間不足通知電源設定

- 【硬碟空間不足時訊息通知】：要不要啟用這項功能，啟用後當硬碟空間不夠時，會主動發電子郵件給管理者。
- 【本機硬碟剩餘空間低於】：當硬碟可用空間少於多少比例，就會觸動這一個寄送通知，預設使 20%。
- 【通知信的主旨】：寄發通知信的主旨。

(三)、網域和使用者被移至資源回收筒後的處理

- 【移至資源回收筒後多久刪除設定】：啟用後，當郵件移到資源回收筒後，經過設定的天數，系統會自動將資源回收筒內的過期郵件清除。
- 【被移至資源回收筒時寄發通知】：當郵件移到資源回收筒後，要不要發通知信給管理者。
- 【被刪除前幾天寄發通知】：前面【移至資源回收筒後多久刪除設定】有啟用，才可以啟用，啟用後，系統刪除資源回收筒的郵件時會寄發通知信給管理者。
- 【資源回收筒中的使用者是否停止統計資料】：系統不會統計資源回收筒中的郵件資訊。

(四)、電源設定

管理者可以對整台設備進行關機、重新開機或是定期性的重新開機等動作，如果要回復成出廠預設值也可以在這裡設定。

- 【系統重新開機/關機設定】: 針對這台設備可以進行下列三個動作：

  重新開機：按下 

，系統會關閉所有運作中的程序，進入重新開機程序。

  關機：按下 

就會進入標準的關機程序，將設備關機。

  恢復出廠設定：按下 

，系統就會將已經設定的資料清除，重新開機後會載入出廠預設值。

- 【自動定時重新開機/關機設定】：要不要啟用定時自動重新開關機的設定，共有三種模式可以選擇，分別是停用、重新開機跟關機，預設是停用這項功能。

- 【排程】：當前面的【自動定時重新開機/關機設定】選擇重新開機或是關機時，系統會啟用這一個選項，管理者可設定每日、每周或是每月的特定時間，例如，半夜 12:00，執行重新開機或是關機動作。

★ 小叮嚀

在透通模式下，對內跟對外的接口設定在使用不具備 ByPass 機制的網路卡，因無法有效得知網路卡失去效用，造成非人為損失, 相關管理者可迅速得知後可將網路線跳過 MArchive 設備，讓郵件伺服器繼續有效收發信件，跳過前 MArchive 設備所收信件待設備網路埠恢復後會將暫存信件往郵件伺服器傳送，可避免信件漏接情況發生，造成損失。

3-4、郵件處理設定

關於郵件歸檔伺服器上被過濾被隔離的郵件該如何通知管理者或是收信者，同時也包含使用這如何取回垃圾郵件清單、對內文做摘要、郵件加密跟 RTF 格式的郵件該如何處理等，都可以在這個章節中設定，其中對內文做摘要的動作是方便管理者快速的辨識搜尋的郵件是不是標的物。

對於紀錄在郵件歸檔伺服器硬碟上的郵件，萬一機器的硬碟被竊取，傳統架構下，偷取者只要用另一台主機器將硬碟掛載起來，裡面的資料(郵件)就有外洩的疑慮，為了避免這樣的情況發生，系統再將郵件存入硬碟前，會用 PGP 的加密程式將資料加密，就連掛載在 NAS 中的 SQL 資料也是加密，在這個狀況下，就算硬碟遺失，資料也不用擔心外洩。

(一)、郵件處理設定

系統有很多行為需要主動發出通知郵件，通知管理者或是使用者，例如，垃圾信的隔離、系統運作狀況等，都會發出通知信，這個地方就是設定通知郵件的規則，例如，通知信使用的語言或是取回隔離信件的網址跟 Port。（圖 3-4）

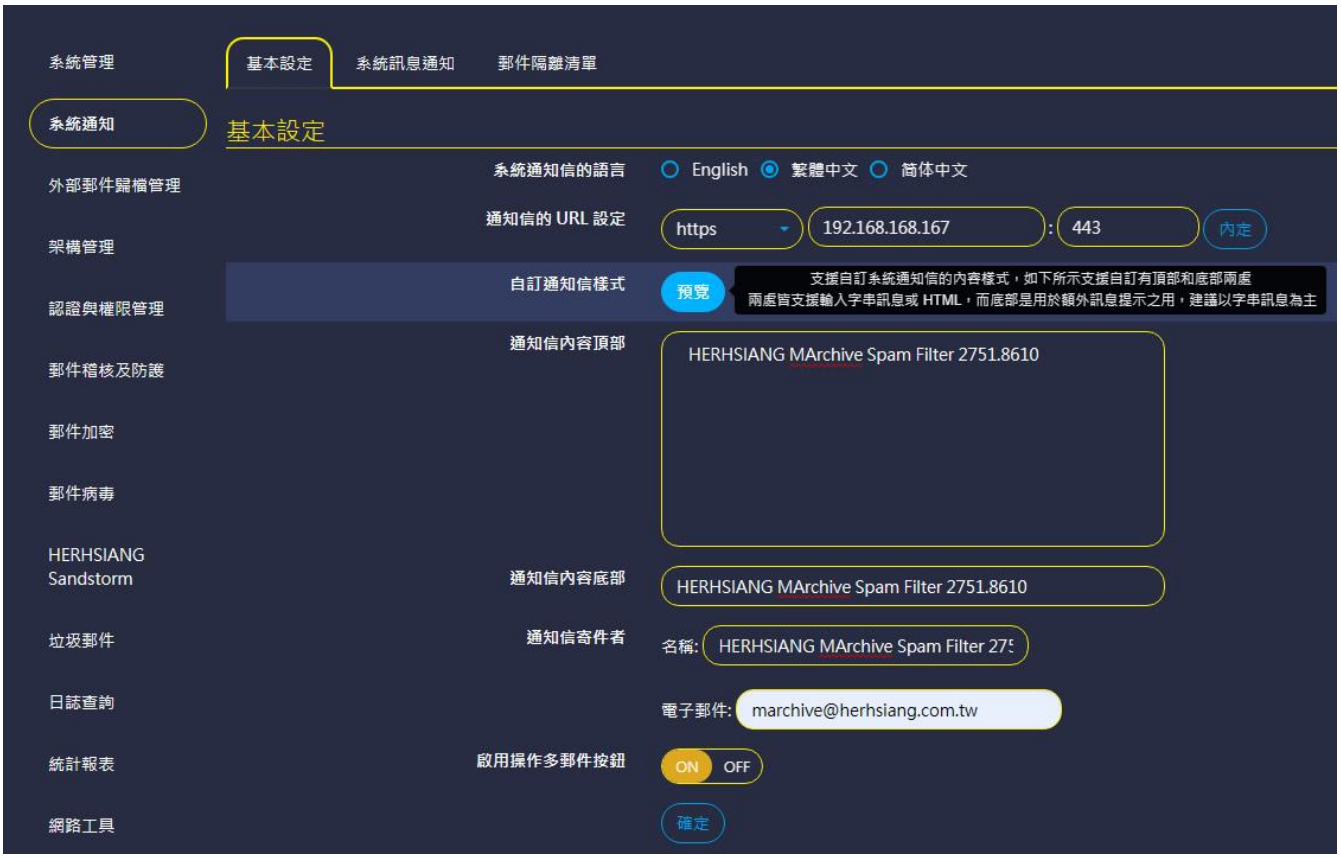


圖 3-4、郵件處理設定

- 【系統通知信的語言】: 郵件歸檔伺服器寄出的通知信是以哪一個語系為主，管理者可以自行決定。

- 【通知信的 URL 設定】: 啟用郵件歸檔伺服器上的垃圾信過濾機制，且對垃圾信的處置方式採用垃圾郵件隔離時(參照 8-1 節)，管理者需要設定這裡的 URL，這樣使用者才能取回被誤判的垃圾郵件。URL 的設定分成下列 3 段。

  第一段是通訊協定，有 2 種協定可以選擇，一個是 http，另一個是 https，預設是使用 https。

  第二段是主機名稱，一般來說會設成這一台設備的主機名稱(參照 3-3 節的伺服器主機名稱)，這個名稱必須在 DNS 伺服器上有相對應的 A 或是 AAAA 紀錄，並且是指向這台系統的 IPV4/IPV6 位址。例如，mailarchive.yourdomain.com。

  第三段是 Port，一般來說，http 是 80 port，https 是 443 port，管理者依照自己的網路架構設定，如果想讓外部的使用者也能順利的取回郵件，在防火牆內也要有相對的導入動

作。預設系統會把 https 的 Port 改為 88 ，因為在 NAT 一對多的環境下，443 Port 是相當珍貴，所以保留給其他更重要的服務使用。

【自訂通知信樣式】: 郵件歸檔伺服器偵測到任何問題下都會寄出的通知信，通知信的格式可以在這裡配置，點選預覽就會出現設計的範本，每一個通知信的內文基本上分成三大塊，頂部、主文及底部，如下所示：(圖 3-5)

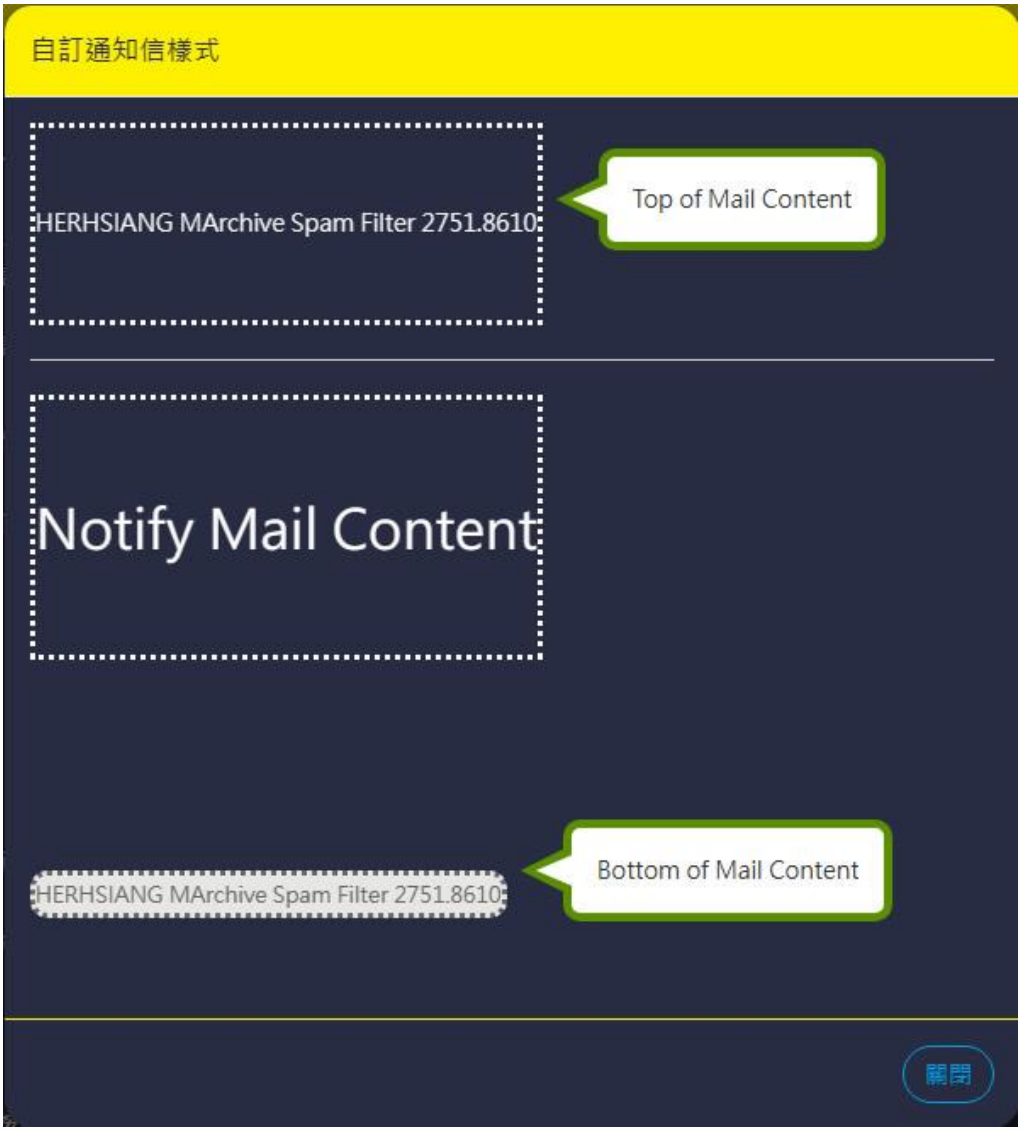


圖 3-5、通知信的預覽及設計

- 【通知信內容頂部】: 哪一些文字要顯示在通知信內文的上方。
- 【通知信內容底部】: 哪一些文字要顯示在通知信內文的下方。
- 【通知信寄件者】: 郵件歸檔伺服器寄出的通知信是用那一個帳號寄出，並且寄件者顯示的名稱。

(二)、郵件摘要擷取設定

設定郵件摘要的目的是方便管理者找尋郵件時，能快速地確認該郵件是不是要搜尋的目標，而不只靠收件者、寄件者、時間或是主旨等有限的資訊。

- 【郵件摘要擷取】: 要不要起用這項功能，啟用後管理者在【日誌查詢】>【郵件日誌】的郵件列表中【詳細】區，就可以看到節錄下來的摘要內容。
- 【擷取字串長度】: 啟用後，每封郵件內文摘要擷取的長度，預設是 125bytes。
- 【不擷取摘要的寄件者】: 哪一些寄件者他的郵件不要被擷取摘要，在這裡設定例外名單，點選空格後從選單中選取或是自行輸入，每一行為一個郵件帳號。

(三)、RTF 格式轉換設定

有一些寄信軟體，寄信時會使用 RTF 格式寄出郵件，導致收信者收到一封附件為 winmail.dat 的郵件，但卻無法查看郵件內容，當啟用這項功能後，郵件歸檔伺服器收到 RTF 格式的郵件，會自動將他轉為正常格式的郵件給收件者，同時也可以讓收信者用 URL 取回的方式取回原本的郵件。（圖 3-6）

圖 3-6、RTF 轉換設定

- 【RTF 格式轉換】：要不要啟用這項功能 ？ 預設值是【關閉】。
- 【轉換的目標】：在閘道器模式下，郵件的來源有 2 個方向，內送的郵件跟外寄的郵件，所以轉換工作是針對哪一個來源的郵件進行轉換，也可以 2 個都選。

  內送的郵件：收到外部的寄件者用 RTF 格式寄給內部的使用者，預先將他轉換成正常的郵件格式，再傳給收件者(也就是內部郵件伺服器上的使用者)。

  外寄的郵件：內部的寄件者用 RTF 格式寄出，為了避免對方收件者困擾，預先將他轉換成正常的郵件格式後再寄出。
- 【提供超連結以下載原始郵件】：是不是要提供收信者下載原始的郵件，會提供這樣的方式是為了避免轉換過程有問題或是收信者就想看到原始郵件，啟用這項功能後，收件者會在轉換完的郵件內容最後面，插入一個 URL 超連結，按下超連結後就可以將原始郵件收下，預設是關閉。
- 【超連結下載說明文字】：設定這個 URL 超連結的描述文字，可以是任何中英文，這些文字就會插入被轉換過的內文中，例如，Please download the attachment(s) from the following link(s) 。
- 【郵件在伺服器保存天數】：RTF 轉換後原始郵件在郵件歸檔伺服器中保存的天數，超過這個天數，系統就會將他刪除，預設是 7 天。
- 【未被下載的逾期郵件】：轉換前的原始郵件超過保留天數後該如何處理，有 2 個選項：

  刪除：直接將原始郵件刪掉。

  再保留：再保留的天數，超過仍然會將他刪除，預設是 7 天。
- 【例外的寄件者】：哪一些寄件者不想用這 RTF 轉換服務，點選空格後從選單中選取或是自行輸入，每一行為一個郵件帳號。
- 【例外的收件者】：哪一些收件者不想用這 RTF 轉換服務，點選空格後從選單中選取或是自行輸入，每一行為一個郵件帳號。

(四)、日誌、統計資料生命週期

郵件歸檔伺服器保存的日誌及統計資料要保留多久？每個項目最長可以保留 120 個月 / 10 年。 (圖 3-7)

圖 3-7、日誌保留時間設定

3-5、SMTP 伺服器設定

郵件歸檔伺服器要寄出通知信時，因為本身並不是郵件伺服器，也沒有郵件帳號，因此需要一個具有 SMTP 寄信功能的帳號，透過郵件伺服器，寄出這些通知信，例如，垃圾郵件清單、系統狀態等通知信。

系統具備多網域的郵件紀錄功能，所以通知信的寄件者，也可以依據網域自動分配，例如，屬於 a.com 網域的通知信就會利用帳號 1@a.com 寄出的通知信，屬於 b.com 網域的通知信就會利用 2@b.com 的帳號寄出，這樣就不會混淆，如果只設定一筆，則所有的通知信都會用那一筆 SMTP 帳號寄出。

系統會列出所有設定的 SMTP 帳號，管理者可進行新增、修改、刪除甚至排序等動作，也可以把設定的資料匯出成 txt 或是 csv 格式方便保留或是轉移。（圖 3-8）

圖 3-8、SMTP 寄信設定列表

當郵件歸檔伺服器寄出通知信失敗，自動記錄下來，管理者可以在【寄送失敗日誌】中查詢。

新增一筆 SMTP 伺服器帳號

點擊  圖示後，就可以進入新增帳號的設定畫面。（圖 3-9）

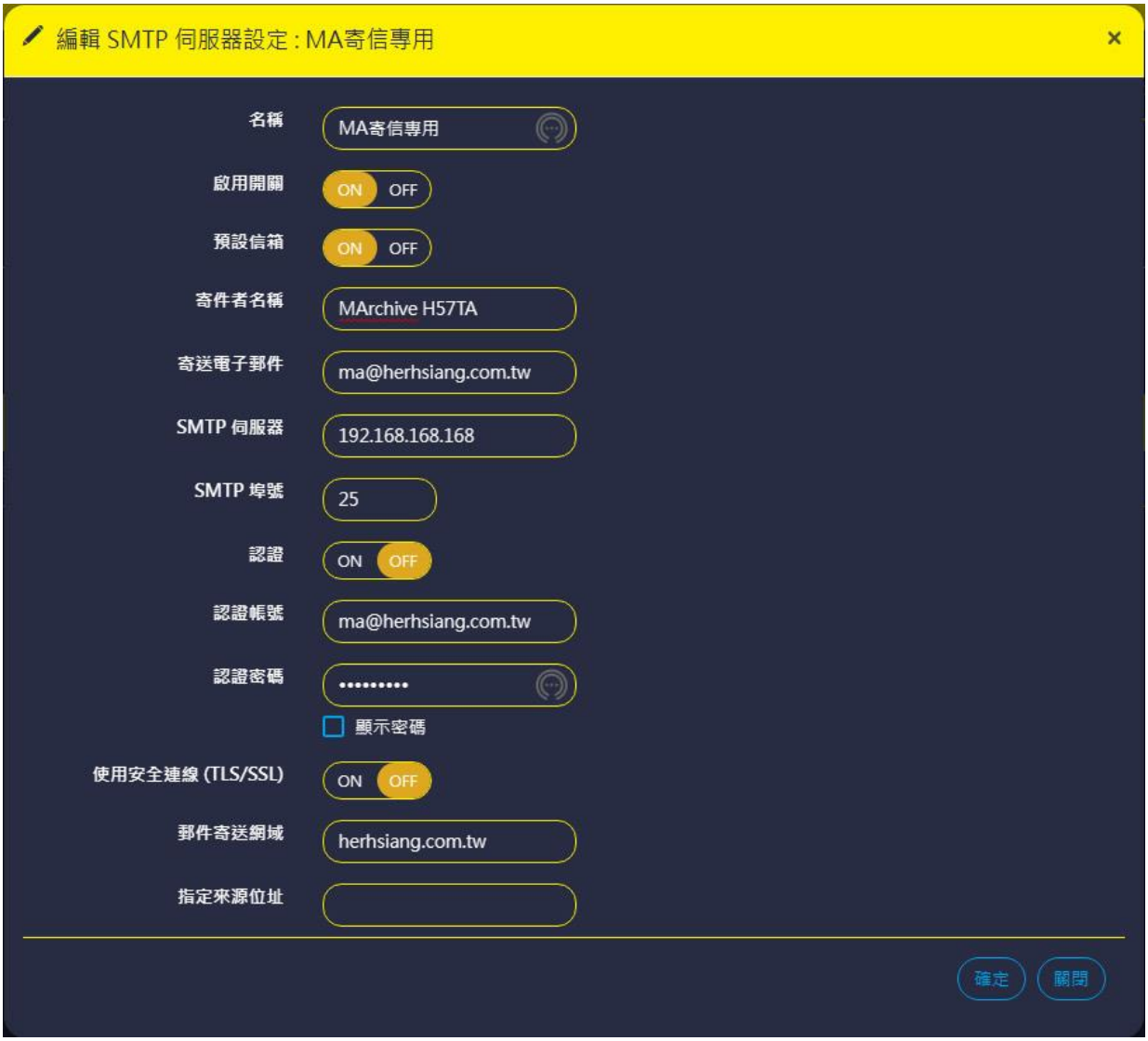


圖 3-9、SMTP 寄信設定

- 【名稱】：這個寄件帳號的名稱，方便管理者辨識，例如，Test。
- 【啟用開關】：設定的寄件帳號要不要啟用。
- 【寄件者名稱】：設定的寄件帳號的名稱，方便管理者或是使用者收到通知信時如易辨識，例如，Marchive H57TA。
- 【寄件者帳號】：設定每一封通知信上顯示的寄件帳號，這個帳號通常會跟實際的認證帳號一致，例如，ma@herhsiag.com.tw。
- 【SMTP 伺服器】：寄件帳號使用的 SMTP 伺服器，可以是 IP 位址或是網域名稱，例如，mail.herhsiang.com.tw。

- 【認證】：設定的 SMTP 伺服器在寄信時，需不需要認證，通常郵件伺服器為了避免被當成寄信跳板，會要求寄件者認證。
- 【認證帳號】：當 SMTP 伺服器要求認證時，郵件歸檔伺服器使用的登入帳號，通常會跟寄件者帳號一致，例如，ma@herhsiag.com.tw。
- 【認證密碼】：當 SMTP 伺服器要求認證時，寄件帳號的的密碼，有個顯示密碼的選項，避免設錯密碼導致通知信無法寄出。
- 【TLS】：要不要用 TLS 加密跟 SMTP 伺服器溝通，預設是關閉。
- 【郵件寄送網域】：指定這個帳號要寄送的網域名稱，例如，herhsiang.com.tw。

  通知信的收件者符合這個網域，則會用這個帳號寄出各類通知信或是垃圾郵件清單，如果系統只有一筆 SMTP 伺服器設定，則所有的通知信都會用這一筆(也就是第一筆)帳號寄出。

  同一個寄件者帳號也可以設定多個郵件寄送網域。
- 【指定來源 IP 位址】：郵件歸檔伺服器用哪個 IP 位址當作來源 IP 位址跟要寄通知信的郵件伺服器通訊，如果這個地方是空白，則在閘道器模式下，會用 br0/br1 設定的 IP 位址，在 POP3 代收模式下使用 LAN 的 IP 位址當作來源 IP 位址，除非管理者要訂特殊 IP 位址或是寄通知信的郵件伺服器有特定的 IP 位址才能寄信，才須要設定上 IP 位址。

設定完成的 SMTP 伺服器資料就會顯示在（圖 3-8）中，管理者可以點選列表中的 圖示，調整先後順序，當寄件網域沒有符合時就會用第一個的帳號寄出通知信。

設定完成後，可以點選列表中【郵件寄送測試】的  圖示，系統會自動寄出一封測試通知信，如果有收到這一筆資料，代表設定的資料是正確。

3-6、備份管理

Marchive H57TA & H91TA 郵件歸檔伺服器本機 Onboard 內建第 2 顆同步備份資料碟 （出廠前已完成定時同步設定動作），主資料碟故障如故障將主資料碟抽出後重新開機鍵盤螢幕選擇備用碟編碼 sdb?就可直接當主資了碟使用,，可利用備份機制，將本機的主資料碟設定定時同步到備用資料碟或是設定檔備份到網路硬碟(Samba)、FTP 伺服器或是 USB 的隨身碟上，萬一設備上的硬碟故障導致運作中斷，在更換新的硬碟後，新硬碟直接當備用資料碟定時同步，以備不時之需馬上切換使用，另可快速的從備份的裝置上還原，讓中斷的設備快速的回復工作。

備份時包含本機所有紀錄的郵件內容及郵件歸檔伺服器的設定資料都會一起打包，並在指定的備份時間將這些資料複製到備份設備上。回復的方式也是一樣，將備份的資料掛載之後，利用還原機制，回復備份時的所有資料內容，每次備份動作，系統會寄給管理者備份結果。

備份的郵件是指存在本機的硬碟的 SQL 資料庫中，如果掛載 NAS 的 SQL 資料庫，NAS 的部分將不會備份。

郵件歸檔伺服器的備份機制在第一次完整備份後是採取差異備份，例如，同一個備份裝置，在 12:00 備份完成後，13:00 備份時只會備份 12:00~13:00 中間多增加的資料。

基本觀念

備份的基本步驟如下：

設定備份裝置 ➔ 備份設定

備份裝置目前本機備份資料碟、支援網路硬碟(Samba)、FTP 伺服器跟 USB 隨身碟 4 種，管理者可以根據自己的需求掛載不同的備份裝置。

備份時根據設定的時間備份郵件歸檔伺服器當下所有的資料，包含紀錄在本機的郵件及設定檔，並把資料複製到備份裝置上，系統最多可以備份到 24 個不同裝置，也就是每小時一個備份動作，同時指向不同的備份裝置，如果同一個小時內有 2 個備份裝置，則只有其中一個有備份資料。

如果設定備份到 24 個不同的裝置，則可以把故障時還原的內容差異時間從一天縮小到一個小時，但此時也需要額外付出更多的系統資源及儲存裝置。

(一)、裝置設定

點選  的圖示，就進入備份裝置的設定畫面。（圖 3-10）

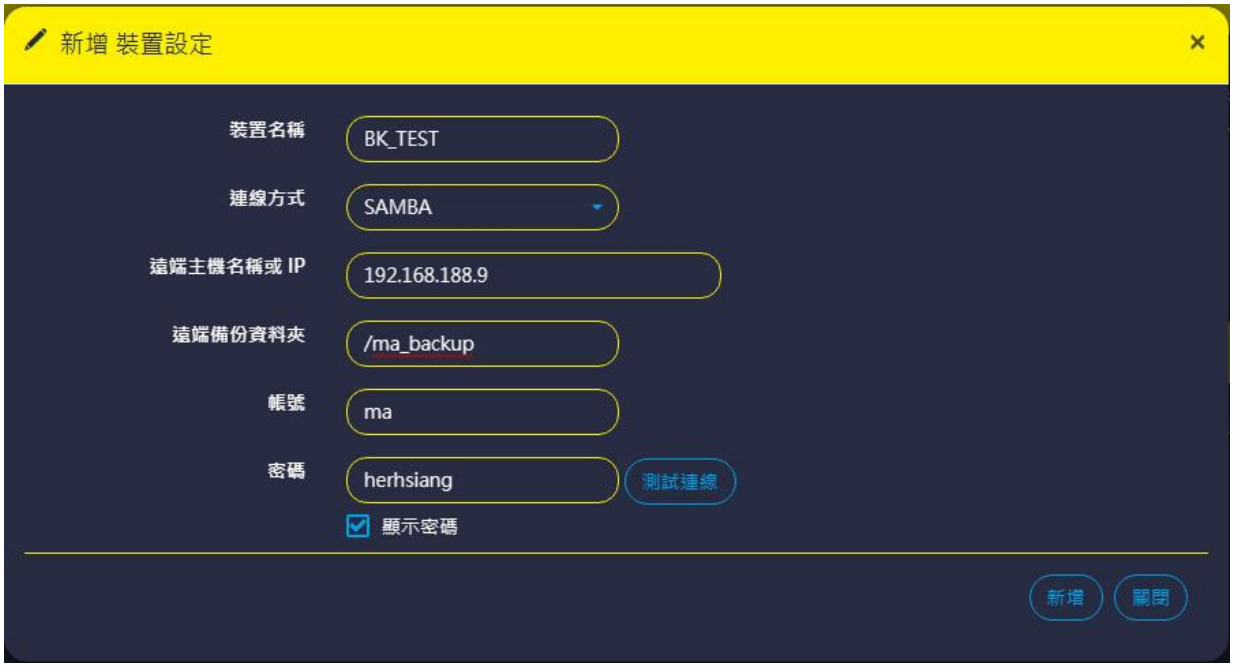


圖 3-10、新增一個網路芳鄰備份裝置

- 【**裝置**名稱】：給這個備份裝置一個容易辨識的名稱，例如，BK_TEST。
- 【**連線方式**】：選擇網路硬碟(Samba)、FTP 伺服器跟 USB 隨身碟 3 種其中之一，選擇之後的設定資料也會不一樣，不同的設定說明如下。

(A)、SAMBA 設定

SAMBA 就是常見的網路芳鄰協定，利用 TCP 中的 138、139 協定跟網路上任何一台分享儲存空間的伺服器溝通。

- 【遠端主機名稱或 IP】：輸入分享儲存空間的網路芳鄰主機網域名稱或是 IP 位址，例如，192.168.188.9。
- 【遠端備份資料夾】：要把資料備份到遠端備份主機上的哪一個目錄，系統會在這個目錄下再建立自己的分類目錄，例如，ma_backup。
- 【帳號】：在備份主機上具有寫入權限的帳號，例如，ma。
- 【密碼】：具有寫入權限帳號的密碼。
- 【顯示密碼】：點選後可以確認自己的輸入的密碼是否輸入正確，同時有 

這一個圖示，可以驗證輸入的資料正確與否。

(B)、FTP 設定

備份裝置也可以是 FTP 伺服器，一般的 FTP 伺服器都是利用 TCP 中的 21 協定溝通，管理者可以自訂通訊埠，跟 Samba 網路芳鄰一樣，需要指定備份資料夾跟給予具有寫入權限的帳號。

- 【遠端主機名稱或 IP】：輸入分享儲存空間的 FTP 主機網域名稱或是 IP 位址，同時需要指定 FTP 的通訊埠，預設是 21，例如，192.168.188.9。
- 【遠端備份資料夾】：要把資料備份到 FTP 主機上的哪一個目錄，系統會在這個目錄下再建立自己的分類目錄，例如，test。
- 【帳號】：在 FTP 主機上具有寫入權限的帳號，例如，ma。
- 【密碼】：具有寫入權限帳號的密碼。
- 【顯示密碼】：點選後可以確認自己的輸入的密碼是否輸入正確，同時有 

這一個圖示，可以驗證輸入的資料正確與否。

(C)、USB 設定

郵件歸檔伺服器依據型號，有 USB 2.0 或是 USB 3.0 的接口，將 USB 備份插入後，系統就會自動辨識，辨識成功，在這裡就會出現裝置的名稱，此時管理者就可以選擇適當的 USB 裝置當作備份裝置。

設定完成的備份裝置會列表，除了顯示連線方式及狀態外，也會把剩餘的容量標示清楚，如下圖所示。（圖 3-11）

圖 3-11、備份裝置列表

(二)、備份設定

配置完成備份裝置後，第二個步驟就是設定備份，例如，備份的時間，備份的結果要通知哪個收件者等資訊。（圖 3-12）

圖 3-12、備份設定

- 【設定名稱】：這個備份設定容易辨識的名稱，例如，Backup。
- 【狀態】：要不要啟用這個備份設定，管理者可以預先設定一些備份機制，再由這個開關動作，決定要啟用哪個機制。
- 【備份裝置】：選擇一個要備份的裝置，這些裝置都已經事先在裝置設定中設定完成。
- 【備份排程】：何時要啟用這個備份，系統是以 24 小時制，每次備份都是差異化備份，所以最高可以建立 24 筆備份，如果同一時間設定 2 筆，則只有第一筆會生效。

- 【週目錄保留份數】：備份時使用週數當作目錄名稱，超過設定值，則最舊的週數會被覆蓋掉，例如設定 52 ，則目錄就會按照週數備份，一年後就蓋掉原來的週數，當設定為 0 時，週數就一直累加，不覆蓋。

- 【完整備份指定時間】：指定 "完整備份" 每週的執行時間，可以在一周內多次的完整備份，

  一行一筆設定值，關鍵字，【D】：星期幾，【T】：時間範圍。

  範例：

  D2T0800-1100：星期二 08:00 ~ 11:00

  D5T1200-1500：星期五 12:00 ~ 15:00

  上述範例為 "星期二 08:00 ~ 11:00" 和 "星期五 12:00 ~ 15:00" 區間內所執行的系統備份會做 "完整備份"，其餘時間為 "增量備份"，若不輸入指定時間就只做 "增量備份"

- 【項目 - 系統設定】：系統設定要不要備份。

- 【項目 – 日誌與郵件】：日誌跟郵件類的資料要不要備份。

- 【通知信收件者】：備份結果要通知哪一些郵件帳號，可以設定多筆資料。

- 【自訂通知信內容】：這個備份設定的通知信內容，在這個地方輸入，例如，這是 USB 備份結果。

備份排程的列表如下。（圖 3-13）

圖 3-13、備份設定的排程

(三)、備份還原紀錄

每個備份動作，都會被記錄下來同時列表在備份還原紀錄中，管理者可以查看列表中備份項目及時間。（圖 3-14）

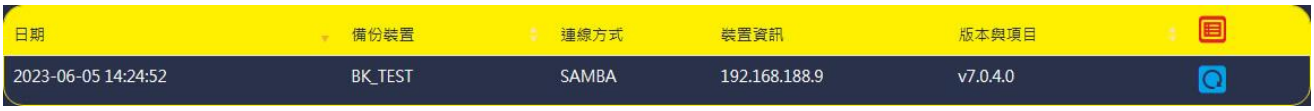


圖 3-14、備份還原列表

系統還原

當管理者決定要執行還原動作時，選擇一個時間檔的備份資料，點選圖示，系統就會開始執行還原動作，將系統回復到這個備份時的狀態。

(四)、完全備份設定

執行完全備份的動作，備份的結果可以在旁邊的【完全備份紀錄】中查詢。（圖 3-15）

圖 3-15、完全備份

- 【備份裝置】：選擇一個要備份的裝置，這些裝置都已經事先在裝置設定中設定完成。
- 【名稱】：這個備份設定容易辨識的名稱，例如，ADATA SP900。
- 【狀態】：要不要啟用這個備份設定，管理者可以預先設定一些備份機制，再由這個開關動作，決定要啟用哪個機制。
- 【備份間隔時間】：每次執行完全備份的時間間隔，可以用關鍵字，【d】：天，【h】：小時，1d/3h 代表 1 天 3 小時。
- 【通知信收件者】：備份結果要通知哪一些郵件帳號，可以設定多筆資料。

【自訂通知信內容】：這個備份設定的通知信內容，在這個地方輸入，例如，這是 USB 備份結果。

3-7、系統更新

郵件歸檔伺服器支援自動韌體下載功能，可以每日定期向韌體更新伺服器自動檢查是否有最新的韌體，有最新的韌體時能自動下載到系統中，管理者只要點擊更新就完成所有動作。

(一)、註冊資訊（圖 3-16）

圖 3-16、註冊資訊

- 【系統目前版本】：郵件歸檔伺服器目前的韌體版本。
- 【註冊資訊】：產品獨一的註冊碼。
- 【上傳更新檔案】：從 HERHSIANG 官網上可下載的升級檔，點選 

的按鈕後，將他上傳到設備中，如果檔案檢查正確就會進入升級程序，升級完成後會重新開機，開機後就完成整個升級動作。

(二)、自動檢查與下載（圖 3-17）

圖 3-17、韌體自動檢查

- 【定時檢查更新】：啟用後，郵件歸檔伺服器會按照設定的時間到更新伺服器中檢查是否有最新的韌體發佈，如果在【下載方式】中設定自動下載，系統會自動將檔案下載下來後，等候管理者更新，也可以按下『立刻檢查』的按鈕，立刻檢查是否有新的韌體。
- 【最後一次檢查狀態】：顯示最近一次跟軟體更新伺服器的更新紀錄。

■ 【下載方式】：共有 2 種可以選擇，自動下載跟手動下載，不論哪一種，下載的更新檔只會放在硬碟中，要更新韌體必須由管理者按下更新鍵，才會真正進入更新程序。

(三)、更新日誌

點選 

按鈕後，系統會顯示郵件歸檔伺服器的歷史更新紀錄。

3-8、套件管理

Machive 系列只有**查詢者-郵件行為分析 (大數據行為分析模組) 需選購**。在購買之前管理者可以先試用，滿意後再購買，試用的動作很簡單，只要按 

按鍵就可以。

註冊資訊（圖 3-18）

圖 3-18、套件試用

■ 郵件行為分析】：輸入正確的授權碼後就可以啟用，在啟用之前可以先試用，在輸入授權碼的地方輸入 Trial 字樣，按下 

按鍵就完成試用的程序，試用期限為 15 天，到期後會自動關閉。啟用後，到使用者介面，主選單就會出現關聯圖、工時表及寄信總計等 3 項郵件使用者行為分析的按鈕。

(一)、郵件履歷

郵件經過反覆的回覆轉寄，在不斷的轉寄中又加入新的收件者，到最後，郵件的收件者搞不清楚這一封郵件的來龍去脈，萬一某個人中途加入，他也很難去追蹤及閱讀郵件，除非他很有耐心的去讀這封郵件，在時間寶貴的現代社會，這是浪費時間的事，而郵件履歷提供郵件追蹤工具，讓能進入歸檔伺服器查詢郵件的使用者，清楚地察看每一封郵件的來歷。

進入使用者介面後，找一封有很多 Re 或是 Fw 的郵件，（圖 3-19）

圖 3-19、郵件履歷的應用

點選  圖標，系統就會自動出現這一封郵件的履歷圖，為了方便閱讀，可以用滑鼠的滾輪，放大或是縮小時間刻度。（圖 3-20）

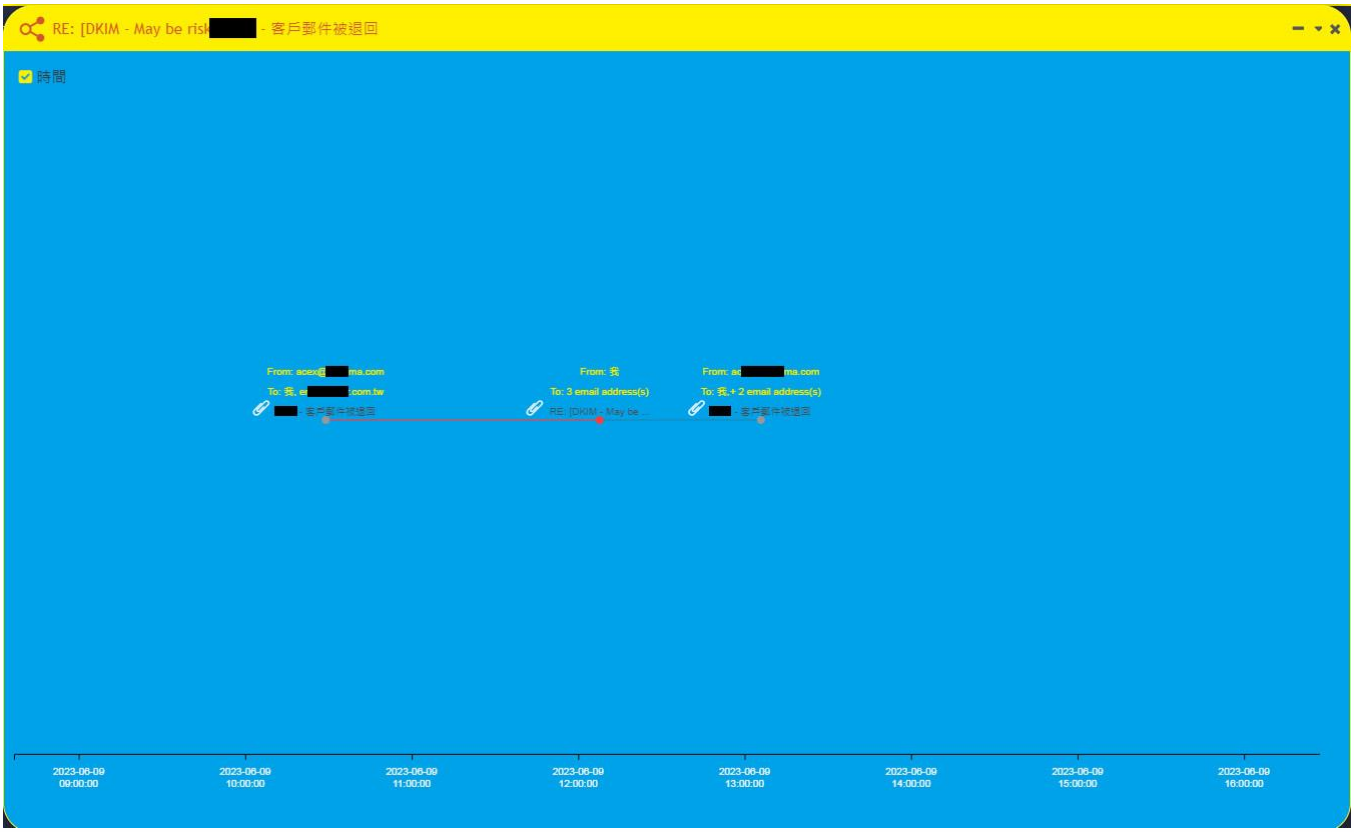


圖 3-20、郵件履歷

系統會按照時間的先後順序排列出郵件的來龍去脈，紅色的線代表目前這一封郵件是由誰轉寄過來，其他的顏色的點只是顯示其中的某一個收件者在哪個時間閱讀這一封郵件。按照時間順序說明：

A：郵件最初的發起者。

B/E：郵件被收件者在哪時候閱讀。

C：轉寄這封郵件的寄件者。

D：當下郵件履歷的郵件。

F：這一封郵件還有下文或是被閱讀。

如果取消時間軸，則郵件履歷只會出現郵件的先後順序圖，而沒有時間刻度。

點選每一個節點，系統就會出現這個節點當下的郵件摘要，點選郵件內容就可以查看此封郵件。（圖 3-21）

圖 3-21、郵件履歷中的郵件摘要

(二)、郵件行為分析（選購）

郵件行為分析包含 3 項子功能，分別是關聯圖、工時表及寄信總計，當具有進入使用者查詢介面的帳戶登入後，可以在主選單中選取要查看的功能。（圖 3-22）

圖 3-22、郵件行為分析切換

(A)、關聯圖

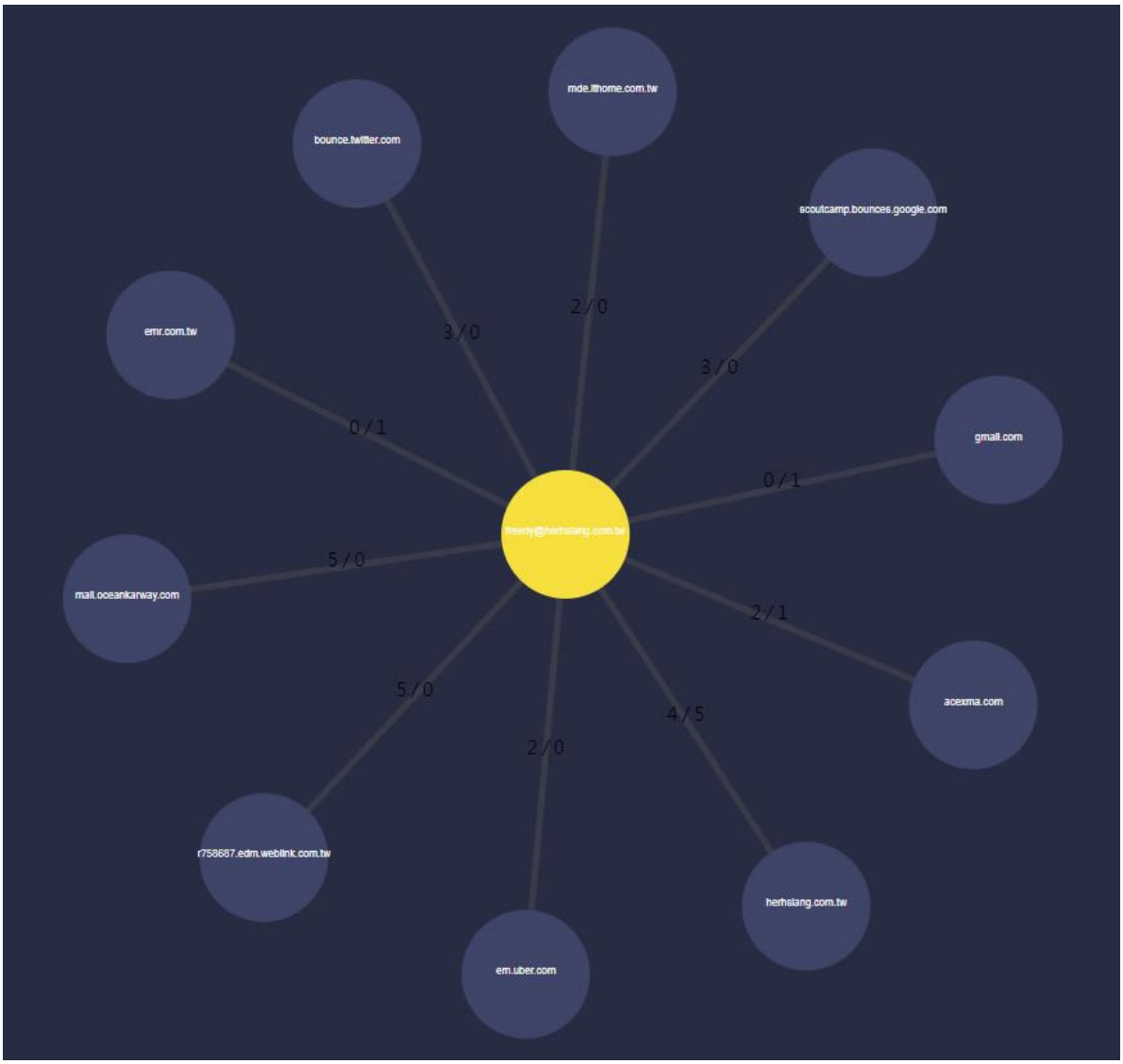
關聯圖的最主要目的是分析帳號/檔案/網域的整體通聯分析，例如，某個特定帳號對哪一個網域、帳號的寄信/收信數量統計分析，能分析的項目如下：

帳號：某個帳號他的通聯數據分析。

網域：某個網域的通聯分析。

檔案：某個檔案被傳遞的通聯分析，最主要可以追蹤檔案被轉寄的過程。

關聯圖的 2 種呈現方式。

星狀圖

列表式

網域	帳號數量	收件數量	寄件數量	total
herhsiang.com.tw	2	4	5	9
r758687.edm.weblink.com.tw	5	5	0	5
mail.oceankarway.com	1	5	0	5
acexma.com	1	2	1	3
bounce.twitter.com	3	3	0	3

在星狀圖可以點選通聯的網域後，系統會列出對這一個網域的帳號寄信/收信的分析圖，借這樣的分析圖表，就可以知道帳號之間的通聯頻率。（圖 3-23）

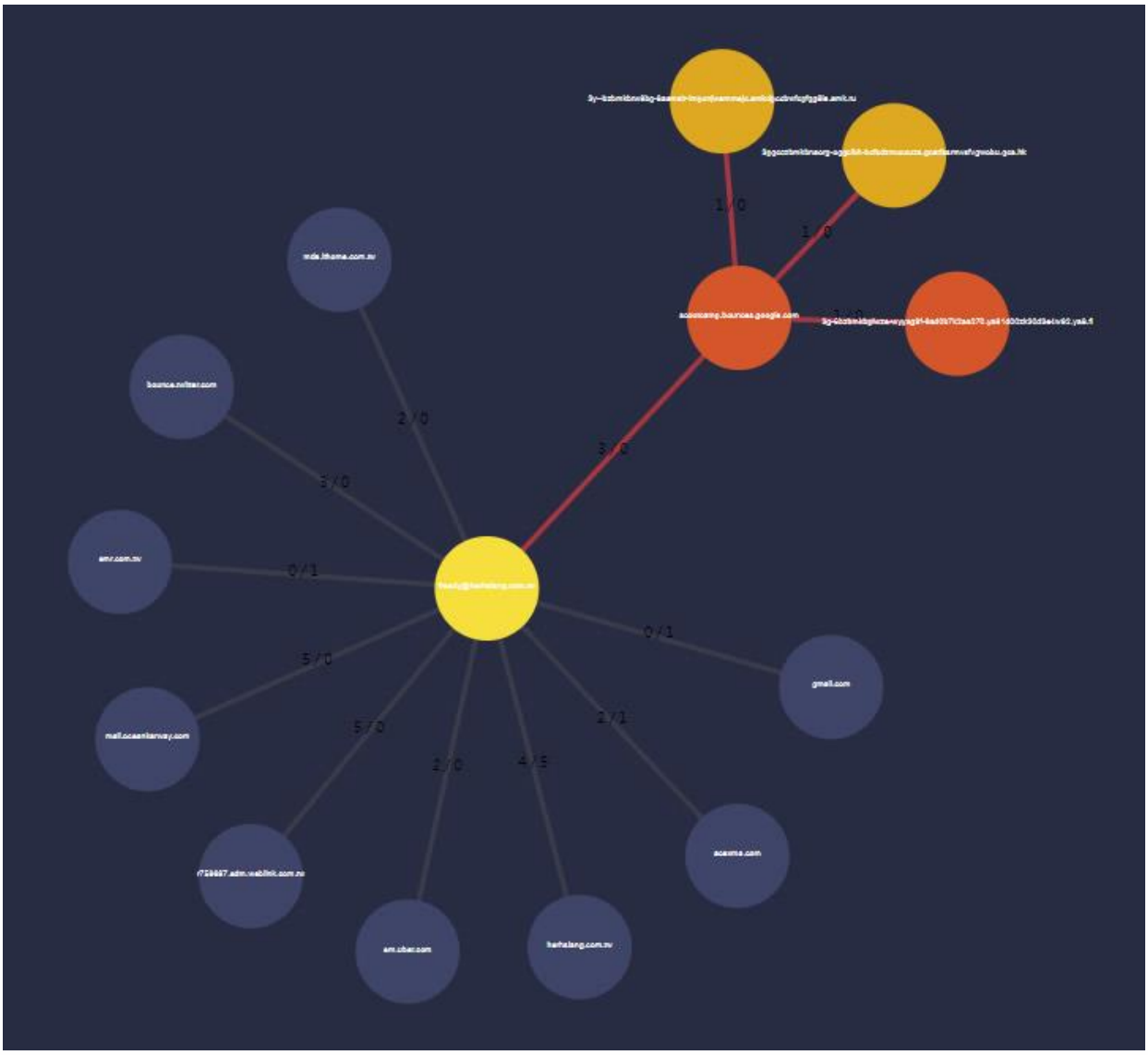


圖 3-23、郵件通聯圖

在列表圖中點選  ，就可以看這一個項目下的所有郵件列表。（圖 3-24）


收件郵件
寄件郵件
Microsoft Outlook 測試郵件
[Spam-Mail][SPF - Sender may be risky]来自您账户的付...
[Spam-Mail][SPF - Sender may be risky]来自您账户的付...
[Spam-Mail][SPF - Sender may be risky]Microsoft Outlo...
« ‹ 1 / 1 › »

圖 3-24、郵件內容列表

關聯圖中，選擇【檔案】模式下，輸入要查詢的檔案名稱或是關鍵字，系統就會把相關類似的資訊列出，以下圖為例，查詢 “報價單” ，系統就會把檔名是報價單的通通列出。（圖 3-25）

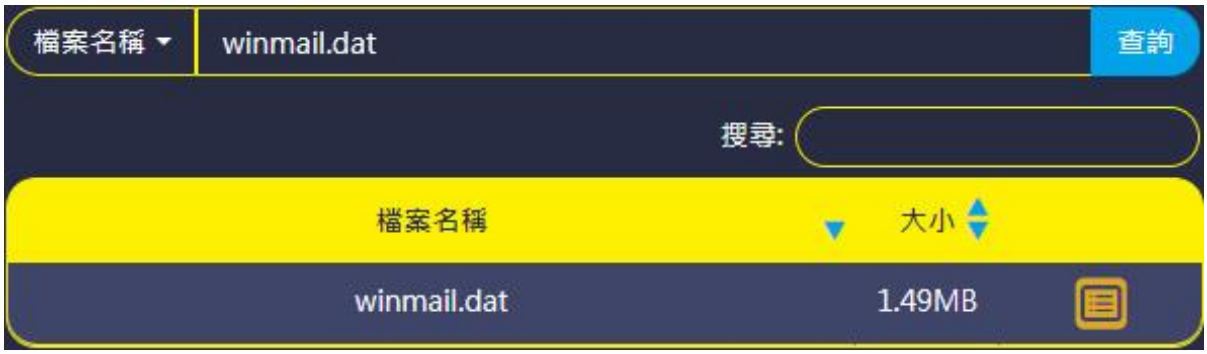


圖 3-25、搜尋列表

在列表圖中點選  ，就可以看這一封原始郵件內容。在列表部分，會依照檔案名稱、相關網域及帳號分類列表，就看使用者想要從哪一個分類進行查詢，裡面的資料都一樣。

在星狀圖中還可以看出這一個檔案是由誰寄給誰，有哪一些人收過這一個檔案。（圖 3-26）

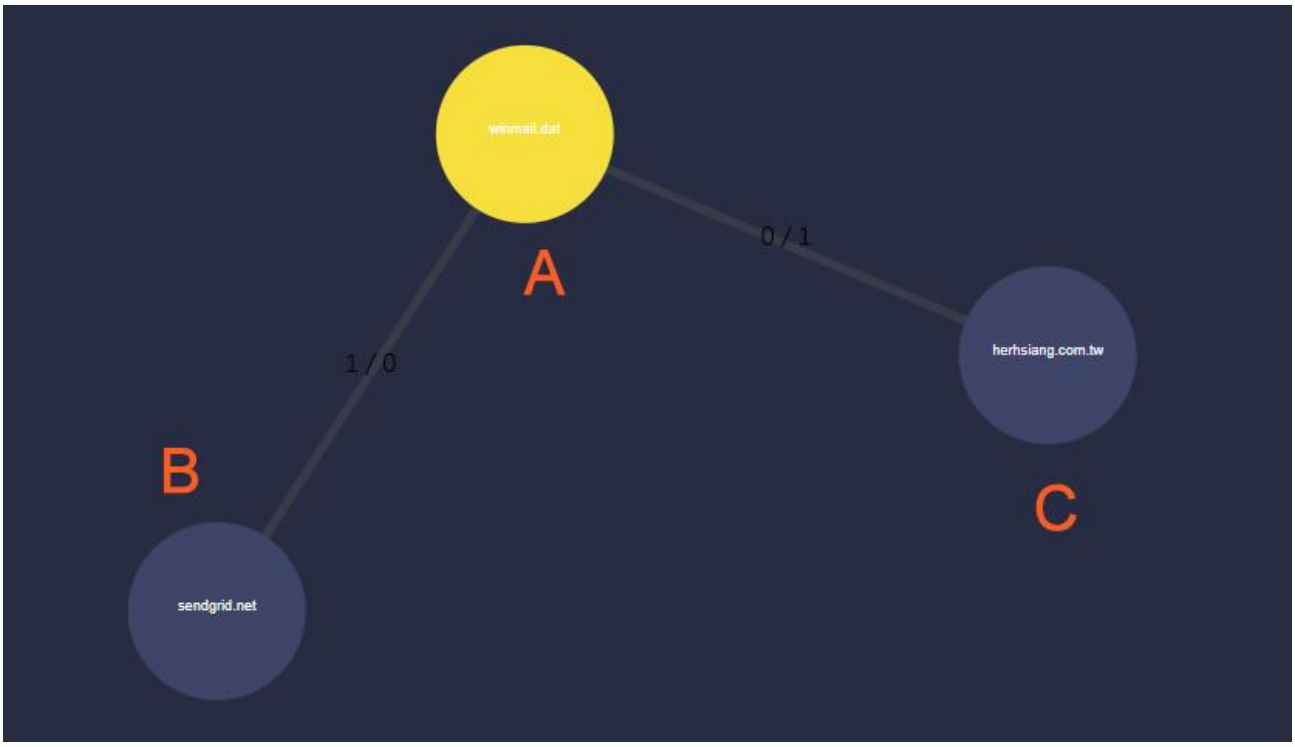


圖 3-26、檔案履歷

A：檔案名稱

B：寄件者帳號

C：收件者帳號

(B)、工時表

工時表也是郵件歸檔伺服器行為分析中一個很重要的功能，他的基本概念是計算每一個帳號的使用者處理郵件的時間統計值，包含讀信及寫信的動作。（圖 3-27）

圖 3-27、工時表總攬

第一個區是工時表的統計區，以時間為橫軸，以上圖為例，郵件工時 12 小時的 1 個帳號，郵件工時 1 小時的有 1 個帳號，統計的區間當然也可以用周、月或是特定時間區間。

第二區則是詳細資訊列表，點選  則出現此帳號的處理郵件時間情況，預設會顯示精簡模式。（圖 3-28）

圖 3-28、工時表

在時間軸上顯示此帳號的郵件處理數量，由上圖可以知道此帳號處理郵件的時間集中在9:40~13:20。點選  可以看到這一封郵件的原始內容。

詳細模式則會列出主旨跟時間軸。（圖 3-29）

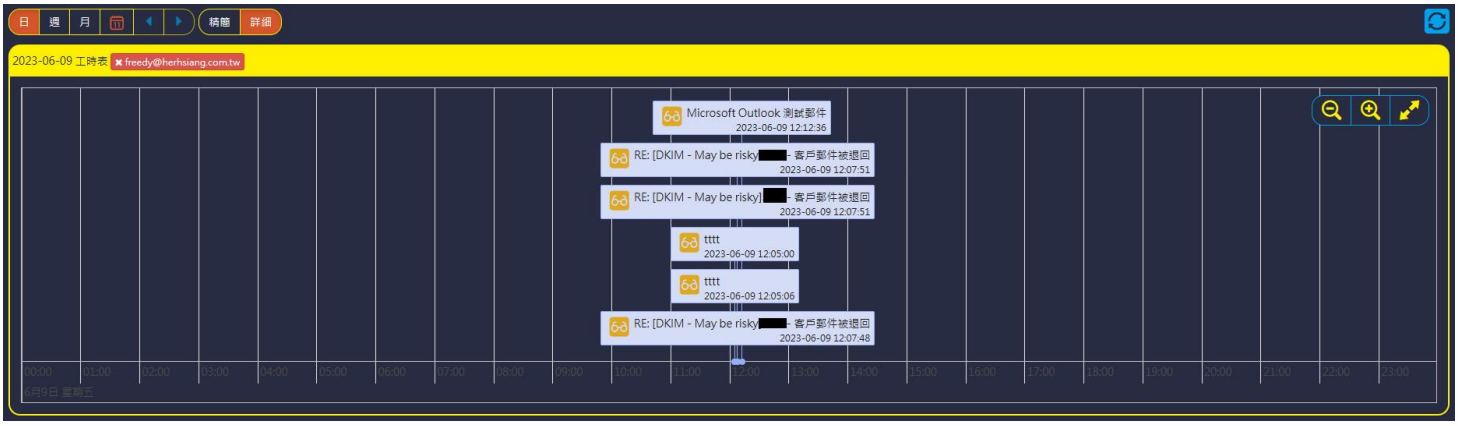


圖 3-29、詳細工時表

(C)、寄信總計

寄信總計會統計每一個帳號的過去一段時間內，他的寄信數量跟今日寄信數量的比較，例如過去一段時間，sys_info 帳號每天寄出 0 封信，但是今日突然寄出 244 封信，數量明顯有差異，此時郵件歸檔設備會通知管理者，這個帳號有異常寄信行為。（圖 3-30）

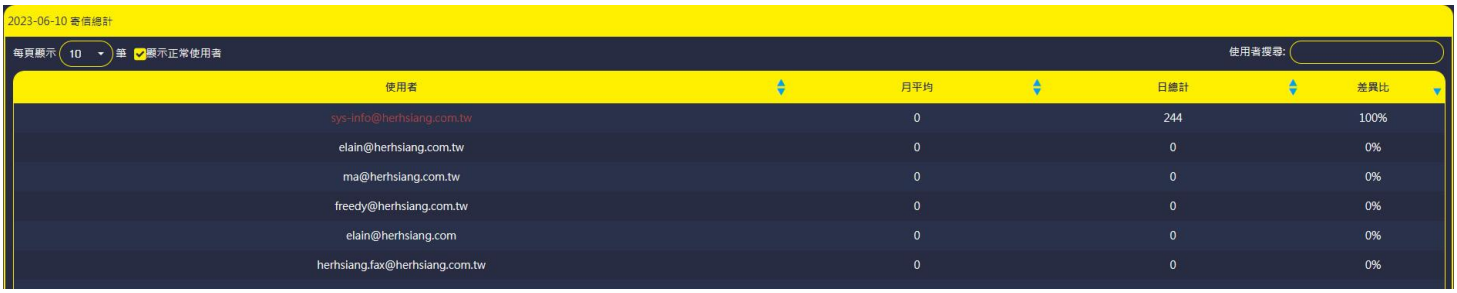


圖 3-30、異常寄信

具有進入郵件歸檔伺服器使用者介面的使用者也察看細節。（圖 3-31）

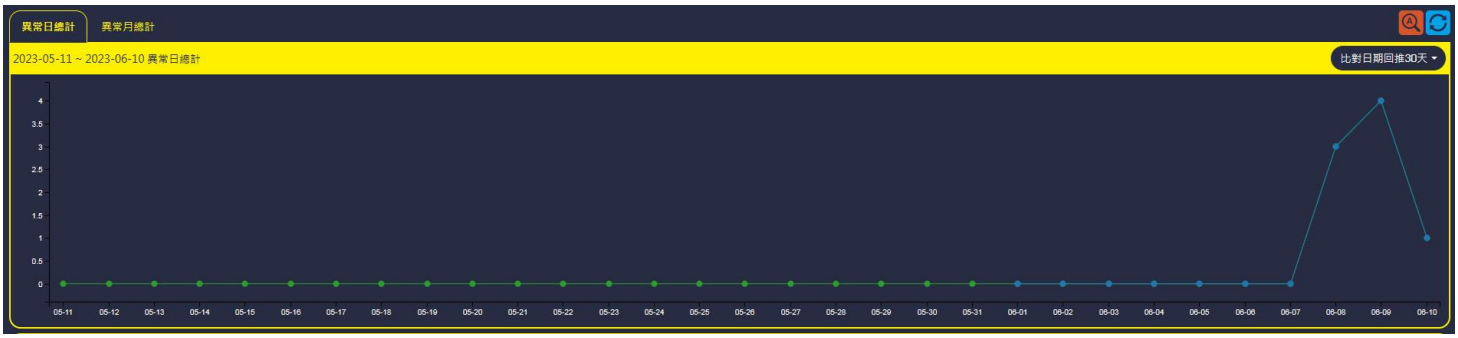


圖 3-31、異常寄信

圖表顯示每一天有異常寄信行為的人有多少，這些數據都讓管理者判斷哪一些帳號對外大量寄信，確保內部的資訊安全。

3-9、高可用性

郵件歸檔伺服器可以運作在雙機熱備援(HA)的架構，在 HA 架構下需要用 LAN IP 位址溝通取得 2 台設備的信任關係後 HA 同步埠會自動啟用同步，同步資料過程不會使用到 LAN 埠的流量，管理者才可以進行接受連線動作，連線完成後，雙方主機就會開始溝通 HA 的機制。(圖 3-32)

圖 3-32、HA 設定

- 【連線主機 LAN IP 位址】：另一台主機的 LAN IP 位址。
- 【我的設備名稱】：設備的主機名稱。
- 【我的辨識碼】：獨一無二的系統辨識碼。
- 【HA 資料同步埠】：請用 HERHSIANG 出廠時附贈 CAT. 6 網路線對接即可同步資料。

3-10、訊息通知

郵件歸檔伺服器發生問題時，可以發訊息通知管理者，傳送訊息的方式有 2 種，第一種是電子郵件，另外一種是使用 Line Notify 將訊息傳送到管理者的 Line 帳號。

(一)、一般設定

- 【寄送間隔時間】：依據問題的嚴重性，設定發送的頻率，目前分 3 個層級分別是【留意】、【注意】及【嚴重】，每一個層級發送的強度也都不一樣，每一個等級代表的事情如下。（圖 3-33）

圖 3-33、事件的嚴重性

使用關鍵字定義時間，【d】：天，【h】：小時，【m】：分，當設定成 1d/3h 代表發送的時間間隔為 1 天 3 小時。

LINE Notify

郵件歸檔伺服器發生問題時，也可以發 LINE 訊息到管理者的 Line 帳號。（圖 3-34）

圖 3-34、Line Notify 通知

- 【Client ID/Secret】：管理者需要先到 Line Notify 的網站，https://notify-bot.line.me/zh_TW/ ，用管理者的 Line 帳號登入 Line Notify 的服務，系統會給予這個服務的一組 ID / Secret ，將 Line Notify 給予的資料填入就完成基本設定。
- 【Callback URL】：填入郵件歸檔伺服器對外的域名，這個域名也要同步填入 Line Notify 註冊時使用的 Callback URL。（圖 3-35）

圖 3-35、Line Notify Callback URL

(二)、通知信群組清單

發訊息通知管理者時，可以再細分那一些訊息通知哪一些管理者，依據問題的嚴重性，有 3 個層級分別是【留意】、【注意】及【嚴重】，可以設定【嚴重】等級通知 A 管理者，其他的層級則分配給 B 管理者。

- 【名稱】：通知群組的名稱。
- 【狀態】：這個通知是開啟或是關閉。
- 【備註】：通知群組容易辨識的說明。
- 【收件者】：通知群組的收件者。
- 【通知項目】：要讓上述群組的人收到哪一些通知。

(三)、Line 通知訊息清單

- 用 Line 發訊息通知管理者時，可以再細分那一些訊息通知哪一些管理者，依據問題的嚴重性，有 3 個層級分別是【留意】、【注意】及【嚴重】，可以設定【嚴重】等級通知 A 管理者，其他的層級則分配給 B 管理者。（圖 3-36）
- 【名稱】：通知群組的名稱。
- 【狀態】：這個通知是開啟或是關閉。
- 【備註】：通知群組容易辨識的說明。
- 【Line Token】：那一些 Line 帳號要接收通知，這些帳號需要事先取得 Line Token。
- 【訊息通知設定】：Line 的發送次數有上限，當發送數量快要到達上限時，系統會自動降低發送的頻率。
- 【通知項目】：要讓上述群組的人收到哪一些通知。

圖 3-36、Line 通知設定

3-11、iSCSI 裝置管理

郵件歸檔伺服器可以用 iSCSI 協議，把網路上的硬碟綁定成自己的硬碟使用，因為用網路連線傳遞資料，管理者可以綁定多條網路線增加頻寬。（圖 3-37）

圖 3-37、iSCSI 設定

- 【聚合模式】：使用哪一種聚合模式，把 2 個網路卡的頻寬綁定，增加速度。

  Balance-RR: 負載平衡模式，採用 round robin 方式，依序由第一個 slave 網卡至最後一個 slave 網卡來傳送封包。

  802.3ad (LACP): 可將多個網路埠組成一個共享相同速度與全雙工的網路聚合，以獲得容

錯、負載平衡與提高傳輸效率的功效。需要 switch 支援 802.3ad 設定。此設定特別針對同型號網卡時使用。

Balance-ALB: 發送與接收同時具備自動負載平衡與容錯功能，其中一個網路埠失效時，仍可持續運作；此模式不需 switch 支援及設定。

- 【iSCSI 的位址/遮罩】：將指定的 Port 綁定一個 IP 位址及網路遮罩， IP 位址，必須能跟提供 iSCSI Target 的服務器能夠互通。

iSCSI 的使用

先輸入提供 iSCSI 服務的 IP 及 Port ，並按下【探索目標】的按鈕。（圖 3-38）

圖 3-38、iSCSI 探索

[探索目標]: 輸入 IP(:port) 來取得 iSCSI 目標。

[刪除目標]: 輸入 IP(:port) 來刪除此 IP 下"所有"的 iSCSI 目標。

[重新整理]: 重新探索所有記錄在本機上的 IP。

[CHAP 登入設定]: 如果 iSCSI 目標有設定 CHAP 認證，按這個按鈕來登入。

[取代主硬碟]: 套用後，將會在下次開機用選擇的 iSCSI 裝置取代主硬碟。

註: "**顏色**" 是用來分組 iSCSI 目標的。

注意: 請先中斷連線，遠端才能停用、刪除連線中的磁碟。

注意: 為了讓主機識別，在連線時"**本機未使用過**"的 iSCSI 裝置會被格式化

注意: 目標"**連線**"時，無法 "重新整理"、"刪除目標" 與 "修改 iSCSI 網路設定"

注意: "容量小於 **8G**" 的 iSCSI 裝置，無法 "取代主硬碟"

3-12、不斷電系統

為了避免郵件歸檔伺服器因為臨時的斷電，導致儲存媒體如硬碟等故障，造成設備的損毀，系統支援不斷電系統(UPS)，萬一停電後，不斷電系統的電源低於設定值，系統會自動進入關機程序，保護裡面儲存的寶貴資料。

- 【UPS 功能】：啟用 UPS 機制。
- 【UPS 連接模式】：郵件歸檔伺服器跟不斷電系統有 2 種連線方法，一個是 USB 連接，另一個是用網路連線，2 種方式的保護機制都雷同，但是用 USB 連接時，郵件歸檔伺服器還可以當 UPS 服務器，用網路方式，通知其他設備不斷電系統的狀態。

USB 連線（圖 3-39）

圖 3-39、不斷電設定

- 【網路不斷電系統伺服器】：郵件歸檔伺服器要不要提供不斷電系統伺服器給網路上其他的設備使用。
- 【使用不網路伺服器的設備 IP 位址】：網路上哪一些 IP 才可以使用郵件歸檔伺服器提供不斷電系統伺服器的功能，例如，192.168.168.100。

- 【等待關機時間】：當 UPS 停電時，如果使用這項服務的設備超過這一個時間都無回應，。則直接下關機命令。
- 【Ping Timeout】：當 UPS 停電時，使用郵件歸檔伺服器提供不斷電系統伺服器功能的設備 ping 的 Timeout 超過設定值，系統就會判斷對方已經關機。

網路不斷電系統伺服器（圖 3-40）

圖 3-40、不斷電設定

- 【網路不斷電系統伺服器 IP 位址/埠號】：輸入不斷電系統的 IP 位址及埠號，系統會自動跟不斷電系統溝通，按下【測試】鈕也可以測試連線是否成功。

網路不斷電共同設定（圖 3-41）

圖 3-41、不斷電共同設定

- 【電池低電量】：當電池的電量低於設定的比例，預設值是 80%，系統就會進入安全模式，此時會中斷對外備份的機制，並且在設定的分鐘數後進入關機程序。
- 【電池電量下限】：當不斷電系統的電池少於設定值，系統直接進入關機程序。
- 【高可用性遠端管理介面對外埠號】：在 HA 模式下，通知另外一台設備要同步執行設定事項。
- 【UPS 日誌】：所有跟不斷電系統的通聯都可以在 UPS 日誌中查詢。

訊息通知

關於 UPS 的訊息通知，目前有 電池低電量、安全模式、電池低電量倒數結束、電池電量達到下限、UPS 恢復市電供電、UPS 連線失敗等通知項目，管理者可以根據需求設定。

第 4 章 外部郵件歸檔管理

郵件歸檔伺服器可將記錄的郵件歸檔到外部的儲存裝置，例如，NAS 等進行長期的備份，這些備份的郵件可以透過郵件查詢介面查詢。

外部郵件歸檔共有 2 個部分，一個是郵件資料庫，另一個是郵件本身，郵件資料庫提供管理者快速查詢郵件的基本資料，例如，寄件者、收件者、主旨、摘要等訊息，並提供真正的郵件內文是儲存在那一個儲存媒體。這 2 個資料庫可以分開儲存在不同的儲存設備。

4-1、資料庫備份設定

資料庫主機需要外部的儲存裝置提供 SQL 的連線方式，郵件歸檔伺服器用 SQL 語法直接加入資料庫中。（圖 4-1）

圖 4-1、資料庫主機設定

- 【主機代碼】：系統自動產生，要跟外部的備份主機配對使用。
- 【名稱】：資料庫備份容易辨識的名稱。
- 【啟用】：這一個備份是否要啟用。
- 【主要備份 / 查詢備份主機】：是主要的備份主機還是備援的主機，主要主機只能設定一台，備份主機則只能使用查詢功能。
- 【快速模式】：要不要啟用快速的備份模式，當遠端的資料庫設定值 myisam_max_sort_file_size 大於 200G 時，快速模式才會啟用，當數值小於 200G，則快速模式會失效。
- 【主機顏色】：備份容易辨識的顏色。
- 【主機名稱或 IP】：外部資料庫的名稱或是 IP 位址，例如，192.168.168.9。
- 【埠號】：資料庫使用的通訊埠，SQL 預設是 3306。
- 【帳號】：外部資料庫具有讀寫權力的帳號。
- 【密碼】：外部資料庫具有讀寫權力帳號的密碼。
- 【測試連線】：設定完成後按下【測試連線】按鈕，驗證上述的設定質是否正確。

4-2、郵件檔案備份設定

郵件實際儲存的位置，用檔案的方式記錄所有歸檔的郵件。（圖 4-2）

圖 4-2、郵件備份設定

- 【裝置名稱】：郵件備份容易辨識的名稱。
- 【標記】：系統自動產生，要跟外部的備份主機配對使用。
- 【啟用】：是否要啟用。
- 【連線方式】：有 3 種連線方式，分別是 SAMBA、USB 跟 iSCSI，每一種都有不同的設定方式。
- 【遠端主機名稱或 IP】：外部儲存裝置的名稱或是 IP 位址，例如，192.168.168.100。
- 【遠端備份資料夾】：備份的資料夾。
- 【帳號】：外部儲存裝置具有讀寫權力的帳號。
- 【密碼】：外部儲存裝置具有讀寫權力帳號的密碼。

【測試連線】：設定完成後按下【測試連線】按鈕，驗證上述的設定質是否正確。

第 5 章 架構管理

郵件歸檔伺服器有 3 種方式記錄郵件，分別是透通模式、閘道模式跟代收模式，管理者根據自己的需求啟用其中一個或是同時啟用多種模式，系統會自動根據收到郵件中網域名稱，自動分類，管理者再根據網域名稱分配不同的查詢者，關於權限分類，請參考第 6 章認證與權限管理。

根據郵件伺服器架設方式跟擺放地點，郵件歸檔伺服器啟用的模式也稍微有不同，管理者可根據實際狀況，採取不同的運作模式，參考架設模式如下表：

郵件伺服器架設及放置地點	透通/閘道	代收
郵件伺服器在自己公司內部	○，註	○
自有郵件伺服器主機，但是託管在 ISP 機房中	○，註	○
跟 ISP 業者承租郵件服務	○，註	○
跟 Gmail / Office 365 / 163 承租郵件服務	○，註	○

註：郵件歸檔伺服器的透通/閘道模式只支援 SMTP / SMTPS 2 種通訊協定紀錄郵件，如果使用者採用 WebMail 的方式，收送郵件，這些郵件就無法被記錄。

(一)、透通/閘道模式

在透通/閘道模式下，郵件歸檔伺服器會把所有進出設備的 SMTP 跟 SMTPS 的連線通通代理下來，經過內部的代理程序後再把這些通訊協定送到目的端。對於自己架設郵件伺服器的環境來說，郵件歸檔伺服器擺放的位置有 2 個地方，如下圖中 A、B 2 個圖示：（圖 5-1）

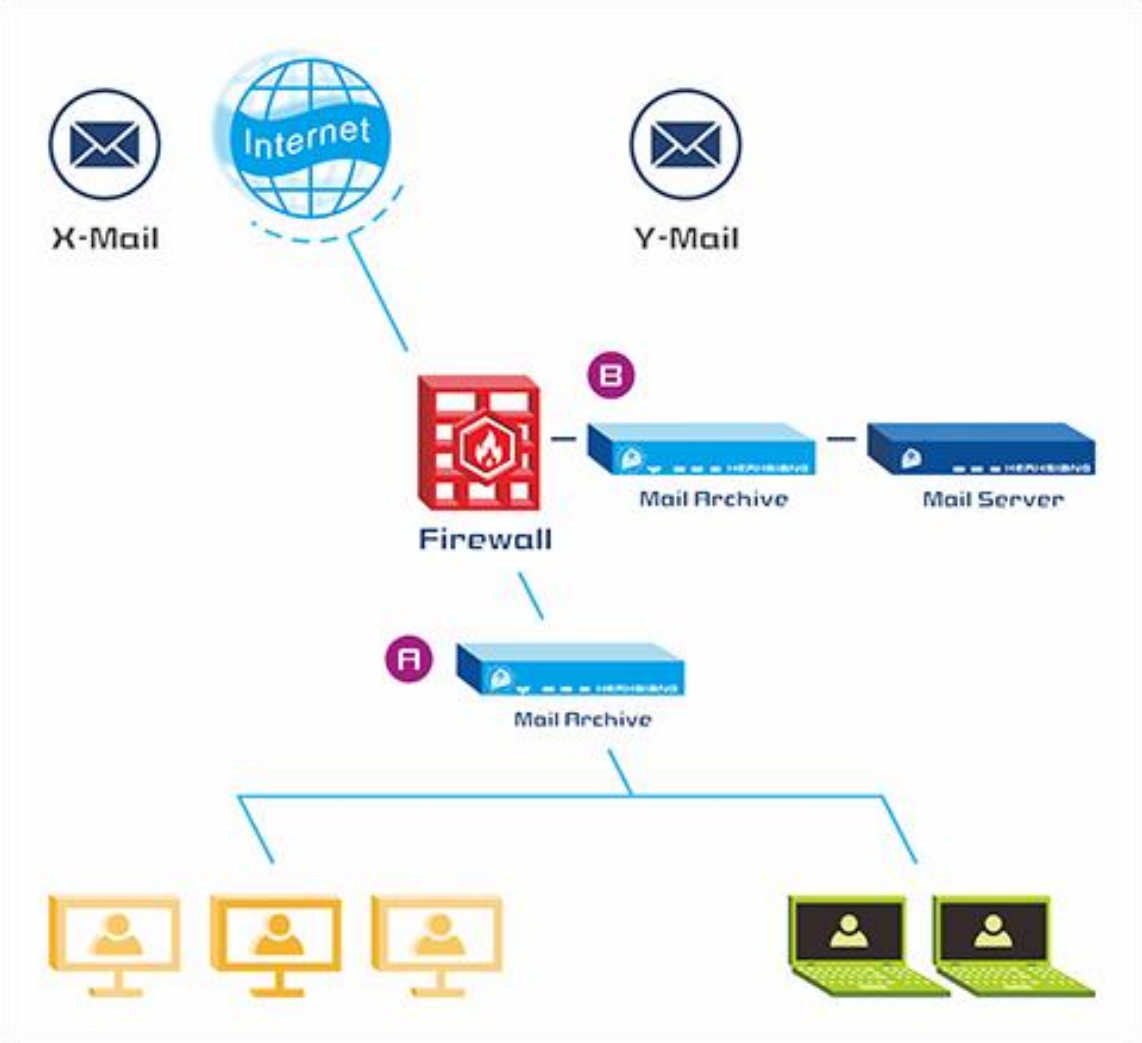


圖 5-1、透通模式配置圖

位置 A ：除了記錄自己的郵件伺服器的通聯記錄之外，如果內部使用者有用外部的郵件伺服器，例如， X-Mail Server / Y-Mail Server 寄發郵件 ，他的郵件也會被記錄下來。這個位置也適用於將郵件伺服器託管在 ISP 機房或是跟 ISP 業者承租郵件空間等環境。

位置 B ：單純記錄自己的郵件伺服器的通聯記錄。

(二)、代收模式

代收的運作原理是在郵件伺服器上建立一個帳號，例如，archive.yourdomain.com，並在郵件伺服器上設定一個規則，將所有進出的郵件都複製一份給 archive.yourdomain.com，郵件歸檔伺服器再依照設定的時間內用 POP3/IMAP 的方式將郵件收到系統中，收到的郵件就會依照網域名稱跟郵件帳號分類，方便管理者、查詢者或是使用者查詢使用。(圖 5-2)

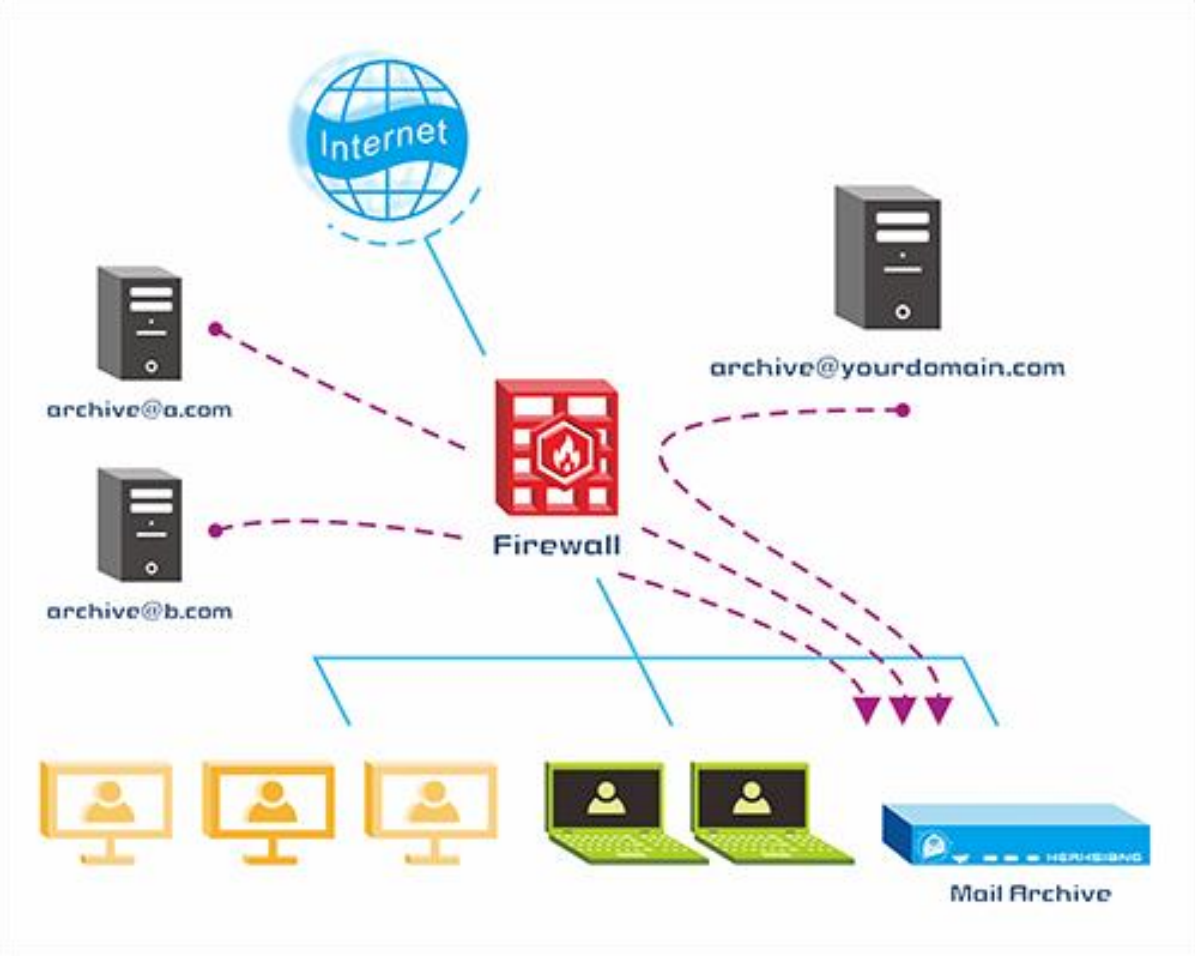


圖 5-2、代收配置圖

在代收郵件，為了避免代收帳號空間爆掉，管理者需要選擇代收後就刪除郵件還是保留數天後刪除郵件。郵件歸檔伺服器可以建立多筆代收帳號分別指向不同的郵件主機。

系統最多可以同時啟用 8 個代收程序跟外部的郵件伺服器收取郵件，如果有超過 8 個的代收帳號，例如，第 9 個，它需要等到前面 8 個中有任一個結束代收程序後，第 9 個才會啟用代收程序，每個代收程序結束後會等 15 分鐘才再次啟用。如果代收程序超過 1 個小時，將會被系統中斷。

5-1、基本設定

郵件歸檔伺服器的透通跟閘道模式，可以定義郵件進出方向，是外面進來還是由內部出去的方向，且每一個方向要進行那一些動作，共有 3 種選項可以選擇，分別是 郵件稽核及防護、垃圾郵件跟病毒過濾等。(圖 5-3)

圖 5-3、架構管理的基本設定

- 【驗證收件者是否有效】：郵件歸檔伺服器不是郵件伺服器，沒有郵件帳號的資料，因此無法判斷收下來的郵件帳號真偽，除了後端有 AD 伺服器或是 HERHSIANG 的郵件伺服器可以自動增加郵件帳號外，如果要增加垃圾郵件辨識率或是降低無效郵件數量，管理者可在【認證與權限管理】>【使用者管理】中加入有效的郵件帳號。

  啟用這個功能後，外部的郵件伺服器要寄信到內部的郵件主機，系統會到後端的郵件主機驗證這個收信者帳號是否有效，有效則會進入郵件接收程序，無效則會拒絕這次的 SMTP 通聯，如果管理者沒有執行任何帳號同步機制或是建立有效的郵件帳號，啟用這個功能會導致郵件無法正常進入後端的郵件伺服器。

  關閉這個功能，代表系統會收下所有收信者的信，不論是有效或是無效收信者然後轉給後端的設備繼續處理。

- 【阻擋日誌】：上面【驗證收件者是否有效】啟用後，被阻擋的郵件會被記錄在這裡。(圖 5-4)

圖 5-4、啟用有效帳號檢查後的日誌

- 【外對內處理】：從外部進入內部的郵件執行那些附加功能，有 3 種附加功能可以選擇，分別是郵件稽核及防護、垃圾郵件及病毒郵件，管理者可以點選空白處選擇要增加的附加功能或是按下『全選』按鍵。

  郵件稽核及防護：對進來的郵件執行郵件稽核過濾功能，詳細說明請參照第 6 章 郵件稽核及防護。

  垃圾郵件：對進來的郵件執行垃圾信過濾功能，詳細說明請參照第 8 章 垃圾郵件。

  病毒郵件：對進來的郵件執行病毒郵件功能，詳細說明請參照第 7 章 病毒郵件。

- 【內對外處理】：針對內部出去外部的郵件執行那些附加功能，有 3 種附加功能可以選擇，分別是郵件稽核及防護、垃圾郵件及病毒郵件，管理者可以點選空白處選擇要增加的附加功能或是按下『全選』按鍵。

  郵件稽核及防護：對外寄的郵件執行郵件稽核過濾功能，詳細說明請參照第 6 章 郵件稽核及防護。

  垃圾郵件：對外寄的郵件執行垃圾信過濾功能，詳細說明請參照第 8 章 垃圾郵件。

  病毒郵件：對外寄的郵件執行病毒郵件功能，詳細說明請參照第 7 章 病毒郵件。

(一)、透通模式

■ 【郵件伺服器備援】：在透通模式下，萬一後端的郵件伺服器故障，郵件歸檔伺服器可以將外部寄給郵件伺服器的郵件紀錄下來，擁有查詢歸檔郵件的使用者可以進入查詢介面，看到郵件內容。(圖 5-4-1)

圖 5-4-1 郵件伺服器備援

(二)、閘道模式

閘道模式跟透通模式不一樣，藉由設定 SMTP 代理的機制，將進出郵件伺服器的郵件紀錄下來，這個模式下，不需要用網路串接的方式改變實際的網路接線。(圖 5-5)

圖 5-5、閘道模式設定

- 【啟用閘道】：啟用這項功能。
- 【回應給使用者端的認證方式清單】：使用哪種驗證機制跟回覆給使用者的 EHLO 的命令，有 3 種，可以複選，方別是 Login、PLAIN 跟 NTLM，當【驗證收件者是否有效】有啟用時才需要設定。
- 【其他認證方式與主機】：非上述的驗證方式使用者，管理者需要自訂方式跟認證主機的 IP 位址，例如，CRAM-MD5/192.168.168.100，當【驗證收件者是否有效】有啟用時才需要設定。
- 【當認證帳號無網域時的認證主機】：郵件帳號中的網域沒有被設定時，跟誰驗證帳號有效，預設是 127.0.0.1，也就是用本機的帳號。
- 【內部的 IP 或網段】：定義內部 IP 區段。

(三)、代收模式

代收模式下，系統用 Pop3、IMAP 跟雲端代收的 3 種方式將郵件代收到伺服器中。(圖 5-6)

圖 5-6、代收模式設定

- 【POP3 代收】：啟用或是關閉 POP3 代收功能，啟用後再到【POP3 代收】這個章節增加代收的帳號。
- 【POP3 連線逾時】：每次 POP3 代收時最長的等待對方郵件伺服器回應時間，超過時間則需要在等設定的間隔時間(系統預設是 15 分鐘)後才會再次收信，預設是 180 秒。
- 【IMAP 代收】：啟用或是關閉 IMAP 代收功能，啟用後再到【IMAP3 代收】這個章節增加代收的帳號。
- 【雲端硬碟代收】：啟用或是關閉雲端硬碟代收功能，啟用後再到【雲端硬碟代收】這個章節增加代收機制。
- 【檢查路徑間隔時間】：每隔多少時間檢查雲端硬碟的資料。
- 【檢查郵件間隔時間】：每隔多少時間檢查郵件。
- 【執行逾時】：檢查時超過多少時間放棄這次檢查。

5-2、網路介面及路由

郵件歸檔伺服器是具有多 Port 的網路設備，除了系統保留的 2 個 Port 分別給 LAN 及 HA 外，根據不同的硬體，管理者可以指定哪些 Port 執行 3 種運作模式：透通、閘道跟代收之一或是全部組合。

(一)、透通模式

在透通模式下需要用 2 個 Port 進行網路封包攔截的動作，一個對外一個對內，如果實體 Port 數足夠，管理者可以設定 2 段透通模式，分別側錄不同的網段。(圖 5-7)

圖 5-7、新增一組透通 Port

- 【埠號綁定】：系統會呈現實際的機器外觀，除了 2 個系統保留 Port 外，管理者可以任意指定 2 個 Port 為一組透通模式，並註明對外或是對內，如果網卡沒被標示為使用中，點選網卡編號的  圖示就可以切換運作模式，運作模式的循環分別是 停用➔對外➔對內。

- 【IPV4 的位址】：設定 IPV4 的 IP 位址，當郵件歸檔伺服器在透通模式下，會把郵件攔下來，經過處理程序後，需要再傳送給目標的郵件伺服器時，就會利用這個 IP 位址當作來源 IP 位址進行傳遞的動作。例如，192.168.168.167，此時後端郵件伺服器就會看到來源 IP 位址 192.168.168.167 的 IP 位址要求寄信。

- 【IPV4 子網路遮罩】：設定 IPV4 的子網路遮罩，例如，255.255.255.0。
- 【IPV4 閘道器位址】：設定 IPV4 的閘道器位址，設上正確的閘道器位址讓郵件歸檔伺服器能夠正常地從網際網路上寄到目標郵件伺服器。例如，192.168.168.254。
- 【IPV6 的位址】：設定 IPV6 的 IP 位址，如果不知道該如何設定 IPV6 的 IP 位址，可以先設定【IPV6 閘道器位址】，再按旁邊的『MAC 轉 IP』按鈕，系統會用機器的 MAC 位址，自動轉換成 IPV6 的位址，例如，2001:b030:c004:0:192:168:168:167。
- 【IPV6 子網路遮罩】：設定 IPV6 的子網路遮罩，範圍可以是 0 ~ 128，一般預設是 64，例如，64。
- 【IPV6 閘道器位址】：設定 IPV6 的閘道器位址，設上正確的閘道器位址讓郵件歸檔伺服器能夠正常地從網際網路上寄到目標郵件伺服器，例如，2001:b030:c004:0:192:168:168:254。

設定完成的資料就會在列表中，如（圖 5-8）

圖 5-8、透通 Port 列表

其中橋接器名稱是系統預設的會從 br0 開始編號，管理人員可以按後面的圖示，對已經建立的透通組合進行修改或是刪除動作。

(二)、閘道模式

使用閘道模式前，需要先在【架構管理 > 基本設定】的【閘道模式】啟用，下列設定才會生效，在閘道模式下只需要用 1 個 Port 對外通訊，系統會自動標示哪一些 Port 已被其他的服務佔據，哪一些 Port 是可以使用。(圖 5-9)

圖 5-9、新增閘道 Port

- 【聚合模式】：使用哪一種聚合模式，把 2 個網路卡的頻寬綁定，增加速度。

  Balance-RR: 負載平衡模式，採用 round robin 方式，依序由第一個 slave 網卡至最後一個 slave 網卡來傳送封包。

  802.3ad (LACP): 可將多個網路埠組成一個共享相同速度與全雙工的網路聚合，以獲得容錯、負載平衡與提高傳輸效率的功效。需要 switch 支援 802.3ad 設定。此設定特別針對同型號網卡時使用。

  Balance-ALB: 發送與接收同時具備自動負載平衡與容錯功能，其中一個網路埠失效時，仍可持續運作；此模式不需 switch 支援及設定。

- 【埠號綁定】: 系統會呈現實際的機器外觀，除了 2 個系統保留 Port 外，管理者可以任意指定 Port，點選網卡編號的  圖示就可以指定使用的 Port。

- IP 設定方式跟透通模式類似。

(三)、路由設定

幫郵件歸檔伺服器手動增加路由表。(圖 5-10)

圖 5-10、新增路由表

- 【名稱】：路由表的名稱。
- 【目的 IP 網路 / 遮罩】：IPV4 或是 IPV6 路由表的區段。
- 【閘道】：目的 IP 網路要往哪裡送？
- 【介面】：上述路由表生效的介面。

5-3、POP3 代收

郵件歸檔伺服器的 POP3 代理可以跟提供雲端郵件服務的業者整合，例如，Gmail、Office365 或是 163 等雲服務業者，只要建立一個帳號並把所有的進出郵件轉給那個帳號，郵件歸檔伺服器就可以將這些郵件下載到本地端，讓企業能夠保有這些重要的郵件資產，新增一筆 POP3 代收。(圖 5-11)

圖 5-11、新增一筆 POP3 代收

(一)、帳戶資訊

- 【名稱】：給這個 POP3 代收帳號一個方便辨識的名稱，例如，放在 Gmail 的網域。
- 【電子郵件地址】：POP3 帳號使用的電子郵件地址，通常會跟認證帳號相同，例如 ma@herhsiang.com.tw。

(二)、內送(POP3)伺服器資訊

- 【POP 伺服器】：POP3 伺服器主機的 IP 位址或是網域名稱，例如，pop3.yourdomain.com。
- 【埠號】：POP3 伺服器使用的通訊埠，預設是 110。
- 【功能狀態】：共有 5 項功能可以選擇。

  1、啟用代收：

  設定完成後，要不要啟用這項功能。

  2、擷取郵件使用安全連線(SSL)：

  是否使用加密的方式 POP3S 去收郵件，POP3S 的預設埠號是 995，點選後，【埠號】會自動更新為 995。

  3、在伺服器上保留已擷取郵件的副本，伺服器上超過幾天郵件刪除：

  收下郵件後要不要把郵件從郵件伺服器刪除，或是保留幾天後刪除，如果設為 0 代表不刪除郵件，此時就要注意這個帳號的容量限制。

  4、自動將郵件學習到垃圾郵件白名單：

  收到的郵件自動放入垃圾郵件的白名單中學習。

  5、自動將郵件學習到垃圾郵件黑名單：

  收到的郵件自動放入垃圾郵件的黑名單中學習。

- 【認證帳號】：用 POP3/POP3S 去收郵件時使用的認證帳號，例如，mail.archive@yourdomain.com。
- 【認證密碼】：POP3/POP3S 認證帳號使用的密碼，要確認輸入是否正確，可以點選顯示密碼，驗證輸入的密碼正確與否。
- 【重收所有郵件】：在 POP3/POP3S 郵件伺服器主機尚未刪除郵件前且系統重建下，可以用 POP3、POP3S 把郵件重新收下來。

建立完成後的列表如下：(圖 5-12)

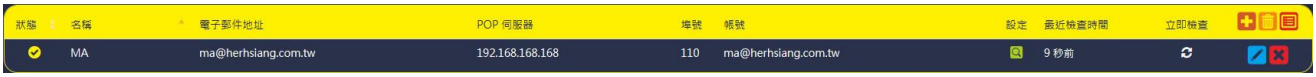


圖 5-12、POP3 代收列表

在列表中會顯示每一個 POP3 帳號最近的收信動作，管理者可以在列表中直接點選立即檢查按鈕，也可對任何一筆資料作修改刪除動作。

對於已經建立的 POP3 帳號，可以執行匯出動作，讓管理者可以保留這些詳細的資料，並且在日後系統重建時執行匯入帳號。

5-4、IMAP 代收

郵件歸檔伺服器的 IMAP 代理可以跟提供雲端郵件服務的業者整合，例如，Gmail、Office365 或是 163 等雲服務業者，只要建立一個帳號並把所有的進出郵件轉給那個帳號，郵件歸檔伺服器就可以將這些郵件下載到本地端，讓企業能夠保有這些重要的郵件資產，新增一筆 IMAP 代收。(圖 5-13)

圖 5-13、新增一筆 IMAP 代收

(一)、帳戶資訊

- 【名稱】：給這個 IMAP 代收帳號一個方便辨識的名稱，例如，放在 Gmail 的網域。
- 【電子郵件地址】：IMAP 帳號使用的電子郵件地址，通常會跟認證帳號相同，例如 ma@herhsiang.com.tw。

(二)、內送(IMAP)伺服器資訊

- 【IMAP 伺服器】：IMAP 伺服器主機的 IP 位址或是網域名稱，例如，mail.yourdomain.com。
- 【埠號】：IMAP 伺服器使用的通訊埠，預設是 143。
- 【功能狀態】：共有幾項功能可以選擇。

  1、啟用代收：

  設定完成後，要不要啟用這項功能。

  2、自動：

  勾選自動後，後面的 3 項 SSL、Start-TLS 及自我簽署憑證將會自動帶入，不需要管理者一一設定。

  3、安全連線(SSL)、TLS 及自我簽署憑證：

  是否使用加密的方式 IMAPS 去收郵件。

  4、在伺服器上保留已擷取郵件的副本，伺服器上超過幾天郵件刪除：

  收下郵件後要不要把郵件從郵件伺服器刪除，或是保留幾天後刪除，如果設為 0 代表不刪除郵件，此時就要注意這個帳號的容量限制。

  5、自動將郵件學習到垃圾郵件白名單：

  收到的郵件自動放入垃圾郵件的白名單中學習。

  6、自動將郵件學習到垃圾郵件黑名單：

  收到的郵件自動放入垃圾郵件的黑名單中學習。

  7、Exchange 日誌報告轉換：

  若收下的郵件為 Exchange 日誌，是否要將裡面的檔案拿出來分析。

- 【認證帳號】：用 IMAP/IMAPS 去收郵件時使用的認證帳號，例如，mail.archive@yourdomain.com。
- 【認證密碼】：IMAP/IMAPS 認證帳號使用的密碼，要確認輸入是否正確，可以點選顯示密碼，驗證輸入的密碼正確與否。
- 【重收所有郵件】：在 IMAP/IMAPS 郵件伺服器主機尚未刪除郵件前且系統重建下，可以用 IMAP 把郵件重新收下來。

5-5、轉移工具

郵件歸檔伺服器可以一次性的把所有的郵件轉移進來，使用的方式不外乎 POP3 跟 IMAP 協定，管理者設定要移轉的伺服器 IP 資訊後，匯入使用者帳號及密碼後一次性的轉移。

(一)、POP3 轉移

圖 5-14、POP3 郵件移轉

- 【郵件伺服器 IP 位址或域名】：POP3 的 IP 位址或是域名。（圖 5-14）
- 【郵件移轉使用的埠號】：POP3 的埠號，預設是 110。
- 【郵件伺服器使用的加密方式】：使用加密協議跟後端的郵件伺服器移轉郵件。
- 【過濾器】：代收下來的郵件要不要再經過郵件過濾器的過濾。
- 【Exchange 日誌報告轉換】：若收下的郵件為 Exchange 日誌，是否要將裡面的檔案拿出來分析。

(二)、IMAP 轉移

圖 5-15、IMAP 郵件移轉

- 【郵件伺服器 IP 位址或域名】：IMAP 的 IP 位址或是域名。（圖 5-15）
- 【郵件移轉使用的埠號】：IMAP 的埠號，預設是 143。
- 【郵件伺服器使用的加密方式】：使用加密協議跟後端的郵件伺服器移轉郵件，選擇自動偵測下，系統會自動偵測後端郵件伺服器使用 SSL、TLS 及憑證的狀態，並回應適當的數值給後端的伺服器。
- 【完整 E-mail 當認證帳號】：使用完整的郵件帳號當作認證的帳號，例如用 ma@herhsiang.com.tw 作為認證帳號。
- 【過濾器】：代收下來的郵件要不要再經過郵件過濾器的過濾。
- 【Exchange 日誌報告轉換】：若收下的郵件為 Exchange 日誌，是否要將裡面的檔案拿出來分析。

5-6、HERHSIANG Sync

郵件歸檔伺服器搭配 HERHSIANG Mail Server 時，可以簡化設定，自動把 Mail Server 的設定資料同步到歸檔伺服器中，解省管理者設定的時間。(圖 5-16)

圖 5-16、HERHSIANG Sync 設定

- 【名稱】：設定容易辨識的名稱。
- 【啟用開關】：要不要啟用他。
- 【伺服器】：郵件伺服器的網域名稱。
- 【伺服器管理介面埠號】：HERHSIANG 郵件伺服器管理介面的埠號，預設是 88 。
- 【連線逾時時間】：跟管理介面連線超過多長時間，就放棄這次連線。【伺服器管理帳號】：郵件伺服器的管理者帳號。
- 【密碼】：管理者帳號的密碼。
- 【檢查伺服器類型】：點選後，系統會自動會跟郵件伺服器溝通，並取得相關資訊。
- 【同步間隔時間】：每隔多久執行同步動作，預設 600 秒。
- 【日誌同步間隔時間】：每隔多久執行日誌同步動作，預設 1800 秒。

同步選項

共有網域、使用者、部門垃圾信信任 IP、系統黑白名單、個人黑白名單及郵件日誌等項目：（圖 5-17）

圖 5-17、HERHSIANG Sync 同步選項

5-7、雲端硬碟代收

郵件歸檔伺服器可以把郵件從舊的設備移轉進來，舊的設備可能是 HERHSIANG 的 Mail Server 、MA、具備郵件紀錄功能的 UTM 或是網路上任何一個儲存郵件的位置。

以 HERHSIANG Mail Server 為例。(圖 5-18)

圖 5-18、HERHSIANG Sync 設定

- 【裝置名稱】：設定容易辨識的名稱。
- 【啟用】：要不要啟用他。
- 【裝置類型】：有 4 個選項，分別是 Mail Server、MA、UTM 及其他。
- 【收取 HERHSIANG MS 垃圾郵件】：要不要把 Mail Servre 的垃圾郵件一併收過來。
- 【Exchange 日誌報告轉換】：若收下的郵件為 Exchange 日誌，是否要將裡面的檔案拿出來分析。

- 【連線方式】：跟儲存裝置的連線方式，有 SAMBA、FTP、SATA、USB 跟 iSCSI。
- 【遠端主機名稱或 IP】：IP 位址或是域名。
- 【遠端資料夾】：郵件存放的目錄。

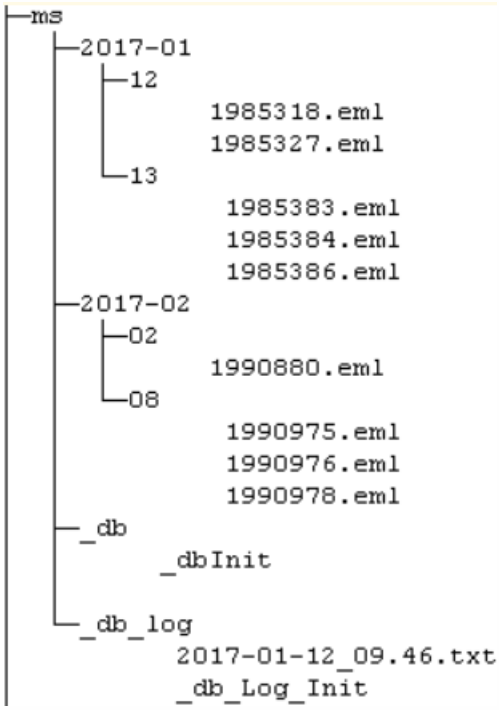
裝置類型的說明

HERHSIANG MS 系列：(MDS / MDispersion)

遠端資料夾下，需要包含 _db、_db_log 跟 {西元年分}-{月}/{日} 的資料夾，只會收取 {西元年分}-{月}/{日} 資料夾中的郵件；

如：遠端 "ms" 資料夾有 _db、_db_log 資料夾，及符合 {西元年分}-{月}/{日} 的 2017-01/12、2017-01/13、2017-02/02 和 2017-02/08 資料夾。

儲存郵件的結構如下：



*. _db_log 資料夾下的 {西元年分}-{月}-{日}_{小時}.{分鐘}.txt 檔案為非必須存在，但若設定 [收取 HERHSIANG MS 垃圾郵件] ，則需要從該檔案中判斷郵件是否為垃圾郵件。

HERHSIANG MA 系列：（MArchive）

遠端資料夾下，需要包含 {備份標記} 資料夾，該 {備份標記} 資料夾內還需要包含 {備份標記}.ini 檔案與 MRC_SAME/{西元年分}-{月}/{日} 資料夾，只會收取 MRC_SAME/{西元年分}-{月}/{日} 資料夾中的郵件，

如：遠端 "ma" 資料夾有符合 {備份標記} 的 q59ev2zg9b 和 y5x0afho0j 資料夾；

q59ev2zg9b 資料夾中也有符合 q59ev2zg9b 的 ini 檔案及符合 MRC_SAME/{西元年分}-{月}/{日} 的 MRC_SAME/2017-06/12 資料夾；

y5x0afho0j 資料夾中也有符合 y5x0afho0j 的 ini 檔案及符合 MRC_SAME/{西元年分}-{月}/{日} 的 MRC_SAME/2017-07/14、MRC_SAME/2017-07/15 資料夾。

儲存郵件的結構如下：

```
ma
  q59ev2zg9b
    q59ev2zg9b.ini
    MRC_SAME
      2017-06
        12
          000a8fe98aeabb598fe1d21a97455186.eml
          00e79fbfd17a528df671a57d271cfec6.eml
  y5x0afho0j
    y5x0afho0j.ini
    MRC_SAME
      2017-07
        14
          0a17eff3b924334f261e3ec0ea39e55a.eml
        15
          0a109e9a0943d0943b81c5b0378dd850.eml
          0b96ba4b35a4e90bcac688aaafdc182d.eml
```

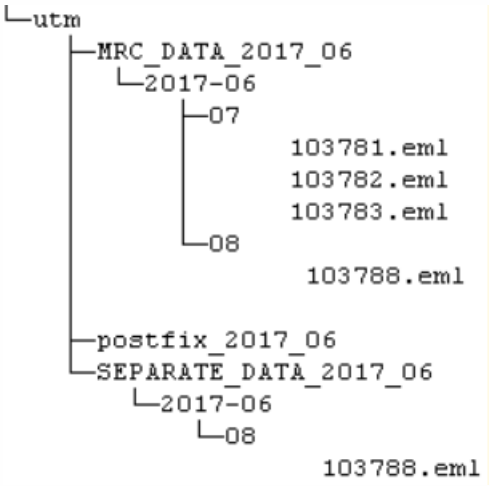
*. HERHSIANG MA 通常為加密後的郵件，若是使用其他的裝置類型收取，將因為無法解析正確的郵件內容而放棄收取郵件

HERHSIANG UTM 系列 :(UTM / NTS / NGS)

遠端資料夾下，需要包含 MRC_DATA_{西元年分}_{月}/{西元年分}-{月}/{日} 資料夾，只會收取 MRC_DATA_{西元年分}_{月}/{西元年分}-{月}/{日} 資料夾中的郵件；

如 : 遠端 "utm" 資料夾有符合 MRC_DATA_{西元年分}_{月}/{西元年分}-{月}/{日} 的 MRC_DATA_2017_06/2017-06/07 和 MRC_DATA_2017_06/2017-06/08 資料夾。

儲存郵件的結構如下：



*. SEPARATE_DATA_{西元年分}_{月}/{西元年分}-{月}/{日} 資料夾為非必須存在，但若有設定 [收取 HERHSIANG UTM 隔離郵件] ，則會從 SEPARATE_DATA_{西元年分}_{月}/{西元年分}-{月}/{日} 資料夾收取隔離郵件，

其他 : 將會收取遠端資料夾下所有郵件檔案

*. 收取郵件時，將只收取表頭內包含 date, from, to, subject, message-id, content-type, received 其中一個資訊的郵件

5-8、透通和閘道佇列列表

當郵件通過歸檔伺服器時，因為特殊原因，寄不出去，系統就會把這一些郵件放置在佇列中，這裡就定義佇列的重送機制。(圖 5-19)

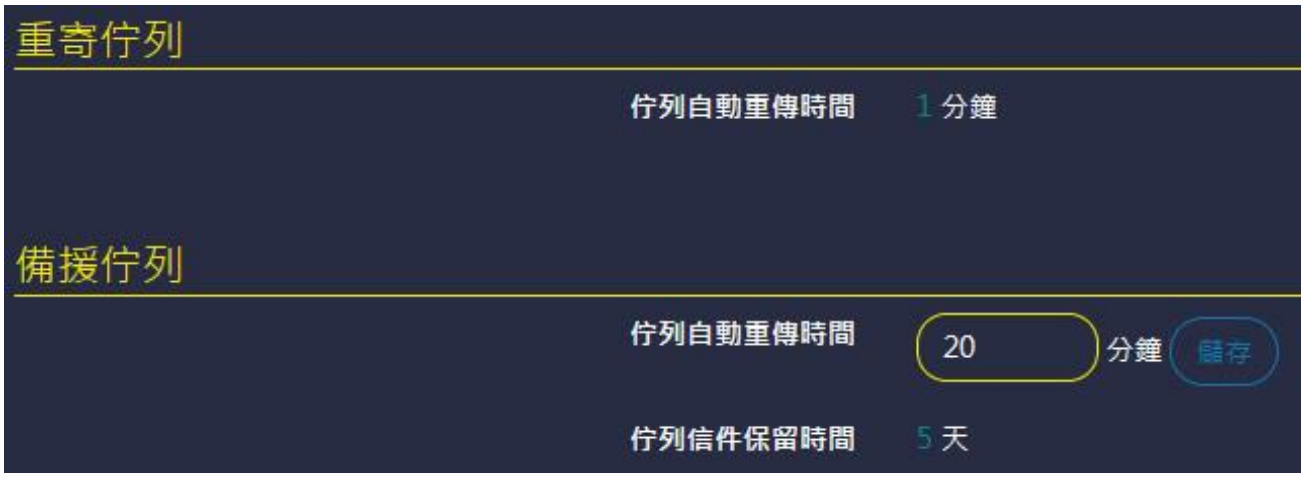


圖 5-19、郵件佇列設定

- 【佇列自動重送時間】：每隔多久自動重送佇列，預設是 20 分鐘。
- 【佇列郵件保留時間】：當超過 5 天的郵件仍然記不出去，系統就放棄重送。

第 6 章 認證與權限管理

郵件歸檔伺服器的驗證模式有三種，分別是本機帳號、跟原本郵件伺服器要求驗證或是跟 Gmail、Office 365 等認證入口網站驗證。驗證成功後才會讓使用者登入系統，同時執行管理者賦予的工作，除了本機帳號外，整個認證的示意圖如下，其中 mail.yourdomain.com 可能是自架的郵件伺服器、託管的郵件主機甚至跟 Gmail Office365 整合的認證機制。(圖 6-1)

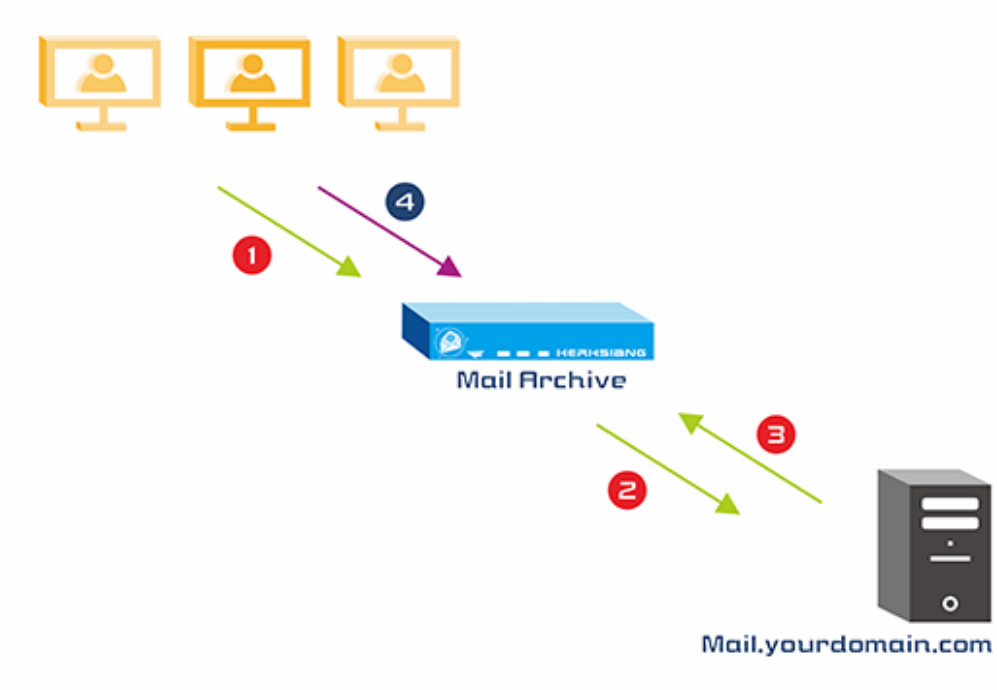


圖 6-1、驗證程序

首先使用者向郵件歸檔伺服器發出認證要求，系統根據使用者管理中的設定，向認證伺服器(可以是郵件伺服器也可以是 Gmail、Office 365 的認證主機)發出認證要求，使用的認證協定可以是 AD、POP3、IMAP、LDAP、Radius、Gmail OAuth 跟 Office365 OAuth 其中一種，當認證伺服器確認輸入的帳號跟密碼無誤後，郵件歸檔伺服器就會讓使用者登入系統。

認證的設定程序如下：

步驟一：建立網域要用的認證方式

郵件歸檔伺服器支援多網域，不同的網域使用不同的認證方法，例如，a.com 的網域使用 AD 伺服器驗證登入的使用者，b.com 的網域用 POP3 協定驗證登入的使用者。

步驟二：建立網域內使用者的角色及權限

並不是設定的網域內所有的帳號都能夠登入系統，管理者決定網域內的使用者哪一些帳號可以登入，登入後的角色扮演是管理者、查詢者、使用者這三種其中一種或是全部，他能執行的權限為何？

6-1、網域管理

不論是用 POP3 代收下的郵件或是透通模式攔截到的郵件，系統會自動根據網域內容分類，不同的網域使用不同的驗證伺服器，驗證方式可以是 AD、POP3、IMAP、LDAP、Radius Gmail OAuth 跟 Office365 OAuth 其中一種，每一個網域只可以設定一種驗證方式。

在【網域管理】就是建立網域跟認證伺服器之間的對應關係，當建立完成後，查詢者/使用者的登入帳號跟密碼就自動去跟認證伺服器驗證，這樣避免查詢者/使用者記住太多組帳號密碼。(圖 6-2)

圖 6-2、新增一筆新的網域

- 【名稱】：這個網域驗證一個容易記住的名稱，例如，herhsiang.com.tw。
- 【備註】：詳細的說明備註，例如，HERHSIANG 網域。
- 【登入】：要不要讓這網域的用戶可以登入。
- 【網域】：被記錄下來郵件的網域名稱，屬於這個網域的使用者，都會用這一個驗證模式，例如，herhsiang.com.tw。

- 【遠端帳號預設角色】：當網域的驗證方式設定成功後，在【使用者管理】中新增加使用者時預設的功能，有 3 種角色，分別是管理者、查詢者跟使用者，在角色扮演上說明上可以參考【使用者管理】。

  點選空白就可以選取，預設是使用者，也可以多選，這個地方只是預設角色，在建立每個帳號的【使用者管理】上，還可以針對每個新建帳號的角色再次分配，同時改變使用者的權限。

- 【驗證模式】：網域的使用者驗證，目前支援 7 種驗證模式，分別是 AD、POP3、IMAP、LDAP、Radius、Gmail OAuth 跟 Office365 OAuth，根據使用的網路環境挑選其中一種，一般來說，為了避免查詢者/使用者記住太多組帳號跟密碼，認證模式會選擇跟郵件伺服器的認證方式相同，例如，原本的郵件伺服器的帳號密碼是跟 AD 伺服器整合，此時就可以選擇 AD 伺服器，使用者要登入郵件歸檔伺服器的帳號跟密碼就跟登入郵件伺服器的一樣，都是向 AD 伺服器要求驗證。

  如果選用 Gmail OAuth 跟 Office365 OAuth 驗證，則要先到第 5-3 章中的 OAuth 驗證設定相關的資訊，底下是每個驗證機制需要設定的項目。

1、AD：

輸入 AD 伺服器的主機及網域名稱跟具有帳號查詢權限的管理者帳號及密碼，設定完成後可以點選 

的按鈕，驗證設定的資料是否正確，以下圖為例，遠端主機是 192.168.188.6，AD 的網域名稱是 herhsiang.com.tw，並以 Administrator 為登入查詢帳號。（圖 6-3）

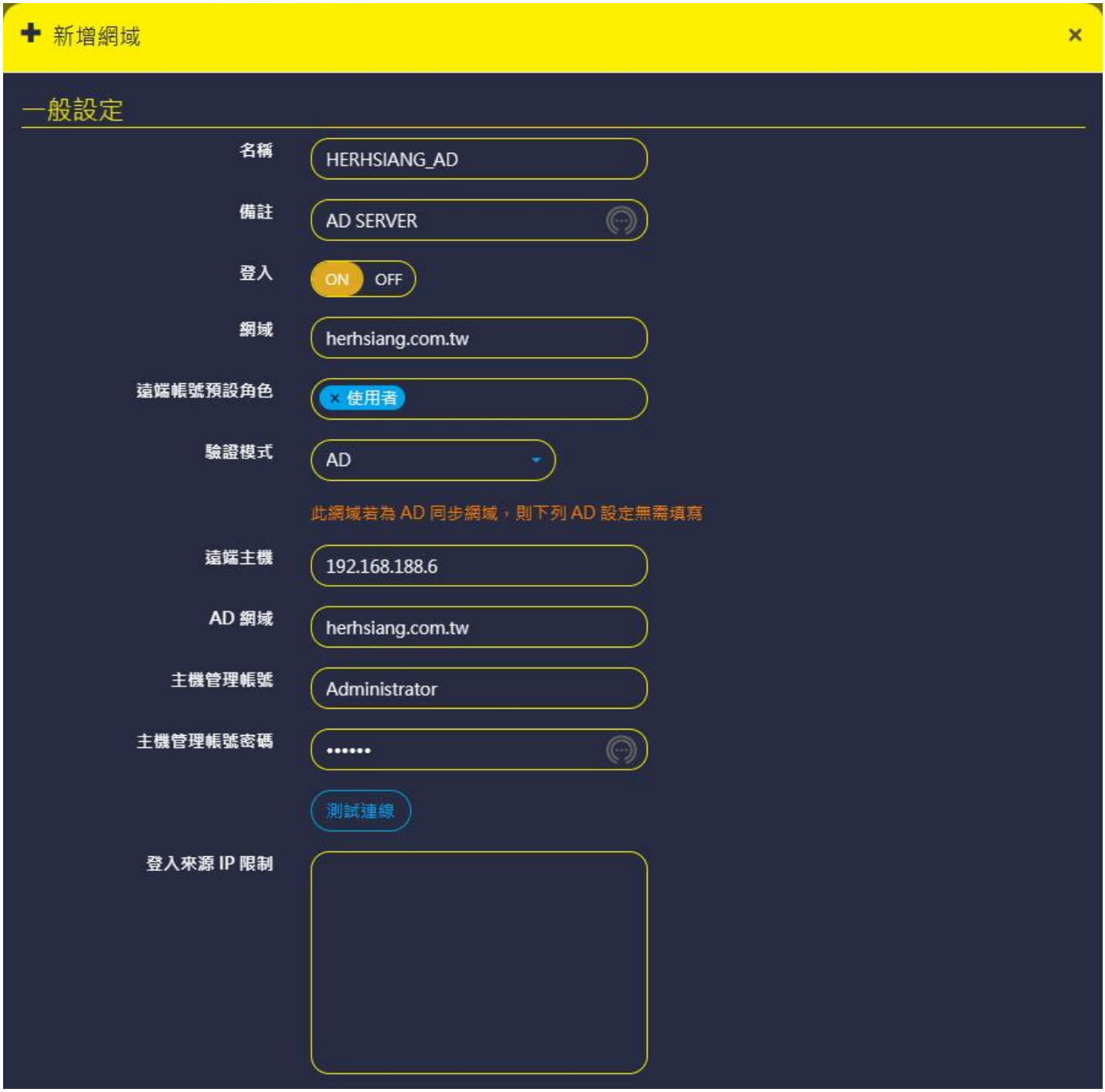


圖 6-3、AD 伺服器驗證設定

2、POP3：

選擇 POP3 驗證方式，就是希望登入帳號跟密碼是跟原本的郵件伺服器一樣，因此在設定區輸入 POP3 主機的 IP 位址或是網域名稱、埠號(預設是 110，如果有啟用 SSL 則是 995)、要不要用 SSL(POP3S)加密連線跟登入等待回應時間超過回應時間，驗證程序就會被中斷。為了安全因素，建議採用 POP3S 的驗證方式，設定完成後可以點選 測試連線 的按鈕，驗證設定的資料是否正確。（圖 6-4）

圖 6-4、POP3 驗證設定

3、IMAP：

選擇 IMAP 驗證方式，就是希望登入帳號跟密碼是跟原本的郵件伺服器一樣，輸入 IMAP 伺服器的 IP 位址或是網域名稱、Port 號(預設是 143)跟加密方式，IMAP 的加密方式共有 4 種，分別是自動、SSL、Start-TLS 跟自我簽署憑證等，為了安全因素，建議採用 IMAPS 的方式驗證帳號密碼，設定完成後可以點選 測試連線 的按鈕，驗證設定的資料是否正確。（圖 6-5）

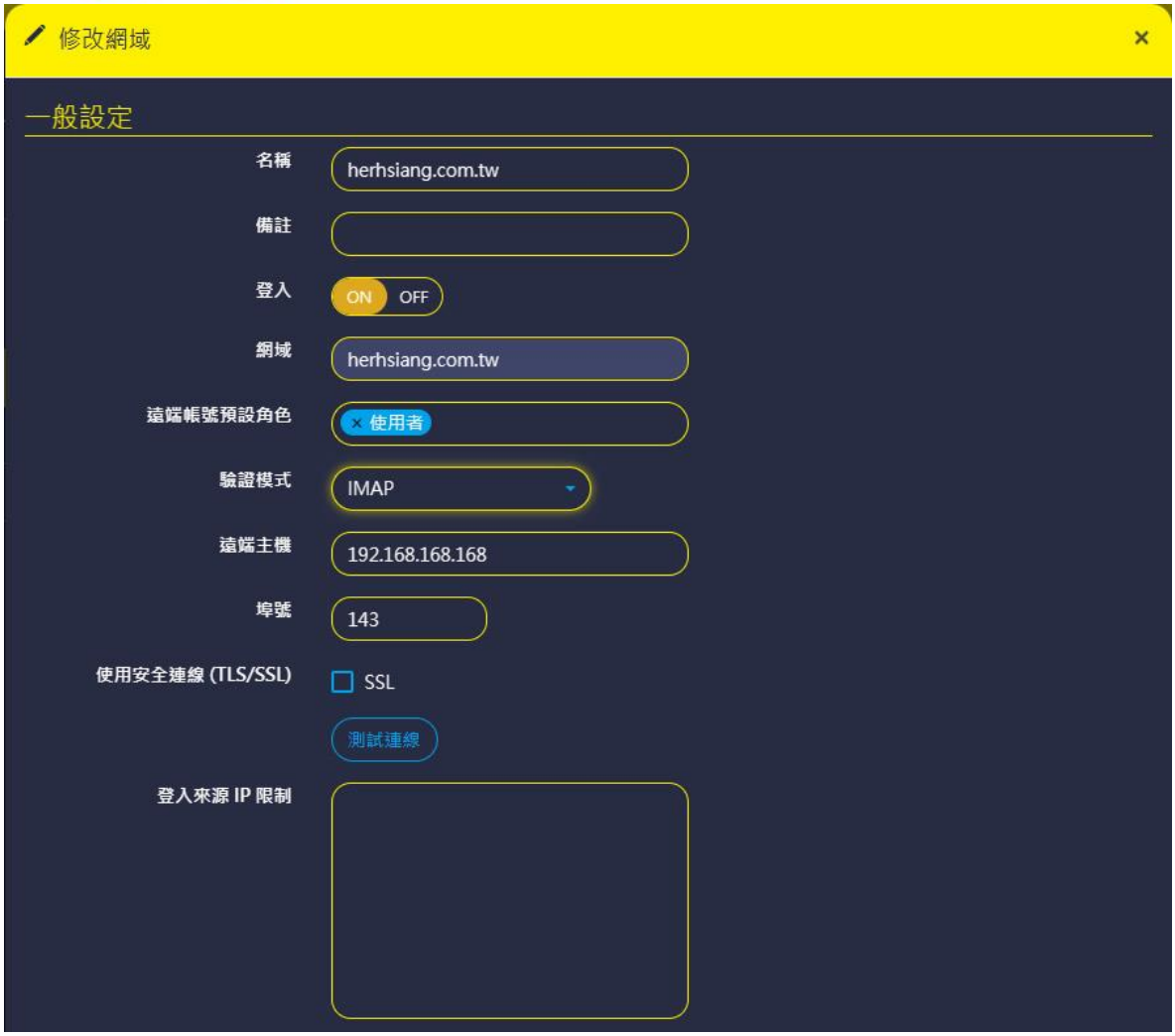


圖 6-5、IMAP 認證方式

4、LDAP：

輸入 LDAP 主機的 IP 位址或是網域名稱、LDAP 使用的 PORT(預設是 389) 號及 Ldap 帳號認證的 DN 是使用 UID 還是 CN，後面的 dc=herhsiang dc=com dc=tw 就是網域資訊，設定完成後可以點選 

的按鈕，驗證設定的資料是否正確。（圖 6-5）

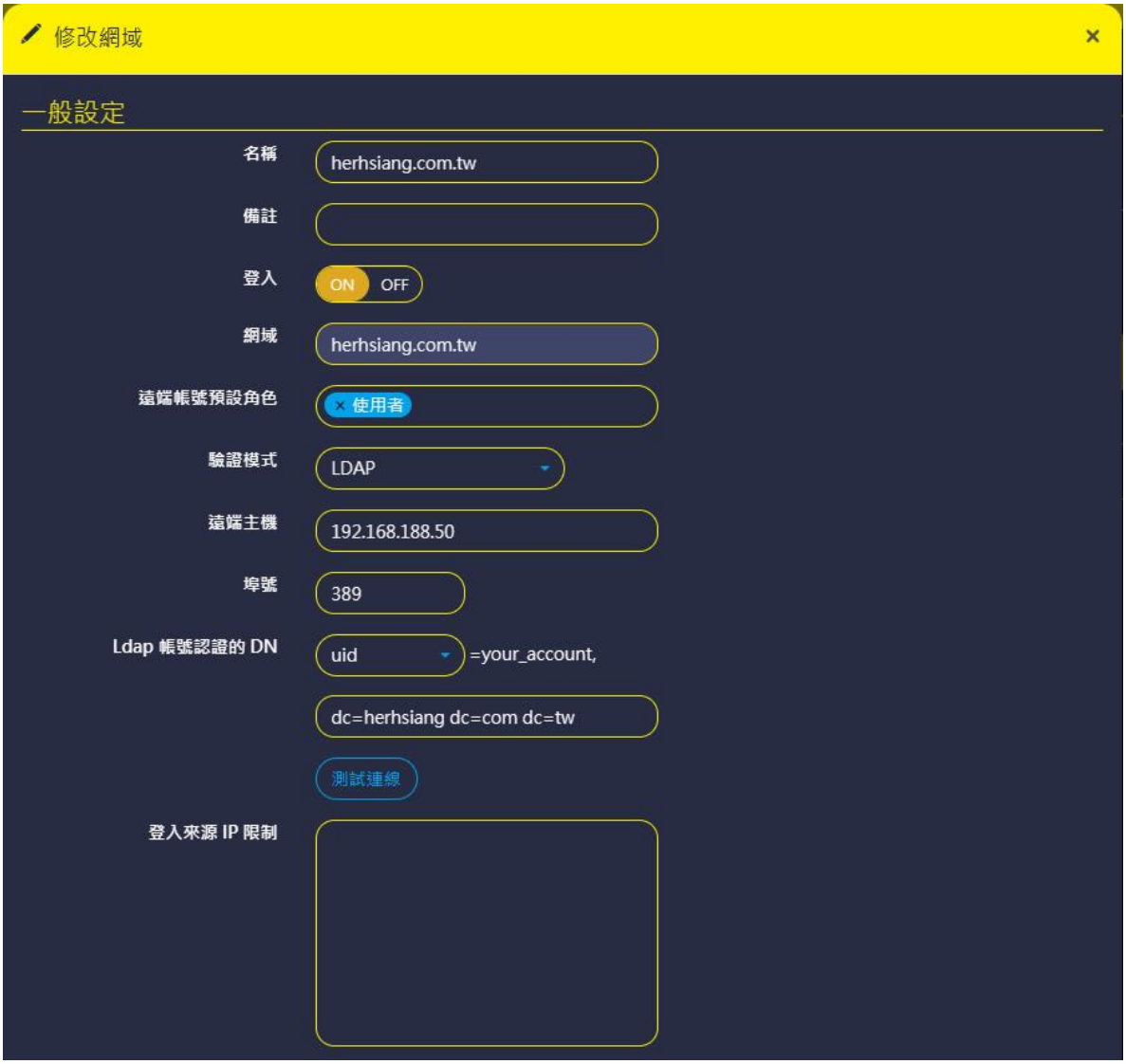


圖 6-6、LDAP 認證方式

5、Radius：

首先選擇驗證的方式是用 PAP 還是 CHAP，輸入 Radius 主機的 IP 位址或是網域名稱、使用的 Port 號(預設是 1812)、跟 Radius 伺服器連線時使用的密鑰、登入等待回應時間超過時間將會中斷這次的驗證及嘗試登入次數等，設定完成後可以點選 

的按鈕，驗證設定的資料是否正確。（圖 6-7）

圖 6-7、Radius 認證方式

6、Gmail OAuth 跟 Office365 OAuth 驗證：

驗證方式必須先到第 5-3 章中的 OAuth 驗證設定完成後才可以選用。

設定完成後可以按下 

按鈕，系統會自動檢查設定值是否正確。

- 【登入來源 IP 限制】：空白代表這個功能是關閉，代表任何來源 IP 位址都可以登入，只要有輸入一筆資料，代表這項限制功能啟用，此時這個網域的登入者如果不是使用設定的來源 IP 位址，將會被拒絕連線。設定值是每行一筆，可以多行，例如，192.168.168.254/24。

(一)、IMAP 郵件還原

當使用者更換電腦或是郵件伺服器換新，導致使用者的郵件通通不見，此時只要有 HERHSIANG 的郵件歸檔伺服器就放心，歸檔伺服器可以將郵件，塞回原本的郵件伺服器原帳號中，執行時光回朔器的功能。(圖 6-8)

圖 6-8、郵件還原

- 【使用 IMAP 驗證模式的設定】：利用 IMAP 的協定將郵件塞回原來的帳號。
- 【還原遠端主機】：輸入後端的郵件主機的 IP 位址或是網域名稱。
- 【埠號】：IMAP 的預設埠號是 143。
- 【加密方式】：選擇後端郵件伺服器的加密機制，如果不知道，就選自動。

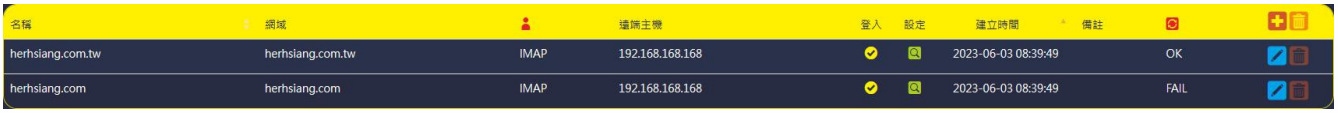
(二)、透通模式

- 【郵件伺服器備援】：啟用郵件伺服器備援功能。
- 【需備援的主機】：那一個郵件伺服器需要備援機制。

(三)、閘道模式

- 【閘道模式】：啟用郵件閘道器模式。
- 【完整 E-mail 當認證帳號】：使用完整的郵件帳號當作認證的帳號，例如用 ma@herhsiang.com.tw 作為認證帳號。
- 【內部郵件伺服器】：那一個郵件伺服器需要閘道模式，輸入域名。

不同的網域可以使用不同的驗證方式，這樣的優點是讓使用者記住一筆帳號密碼就可以，設定完成的資訊列表如下。(圖 6-9)



名稱	網域		遠端主機	登入	設定	建立時間	備註		
herhsiang.com.tw	herhsiang.com.tw	IMAP	192.168.168.168	✓		2023-06-03 08:39:49		OK	
herhsiang.com	herhsiang.com	IMAP	192.168.168.168	✓		2023-06-03 08:39:49		FAIL	

圖 6-9、認證方式列表

對於已經建立的認證機制，可以執行匯出動作，讓管理者可以保留這些詳細的資料，並且在日後系統重建時執行匯入認證機制的動作。

6-2、使用者管理

對於每一個要登入郵件歸檔伺服器的使用者來說，有 2 種方式，一種是本機帳號，另一個就是跟認證伺服器驗證的帳號，認證伺服器可以是郵件伺服器、LDAP、AD、Radius 伺服器或是 Gmail / Office365 入口整合帳號其中一種，關於認證伺服器的設定，參考第 5-1 章 認證管理。

在設定使用者之前，先了解關於帳號的限制跟角色扮演，帳號的來源有本機帳號跟網域帳號 2 種，帳號的來源是本機帳號時，只能執行管理者的角色而不能查詢任何網域的郵件，網域的帳號則沒有此限制，可以是管理者、查詢者或是使用者角色其中之一。

關於角色，郵件歸檔伺服器有 3 種不同的身分，每一個身分的權限都不一樣。

管理者

擁有這個權限的使用者只能登入郵件歸檔的管理者介面，設定整台或是部分功能及查詢郵件紀錄，但無法用這個帳號登入郵件內容查詢介面。

查詢者

這個帳號可以登入郵件內容查詢介面，執行管理者賦予的查詢郵件或是觀看轉寄郵件的權限，例如，全部網域或是指定的網域、使用者的郵件內容。

使用者

登入郵件內容介面後只能看自己帳號內的郵件。.

(一)、新增一筆管理者帳號

底下的範例將會新增一筆管理者的帳號。(圖 6-10)

圖 6-10、新增管理者帳號

- 【帳號類型】：這個帳號的認證來源是本機或是由網域的驗證伺服器提供，如果是本機則需要輸入帳號、密碼跟驗證密碼，如果由驗證伺服器提供，則選擇網域名稱。
- 【名稱】：帳號的名稱，例如，freedy 的帳號。
- 【備註】：關於這個帳號的詳細備註，例如，管理部楊先生。
- 【登入】：帳號是否具有登入使用者介面的權限，on 代表帳號可以登入使用者介面查詢屬於自己的郵件，off 則沒有登入的權限。
- 【角色】：在這個範例是管理者，如果是本機帳號，也只有管理者這個選項可以選擇，如果是經由驗證伺服器的網域帳號，角色可以多選。

- 【帳號】：登入系統的帳號，例如，freedy@herhsiang.com.tw。
- 【權限】：當角色選擇管理者能夠進入管理介面，管理介面有主選單跟很多子選單，管理者賦予的權限可以細到每個子選單的讀取或是修改。
- 【登入來源 IP 限制】：空白代表這個功能是關閉，代表任何來源 IP 位址都可以登入，只要有輸入一筆資料，代表這項限制功能啟用，此時管理者如果不是使用設定的來源 IP 位址，將會被拒絕連線。設定值是每行一筆，可以多行，例如，192.168.168.254/24。

(二)、新增一個查詢者帳號

底下的範例將會新增一筆查詢者的帳號，具有查詢者權限的帳號，除了可以查詢管理者賦予的網域或是部門內的郵件外，本身也是預設有使用者的權限。(圖 6-11)

圖 6-11、新增查詢者帳號

- 【帳號類型】：查詢者帳號必須由驗證伺服器提供，選擇網域名稱。
- 【名稱】：帳號的名稱，例如，sunny 的帳號。
- 【備註】：關於這個帳號的詳細備註，例如，管理部許小姐。
- 【登入】：帳號是否具有登入使用者介面的權限，on 代表帳號可以登入使用者介面查詢屬於自己的郵件，off 則沒有登入的權限。
- 【角色】：在這個範例是查詢者，角色可以多選，甚至選擇也是個管理者。
- 【帳號】：登入系統的帳號，例如，sunny@herhsiang.com.tw。
- 【登入來源 IP 限制】：空白代表這個功能是關閉，代表任何來源 IP 位址都可以登入，只要有輸入一筆資料，代表這項限制功能啟用，此時查詢者如果不是使用設定的來源 IP 位址，將會被拒絕連線。設定值是每行一筆，可以多行，例如，192.168.1.1/24。

- 【可查詢目標】：共有 3 種，無限制、網域跟帳號，無限制代表整台郵件歸檔伺服器內的所有被記錄的郵件都可以查詢跟觀看郵件內容，網域跟帳號都可以複選。
- 【允許存取的網域或帳號】：在【可查詢目標】決定網域或是帳號後，就會出現讓管理者選填，點選空白處就可以選擇或是直接輸入網域、帳號。
- 【帳號別名】：給查詢者一個別名帳號，可以隱匿真實的登入帳號。

(三)、新增一個使用者帳號

底下的範例將會新增一筆使用者的帳號。(圖 6-12)

圖 6-12、新增使用者帳號

- 【帳號類型】：查詢者帳號必須由驗證伺服器提供，選擇網域名稱。
- 【名稱】：帳號的名稱，例如，brendon 的帳號。
- 【備註】：關於這個帳號的詳細備註，例如，業務部鄭先生。
- 【啟用】：帳號是否具有登入使用者介面的權限，on 代表帳號可以登入使用者介面查詢屬於自己的郵件，off 則沒有登入的權限。
- 【角色】：在這個範例是使用者，角色可以複選，甚至選擇也是個管理者。
- 【帳號】：登入系統的帳號，例如，brendon@herhsiang.com.tw。
- 【登入來源 IP 限制】：空白代表這個功能是關閉，代表任何來源 IP 位址都可以登入，只要有輸入一筆資料，代表這項限制功能啟用，此時使用者如果不是使用設定的來源 IP 位址，將會被拒絕連線。設定值是每行一筆，可以多行，例如，192.168.168.254/24。

■ 【帳號別名】：給查詢者一個別名帳號，可以隱匿真實的登入帳號。

建立完成的使用者列表如下，管理者也可以對這些資料進行匯入、匯出等動作。(圖 6-13)

主機	名稱	帳號	登入	設定	建立時間	備註	
本機	admin	admin			2023-06-03 08:29:50		
herhsiang.com.tw	freedy	freedy@herhsiang.com.tw			2023-06-03 08:39:51		
herhsiang.com	freedy	freedy@herhsiang.com			2023-06-03 08:39:52		
herhsiang.com.tw	sunny	sunny@herhsiang.com.tw			2023-06-03 08:39:52		
herhsiang.com	sunny	sunny@herhsiang.com			2023-06-03 08:39:52		
herhsiang.com.tw	elain	elain@herhsiang.com.tw			2023-06-03 08:39:52		
herhsiang.com	elain	elain@herhsiang.com			2023-06-03 08:39:52		
herhsiang.com.tw	brendon	brendon@herhsiang.com.tw			2023-06-03 08:39:52		
herhsiang.com	brendon	brendon@herhsiang.com			2023-06-03 08:39:52		
herhsiang.com.tw	郵件歸檔寄信用	ma@herhsiang.com.tw			2023-06-04 21:10:33		

圖 6-13、使用者帳號列表

6-3、OAuth 認證

郵件歸檔伺服器可以跟 Gmail / Office365 等入口帳號整合，也就是使用者只要記住雲服務的帳號密碼就可以，當有使用者要求登入時，系統會自動去做後端的認證伺服器執行驗證工作。(圖 6-14-1，6-14-2)

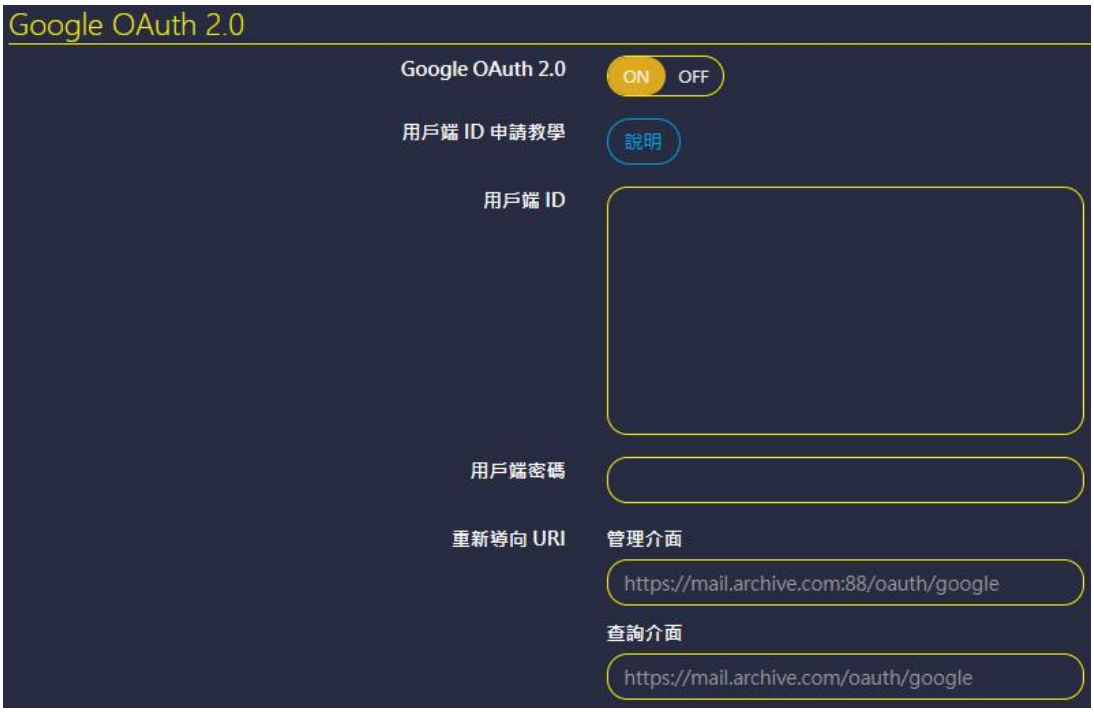


圖 6-14-1、Gmail 帳號整合

圖 6-14-2、Office365 帳號整合

(一)、Google oAuth 2.0

- 【用戶端 ID 申請教學】：點選說明的圖示，就有詳細的使用說明及網路連結，說明範例如下：（圖 6-15）

創建一個 Google API 控制台專案和用戶端 ID

您要整合 Google 登錄到你的網站之前，你必須擁有一個 Google API 控制台專案。在專案中，創建一個用戶端 ID，您需要呼叫登錄 API。

要創建一個 Google API 控制台專案和用戶端 ID，請按照下列步驟操作：

1. 進入Google API 控制台。
2. 從專案下拉列表中，選擇現有專案，或創建透過選擇創建一個新專案。
3. 在透過 "API 管理員" 的工具列，選擇憑證，然後選擇 OAuth 同意畫面。
   a. 選擇一個電子郵件地址，指定商品名稱，然後按儲存。
4. 在憑證選項，選擇建立憑證下拉列表，然後選擇 OAuth 用戶端 ID。
5. 在應用程式類型，選擇網路應用程式。
   a. 請輸入已授權的 JavaScript 來源或已授權的重新導向 URI，然後按建立。
6. 從返回的 OAuth 用戶端對話視窗，複製用戶端 ID。用戶端 ID 可以讓你的網站存取啟用後的 Google API。

圖 6-15、Gmail 帳號整合說明

- 【用戶 ID】：申請 Google oAtuh 服務時，Google 給的用戶 ID。
- 【用戶端密碼】：輸入 Google oAuth 的密碼。
- 【重新導向管理介面 URI】：具有管理權限的用戶 ID 在 Google 認證成功後，要轉向那一個 URI，一般會設定轉向郵件歸檔伺服器的管理介面。
- 【重新導向查詢介面 URI】：具有查詢者 / 使用者權限的用戶 ID 在 Google 認證成功後，要轉向那一個 URI，一般會轉向郵件歸檔伺服器的使用者介面。

(二)、Office 365 oAuth 2.0

- 【用戶端 ID 申請教學】：點選說明的圖示，就有詳細的使用說明及網路連結。（圖 6-16）

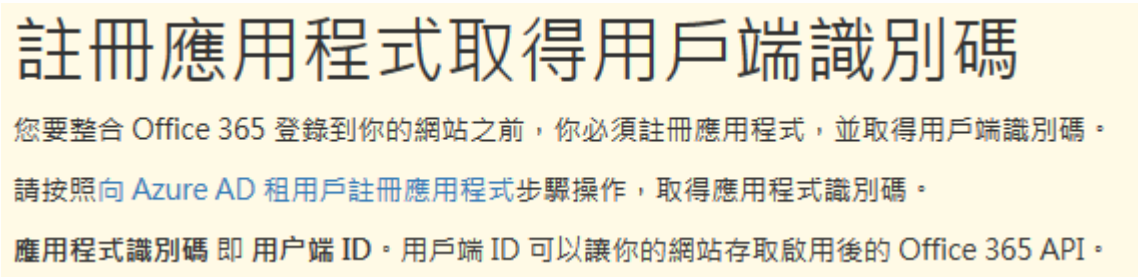


圖 6-16、Office 365 帳號整合說明

- 【用戶 ID】：申請 Office 365 oAtuh 服務時，Microsoft 給的用戶 ID。
- 【用戶端密碼】：輸入 Office 365 oAuth 的密碼。
- 【重新導向管理介面 URI】：具有管理權限的用戶 ID 在 Office 365 認證成功後，要轉向那一個 URI，一般會設定轉向郵件歸檔伺服器的管理介面。
- 【重新導向查詢介面 URI】：具有查詢者 / 使用者權限的用戶 ID 在 Office 365 認證成功後，要轉向那一個 URI，一般會轉向郵件歸檔伺服器的使用者介面。

6-4、部門管理

一般的郵件伺服器都有部門或是群組帳號的功能，可以用一個虛擬的帳號代表很多個實體帳號，例如，sales@a.com 是一個銷售部門的虛擬帳號，裡面的成員有 user1@a.com、user22@a.com ...，因此，寄給 sales@a.com 的郵件，裡面的成員(user1、user2 ..)都會收到相同的郵件。

郵件歸檔伺服器從網路上收下來的原始郵件收件者卻只有寄給 sales@a.com 的郵件，如果沒有開放使用者進入查詢介面，就沒有太大的差異，如果群組帳號的成員可以登入使用者介面，例如，user1@a.com 具有登入使用者介面查詢自己的郵件時，在沒建立群組帳號下，寄給 sales@a.com 的郵件不會被歸檔到 user1@a.com 中，為了解決這樣問題，管理者需要在【部門管理】，建立一份跟郵件伺服器一樣的部門或是群組帳號，讓郵件歸檔伺服器有依據可以將郵件歸檔到每一個使用者的信箱中。

AD 部門自動同步

在【網域管理】中驗證模式選擇【AD 伺服器驗證】的網域，在同步的過程中，會自動將 AD 伺服器裝的部門及部門成員帶給郵件歸檔伺服器，所以在這個驗證模式下，管理者不需要額外的設定，在【部門管理】中就會有這些資訊。

手動建立部門—架構說明

一個典型的部門或是群組帳號如下圖所示，網域內分 2 個部門，業務/工程，每一個部門有不同的成員，成員是可以跨部門，例如，freedy 就分屬 2 個群組。在業務部門中，他的虛擬帳號是 td@herhsiang.com.tw，當郵件歸檔伺服器紀錄下的郵件收件者有這個帳號，就根據設定，將此郵件類到部門成員中。(圖 6-17)

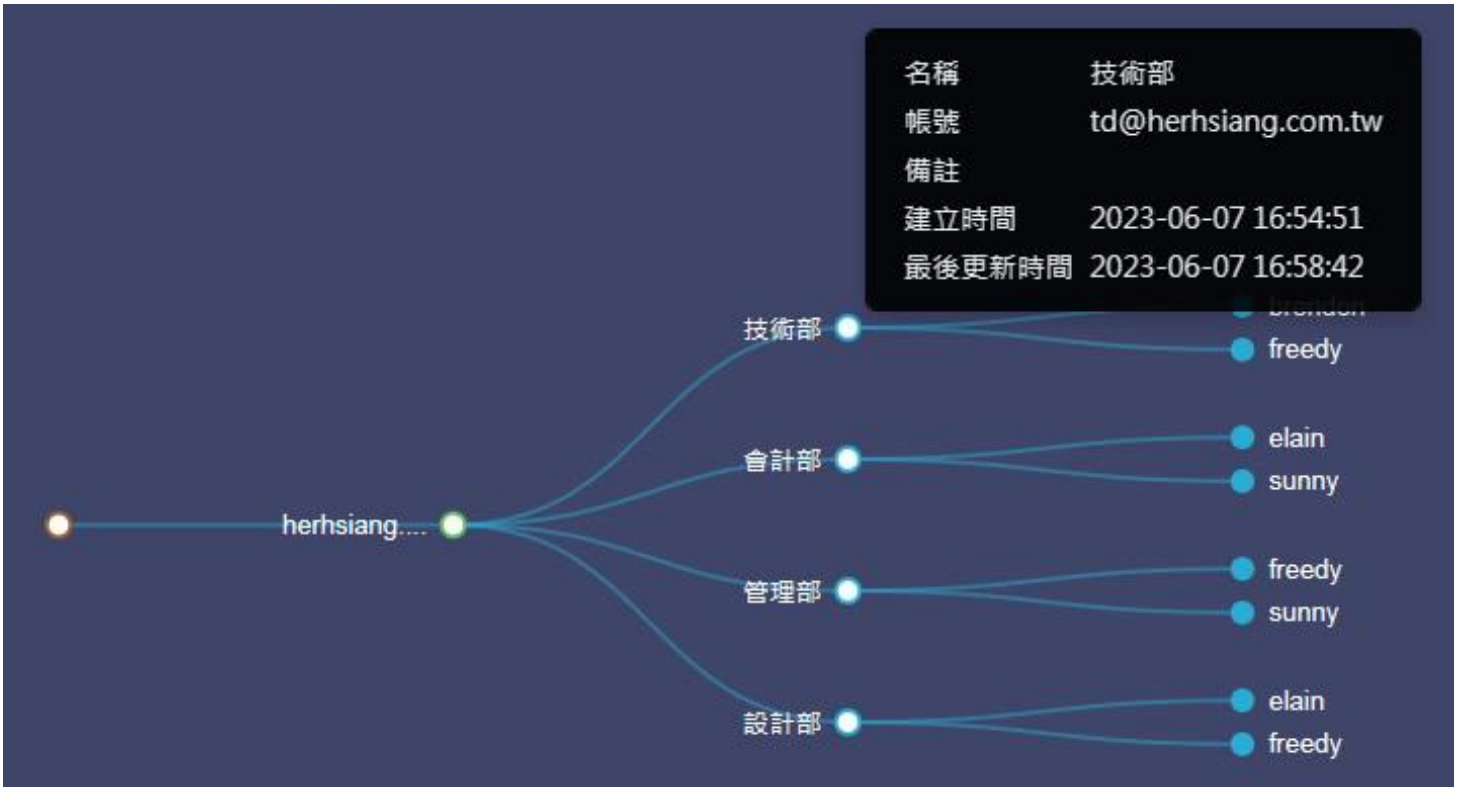

名稱 技術部
帳號 td@herhsiang.com.tw
備註
建立時間 2023-06-07 16:54:51
最後更新時間 2023-06-07 16:58:42
herhsiang....
技術部
會計部
管理部
設計部
freedy
elain
sunny
freedy
sunny
elain
freedy

圖 6-17、部門群組架構

手動建立部門—圖示說明

部門是用樹狀結構顯示，分成 2 種模式，本機跟 AD 同步，每一個節點的說明如下圖。(圖 6-18)

圖 6-18、部門成員圖示

手動建立部門—建立說明

點選要建立部門的節點後，可以用滑鼠右鍵開啟次選單，或是直接點選 

的選單後就可以開啟，在部門管理區，全面支援滑鼠右鍵的次選單功能，次選單的項目有新增部門、編輯部門跟刪除三種，當新增一個部門後，設定畫面如下。(圖 6-19)


新增部門
部門名稱
業務部
部門帳號
sales@herhsinag.com.tw
備註
業務部門帳號
部門成員
freedy@herhsiang.com.tw
sunny@herhsiang.com.tw
elain@herhsiang.com.tw
brendon@herhsiang.com.tw
確定
取消

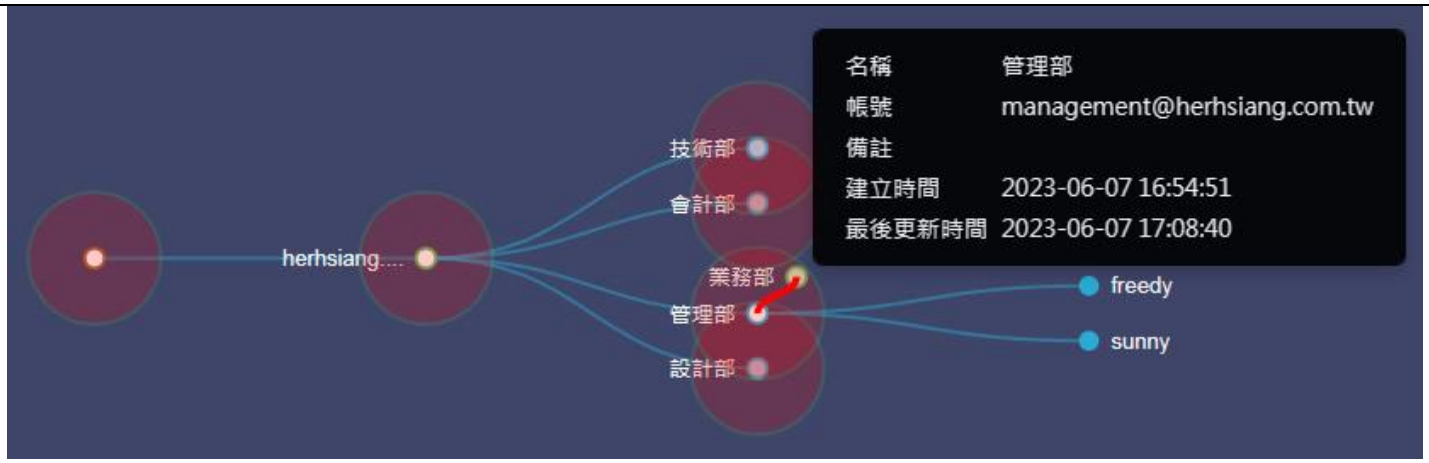
圖 6-19、部門建立

- 【部門名稱】：給一個容易辨識的名稱，例如，工程部。
- 【部門帳號】：輸入跟原本郵件伺服器相同的部門帳號或是虛擬帳號，例如，sales@herhsiang.com.com.tw 代表是工程部的部門帳號。
- 【備註】：輸入說明文字，例如，業務部的部門帳號。
- 【部門成員】：輸入這個部門的帳號，這些帳號是已經事先建立在【使用者管理】中。

手動建立部門—啟用拖曳

部門是用樹狀結構顯示，因此可以建立多層的部門架構，當管理者建立好部門及設定成員後，就可以選擇啟用拖曳機制，將部門或是成員用拖曳的方式改變樹狀結構。(圖 6-20)

拖曳中



拖曳結果

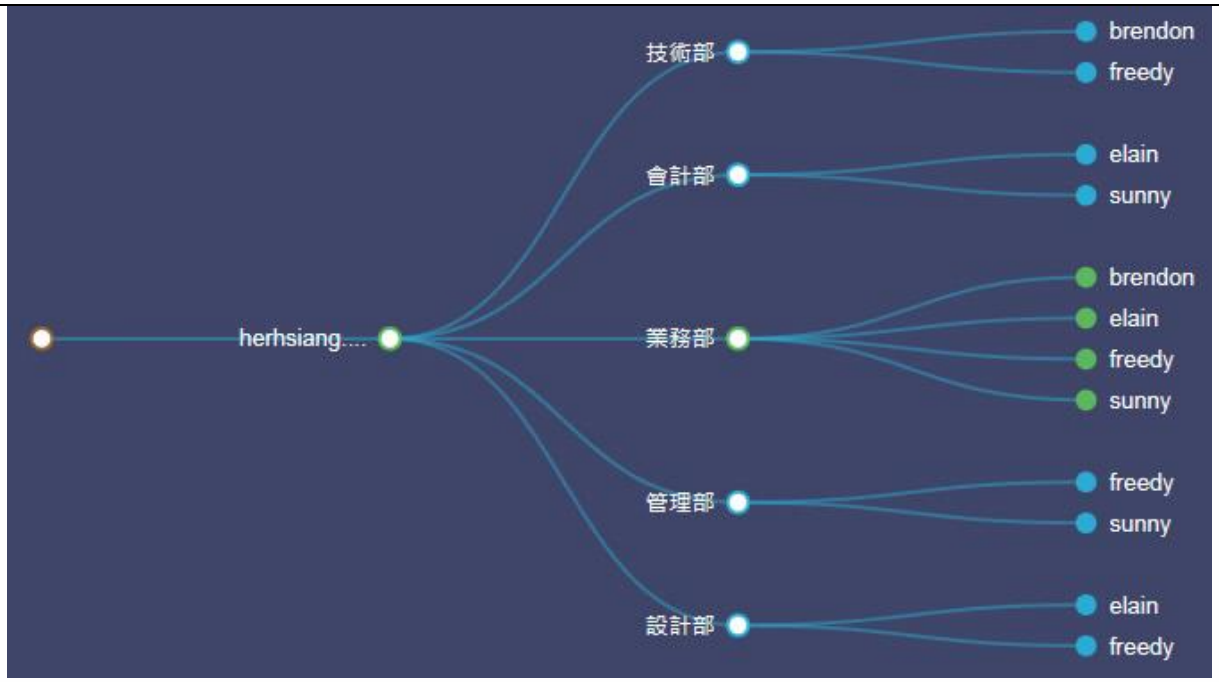


圖 6-20、拖曳功能

6-5、系統登入帳號及 IP 限制

要限制或是允許特定的帳號才能登入郵件歸檔伺服器的管理或是使用者介面，管理者有 2 種方式，一個是限制登入帳號或是允許特定的登入帳號，另一個是限制登入 IP 位址，不過使用上要特別注意，錯誤的設定會讓自己無法登入，2 種選擇其中之一設定。

(一)、系統登入帳號限制

設定限制帳號的模式有 2 種，一種是正向允許，另一個是負向拒絕，設定時務必小心設定的帳號，避免限制太多導致自己無法登入。

正向允許

選擇 僅允許符合下列設定之帳號 ，預設是空白，代表沒有限制，只要新增一筆，代表這個限制規則生效，管理者在設定時務必把自己的帳號設為第一筆，否則就無法登入管理介面，新增帳號後，則系統除了這些帳號外，拒絕其他任何帳號進入，就算在使用者管理中有設定登入的權限也無用。(圖 6-21)

圖 6-21、系統登入限制帳號設定

- 【名稱】：給一個容易辨識的名稱，例如，楊 OO。
- 【狀態】：要不要啟用這個帳號。
- 【帳號】：從已經建立的使用者列表中選擇帳號。

負向拒絕

選擇 僅拒絕符合下列設定之帳號 ，然後新增一個帳號，則系統除了這個帳號無法登入外，其他在使用者管理中設定的帳號都可以進入。

(二)、系統登入 IP 限制

設定限制登入 IP 位址的模式有 2 種，一種是正向允許，另一個是負向拒絕，設定時務必小心設定 IP 範圍，避免限制太多導致自己無法登入，2 種選擇其中之一設定。

正向允許

選擇 僅允許符合下列設定之 IP ，預設是空白，代表沒有限制，只要新增一筆，代表這個限制規則生效，管理者在設定時務必把自己的 IP 設為第一筆，否則就無法登入管理介面，新增 IP 位址或是範圍後，系統除了這些 IP 位址及區段外，拒絕其他任何 IP 位址登入，使用前必須確認允許登入的 IP 位址都有填入，否則會造成無法登入系統現象。(圖 6-22)

圖 6-22、系統登入限制 IP 設定

- 【名稱】：給一個容易辨識的名稱，例如，IP 位址。
- 【狀態】：要不要啟用這個 IP 位址或範圍限制。
- 【網路/遮罩】：輸入 IP 位址及範圍。

負向拒絕

選擇 僅拒絕符合下列設定之 IP ，然後新增一個 IP 位址或是範圍，則系統會拒絕這些 IP 位址或是範圍的登入需求，其他的 IP 位址跟範圍都可以進入。

第 7 章 郵件稽核及防護

郵件歸檔伺服器的稽核及防護功能，共分 2 大部分，一個是稽核過濾器另一個是郵件防火牆，詳細說明如下：

稽核過濾器

稽核過濾器是針對進出的郵件進行比對，比對項目除了寄件者、收件者外，內文，附件大小或是類型等也可以是比對條件，當發現符合比對規則的郵件後，系統可以做一些處置，讓郵件的運作規則更符合企業內部的管理需求，共有 4 種處置方式，表列如下：

處置一：

將郵件攔下來並轉給稽核人員，由稽核人員決定這一封郵件要不要放行。

處置二：

決定這類型的郵件要不要進入歸檔程序。

處置三：

要不要將此封郵件抄送給相關人員，例如，把寄給 brendon@herhsiang.com.tw 的郵件通通複製一份給 freedy@herhsiang.com.tw。

處置四：

針對符合過濾器的郵件進行垃圾郵件處理程序，例如，加、減權重，轉入隔離區等。

稽核過濾器的設定是一個相當複雜的機制，有很多的比對項目，因此在介面的設計上，預設只會出現基本項目的比對，如果不足，管理者可再開啟進階選項，滿足條件比對上的要求。

每一條稽核過濾器基本上由 3 個部分組合而成，稽核過濾器運作時間、郵件比對規則跟處置動作，在過濾器章節會詳細介紹。

郵件防火牆

寄信的動作都是用 SMTP 協定，一般的郵件主機會要求寄件者寄信時輸入密碼，確保寄件者是授權的用戶，沒有 SMTP 認證要求的郵件主機很容易就變成垃圾信的跳板。就算是有 SMTP 認證的郵件主機，有心人還是可以用嘗試錯誤法測試帳號的密碼，因此郵件防火牆的功能就可以提供後端的郵件伺服器這方面的保護，不論是要猜測密碼、寄件者跟驗證帳號不符合及短時間內重複內容的寄信或是大量寄信，通通可以保護。

7-1、過濾器

(一)、過濾器運作時間

設定郵件過濾器運作的時間跟名稱等基本資訊。(圖 7-1)

圖 7-1、過濾器的基本設定

- 【過濾器名稱】：給一個容易辨識的名稱，例如，過濾_test。
- 【啟用開關】：要不要啟用這個過濾器。
- 【備註】：過濾器的詳細說明及備註。
- 【執行時間】：過濾條件生效的時間，有 3 個選項分別是永久有效、每周執行或是指定的時間範圍內生效，以指定時間執行為範例，管理者除了指定開始時間跟結束時間外，當時間到期後，還可以決定要不要自動刪除這一條過濾條件。

(二)、郵件比對規則

設定規則及特定字元如下：

1、標示【*】的條件可以輸入特殊定義字，特殊字元包含【！】、【null】及【，】三個，其中【！】表示【非】的意思、【null】表示【沒有】，多個條件可以用【，】的符號隔闔，它代表【OR】的邏輯。

範例一：

主旨輸入【null】字元，表示當郵件沒有主旨文字時、

範例二：

來源 IP 輸入【！192.168.1.】表示寄件者來源不是介於 192.168.1.0~192.168.1.255 之間。

範例三：

在過濾條件《寄件人包含》中設定[@yourdomain.com,sales@mydomain.com]，就代表寄件者是 yourdomain.com 的任何一個帳號，或是 sales@mydomain.com 的帳號，都符合《寄件人包含》這個過濾條件。

2、勾選【不包含】代表除了設定值以外的都符合，例如，將設定過濾條件設為空白，並勾選【不包含】，代表這項設定值只要有任何數值，都符合過濾條件。

3、勾選【內部網域】代表透通模式下的網域設定上的所有網域名稱，此時，設定畫面就會變成灰色，管理者無法自行輸入。

基本設定區如（圖 7-2）

圖 7-2、過濾器的基本設定

- 【過濾條件組合方式】：以（AND）或是（OR）的邏輯來決定下面設定的過濾條件是不是全部要符合或是只要有一項符合就有效，以（AND）來說，所有的比對規則必須全部符合才會滿足設定條件，以（OR）來說，所有的比對規則只要有一個比對成功就符合設定條件。

★ AND 設定範例

在【過濾條件組合方式】選(AND)，同時在過濾條件《寄件人包含》中設定[@yourdomain.com]及《郵件主旨包含》中設定[報價單]，這 2 項比對條件，其他比對條件都是空白，它代表從 yourdomain.com 中的任何一個帳號往外寄信時，且郵件的主旨有包含[報價單]這 3 個字，這個過濾器的條件才會成立。

★ OR 設定範例

在【過濾條件組合方式】選(OR)，同時在過濾條件《寄件人包含》中設定[@domain.com]，並在《郵件主旨包含》中設定[報價單]，它就代表從 domain.com 中任何一個帳號寄信，或是 經過郵件歸檔伺服器的傳送、接收郵件(不一定是@domain.com 的帳號)的郵件主旨有[報價單]這 3 個字，這個過濾器的條件就會成立。

- 【寄件者包含】：加入要過濾的寄件者 E-Mail 位址就可以，這裡所指的寄件者不光是內部網域的帳號，外部郵箱寄給內部網域的信，《外部郵箱》就代表是寄件者。

  例如：abc@google.com 寄給 sales@yourdomain.com ，abc@google.com 就是寄件者。勾選內部網域時，所有在網域管理中的網域名稱都符合條件。

- 【收件者包含】：加上要過濾的收件者 E-Mail 位址就可以，這裡所指的收件者不光是內部網域的帳號，內部網域寄給外部郵箱的信，《外部郵箱》就代表是收件者。

  例如：sales@yourdomain.com 寄給 abc@google.com，abc@google.com 就是收件者。當勾選所有收件者符合時，只有郵件的收件者有郵件帳號，就符合條件，同樣勾選內部網域時，所有在網域管理中的網域名稱都符合條件。

進階設定區

- 【內文寄件者包含】：加入要過濾的內文寄件者 E-Mail 位址就可以，一般的郵件內文寄件者跟郵件表頭上的寄件者是同一筆帳號，因為某些偽裝寄件者的因素，使用者在寄信時可以將 2 個設成不一樣的，這樣的技巧通常會用在寄發垃圾郵件的上。

  選擇同寄件者代表郵件表頭的寄件者跟實際內文的寄件者必須一致才能符合條件，選擇同網域代表網域相同就符合過濾條件。

- 【通聯寄件者與內文寄件者不同】：通聯寄件者跟內文寄件者不同時，要不要當成一個過濾條件，關閉，代表 2 個要相同才會滿足過濾條件。
- 【寄件者偽造內部網域】：寄件者偽造網域名稱與郵件歸檔伺服器在透通模式下的內部的郵件伺服器相同時，滿足過濾條件，因為一般垃圾郵件過濾機制對內部的郵件通常比較寬鬆，不會被判斷成垃圾郵件，這也是廣告信業者常用的發信方法。

  勾選項目可以選擇他是偽造通聯寄件者還是內文寄件者。
- 【寄件者來源 IP 位址包含】：填入 IP 位址，所有從這些 IP 位址，寄的郵件都符合過濾器設定條件，支援 IPV4 跟 IPV6 2 種輸入。
- 【郵件表頭包含】：填入要過濾的郵件表頭內容。
- 【郵件主旨包含】：填入要過濾的郵件主旨，例如（報價單），則所有外寄、內送的郵件主旨出現這 3 個字就符合過濾規則，不論它原來的主旨是（新聞報價單據）或是（報價單單是一個笑話），都是符合的。
- 【郵件內容包含】：填入要過濾的郵件內容，例如（最新設計圖）字樣，如果內容有含這些文字就符合過濾器設定條件，郵件內容是郵件的本文，不包含郵件所夾帶的檔案，郵件夾帶檔案的內容無法用這個功能判斷，目前只能用整封郵件的大小及郵件附件檔名作為判斷依據。
- 【郵件容量介於】：郵件容量介於多少 Bytes，包含所夾帶的檔案，就符合過濾器設定條件，通常郵件的容量大小是整封郵件的原始格式的大小，預設 0 代表不限制。
- 【郵件附件檔名包含】：郵件附件檔名可以含有特定字元，例如，（MArchive 報價單），也就是所有的郵件，只要附帶檔案的檔案名稱有（報價單），就符合過濾器設定條件，不論是（2023_Marchive_最新報價單.DOC）或是（MArchive 報價單據.pdf）。
- 【郵件附件大小介於】：郵件的所有附件檔案介於多少 Bytes，就符合過濾器設定條件，預設 0 代表不限制。
- 【郵件方向】：在閘道器模式下，郵件是往內部寄還是由內部往外寄出，可以單選也可以複選。

進階設定區—個資

- 【個資】：郵件內文或是附件檔中含有特定的個資資訊，如、身分證號碼、出生日期、電話號碼、行動電話號碼、信用卡卡號及電子郵件等，當加權分數大於 1 時，就滿足觸發條件。（圖 7-3）

圖 7-3、過濾器的個資設定

個資觸發條件是以權重分數計算，以身分證為例，當整封郵件找到的身分證格式的資料共幾筆，將筆數除以權重，就是權重分數，再把所有有勾選的權重分數加起來，大於 1，就滿足觸發條件。資料的格式都是台灣地區慣用的格式，例如，身分證是 E121212121，第一個數字是英文，後面 9 碼是數字，以簡單的運算式說明如下：

身分證加權分數 =找到的身分證筆數 / 權重

加權分數 = 身分證加權分數 + 出生日期加權分數 +...

正規表達式，管理者也可直接用正規表達式，滿足這些過濾條件。

(三)、處置動作

對於符合過濾條件的郵件，共有四種處置方式

處置一：

轉給稽核人員，由稽核人員決定這一封郵件要不要放行。

處置二：

決定這類型的郵件要不要進入歸檔程序。

處置三：

處置動作進階設定--副本抄送給相關人員。

處置四：

處置動作進階設定--進行垃圾郵件的處理程序。

在處置動作中，三跟四是屬於進階設定，只適用在閘道器模式下，POP3 代收的郵件並不適用，底下是 4 種方式的詳細說明：

處置一、轉給稽核人員

這個處置適用於閘道器模式，在 POP3 代收的模式並不合適，運作原理是從郵件伺服器外寄的郵件一旦符合過濾條件時，會自動將郵件放在佇列中不會放行，同時寄發通知信給稽核人員，稽核者針對此郵件可進行下載、放行、延遲、刪除、退回等動作。(圖 7-4)

■

圖 7-4、轉給稽核人員處置

- 【稽核人員】：在閘道器模式下，攔下來的郵件要轉給哪一個稽核人員處理後續郵件的動作，可輸入多筆郵件帳號，每一行一個郵件帳號，這些郵件帳號都會收到相同的稽核通知信，稽核人員對這封郵件具有查看郵件內容、放行、延遲或是退回等權限。
- 【代理稽核人員】：當主要稽核人員在設定時間內未處理時，系統會自動將稽核通知信轉送給代理稽核人員處理，可輸入多筆郵件帳號。
- 【稽核信主旨】：發出稽核通知郵件時，郵件的主旨，例如，稽核郵件。

稽核人員收到稽核郵件時，根據郵件的內容有 5 種方式處理郵件：

1、下載：把郵件下載後，瀏覽郵件內容。

2、放行：郵件直接放行，寄送出去。

3、延遲：會依系統設定延遲時間寄出，例如：系統設定時間為 11 點，則所有被列為延遲郵件都會到每日 11 點才會寄出。

4、刪除：直接將郵件刪除，不允許寄送。

5、退回：將郵件退回原寄件者，原寄件者會收到一封退回的郵件。

處置二、不要進入歸檔

符合過濾規則的郵件，就不進行郵件歸檔動作，日後只能查詢郵件通聯紀錄而不會有這一筆的內容紀錄。

- 【停止處理更多規則】：當觸發過濾規則並執行處置動作後，這些符合規則的郵件要不要再繼續比對其他的過濾器，預設是關閉，如果管理者設定 10 條過濾器規則，則會從第 1 條一直比對到最後一條，只要有符合，就會進行處置動作。

  範例一

  過濾器 1，寄件者 sales@yourdomain.com 處置動作，轉給稽核人員。

  過濾器 10，寄件者 sales@yourdomain.com 處置動作，抄送副本給 zzz@yourdomain.com。

  結果：sales@yourdomain.com 轉給稽核人員且抄送副本給 zzz@yourdomain.com。

  範例二

  過濾器 1，寄件者 sales@yourdomain.com 處置動作，轉給稽核人員，啟用【停止處理更多規則】。

  過濾器 10，寄件者 sales@yourdomain.com 處置動作，抄送副本給 zzz@yourdomain.com。

  結果：sales@yourdomain.com 轉給稽核人員。

處置三、副本抄送給相關人員

針對符合過濾條件的郵件，將這封郵件轉寄給特定的收件者，不論是外部寄給內部、內部互寄、內部寄給外部的所有郵件，統統會轉寄，連同夾帶的檔案也會一併轉寄，不論原本的收件者或是寄件者都不會察覺這一封郵件已經被轉寄。(圖 7-5)

圖 7-5-1、抄送副本

圖 7-5-2、通知收件者信件以被轉寄

- 【收件者】：符合過濾器的郵件，要轉寄給特定的收信者，例如，過濾器設定只要寄件者是 sales@yourdomain.com 就符合條件，這個地方將收件者設為 zzz@yourdomain.com，則只要 sales@yourdomain.com 有寄出郵件，zzz@yourdomain.com 就會收到一封相同的郵件。

- 【主旨提示文字】：轉寄時，郵件歸檔伺服器會發出通知信時，郵件的主旨，例如，來自 sales@yourdomain.com 的信。
- 【通知寄件者】：符合過濾器的郵件，被轉寄給特定的收信者後，要不要讓寄件者知道，郵件有被轉寄，例如，過濾器設定只要寄件者是 sales@yourdomain.com 就符合條件，並把郵件轉寄給 zzz@yourdomain.com，啟用後，系統會再寄一封通知信給 sales@yourdomain.com，通知他郵件被轉寄給 zzz@yourdomain.com 。

  這個機制預設是關閉。
- 【通知信的收件者】：啟用【通知寄件者】功能後，符合過濾器的郵件通知哪一些寄件者，郵件已被轉寄，通常是原本的郵件寄件者。
- 【通知信的主旨】：寄發通知信時，郵件的主旨，例如，你的信被轉寄給 zzz@yourdomain.com。

處置四、垃圾郵件的處理

針對符合過濾條件的郵件，要不要再進行垃圾郵件過濾或是把它直接放到隔離區中。(圖 7-6)

圖 7-6、過濾器進階處理

- 【忽略垃圾信掃描】：符合過濾器條件的郵件，要不要再進入垃圾郵件過濾機制，預設是關閉，所以過濾完還是會進入垃圾信過濾。
- 【增減垃圾郵件分數】：當【忽略垃圾信掃描】被關閉後，符合過濾器的郵件會再進入垃圾郵件過濾，此時要對這類型的郵件增/減分數，預設是 0。
- 【直接轉到隔離區】：符合過濾器條件的郵件，要不要直接到垃圾郵件的隔離區。
- 【直接刪除】：直接刪除符合過濾器條件的郵件，當啟用直接刪除後，【直接轉到隔離區】的功能就會自動關閉。
- 【封鎖寄件者 IP 位址】：管理者認為寄件者的來源 IP 位址有高度危害，直接要郵件歸檔伺服器直接封鎖寄件者的來源 IP 位址。

■ 【移除過濾郵件中的附件】：符合過濾器條件的郵件，移除附件後傳給收信者。

建立完成的過濾條件會列表出如下，管理者可以調整優先權的順序，改變郵件過濾器的比對先後順序。(圖 7-7)

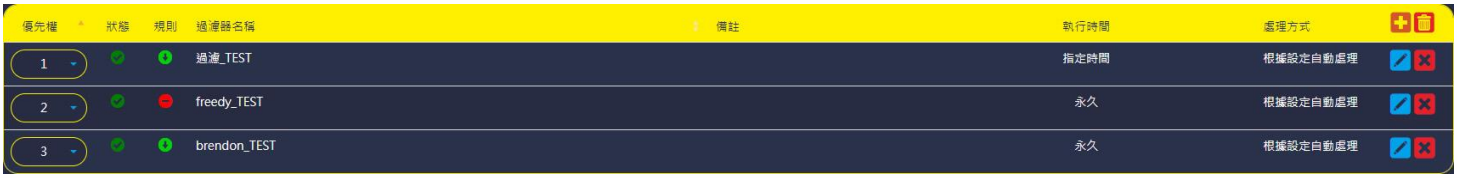


圖 7-7、過濾器順序

7-2、進階設定

符合過濾器的郵件在轉給稽核人員處理後，稽核人員多久時間沒回應或是處理，系統會自動轉給代理人員處理，當稽核郵件都沒有人處理，過期的郵件該如何處理，這裡都有詳細的設定，整個流程如下：

稽核郵件 ➔ 主要稽核人員 (沒處理) ➔ 代理稽核人員 (逾時沒處理) ➔ 退回或是刪除。(圖 7-8-1)

圖 7-8-1、被稽核郵件的進階設定

- 【每隔多久寄送稽核通知信】：當有符合稽核條件的郵件，系統會在設定時間寄一封稽核通知郵件給稽核人員，通知郵件的時間設定格式為 天(d)/小時(h)/分，其中 d 及 h 分別是 day 跟 hour 的代表符號，例如，5h/30，代表每 5 小時 30 分會寄一封通知信。
- 【主稽核人員未回應，轉寄給代理人員】：系統寄稽核郵件通知信給主要稽核人員，在設定的時間內，主要稽核人員並沒有對這一封稽核信內的郵件進行處置，超過設定的時間後，會自動再發一封稽核通知信給代理稽核人員。設定的時間單位是分鐘，預設為 60 分鐘。
- 【稽核郵件保存期限】：主要的稽核人員跟代理稽核人員都未處理稽核通知信內的郵件，被稽核的郵件在系統中保存超過設定的時間，就稱為過期的稽核郵件，時間單位是小時，預設為 24 小時。

- 【過期的稽核郵件處理方式】：超過 【稽核郵件保存期限】時間的過期稽核郵件該如何處理 ？ 共有 3 種處置方式：

  1、退回原寄件者

  被稽核的郵件無法順利寄出，退回給原寄件者，原寄件者會收到被稽核機制退回通知郵件。

  2、自動放行

  被稽核的郵件自動放行，郵件可以順利寄出。

  3、刪除該郵件

  被稽核郵件無法寄出，系統會刪除這封郵件，原寄件者會收到被稽核機制刪除通知郵件。'

- 【過期的稽核郵件是否歸檔】：過期的稽核郵件因為未完成寄信動作，要不要歸檔保存，由管理者決定。

- 【每日何時寄出自動放行的郵件】：當過期的稽核郵件且【過期的稽核郵件處理方式】是設為自動放行，會在固定的時間將所有被稽核郵件放行，預設是凌晨 1:00。

- 【寄送刪除郵件的通知信】：被稽核機制刪除的郵件，要不要寄刪除通知郵件給原寄件者，通知郵件的主旨跟內容在【刪除郵件】中設定。

- 【退回信參數】：當過期稽核郵件的處置方式在【過期的稽核郵件處理方式】中設為退回/刪除，或是經由稽核人員選擇退回/刪除時，會寄出一封退回/刪除通知信給原寄件者，有數個參數可以設定在通知信的主旨或是內文上，讓通知信的內容更容易閱讀，這些參數是

  收件日期，用 $date 代表。

  郵件主旨，用 $subject 代表。

  收件者，用 $receiver 代表。

  稽核人員，用 $auditor 代表。

退回郵件

- 【退回郵件的通知信主旨】：被稽核系統退回的郵件，原寄件者會收到一封退回通知信，退回通知信的主旨在這裡設定，例如，在這裡輸入 Your mail is rejected.--$subject--$date，則原寄件者會收到退回通知信的主旨就會顯示為 Your mail is rejected.—報價單—2023-1-1，其中”報價單”是原寄件者郵件的主旨。
- 【退回郵件的通知信內容】：被稽核系統退回的郵件，原寄件者會收到一封退回通知信，退回通知信的內容在這裡設定，例如，在這裡輸入 Your mail is rejected.--$subject--$receiver，則原寄件者會收到退回通知信的內容就會顯示為 Your mail is rejected.—報價單—sales@yourdomain.com。其中”報價單”是原寄件者郵件的主旨，sales@yourdomain.com 是原本郵件的收信者。

刪除郵件

- 【刪除郵件的通知信主旨】：被稽核系統刪除的郵件，原寄件者會收到一封刪除通知信，刪除通知信的主旨在這裡設定，例如，在這裡輸入 Your mail is rejected.--$subject--$date，則原寄件者會收到刪除通知信的主旨就會顯示為 Your mail is rejected.—報價單—201231-1，其中”報價單”是原寄件者郵件的主旨。
- 【刪除郵件的通知信內容】：被稽核系統刪除的郵件，原寄件者會收到一封刪除通知信，刪除通知信的內容在這裡設定，例如，在這裡輸入 Your mail is rejected.--$subject--$receiver，則原寄件者會收到刪除通知信的內容就會顯示為 Your mail is rejected.—報價單—sales@yourdomain.com。其中”報價單”是原寄件者郵件的主旨，sales@yourdomain.com 是原本郵件的收信者。

加密規則

- 當信件被過濾器過濾到進而轉交稽核人員時，稽核人員可選擇加密方式放行(圖 7-8-2)。

圖 7-8-2、稽核人員加密後放行

7-3、稽核隔離郵件通知清單設定

任何郵件，只要被郵件歸檔伺服器的稽核機制攔下來，不論後續的處置動作是放行、退回或是刪除，會定期的發送曾經被稽核機制過濾下來郵件的清單給指定的郵件帳號，被稽核機制過濾的寄件者也同樣收到清單，這些通知清單的寄送由管理者決定哪一些郵件帳號可以收到。

管理者稽核隔離郵件清單

指定的郵件帳號會收到被稽核機制過濾下來的所有郵件表列清單，發送清單的機制預設是關閉。(圖 7-9)

圖 7-9、管理者稽核清單

■ 【管理者稽核隔離郵件清單】：預設是關閉，啟用後，系統會將所有被稽核的郵件，不論他的處置動作是退回、刪除或是放行，將這些郵件以表列清單的方式寄給指定的收件者，

這些收件者必須有管理者權限，如果在設定的時間內沒有任何稽核郵件，則這封清單郵件將不會發送。

- 【傳送時間】: 2 種表列清單寄送時間設定模式，一個是指定時間另一個是設定間隔時間後週期性的發送，當有郵件被稽核且在表定的時間內，系統就會發送出這些通知清單郵件。設定間隔時間格式以天(d)/小時(h)/分，其中 d 及 h 分別是 day 跟 hour 的代表符號，例如，2h/30 代表 2 小時 30 分，代表每 2 小時 30 分會寄一封通知信。
- 【稽核隔離郵件清單的主旨】：發出稽核通知信的主旨，例如，Filter Mail List。
- 【接收稽核隔離郵件清單的管理者】：點選後可以選擇要收到通知郵件的管理者帳號，這些帳號都是預先建立在使用者群組中，且具有管理者權限者。

7-4、郵件防火牆

在合理應用情況下，郵件的寄件者名稱會與 Smtp 認證帳號相符，但是寄送垃圾郵件的駭客，認證時會使用他所能找到或猜到密碼的帳號，至於寄件名稱為了方便塞信，就會天馬行空隨意輸入，所以當啟動郵件防火牆功能後，會阻擋 Smtp 認證帳號與寄件者名稱不符者的來源 IP 位址，而原寄件者帳號與經常使用的來源 IP 不會受到任何影響。

郵件防火牆處理流程圖，(圖 7-11)

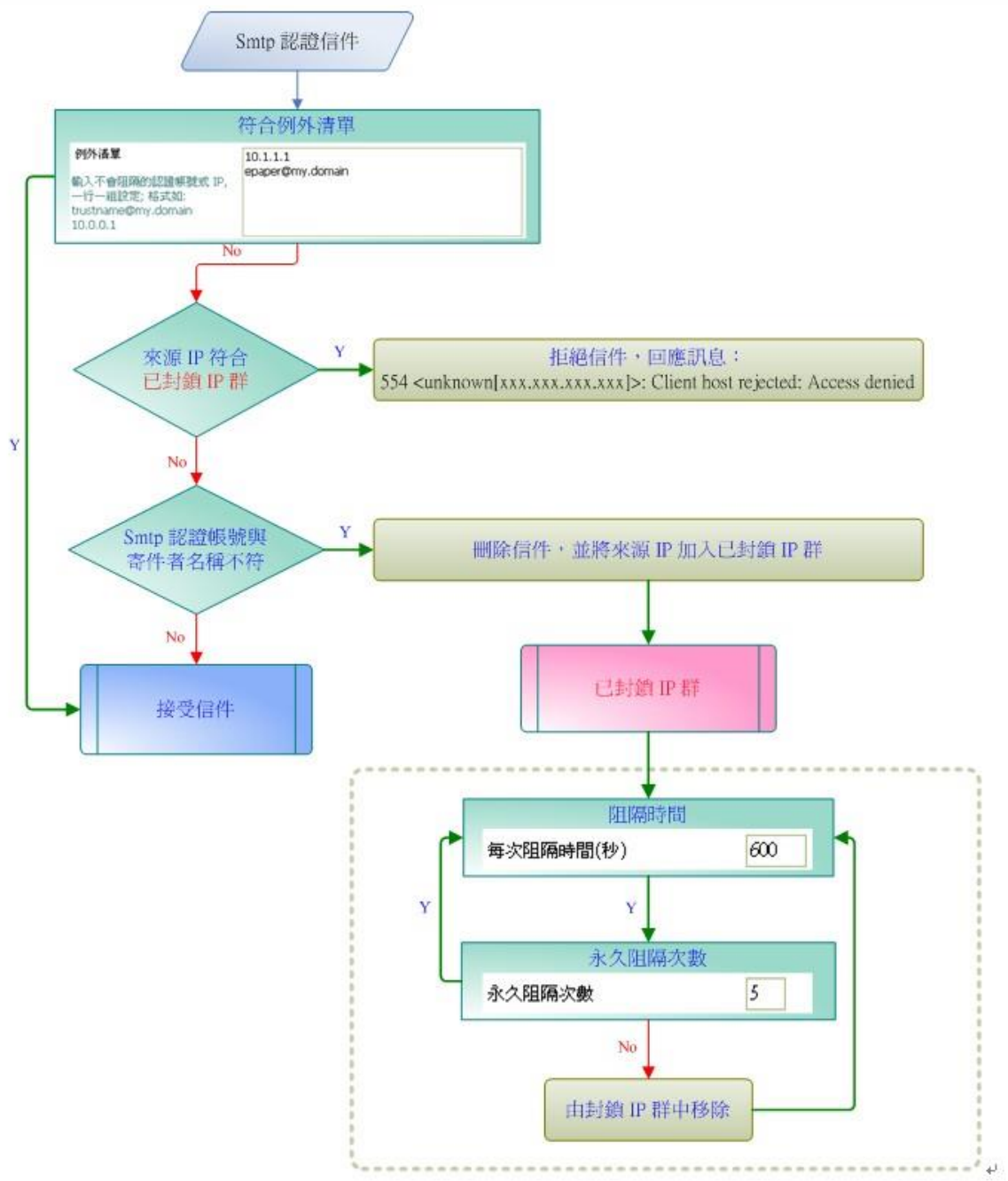


圖 7-11、郵件防火牆運作規則

(一)、郵件防火牆設定

垃圾信的發送業者會猜測郵件伺服器的帳號跟密碼，如果猜中後，會利用這一個帳號跟密碼狂發垃圾郵件，例如，freedy@yourdomain.com 的 SMTP 密碼設為 13579，就是一個典型容易被猜中的帳號及密碼，駭客非常容易就猜中密碼，一旦猜中後就可以利用這個帳號寄發大量的垃圾郵件。

郵件防火牆機制發現 SMTP 認證帳號與寄件者名稱不一致，郵件稽核過濾伺服器會封鎖寄件者的 IP 位址一段時間，封鎖的詳細設定請參考【IP 封鎖設定】。所以啟用這項功能後，就可以避免後端的郵件伺服器被當成垃圾郵件的轉信站。(圖 7-12-1，7.-12-2，7-12-3)

圖 7-12-1、郵件防火牆

圖 7-12-2、郵件防火牆

圖 7-12-3、郵件防火牆

- 【SMTP 認證漏洞】：啟用後會阻擋寄件者名稱跟 SMTP 驗證帳號不一樣的寄信動作，避免被當成垃圾郵件的跳板。
- 【寄件者帳號/認證帳號例外清單】：哪一些內部帳號不接受這個保護，輸入不被保護的寄件者帳號或寄件者帳號/認證帳號，一行一組設定，例如，freedy@yourdomain.com。

(二)、異常寄送偵測

發送垃圾郵件、釣魚郵件或是勒索病毒的業者，為了增加寄信的成功率，會對同一個網域的所有帳號或是特定帳號發送重複且帶特定附件的郵件，站在管理者的立場，就會看到有大量類似主旨或是特定執行檔的郵件進入郵件系統中，郵件歸檔伺服器能針對這類型的郵件或是它的變種郵件設定過濾規則，有效地偵測這類型的釣魚或是勒索郵件並且阻擋。

管理者可以設定 4 個比對規則，其中規則 4 是比對附件的格式，不論是在壓縮檔內或是單獨的附件檔，只要符合附件附檔名的規則，就滿足比對條件。

每一個規則比對原則如下：

1、主旨是否有重複字

如果比對的字元設為前 5 個相同，例如，主旨是 “這是一個好玩遊戲” 跟” 這是一個好棒的軟體” ，會被觸發比對規則。

2、附件檔的檔名是否有重複字

如果比對的字元設為前 5 個相同，例如，附件檔檔名是 “這是一個好玩遊戲.exe” 跟” 這是一個好棒的軟體.com” ，會被觸發比對規則。

比對規則也可以調整優先順序，每一個規則的設定如下。（圖 7-13）

圖 7-13、異常寄送的規則

■ 【異常寄送偵測】：針對主旨或是附件檔名的重複性文字可設定 4 個偵測規則並加上寄信頻率偵測，當觸發異常規則設定的郵件，將它送到隔離區或是封鎖寄件者的 IP 位址。

每個條件都可以加入邏輯判斷 OR / AND，增加運作的彈性，偵測的條件說明如下：

★ 偵測必要條件

主旨前幾個文字內容相同是偵測機制的必要條件，管理者可以決定比對字數的多寡，比對字數的多寡關係到誤判的機率，例如，比對字數設為 1，則誤觸發比對規則的機率就很高，一般以預設值 5 個文字誤觸發的機率就比較低。

另一個必要條件是寄信頻率，當寄件者的寄信頻率超過設定值，也會觸發比對規則，以（圖 6-13）範例，當寄信的頻率沒超過 1 分鐘 1 封信，偵測規則不成立。

★ 邏輯比對

附件的比對條件有 2 種，一種是檔名文字數量的比對，另一種是附件規則，對這 2 個比對方式可以配置邏輯比對 AND / OR，也就是當必要條件成立時，附件比對的條件是必要條件還是選擇之一。

★ 主旨比對條件

對於相同主旨或是變形主旨，都會視為相同的郵件，例如，

想要轉大錢 ? freedy 機會來了

想要轉大錢 ?elain 機會來了

都會視為相同的郵件，此時只要寄信的頻率被觸發，就會被歸類為異常寄信。

★ 附件檔名比對條件

對於相同附件檔名或是變形附件檔名，都會視為相同的郵件，例如，

好看的影片.exe

好看的影片-刺激.exe

都會視為相同的郵件，此時只要寄信的頻率被觸發，就會被歸類為異常寄信。

★ 附件規則比對條件

異常偵測會自動解開壓縮檔的附件，只要附件符合滿足下列 3 個規則，都會被視為異常。

1. 附件檔案有壓縮檔（zip / rar）
2. 單一壓縮檔小於 100 KB
3. 壓縮檔內有副檔名為下列設定的檔案，例如，exe、js、jse 及 scr。

★ 符合規則比對的處置

符合偵測規則的異常郵件，有 3 種處置方式，分別是轉到隔離區、封鎖寄件者 IP 跟不歸檔，當選擇封鎖寄件者 IP 時，就不會再收到相同的郵件。

- 【例外規則】：針對特定確認安全無慮的寄件者、主旨或是附件檔名，管理者可自行建立例外規則，符合例外規則的寄件者、主旨及附件檔名都不會被列入異常寄信行為偵測中，在主旨及附件檔名的設定上，可以使用正規表達式。

  通過 SMTP 認證的郵件也可以設為例外規則，符合上述的例外規則的郵件，就不會被再次偵測及比對。

- 【異常寄送郵件快取】：異常偵測是連續性的偵測機制，當某個比對規則符合後，在 24 小時內只要是重複類型的郵件，就不受寄件頻率的限制，自動歸類為異常寄信，這樣的優點是加快比對速度及降低系統負荷，缺點是會有誤判的機率。管理者也可以把它清除，重新開始學習比對。

(三)、信任 IP 清單

管理者可以增加信任的 IP 位址，這一些寄件者的來源 IP 位址，就不會經過郵件防火牆的比對跟過濾。（圖 7-14）

圖 7-14、信任 IP 位址

- 【名稱】：給信任 IP 位址容易辨識的名稱，例如，內部網路。
- 【網路 / 遮罩】：選擇 IP 位址模式是 IPV4 或 IPV6，並輸入 IP 位址及區段，例如，IPV4 的 192.168.168.0/24 ，代表 192.168.168.0 這個 C 網段。

(四)、IP 阻擋清單

管理者可以增加阻擋 IP 位址，這一些寄件者的來源 IP 位址，就不能經過郵件防火牆到後端的郵件伺服器寄信，就是寄信黑名單。（圖 7-15）

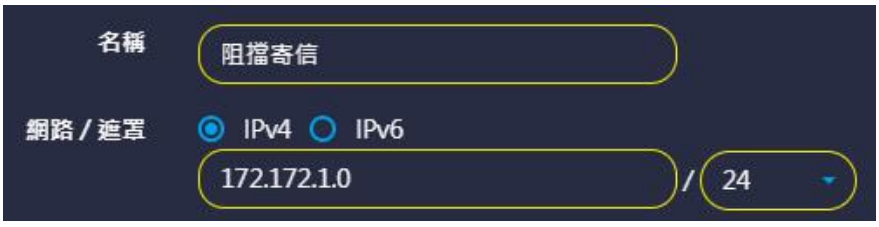


圖 7-15、IP 阻擋清單

- 【名稱】：給 IP 阻擋清單容易辨識的名稱，例如，不給寄信。
- 【網路 / 遮罩】：選擇 IP 位址模式是 IPV4 或 IPV6，並輸入 IP 位址及區段，例如，IPV4 的 172.172.1.0/24 ，代表 172.172.1.0 這個 C 網段。

7-5、IP 封鎖設定

不論是稽核條例上設定的封鎖或是郵件防火牆上的封鎖機制，當某個偵測機制被觸發之後，郵件歸檔伺服器就會按照這裡設定的封鎖機制，將寄件者、寄件 IP 位址封鎖一段時間，同時會將封鎖紀錄紀錄下來同時寄發通知信給寄件者，封鎖機制的共同設定，都會在這裡配置。

通知設定包含啟動通知、每日寄送、永久阻隔次數。(圖 7-16)

圖 7-16、IP 封鎖設定

- 【封鎖次數】：觸發封鎖機制超過設定的次數後，就會進入永久封鎖的程序，除非管理者解除封鎖，否則寄件者或是寄件 IP 位址就無法正常通過郵件稽核歸檔設備。

- 【每次封鎖時間(秒)】：

  當封鎖的條件觸發後，郵件歸檔伺服器會自動封鎖來源 IP 位址的時間，在這段期間內，無法對郵件伺服器寄信，單位為秒。

  例一：設為 600，則滿足封鎖觸發條件後，該來源 IP 位址會被封鎖 600 秒。

  例二：設為 600,900,1200，則第一次滿足封鎖觸發條件後，該來源 IP 位址會被封鎖 600 秒，第二次滿足封鎖觸發條件後，該來源 IP 位址再會被封鎖 900 秒，第三次滿足封鎖觸發條件後，該來源 IP 位址再會被封鎖 1200 秒。

  在【每次封鎖時間(秒)】中設定的偵測次數數量超過 【永久封鎖次數】，後面的時間就沒任何意義了，例如，設為：600,900,1200,1500，但是在 【永久封鎖次數】中設為 3，在上述的範例中 1500 這個設定值就沒任何意義。

- 【通知信】：啟動後，定時發送最新 IP 阻擋紀錄及封鎖紀錄給設定的帳號，寄送間隔時間以小時為計算單位。
- 【每日寄送日誌與當日阻隔名單】：啟動後，每日會定時發送封鎖日誌及被封鎖的帳號給通知信的收進者。
- 【收信者】：輸入要收到通信的帳號，例如，ma_info@yourdomain.com。
- 【永久封鎖 IP 處理方式】：當 IP 位址被判斷為永久封鎖後，要不要自動在一段時間後，解開，時間單位是以月為主。

7-6、異常寄送通知清單設定

管理者郵件防火牆異常寄送郵件清單

被郵件防火牆偵測出來的異常寄信，系統會自動對管理者跟使用者寄發通知信，讓管理者知道哪一些 IP 位址或是寄件帳號被阻擋，同時也可通知被濫用帳號寄信的寄件者。(圖 7-17)

圖 7-17、管理者郵件火牆異常清單通知信

- 【管理者異常寄送郵件清單】：啟用或是關閉異常郵件通知，開啟後，如果有異常行為，管理者會收到通知郵件。
- 【傳送時間】：異常郵件通知信是在哪個時間寄送，可以自訂時間或是在間隔的時間內寄送。
- 【異常寄送郵件清單的主旨】：異常郵件通知信的主旨，例如，Abnormal Mail List。
- 【接收異常寄送郵件清單的管理者】：接收異常郵件通知信的人，不一定是郵件歸檔伺服器的管理者，可以加入其他的郵件帳號。

第 8 章 郵件加密

郵件主機讓企業可以在既有郵件系統架構之下，提供閘道端與終端更安全的運作架構。

管理者可以針對特定人員將其整封.eml 郵件轉為加密 PDF 檔，或是僅對其電子郵件的附件進行加密壓縮，確保郵件傳輸時被竊取而洩漏重要訊息。

而接收方當收到郵件時可使用 PDF 閱讀程式，輸入密碼就可以檢視原始郵件內容，當然包含其夾寄的附件檔。

8-1、郵件加密規則

進行加密的郵件會因為加密模式的不同，所需要花費的加密時間也有所不同，請耐心等候，郵件加密進度可至日誌查詢 - > 加密使用者申請日誌查詢。

郵件加密設定的優先順序 ：

1. 寄件者透過 WebMail 寄信時的設定。2.符合條件的 [郵件加密規則]

加密時密碼的來源順序如下 ：

1. 收件者自訂的密碼。2.本機寄件者透過 WebMail 寄件時設定的密碼。3.[郵件加密規則] 處方式的密碼。

當郵件格式屬於數位簽章、加密、 Calendar 或 RTF (未處理格式轉換)，將強制以超過限制的處理方式。

(一)、新增規則

郵件加密規則的顯示名稱，郵件加密規則目前的啟用狀態，郵件加密規則目的詳細說明，郵件加密規則的執行時間，預設為 [永久執行] （圖 8-1）。

圖 8-1、新增加密規則名稱

(二)、加密規則設定

選擇郵件加密規則的比對邏輯，共有 AND、OR 2 種，規則設定說明 ：

標示 * 的欄位可以輸入特殊定義字，如【!】表示【否定】的意思，【null】表示【空白】，支援萬用字元 [? *]，多個規則可以用【,】符號隔開，它代表【或】的組合，比對關鍵字時，不區分

大小寫。

寄件者包含的關鍵字，例如，輸入 sales 同時選擇 '不包含'，代表只要不是 sales 的都滿足條件。

選擇收件者規則的比對邏輯，本機網域包含 ：收件者中包含有本機網域的帳號，網域包含 ：收者中包含有 [網域包含] 清單中的帳號。

收件者包含 ：收件者中包含有 [收件者包含] 清單中的帳號，群組、部門、別名帳號僅提供方便設定其包含的成員帳號，並非郵件中的收件者需包含該群組、部門、別名帳號。

所有收件者符合 ：需要所有收件者皆包含在設定中，相反結果 ：若原本結果為符合，則將會改判斷為不符合。

網域包含、收件者包含可以在自訂欄位中輸入特殊定義字，如【!】表示【否定】的意思，支援萬用字元 【?*】(圖 8-2) 。

圖 8-2、加密規則設定

(二)、符合規則處理方式

PDF : 將郵件內容擷取出並轉換為 PDF 檔中加密後，再附加在一封新郵件中寄出。

※若郵件內容中包含許多外部連結的圖片，將會下載此些圖檔至本機在附加至 PDF 中顯示

ZIP : 僅將郵件附件擷取打包至 ZIP 檔中加密後，再附加在郵件中寄出 (圖 8-3) 。

圖 8-3、規則符合處理

8-2、郵件加密進階設定

(一)、郵件加密密碼強度限制

加密條件包含英文 (不區分大小寫)，英文大寫，英文小寫，數字，符號等選項，安全性高 (圖 8-4) 。

圖 8-4、郵件加密強度

(二)、使用者加密進階設定

若需要加密的收件者超過上限，此封郵件將暫時不進行加密。且將會發送一封通知信給寄件者，由寄件者決定是否要發送此封郵件 (圖 8-5) 。

圖 8-5、使用者進階加密

(三)、PDF 加密內容設定

支援自訂 PDF 加密郵件的內容樣式，如下所示支援自訂郵件加密 Logo 圖示、郵件加密鎖圖示、聲明內容和郵件底部的版權聲明。

聲明內容、郵件底部的版權聲明僅支援輸入字串訊息（圖 8-6）。

圖 8-6、PDF 加密模式

(四)、非本機帳號密碼強度限制

加密條件包含英文 (不區分大小寫)，英文大寫，英文小寫，數字，符號等選項，安全性高 (圖 8-7) 。

圖 8-7、非本機郵件加密強度

(五)、非本機帳號申請設定

讓非本機帳號的使用者申請帳號 (圖 8-8) 。

圖 8-8、非本機帳號申請

8-3、加密使用者管理

(一)、新增使用者

新增本機帳號或非本機帳號（圖 8-9）

圖 8-9、使用者新增

(二)、寄件者加密模式

PDF：將郵件內容擷取出並移除超連結後存入 PDF 檔中加密，再附加在一封新郵件中寄出

※若郵件內容中包含許多外部連結的圖片，將會下載此些圖檔至本機在附加至 PDF 中顯示

ZIP：僅將郵件附件擷取打包至 ZIP 檔中加密後，再附加在郵件中寄出（圖 8-10）

圖 8-10、寄件者加密模式設定

(三)、收件者加密模式

郵件加密為 PDF 或 ZIP 檔案時所使用的密碼

固定密碼 ： 不允許只有空白字元

隨機密碼 ： 將依照設定包含的字元產生設定字元長度的密碼，範圍 ：10 - 255 (圖 8-11)

圖 8-11、收件者加密模式設定

第 9 章 郵件病毒

郵件病毒肆虐，讓人防不勝防，對於熟悉病毒運作原理的網管人員，接收到有問題的郵件時，例如特殊的圖片、網址超連結、 * .exe..等檔案，通常不會貿然的點選，當然感染病毒的機會就少很多，但是一般的使用者不一定有這樣的警覺，所以在郵件中提供掃毒服務是一個很重要的工作。

郵件歸檔伺服器具有病毒郵件過濾功能，不論是閘道器或是 POP3 代收模式，都可以啟用郵件掃毒功能。郵件歸檔伺服器內建 2 套掃毒引擎，ClamAV(免費)跟 Kaspersky (付費)，預設會啟用 ClamAV 掃毒引擎，當管理者匯入 Kaspersky 的授權碼，就可啟用 Kaspersky 掃毒引擎。

9-1、基本設定

系統內建 2 套防毒引擎，ClamAV 跟 Kaspersky，管理者可以啟用其中之一或是 2 個都啟用，但是 Kaspersky 如果沒有上傳授權碼，就算啟用也無法進入 Kaspersky 的掃毒程序。當被防毒引擎判斷為病毒郵件後，系統該如何處置，都會在這個章節設置。

(一)、郵件掃毒設定

郵件伺服器預設是使用 ClamAV 掃毒引擎，如果不放心免費的掃毒軟體，另外提供一套商業版的掃毒軟體機制，只要購買使用版權，不需要安裝，匯入資料，就可以使用。(圖 9-1)

圖 9-1、掃毒引擎設定

- 【郵件掃毒功能】：要不要在郵件歸檔伺服器啟用掃毒功能，閘道器跟 POP3 代收模式都可以啟用這個功能。
- 【掃毒引擎】：目前郵件伺服器內建兩套掃毒引擎，ClamAV、Kaspersky，同一時間只需要選擇一套防毒軟體就好。

  ClamAV：系統預設的掃毒引擎，不需要使用費用，定時更新病毒碼。

  Kaspersky：需要另外購買使用版權，以使用人數及時間計算費用，定時更新病毒碼。

- 【不掃描的附件副檔名】：建立不掃瞄的檔案名稱，增加郵件處理的速度，經過郵件歸檔伺服器郵件，如果夾帶檔案的副檔名跟設定的一樣，掃毒系統就會跳過這個病毒檢查程序。

  系統預設不掃描圖形檔(jpg、jpeg、gif、bmp)、影片檔(avi、dat、mpeg、mpg、mp3、mid、wav、rm)。

- 【掃描附件檔案的最大容量】：當郵件夾帶的附件檔超過設定容量後，掃毒引擎將不會掃描附件，預設是 640KBytes。

- 【病毒碼自動更新時間】：病毒碼更新時間，設定間隔時間格式以天(d)/小時(h)/分，其中 d 及 h 分別是 day 跟 hour 的代表符號，例如，2h/30 代表 2 小時 30 分，每 2 小時 30 分會自動到網路上更新病毒碼。

(二)、中毒郵件處理方式

當收到中毒的郵件時，郵件伺服器可以做下列處理（圖 9-2）。

圖 9-2、中毒郵件處理

- 【中毒郵件是否不歸檔】：預設是起用，中毒的郵件不要歸檔，關閉則代表，中毒的郵件也會存在郵件歸檔伺服器的資料庫中。
- 【中毒郵件轉到隔離區】：中毒的郵件會被歸類到隔離區中，使用者就不會收到這一封郵件，如果病毒信通知清單有啟用，使用者會收到一封病毒郵件的通知清單。
- 【中毒郵件副檔名改為】：郵件夾帶的病毒檔案會被防毒軟體清除，同時更改副檔名為設定的名稱，預設的名稱是 virus，並且在主旨文字通知收件者這封郵件是有病毒，請收信者小心。
- 【中毒郵件通知信主旨】：掃毒軟體判斷郵件中毒後，如果在【中毒郵件處理方式】中沒有選【中毒郵件轉到隔離區】的功能，這封信仍會送給收件者，同時在主旨文字加上【中毒郵件通知信主旨】中輸入的字元，預設值為[This mail hasVirus]，通知收件者這封郵件是有病毒。

9-2、掃毒設定

ClamAV 全名是 Clam AntiVirus，它跟 Linux 一樣強調公開程式碼、免費授權等觀念，ClamAV 24 小時更新及維護病毒資料庫，任何人發現可疑病毒也可以隨時跟她們取得聯繫，立刻更新病毒碼。

(一)、ClamAV 掃毒引擎設定

郵件伺服器採用 ClamAV 專門提供給郵件伺服器在 Linux 平台下使用，所以跟其他商業運轉的防毒軟體有區隔（圖 9-3）。

圖 9-3、ClamAV 掃毒引擎

- 【ClamAV 掃毒引擎目前狀態】：郵件歸檔伺服器預設的 ClamAV 掃毒引擎是開啟的，想切換掃毒引擎設定，可以進入【郵件病毒】>【基本設定】切換。
- 【掃毒引擎版本】：顯示掃毒引擎目前使用的引擎版本及病毒碼更新時間，它的顯示如下：

  ClamAV 0.103.7/26932/Thu Jun 8 07:45:53 2023

  0.103.7 是引擎版本，Thu Jun 8 07:45:53 2023 是病毒碼更新時間。
- 【病毒碼數量】：顯示目前在郵件伺服器的病毒碼數量，點選立即更新就可以馬上跟病毒碼更新伺服器更新最新的病毒碼。

- 【病毒碼更新主機】：可以自選病毒碼更新主機，依照郵件歸檔伺服器所在的國家選擇最快的病毒更新引擎，選擇後需要按下套用的按鍵才會生效。
- 【ClamAV 病毒碼更新紀錄】：所有的更新過程都會記錄在更新紀錄中，移動游標就可以知道這次的更新，增加了哪些病毒碼。
- 【清除紀錄】：按下【清除紀錄】按鍵，會將上面的更新紀錄全部清除掉。

(二)、Kaspersky 掃毒引擎設定（需另付費，以年計算）

郵件防毒軟體牽涉到使用者的信心問題，有時候考慮的不只是費用問題，郵件歸檔伺服器幫使用者考慮到這個問題，所以預先安裝了商業運轉的防毒程式，Kaspersky，授權以使用者數量計算，只要將指定的授權檔案上傳到郵件歸檔伺服器馬上完成啟用，防護功能就會自動啟動。(圖 9-4)。

圖 9-4、Kaspersky 掃毒引擎

- 【Kaspersky 掃毒引擎目前狀態】: 郵件歸檔伺服器的 Kaspersky 掃毒引擎預設是關閉的，想切換掃毒引擎設定，可以進入【郵件病毒】>【基本設定】切換，在【上傳 Kaspersky 版權文件】中上傳授權文件就啟用引擎。
- 【掃毒引擎版本】：顯示掃毒引擎目前使用的引擎版本及病毒碼更新時間。
- 【檢查掃毒引擎版本更新】：啟用後才會出現，當系統偵測到有新的掃毒引擎後，顯示會出現有更新可供使用的字樣，點選執行下載並更新按鈕後就會自動下載軟體並安裝。
- 【授權狀態】：顯示目前掃毒引擎的授權狀態。
- 【病毒碼數量】：啟用後，顯示目前在郵件伺服器的病毒碼數量，點選立即更新就可以馬上跟病毒碼更新伺服器更新最新的病毒碼。
- 【Kaspersky 病毒碼更新紀錄】：所有的更新過程都會記錄在更新紀錄中，移動游標就可以知道這次的更新，增加了哪些病毒碼。
- 【清除紀錄】：按下【清除紀錄】按鍵，會將上面的更新紀錄全部清除掉。
- 【上傳 Kaspersky 版權文件】：上傳授權文件就啟用引擎。

9-3、病毒郵件通知清單設定

任何郵件，只要被郵件歸檔伺服器的病毒引擎攔下來，不論後續的處理動作，系統會定期的發送曾經被攔下的病毒郵件清單給系統管理者或是原本的收件者，這些清單的寄送是由管理者決定。

(一)、管理者病毒隔離郵件清單

管理者病毒隔離清單預設是關閉。(圖 9-5)

圖 9-5、管理者病毒清單

- 【管理者病毒隔離郵件清單】：預設是關閉，啟用後，系統會將所有被病毒引擎判斷為中毒的郵件，以清單的方式寄給指定的收件者，這些收件者必須有管理者權限，如果在設定的時間內沒有任何中毒郵件，則這病毒清單郵件將不會發送。
- 【傳送時間】: 2 種設定模式，一個是指定時間另一個是設定間隔時間後週期性的發送，當有中毒郵件且在表定的時間內，系統就會發送出這些通知清單郵件，設定間隔時間格式以天(d)/小時(h)/分，其中 d 及 h 分別是 day 跟 hour 的代表符號，例如，2h/30 代表 2 小時 30 分，每 2 小時 30 分會傳送通知信。
- 【病毒隔離郵件清單的主旨】：發出中毒通知信的主旨，例如，Virus Mail List。
- 【接收病毒隔離郵件清單的管理者】：點選後就可以選擇要收到通知郵件的管理者帳號。這些帳號都是預先建立在使用者群組中，且具有管理者權限者。

(二)、使用者病毒隔離郵件清單

使用者病毒隔離清單預設是關閉。(圖 9-6)

圖 9-6、使用者病毒清單

- 【使用者病毒隔離郵件清單】：預設是關閉，啟用後，系統會將所有中毒的郵件，以清單的方式寄給原本的收件者，如果在設定的時間內沒有任何中毒郵件，則這封清單郵件將不會發送。
- 【傳送時間】: 2 種設定模式，一個是指定時間另一個是設定間隔時間後週期性的發送，當有中毒郵件且在表定的時間內，系統就會發送出這些通知清單郵件，設定間隔時間格式以天(d)/小時(h)/分，其中 d 及 h 分別是 day 跟 hour 的代表符號，例如，2h/30 代表 2 小時 30 分，每 2 小時 30 分會傳送通知信。
- 【病毒隔離郵件清單的主旨】：發出中毒通知信的主旨，例如，Virus Mail List。
- 【不接收病毒隔離郵件清單者】：點選後就可以選擇不要收到通知郵件的使用者帳號，除了這一些指定不接收者不會收到外，其他中毒郵件的收件者都會收到通知郵件，空白代表所有中毒郵件的收件者都會收到通知信。

第 10 章 HERHSIANG Sandstorm

進階 HERHSING Sandstorm 可有效偵測未知的進階惡意程式附檔，諸如常見 Microsoft、Word、Excel、Power Point 或 PDF；或針對性的釣魚郵件，甚至壓縮檔，如常見的是 ZIP 與 RAR，Sandstorm 防禦在企業郵件掃描 Spam 或 Virus 前，針對可疑的附件先做比對，將有問題的信件進行隔離，讓潛藏的惡意程式現出原形，避免影響使用者郵件接收。

(一)、最後更新時間

系統會每天自動檢查更新一次 (圖 10- 1)。

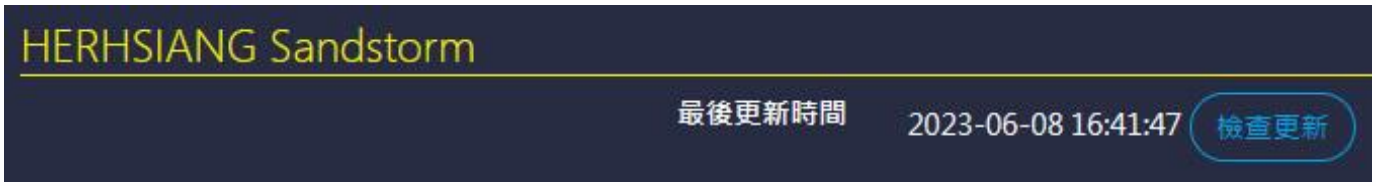


圖 10- 1 、版本更新檢查時間

(二)、惡意程式過濾

郵件會進行惡意程式過濾分析，系統會每天自動檢查更新一次，表列的副檔名都不會進入分析，數值需大於 0 KB，建議數值為 1024 KB，當分析檔案越大，所耗用的系統效能越重分析上傳檔案是否為惡意程式或包含惡意程式 (圖 10-2)。

圖 10-2、惡意程式過濾

(三)、惡意程式處理方式

符合過濾的郵件會轉到隔離區，收件者不會收到通知信，將符合過濾的附件的副檔名改掉，避免收件者混淆，將符合過濾的附件內容清除，寄給收件者的郵件通知信主旨，範例：郵件發現了惡意程式 (圖 10-3)！

。

圖 10-3、惡意程式處理方式

(四)、URL 過濾

郵件會進行 URL 連結過濾分析，系統會每天自動檢查更新一次，過濾的惡意程式風險等級 (圖 10-4)。

圖 10-4、URL 過濾

(五)、IP 過濾

郵件會進行 IP 過濾分析，系統會每天自動檢查更新一次，過濾的惡意程式風險等級 (圖 10-5)。

圖 10-5、IP 過濾

(六)、網域過濾

郵件會進行網域過濾分析，系統會每天自動檢查更新一次，過濾的惡意程式風險等級（圖 9 -6)。

圖 10-6、網域過濾

(七)、URL/IP/網域 處理方式

可選擇直接轉到隔離區或比對目前垃圾郵件過濾設定參數，的設定為主旨加入提示文字，判斷分數 = 5，垃圾郵件在隔離區並發送清單，判斷分數 = 10，直接刪除，判斷分數 = 15（圖 10-7)。

圖 10-7、URL/IP/網域 處理方式

第 11 章 垃圾郵件

郵件歸檔伺服器具有垃圾郵件過濾功能，這個機制適用於透通跟 POP3 代收模式，在透通模式運作下，垃圾郵件過濾機制是外部郵件在進入郵件伺服器前就進行過濾垃圾郵件的動作，但是在 POP3 代收模式下，使用者的郵箱已經收下所有郵件，所以系統的過濾機制只能降低歸檔的無效郵件數量，這是 2 種模式在垃圾郵件過濾上最大的不同。

垃圾郵件基本的運作是去檢查整封信的特徵值，根據每一個特徵值給予不同的評分，將這些評分加總後就是垃圾郵件分數，底下就是一個範例。

★垃圾郵件分數範例

郵件伺服器是用整封郵件行為，並將它轉換成綜合判斷分數，一般垃圾郵件評分如下所示：

0.1 MIME_HTML_ONLY BODY: Message only has text/html MIME parts

0.0 HTML_MESSAGE BODY: HTML included in message

2.2 HTML_IMAGE_ONLY_02 BODY: HTML: images with 0-200 bytes of words

0.7 MIME_HTML_NO_CHARSET RAW: Message text in HTML without charset

1.9 MIME_HEADER_CTYPE_ONLY 'Content-Type found without required MIME headers

1.6 FORGED_MUA_OUTLOOK Forged mail pretending to be from MS Outlook

X-Spam-Status: Yes，hits=6.5 required=6.0 tests=FORGED_MUA_OUTLO

上述的範例說明，判斷的機制是針對郵件的行為給予不同的分數，例如：某個收件者收到一封信，在郵件的本文中只有網址超連接，沒有其他的文字說明，它很有可能是要誘惑收信者點選某一個特定網站，有相當程度上它可能會是垃圾郵件，以上述的例子，給予 0.1 分。

將這些判斷機制的分數統統加總起來，就是這封郵件的垃圾郵件分數，分數越高，是垃圾郵件的可能性高。

以上面的範例來說，加總為 0.1+0.0+2.2+0.7+1.9+1.6＝6.5，再根據管理者的設定，決定 6.5 分是不是垃圾郵件。

對於垃圾郵件的處理方法共有 3 種，主旨加入提示文字、放在隔離區、刪除，詳細的說明會在【基本設定】>【垃圾郵件處理方式】中說明。

11-1、基本設定

(一)、垃圾郵件過濾的基本設定

垃圾郵件過濾機制是否啟用。(圖 11-1)。

圖 11-1-1、垃圾郵件基本設定

- 【目前垃圾郵件過濾狀態】：顯示目前垃圾郵件過濾機制的運作狀態，是正常運作或是停止運作，有些垃圾郵件的判斷機制會使用網路檢查最新的狀況，網路不通的情況下，這個地方會顯示停止運作的狀態。
- 【垃圾郵件過濾】：啟用後，垃圾郵件過濾機制才會運作。
- 【通過 SMTP 認證後的郵件】：對於已經通過 SMTP 認證的寄件者寄出的郵件，垃圾郵件過濾機制該如何處理，有 2 種處置方式

  1.再次進入垃圾郵件過濾

  2.皆視為正常郵件

  管理者可以根據使用者的帳號密碼安全性決定，如果每個使用者的帳號密碼安全性足夠且沒有被當跳板的機會，就可以選擇【皆視為正常郵件】。

■ 【垃圾郵件學習共享】：啟用後，系統會將疑似垃圾郵件的郵件去除敏感資料後，送到後端的共享垃圾郵件過濾平台進行更精密的分析，分析後再把這一些結果分享給有提供分享機制的設備，結合眾人的力量，讓垃圾郵件的判斷機制更準確。

(二)、AI Spam 自動化垃圾郵件防護功能模組 [精準度 99.5%]

(需另付費, 以年計算)

收集龐大的中文斷詞資料庫，AI Spam 的演算基礎就是繁/簡體中文斷詞資料庫， 中文跟英文不一樣的地方是斷詞的精準度決定郵件意圖分析中的關鍵， 例如: 前往全球資訊網路路上斷詞決定了上述文字的語意分類， 研發單位做了研究顯示， 不斷詞跟斷詞後進入 AI Spam 演算後，精準度差為距 1~2%。些微差距， 就呈現在最後郵件判斷的精確度上，藉由研發單位建立的中文斷詞資料庫，讓 AI Spam 在演算郵件分類路上，更顯得精確及簡單 (圖 11-1-1)。

圖 11-1-2、AI Spam 自動化垃圾郵件防護功能模組

(二)、EDM-電子報

依據 Rspamd 掃描結果，判定信件是否屬於 [EDM - 電子報] 類型的信件

[日誌查詢 > 郵件日誌 >] 支援顯示掃描結果為 [EDM - 電子報] 類型的信件

圖 11-1-3、電子報過濾模組

(二)、垃圾郵件處理方式

對於垃圾郵件的處理方式共有 4 種，其中 3 種是屬於垃圾郵件的分類機制，根據系統判斷的垃圾信分數進行處置，這 4 種動作可以任意啟用其中一種或是全部都啟用，4 種處理方式分別如下。(圖 11-2)

1、垃圾郵件不歸檔。

2、垃圾郵件主旨加入提示。

3、垃圾郵件隔離。

4、垃圾郵件刪除。

圖 11-2、垃圾郵件處理方式

★ 經驗範例

一開始設定判斷分數時可以將它的分數稍微調高一下，例如 7～8 分，管理者再根據使用者的反應，或是實際自己郵箱的運作情況調整，如此就可以調整到適合公司運作的垃圾郵件判斷分數或者先啟用在主旨加入特定文字，觀察判斷分數對郵件的影響。一般來說，判斷分數 5 分，是一個垃圾郵件跟正常郵件的分水嶺。

1、垃圾郵件不歸檔。

啟用這個選項後，超過 3 種垃圾郵件判斷分數(主旨提示文字、隔離跟刪除)的郵件，通通不會進入郵件歸檔程序，也就是使用者日後查詢不會看到這一封郵件。

2、垃圾郵件主旨加入提示。

根據判斷分數判斷為垃圾信後，在這封郵件的主旨最前面加上一段預設的文字，再將這封郵件傳給原來的收件者，所以收件者會收到所有的郵件，使用者再靠這個特殊文字，判斷是正常郵件或是垃圾郵件。

- 【主旨提示文字】：輸入在主旨的前面加入的文字，可以是文字或符號，當然也可以是空白文字，例如，[Spam-Mail]或是 ___。
- 【主旨提示分數】：垃圾郵件判斷分數是多少才會啟用主旨提示文字。

★ 經驗範例

一般經驗這個數值可以先調成 5，管理者再根據使用者的反應，或是實際自己郵箱的運作情況調整，如此就可以調整到適合公司運作的垃圾郵件判斷分數。

3、垃圾郵件隔離。

被判斷成垃圾郵件的郵件會先被放在隔離區中，在隔離區的郵件並不會被刪除，郵件歸檔伺服器會定時的將隔離區的郵件整理，並寄一封垃圾郵件清單給使用者，垃圾郵件清單通知信會列出收信時間、寄件者、收件者、主旨、綜合垃圾郵件判斷分數等資料，收信者可以根據自己的需要，取回認為被誤判的郵件。

- 【隔離分數】：垃圾郵件判斷分數是多少才會啟用將郵件放在隔離區。

★ 經驗範例

一般經驗這個數值可以先調成 10，管理者再根據使用者的反應，或是實際自己郵箱的運作情況調整，如此就可以調整到適合公司運作的垃圾郵件判斷分數。

4、垃圾郵件刪除。

被判斷成垃圾郵件的郵件會先被放在刪除區中，系統會在固定時間內將在刪除區的郵件刪除，使用者不會收到任何通知。

■ 【刪除分數】：垃圾郵件判斷分數是多少才會啟用將郵件放在刪除區。

★ 經驗範例

一般經驗這個數值可以先調成 15 或是 20 ，通常超過這分數，都是垃圾郵件。管理者可再根據系統的刪除區郵件調整到適合公司運作的垃圾郵件判斷分數。

(三)、信任 IP 位址設定

垃圾郵件過濾機制可以設定信任 IP 位址，當寄件者的來源 IP 位址是表列的範圍，則直接不進入垃圾郵件過濾機制，再經過郵件歸檔程序後，寄給原收件者。

如同白名單的功能，為避免某些內部使用者 (可能分散各地上班的同事)，寄出的郵件被當成垃圾郵件，使用信任的 IP 位址設定，可以減少這樣的困擾，管理者可利用此功能填入信任的 IP 位址或 IP 區段以修正判別垃圾郵件的問題。(圖 11-3)。

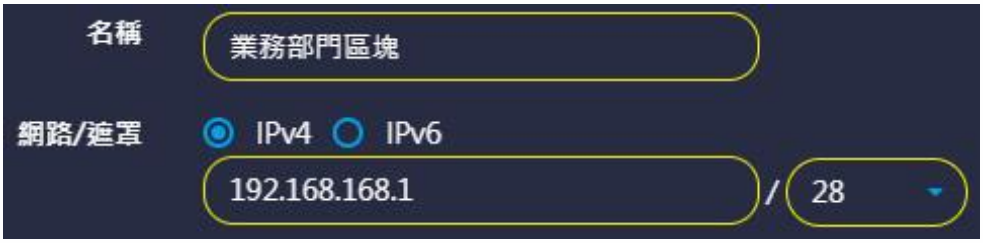


圖 11-3、信任 IP 位址設定

- 【名稱】：給這信任 IP 位址一個名稱，例如，業務區。
- 【網路/遮罩】：信任 IP 位址支援 IPV4 跟 IPV6 2 種模式，以 IPV4 為例，設定成 192.168.168.1 /28 ，代表來自 192.168.168.1 ~ 192.168.168.15 來源 IP 位址的寄件者，他的郵件都不會經過垃圾郵件過濾機制。

  IPV6 的範例，IP 位址 2001:b030:c201:ff00::254 (/64)，這個網段的寄件者不會經過垃圾郵件過濾。

信任 IP 位址的列表如下：(圖 11-4)

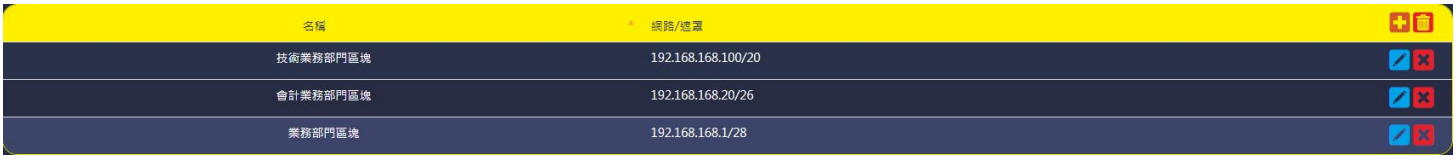


圖 11-4、信任 IP 位址的列表

11-2、參考資料庫

郵件歸檔伺服器的垃圾郵件過濾機制，除了預設的垃圾信特徵過濾一定啟用外，使用額外 4 種垃圾郵件的辨識方法可供管理者啟用或是關閉，這一些額外的選項能更精準的判斷出是否為垃圾郵件。

除了郵件特徵外，針對郵件的內文中的 URL 連結跟資料庫比對後，也可判斷是否為異常的網站，當郵件內文中的 URL 為異常的網站時，管理者可針對這類型的郵件進一步的處置。

(一)、垃圾信辨識機制

共有 4 種選擇機制，分別是 IP 位址信用評等、貝氏過濾法、貝氏過濾法自動學習機制及郵件表頭附加註記，讓管理者選用，一般來說，都會全部使用，增加判斷的準確度。(圖 11-5)

圖 11-5、垃圾郵件過濾

1、IP 位址信用評等

這個功能參照網際網路上的黑名單 IP 位址資料庫，如果寄件者的 IP 位址來自於被列入黑名單 IP 位址資料庫的 IP，那他是垃圾郵件的比率就相當高。

一般來說，寄件者的 IP 位址是動態的，是垃圾郵件的比率也是相當高的，這個選項需要向網際網路的黑名單資料庫查詢，需要網路暢通才能正常運作，所以選擇啟動時要注意，郵件歸檔伺服器對外的通訊是否正常。

2、貝氏過濾法

貝氏過濾法是將郵件之內文以貝氏資料庫之規則來評分，分數越高者其越有可能是垃圾郵件。一般來說「貝氏過濾法」會有個資料庫，當一封郵件進入系統的時候會把郵件分解成單詞，比對目前「貝氏過濾法資料庫」，分析以往的經驗，判斷此封郵件為垃圾郵件的機率，且貝氏過濾資料庫具有自動學習的功能，可以依照不同企業收信的狀態來調整最適合的過濾條件。

3、貝氏過濾法自動學習機制

是否要啟動垃圾郵過濾機制中貝氏過濾法的自動學習機制。

4、信件表頭附加註記

是否要檢查郵件表頭是否有額外的註記。

垃圾信特徵過濾

由於垃圾郵件發送的特徵不斷的在做改變，郵件歸檔伺服器除了透過使用者定時回報，持續不斷累積「過濾經驗」，經由特徵採樣、資料庫更新速度和自動學習的能力提高設備過濾的及時性與效率。

(二)、內文連結過濾機制

郵件的內文如果有 URL 的連結，垃圾郵件過濾機制能利用 URL 黑名單資料庫的資料，判斷這一封郵件是否為垃圾郵件，可以增加判斷的準確度。(圖 11-6)

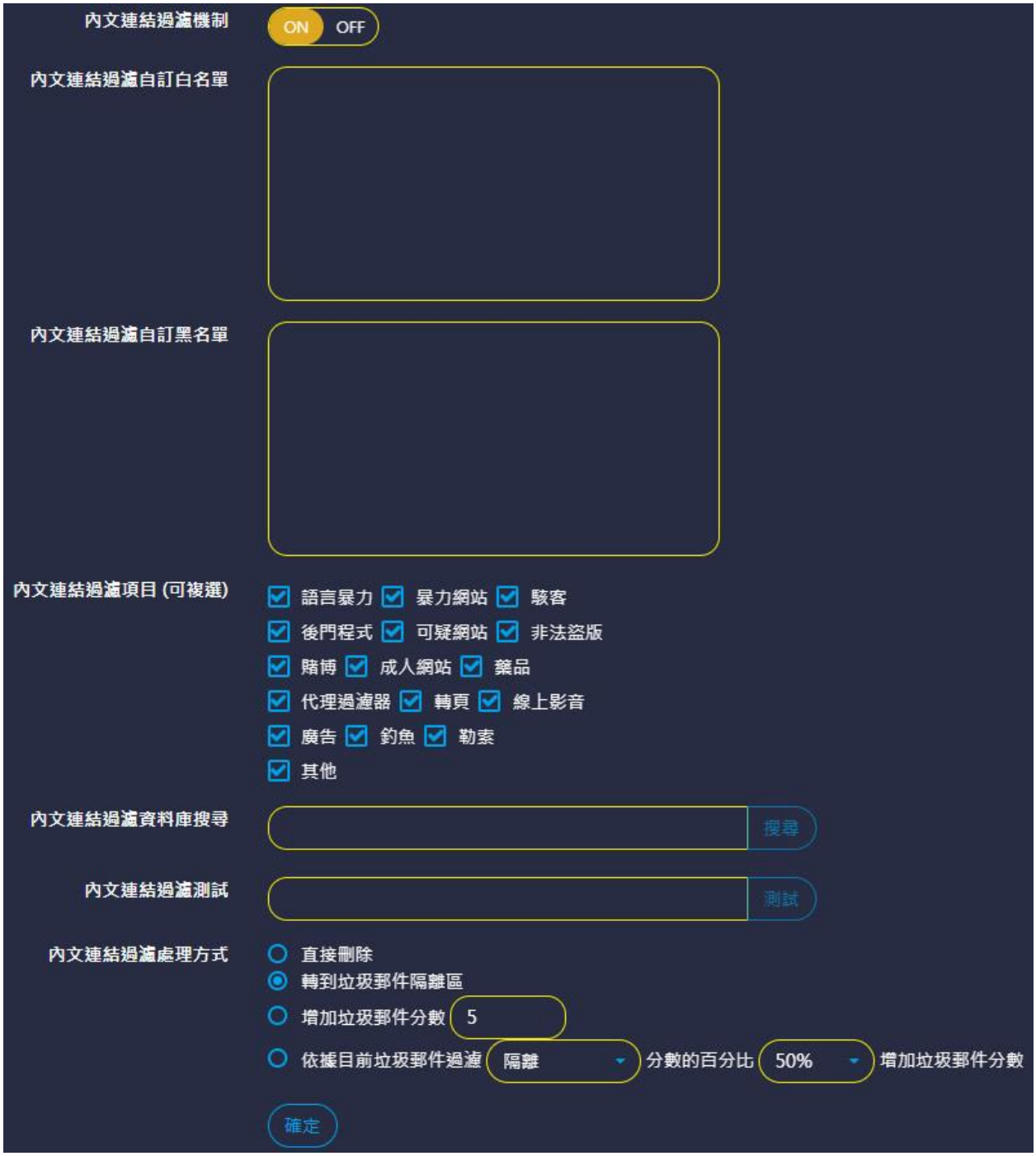


圖 11-6、內文 URL 過濾

- 【內文連結過濾自訂白名單】：避免誤判下，自定義白名單 IP 及網域。
- 【內文連結過濾自訂黑名單】：自定義黑名單 IP 及網域。
- 【內文連結過濾機制】：要不要啟用這項服務，建議啟用增加垃圾郵件判斷的準確度。

- 【內文連結過濾項目(可複選)】：郵件內文要檢查的 URL 資料庫，可以選擇檢查特定 URL 資料庫或是全選。
- 【內文連結過濾資料庫搜尋】：判斷某個 URL 是否已經被歸類在 URL 資料庫中，輸入後按搜尋按鍵，系統就會回報結果。
- 【內文連結過濾處理方式】：對於符合 URL 黑名單資料庫的郵件處理方式，有下列數種選項：

  1、直接刪除。

  2、轉到垃圾郵件隔離區。

  3、增加垃圾郵件分數。

  4、依據目前垃圾郵件過濾機制，再增加特定比例的垃圾分數，例如，隔離區的分數是 10 分，當有符合 URL 黑名單的郵件時，他會再增加 10 乘以設定的百分比的垃圾郵件判斷分數。

11-3、垃圾郵件通知清單設定

當管理者將【垃圾郵件】>【基本設定】中，垃圾郵件處理方式，選擇垃圾郵件在隔離區並發送清單，啟動時，郵件伺服器會將被判斷為垃圾郵件的郵件放入隔離區。

在隔離區的郵件如何讓管理者或使用者知道，透過寄發垃圾郵件清單的方式告知使用者與管理者，系統將累積在隔離區的垃圾郵件，以清單列表的方式通知原收件者。

(一)、管理者垃圾郵件清單

管理者垃圾隔離清單預設是關閉。(圖 11-7)

圖 11-7、管理者垃圾清單

- 【管理者垃圾郵件清單】：預設是關閉，啟用後，系統會將所有被垃圾郵件引擎判斷為垃圾的郵件，以表列清單的方式寄給指定的收件者，這些收件者必須有管理者權限，如果在設定的時間內沒有任何垃圾郵件，則這垃圾郵件清單將不會發送。
- 【傳送時間】: 2 種設定模式，一個是指定時間另一個是設定間隔時間後週期性的發送，當有垃圾郵件且在表定的時間內，系統就會發送出這些通知清單郵件，設定間隔時間格式以

天(d)/小時(h)/分，其中 d 及 h 分別是 day 跟 hour 的代表符號，例如，2h/30 代表 2 小時 30 分，每 2 小時 30 分會傳送通知信。

- 【垃圾郵件清單的主旨】：發出垃圾郵件通知信的主旨，例如，Spam Mail List。
- 【接收垃圾郵件清單的管理者】：點選後就可以選擇要收到通知郵件的管理者帳號。這些帳號都是預先建立在使用者群組中，且具有管理者權限者。

(二)、使用者垃圾郵件清單

要不要讓使用者收到垃圾郵件清單。(圖 11-8)

圖 11-8、使用者垃圾郵件清單

- 【使用者垃圾郵件清單】：預設是關閉，啟用後，系統會將所有被判斷成垃圾的郵件，以清單的方式寄給原本的收件者，如果在設定的時間內沒有任何垃圾郵件，則這封清單郵件將不會發送。
- 【傳送時間】: 2 種設定模式，一個是指定時間另一個是設定間隔時間後週期性的發送，當有垃圾郵件且在表定的時間內，系統就會發送出這些通知清單郵件，設定間隔時間格式以天(d)/小時(h)/分，其中 d 及 h 分別是 day 跟 hour 的代表符號，例如，2h/30 代表 2 小時 30 分，每 2 小時 30 分會傳送通知信。
- 【垃圾郵件清單的主旨】：發出垃圾郵件清單通知信的主旨，例如，Spam Mail List。
- 【不接收垃圾郵件清單者】：點選後就可以選擇不要收到通知郵件的使用者帳號，除了這一些指定不接收者不會收到外，其他垃圾郵件的收件者都會收到通知郵件，空白代表所有垃圾郵件的收件者都會收到通知信。

11-4、垃圾郵件自動學習

垃圾郵件過濾機制除了使用垃圾郵件過濾引擎來判別垃圾郵件外，為了增加垃圾郵件判斷率，可在設定垃圾郵件學習機制，這個機制會在郵件歸檔伺服器中建立一個學習資料庫，定期的學習新的垃圾郵件特徵值。除了自動學習外，也可以設定系統的黑白名單跟個人的黑白名單，增加判斷率跟降低誤判率。

在垃圾信學習機制上，設計成 2 個郵件帳號，黑名單學習帳號、白名單學習帳號，一旦使用者認為他的正常郵件被郵件伺服器誤判，則可以將被誤判的郵件寄到白名單學習帳號，相反地，如果垃圾郵件沒有被過濾機制判斷出來，將這封信轉寄到黑名單學習帳號。

下一次，同一個寄件者寄來的郵件，就不會被誤判，注意郵件要用單封轉寄，不能使用群組或是夾檔轉寄否則會無法學習。(圖 11-9)

圖 11-9、使用者垃圾郵件清單

- 【定時自動學習】：垃圾信的學習機制要不要啟動，啟動後郵件伺服器就會定時地在時間內，將黑名單學習帳號、白名單學習帳號的郵件匯入垃圾信學習資料庫中。
- 【垃圾信多久學習一次】：設定多久時間跟學習帳號自動學習，設定間隔時間格式以天(d)/小時(h)/分，其中 d 及 h 分別是 day 跟 hour 的代表符號，例如，2h/30 代表 2 小時 30 分，也可以按【立即學習】按鍵，將黑名單學習帳號、白名單學習帳號的郵件匯入垃圾信學習資料庫中。

學習紀錄

按下垃圾郵件的【學習紀錄】按鍵，會顯示黑名單學習帳號、白名單學習帳號的郵件匯入垃圾信學習資料庫中的所有學習紀錄，包含學習的總筆數、學習日期、從幾封信中學習到幾筆資料。(圖 11-10)。

圖 11-10、學習記錄

- 【黑名單總學習筆數】：目前黑名單學習的筆數。
- 【白名單總學習筆數】：目前白名單學習的筆數。
- 【垃圾信學習資料庫】：對於垃圾郵件學習資料庫的學習資料，管理者可以將它匯出或是匯入。

11-5、黑白名單設定

黑白名單分成 2 個部分，系統黑白名單跟個人黑白名單，系統的黑白名單適用於全部的收件者，管理者可針對垃圾郵件的運作狀況，增減這些黑白名單，讓整體的垃圾郵件判斷率增加並降低誤判率。

(一)、系統黑白名單

對某些特定寄件者的郵件，直接把它歸類為垃圾郵件(黑名單)或是正常郵件(白名單)，這就是系統黑白名單的主要功能，建置完成的資料可以匯出儲存，也可以將之前備份的資料匯入新的系統中，(圖 11-11)。

圖 11-11、系統黑白名單

- 【名稱】：輸入方便辨識的名稱，例如，系統黑名單。
- 【加入的帳號】：輸入要加入黑名單的帳號，可以使用萬用字，如 “*” 等，例如，black.list@abc.com。
- 【黑/白名單】：選擇黑白名單，當選擇設定為黑名單時，需要再選擇黑名單的處理方式。

■ 【黑名單處理方式】：針對黑名單寄來的郵件，如何處理，目前有 4 種處理方式。

1、不歸檔：郵件不進入歸檔資料庫。

2、主旨提示文字：在主旨前面加入特定文字，例如，[spam-mail]。

3、轉到隔離區：轉到垃圾郵件隔離區，再根據設定值要不要發送垃圾郵件清單給收件者。

4、直接刪除：放到垃圾郵件刪除區，在特定時間內管理者沒進來取回，系統會自動清除。

目前黑名單學習的筆數。

匯入/匯出黑名單

郵件伺歸檔服器也會提供黑名單檔案的匯入、匯出，管理者可以將平常收集的黑名單資料庫收集下來，必要時將這個檔案上傳即可。

匯入/匯出白名單

郵件歸檔伺服器也會提供白名單檔案的匯入、匯出，管理者可以將平常收集的白名單資料庫收集下來，必要時將這個檔案上傳即可。

(二)、個人黑白名單

對某些特定寄件者的郵件，使用者直接把它歸類為垃圾郵件(黑名單)或是正常郵件(白名單)，這就是個人黑白名單的主要功能，建置完成的資料可以匯出儲存，也可以將之前備份的資料匯入新的系統中，(圖 11-11)。

圖 11-11、系統黑白名單

- 【使用者】：挑選一個要加入個人黑白名單的帳號。
- 【黑名單】：輸入要加入黑名單的帳號，每行一筆帳號，可以使用萬用字，如 “*” 等，例如，black.list@abc.com。

- 【黑名單處理方式】：針對黑名單寄來的郵件，如何處理，目前有 3 種處理方式。

  1、主旨提示文字：在主旨前面加入特定文字，例如，[spam-mail]。

  2、轉到隔離區：轉到垃圾郵件隔離區，再根據設定值要不要發送垃圾郵件清單給收件者。

  3、直接刪除：放到垃圾郵件刪除區，在特定時間內管理者沒進來取回，系統會自動清除。

  目前黑名單學習的筆數。

- 【白名單】：輸入要加入白名單的帳號，每行一筆帳號，可以使用萬用字，如 “*” 等，例如，white.list@xyz.com。

  匯入/匯出黑名單

  郵件歸檔伺服器也會提供黑名單檔案的匯入、匯出，管理者可以將平常收集的黑名單資料庫收集下來，必要時將這個檔案上傳即可。

  匯入/匯出白名單

  郵件歸檔伺服器也會提供白名單檔案的匯入、匯出，管理者可以將平常收集的白名單資料庫收集下來，必要時將這個檔案上傳即可。

11-6、垃圾郵件防護

郵件歸檔伺服器除了標準的垃圾郵件辨識引擎、共享垃圾郵件機制還有進階的垃圾郵件防護，無非就是想把郵件檔在外部，進階的垃圾郵件防護目前有 4 種機制，分別是 SPF 驗證、灰名單、DKIM 驗證及 IP 位址反解驗證等。

(一)、SPF 驗證

郵件歸檔伺服器收到寄件者的寄信請求後，去驗證對方的郵件伺服器的 SPF 紀錄是否合法，確定他是否為該網域合法的寄件者寄出的郵件。(圖 11-12)。

圖 11-12、SPF 設定

- 【SPF 驗證功能】：啟用 SPF 驗證機制。
- 【合法來源】：對方郵件伺服器的 SPF 紀錄驗證完全符合正常格式，從它寄來的郵件通常會認為是正常郵件。處理的方式有 2 種：

◆ 不做處理：不增減垃圾郵件分數。

◆ 減少垃圾郵件分數：減少分數，讓這類型的郵件確定少於垃圾郵件分數。

■ 【來源可能有風險】：對方郵件伺服器的 SPF 紀錄驗證”不”完全符合正常格式，從它寄來的郵件通常會認為是有一些風險，疑似垃圾郵件，處理的方式下列方式：

◆ 不做處理：不增減垃圾郵件分數。

◆ 直接刪除：將這類型的郵件直接刪除掉。

◆ 轉到垃圾郵件隔離區：將這類型的郵件放在垃圾郵件隔離區。

◆ 增加垃圾郵件分數：增加分數，讓這類型的郵件有比較高的機率高於垃圾郵件分數。

◆ 附加主旨提示文字：這類型郵件的主旨加入特定文字，讓使用者收到後容易判斷是否為垃圾郵件。

■ 【非法來源】：對方郵件伺服器的 SPF 紀錄驗證”偽造”正常格式，從它寄來的郵件通常會認為有很大機率有問題，處理的方式下列方式：

◆ 不做處理：不增減垃圾郵件分數。

◆ 直接刪除：將這類型的郵件直接刪除掉。

◆ 轉到垃圾郵件隔離區：將這類型的郵件放在垃圾郵件隔離區。

◆ 增加垃圾郵件分數：增加分數，讓這類型的郵件有比較高的機率高於垃圾郵件分數。

◆ 附加主旨提示文字：這類型郵件的主旨加入特定文字，讓使用者收到後容易判斷是否為垃圾郵件。

■ 【無效 SPF 紀錄】：對方郵件伺服器的 SPF 紀錄無效，從它寄來的郵件通常會是垃圾郵件，處理的方式下列方式：

◆ 不做處理：不增減垃圾郵件分數。

◆ 增加垃圾郵件分數：增加分數，讓這類型的郵件有比較高的機率高於垃圾郵件分數。

■ 【信任寄件者】：輸入信任的寄件者或是網域，例如，freedy@example.com，*@example.com，這些來源的寄件者就不執行 SPF 紀錄檢查。

■ 【信任 IP】：輸入信任的 IP 位址，例如，192.168.188.254/24，從這一些來源 IP 的郵件不執行 SPF 紀錄檢查。

(二)、灰名單

郵件歸檔伺服器收到每個寄件者的寄信請求後，第一次會拒絕連線，當對方的郵件伺服器再次嘗試寄信時，第二次就會接受它的寄信請求，這就是灰名單防護的機制。(圖 11-13)。

圖 11-13、灰名單設定

- 【灰名單功能】：啟用 灰名單 驗證機制。
- 【略過灰名單】：當對方的郵件伺服器有完整的 SPF 紀錄時，就不執行灰名單機制。
- 【收信延遲時間】：當對方的郵件伺服器在這個時間後再重新寄信，歸檔伺服器就會把它收下來，並把這一個郵件伺服器的紀錄下來，下次從這個郵件伺服器寄來的郵件，就不會再進入灰名單的機制中，預設值是 60 秒。
- 【信任寄件者】：輸入信任的寄件者或是網域，例如，freedy@example.com，*@example.com，這些來源的寄件者就不執行灰名單檢查。
- 【信任 IP】：輸入信任的 IP 位址，例如，192.168.188.254/24，從這一些來源 IP 的郵件不執行灰名單檢查。

(三)、DKIM 驗證

郵件歸檔伺服器收到寄件者的寄信請求後，去驗證對方的郵件伺服器的 DKIM (Domain Key Identified Mail) 是否合法，確定他是否為該網域合法的寄件者寄出的郵件。(圖 11-14)。

圖 11-14、DKIM 設定

- 【DKIM 驗證功能】：啟用 DKIM 驗證機制。
- 【合法來源】：對方郵件伺服器的 DKIM 紀錄驗證完全符合正常格式，從它寄來的郵件通常會認為是正常郵件。處理的方式有 2 種：
  - ◆ 不做處理：不增減垃圾郵件分數。
  - ◆ 減少垃圾郵件分數：減少分數，讓這類型的郵件確定少於垃圾郵件分數。

- 【來源可能有風險】：對方郵件伺服器的 DKIM 紀錄驗證”不”完全符合正常格式，從它寄來的郵件通常會認為是有一些風險，疑似垃圾郵件，處理的方式下列方式：
  - ◆ 不做處理：不增減垃圾郵件分數。
  - ◆ 直接刪除：將這類型的郵件直接刪除掉。
  - ◆ 轉到垃圾郵件隔離區：將這類型的郵件放在垃圾郵件隔離區。
  - ◆ 增加垃圾郵件分數：增加分數，讓這類型的郵件有比較高的機率高於垃圾郵件分數。
  - ◆ 附加主旨提示文字：這類型郵件的主旨加入特定文字，讓使用者收到後容易判斷是否為垃圾郵件。
- 【非法來源】：對方郵件伺服器的 DKIM 紀錄驗證”偽造”正常格式，從它寄來的郵件通常會認為有很大機率有問題，處理的方式下列方式：
  - ◆ 不做處理：不增減垃圾郵件分數。
  - ◆ 直接刪除：將這類型的郵件直接刪除掉。
  - ◆ 轉到垃圾郵件隔離區：將這類型的郵件放在垃圾郵件隔離區。
  - ◆ 增加垃圾郵件分數：增加分數，讓這類型的郵件有比較高的機率高於垃圾郵件分數。
  - ◆ 附加主旨提示文字：這類型郵件的主旨加入特定文字，讓使用者收到後容易判斷是否為垃圾郵件。
- 【信任寄件者】：輸入信任的寄件者或是網域，例如，freedy@example.com，*@example.com，這些來源的寄件者就不執行 SPF 紀錄檢查。
- 【信任 IP】：輸入信任的 IP 位址，例如，192.168.188.254/24，從這一些來源 IP 的郵件不執行 SPF 紀錄檢查。

(四)、IP 位址反解認證

郵件歸檔伺服器收到每個寄件者的寄信請求後，會用寄件者的來源 IP 位址，檢查是否有完整的反解名稱。

以下列的範例說明，當寄件者從 220.142.2.128 寄一封信給郵件伺服器時，IP 位址反解機制會去驗證這一個 IP 位址是否有作反解，220-142-2-128.dynamic-ip.hinet.net 就是這 IP 的反解，相反地如果沒有作反解，查詢的結果就如 220.142.2.128 這樣。(圖 11-15)

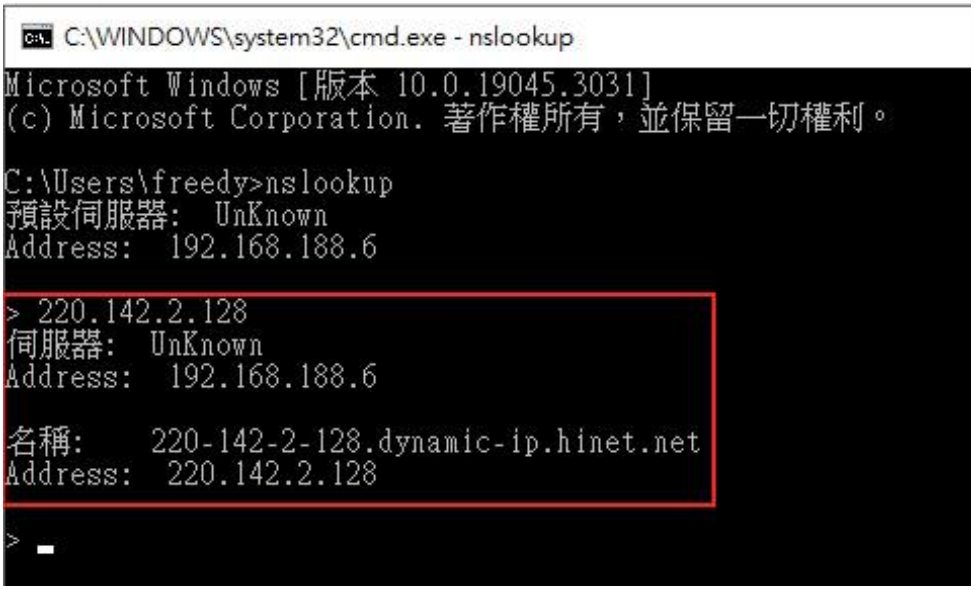


圖 11-15、IP 位址反解說明

IP 位址反解可以確認郵件伺服器的 IP 位址是正常的。(圖 11-16)。

圖 11-16、IP 位址反解設定

- 【IP 位址反解驗證功能】：啟用 IP 位址反解 驗證機制。
- 【未通過驗證處理方式】：當對方的郵件伺服器 IP 位址沒有做 IP 位址反解它的處理方式。
  - ◆ 直接刪除：將這類型的郵件直接刪除掉。
  - ◆ 轉到垃圾郵件隔離區：將這類型的郵件放在垃圾郵件隔離區。
  - ◆ 增加垃圾郵件分數：增加分數，讓這類型的郵件有比較高的機率高於垃圾郵件分數。
- 【信任 IP】：輸入信任的 IP 位址，例如，192.168.168.254/24，從這一些來源 IP 的郵件不執行灰名單檢查。

第 12 章 日誌查詢

郵件歸檔伺服器有關的日誌，包含郵件日誌、垃圾信的隔離區跟系統登入等，都在這個選單中顯示跟列表，管理者可以藉由搜尋動作，追蹤郵件的進出狀況，使用量，進一步掌握郵件歸檔伺服器運作的情況。

12-1、郵件日誌

郵件日誌是管理者查詢進、出郵件的最主要地方，舉凡所有經過郵件歸檔伺服器的郵件處置情況，都會在這裡呈現，當管理者要找尋使用者的郵件問題，也可以在這裡找到原因。

(一)、搜尋郵件日誌

郵件日誌的搜尋條件有 2 種，基本搜尋跟進階搜尋，管理畫面預設是顯示基本搜尋，如果不足，可以再開啟進階搜尋，讓搜尋的目標縮小。

基本搜尋條件

郵件歸檔伺服器傳送、接收郵件的筆數相當多，使用搜尋的功能，尋找特定的郵件，加快搜尋速度，搜尋的條件如下（圖 12-1）。

圖 12-1、基本搜尋條件

- 【開始時間】：填入要查詢的開始日期、時間。
- 【結束時間】：填入要查詢的結束日期、時間。
- 【通聯寄件者】：查詢目標郵件的寄件者。.
- 【收件者】：查詢目標郵件的收件者。
- 【郵件主旨】：要查詢郵件的主旨，可用萬用字元 * 。
- 【來源 IP】：寄件者的來源 IP 位址。

進階搜尋條件

當基本搜尋條件無法滿足管理者的查詢需求時，點選  的按鍵後，就進入進階搜尋的介面，進階部分大概可以分成 2 個部分，郵件本身跟處置行為的搜尋，郵件本身說明如下：(圖 12-2)

圖 12-2、進階搜尋—郵件本體

- 【開始時間】：填入要查詢的開始日期、時間。
- 【結束時間】：填入要查詢的結束日期、時間。
- 【通聯寄件者】：查詢目標郵件的寄件者。
- 【收件者】：查詢目標郵件的收件者。
- 【郵件主旨】：要查詢郵件的主旨，可用萬用字元 * 。
- 【來源 IP】：寄件者的來源 IP 位址。
- 【目的 IP】：收件者的 IP 位址。
- 【內文寄件者】：郵件內文的寄件者。
- 【郵件大小 KB】：查詢目標郵件的容量大小範圍，以 KB 為單位。
- 【附件名稱】：查詢特定檔案名稱。

進階搜尋—郵件處置（圖 12-3）

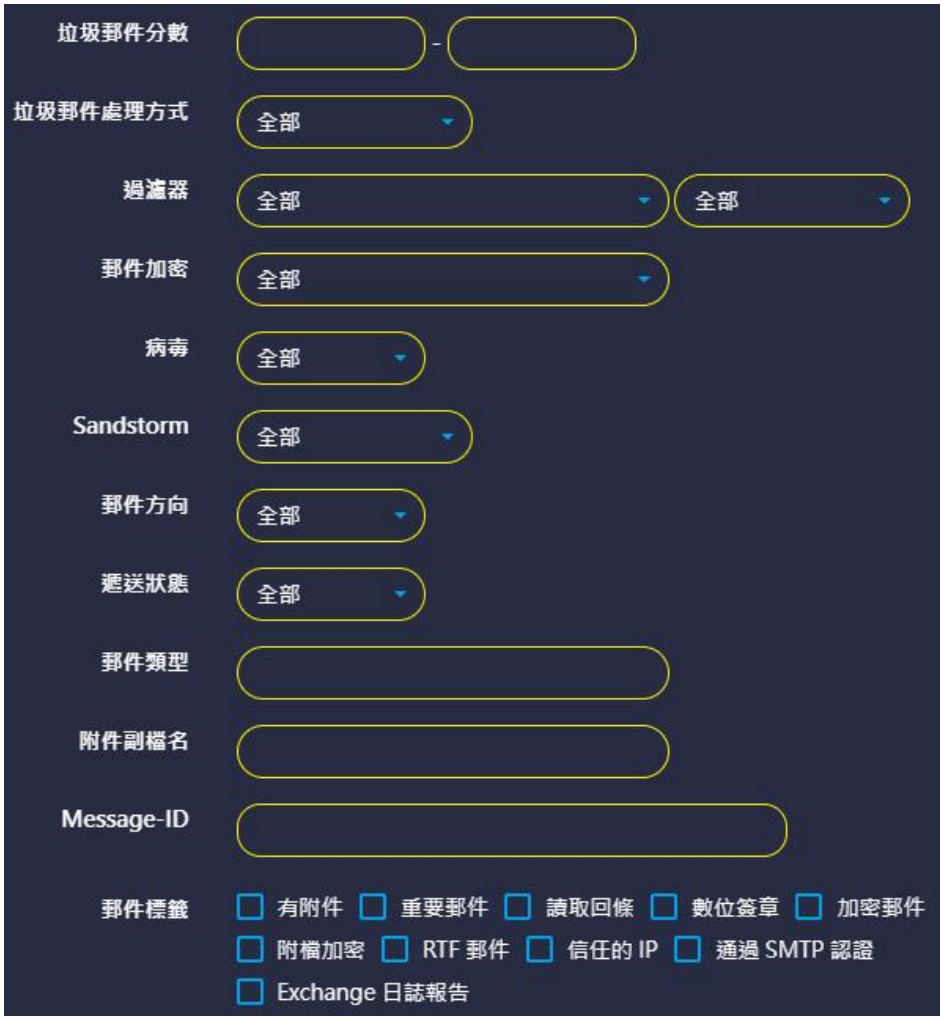


圖 12-3、進階搜尋—處置行為

- 【垃圾郵件分數】：垃圾郵件過濾機制評分的判斷分數範圍。
- 【垃圾郵件處理方式】：經過垃圾郵件過濾機制後，系統的處置方式，共有全部、正常信件、隔離、刪除、垃圾主旨及沒有掃描等。
- 【過濾器】：查詢的郵件是否有被設定的過濾器出發過，觸發後的處置行為是隔離、刪除跟稽核的哪一種或是全部。
- 【病毒】：查詢的郵件是否帶有病毒、被隔離或是根本沒掃描過。
- 【郵件方向】：在閘道器模式下，查詢的郵件方向，有內對內、內對外或是外對內。
- 【郵件類型】：查詢的郵件是在透通或是 POP3 代收模式下被記錄的。
- 【附件附檔名】：查詢檔案的副檔名，例如，pdf、dat 等。
- 【郵件標籤】：查詢郵件是否有被系統加入標籤，藉由標籤的選擇，更容易找到特定的郵件。

(二)、郵件列表

所有進出郵件歸檔伺服器的郵件都會在這裡顯示，除了基本的時間、寄件者 IP 帳號及主旨外，郵件經過系統的垃圾郵件、病毒掃描引擎及過濾器的處置動作，都可以在列表中看到。(圖 12-4)

	來源 IP	目的 IP	寄件者	收件者	郵件主旨	大小			分數	類型		處理		
06-09 13:29	175.156.72.7	192.168.168.168	utriukpa@soxl.com	freedy@herhsiang.co...	Canadian Online Pharmacy	783 B	拒絕		30.96	透通		刪除		
06-09 13:06	220.130.227.122	192.168.168.168	acex@acexma.com	freedy@herhsiang.co...	客戶郵件被退回	732.0 KB	接受	-	0.04	透通		-		
06-09 12:40	2.56.58.79	192.168.168.168	qwjyhdaove@a.kjmvb...	freedy@herhsiang.co...	Louis Vuitton Bags Up To 90...	1.8 KB	拒絕		46.79	透通		刪除		
06-09 12:32	185.255.8.48	192.168.168.168	member@event.myca...	freedy@herhsiang.co...	?【開信領15元現金券】剩餘.....	54.1 KB	接受		-0.84	透通		-		
06-09 12:20	59.124.97.230	192.168.168.168	return.eid5e2b1e20.fr...	freedy@herhsiang.com	?618年中大促，破億回饋滴一咖	70.5 KB	接受		1.14	透通		-		
06-09 12:12	192.168.168.111	192.168.168.168	freedy@herhsiang.co...	freedy@herhsiang.co...		0 B	其他	-	0	透通		-		
06-09 12:12	192.168.168.111	192.168.168.168	freedy@herhsiang.co...	freedy@herhsiang.co...	Microsoft Outlook 測試郵件	1022 B	接受	-		透通		-		
06-09 12:05	209.85.166.42	192.168.168.168	freedy.yang+caf_=free...	freedy@herhsiang.com	tttt	25.9 KB	拒絕			透通		刪除		
06-09 12:03	118.163.243.20	192.168.168.168	root@mail.oceankarw...	freedy@herhsiang.co...	Successful mirror disk at 202...	1.1 KB	接受	-	0	透通		-		
06-09 11:19	210.71.218.38	192.168.168.168	webmail@ecfscop.epa...	freedy@herhsiang.com	SteelSeries | 56折起送3%P幣...	5.7 KB	接受		11.99	透通		更名		

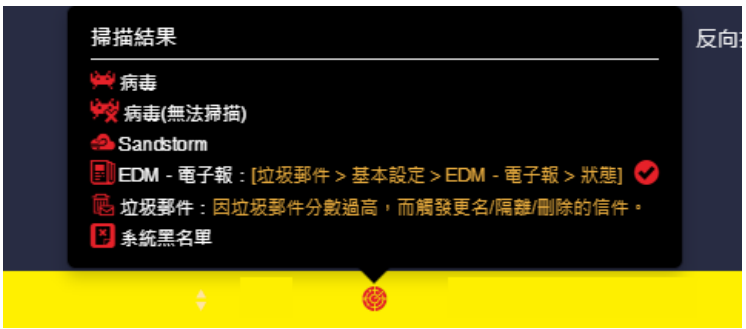
圖 12-4、郵件列表

- 【寄件者】：寄件者的郵件帳號。
- 【收件者】：此封郵件的收件者。
- 【郵件主旨】：郵件的主旨。
- 【大小】：列表郵件的容量。
- 【 】：郵件經過系統後的後續處置狀況，共有 3 種狀況，成功、接受跟拒絕。

  成功：代表郵件從內部成功寄給外部的收件者。

  接受：代表郵件從外部接收完成，還是要經過垃圾郵件、病毒及稽核過濾器後才能正常的進入收件者郵箱中。

  拒絕：外部要進來的郵件，被系統拒絕。

- 【 

】：掃描結果列表，以圖示  代表此封郵件事有病毒。
- 【分數】：列表郵件經過垃圾郵件引擎判斷後的分數。
- 【類型】：列表的郵件是經由哪一種模式收下來，透通模式還是 POP3 代收模式。

- 【 】：列表郵件進出系統 A 的方向，代表從外面到內部郵件伺服器，代表從內部寄到外面的收件者。
- 【處理】：列表郵件經過系統後，系統如何處理，是隔離、刪除還是放行？
- 【 】：列表郵件是否有被歸檔，代表被歸檔，日後使用者可以查詢此封郵件，代表此封郵件沒被歸檔，代表重複的郵件，系統只會歸檔其中一封。
- 【 】：列表郵件的詳細內容，點選每一封列表的郵件這個圖示後，就會詳細列出此封郵件的所有資料，包含 SMTP 通聯狀況、過濾器、垃圾病毒判斷及郵件主旨等詳細的資訊，方便管理者判讀。（圖 12-5）

圖 12-5、郵件的詳細資料

在詳細資料中有主機收件通訊過程這一個項目，他會詳細列出雙方 SMTP 通聯過程，讓管理者方便判斷原因。(圖 12-6)

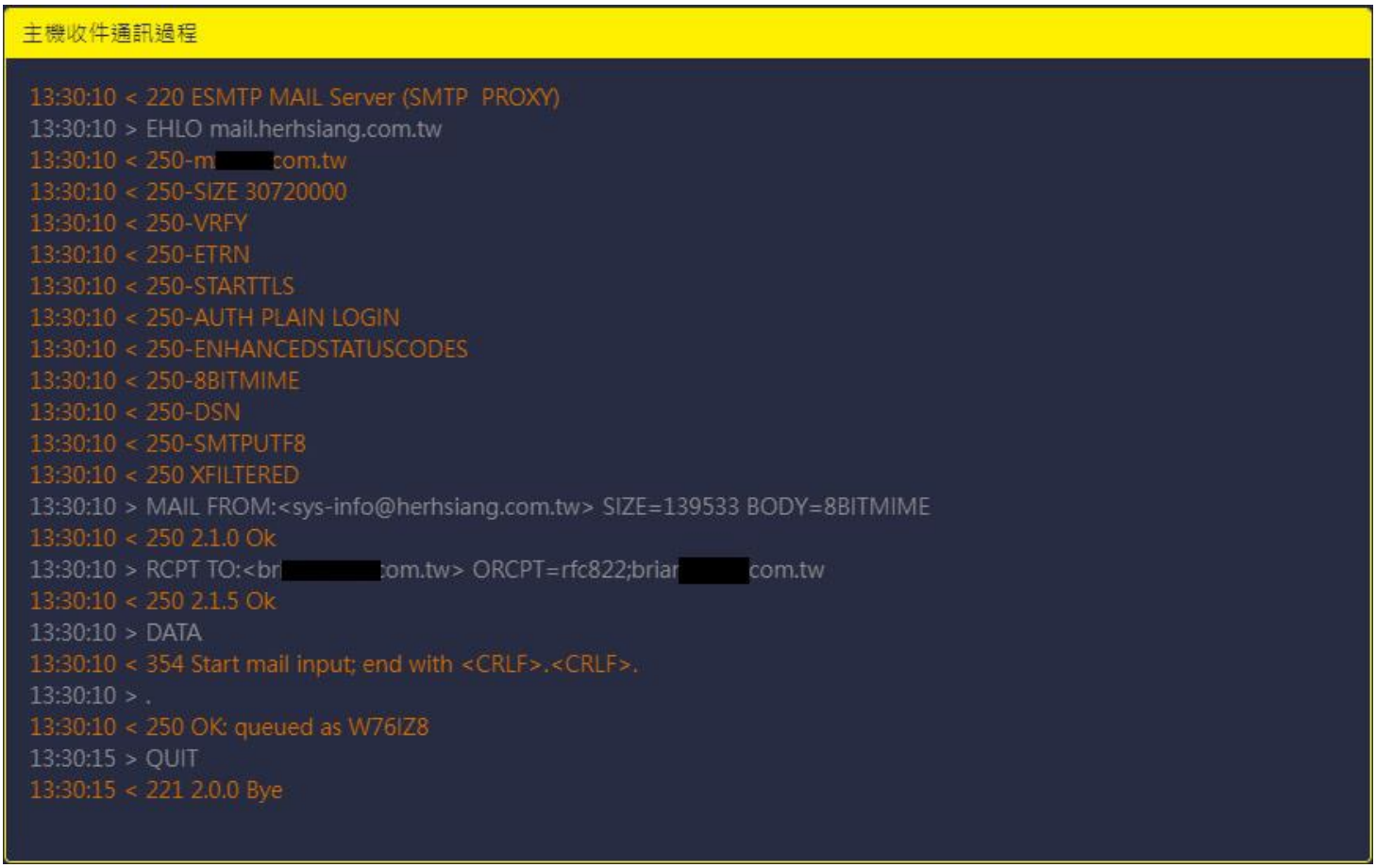


圖 12-6、SMTP 通聯資料

10-2、隔離及封鎖日誌

(一)、隔離日誌

所有被郵件歸檔伺服器隔離的郵件，通通會列表在此，管理者可以搜尋或是查看郵件被隔離的原因。跟郵件日誌一樣，搜尋時分基本搜尋及進階搜尋，詳細的動作請參考郵件日誌的搜尋部分。

郵件列表

所有進出被隔離的郵件都會在這裡顯示，除了基本的時間、寄件者 IP 帳號及主旨外，郵件是因為觸發哪一個條件才被隔離，例如，被垃圾過濾引擎隔離還是被病毒隔離等，可以在列表中看到。(圖 12-7)

圖 12-7、郵件列表

- 【寄件者】：寄件者的郵件帳號。
- 【收件者】：此封郵件的收件者。
- 【郵件主旨】：郵件的主旨。
- 【大小】：列表郵件的容量。
- 【隔離類型】：郵件是觸發哪一個隔離機制。
- 【  】：列表郵件的詳細內容，點選每一封列表的郵件這個圖示後，就會詳細列出此封郵件的所有資料，包含 SMTP 通聯狀況、過濾器、垃圾病毒判斷及郵件主旨等詳細的資訊，方便管理者判讀，可以參考 (圖 12-5) 。

(二)、封鎖日誌

封鎖日誌的搜尋條件有 2 種，基本搜尋跟進階搜尋，管理畫面預設是顯示基本搜尋，如果不足，可以再開啟進階搜尋，讓搜尋的目標縮小。

基本搜尋條件

郵件歸檔伺服器使用搜尋的功能，尋找特定的郵件，加快搜尋速度，搜尋的條件如下（圖 12-8）。

圖 12-8、基本搜尋條件

- 【開始時間】：填入要查詢的開始日期、時間。
- 【結束時間】：填入要查詢的結束日期、時間。
- 【封鎖類型】：有 3 種封鎖機制，分別是 SMTP 認證漏洞、過濾器跟異常寄送偵測。
- 【來源 IP】：寄件者的來源 IP 位址。
- 【狀態】：查詢封鎖 IP 位址目前的狀態，共有 5 種，封鎖、解除封鎖、永久封鎖、暫時封鎖跟留意。

進階搜尋條件

當基本搜尋條件無法滿足管理者的查詢需求時，點選  的按鍵後，就進入進階搜尋的介面。(圖 12-9)

圖 12-9、封鎖日誌進階搜尋

- 【開始時間】：填入要查詢的開始日期、時間。
- 【結束時間】：填入要查詢的結束日期、時間。
- 【封鎖類型】：有 3 種封鎖機制，分別是 SMTP 認證漏洞、過濾器跟異常寄送偵測。
- 【狀態】：查詢封鎖 IP 位址目前的狀態，共有 5 種，封鎖、解除封鎖、永久封鎖、暫時封鎖跟留意。
- 【來源 IP】：寄件者的來源 IP 位址。
- 【寄件者】：查詢被封鎖的寄件者。
- 【認證帳號】：查詢被封鎖的 SMTP 認證帳號。
- 【封鎖次數】：以封鎖次數為搜尋條件。

10-3、使用紀錄

每個登入郵件歸檔伺服器的管理者他在系統上所有的操作，都會被詳細的紀錄下來，包含系統自動到網路上自動更新病毒碼，他也會記錄下來。

紀錄列表

所有進出的管理者做的行為，都可以在列表中獲得初步的結果。(圖 12-10)

時間	使用者	登入 IP	功能	事件	狀態	
06-09 14:47:19	admin	192.168.168.111	系統認證	登入	正常	
06-09 14:47:13	herhsiang	192.168.168.111	系統認證	登入	錯誤	
06-09 14:47:13	herhsiang	192.168.168.111	系統認證	使用者不存在	錯誤	
06-09 14:41:45	SYSTEM		郵件病毒 > 掃毒設定	ClamAV 自動更新	正常	
06-09 14:17:50	admin	192.168.168.111	日誌查詢 > 封鎖日誌	解除 IP 封鎖	正常	
06-09 14:17:45	admin	192.168.168.111	日誌查詢 > 封鎖日誌	解除 IP 封鎖	正常	
06-09 14:17:40	admin	192.168.168.111	日誌查詢 > 封鎖日誌	解除 IP 封鎖	正常	
06-09 14:17:23	admin	192.168.168.111	郵件稽核及防護 > 郵件防火牆	儲存	正常	
06-09 13:55:26	admin	192.168.168.111	垃圾郵件 > 垃圾郵件防護	基本設定	正常	
06-09 13:39:45	SYSTEM		系統通知 > 系統訊息通知	訊息通知狀態	正常	

圖 12-10、管理者使用紀錄列表

- 【時間】：使用紀錄的時間。
- 【使用者】：哪一個管理者做的動作，如果是系統去執行的則會標示 SYSTEM，例如，病毒碼自動更新這個動作就是由系統去執行。
- 【登入 IP】：管理者用哪一個 IP 登入系統，如果是 SYSTEM，則不會顯示 IP 位址。
- 【功能】：管理者執行的項目及路徑。
- 【事件】：管理者執行的動作。
- 【狀態】：管理者的這項操作是否正常或是失敗。
- 【功能】：管理者執行的項目。

- 【  】：列表動作的詳細內容，點選每一封列表的動作這個圖示後，就會詳細列出此封郵件的所有資料，如果是管理者做的，則不會有這個圖示。（圖 12-11）

圖 12-11、管理者詳細使用紀錄

基本搜尋條件

郵件歸檔伺服器管理者使用搜尋的功能，尋找特定的內容，加快搜尋速度，搜尋的條件如下（圖 12-12）。

圖 12-12、使用紀錄基本搜尋條件

- 【開始時間】：填入要查詢的開始日期、時間。
- 【結束時間】：填入要查詢的結束日期、時間。
- 【使用者】：搜尋的對象，也可以自行輸入帳號。
- 【登入 IP】：使用者的登入 IP 位址。
- 【狀態內容關鍵字】：管理者動作的關鍵字，例如，登入，則只會出現所有登入的紀錄。

進階搜尋條件

當基本搜尋條件無法滿足管理者的查詢需求時，點選  的按鍵後，就進入進階搜尋的介面。(圖 12-13)

圖 12-13、使用紀錄進階搜尋

- 【開始時間】：填入要查詢的開始日期、時間。
- 【結束時間】：填入要查詢的結束日期、時間。
- 【使用者】：搜尋的對象，也可以自行輸入帳號。
- 【登入 IP】：使用者的登入 IP 位址。
- 【狀態內容關鍵字】：管理者動作的關鍵字，例如，登入，則只會出現所有登入的紀錄。
- 【主功能/次功能】：查詢動作是在哪一個功能。

第 13 章 系統狀態

郵件歸檔伺服器會將系統的資源使用狀況及服務流量等資訊紀錄下來，方便管理者查詢過去某個特定時間的資源使用狀況或是流量圖，一般來說，資源使用部分會記錄 CPU、記憶體、系統負荷及硬碟 IO 等，在網路服務流量部分會把 SMTP/SMTPS 及管理介面的流量記錄下來，同時以圖表的方式顯示，管理者可以依照時間搜尋特定時間的訊息。

(一)、設定時間

系統預設會顯示的統計圖形是從現在起往回到 24 小時，管理者可以更改顯示的時間區段，藉以找出關鍵的時間點。(圖 13-1)

圖 13-1、系統狀態圖搜尋

- 【開始時間】：填入要查詢的開始日期、時間。
- 【結束時間】：填入要查詢的結束日期、時間。
- 【系統項目】：選擇圖形要顯示的資料，共有 CPU 及負載、Memory/Swap、網卡流量、及硬碟的讀寫速度。
- 【服務項目】：選擇圖形要顯示的服務，有 SMTP/SMTPS 的流量，管理/查詢介面流量等。

(二)、CPU 負載圖

當滑鼠移到圖形中，會進一步顯示這個時間點的詳細資訊，以（圖 13-2）為例，在 6 月 9 日 00:01:40 時，CPU 使用 8.58%，系統平均負載為 0.24，前 5 名佔用 CPU 資源的分別是 mail process、spam process、httd、HA 及 sql，其中 System 是郵件歸檔郵件處理模組的運作程序。

有了這些資訊，管理者就非常容易找出過去的某個特定時間，哪幾個服務把系統的資源用盡。

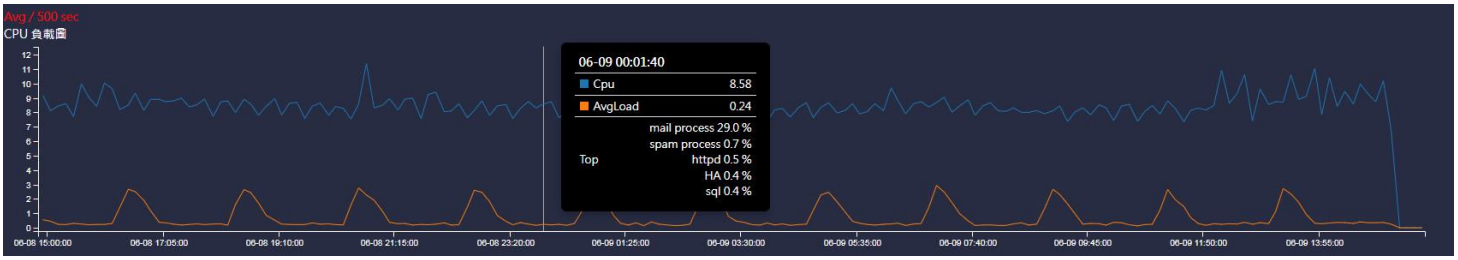


圖 13-2、CPU 負載圖

(三)、記憶體負載圖

當滑鼠移到圖形中，會進一步顯示這個時間點的詳細資訊，以（圖 13-3）為例，在 6 月 9 日 05:35:00 時，Memory 總共使用 2.35GB，Swap 使用 0.00MB，第一名佔用 Memory 1.3GB 的服務是 ClamAV。

有了這些資訊，管理者就非常容易找出過去的某個特定時間，哪幾個服務用最多的 Memory 資源。

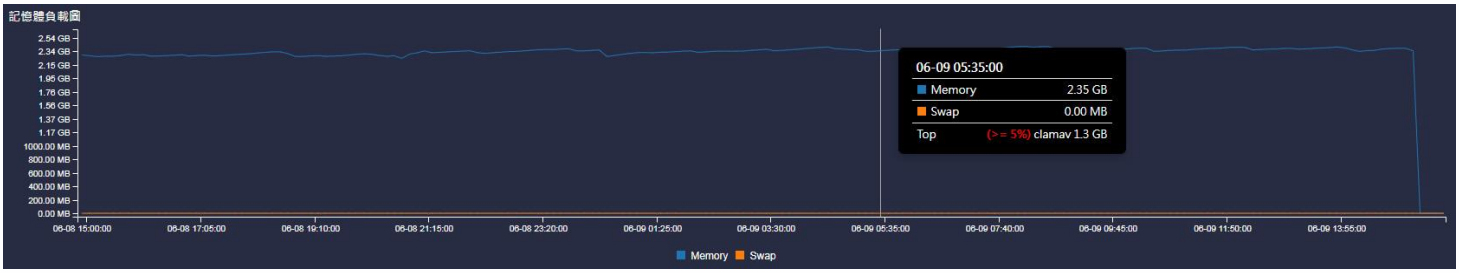


圖 13-3、記憶體負載圖

(四)、網路接口

郵件歸檔伺服器是個多 Ethernet 接口的設備，每個接口的網路流量可以在這裡顯示，當滑鼠移到圖形中，會進一步顯示這個時間點的詳細資訊，以（圖 13-4）為例，在 6 月 8 日 16:16:40 時，Port 1 的接收 / 傳送流量是 5.42MB / 124.34KB，Port 2 的接收 / 傳送流量是 3.12KB / 9.99KB，至於管理介面用的 LAN 介面他的接收/傳送流量是 348.33Bytes / 0Bytes。

再看一個設備的配置，Port 2 跟 Port 3 設成透通模式，一個對內一個對外，所以她的接收 / 傳送的流量剛好成對。有了這些資訊，管理者就非常容易找出過去的某個特定時間，流量的瓶頸。

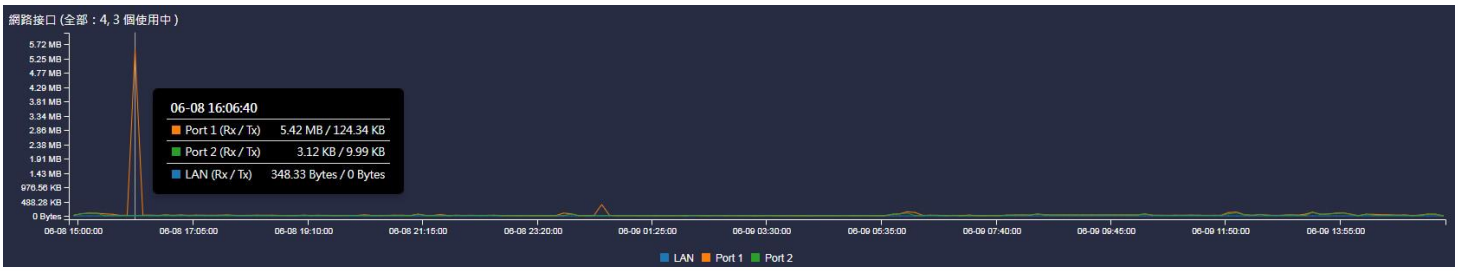


圖 13-4、網路 Port 負載圖

(四)、網路流量圖

所有經過郵件歸檔伺服器設備的流量在這裡顯示，當滑鼠移到圖形中，會進一步顯示這個時間點的詳細資訊，以（圖 13-5）為例，在 6 月 9 日 00:35:00 時，全部的接收 / 傳送流量是 382.5KB / 14.85KB。

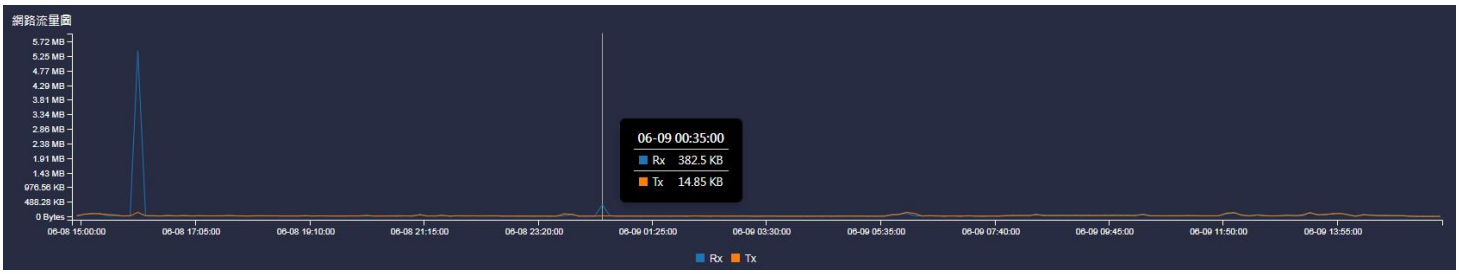


圖 13-5、網路流量圖

(五)、硬碟負載圖

硬碟的讀寫速度也是影響郵件歸檔伺服器效能的評估因素之一，設備的硬碟讀寫速度在這裡顯示，當滑鼠移到圖形中，會進一步顯示這個時間點的詳細資訊，以（圖 13-6）為例，在 6 月 9 日 03:38:20 時，硬碟的讀 / 寫 分別是 38.38KB / 0Bytes。

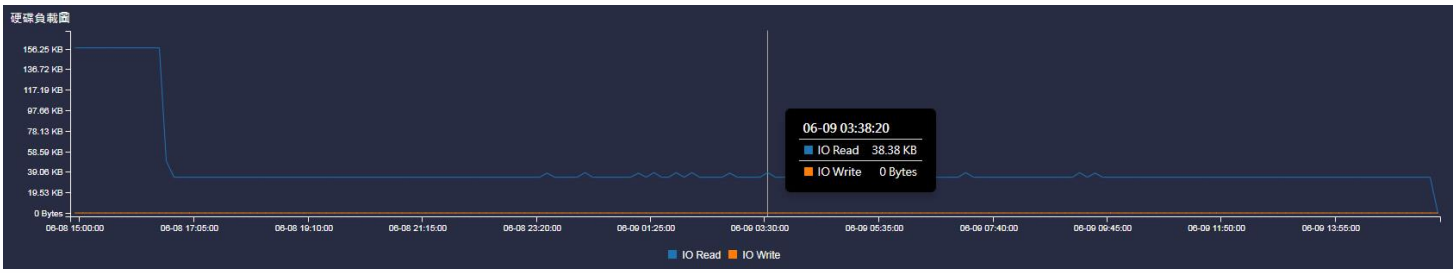


圖 13-5、硬碟負載圖

(六)、異常郵件數量流量圖

經過郵件歸檔伺服器的異常郵件流量是多少？可在這裡顯示，當滑鼠移到圖形中，會進一步顯示這個時間點的詳細資訊，以 (圖 13-7) 為例，在 6 月 9 日 09:36:40 時，異常流量透通外對內 23%異常 IP 第一名 85.217.144.247。

圖 13-7、異常郵件數量圖

(七)、郵件數量流量圖

經過郵件歸檔伺服器的郵件流量是多少？可在這裡顯示，當滑鼠移到圖形中，會進一步顯示這個時間點的詳細資訊，以 (圖 13-8) 為例，在 6 月 9 日 16:28:20 時，流量透通外對內 32%，IP 第一名 192.168.168.254。

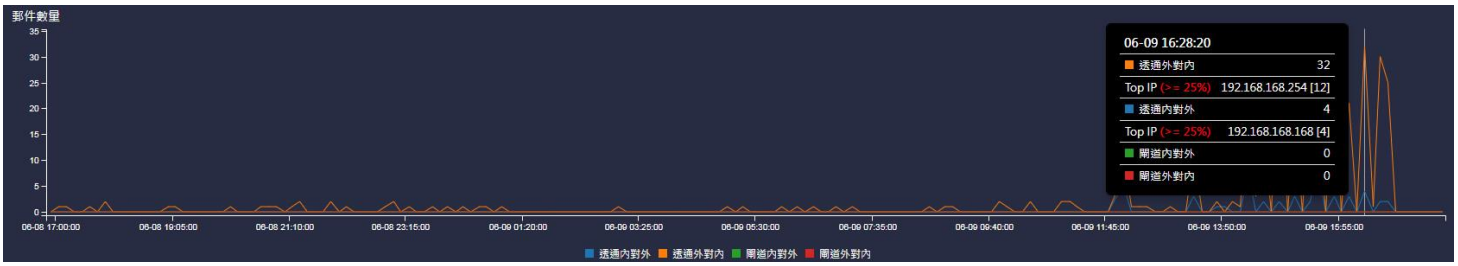


圖 13-8、郵件數量圖