UMail v5 管理員使用手冊

https://www.ublink.org





http://line.naver.jp/ti/p/%40xat.0000132120.jmw



help@ublink.org

UMail v5 管理員使用手冊	1
系統需求	7
系統安裝	8
安裝步驟:	8
使用光碟安裝:	8
使用 USB 拇指碟安裝:	8
使用虛擬機器安裝:	8
開始安裝	
控制台設定	11
configure WAN IP:設定第一片網路卡 或對外網路設定	13
configure LAN IP:設定第二片網卡 或對內網卡 IP	
Set console access password:設定此控制台進入選定需要的密碼	
Reset system admin password ,重置管理員密碼	16
Reset Webadmin allow access IPs: 重置管理介面登入限制 IP	
Reset SSL CA file:重置 SSL憑證	
Restore password file to previous one:將帳號密碼回復到指定的某一天	17
Check user quota status:修復使用者 quota (磁碟配額及使用率) 的統計資料	17
Restore all entry data from backup:恢復 系統設定/系統定時備份 的資料 ,	
Open the service mode:開啟服務通道	18
Poweroff/shutdown th server:關閉伺服器	
Exit to ready console: 退出選單	18
登入管理介面 Webadmin	19
保護管理介面	20
Webadmin 首頁	21
系統狀態概觀頁面	
帳號管理	
瀏覽帳號	
帳號數量	
帳號已停用	
磁碟配額	24
查看用戶密碼	
搜尋	
新增帳號	26
編輯帳號	28
刪除帳號	
刪除帳號	29
批次建立帳號	
一. 以流水號建立大量帳號	
二. 以匯入檔案方式建立大量帳號	
三. 以匯入 unix 帳號檔案方式建立大量帳號	
批次編輯帳號	33

匯出帳號	34
群組管理	35
輔助與雜項設定	36
初值設定	36
密碼安全設定	37
用戶通知設定	39
申請與審核	40
帳號整合	46
Windows AD	47
Linux LDAP	50
POP3 IMAP	52
公佈欄	54
發佈公布事項	55
用戶按下跑馬燈標題查看內容	56
行事曆	56
SMTP 服務設定	58
基本設定	58
進階設定	61
防護設定	64
地址化名	67
雜項設定	68
POP IMAP 服務設定	70
郵件儲列管理	72
郵件轉發路由	73
伺服器對應轉寄	76
代收外部信箱	78
郵件發送回收機制	80
灰名單機制	83
域名識別機制 DKIM	85
收發信對象管制	87
外寄簽章	90
郵件使用報告	91
記錄查詢	92
記錄器設定	94
基本設定	94
長期備份設定	96
記錄區段管理	98
長期備份查詢	99
裁判設定	100
基本設定	100
評分設定	103
通知設定	106

隔離區	107
舉報與學習	109
過濾器設定	110
基本設定	110
條件設定	111
過濾條件列表	111
新增與編修	112
基本設定	112
條件設定	114
執行動作	115
刪除信件記錄區	120
待審信件記錄區	122
延遲信件記錄區	124
轉寄信件記錄區	127
自動回信記錄區	129
放行記錄區	131
郵件掃毒器	134
防毒設定	134
病毒隔離區	135
群組信件派送	137
記錄查詢	137
群組派送設定	137
基本設定	137
名單設定	138
其他伺服器	140
DNS 伺服器	140
基本設定	140
轄區 Zone 管理	140
紀錄管理	141
Web 伺服器	142
基本設定	142
進階設定	143
網站設定	143
基本設定	143
進階設定	144
FTP 伺服器	145
基本設定	145
虛擬使用者管理	147
網路芳鄰伺服器	148
基本設定	148
共用分享區設定	149
DHCP 伺服器	150

基本設定	150
位址綁定	151
資料庫伺服器	151
基本設定	151
my.cnf	152
phpMyAdmin	152
LDAP 伺服器	153
基本設定	153
共用通訊錄 / 新增編輯通訊錄	154
共用通訊錄 / 新增編輯聯絡人	155
網路設定	155
WAN 介面設定	155
IPV4	155
IPV6	157
hosts	157
LAN 介面設定	157
靜態路由	157
連接設定	158
網路測試工具	158
DNS 查詢	158
PING	159
Tracerouter	159
Web test	159
防火牆設定	159
一般設定	159
自動防禦阻斷	160
防禦設定	160
白名單	161
已阻斷中紀錄	161
手動防禦設定	161
虛擬服務轉阜	162
系統日誌	162
選擇查詢區段	
搜尋	
匯出	
 設定	
事件記錄	
事件記錄	
主機事件	
主機事件	
工版字	
SMTP 記錄	
· ·	

POP IMAP	164
POP IMAP 記錄	164
郵件掃毒	165
郵件掃毒記錄	165
攻擊阻斷記錄	165
攻擊阻斷記錄	165
FTP 伺服器	167
DNS 伺服器	167
網頁伺服器	167
LDAP 伺服器	167
伺服器監視	167
系統設定	167
偏好設定	167
管理員任務分派	167
電源管理	167
SSL 憑證管理	167
系統定時備份	167
規劃鏡射碟	167
磁碟管理	168
規劃備援機	168
系統更新	168
授權註冊	168
岑 典	168

08/22/2024 Write

系統需求

UMail v5採用 Linux 核心爲作業系統,目前核心爲 5.0.x 是 linux 最新的穩定版核心,由於核心是由本公司研發團隊自行調整重新編譯,與市面上的其他 linux distribution,例如 ubuntu, fedora, centos ··· 不同,由於需要簡化爲嵌入式系統,我們幾乎都是自行打造的系統架構,事實上 UMail v5整個系統體積 大約只有 200MB,由於精簡化減少安裝不必要的系統程式與套件,其穩定性及安全性相對與一般的 Linux 系統更安全,使用上也更方便(我們有整體的 web 管理界面),您不需要像一般的 linux 系統 需要登入使用終端機登入 使用文字界面設定伺服器

UMail v5 可以安裝於實體機器或是虛擬機器

實體機器建議:

- CPU: Intel 64 位元,或 AMD,建議 intel i3 /i5/i7
- 顯示卡:建議使用內顯較為節省能源
- 記憶體: 2G 以上, 建議 4G~16G
- 光碟機:建議一部,若使用 USB 拇指碟開機 可以不需光碟機
- 硬碟:40G以上,建議 1T 硬碟,或 SSD(主碟)+1T 硬碟(鏡射或備份碟)
- 網路卡: 主機板內建或 PCI-e 介面卡,支援 100/1G/10G 網卡,主機版內建不一定全部都支援,購買前請先使用試用版測試,內建無法支援時建議插上 PCIe 介面卡

虛擬機器建議

- VirtualBOX:https://www.virtualbox.org/
- VMware:https://www.vmware.com/
- Proxmox:https://www.proxmox.com/
- Hyper-V: Microsoft, 設定時請選 Gen-1
- XenServer: CITRIX

虛擬機器安裝時請下載 CD 版本的 ISO 檔,將 ISO2 檔掛載於虛擬機器的光碟開機

系統安裝

安裝步驟:

使用光碟安裝:

- 如果您已經購買本產品,請取出產品包裝內的光碟片,如果您尚未購買本產品,可以到產品官方網站,下載最新的光碟版 ISO 檔案,並以燒錄印象檔方式燒錄光碟
- 將光碟片置入光碟機, 開機進入系統的 BIOS
- 選擇 BIOS 的開機項目為光碟開機,必要時請檢查並校正日期和時間
- 重新開機,進入第一次安裝程序

使用 USB 拇指碟安裝:

- 如果欲安裝本系統的伺服器沒有光碟機,您可以使用 USB 拇指碟或是 SATA DOM(一種微型的 SATA 晶片,可直接插在主機板上的 SATA 插槽),容量必須大於 500MB 且 小於 64GB
- 至產品官方網站下載最新的USB製作ISO檔,並以燒錄印象檔方式燒錄光碟,**注意:切勿使** 用坊間的 CD 轉 USB 工具進行此步驟
- 將剛剛燒錄好的光碟插入機器的 USB 插槽(本系統支援 USB3 及以下的規格),並將光碟插入光碟機, BIOS 選擇光碟開機
- 上述燒錄 USB 拇指碟的機器可以使用其他的機器製作,並不一定要使用欲安裝系統的伺服器,燒錄 BIOS 時建議將硬碟先離線,避免失誤格式化硬碟資料
- 將燒錄好的 USB, 插入欲安裝本系統的伺服器
- 選擇 BIOS 開機選項為 USB硬碟
- 重新開機, 進入第一次安裝程序

使用虛擬機器安裝:

- 如果您要將系統安裝在虛擬機器上,到產品官方網站,下載最新的光碟版 ISO 檔案
- 下載的 ISO 檔案 不需燒錄光碟,通常虛擬機器都支援 ISO檔模擬光碟

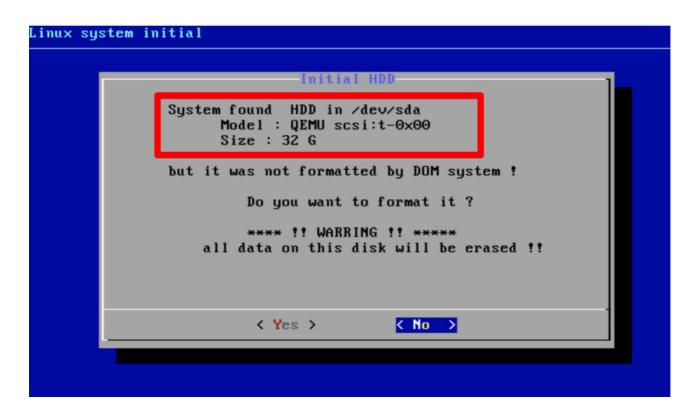
開始安裝

```
SeaBIOS (version rel-1.14.0-0-g155821a1990b-prebuilt.qemu.org)
Machine UUID 65124627-3a5d-4d88-9df1-e44335b9966d
Booting from DVD/CD...

ISOLINUX 6.03 ETCD Copyright (C) 1994-2014 H. Peter Anvin et al
type CHKDSK --> do check/fix disk
type CLEARDISK --> do clear all data on disk and reinitialize disk
boot:
```

UMail v5 安裝步驟,並不是將光碟片的系統安裝到硬碟,主要是來格式化硬碟用來儲存日後產生的資料及設定,所以安裝完成之後仍然需要使用光碟或 USB 拇指碟來開機

開機後重新此畫面表示有正確由系統光碟開機, 稍後幾秒鐘後將將進入核心引導



請仔細檢查系統偵測到的硬碟是否正確(如果系統內由多顆硬碟,建議在安裝時僅保留一顆), Model (型號) 及 Size(容量)大小是否正確, 正確的話 請用 鍵盤的方向鍵或 Tab 鍵將 移到 再按下 Enter 鍵或按 Y



此時系統詢問硬碟要分割的 SWAP(記憶體交換檔) 要預留多大 ? 通常建議保留安裝記憶體的 2 倍 , 但最大不要超過 16G , 4G(4096)是個不錯的建議值

```
format disk
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
1597440 inodes, 6388603 blocks
319430 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2155872256
195 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
       32768, 98304, 163840, 229376, 294912, 819200, 884736, 1
       4096000
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
```

回答問題後系統會自動格式化硬碟並安裝系統,過程視硬碟大小及硬碟的讀寫速度,通常不會超過3分鐘,硬碟格式化之後系統會立即重新開機

請勿取出光碟片 或 拔出 USB 拇指碟 , 之後的每次開機都必須使用光碟或 USB 碟開機 , 兩種開機 模式可以互相取代 , 不需重新格式化硬碟

例如:當USB拇指碟 故障,可以先燒錄一片CD版的光碟用光碟開機,或是當轉換主機沒有光碟時也可以切換使用USB拇指碟為開機裝置

重新開機後應該重新此畫面,若是沒有進入開機畫面,則可能你的 BIOS 沒有調整好使用光碟開機

Linux Server is ready.

DATE : 2021-09-06

TIME: 14:40:52 up 7 min

WAN: 192.168.8.24 (eth0)

WebAdmin: https://192.168.8.24:88

WebMail: https://192.168.8.24

Press key (s) to setup menu ...

DATE: 顯示伺服器日期

TIME:顯示伺服器時間

若是日期或時間不準確 , 請關機後至 BIOS 下設定好日期和時間 ,或是稍後進入管理介面設定好時 區由網路自動對時

WAN:目前第一張網路卡的 IP(預設是以 DHCP 取得)請重新選擇為固定 IP,若有第二片網卡且有啟動時,會出現 LAN IP

IP 可以稍後按 s 進入修改,或是到管理介面修改

WebAdmin: 進入管理介面的網址

WebMail: 進入線上郵箱的網址

控制台設定

伺服器開機後會停留在這個畫面 , 畫面上會顯示 伺服器日期/時間 和 伺服器 IP

這個畫面 稱為伺服器 console (伺服器控制台)

```
Linux Server is ready.

DATE: 2021-09-06
TIME: 14:59:13 up 25 min

WAN: 192.168.8.24 (eth0)

WebAdmin: https://192.168.8.24:88
WebMail: https://192.168.8.24

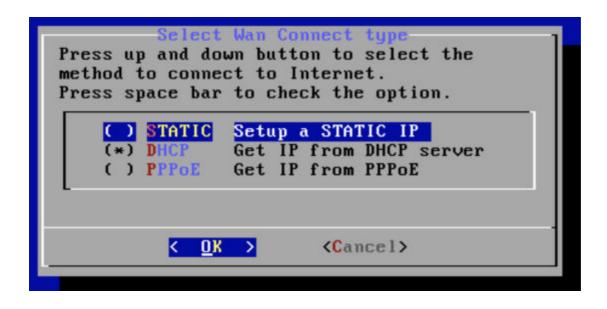
Press key (s) to setup menu ...
```

平常伺服器應該持續顯示在這個畫面,系統管理員可以按 鍵盤 s 按鍵 進入控制台選單



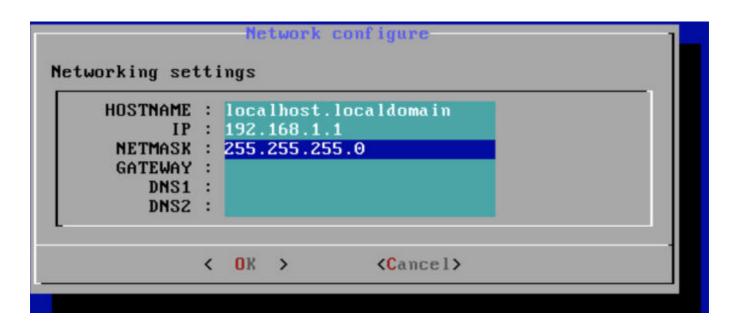
可以按下功能表前方的代碼 X0123456789P, 快速定位到功能項目或是用上下按鍵移動光標, 定位 好後按下 enter鍵即可進行該項目的設置

configure WAN IP: 設定第一片網路卡 或對外網路設定



先選擇網路的連接形態 ,可以選擇 STATIC(固定 IP) 或 DHCP 動態取得 ,或使用 PPPoE(撥接網路) 伺服器若安裝於防火牆內 ,請在 WAN 設定為內部的虛擬網段 ,再透過公司防火牆導入服務 port

使用上下按鍵移動光標,使用空白鍵 選定,按 Enter確認進入設定



輸入個別欄位 ,可以使用 上下鍵移動輸入的光標 ,全部輸入完成後按 Tab 鍵 跳到 < OK > 並按下 Enter確認修改

configure LAN IP: 設定第二片網卡 或對內網卡 IP

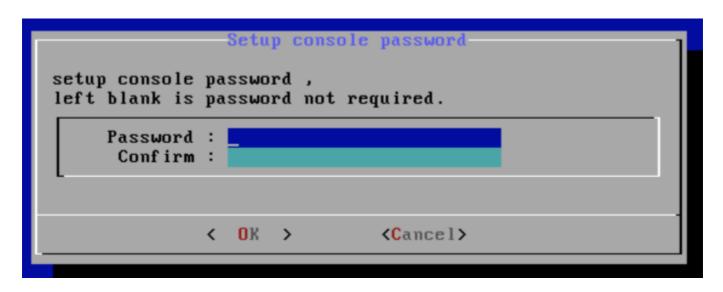


系統預設第二片網卡是不啟用 , 如果機器上有第二片網卡且要使用 ,必須先啟用系統才能使用 通常網路卡的順序是由 IRQ 順序 , 經驗上 插卡的順序優先於主機版上內建的 ,

例如若主機版內建一個網路孔, PCIe 上再插上一片網路卡時, 通常 WAN 為網路卡, LAN為主機版內建

Set console access password: 設定此控制台進入選定需要的密碼

預設 console 進入選單是不需要密碼 ,如果您的伺服器安裝放置的位置有安全性考量(例如放置於代管機房),可以考慮設定選定密碼 ,防止不明人士進行操作或修改設定



進入設定後請輸入密碼,輸入時不會顯示 ,請在 Password 和 Confirm 輸入相同的密碼 ,輸入後請按 OK



下次要進入 console 選單時 會要求輸入密碼

若要解除密碼,請重新設定 並將密碼設定為 "空"即可

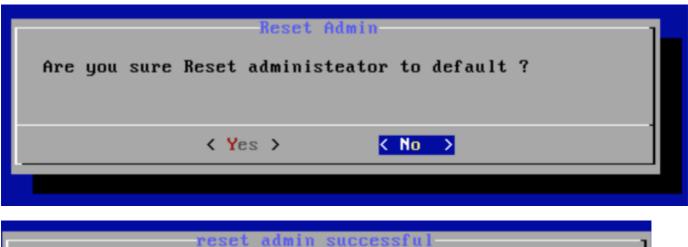
萬一 忘記密碼時 ,可以進入管理介面 的系統設定/偏好設定的一般選項內 找到 清除 console 登入 密碼 ,將 console 密碼清除

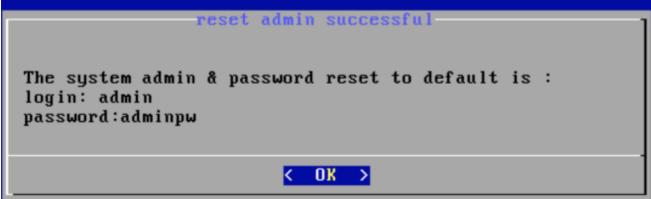


請注意:如果同時 忘記或遺失 console 登入密碼 和管理介面 admin 密碼,系統將無法進入管理, 且無法透過遠端工程師進行密碼重置,若遇此時狀況 必須將機器寄回原廠進行解密處理,若要設 定雙重密碼必須謹慎為之

Reset system admin password,重置管理員密碼

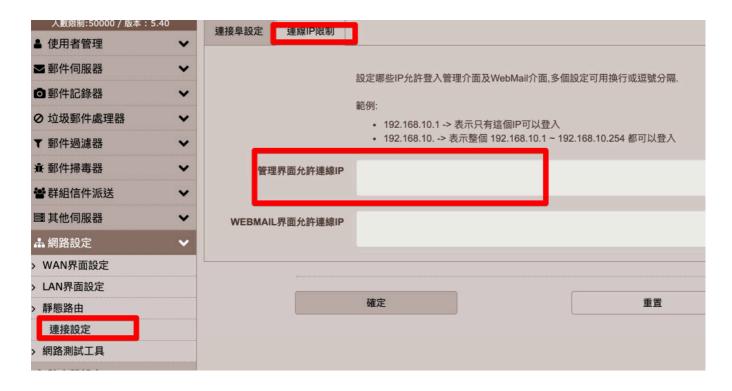
萬一忘記或遺失登入管理介面的密碼 通常是 admin 的密碼 , 或是指定的超級管理員忘記或遺失密 碼時 , 可以使用此選單功能進行重置 admin 初始密碼





重置後的管理介面登入帳號為 初始 管理員 admin, 密碼為:adminpw

Reset Webadmin allow access IPs: 重置管理介面登入限制 IP



安全性考慮下管理員可以設定指定只有某些 IP 才可登入管理介面 , 設定位於管理介面的 網路設定 /連接設定 : 連線 IP 設定

萬一設定時將自己或指定的 IP 誤檔 , 此時可以由此 console 選單進行回復

Reset SSL CA file: 重置 SSL憑證

系統預設是使用自簽的封閉憑證 ,自然瀏覽器無法認證每次都會出現憑證錯誤 ,系統管理員可以自行購買第三方的公正憑證安裝 ,但有時候管理員在安裝憑證有可能會因為安裝時剪貼憑證錯誤 ,造成管理介面整個無法啟動及登入時 ,可以透過此 console 選單進行重置回復可登入狀態

Restore password file to previous one: 將帳號密碼回復到指定的某一天

注意:回復帳號密碼 並不會恢復帳號的資料(檔案或郵件)

Check user quota status:修復使用者 quota (磁碟配額及使用率)的統計資料

通常發生於多次不正常斷電系統意外重啟狀況下,可能造成 資料遺失或 Quota 不準確,例如用戶沒有郵件或檔案時 數據顯示使用大量的空間時,可以執行此功能,讓系統重新計算一次 quota 統計值,執行期間系統可以正常運作不需停止,執行完成後也不需重新開機

Restore all entry data from backup:恢復系統設定/系統定時備份的資料,

詳細備份功能請參考管理介面使用說明

Open the service mode: 開啟服務通道

此功能不開放給一般用戶使用,僅保留給原廠工程師在需要的時候從伺服器端開啟遠程服務功能, 通常目的為問題檢查或進階的系統維護或修復時需要

Poweroff/shutdown th server:關閉伺服器

伺服器若要關閉或重新啟動 ,切勿直接關閉電源開關 ,必須由此功能進行伺服器關閉或是由管理介面的 系統管理/電源管理 進行關機

Exit to ready console: 退出選單

回到 Ready console

登入管理介面 Webadmin



預設的管理介面入口為伺服器 IP(或主機名稱) 以 https 加密方式, port 號預設為88,

請使用瀏覽器登入, 瀏覽器必須是現代化的瀏覽器,舊型的例如 IE10 以下的瀏覽器無法支援, 建議使用 chrome 或 firefox 或 edge, safari

- 介面語言目前支援 正體中文/簡體中文/英文
- 預設管理員帳號為:admin 預設密碼為:adminpw
- 請登入後盡快至 使用者管理 / 帳號管理 更改密碼

如果不確定伺服器的 IP, 可以到伺服器 console(伺服器螢幕), 查看伺服器 ready console 畫面的指示

萬一忘記管理介面的管理員或密碼時可以至,伺服器主機的螢幕下按s,進入設定選單執行Reset system admin**and password**

保護管理介面

伺服器一旦正式上線後, 難免會有網路安全的顧慮, 為了防止有心人士刺探登入管理介面, 有幾個建議設定如下

- 伺服器安裝於防火牆後面,再由防火牆導入服務 port 到伺服器上
- 若沒有必要管理介面 port:tcp/88 建議不要導入
- 管理員密碼使用較複雜的組合

到系統設定 /偏好設定/管理介面佈局: 啟用 登入圖形檢查碼,以防止網路機器人探測密碼



設定 防火牆設定/自動防禦阻斷/防禦設定 啟動 webadmin-auth 功能,當嘗試登入錯誤超過設定次數,可即時斷開該來源 IP 的連線

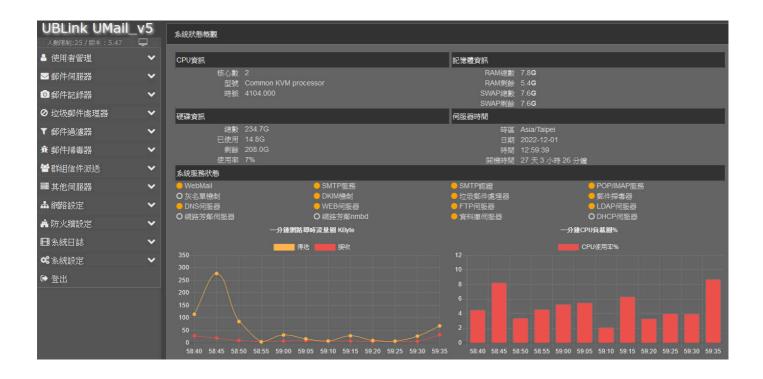


設定網路設定/連接設定/連線IP限制:管理界面允許連線IP,可以設定只允許某些特定的IP才能訪問管理介面

連接阜設定 連線IP限制	
	設定哪些IP允許登入管理介面及WebMail介面,多個設定可用換行或逗號分隔.
	範例:
	 192.168.10.1 -> 表示只有這個IP可以登入 192.168.10> 表示整個 192.168.10.1 ~ 192.168.10.254 都可以登入
管理界面允許達	
WEBMAIL界面允許連	l線IP

Webadmin 首頁

系統狀態概觀頁面



登入管理介面後出現的第一個畫面是系統狀態概觀頁面 ,這個頁面稍後也可以按下畫面的左上角的產品名稱宣告打開此頁面

CPU 資訊

顯示此伺服器的CPU核心數量及目前的執行時脈 ,若在虛擬機器下顯示的可能是虛擬的CPU及核心數量

記憶體資訊

顯示此伺服器安裝的記憶體(RAM),及安裝時所規劃的交換記憶體(SWAP),安裝的總量及目前剩餘的數量

通常伺服器會盡量使用所有的記憶體也獲得最佳的伺服器的效能 ,如果您發現伺服器的 RAM 剩餘 很少,請不必擔心

硬體資訊

顯示伺服器安裝的硬碟狀況,這裡顯示的為主要硬碟的資訊,並不包含鏡射碟/備份碟及記錄碟的資訊 總數是已經扣除 SWAP 及 TMP 所切割後的容量,所有會稍小於您實際購買的容量,這是正常的,請不需擔心

如果要查看所有的硬碟資訊,可以到系統設定/磁碟管理查看

伺服器時間

顯示目前伺服器時間,伺服器時間的調整是參考 1. 開機時 BIOS 內所設定的時間,2. 開機後每一段時間會進行網路對時

關於網路時間對時 , 可以到系統設定/偏好設定 內的 伺服器時區, 世界協調時間 , 及設定 NTP 時間伺服器 ,已取得正確的伺服器時間

伺服器内的所有相關時間的記錄, 皆以伺服器時間為戳記, 非參考用戶端所在的地區時間

系統服務狀態

此處列出此伺服器顯見的服務啟動狀態 ,實心圓標記為啟動中 ,空心圓表示該服務目前處於關閉狀態 ,每個服務器的是否開啟 ,可以至各個服務功能進行設定調配

網路即時流量圖

顯示網路傳輸狀況 , 分為 傳送: 伺服器的傳送到客戶端的流量 , 接收: 客戶端上傳伺服器的流量 共分為 最近一分鐘 / 最近一小時 / 最近一天 及最近一週 的流量狀況

查看圖表時需主要,縱軸為頻寬 單位為 Kbyte/每秒,系統會自訂調配出當時最佳的最大值,查看時要參考縱軸的最大值,橫軸為時間,依照不同的圖表切割為每5秒/每5分鐘/每小時/每一天,最右邊的時間表示目前或最接近目前時間的資料

若要查看更詳細的連線資訊,可以到系統日誌/伺服器監視的 netstat 及 iftop查看

CPU 負載圖

顯示 CPU 負載的狀況圖 單位為 % 使用率.

共分為 最近一分鐘 / 最近一小時 / 最近一天 及最近一週 的使用狀況

若要查看更詳細的 CPU 資訊,可以到系統日誌/伺服器監視 top

帳號管理

瀏覽帳號

帳號數量



本系統在購買的時候, 單位可依照實際或預留的使用人數來選購產品

欲查看購買的版本最高可使用的人數 可以觀察登入頁面的左上角產品徽章下的人數限制數值

預設的 admin 帳號 不列入人數限制,也不能刪除 admin 這個帳號,但可以將 admin 帳號降為一般使用者,可參考**管理員任務分派**

帳號已停用

foo	foo	2 G	351.7 M /	● 16 天		ø 1	Î
jerry	jerry	2 G	= 25.1 M /	461 天		₽ 1	
jerry.yeh	jerry	2G	-668.0K / 1 天	● 491	□-\$	<i>0</i> - 1	î Î
jerry2	jerry2	2 G	≅ 724.0 K /	③ 486	므소테르종를	ø	ì
k1	k1	無限	≣ 735.0 M	9 734		ø 1	D D

停用的帳號也算在購買的授權帳號數量內 ,停用的帳號會以紅色的字體表示並以帳號加上刪除表示 帳號會停用通常是

- 帳號設定的使用天數進入負值
- 帳號密碼超過管理員設定未修改的天數(參考輔助與雜項設定/密碼安全與設定:強迫用戶定時更換密碼)

停用帳號若超過一定時間未理會,系統會自動刪除該帳號(參考輔助與雜項設定/初值設定)

磁碟配額

管理員可以指定每個使用者帳號最多可以使用多少磁碟空間,此配額設定不會預先切割空閒空間給用戶,管理員還是要注意整個伺服器總空間是否足夠.

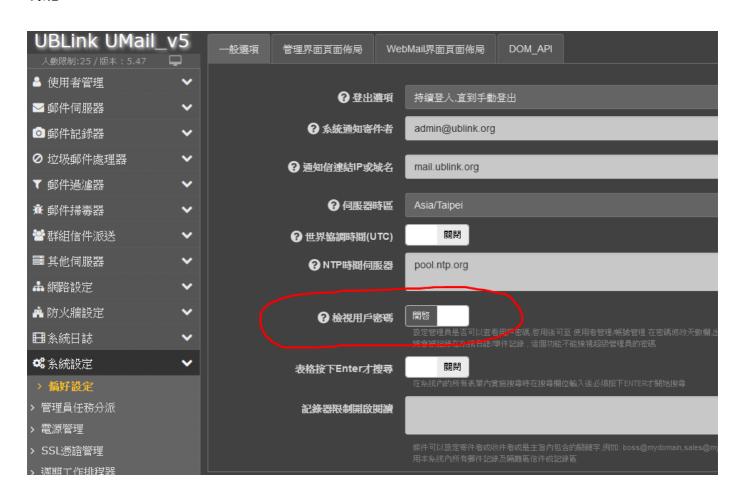
使用者會在空間屆滿約 70% 與 90% 用不同的顏色來顯示,方便管理員管理查看

管理員也可以在 輔助與雜項設定/用戶通知設定, 磁碟屆滿的通知設定, 當空間屆滿時以郵件通知使用者.

按下檔案列表圖示,可以查看屬於該用戶的檔案列表,此功能有助於管理員查閱用戶在伺服器上的檔案分布狀況.

查看用戶密碼

系統預設管理員不可查看用戶密碼,若需要此功能可以到 **系統設定/偏好設定** 啟動 檢視用戶密碼功能



開啟功能後在使用者列表上的 "密碼已修改的欄位" 會出現一個**眼睛圖示**按下眼睛即可查看該用 戶密碼



注意:admin 或被指定為超級管理員的用戶密碼不能被檢視

管理員檢視用戶密碼 此動作會被記錄在 系統日誌/事件記錄

搜尋



若帳號數量多時,可以利用搜尋功能,篩選出特定的帳號

新增帳號

按下畫面下的 +新增 按鈕 即可開始新增帳號



帳號

- 最長爲 30 個字母
- 英文字母只能用小寫
- 符號僅允許使用.
- 本系統因應特殊運用,特別設計允許純數字帳號

名稱

- 可以使用中文或英文
- 不能使用特殊符號 **@ <>:

密碼

- 使用者密碼初次由管理員建立,建議密碼不要太過於簡單.
- 用戶可於帳號開始使用後,登入 Webmail 後至個人設定更改密碼
- 建議管理員開啓 使用者管理/輔助與雜項設定/密碼安全設定 -> 強迫用戶定時更換密碼,用戶若未依照規定更換定期更換密碼,系統將依照管理員設定予以帳號停權甚至刪除.
- 使用者更改密碼必須依照強度規定設定新密碼,預設至少6個字且必須包含數字與字母(詳細可至使用者管理/輔助與雜項設定/密碼安全設定密碼強度設定)
- 管理員於本頁面設定密碼 不受密碼強度限制

磁碟配額

- 帳號設定(分配)到的磁碟空間 , 可用於用戶存放電子郵件 email , 如果有開啓其他功能 , 像 是 網路硬碟 / ftp 或網路芳鄰功能 , 還可以用相關的工具將檔案存放於這個磁碟空間內
- 設定值爲 0 時 ,表示不對這個用戶設定配額控制 ,意即這個用戶可以使用最大的磁碟空間 爲無限 ,直到硬碟空間用盡 ,建議除非是特殊用戶 ,盡量還是要設定磁碟配額.
- 這個設定並不會事先將空間圈用,對硬碟總空間並不會立即使用掉,不過管理員還是要注意如果用戶的配額設定太大時,要考慮使使用的磁碟是否夠大.
- 當空間配額屆滿前,系統會發通知信通知該用戶,用戶應該要適時刪除一些檔案或是信件.
- 當配額完全用完時 ,用戶將無法收取新的信件 * 相關設定: 使用者管理 / 輔助與雜項設定 / 用戶通知設定 -> 空間屆滿通知

帳號可行使功能

• 線上信箱:即 webmail,可在任何一部具有現代化瀏覽器的電腦或行動裝置上進行電子郵件收信/發信,如用戶具備有此功能可以在網址列上輸入 https://伺服器網址,即可進入登入畫面,登入後即可進行信件的收發

網路硬碟:使用者可以透過登入線上信箱介面,進入網路硬碟的使用介面,進行用戶家目錄檔案存取,收信時可以將附件直接存到網路硬碟,寫信時可以直接由網路硬碟夾帶檔案寄出,網路硬碟亦可方便設定檔案的存取屬性.

- 網路芳鄰:用戶可以用 windows 檔案總管輸入 \ serverip \ 用戶名稱,例如: \ 192.168.1.1 \ john,存取用戶家目錄的檔案,MacOS 用戶可以用 command+k 輸入 cifs://john@192.168.1.1 連線,網路芳鄰只能用於區域網路內,你不能在公共網路透過網路芳 鄰連結伺服器
- 登入 ftp:用戶開啟這個功能,即可使用該用戶的帳號密碼 以慣用的 ftp 用戶端軟體進行連線,存取自己家目錄下的檔案
- 網頁空間:開啟這個功能,用戶空間可以用來架設網站,可以把網頁檔案 透過 網路芳鄰 或 ftp 甚至是網路硬碟功能,上傳到個人家目錄下的 _www_ 目錄下,如果管理員有啟動 用戶個人網站功能(此設定於 其他伺服器/web 伺服器/基本設定),即可透過網址 http://serverip/~帳號/,例如 http://192.168.1.1/~john/,注意最後需要有 "倒斜線" 結束
- 個人資料庫:本系統內建有一套 SQL (MariaDB 伺服器),功能與 MySQL 相同,當建立用戶時勾選此選項時,系統會自動建立一個同名資料庫,與一個同名資料庫用戶,例如建立帳號 john,會建立一個叫 john 的資料庫用戶,及一個 john 他資料庫,當登入或連線資料庫時使用 john 時 只會看到 john 這個資料庫,不同用戶資料庫不會被互相窺探會異動操作,若需要完整操作資料庫時才需要以 root 登入

帳號可用天數

- 設定這個帳號可使用的天數
- 設定值 0 時,表示不限使用天數
- 設定 負值時,該使用者無法登入 webmail 也不能登入 pop3/imap 收發信件,但其他人還是可以寄信到這個帳號的信箱
- 當負值增加到一定的天數(視: 使用者管理/輔助與雜項設定/儲值設定 -> 帳號過期天數後自動 刪除 的設定值,預設爲365天),該帳號會自動被系統刪除

編輯帳號

按下帳號列表內帳號最右邊的 "筆" 圖示 進行該帳號的編輯



帳號編輯與新增帳號的操作方式大略相同,唯一不同的是帳號是不能被修改

密碼若不修改只要保持空白即可

磁碟配額若修改後小於目前實際佔用的空間時,系統不會主動刪除用戶的資料,但用戶可能會無法繼續收信或上傳資料到伺服器

若停用個人資料庫功能,系統不會刪除已經建立的資料庫,僅會停止該用戶存取資料庫的權限

刪除帳號

刪除帳號

按下帳號列表內帳號最右邊的 "垃圾桶" 圖示 進行該帳號的刪除



系統會再次確認是否要刪除該帳號



admin 此帳號不能被刪除,即使該帳號已經被解除管理員身份也不能被刪除

另外只要具有管理員身份的帳號,也不能被刪除 , 刪除該帳號前必須先到 , 系統管理/管理員任務分 派 將其管理員身份解除之後方能刪除此帳號

帳號刪除後系統會自動保留7天的資料恢復功能,若誤刪了帳號,可以在7天內重新建立相同的帳號,新增後進行該帳號的編輯,此時編輯畫面會稍有不同,你會看到恢復數據的提示

	請輸入	與上方密碼欄位相同		
→ 磁碟配額	-	2048	MB	+
	設定此	帳號可用最大磁碟空間	引, 0:表示》	馬無限制
❷ 帳號可行使功能	☑ 線上信	言箱 ☑ 網路硬碟 □	網路芳如	嘟 □ 登入FTP □ 網頁空間 □ 個人資料
♂可用天數	-	0	天	+
	設定此	展號可用天數,0:代表	帳永遠有效	效,負的數字:表示停用該帳號
❷ 恢復數據	□可恢復	复數據:140.0K		
確	定			取消

若要恢復此帳號的資料,可以勾選後按下確定按鈕即可

批次建立帳號



批次建立帳號可以讓管理員可以很快速的建立多個帳號, 系統提供三種建立大量帳號的方式

一. 以流水號建立大量帳號

建立大量帳號方式	以流水號建立大量帳號		
❷ 帳號	user(*)		
流水號: 從~	例如: user(*) , (*): 由流水號 - 1	和文化 中	
流水號: ~到	- 3	+	
② 密碼			
② 磁碟配額	- 2048	MB +	
② 可用天數	- 0 設定此帳號可用天數,0:代	天 + 表帳永遠有效,負的數字:	表示停用該帳號
❷ 帳號可行使功能	☑ 線上信箱 ☑ 網路硬碟	□ 網路芳鄰 □ 登入F	TP □網頁空間 □ 個人資料庫
	確定		取消

- 此方式可以讓管理快速依照流水號建立大量帳號 , 例如 user1,user2,user3,user4..... * 帳號格式 設定時 (*) 會用 流水號 從 ... 到 的編號代入
- 密碼設定預設建立的帳號為相同的密碼,用戶可以自行到 WebMail 進行密碼更改

二. 以匯入檔案方式建立大量帳號



- 匯入的檔案支援 CSV 格式的檔案,第一行為表頭,順序如下表 ,檔案的文字編碼必須是 UTF-8, 否則中文會變成亂碼
- 可以使用 excel 或一般文書編輯器製作好來源檔案, 然後按選擇檔案之後匯入該檔案即可
- 若帳號已經存在系統會自動略過該帳號
- 可以匯入本系統匯出帳號的檔案格式

三. 以匯入 unix 帳號檔案方式建立大量帳號



- 管理員必須要想辦法到原本的 UNIX 系統取得 /etc/passwd 和 /etc/shadow 這兩個檔案,再分別 匯入這兩個檔案到正確的位置
- 以此種方式匯入的帳號其密碼為加密格式密碼,系統暫時無法記錄其密碼,必須等候用戶至少登入一次 WebMail 後才能記憶密碼

批次編輯帳號



先將要進行編輯的帳號勾選,按下批次編按鈕



將欲修改的項目進行修改,若不改變的選項請保留空白或選 "不改變"

匯出帳號

+ 新增	替 批次編	輯	建立帳號	匯出帳號 前 删除			搜尋
示第 1	1 到第 20 項記録	錄,總共 30 項詞	記錄 每頁顯示	10 → 項記錄			
•	帳號	姓名	♦ 磁碟配額	磁碟使用狀況	可用	密碼已 ♦	帳號可行傾
	mvc	mvc	2 G	440.0 K / 0		● 87 天	旦土間=
2	mymenu	mymenu	2 G	355.2 M /		● 80 天	□土祖=
Z	notebook	notebook	4G	= 1.1 M / 0.0		● 489 天	□土間=
Z	p1	p1	2 G	= 200.0 K / 0		🧆 188 天	□± #=
☑	qqq	qqq	2 G	336.0 K / 0		● 288 天	□≛□
Z	smb	smb	2 G	380.0 K / 0		● 443 天	□土間=
	super1	123	2 G	336.0 K / 0		● 351 天	旦土
(page	super2	super2	2 G	≣ 336.0 K / 0		● 351 天	□土田=

先勾選要匯出的帳號 (若要匯出全部帳號,則不需勾選),再按下 匯出帳號 按鈕

您的電腦會下載一個 .csv 格式的檔案

csv 格式的檔案 通常在 windows 會被 excel (如果電腦有安裝此軟體) 開啟編輯 , 特別要注意的是本系統一律都是以 UTF-8 為編碼 , 若您看到的是亂碼 請調整您的 excel 開檔時的編碼 為 utf-8

或是建議您可以下載免費的 openoffice 或是 <u>LibreOffice</u>, 來開啟或編輯 csv 檔案 , 此二系統預設都是以 utf8 開啟 csv 檔案

或是您也可以用文字編輯器來開啟,建議可以使用 EditPlus,或 vscode 這類的語法編輯器

群組管理



群組是把選定的帳號使用另一個別名來代表



例如建立一個群組帳號為 sales, 並將公司內的業務員,從右邊選入到左邊, 確定後即可建立一個 sales 的群組帳號(sales 必須是一個不存在的帳號)

當信件寄給 sales 時 , 所有的業務員都可以收到此信件

臨時要接收別人的來信,又不想讓對方知道您真正的帳號名稱,此時何以建立一個別名,再將自己選入,如此對方寄到這個別名帳號您也可以收到信件,若不想再收到這個信件可以將群組刪除即可.

輔助與雜項設定

初值設定

❷ 帳號過	期天數後自動刪除		365	天	+		
•	空間配額初始值		2048	MB	+		
0	可使用 WebMail	₩M:	允許報號使用 V	VebMail 收	發信件		
•	可使用網路硬碟	☑WH:	允許帳號使用 V	VebMail 內	的 網路硬石	功能	
•	可使用網路芳鄰	SMB	:允許使用網路上	的芳鄰連結	個人目錄		
	② 可使用FTP	□FTP:	允許帳號透過F	TP 連線個人	目鋒		
•	可使用個人網站	□ WEB	:允許在個人目前	下的_ww	v_ 建立個。	人網站	
② 允許並	建立專屬的資料庫	□ SQL:	建立一個與帳號	同名資料庫	,使用者可	用自己的帳	战及密碼管理該資料庫

初值設定會自動在新增帳號時以這個初始值為預設

- 例如新增帳號時用戶大多給 10G 空間配額,可以先在 空間配額初始值設定為 10240 MB,這 樣在每次新增帳號時就不需要經常調整
- 帳號過期天數後自動刪除:這個設定當帳號因為帳號建立時有設定使用天數,而該帳號已經 過期,且超過這個指定時間時系統會自動刪除這個帳號
- 系統設定帳號需定時更新密碼,而該帳號逾期未更新密碼而遭到停用,且超過這個指定時間時系統會自動刪除這個帳號
- 其他的設定可以參考 帳號管理/新增帳號? 內的說明

密碼安全設定

初值設定 密碼安全設定 用	戶通知設定				
② 允許用戶設定自動轉寄	關閉 允許用戶在WebMail介面 設定/自動轉寄或進階過濾器內進行信件自動轉寄				
❷ 例外名單	排除上述策略以外的名單				
② 允許用戶更改密碼	開客 用戶可以登入WebMail介面 設定/更改密碼				
❷強迫用戶定時更換密碼	用戶必須購一段時間更換密碼				
❷ 將逾期帳號停用	□ 逾期未更換密碼用戶將被停用,停用之使用者無法登入信箱,必須由管理員協助啟用				
❷ 密碼有效天數	- 180 天 +				
❷ 逾期前幾天通知用戶	- 7 天 +				
❷ 通知信主旨	請注意! 您的帳號即將要過期				
❷ 通知信內容	您必須於 #DAY 日內更換新的密碼,否則帳號將於 #DATE 到期,到期後您將無法登入.				
	可套用變數: #DAY: 尚餘日數, #DATE: 到期日				
❷ 例外帳號	admin x				
密碼長度至少	- 6 +				
❷ 密碼強度必須包含	☑數字☑小寫字母□大寫字母□符號				

允許用戶更改密碼:

啟用此功能,允許用戶可以在 WebMail 介面下 自行更改帳號密碼, 若關閉此功能 ,則更改密碼必 須由管理員實施

強迫用戶定時更換密碼:

開啓此功能 將會強迫建議用戶 一段時間內(密碼有效天數)必須更改一次密碼

將逾期帳號停用:

逾期未更換密碼用戶將被停用,若未開啟此功能則系統僅會發通知警告用戶

密碼有效天數:

設定 用戶多久內必須要更改一次密碼

逾期前幾天通知用戶:

設定密碼到期前幾天 開始通知用戶 準備要更改密碼了

通知信主旨:

通知吹促用戶更改密碼的信件 可套用變數: #DAY: 尚餘日數 #DATE: 到期日 範例: 請注意! 您的密碼請在#DAY內更換 通知信內容: 通知吹促用戶更改密碼的信件:內容可套用變數:

#DAY: 尚餘日數 #DATE: 到期日

範例: 您必須於 #DAY 日內更換新的密碼,否則帳號將於 #DATE 到期,到期後您將無法登入.

例外帳號:

設定例外帳號 可以不受的 此規則約束 , 多個帳號可以用 逗點 或分號 分開 密碼長度至少 : 設定 密碼長度至少要多少個字元 密碼強度必須包含 : 設定密碼強度 ,密碼必須包含那些元素 , 數字 / 小寫字母 / 大寫字母 / 符號

用戶通知設定



空間配額屆滿通知

啟用此功能 當用戶空間快滿之前,系統會發出通知信 通知用戶 或管理員

通知信主旨

可套用變數:

#QUOTA:配置硬碟容量

#USED:目前已使用

範例:請注意! #USER 您的配置硬碟空即將屆滿

通知信內容

可套用變數:

#QUOTA:配置硬碟容量

#USED:目前已使用

範例: 您的帳號: #USER 配置硬碟: #QUOTA 目前使用: #USED 請儘速刪除舊信件或個人空間下的檔案,如無法排除請聯絡伺服器管理員.

通知指定管理員

當狀況發生時即時通知管理員,輸入本機帳號(非完整 Email),多人可用 『,』逗號 『;』分號,空格或 跳行 隔開皆可

申請與審核

基本設定申請者列表	
	☑ 了解什麼是帳號申請與審
啓用服務	開啓
審核人員	jerry x
帳號申請須知	新進人員可以在此進行新電子信箱帳號申請,請注意以下須知: 1. 僅允許公司/單位人員提出申請 2. 姓名欄位請填寫真實姓名
❷ 審核通知信的主旨	請審核此新進帳號申請,並決定是否新增此帳號
❷ 審核通知信內容	目前有一人員透過帳號系統進行新帳號申請,請您查看以下申請資訊並審核是否允許此帳號建立.申請資料如下:
❷ 使用圖形檢查碼	開閉
❷ 審核結果通知書主旨	#USER#(#NAME#)::帳號申請審核結果通知書
② 審核結果通知書內容	#NAME# 您好, 你所申請的帳號:#USER#,目前申請結果如下 結果:#RESULT#

帳號申請與審核可以提供新進人員自己填表申請之後由系統管理員審核通過的方式來建立新進帳號 啟動此功能後,在 WebMail 介面的登入畫面會增加一個申請帳號的按鈕



vvv.dom WebMail 申請帳號

新進人員可以在此進行新電子信箱帳號申請,請注意以下須知:

- 1. 僅允許公司/單位人員提出申請
- 2. 姓名欄位請填寫真實姓名
- 3. 帳號至少要2碼,最多為30碼,只能使用英文小寫及數字或符號._-
- 4. 密碼至少為6碼,必須包含 英文小寫+大寫+數字+符號,例如 Abcd\$123,符號不能有:(冒號)
- 5. 請提供一個目前您可以收到信件的Email信箱,申請結果會以Email通知

王小美

may.wang

......

● 按一下眼睛,顯示或隱藏密碼

vvv@vvv.dom

我是王小美,新進人員請多多指教

886656

886656

申請帳號

返回登入頁面

審核人員

設定當申請提出後由誰(本機的帳號)來進行審核,審核者可以有多位,優先審核通過者申請即通過, 審核通過會被記錄在系統日誌的事件記錄內

帳號申請須知

設定顯示在申請表單最上面的申請須知說明

審核通知信的主旨

設定當申請者提出申請後 寄發給審核者的通知信主旨

審核通知信內容

設定當申請者提出申請後 寄發給審核者的通知信的內容

其中有幾個變數可以套用

姓名:#NAME# 帳號:#USER#

密碼:#PASSWORD#

信箱:#EMAIL# 申請時間:#DATE#

備註:#MEMO#

按 {Y[准于建立]} 審核通過建立此帳號

按 {N[不允許建立]} 審核不通過

審核按鈕語法 其中 {Y[????]} 中的 ???? 可以自訂修改

使用圖形檢查碼

設定申請表單時 是否要使用圖形驗證來避免網路機器人的攻擊

審核結果通知書主旨

設定審核者審查之後的結果透過信件寄發給申請者的主旨

變數可用

帳號:#USER#

姓名:#NAME#

審核結果通知書內容

設定審核者審查之後的結果透過信件寄發給申請者的內容

變數可用

帳號:#USER#

姓名:#NAME#

結果:#RESULT#

申請人送出申請表單後 指定管理員會收到一封格式如下的審核信件

請審核此新進帳號申請,並決定是否新增此帳號

Date: 2022-04-14 12:07:33

From: <admin@localhost.localdomain> IIII
To: <admin@localhost.localdomain> IIII

目前有一人員透過帳號系統進行新帳號申請,請您查看以下申請資訊並審核是否允許此帳號建立.

申請資料如下: 姓名:王小美 帳號:may.wang 密碼:a123b321 信箱:vvv@vvv.dom

申請時間: 2022-04-14 12:07:33 備註: 我是王小美,新進人員請多多指教

按[准于建立] 審核通過建立此帳號

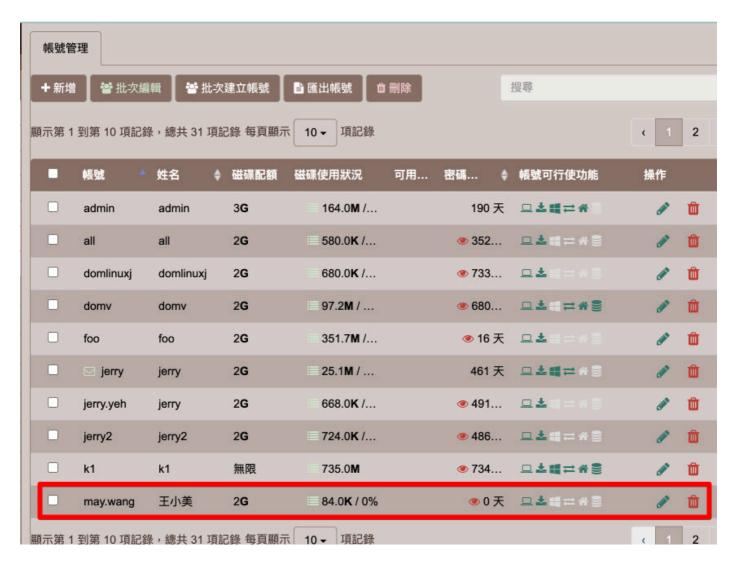
按[不允許建立] 審核不通過

審核者 可以按下 准予建立 或 不準許建立

管理員可以申請者列表看到



在備註欄位上可以看到 什麼時間由誰允許建立此帳號



在帳號管理上可以看到 王小美 已經被建立帳號

王小美也會在他自己的備用帳號上收到通知信,通知帳號申請已經成功



你所申請的帳號:may.wang,目前申請結果如下

結果:成功

王小美可以使用申請的帳號進行登入

vvv.don	n WebMai	电丁后和	1	
may.war	ng			
登入				申請帳號

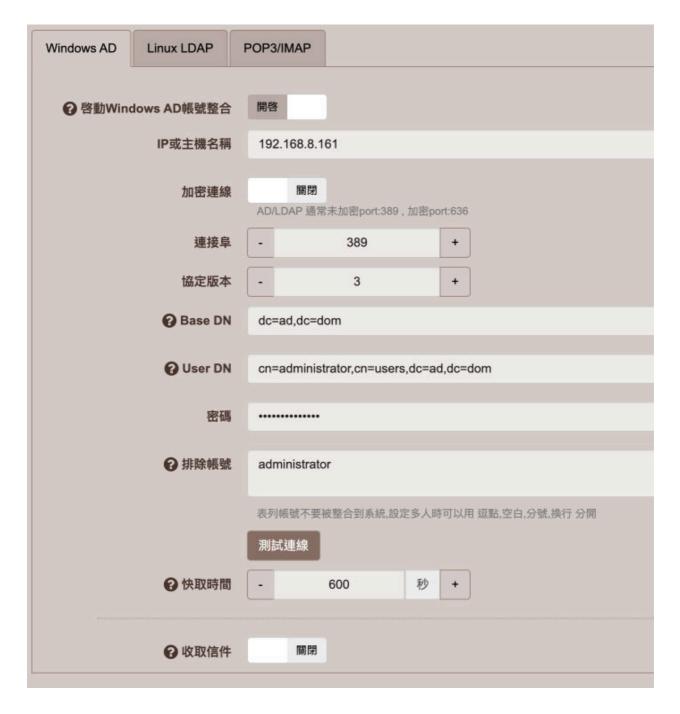
帳號整合



帳號整合功能,可以讓其他正在運作的服務器例如 Windows AD, LDAP 伺服器或是其他品牌的郵件伺服器(提供有 POP 或 IMAP 服務),通過帳號整合功能將其帳號學習並與本系統合併.

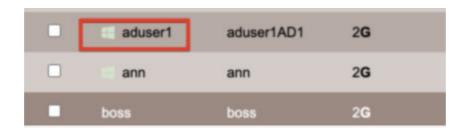
可以使用其帳號接收對應的郵件伺服器的信件,帳號整合功能是將其目標伺服器的帳號與密碼學習 過來並在本地端自動建立相同的帳號密碼

Windows AD



- 可以在設定好的場景下將 AD 帳號與密碼自動建立於本系統下
- 首先必須設定好下列的各項設定,並以連線測試完成確認後,在以下幾個場景下可以自動建立帳號
- 1. 當原先的用戶使用 AD的帳號與密碼登入本系統時,如果系統上尚未有該帳號時,系統會自動建立該帳號與密碼,登入動作包含以 webmail 登入或 pop3,pop3s,imap,imaps 登入方式
- 2. 當信件寄到該帳號時,系統若確認該帳號在 AD 是存在的帳號時,此時系統會自動建立該帳號,並將此信件收下,不過因為還不知道該帳號的密碼,所以暫時以系統內建的亂數密碼取代,等候使用者第一次登入時系統會自動校正正確的密碼.

- 如果 AD 更改密碼時 , 系統容許用戶使用舊密碼及新密碼登入 , 但一旦使用新密碼登入後 , 舊密碼就不再可以用來登入
- 如果AD帳號刪除後,系統上的帳號不會自動刪除,若需要刪除帳號需要管理員自行刪除帳號
- 帳號若是使用 AD 整合的來源帳號,在帳號的前方會有一個窗旗標提示



一旦帳號在本地更改密碼,且密碼與AD密碼不同時,AD整合的關聯性即斷開,若要重新關聯必須將密碼設定與AD相同之後再連線後即可

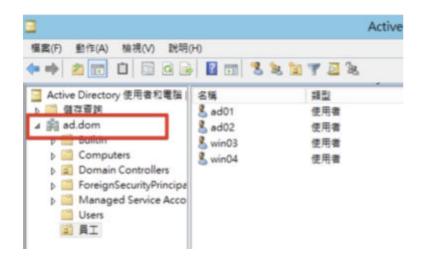
設定項目:

• IP 或主機名稱: 輸入 windows AD 的服務器 IP 或 fqdn 名稱

加密連線:如果您公司內的 AD 伺服器 需要加密連線請啟用

• 連接阜/協定:請依照公司內的 AD 伺服器設定

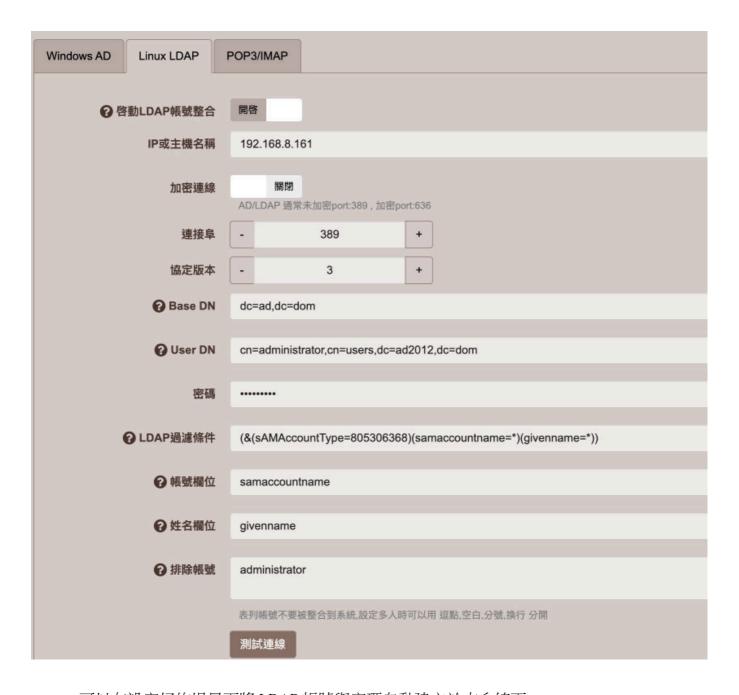
Base DN:務必與您的 AD 伺服器上的設定相同



- User DN: UserDN 通常是設定 Administrator, 但也可以使用有同等權限的 AD 使用者, 通常 administrator 位於 cn=users 的樹下,所以可寫成 cn=administrator,cn=users,dc=ad,dc=dom
- 排除帳號:如果在帳號整合時不想該帳號被自動整合學習時可以加入排除,多個帳號可以 用,或空白或換行來表示
- 快取時間:當外部信件寄到本系統時若帳號不存在時,本系統會去查詢AD 伺服器,詢問是 否帳號存在,這個快取時間表示 在指定時間內只會去詢問一次,系統會在本機建立快取資料,當快取資料逾時後才會再去AD詢問一次帳號列表,以免太過頻繁查詢AD,造成AD 伺服器的負擔

- 收取信件:當帳號被整合後,系統可以設定自動去收取指定的郵件伺服器,將信件一併整合收到這個帳號的信箱內,目標伺服器收取的信件後不會將該信件刪除,系統會自動比對信件是否郵件收取過,並只收取新信件
 - 。 嘗試本地帳號收信: 啟用此功能,系統在收取整合伺服器信件時回嘗試本地端其他的帳 號,若帳號密碼符合登入條件時會自動下載該帳號對應的郵件.
 - 。 郵件伺服器 IP 或主機名稱: 要收取信件的目標郵件伺服器.
 - 。 通訊協定:通訊協定若使用 pop3,只會收取該伺服器的 INBOX 信件匣,若設定為 IMAP 會連同所有的信件匣全部收到並自動建立相同的信件匣,通常建議使用 imap.
 - 。 加密連線:若目標伺服器有支援加密可以啟用,建議若是伺服器都在內部可以使用不加密,若是在不同的網段時建議使用加密.
 - 。 帳號樣式:設定目標伺服器登入時需要的帳號樣式 是僅帳號 還是需要代入伺服器名稱,若伺使用 帳號@網域 方式時 相同會自動代入 "郵件伺服器 IP 或主機名稱" 這個欄位的設定在 @ 之後,所以這個欄位必須設定為 FQDN,而不能使用 IP.
- **嘗試本地帳號收信**: 在收取信件時將不是由 AD 整合的帳號 也嘗試使用本地的帳號密碼去收取信件,成功條件為帳號與密碼必須與 AD 內的帳號密碼相同

Linux LDAP



- 可以在設定好的場景下將 LDAP 帳號與密碼自動建立於本系統下
- 首先必須設定好下列的各項設定,並以連線測試完成確認後,在以下幾個場景下可以自動建立帳號
 - 1. 當原先的用戶使用 LDAP 的帳號與密碼登入本系統時,如果系統上尚未有該帳號時, 系統會自動建立該帳號與密碼,登入動作包含 以 webmail 登入或 pop3,pop3s,imap,imaps 登入方式
 - 2. 當信件寄到該帳號時,系統若確認該帳號在 LDAP 是存在的帳號時,此時系統會自動建立該帳號,並將此信件收下,不過因為還不知道該帳號的密碼,所以暫時以系統內建的亂數密碼取代,等候使用者第一次登入時系統會自動校正正確的密碼.
- 如果 LDAP 更改密碼時 , 系統容許用戶使用舊密碼及新密碼登入 , 但一旦使用新密碼登入 後 , 舊密碼就不再可以用來登入

- 如果 LDAP 帳號刪除後, 系統上的帳號不會自動刪除, 若需要刪除帳號需要管理員自行刪除 帳號
- 帳號若是使用 LDAP 整合的來源帳號,在帳號的前方會有一個企鵝旗標提示



一旦帳號在本地更改密碼,且密碼與 LDAP 密碼不同時,LDAP 整合的關聯性即斷開 ,若要重新關聯 必須將密碼設定與 LDAP 相同之後再連線後即可

設定項目

- IP 或主機名稱:輸入 Linux/LDAP 的服務器 IP 或 fqdn 名稱
- 加密連線:如果您公司內的 LDAP 伺服器 需要加密連線請啟用
- 連接阜/協定:請依照公司內的 LDAP 伺服器設定
- Base DN:務必與您的 LDAP 伺服器上的設定相同
- User DN: UserDN 通常是設定 root, 但也可以使用有同等權限的 LDAP 使用者
- LDAP 過濾條件:請參考您的LDAP的設定架構,如不清楚設定 請洽詢 LDAP 伺服器管理員或使用 LDAP browser 類所工具查看 LDAP 的架構
- 帳號欄位:指定用 LDAP 的那個欄位(機碼)當作帳號欄位,通常可能是 uid
- 姓名欄位:指定用 LDAP 的那個欄位(機碼)當作姓名欄位,通常可能是 gecos
- 排除帳號:如果在帳號整合時不想該帳號被自動整合學習時可以加入排除,多個帳號可以 用,或空白或換行來表示
- 快取時間:當外部信件寄到本系統時若帳號不存在時,本系統會去查詢LDAP 伺服器,詢問是否帳號存在,這個快取時間表示 在指定時間內只會去詢問一次,系統會在本機建立快取資料,當快取資料逾時後才會再去LDAP詢問一次帳號列表,以免太過頻繁查詢LDAP,造成LDAP 伺服器的負擔
- 收取信件:當帳號被整合後,系統可以設定自動去收取指定的郵件伺服器,將信件一併整合 收到這個帳號的信箱內,目標伺服器收取的信件後不會將該信件刪除,系統會自動比對信件 是否郵件收取過,並只收取新信件
 - 。 嘗試本地帳號收信: 啟用此功能,系統在收取整合伺服器信件時回嘗試本地端其他的帳 號,若帳號密碼符合登入條件時會自動下載該帳號對應的郵件.
 - 。 郵件伺服器 IP 或主機名稱: 要收取信件的目標郵件伺服器.
 - 。 通訊協定:通訊協定若使用 pop3,只會收取該伺服器的 INBOX 信件匣,若設定為 IMAP 會連同所有的信件匣全部收到並自動建立相同的信件匣,通常建議使用 imap.

- 。 加密連線:若目標伺服器有支援加密可以啟用,建議若是伺服器都在內部可以使用不加密,若是在不同的網段時建議使用加密.
- 。 帳號樣式:設定目標伺服器登入時需要的帳號樣式 是僅帳號 還是需要代入伺服器名稱,若伺使用 帳號@網域 方式時 相同會自動代入 "郵件伺服器 IP 或主機名稱" 這個欄位的設定在 @ 之後,所以這個欄位必須設定為 FODN,而不能使用 IP.
- **嘗試本地帳號收信**:在收取信件時將不是由整合的帳號 也嘗試使用本地的帳號密碼去收取信件,成功條件為帳號與密碼必須與整合端內的帳號密碼相同

POP3 IMAP

Windows AD Linux LDAP	POP3/IMAP
② 啓動POP/IMAP帳號整合	開啓
IP或主機名稱	192.168.8.160
❷ 通訊協定	IMAP
② 加密連線	關閉
❷ 帳號樣式	僅帳號
● 排除帳號	admin
	表列帳號不要被整合到系統,設定多人時可以用 逗點,空白,分號,換行 分開
② 收取信件	開啓
❷ 嘗試本地帳號收信	開客 取用此功能,系統在收取整合伺服器信件時回嘗試本地端其他的帳號,若帳號密碼符合登入條件時會自動件。
❷ 測試連線	關閉

- 可以在設定好的場景下將 LDAP 帳號與密碼自動建立於本系統下,首先必須設定好下列的各項設定,並以連線測試完成確認後,在以下幾個場景下可以自動建立帳號
- 當原先的用戶使用的帳號與密碼登入本系統時,如果系統上尚未有該帳號時,系統會自動建立該帳號與密碼登入動作包含以 webmail 登入或用戶端(例如 outlook)pop3,pop3s,imap,imaps 登入方式
- 如果被整合的伺服器更改密碼時 , 系統容許用戶使用舊密碼及新密碼登入 , 但一旦使用新密碼登入後 , 舊密碼就不再可以用來登入
- 如果被整合的伺服器帳號刪除後,系統上的帳號不會自動刪除,若需要刪除帳號需要管理員自行刪除帳號

帳號若是使用 POP/IMAP 整合的來源帳號,在帳號的前方會有一個信箱旗標提示



一旦帳號在本地更改密碼,且密碼與被整合的伺服器密碼不同時 ,整合的關聯性即斷開 ,若要重新 關聯必須將密碼設定與被整合的伺服器相同之後再連線後即可

設定項目

- IP 或主機名稱:輸入 POP/IMAP 被整合伺服器 IP 或 fqdn 名稱
- 通訊協定: 通訊協定若使用 pop3, 只會收取該伺服器的 INBOX 信件匣, 若設定為 IMAP 會連同所有的信件匣全部收到並自動建立相同的信件匣, 通常建議使用 imap.
- 加密連線:如果伺服器需要加密連線請啟用
- 帳號樣式:設定目標伺服器登入時需要的帳號樣式 是僅帳號 還是需要代入伺服器名稱,若 伺使用 帳號@網域 方式時 相同會自動代入 "郵件伺服器 IP 或主機名稱" 這個欄位的設定在 @ 之後,所以這個欄位必須設定為 FQDN,而不能使用 IP.
- 排除帳號:如果在帳號整合時不想該帳號被自動整合學習時可以加入排除,多個帳號可以 用,或空白或換行來表示
- 收取信件:當帳號被整合後,系統可以設定自動去收取指定的郵件伺服器,將信件一併整合 收到這個帳號的信箱內,目標伺服器收取的信件後不會將該信件刪除,系統會自動比對信件 是否郵件收取過,並只收取新信件
- 嘗試本地帳號收信: 啟用此功能,系統在收取整合伺服器信件時回嘗試本地端其他的帳號,若 帳號密碼符合登入條件時會自動下載該帳號對應的郵件.
- 測試連線:依照上方的參數設定進行一次連線測試
 - 。 測試帳號: 輸入欲收取信件的伺服器前可以登入的帳號
 - 。 密碼: 輸入測試帳號的密碼
 - 。 按下測試連線,確認上面的設定及欲整合的伺服器符合整合條件
- **嘗試本地帳號收信**:在收取信件時將不是由整合的帳號 也嘗試使用本地的帳號密碼去收取信件,成功條件為帳號與密碼必須與整合端內的帳號密碼相同

公佈欄

公佈欄	
	0 7
啓用服料	新 爾
公告標品	例如: 公司公告
字體大	14 +
掩動速息	10 +
預	:這是公佈欄設定的預覽結果,您可以調整字體
允許發佈新訊息人員名目	admin admin
	輸入本機條號名單,例如: john,mary 或 * 表示所有人,減號表示扣除 例如 * .jerry,可用 迴點 分號 空白 換行 隔開多筆 符合上列表列人員,可在 Webmail 介面上的 『公佈欄』之『發佈公告』功能內進行發佈公告,其餘人員僅可以復報公布內容
	確定

啟動公布欄功能後 若指定可發佈訊息的人員發佈訊息後, 指定收訊息的人員可以在 WebMail 的頂端看到跑馬燈訊息

設定項目:

- 啓用服務: 啟動服務後用戶才會在 webmail 的上方功能項目看到此功能
- 公告標題:在每則公告的最前面添加的提醒標題
- 字體大小: 設定公告使用的字體大小
- 捲動速度:設定公告跑馬燈捲動的速度
- 允許發佈新訊息人員名單:設定表列人員才具備有發佈公告的權利,
 - 。 輸入本機帳號名單 ,例如: john,mary 或 * 表示所有人
 - 。 減號表示扣除 例如 *,-jerry
 - 。 可用 逗點 分號 空白 換行 隔開多筆 符合上列表列人員 , 可在 Webmail 介面上的 『公佈欄』之『發佈公告』功能內進行發佈公告 , 其餘人員僅可以查看公布內容 發佈 公告人員可以在 WebMail 介面內進行公告的發佈及管理 , 發佈者可以觀察到哪些人已 經看過這個公布欄事項

發佈公布事項



- 被管理員指定為允許發布訊息人員,可以進行訊息發布,其餘人員僅能查看發布的訊息
- 在 WebMail / 公佈欄,選擇公布發佈管理,此處可看到關於您自己發佈的訊息,包含可以 看到有那些人應該讀取那些人已經讀取及讀取的時間



用戶按下跑馬燈標題查看內容



用戶在 WebMail 跑馬燈顯示 ,按下標題 或是進入公布欄頁面查看內容,已經查看過的公告事項不會再出現在跑馬燈箱上 ,若需查看需進入公佈欄項目內查看歷史公告



行事曆

可以讓用戶在 WebMail 介面下規劃自己的行事曆,管理員可以制訂行事曆群組,讓群組成員可以 新增共享的行程



設定群組成員



SMTP 服務設定

基本設定

 ・	基本設定 進階設定 防護設定	世 地址化名 雜項設定
a.dom b.dom		
■重置WEBMAIL環境設定內之寄信身份列表設定 ② SMTP歡迎詞 MailServer ready. 例如:welcome to mail server for our company,建議盡量用英文語詞. 192.168.8.66 通常保留空白,或輸入IP:10.1.1.1.或整個網段:10.1.1.0/24,多個項目請以就行隔開 ② 一封信件最大容量 — 500 MB + 信件中的附件因馬傳遞中需要重新編碼,所以通常會比原來膨脹約30%,如有經常寄送大檔案附件時需稍放寬此 ② 一封信件最多收件人 — 300 人 + 設定一封信件最多收件人可以寄給過少收件者 ② 多收件者分割寄送 — 50 人 + 若一封信件收太多時,系統會將收件者分批次寄出,每次分配收件者最多以此數量。 分割分次寄送可避免對方何服器拒絕單封信太多收件者。	→ 伺服器名稱	a.dom
例如:welcome to mail server for our company , 建議盡量用英文語詞. 192.168.8.66 通常保留空白,或輸入IP:10.1.1.1,或整個網段:10.1.1.0/24 , 多個項目請以跳行隔開 - 對信件最大容量 - 500 MB + 信件中的附件因爲傳遞中需要重新編碼,所以通常會比原來膨脹約30%,如有經常寄送大檔案附件時需稍放寬此 - 對信件最多收件人 - 500 人 + 設定一對信件最多收件人可以寄給過少收件者 - 50 人 + 若一封信件收太多時,系統會將收件者分批次寄出,每次分配收件者最多以此數量。 分割分次寄送可避免對方何服器拒絕單封信太多收件者。		
② 允許Relay來源 192.168.8.66 通常保留空白,或輸入IP:10.1.1.1,或整個網段:10.1.1.0/24,多個項目請以跳行隔開 ② 一封信件最大容量 - 500 MB + 信件中的附件因爲傳遞中需要重新編碼,所以通常會比原來膨脹約30%,如有經常寄送大檔案附件時需稍放寬此 ② 一封信件最多收件人 - 500 人 + 設定一封信件最多收件人可以寄給過少收件者 - 50 人 + 若一封信件收太多時,系統會將收件者分批次寄出,每次分配收件者最多以此數量。分割分次寄送可避免對方何服器拒絕單封信太多收件者.	❷ SMTP歡迎詞	MailServer ready.
通常保留空白,或輸入IP:10.1.1.1,或整個網段:10.1.1.0/24,多個项目請以跳行隔開	0 (1111) 177	
② 一封信件最大容量 - 500 MB + 信件中的附件因爲傳遞中需要重新編碼,所以通常會比原來膨脹約30%,如有經常寄送大檔案附件時需稍放寬此 ② 一封信件最多收件人 - 500 人 + 設定一封信件最多收件人可以寄給過少收件者 - 50 人 + 若一封信件收太多時,系統會將收件者分批次寄出,每次分配收件者最多以此數量。分割分次寄送可避免對方何服器拒絕單封信太多收件者.	が が が が が が が が の の の の の の の の の の の の の	192.168.8.66
信件中的附件因爲傳遞中需要重新編碼,所以通常會比原來膨脹約30%,如有經常寄送大檔案附件時需稍放寬此 - 對信件最多收件人		通常保留空白,或輸入IP:10.1.1.1,或整個網段:10.1.1.0/24,多個项目請以跳行隔開
設定一封信件最多收件人可以寄給過少收件者 - 50	❷ 一封信件最大容量	
 ② 多收件者分割寄送 若一封信件收太多時,系統會將收件者分批次寄出,每次分配收件者最多以此數量。 分割分次寄送可避免對方何服器拒絕單封信太多收件者。 	❷ 一封信件最多收件人	
分割分次寄送可避免對方伺服器拒絕單封信太多收件者.	② 多收件者分割寄送	
		分割分次寄送可避免對方伺服器拒絕單封信太多收件者.

啟用服務:

設定啟用或停止 SMTP(s)服務

服務狀態:

顯示服務目前的執行狀態

master pid: 主程式的執行序號(每次啟動都會不同)

saslauthd pid: smtp 認證寄信程序的執行序號(通常每次也都會不同)

伺服器名稱:

設設定 smtp 伺服器名稱,此名稱通常是 您的網域名稱(根據網域管理 MX 設定),

多個網域可以填寫多行,錯誤的設定可能會拒絕收信

MX 設定 狀況一

mydomain.com MX 10 mydomain.com 這樣的範例僅需填寫: mydomain.com

MX 設定 狀況二:

mydomain.com MX 10 mail.mydomain.com 這樣的範例 需填寫兩行 mydomain.com mail.mydomain.com

SMTP 歡迎詞:

伺服器收到 smtp 交談時的 EHLO 所發出的禮貌性 回覆詞,通常是表明我方的公司名稱或代表詞

允許 Relay 來源:

填寫在此處的 IP 或網段 表示這些來源 "不需要" 經過認證即可寄信,通常這裏沒必要不需填寫任何 內容

下列狀況可能會需要指定:

狀況一:例如公司的無人看管的傳真印表機 ,當收到傳真時轉 Email ,此時可以將該傳真機 IP 填寫 到此

狀況二:若要幫其他的伺服器代轉信件時,可填寫該伺服器 IP

狀況三:公司 ERP 軟體,有寄信需求 軟體設計上沒有 smtp 帳號認證功能時

一封信最大容量:

設定單一封信件最大容量,通常除了考量本身的伺服器設定外,如果是寄給別人的伺服器還要考慮對方是否要接收太大的信件,所以通常不應設定過大

另外郵件夾帶的附件檔會因為信件傳送時的編碼,附件的大小通常會比原來的檔案大小膨脹約 1.3 倍,這些都是設定此參數需考慮的因素.

一封信件最多收件人:

設定單一封信最多能夠有多少收件者,最高值為 3000,但不建議設定太大的值,通常建議 100 以下,超過人數處理原則 通常是看發信軟體決定,例如 outlook 可能是全信不發,有些發信軟體是能發幾人算幾人這些原則不是伺服器決定,另外也有可能因為收件者在不同伺服器,或人數過多時由 "多收件者分割寄送" 的參數,將信件分割成多人多次寄送(分割信件的 messaie-id 會都相同)

多收件者分割寄送:

若一封信件收太多時,系統會將收件者分批次寄出,每次分配收件者最多以此數量,分割分次寄送可避免對方伺服器拒絕單封信太多收件者,但可能會影響郵件過濾器條件比對的精確性.

進階設定



外寄伺服器:

此欄位通常是保留空白直接由本機的 SMTP 信件發送 , 下列狀況可能會需要設定.

應用場景 一: 你有代理的 SMTP 伺服器,例如 spam/antivirus gateway,可以填寫該機器 IP

應用場景 二:你的 IP 被列入黑名單 ,可暫時將此設定願意幫你代寄信件的伺服器 ,通常可能是你的上游單位 或 ISP ,例如是 mas.hinet.net 或 168.95.4.211

儲列重試間隔:

傳送失敗或延遲的信件將會暫時在儲列排隊等候發送,等待之信件會在此時間後嘗試發送 ,同一封信次失敗多次後會自動增加(拉長)重試的時間 ,以減少系統的資源浪費

儲列保存時間:

信件在儲列重試一直到保存時間過後若無法寄送成功,信件將會放棄寄送並刪除 , 一般都會傳送退信 訊息給寄件者

網路協定:

設定是否使用 ipv6 或僅使用 ipv4,通常這必須看你的網路環境來決定

伺服器 TLS 傳輸:

設定伺服器對伺服器傳輸時是否使用加密方式,通常建議設定讓系統自動判斷

TLS 加密層級:

設定使用加密的最低層級 , 若設定為 TLSv1, 意味接受 TLSV1+V1.1+V1.2+V1.3,

一般企業建議設定在 TLSv1 避免客戶伺服器系統老舊無法與我方伺服器通訊

若為公家單位因應上級單位稽查,建議設定在 TLSV1.2

密碼(ciphers)等級:

通常設定為中級 , 若公家單位因應稽核可以調整為高級 , 但若是對於對方是較舊的郵件伺服器系統, 可能會無法與我方伺服器對應連線的問題

寄信帳號認證:

設定用戶在寄信時是否需要使用帳號認證,若停用認證:只有允許 Relay 來源列表 IP 的電腦可以不需認證直接寄信.否則用戶必須在郵件軟體(例如 outlook)勾選:我的伺服器需要認證.

SMTP 連線逾時:

當 smtp(通常是 tcp/port:25 連線)閒置超過指定時間,系統將會主動將連線剔除(disconnect),如果伺服器線路不穩定或頻寬不足時可以調整數值較大,避免非預期斷線影響收發品質

SMTP 最大連線數:

設定 SMTP 同時間可以平行處理連線的能力,如果伺服器有較大的效能及頻寬可以調大數值

無此收件人退信行爲:

設定伺服器收信時收件者錯誤的處理方式 無此收件人

退回: 退回對方伺服器 .告知對方沒有這個收件者避免寄件人筆誤寫錯名字

不回應: 不退訊息給對方伺服器,直接刪除此信, 丟棄此信,避免的=寄件人用來探測是否有此帳號

防護設定



來信 SPF 檢查:

SPF 主要的功能是郵件伺服器根據來信中寄件者網域資料主動去向寄信端所屬的 DNS 伺服器核對其 SPF 紀錄,依照比對結果做接收與否的決定.

SPF 主要的目的就是避免別人冒用網域名稱寄信, 此功能會檢查 來信的 spf , 如果不符合系統會依照 spf 的設定予以拒絕 ,是目前防偽造信件非常有效的工具 .

例外網域:

列出的網域不會受到 SPF 檢查 , 若來信對象的 SPF 設定有誤 , 或避免誤退對方信件 , 可以將這些網域加入例外名單

例外 IP:

列出的IP不會受到SPF檢查,例如 1.2.3.4,或 1.2.3.0/24,每個設定可用 逗點,空白,分號或跳行隔開

防止帳號盜用機制:

此機制啟動後,當用戶寄信時會檢查認證帳號與寄件者 email 是否一致,此功能可預防萬一帳號密碼被 猜到或是被盜取時,盜用者僞造寄件者 email 隨意發信

通知用戶:當機制被觸發時以 email 通知用戶該認證帳號之用戶

通知指定管理員: 當機制被觸發時以 email 通知指定的管理員

通知主旨: 設定通知信的主旨

通知內容:設定通知信的內容

通知信發送間隔:防止連續寄發通知信,可設定每次發送通知信至少間隔時間

例外帳號:表列出的帳號可以不被此規則監視,但務必要設定具複雜的密碼

限制帳號單日發送數量:

啓用此功能可以限制每位用戶單日發送信件(收件人)數量,數量是以收件人數計算,如果一封信寄給 10 個收件者,計數器爲 10

限制發送量:設定每人每天發信數量限制數,每日凌晨 00:00 計數器歸零

內部帳號不列入計數:勾選此項目會忽略計數寄給內部伺服器的人員

通知用戶:當機制被觸發時以email 通知用戶該認證帳號之用戶

通知指定管理員:當機制被觸發時以email 通知指定的管理員

通知主旨:設定通知信的主旨

通知內容:設定通知信的內容

通知信發送間隔:防止連續寄發通知信,可設定每次發送通知信至少間隔時間

例外帳號:表列出的帳號可以不被此規則監視,但務必要設定具複雜的密碼

儲列保護值:

設定一個儲列上限保護值,目前預設是 3000, 儲列超過此值時伺服器的 smtp 服務將會暫時停止服務,直 到伺服器管理員將問題排除後 smtp 服務會自動啟動

儲列通常在伺服器正常運作下不太可能和堆積太多的信件,這問題通常會發生在伺服器被當跳板大量寄信,而最終問題可能是某位用戶的帳號密碼設定太過於簡單或電腦被木馬病毒入侵,以至於帳號密碼被盜用,用來執行大量垃圾信的寄發

合理的設定此數值可以有效的防護伺服器,當遭受帳號盜用時可以減少伺服器的信譽損失

地址化名



郵件地址化名設定可幫助用戶在不更改用戶信件軟體(例如 outlook)設定下由伺服器端自動改寫信件內的 emai 地址.

例如 在寄件者地址設定:

jerry sales, 這個設定表示帳號 jerry 寄信時寄件者 將被改寫成 sales.網域保持不變

@abc.com @xyz.com, 這個設定表示整個 @abc 寄出的信件,寄件者網域將會被改為 @xyz.com

使用場景:

例如: mail 這個帳號系統保留帳號, 通常是無法使用來收發信件, 但是某些時候一定要使用這個 名稱時, 此時可透過這功能來達到使用要求

•

。 首先先建立一個帳號: 例如 mymail

。 在寄信者地址化名欄位輸入: mymail mail

。 在收信者地址化名欄位輸入: mail mymail

如此設定後 當 mymail 寄信給對方,對方看到的收件者會是 mail 而不會是 mymail

當對方回信給 mail@ 到我們自己的伺服器後 會自動化名為 mymail@,信會進入 mymail 用戶的信箱,且在收件者欄位上看到的是 mymail@ 而不是 mail@

雜項設定

超大附件轉超連結

超大附件轉超連結	開啓 此功能可將寄信原本的附件自動提出並轉換爲超連結,可防止收件方伺服器無法收取太大的信件或允許信件。 將存於伺服器數日,收件者可以按下超連結下載該附件.			
❷ 附件大小	- 1 MB + 當附件大小超過此設定值,將該附件轉換爲超連結			
❷ 附件保存天數	- 7 天 + 收件者必須在收到信件在此天數內下載此附件,逾期此附件將自動刪除			
❷ 附件下載提示	- 下載提示 請在 %DATE% 前, 按以下連結下載附件, 或將超連結拷貝至瀏覽器.			
	此提示語將增加於本文最前方,可用變數 %DATE%:檔案下載期限日期			

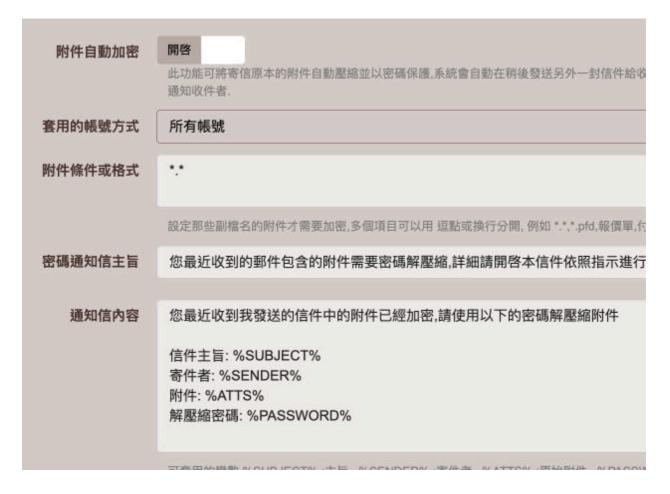
此功能可將寄信原本的附件(超過設定大小)自動提出並轉換爲超連結,可防止收件方伺服器無法收取太大的信件或不允許信件內有附件,轉換後附件將存於伺服器數日,收件者可以按下超連結下載該附件.

附件大小: 設定超過多大的附件要轉換成超連結

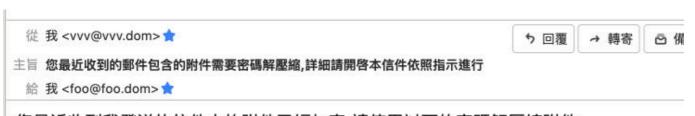
附件保存天數: 設定轉換後的超連結要在伺服器內保留多少天,在這個天數內收件者可以按下信件 內的超連結取回附件

附件下載提示: 設定轉換為超連結的附件在信件的本文如何顯示提示, 此提示語將增加於本文最前方,可用變數 %DATE%: 檔案下載期限日期

附件自動加密



此功能會將符合條件的信件內的附件自動用 zip 壓縮並加密碼(密碼隨機產生),並自動在稍後將密碼以信件方式寄送通知給原收件者



您最近收到我發送的信件中的附件已經加密,請使用以下的密碼解壓縮附件

信件主旨: 防疫戰略已變! 名醫: 自然感染增加, 有助群體免疫與抗體維持

寄件者: vvv@vvv.dom 附件: 測試報價單.pdf 解壓縮密碼: Id5YzFjf

Updated on 2022 年 4 月 14 日

POP IMAP 服務設定

提供給用戶端 例如 Outlook 透過此 2 項服務來伺服器的個人帳號內提取信件

基本設定						
	啓用服務	開啓				
	服務狀態	服務中, ver:	2.3.17 , pid: 394	19		
	啟用Webmail服務	開啓				
	❷ POP迎賓詞	MailServer pop3/imap ready.				
		例如:pop3/im	ap service ready.			
	2 最大連線數	-	800	+		
	2 最大同時處理數	-	100	+		
	② 單IP最大連線數	-	10	+		
	相容模式	□降低伺服器	SSSL加密的規格	B及加密演算法	以相容舊版的收信軟體,例如:舊版本 ou	
ħ	禁止密碼以明碼方式傳送	□通常建議局	效用避免密碼被提	闡截,但若是用戶	使用較舊的郵件軟體有可能會無法登入	
	僅允許加密連線	□關閉非加密	密阜 pop3:110 / ii	map:143,僅允	許使用 pop3s:995 / imaps:993 連線	

啓用服務:

設定是否啟動服務

服務狀態:

顯示服務是否正確服務中, 及執行的 PID

啟用 Webmail 服務:

設定是否要啟動 WebMail(網頁式收信端)

POP 迎賓詞:

當用戶端軟體與 pop3 伺服器連線時 發出的禮貌性用詞

最大連線數:

設定 imap/pop3 同一時間的最大連線數

最大同時處理數:

同一時間可以處理(process)的數量

單 IP 最大連線數:

允許從相同IP連線數,這通常可能是公司從同一個閘道出口來連結伺服器,有此狀況時建議將此設定值調整稍大

相容模式:

如果你的用戶有使用舊版軟體,例如:舊版本 outlook(例如 2003) 來收發 email,可能需要將此相容模式功能啓動,降低伺服器 SSL 加密的規格及加密演算法以相容舊版的收信軟體

禁止密碼以明碼方式傳送:

通常建議啟用避免密碼被攔截,但若是用戶使用較舊的郵件軟體有可能會無法登入

僅允許加密連線:

關閉非加密阜 pop3:110 / imap:143, 僅允許使用 pop3s:995 / imaps:993 連線

郵件儲列管理

儲列或佇列(spool) 是郵件伺服器 收發信件的暫時排隊區,採用先進先出的處理順序,這好比是排隊買門票的概念,因為售票口的營業員一次能處理的客戶有限,所以當大量的客戶想要進入口,而營業員無法一時間替所有人馬上服務,形成一種排隊的機制儲列特性除了會以先進先出的概念外,若傳輸失敗會依照對方伺服器或我方的伺服器設定的參數進行細項操作.例如:當傳送失敗,對方伺服器告知我方 拒絕(reject),此時伺服器會馬上將信件退回給寄信者,或 只是暫時的無法通訊(deferred),伺服器將會將信件重新置回儲列等待儲列重試時間後再次嘗試,直到 儲列保存時間到後若無法仍無法寄出,最後會退回給寄件者一般時候除非你的伺服器線路問題或是正在寄大量的業務開發信,通常儲列不應該有太多的信件等待,如有過多的儲列數量 請檢查儲列信件內容,可以按儲列序號 打開信件查看完整信件內容.

到達時間

一封信從寄件者到收件者中間可能進出儲列不只一次 , 通常如果是本機帳號進出時例如使用 outlook 寄信: outlook -> 儲列 -> 處理信件 -> 儲列 -> 遞送至收件方伺服器例如外部寄給內部: 對方伺服器 -> 儲列 -> 處理信件 -> 儲列 -> 本地用戶信箱此處的到達時間指的是目前正在處理儲列的開始時間

儲列名稱

顯示此 job 目前處於那個階段,以下是可能出現的描述

•

- o active:目前正在準備發送的信件。 在 儲列序號 後會多加一個 * 號)
- o bounce:每一位收件者的傳送狀態,並記載為何會被退信
- o corrupt:信件損毀導致無法傳送的信件
- 。 defer: 暫時無法被傳送的信件,並記載為何會被延遲傳送。這種情形最常發生在對方的 灰名單機制暫時阻擋您並等候認證
- o deferred:無法被傳送的信件會放置在此目錄,但 Mail Server 還是會嘗試幫你繼續送, 只是必須等更多時間
- 。 hold:被暫時停止發送的信件,如要發送出去,需要由手動(在 儲列序號 後會多加一個!號)
- o incoming: 從外部或本地寄送到本機的信件

儲列序號

儲列序號 是每個 job 進入儲列時會賦予一個當時唯一的序號 ,可以提供到 SMTP log 系統日誌查詢 的關鍵字

大小

目前這個 job 的郵件大小

寄信者

目前這個 job 的郵件的寄件者

收信者

目前這個 job 的郵件的收件者

儲列狀態

若信件未順利遞交,此處可能會出現一些可參考的描述

郵件轉發路由

在某些狀況下可能目的(對方)伺服器拒絕接收我方伺服器 IP 將郵件遞送過去, 此時可以使用這個郵件轉發路由功能, 將信件透過第三方的伺服器將信件遞送給目的(對方)

伺服器 透過此功能的設定之後,因爲目的伺服器看到的 IP 是第三方(轉發路由)的伺服器 IP, 若目的伺服器允許第三方伺服器遞送信件,此時您的信件即可成功遞送.

提示: 此第三方伺服器通常會是你的 ISP 提供的 SMTP 服務,

例如: hinet 的 msa.hinet.net IP:168.95.4.211,轉發可依照目的伺服器不同設定不同的

啓用	開啓
❷ 目標收件者伺服器	請輸入收件者地址@後面的文字,例如: gmail.com
② 代轉伺服器	Hinet用戶可以輸入msa.hinet.net : 168.95.4.211
❷ 需要認證	□ 如果代轉伺服器要求需要帳號密碼認證請勾選
❷廣域代轉	□ 只有當收件伺服器爲私有時才可勾選,如不瞭解用途請勿勾選此選項

轉發路由器

啟用此服務之後就可以新增刪除或者是編輯路由表規則 每一個路由表規則可以設定以下的參數

啟用

設定這個路由表規則是否啟用

目標收件者伺服器

請輸入收件者地址@後面的文字,例如: gmail.com, 一次只能設定一個目標

代轉伺服器

欲幫你代轉的伺服器,通常是你的上游伺服器,或是你的 ISP

例如 hinet 用戶可以設定爲 msa.hinet.net 或 IP: 168.95.4.211

需要認證

若代轉伺服器需要帳號密碼認證 ,請勾選 並設定認證帳號及密碼 通常 ISP 大多不需要設定認證但是限定必須在所屬的線路使用

廣域代轉

只有當目的伺服器是自己的伺服器才建議開啟此功能 , 如不瞭解用途請勿勾選此選項 此功能開啟後 從廣域進入的信件會依照此規則代替轉送這至目的伺服器

ISF	P業者 SMTP 外寄郵件伺服器設定資料僅供參考實際由您的 ISP 資料爲主
•	
0	msa.hinet.net
0	ms1.hinet.net~ms78inet.net(其中不包含 ms10、20、30、40、44、50、60、70)
•	seed.net.tw
0	eagle.seed.net.tw
•	
0	so-net.net.tw
TF.	N:
•	
0	smtp.anet.net.tw
AP	POL
•	
0	smtp.apol.net.tw
TT	N:
•	
_	smtp.ttn.net
	•

速博 Sparq:

•

- o smtp.sparqnet.net
- o sparquet.net

和信 GIGA:

•

o asmtp.giga.net.tw

東森 Cable Modem:

•

o ethome.net.tw

東森寬帶:

•

o mail.apol.com.tw

PChome:

•

o smtp.pchome.com.tw

伺服器對應轉寄

伺服器對應轉寄服務 ,是一項特別的郵件服務 , 這項服務允許你將本地端指定或全部的使用者或部分(可使用*萬用字元)使用者 , 當收到信件時自動由伺服器轉寄到另一部指定的伺服器上同名的帳號 , 這個功能常被運用在總公司與分公司據點分別架設郵件伺服器時的需求 , 基本設定 啟動服務後即可開始設定轉寄規則

啓用	開啓
轉寄名稱	例如: 轉寄到總公司
❷ 帳號方式	所有帳號
❷ 目標伺服器	信件轉發目的伺服器多筆資料可用 逗點 分號 跳行分隔,例如 master.com,m
② 主旨標示	添加在主旨前方,例如:由伺服器轉寄,也可以保留空白
② 本地端保留	☑本地端保留
確	定

啟用

設定這個轉寄規則是否啟用

轉寄名稱

設定這個規則的名稱 , 例如轉寄到總公司

帳號方式

設定全部或正向表列或反向表列方式來決定影響的帳號

目標伺服器

設定當符合上述帳號的收件時,信件將對應轉寄到那個伺服器

需輸入 郵件地址 @ 後面的名稱, 通常是 MX 記錄的設定值, 大多可能是網域名稱

主旨標示

為了讓收件端清楚辨識此信是由對應轉寄過去的信,可以設定此標記,此標記將會出現在信件主旨最前方

注意: 若有設定此標記,會強制將主旨的編碼格式改為 UTF-8, 以防止亂碼產生, 但對於有些廣告信可能由於信件使用程式碼產生, 並未符合標準的信件標示格式 也有可能會造成全部或部分的亂碼

本地端保留

設定此信是否也要在本地端相同的帳號下保留一份相同的信件

代收外部信箱

啓用	開啓
外部信箱名稱	例如: 業務的Gmail信箱
連接方式	POP3
收件伺服器	例如: imap.gmail.com
登入帳號	例如: tom@gmail.com
登入密碼	
本地帳號	例如: admin,多人可用逗點隔開
收信間隔	- 5 分鐘 +
保留信件	開 啓 代收後不刪除遠端信件
	連線測試

設定可以指定本地端的帳號定時間隔時間透過 pop3 或 imap 方式去收取其他伺服器的信件,並將收到的信件整合入指定的帳號內

目前對方一般伺服器可以正常,但對於一些大型伺服器例如 gmail,需要兩段式帳號驗證的來源,建 議取消該帳號的兩段式驗證或依照他方的指示進行正確的兩段式驗證後才能正確代理收信,在基本 設定 啟動服務後即可開始設定代收規則

啟用

設定這個代收規則是否啟用

連接方式

連接方式可以設定 IMAP 或 POP3,後綴有 s 的設定為加密通道 不論使用哪個連結方式,都只會檢查收件夾(INBOX)是否有新的信件,並收取

收件伺服器

可以設定收件伺服器的 IP 或 DNS 的名稱

登入帳號

設定要登入的帳號

登入密碼

設定登入的密碼

本地帳號

設定收取的信件要與本地哪一個帳號整合

收信間隔

設定間隔多久去收取一次

保留信件

設定代收後信件要不要保留在原來的收件伺服器

郵件發送回收機制



郵件發送回收機制是是一種爲了防止失誤寄出信件,讓寄件者在短時間內可以阻止信件發送到收件者,

其工作原理如下: 系統管理員需先啟動此機制的功能,並指定那些用戶(帳號)可以套用此機制 當被套用的用戶寄信時信件將會延遲一些時間才寄出

在延遲期間寄件者將會收到一封通知信(信件內容可以在本頁面自定)

在信中可以提示操作方式,其中可以 收回信件,或 直接寄出信件

如果該信件逾時沒有任何處置,信件將於逾時後順序寄出

設定細節如下

啟用服務

設定是否要啟用這個功能

套用帳號的方式

决定那些如何影響那些帳號生效的方式

所有帳號:表示本機所有帳號都套用此功能

僅列表帳號:表示只有這些被列入的帳號會被套用此功能,設定請輸入帳號,可用 逗點,分號 或

跳行分隔多個項目

排除表列帳號:表示除了這些表列帳號以外的所有本機帳號皆會被套用此功能

延遲發送時間

設定當寄件者按下發送要延遲多少時間才真正將信件發送出去 , 這段時間之內寄件者可以有緩衝時 間將信件回收

通知信推送的信箱

在延遲發送時間之內,寄件者將會收到此通知信件提醒寄件者有機會可以將信件回收,這個設定決定將通知推送到寄件者的那一個信箱,通常建議在收件匣

通知信的主旨

設定這封通知信的主旨,信件主旨可套用的變數如下

%USER%:寄信的帳號

%TIME%:延遲到期時間

通知信的內容

設定這封通知信的內容,信件內容可套用的變數如下

%USER%:寄信的帳號

%SUBJECT%:主旨

%RECIPIENT%:收件者

%S TIME%:原始寄信時間

%TIME%:到期時間

{R[????]}:回收信件按鈕:問號可以自行更改文字

{S[????]}: 立即寄出按鈕: 問號可以自行更改文字



主旨 郵件發送回收機制通知: vvv 您剛剛發送的郵件可以在 15:44:19 前決定回收或直接寄出信件,詳細請開啓本信件依照指示進行

☎ 備存

ð 垃圾重

給 vvv@localhost.localdomain 公

vvv 您好,

您最近發送的信件因爲系統啓動郵件回收機制,信件將會延遲一小段時間後才會寄出,在這段時間您會 以回收該信或強迫立即寄出,如果您不做特別處理,該信件將會於到期後自動寄出.

信件主旨: 台灣半數人口仍無足夠保護力

收件者: foo@foo.dom 寄信時間: 15:43:19

如果需要立即回收此信件請按下....[回收信件] 如果需要立即將信件寄出請按下....[立即寄出] 如果未特別處理,此信將於 15:44 19 自動寄出

寄出信件後會立即收到通知

灰名單機制

基本設定記錄		
啓用服務	關閉	
服務狀態	未啓動	
♂ 陌生來源首次延遲	- 300 秒 +	
② 逾時重新驗證	- 7 天 +	
❷ 資料庫保留天數	- 30 天 +	
❷ 信任大型主機群	☐ Gmail/google ☐ Yahoo mail ☐ Apple icloud ☐ Microsoft Outlook/hotmail ☐ facebook	
	☐ Hinet ms* ☐ PCHome/Ruten ☐ qq.com ☐ 163.com	
❷ 寄信者來源白名單		
	可填寫網來源主機名稱(必須有反解 DNS/PTR),IP,或整段網路, 例如:myhost.com , 1.2.3.4 , 1.2.3.0/24 , 也可以用正規表示法表示一辈主機 ,例如:/^mail*\.google\.com\$/	i i
❷ 收信者白名單		
	設定那些收件者不受灰名單影響,信件可以直接進入,例如:postmaster@ 或 abuse@	6
	確定	

灰名單的作法主要是針對以發送垃圾郵件的程式做有效的防堵.

一般垃圾信的發送是直接採用程式對郵件主機發送,他們會以程式動態修改內容來達成差異性的大量傳送,

灰名單的作法是讓主機分判是否為程式單發送,還是真正有郵件主機的來源,

若為主機來源則保留進入的授權

當每一封郵件進入 的時候 系統會檢查三個重要的資訊

寄件者來源 IP (大多數是對方的伺服器)

寄件者 email 地址

收件者 email 地址

這三個資訊會組成一個認證 ,如果這樣的認證存在 ,且未超過逾時重新驗證的天數 ,則這封信會 放行進入伺服器進行繼續的傳遞

如果沒有驗證通過,系統會將此信退回給對方伺服器,請對方伺服器在一定的時間後再次遞送過來 如果對方伺服器依照約定在時間後再次遞送過來,系統就會接受該信件,

並將此信件的條件產生一個驗證,爾後同樣的驗證條件再寄信過來在一定的時間內就不需受到延遲的限制

由於大多數的發垃圾信的業者通常是使用 "程式" 直接發送信件, 並不是使用 smtp 伺服器來發信

這種軟體通常是沒有儲列的設定 , 也就是採用 "發送後不理" 不管對方伺服器回應 , 所以通常都會被此機制攔截

你可能會問那垃圾郵件發送業者為什麼不要自己架設 mail server 寄信呢 ,答案很簡單就是成本太高,另外很容易被檢舉被檢舉之後這個 IP 就會被列入黑名單後面的信件就無法再繼續寄信,所以這些業者通常都會採用動態 IP 寄發信件

灰名單的過濾機制雖然很有效,但有個很大的問題是 通常大型的郵件供應商 例如: gmail,有個特性是每次信件發送總是用不同的 IP,這造成在驗證上的困難,因爲完全違反灰名單的檢查機制,所以我們有個特別的功能針對大型主機開出特例的信任(信任大型主機群),我們假設這些主機商會很有效率的管理他們的伺服器,不會讓發垃圾郵件的商人利用來發垃圾信,你只要勾選這些特別的選項即可避免上述的問題

你可能會問,如果對方僞造 寄件者爲 gmail.com 或是 qq.com,因爲系統是檢查 IP,網域名稱是會檢查反解(PTR),所以亂設定是不通的 對於僞裝網域的信件可以啓用 SMTP 服務/防護設定/內的來信 SPF 檢查,即可對這些信件直接拒絕

域名識別機制 DKIM



域名密鑰識別郵件(DomainKeys Identified Mail, DKIM)是一套電子郵件認證機制,使用公開金鑰加密的基礎提供了數位簽章與身份验证的功能,以檢測寄件者、主旨、內文、附件等部份在寄件者發出後中間到最後收件端有否被偽冒或竄改。

先不要勾選啟用服務

填寫好簽章域名後,如果是第一次或要重新產生簽章密鑰,請勾選 重新產生密鑰

如果已經在另外一部機器生成好的密鑰(通常是備接機) 也可以直接剪貼密鑰與 DNS TXT 過來

如果 DNS 由本機自行管理的話,可以到 其他伺服器/DNS 伺服器 在轄區內新增一筆 DKIM 的記錄, 系統會讀取這邊的 TXT 設定並自動產生 DKIM 的 DNS 設定

若是在其他的地方管理 DNS,需要在 DNS 管理下新增一筆 TXT 記錄

例如:網域名稱為 mydomain default._domainkey.mydomain IN TXT ("v=DKIM1;k=rsa;" "p=.. 貼上 DKIM DNS TXT ..")

注意: 由於 DKIM DNS TXT 字串相當長 , 如果 DNS 管理不能輸入太長的 TXT 值 就不適合用來管理 DKIM

新增記錄:domlinux.com(domlinux.com)		
啓用	開告	
記錄形態	DKIM	
② 主機名稱	defaultdomainkey	.domlinux.com
⊘ DKIM描述		MIGfMA0GCSqGSlb3DQEBAQUAA4GNADCBiQKBgQC8bMKNT/zCokCGX9jE9
	"v=DKIM1;k=rsa;" p=	vX8hK9dkUbyiMQIDAQAB
		CIM 域名識別機制 的 DNS TXT 複製內容 開業,可以將結識別內容貼於此欄位。
⊘ TTL	- 14400	₩ +

最後若要驗證是否生效 ,可以寄一封信到 Gmail 收件者 再觀察 信件表頭 中的 DKIM 是否爲 Pass

原始郵件



Updated on 2022 年 4 月 14 日

收發信對象管制

條件設定	執行動作	
	啓用	開啓
	❷ 執行順序	最優先
	規則名稱	輸入一個易於辨識的敘述
	② 認證帳號	
		輸入欲管制的帳號(不是完整Email),多個帳號可以用 逗點,分號,或跳行 分開
	❷ 管制策略	僅允許發送給下列人員或網域,其餘全部禁止
	② 郵件地址或網域	
		設定收件者或收件網域條件,多個可以用 逗點,分號,或跳行 分開

收發信對象管制功能,可以讓管理員設定限制本機帳號寄信或收信的對象 啟用此功能後,即可新增刪除或編輯管制的規則

條件設定

啓用

設定此規則是否啟用

執行順序

所有的規則會依照順序執行, 過濾規則若遇到有設定規則有衝突時以順序優先為主

認證帳號

設定此規則影響(限制)的帳號

管制策略

限制符合帳號的用戶以下行為:

1.

- 1. 僅允許發送給下列人員或網域,其餘全部禁止
- 2. 禁止發送給下列人員或網域,其餘全部允許
- 3. 僅允許發送給及接收下列人員或網域,其餘全部禁止
- 4. 禁止發送給及接收下列人員或網域,其餘全部允許

郵件地址或網域

設定上述的管制策略 實施限制或僅允許的網域或郵件地址,多個條件可以用 逗點(,)分號(;)或跳行 來隔開每個選項

可以輸入完整的對象(email) 例如 jerry@mydomain.com,表示 這個對象,請注意 yehjerry@mydomain.com 也符合這個條件,因爲比對是採用部分文字比對

例如

@mydomain.com 表示 這個網域的所有人

mydomain.com 可能 ms1.mydomain.com, ms2.mydomain.com 都符合

執行動作

轉寄給

當管制條件符合觸發時要將此信件另外轉寄給指定人員, 請輸入 email 或 本地帳號 , 多筆資料可以 用 逗點 分號 跳行 隔開

寄通知信

設定觸發條件成立後是否要寄發通知信

通知帳號擁有者:

當管制條件符合觸發時,是否要通知該用戶(寄發通知信)

通知指定的人員:

當管制條件符合觸發時,指定通知管理員或主管(寄發通知信)

通知主旨:

設定通知信的主旨,可用變數:

#USER 表示 該用戶帳號

例如:#USER 你所寄發的信件依照公司的安全佈署,部分收件將無法收到

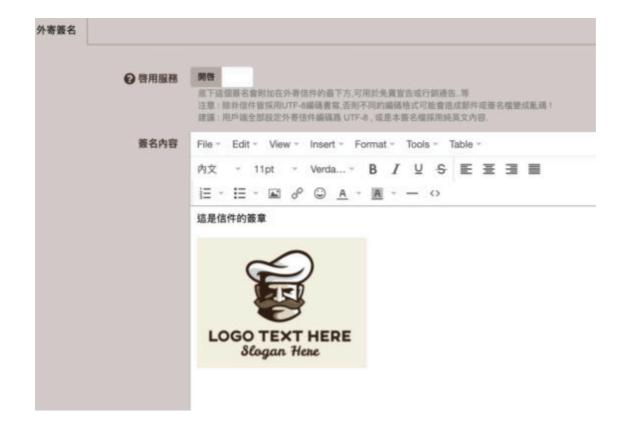
通知内容:

設定通知信的內容,可用變數:

#USER 表示 該用戶帳號,原始郵件將會附加為附件檔名: source.eml-

例如:#USER 你好,基於公司規定伺服器的安全佈署,寄發對象將有管制,以下信件與收件者將無法收到你寄發的信件,如需要檢視完整內容請開啟附件 source.eml

外寄簽章



這個簽名會附加在外寄信件的最下方,可用於免責宣告或行銷通告..等

注意:除非信件皆採用 UTF-8 編碼書寫,否則不同的編碼格式可能會造成郵件或簽名檔變成亂碼!

建議: 用戶端全部設定外寄信件編碼爲 UTF-8, 或是本簽名檔採用純英文內容.

如需要使用圖檔,可以有兩個方式:

- 1. 超連結其他網站的圖檔
- 2. 直接剪貼圖片, Ctrl+C, Ctrl+V, (Mac 電腦用 Command+V)

郵件使用報告



郵件使用排行榜可以用來快速統計一段時間內用戶的信件收發數量

當某個帳號有異常的發送數量時,有可能是帳號被盜用,請盡快通知用戶並更改密碼

記錄查詢



郵件記錄器會將這個伺服器上來往的信件全部記錄一份 , 這功能就好比是監視錄影器 , 管理員可以 很清楚知道有那些信件進出

郵件記錄列表最上方為最新的進出列表

日期

記錄的是信件進入伺服器的時間,並非信件內所表示的時間(這有可能因為時區不同),兩者不同是 正常的

主旨

點按可以開啟信件,並查看該信件的完整內容

表頭:可以看該信件的信件表頭,信件表頭會記錄這封信件的傳遞路由及簽章或認證消息

另存: 可以將該信將下載儲存為 eml 格式, 這個格式可以在大多數的用戶端郵件軟體打開或匯入

方向

若呈現綠色圖示:表示此信件是從他方的伺服器寄入本伺服器的信件,例如 從 gmail.com 或 yahoo.com......

若呈現紅色圖示:表示此信件是由本地帳號寄出,有可能是寄給外部信箱或本地用戶,皆會標示為寄出

認證

記錄的是本信在寄信時是使用哪一個帳號 smtp 認證成功寄出 , 認證需要該帳號的帳號名稱及密碼

收件者

是這封信實際的收件人(數),可能會和打開信件後看到的收件者不同,這是有可能的,而且是以列表上看到的為主

管理員可以透過搜尋來快速找到信件,也可以在欄位的上方空白輸入處指定搜尋的項目,例如主旨上或收件者....

搜尋時一次只能針對一個區段搜尋 , 預設每一個段落為 1G 的信件集合 , 這個設定可以在稍後的記錄器設定上指定

搜尋到的信件可以進行

重新發送: 將信件重新發送一次 (相同的收件者)

發送給: 信件發送給指定的收件者

這是垃圾信: 將指定的信件回報為垃圾信樣本

這不是垃圾信: 將指定的信件回報為非垃圾信樣本

刪除郵件記錄器上的信件,並不會刪除用戶信箱內的信件

郵件記錄器和監視錄影器一樣有一定的容量,當容量滿的時候,最舊的信件會被自動刪除,這個容量值可以在稍後的郵件記錄器設定上指定

記錄器設定

基本設定

基本設定	長期備份設定					
	❷ 啓用服務	開聲				
	② 記錄方向	雙向記	綠			
	空間使用	資料數:	3961 , 空間: (652.8 M		
	❷ 記錄器空間	-	2	GByte	+	
		設定記憶	非器最大使用的		2空間は	亞邊設定值時將自動無除最早的紀錄資料
	❷ 分段最大空間	每個段	1 基大使用空間	GByte 設定越大一次技	女母節	圍越大,但搜尋速度越慢
	❷ 排除寄件者符合					
		當信件	『寄件者』符合	設定值,該郵件不	會被制	2錄,多筆設定可以用 逗點,空白,分號 分開
	● 排除收件者符合	boss@	d			
		型体化:	Dib/作者,符合	均完值 註部供達	Celebrate	248 名號如中間以田 招數 四凸 公開 公開

啟用服務:

設定是否啟用郵件記錄器服務

記錄方向:

設定要記錄的方向,方向判定請參考上一節 郵件記錄查詢的說明

記錄器空間:

設定要規劃多少空間給郵件記錄使用

分段最大空間:

指定郵件記錄器累積到多少空間時切換成一個區段,這個設定值會影響郵件記錄查詢時每次可查詢的範圍

排除寄件者符合:

設定那些寄件者的信件不要被記錄器進行記錄

排除收件者符合:

設定那些收件者的信件不要被記錄器進行記錄,

若信件爲多個收件者,`只要該信件符合任何一個收件者此信即不進行記錄

例如:boss@,@mydomain.com,boss@mydomain.com

多筆設定可以用 逗點,分號,或換行分開

長期備份設定

基本設定	長期備份設定	
	② 長期備份查詢慣用 ② 備份時間	網路芳鄰備份 若有設定下面多個備份方案,請選擇其中一個爲預設查詢方案 下午 12:30
	② 網路芳鄰備份	開啓
	② SMB協定版本	smb 2.0 / Vista SP1, Windows Server 2008
	❷ 備份主機	備份目標IP
	❷ 分享名稱	
	❷ 備份目錄	例如: backup1
	❷ V3資料轉V5	□ 如果存儲點已經有原先的舊版V3資料,可以勾選此選項進行一次性資料庫轉換,勾選後按例行資料轉換. 請稍後再進入長期備份查詢進行查詢 備份目錄請設定一個空的目錄,例如 v5 或 mr,系統會將舊版資料庫轉換後放置於此目錄內,原本的V3資
	② 登入帳號	
	登入密碼	
		測試連線

如上一節的記錄器空間設定中,當記錄器空查詢間使用已滿,會自動將最舊的信件刪除,若要將郵件記錄器長期備份,需要設定將記錄器內容備份到另外的空間例如 NAS 或者是另外一顆硬碟(建議使用 USB 外接硬碟),設定好長期備份系統會自動在適當時候將信件推送到長期備份的空間裡

長期備份查詢慣用:

長期備份的儲存方式有三種,管理員可以計畫一種或多種方式進行備份方案

網路芳鄰備份:

可以使用 windows 的網路芳鄰分享或是 NAS 的 SAMBA 分享儲存空間

V3 資料轉 V5: 如果存儲點已經有原先的舊版 V3 資料,可以勾選此選項進行一次性資料庫轉換,

勾選後按確定系統將會在背景進行資料轉換.

RSYNC 備份:

可以使用 Rsync 協定的目的分享空間

外接硬碟備份:

可以使用另外一顆內接硬碟或外接 USB 硬碟,

硬碟使用前需先到 系統設定/磁碟管理 將硬碟規劃為 記錄器碟

備份時間:

當指定時間到時,郵件記錄器檢查除了目前正在使用中的段落(最新的一段落),若尚未備份者會將 記錄器單向備份到上述指定的一個或多個儲存設備內.

當郵件記錄器已經往長期備份儲存後,日後要查詢較早期的郵件時可以到 長期備份查詢 功能下進 行查詢,近期的郵件則仍需要到 記錄查詢頁面下查詢

記錄區段管理



郵件記錄器是會以郵件記錄器設定的 記錄器空間及分段最大空間 來分段儲存資料.

例如:

記錄器空間:20G

分段最大空間:2G

這樣的設定每當郵件記錄器滿 2G 時會分成一個新段落

以時間排序,最接近現在的區段置於頂,通常第一筆資料為目前正在使用中的記錄資料庫 管理員可以對分段資料進行:

刪除:

刪除分段會將該分段的資料庫索引及實體郵件刪除(不會刪除用戶的郵件)

合併區段:

若區段內因為郵件較大可能會在一個區段內記錄較少的郵件數量,此時可以將兩個或多個分段合併,注意: 合併時請勾選連續的分段進行合併

第一段(目前使用中)的區段不能用於合併

長期備份查詢

如果已經有設定好,記錄器設定/長期備份設定,並選定長期備份慣用設備,此處會列出備份來源的查詢資料

介面查詢的方式與郵件記錄器/記錄查詢的操作相同,惟此長期備份資料庫無法進行單筆資料刪除 查詢到的信件可以重新發送或發送給指定信箱或人員

裁判設定

基本設定



本系統垃圾郵件過濾器採用 spamassassin (https://spamassassin.apache.org/),此垃圾郵件過濾系統是由 apache 軟體基金會 所提供的一套免費的垃圾郵件過濾核心 ,本身是採用 貝氏分析法(Bayesian filtering) 來評判郵件是否可能是垃圾郵件 ,如對此有特別興趣的可以上官方網站進一步瞭解.

本系統只會對信件方向是 "收信" 的信件進行垃圾郵件判斷 , 另外如果信件大於 250Kbyte(可自訂) 將不會進行判斷, 通常垃圾郵件大多不會太大

spamassassin 核心會對提供的信件進行垃圾郵件評分,通常是-100~+100,分之間,分數越高表示垃圾郵件的可能性越高

定義在黑名單的來源,基本分數即爲100分

定義在白名單的來源,基本分數即爲-100分

若未任何定義的來源,基本分數爲 0分 經驗上,大約超過5分的信件 已經很可能是垃圾信,這個分數的分界線管理員可以在下方的 垃圾信分數 項目設定,設定分數越高表示越寬鬆,設定分數越低表示越嚴格 spamassassin 會透過自動學習,來增加垃圾郵件的判別能力 一旦信件被判斷爲垃圾郵件,系統會將該信件隔離於系統隔離區,就不會傳遞給收件者,收件者將會在一段時間後收到一封垃圾郵件報告書,信件內有這一段時間內所收到的垃圾郵件列表,如果有信件誤判成垃圾信 可以依照報告書內的指引立即取回該信件,隔離區內的信件若未被取回 將在一定的時間(通常是7天,可由管理員自定),自動刪除該信件

啟用服務

設定是否啟用垃圾郵件處理器

服務狀態

顯示系統功能是否服務中

主旨附加標記

當信件被判斷為垃圾信時,會在信件的主旨最前面增加此段文字,通常建議盡量英文文字避免造成混碼產生無法辨識的亂碼

垃圾信分數

本系統只會對信件方向是 "收信" 的信件進行垃圾郵件判斷, spamassassin 核心會對提供的信件進行垃圾郵件評分,通常是 -100~+100,分之間,分數越高表示垃圾郵件的可能性越高

隔離區保留天數

垃圾郵件保留於隔離區的天數,超過這個天數的垃圾信將被刪除,

預設爲7天,管理員可以視伺服器的負載及容量增減

略過評分

通常垃圾郵件為了要大量發送,信件本身都不會太大,所以對於一定大以上的信件,可以忽略判斷,如此可以減少伺服器的負載

設定信件若超過指定的大小時,則略過垃圾信評分,意即該信件不會被當成垃圾郵件

参考線上黑名單 RBL

設定 spamassassin 在評定信件垃圾信分數時是否要參考線上的黑名單組織 ,通常建議開啟此功能若你的系統相對繁忙則建議關閉 ,或是你的客戶已經被列入黑名單 ,而你必須要收到他的信件時也可以考慮關閉

黑名單

設定爲黑名單的對象將會在垃圾郵件評分上直接 +100 分 , 如此該信件被判斷爲垃圾郵件的可能性 幾乎是絕對的

設定可以用直接指定或萬用字元指定

例如:badboy@yourdomain.com,或*@yourdomain.com

白名單

設定爲白名單的對象將會在垃圾郵件評分上直接 -100 分 , 如此該信件被判斷爲垃圾郵件的可能性 幾乎是不可能

設定可以用直接指定或萬用字元指定

例如:badboy@yourdomain.com,或*@yourdomain.com

評分設定

基本設定	評分設定	通知設定	
	0	評分定義	
_			
	❷ 寄信與回信	地址不同	- 10.0 評分 +
			信件若有此狀況很有可能是詐騙信件,SPAMTag: FROM_NOT_REPLYTO
•	寄信者名稱例	使用Email	- 10.0 評分 +
			信件若有此狀況很有可能是詐騙信件,SPAMTag: FROM_2_EMAILS_SHORT
	O		
	② 主旨關鍵	子黑名里	
			每一筆設定需以換行分隔,可以用 * 代表任何字 例如: [Report NO:*]
		評分數	- 5.0 評分 +
	② 主旨關鍵	字白名單	
	<u> </u>		
			每一筆設定需以換行分隔,可以用 * 代表任何字 例如: [Report NO:*]
		評分數	- 5.0 評分 +
-			
	② ■	碼黑名單	
			設定來自於某些國家的信件增加其垃圾郵件的分數,分數如下自訂,國碼為2位數大寫 或分行空白或跳行隔開,國碼請參考ISO文件:3166,也可以從來信中的表頭 X-Spam-l
		評分數	- 1.0 評分 +

評分定義

通常我們不太需要重新定義 spamassiassin 的評分 ,如果您對預設的評分設定不滿意 ,則可以根據 收到信件的表頭評分自行定義分數.

例如: 您可以對 SPF PASS 這個分數 重新定義

語法如下: score SPF_PASS -1.0,表示來信來源的 IP 如果有通過 SPF 認證,就減少垃圾郵件的可疑度 1分

您可以參考此線上文件:https://spamassassin.apache.org/old/tests_3_3_x.html 或 根據來信開啟表頭觀察

寄信與回信地址不同

在電子郵件的標頭內 From: 表示寄件者,通常收件者回信時會自動回給這個信箱地址,而在標頭內有一個 Reply-To: 表示回信地址,當信件標頭內有此標籤時 回信時會預設回覆到此地址 一般狀況下大都不會特別指定 Reply-To:,或指定到與 From: 相同的地址 然而某些詐騙者會刻意將信件的 Reply-To: 指定到其他的信箱地址,收件著看到 From 是熟悉的寄件者,不疑回信,但確是將信件回覆到 Reply-To: 的地址,詐騙者即可成功獲取信件內容 此一功能設定,可以讓系統檢查信件是否有此問題,若檢查有此問題時可以設定讓此信的 spam 分數,增加指定的分數 當總分數超過 spam 門 檻時 信件即被判斷為垃圾郵件並隔離,若要取回此信可以從垃圾郵件通知信上取回

寄信者名稱使用 Email

在電子郵件的標頭內 From: 表示寄件者 , 通常收件者回信時會自動回給這個信箱地址 . 例如: From: tom@mydomain.com , 或是 From: "tomcat"<tom@mydomain.com>

其中第二種寫法 tomcat 表示 name, tom@mydomain.com 為 Email 地址, 通常我們在郵件軟體上因為畫面上的精簡可能只會看到 tommy 這個名稱,而不會直接顯示 Email

然而詐騙者可能會 寫成 "tom@mydomain.com"<haker@other.com>

收件者可能會在閱讀信件時看到的寄件者是 tom@mydomain.com,但真正回信時可能會回覆到 haker@other.com 詐騙者即可成功獲取信件內容

此一功能設定,可以讓系統檢查信件是否有此問題,若檢查有此問題時可以設定讓 此信的 spam 分數,增加指定的分數 當總分數超過 spam 門檻時 信件即被判斷為垃圾郵件並隔離,若要取回此信可以從垃圾郵件通知信上取回

主旨關鍵字黑名單

若信件主旨出現指定的關鍵字,系統會根據下面的指定評分數,增加指定的分數

當總分數超過 spam 門檻時 信件即被判斷為垃圾郵件並隔離,若要取回此信可以從垃圾郵件通知信上取回

* 可以代表任意字,例如:請問*報價

每一個設定必須單寫在一行

主旨關鍵字白名單

參考上方 "主旨關鍵字黑名單" 之設定

國碼黑名單

伺服器會依據信件路由的 IP 反查 IP 來自於那個國家, 設定來自於某些國家的信件減少其垃圾郵件的分數,分數如下自訂,

國碼為 2 位數大寫字元, 例如 US,CN,TW, 設定時可以用 逗點或分行空白或跳行隔開,

國碼請參考 ISO 文件:3166,

也可以從來信中的表頭 X-Spam-Relay-Country 查看該信件的來源國家

國碼白名單

設定說明請參考 "國碼黑名單"

通知設定

基本設定 評分設定 通知設	定
垃圾信報告通知	垃圾信隔離區將每隔一段時間主動寄發報告書通知原收件者
❷ 報告書發送頻率	- 24.0 小時 +
₹ 星期六日不發送報告	☑ 休假日停止發送,並累積至假日結束一併發送
❷ 通知信主旨	#USER 您的垃圾廣告郵件隔離報告書
→ 通知信內容	#USER, 以下列出的郵件已經被伺服器系統判斷爲垃圾廣告郵件,目前隔離在系統隔離件,該信件將會發送到你的信箱收件匣內.信件將被保存 #EXPIRE 天, 如有需取回信件請於期限內取回.

當伺服器判斷信件為垃圾信時 , 會將該信件隔離於隔離區內 , 系統會在一段時間 , 以垃圾郵件報告書分別通知各收件者

若逾時未取回 , 通常在 7 天後即會被清除 , 此保留時間可以在基本設定內設定 有那些信件被隔離中 , 可以在隔離區內查看

報告書發送頻率

設定垃圾郵件多久發送一次,如果沒有垃圾郵件在隔離區,則不會發送給該用戶

星期六日不發送報告

休假日停止發送,並累積至假日結束一併發送

通知信主旨

設定垃圾郵件報告書的主旨

變數: #USER 表示 目前要寄給的用戶帳號

通知信內容

設定垃圾郵件報告書的信件內容樣板

內容可以使用 html 格式

變數:#USER,目前要發送報告書的對象帳號,#EXPIRE:垃圾信幾天後會被自動刪除

隔離區

隔離區	1												
☆ 刪除	1 重新	發送	† 5	發送給	1	專送給名單內的人員,多人可用逗點分隔		搜尋					S
顯示第 1	到第 10 項記	錄,總	共 79	98 項記錄	录名	專頁顯示 10 ▼ 項記錄			1 2 3 4	1	5	5111	80 >
	日期	通知	+	評分	+	主旨(寄信者 💠	收信者 💠		附件	ŧ	大小 🛊
			×			請輸入關鍵字搜尋,複合搜尋可用逗點表示	I			I			例:>10k
	2022-04-14 15:00:14			17.3		钴菜 上海口岸出口澳洲航线拼箱价格		max-charlotte@m 183.194.172.183	jerry@jerry.com.tw				6.2 k
	2022-04-14 11:07:15			14.9		撒瓦底卡人泰泰們,一起慶祝潑水節吧		privaterelay.bounc 17.58.38.71	jerry@domlinux.com				47.2 k
	2022-04-14 10:09:47			104.4		[新聞快訊]防疫隔離假雇主可不給薪,確診 可改請病假領半薪		root@oms12.104 122.147.53.132	jerry@domlinux.com				41.4 k
	2022-04-14 05:59:07			7.1		Stop interrupting others sleep use this instead		info@assetspring.co 193.30.241.37	sales@domlinux.c				5.4 k
	2022-04-14 05:57:57			7.1		Power Pod gives you HOURS more power, and it fits on any keychain!		info@assetspring.co 193.30.241.37	sales@mailvsr.com				6.1 k
	2022-04-14 05:29:19			7.1		This is how you can get girls to squirt		info@amusecuttin 193.30.241.36	sales@mailvsr.com				11.7 k
	2022-04-14 05:29:04			7.6		AMAZING LITTLE WRIST BAND STOPPED MY HUSBAND'S SNORING WHILE WEARING IT!!		info@amusecuttin 193.30.241.36	sales@domlinux.c				8.5 k
	2022-04-14 04:59:07			7.1		GPS Vehicle Trackers That Might Blow Your Mind		genetics@firsthair 193.30.241.35	sales@mailvsr.com				9.3 k

當信件被判斷為垃圾郵件後,會被隔離於此隔離區,信件不會遞送給原先的收件者,使用者可以透過收到的垃圾郵件報告書若有誤判或需要的信件可以進行取回也可以由管理員在此頁 進行操作

查詢

可以在搜尋欄位進行概略查詢,或是在每個欄位雙方針對該欄位內容指定搜尋單一欄位輸入可以用 逗點分開,其邏輯組合為 OR,例如 在主旨欄輸入:報價,請款,表示主旨只要出現由上述兩個關 鍵字其中一個即符合條件多個欄位搜尋,其搜尋邏輯組合為 AND,必須所有欄位皆符合條件才會被列出

勾選

可以在每個列最左邊的格狀勾選,被勾選的列(信件),可以進行以下的操作

刪除

勾選項目後按下刪除,即可立即刪除

通常不建議進行刪除,隔離區的信件會自動在逾時後自動刪除

重新發送

勾選項目後 按下重新發送按鈕,可以將信件立即依照原先的收件者寄發

發送給

勾選項目後,並填寫 右邊的 傳送給名單內的人員,再下發送給按鈕,可以將信件發送給指定的 人

名單若為內部人員 可以只填寫帳號 , 若是外部信箱 則必須填寫完整 Email , 多筆人員可以以 逗點隔開

舉報與學習



垃圾郵件處理器可以透過有效信件的學習,會越來越聰明的判斷垃圾郵件的準確性,通常有效信件的學習可以透過

1.系統的自動學習

2. 由用戶回報給系統

- 透過學習可以增加垃圾郵件的判斷率,減少誤判率!
- 若要舉報垃圾郵件,可以將信件轉寄給 spam 這個虛擬用戶.
- 若要舉報非垃圾郵件,可以將信件轉寄給 notspam 這個虛擬用戶.
- 多封信件可以在寄信軟體下一次多選以附件方式轉寄.
- 用戶可以在個人的 WebMail 介面下,選取信件回報 這是垃圾信或這不是垃圾信.
- 管理員可在郵件記錄器或垃圾郵件隔離區,選取信件回報 這是垃圾信或這不是垃圾信.
- 舉報之郵件會每隔一小時統一由系統排定行程分析信件及學習樣本.
- 垃圾郵件、非垃圾郵件樣本數必須達到各200筆以上才會啟用學習資料庫.

匯入學習樣本

可以將之前匯出的學習樣本進行匯入,或是從 A 機器匯出,再匯入到 B 機器內

匯出學習樣本

可將目前的學習樣本匯出檔案保存

立即學習

如果用戶端有透過回報樣本 (寄給 spam 或 notspam), 系統會在每個小時自動將這些數據分析整理 成有效的樣版本

如果要立即執行學習分析,可以按下此按鈕(通常不必可以刻意按此按鈕)

過濾器設定

基本設定

郵件過濾器可以讓系統管理員制定過濾規則,進行信件的審核,延遲,刪除,轉寄及自動回覆,定製規則可到條件設定進行設置

啓用服務

過濾器功能的總開關,開啟此開關後,才會執行之後的條件設定

保留天數的設定

當信件被過濾器判斷符合條件,並執行其動作,動作分為:刪除,待審,延遲,轉寄,自動回信,放行等策略,當執行策略後會將信件複製於每個紀錄區,紀錄區保留完整的信件,該信將可以被下載,重寄,轉寄...

此可以設定每個紀錄區的信件要保留多久,超過時間後信件即會被刪除

條件設定

過濾條件列表

列出已經自行定義好的所有過濾條件規則一覽表

順序

過濾條件是由上而下的執行順序

啟用

顯示該條件是否啟用

規則名稱

設定的規則名稱

有效時機

條件的有效時間及信件方向

條件策略

條件的比對條件

執行動作

當符合條件的時候要執行的動作

條件匯出

勾選要匯出的條件後按匯出按鈕,可以將指定的條件匯出至檔案儲存 若不勾選任何條件,則會把所有的條件全部一次匯出並存儲為檔案

條件匯入

允許匯入上述所匯出的過濾條件檔案,A機器的匯出檔案可以匯入 B機器,但要注意條件內容上是否可以符合邏輯

新增與編修

基本設定

啟用

設定此則條件是否啟用

執行順序

設定 管制規則的執行優先順序,所有的規則會依照順序執行一次 過濾規則若遇到有設定 主要動作,又該信件符合條件,則不再往下一條過濾條件比對 反之 則順序往下比對到最後一條規則

規則名稱

信件方向

設定 此規則條例僅對這個方向的信件有效

寄信方向:

內部用戶認證寄出的信,不管信件是寄給內部人員還是外部人員,另外設定在郵件伺服器的 SMTP 服務設定內的 允許 relay 來源 的 IP,所寄的信件不管是否有帳號認證 皆爲寄信方向

收信方向:

非符合寄信都視爲收信

有效時間

設定過濾器在那些時間生效,預設是任何時間

自訂時間

日期區間:

設定過濾條件生效的日期,若日期未設定 則表示每一天

時間:

設定過濾條件生效的時間, 從幾點幾分 到 幾點幾分

若 後者時間 小於 前者 , 表示時間誇過夜晚 , 例如 $20:00 \sim 06:00$, 表示 從前一晚的 08:00 到隔天的 06:00

若未設定,表示整日有效

星期:

設定過濾條件生效星期,若全部不選或全部都選表示不考慮星期幾,反之如果有勾選任何一星期, 表示只有符合該日才生效

條件設定

條件組合

設定過濾條件要比對的項目,比對的組合邏輯

OR: 只要其中有一個條件符合即可

AND: 所有的條件都必須符合

主旨

若主旨符合條件

條件設定可用 逗點(,) 加號(+) 和 括號來組合

例如: 報價,詢價,表示主旨只要有提到報價或詢價關鍵字即符合條件

例如: 報價+回覆 ,表示 主旨內必須要同時出現 報價 和 回覆 兩個關鍵字 ,關鍵字不需依照順序

或連接

例如: (報價,詢價)+回覆,表示主旨要有回覆關鍵字,且必須要有報價或詢價關鍵字

信件內文

参考上方主旨條件設定方法

寄件者

寄信者條件 可參考主旨設定方式,可以使用完整比對

完整比對可以用 "{ }" 來表示條件

例如: {kevin@mydomain.com}:

表示只有 kevin@mydomain.com 可以吻合, 如:mykevin@mydomain.com 則不能吻合

收件者

請參考 寄信者條件設定方式

表頭

比對出現在表頭的內容,你可以透過郵件記錄器 打開信件後可觀察表頭的內容,通常由表頭可以 觀察到信件是由什麼軟體製造的

信件編碼格式 ...

來信 IP

檢查信件是來自於哪個 IP 或那一段 , 例如:

123.123.123.1

123.123.123.

123.123

附件

如果信件有附件請可以檢查附件檔名是否符合

例如 *.doc, *.do? 或是 report_*.doc

信件大小

檢查信件大小,可以用 < 或 > 及 b,k,m

例如:<2k:小於2k,>2m:大於2MB

執行動作

主要動作

無

無特別動作,可搭配下方的轉寄及自動回信設定,郵件會繼續往下一個條件比對,若有附加設定轉寄或自動回信會執行功能

直接刪除

信件將被直接刪除(置於刪除信件記錄區),郵件不會繼續往下一個條件比對,若有附加設定轉寄或自動回信會執行功能

評為垃圾郵件並隔離

與直接刪除略有不同,此信件會被標為垃圾郵件,並進入垃圾郵件隔離區,用戶可以在之後收到 垃圾郵件隔離清單時可以決定是否取回該信件

阻擋待審核

信件將暫時停放在待審信件記錄區,並依照待審的設定進行待審要求,郵件不會繼續往下一個條件 比對,若有附加設定轉寄或自動回信會執行功能

審核人員:

設定符合條件由什麼人來進行審核 , 請輸入審核者本機的帳號 , 若審核者有多人 可用 逗點 分號 隔開

例如: jerry,tom

審核通知信的主旨:

當信件符合條件時,系統會寄發一封通知信給上述的審核人員,此處設定寄給審核人員的通知審核信的主旨

審核通知信內容:

設定寄給審核人員的通知審核信的內容,此內容可以設定說明並引導審核者決定是否放行此信特殊設定:

{Y[XXXX]} 產生一個 放行的按鈕,例如:{Y[准于放行]}

{N[XXXX]} 產生一個 拒絕的按鈕 , 例如 : {Y[不放行]}

逾時:

若審核者需在時間內進行審核

逾時未審核處理原則

若逾時該信件沒有人進行審核,信件的處理方式

放行:該信件自動放行

刪除:該信件自動刪除

延遲發送

信件將暫時被停放在 延遲發送記錄區,並依照延遲發送的設定,在指定時間自動寄出,郵件不會繼續往下一個條件比對,若有附加設定轉寄或自動回信會執行功能

延遲形態:

設定延遲發送信件的方式

指定時間:

設定該信件延遲到指定的時間進行發送 , 注意 : 指定時間是指這個時間之後 , 伺服器忙碌時可能 會延後

延遲一段時間:

設定信件延遲一段時間後再寄送

放行並跳過垃圾郵件檢查

信件不執行任何動作 , 也不會被垃圾郵件評分 , 收件者保證能收到此信件, 郵件不會繼續往下一個條件比對 , 若有附加設定轉寄或自動回信會執行功能

主旨提示標簽

設定若信件符合條件後在信件的主旨前增加提示文字,例如:這封信可能是詐騙信件!!

轉寄給

設定信件若符合條件 ,可以把此信密送給指定的收件人 ,如果是內部人員可以只輸入帳號 ,如果是寄給外部信箱需輸入完整的 Email地址

轉寄信主旨標籤:

設定轉寄信件時 要添加在原來主旨前的 辨識標籤

若保留空白 則不改變原來的主旨

請注意: 若使用中文的辨識標籤,可能會造成 與原來信件編碼不相同時 有可能會造成主旨變成亂碼,建議儘量使用英文,例如: FW

垃圾信不轉寄:
勾選此選項 ,信件如果判斷為垃圾郵件不進行轉寄 ,反之則全部都會轉寄
自動回信
將符合過濾條件的信件自動回信給寄件者,通常可以用於公司的客戶服務帳號
或是帳號人員已經離職,可以自動回信通知對方
或休假人員 (個人休假自動回信建議到自己的 webmail 下設定)
回信寄件者:
設定自動回信時要套用什麼 email 來當寄件者,通常不設定即自動用第一個收件者 當作回信者,也可以指定例如 admin來回信
回信主旨:
設定自動回信時的主旨
回信內容:
設定自動回信的信件內容 ,告知原寄件者相關的事項
包含原信內容:
勾選此項目會在回信的信件內文中,含入原信的信件內容(文字),方便對方理解是哪一封信件

刪除信件記錄區

所有符合過濾條件執行刪除的信件,會暫時置於此隔離區,信件會在此保留一段時間後自動刪除 (保留時間可參考基本設定內的 刪除信件保留天數之設定值)

日期

記錄的是信件進入伺服器的時間,並非信件內所表示的時間(這有可能因為時區不同),兩者不同是 正常的

規則

顯示此郵件是觸發哪一個過濾器而隔離於此

方向

若呈現綠色圖示:表示此信件是從他方的伺服器寄入本伺服器的信件,例如 從 gmail.com 或 yahoo.com......

若呈現紅色圖示:表示此信件是由本地帳號寄出,有可能是寄給外部信箱或本地用戶,皆會標示為寄出

主旨

點按可以開啟信件,並查看該信件的完整內容

表頭:可以看該信件的信件表頭,信件表頭會記錄這封信件的傳遞路由及簽章或認證消息

另存: 可以將該信將下載儲存為 eml 格式,這個格式可以在大多數的用戶端郵件軟體打開或匯入

寄信者

顯示此信的寄信者

收信者

是這封信實際的收件人(數),可能會和打開信件後看到的收件者不同,這是有可能的,而且是以列表上看到的為主

附件

顯示此信有無附加

大小

顯示此信的大小

刪除

勾選項目(可多選)後,按下刪除即可刪除會刪除隔離區的記錄及隔離的實體信件,但不會刪除已經傳送到用戶端的信件

通常不建議手動刪除信件,信件會在隔離到期後自動刪除

重新發送

勾選項目(可多選)後,按下重新發送,即可將信件重新發送給原先的收件者,該信件若有執行過 重新發送,會被記錄在主旨欄位下以較為細小的文字記錄

發送給

勾選項目(可多選)後,填寫傳送名單後按下發送給按鈕,即可將信件發送給指定的收件者,該信件若有執行過指定發送,會被記錄在主旨欄位下以較為細小的文字記錄

管理員可以透過搜尋來快速找到信件,也可以在欄位的上方空白輸入處指定搜尋的項目,例如主旨上或收件者....

待審信件記錄區

所有符合過濾條件執行待審的信件,會暫時置於此隔離區,信件會在此保留一段時間後自動刪除 (保留時間可參考基本設定內的 待審信件保留天數之設定值)

日期

記錄的是信件進入伺服器的時間,並非信件內所表示的時間(這有可能因為時區不同),兩者不同是正常的

規則

顯示此郵件是觸發哪一個過濾器而隔離於此

審核者

此信須有此審核者決定是否放行

審核時間

若已經執行放行,此欄位記錄審核者決定放行的時間

放行

若已經執行放行,此欄位會打勾

方向

若呈現綠色圖示:表示此信件是從他方的伺服器寄入本伺服器的信件,例如 從 gmail.com 或

yahoo.com.....

若呈現紅色圖示:表示此信件是由本地帳號寄出,有可能是寄給外部信箱或本地用戶,皆會標示為寄

出

主旨

點按可以開啟信件,並查看該信件的完整內容

表頭:可以看該信件的信件表頭,信件表頭會記錄這封信件的傳遞路由及簽章或認證消息

另存:可以將該信將下載儲存為 eml 格式,這個格式可以在大多數的用戶端郵件軟體打開或匯入

寄信者

顯示此信的寄信者

收信者

是這封信實際的收件人(數),可能會和打開信件後看到的收件者不同,這是有可能的,而且是以列表上看到的為主

附件

顯示此信有無附加

大小

顯示此信的大小

刪除

勾選項目(可多選)後,按下刪除即可刪除會刪除隔離區的記錄及隔離的實體信件,但不會刪除已經傳送到用戶端的信件

通常不建議手動刪除信件,信件會在隔離到期後自動刪除

放行

勾選項目(可多選)後,按下放行,即可將信件重新發送給原先的收件者,該信件若有執行過放行, 會被記錄在主旨欄位下以較為細小的文字記錄

發送給

勾選項目(可多選)後,填寫傳送名單後按下發送給按鈕,即可將信件發送給指定的收件者,該信件若有執行過指定發送,會被記錄在主旨欄位下以較為細小的文字記錄

管理員可以透過搜尋來快速找到信件,也可以在欄位的上方空白輸入處指定搜尋的項目,例如主旨上或收件者....

延遲信件記錄區

所有符合過濾條件執行延遲的信件,會暫時置於此隔離區,信件會在此保留一段時間後自動刪除 (保留時間可參考基本設定內的 延遲信件保留天數之設定值)

日期

記錄的是信件進入伺服器的時間,並非信件內所表示的時間(這有可能因為時區不同),兩者不同是 正常的

規則

顯示此郵件是觸發哪一個過濾器而隔離於此

放行

顯示此信件是否已經放行

放行時間

顯示此信件的放行時間

方向

若呈現綠色圖示:表示此信件是從他方的伺服器寄入本伺服器的信件,例如 從 gmail.com 或 yahoo.com......

若呈現紅色圖示:表示此信件是由本地帳號寄出,有可能是寄給外部信箱或本地用戶,皆會標示為寄出

主旨

點按可以開啟信件,並查看該信件的完整內容

表頭:可以看該信件的信件表頭,信件表頭會記錄這封信件的傳遞路由及簽章或認證消息

另存:可以將該信將下載儲存為 eml 格式,這個格式可以在大多數的用戶端郵件軟體打開或匯入

寄信者

顯示此信的寄信者

收信者

是這封信實際的收件人(數),可能會和打開信件後看到的收件者不同,這是有可能的,而且是以列表上看到的為主

附件

顯示此信有無附加

大小

顯示此信的大小

刪除

勾選項目(可多選)後,按下刪除即可刪除會刪除隔離區的記錄及隔離的實體信件,但不會刪除已經傳送到用戶端的信件

通常不建議手動刪除信件,信件會在隔離到期後自動刪除

重新發送

勾選項目(可多選)後,按下重新發送,即可將信件重新發送給原先的收件者,該信件若有執行過 重新發送,會被記錄在主旨欄位下以較為細小的文字記錄

發送給

勾選項目(可多選)後,填寫傳送名單後按下發送給按鈕,即可將信件發送給指定的收件者,該信件若有執行過指定發送,會被記錄在主旨欄位下以較為細小的文字記錄

管理員可以透過搜尋來快速找到信件,也可以在欄位的上方空白輸入處指定搜尋的項目,例如主旨上或收件者....

轉寄信件記錄區

所有符合過濾條件執行轉寄的信件,會記錄於此記錄區,信件會在此保留一段時間後自動刪除(保留時間可參考基本設定內的轉寄信件保留天數之設定值)

日期

記錄的是信件進入伺服器的時間,並非信件內所表示的時間(這有可能因為時區不同),兩者不同是 正常的

規則

顯示此郵件是觸發哪一個過濾器而隔離於此

方向

若呈現綠色圖示:表示此信件是從他方的伺服器寄入本伺服器的信件,例如 從 gmail.com 或 yahoo.com......

若呈現紅色圖示:表示此信件是由本地帳號寄出,有可能是寄給外部信箱或本地用戶,皆會標示為寄出

主旨

點按可以開啟信件,並查看該信件的完整內容

表頭:可以看該信件的信件表頭,信件表頭會記錄這封信件的傳遞路由及簽章或認證消息

另存:可以將該信將下載儲存為 eml 格式,這個格式可以在大多數的用戶端郵件軟體打開或匯入

轉寄

此信轉寄給何人

寄信者

顯示此信的寄信者

收信者

是這封信實際的收件人(數),可能會和打開信件後看到的收件者不同,這是有可能的,而且是以列表上看到的為主

附件

顯示此信有無附加

大小

顯示此信的大小

刪除

勾選項目(可多選)後,按下刪除即可刪除會刪除隔離區的記錄及隔離的實體信件,但不會刪除已經傳送到用戶端的信件

通常不建議手動刪除信件,信件會在隔離到期後自動刪除

重新發送

勾選項目(可多選)後,按下重新發送,即可將信件重新發送給原先的收件者,該信件若有執行過 重新發送,會被記錄在主旨欄位下以較為細小的文字記錄

發送給

勾選項目(可多選)後,填寫傳送名單後按下發送給按鈕,即可將信件發送給指定的收件者,該信件若有執行過指定發送,會被記錄在主旨欄位下以較為細小的文字記錄

管理員可以透過搜尋來快速找到信件,也可以在欄位的上方空白輸入處指定搜尋的項目,例如主旨上或收件者....

自動回信記錄區

所有符合過濾條件執行自動回覆的信件,會記錄於此記錄區,信件會在此保留一段時間後自動刪除 (保留時間可參考基本設定內的 自動回信信件保留天數之設定值)

日期

記錄的是信件進入伺服器的時間,並非信件內所表示的時間(這有可能因為時區不同),兩者不同是 正常的

規則

顯示此郵件是觸發哪一個過濾器而隔離於此

方向

若呈現綠色圖示:表示此信件是從他方的伺服器寄入本伺服器的信件,例如 從 gmail.com 或

yahoo.com.....

若呈現紅色圖示:表示此信件是由本地帳號寄出,有可能是寄給外部信箱或本地用戶,皆會標示為寄

出

主旨

點按可以開啟信件,並查看該信件的完整內容

表頭:可以看該信件的信件表頭,信件表頭會記錄這封信件的傳遞路由及簽章或認證消息

另存:可以將該信將下載儲存為 eml 格式,這個格式可以在大多數的用戶端郵件軟體打開或匯入

自動回覆

此信自動回覆對象

寄信者

顯示此信的寄信者

收信者

是這封信實際的收件人(數),可能會和打開信件後看到的收件者不同,這是有可能的,而且是以列表上看到的為主

附件

顯示此信有無附加

大小

顯示此信的大小

刪除

勾選項目(可多選)後,按下刪除即可刪除會刪除隔離區的記錄及隔離的實體信件,但不會刪除已經傳送到用戶端的信件

通常不建議手動刪除信件,信件會在隔離到期後自動刪除

重新發送

勾選項目(可多選)後,按下重新發送,即可將信件重新發送給原先的收件者,該信件若有執行過 重新發送,會被記錄在主旨欄位下以較為細小的文字記錄

發送給

勾選項目(可多選)後,填寫傳送名單後按下發送給按鈕,即可將信件發送給指定的收件者,該信件若有執行過指定發送,會被記錄在主旨欄位下以較為細小的文字記錄

管理員可以透過搜尋來快速找到信件,也可以在欄位的上方空白輸入處指定搜尋的項目,例如主旨上或收件者....

放行記錄區

所有符合過濾條件執行放行的信件,會暫時置於此隔離區,信件會在此保留一段時間後自動刪除 (保留時間可參考基本設定內的放行信件保留天數之設定值)

日期

記錄的是信件進入伺服器的時間,並非信件內所表示的時間(這有可能因為時區不同),兩者不同是 正常的

規則

顯示此郵件是觸發哪一個過濾器而隔離於此

方向

若呈現綠色圖示:表示此信件是從他方的伺服器寄入本伺服器的信件,例如 從 gmail.com 或 yahoo.com......

若呈現紅色圖示:表示此信件是由本地帳號寄出,有可能是寄給外部信箱或本地用戶,皆會標示為寄出

主旨

點按可以開啟信件,並查看該信件的完整內容

表頭:可以看該信件的信件表頭,信件表頭會記錄這封信件的傳遞路由及簽章或認證消息

另存: 可以將該信將下載儲存為 eml 格式, 這個格式可以在大多數的用戶端郵件軟體打開或匯入

寄信者

顯示此信的寄信者

收信者

是這封信實際的收件人(數),可能會和打開信件後看到的收件者不同,這是有可能的,而且是以列表上看到的為主

附件

顯示此信有無附加

大小

顯示此信的大小

删除

勾選項目(可多選)後,按下刪除即可刪除會刪除隔離區的記錄及隔離的實體信件,但不會刪除已經傳送到用戶端的信件

通常不建議手動刪除信件,信件會在隔離到期後自動刪除

重新發送

勾選項目(可多選)後,按下重新發送,即可將信件重新發送給原先的收件者,該信件若有執行過 重新發送,會被記錄在主旨欄位下以較為細小的文字記錄

發送給

勾選項目(可多選)後,填寫傳送名單後按下發送給按鈕,即可將信件發送給指定的收件者,該信件若有執行過指定發送,會被記錄在主旨欄位下以較為細小的文字記錄

管理員可以透過搜尋來快速找到信件,也可以在欄位的上方空白輸入處指定搜尋的項目,例如主旨上或收件者....

郵件掃畫器

防毒設定

本系統採用ClamAV 初安裝好可以會因為尚無下載病毒碼,可能無法啟動服務,請等候系統自動在後台下載之後再進行啟動系統會每 12 小時對 clamav 的 mirror 站台自動更新病毒碼,若無法下載或更新,大多可能是你的前方防火牆 阻止了伺服器透過 https (tcp 443),對外進行資料下載,請檢查你的防火牆或 UTM的設定另外若不良的的 dns 伺服器也有可會造成無法解析到 clamav mirror 站台導致無法進行病毒碼更新

啓用服務

設定是否啟用此服務

服務狀態

顯示此服務是否正常執行中

病毒碼資訊

顯示掃毒引擎版本及病毒碼更新日期

掃毒方向

設定什麼方向的信件才要進行掃毒

預設是外來的信件才進行掃毒,對於內互寄或是內部外寄的信件將不進行掃毒

如果你有特殊原因可以調整從設定

隔離區保留天數

設定信件若被判斷為病毒信件,將會被隔離到病毒隔離區,此設定可以設定隔離區保留的時間,此期間內管理員可以至隔離區進行重新發送或下載該信件,超過此時間後系統會自動刪除

忽略掃毒當信件大於

設定信件若大約此設定值 則不進行病毒掃描

通常病毒都不會有太大的體積(file size),此設定可以減低伺服器的負載

病毒隔離區

當信件被判斷為病毒信件時,會置於此隔離區,信件會在此保留一段時間後自動刪除(保留時間可參考防毒設定內的隔離區保留天數)

日期

記錄的是信件進入伺服器的時間,並非信件內所表示的時間(這有可能因為時區不同),兩者不同是正常的

主旨

點按可以開啟信件,並查看該信件的完整內容

表頭:可以看該信件的信件表頭,信件表頭會記錄這封信件的傳遞路由及簽章或認證消息

另存: 可以將該信將下載儲存為 eml 格式, 這個格式可以在大多數的用戶端郵件軟體打開或匯入

病毒

顯示受感染的病毒名稱

寄信者

顯示此信的寄信者

收信者

是這封信實際的收件人(數),可能會和打開信件後看到的收件者不同,這是有可能的,而且是以列表上看到的為主

附件

顯示此信有無附加

大小

顯示此信的大小

删除

勾選項目(可多選)後,按下刪除即可刪除會刪除隔離區的記錄及隔離的實體信件,但不會刪除已經 傳送到用戶端的信件

通常不建議手動刪除信件,信件會在隔離到期後自動刪除

重新發送

勾選項目(可多選)後,按下重新發送,即可將信件重新發送給原先的收件者,該信件若有執行過 重新發送,會被記錄在主旨欄位下以較為細小的文字記錄

發送給

勾選項目(可多選)後,填寫傳送名單後按下發送給按鈕,即可將信件發送給指定的收件者,該信件若有執行過指定發送,會被記錄在主旨欄位下以較為細小的文字記錄

管理員可以透過搜尋來快速找到信件,也可以在欄位的上方空白輸入處指定搜尋的項目,例如主旨上或收件者....

群組信件派送

記錄查詢

群組派送設定

基本設定

群組派送設定,有別於 使用者設定的群組帳號功能

使用者設定的群組帳號功能 是可以任何人或外部的人員皆可寄給此帳號,且此帳號只能代表本機內的帳號

群組派送設定 可以設定指定只有某些人才能寄送給此帳號,且可以指定此帳號代表本機的某些帳號及外部的郵件地址

使用場景:

如要指定公司的 sales 是那幾個人,當寄給 sales 時信件會自動轉到設定的群組人員 此時適用於使用者設定的群組帳號功能

如果公司內部要發送公告給所有的人員,建議使用此群組派送功能,或是寄發會員信件也非常適用此功能

啓用服務

設定是否啟動此功能

記錄保留天數

設定派送記錄保留的天數

發送頻率控制

設定發給外部郵件的速度與頻率,若送給內部的帳號會全速送達

通常群組信件派送可能和有大量的信件發送,為了不影響同時間其他人收發信件 ,可以設定發送頻率 參數值來分散群組發送的鬆緊度

同時發送數量

設定群組信件在儲列處理時每次處理的信件數量

間隔延遲

設定群組信件在儲列處理時每次處理的信件數量之後要休息多少時間

名單設定

按下+新增 可以開始新增一則設定

按下每則過濾器的最右邊操作欄內的 "筆" 可進行該筆設定的編輯修改

啟用

設定此虛擬群組是否啟用

群組名稱

設定一個易於辨識的名稱,例如:所有同事

虛擬群組帳號

設定一個代號,此代號不可與 "帳號" 及 "群組" 重複,建議加上一個唯一的前導例如 gr all

允許寄件認證帳號

僅允許這些內部帳號可以可以寄給此虛擬群組帳號, 其他人若寄給此帳號將會收到無此收件者的回應

可以用 * 代表全部,或使用萬用字元 ? 來設定

多人可以用,或换行來表示

本機帳號名單

設定本機帳號的名單,可以用 * 表示全部或 用萬用字元?表示

另外可以設定全部 再排除其他人 例如 *,-admin,-tom,表示全部的人 但排除 admin 和 tom

外部電子郵件地址名單

設定外部的電子郵件地址, 通常可以設定發送會員電子報的名單

請注意: 請勿隨意亂寄發廣告信, 否則可能會伺服器 IP 可能會被舉報為黑名單

其他伺服器

DNS 伺服器

DNS 伺服器可以管理網域名稱的域名正解,若線路上游授權反解管理則亦可管理反解設定

基本設定

- 啟用服務
 - 。 設定是否啟用此服務
- 服務狀態
 - 。 顯示服務是否正常運作中
- 允許查詢
 - 。 設定可以進行本機網域查詢的來源,通常可以設定為 anv;注意最後要有分號結尾
- 允許遞迴查詢
 - 。 設定僅允許這些來源 可以用此伺服器查詢其他網域的結果 , 通常建議僅允許內部網 段或公司的共用 IP 網段
- 網內區段
 - 。 定義網內網段的範圍,此設定值可以用來區分設定轄區視界(view)的分隔

轄區 Zone 管理

轄區指的是一個授權的域名或子域名的設定組,形態可以是網域正解或網域反解

- 啟用
 - 。 設定此轄區是否啟用
- 轄區名稱
 - 。 可以輸入一個可以辨識的說明,例如: 公司的網域
- 轄區視界
 - 。 設定這個轄區是讓內部讀取或外部讀取,或是都是
- 轄區形態
 - 。 設定此轄區管理的是正解或是反解域名
- 網域名稱
 - 。 設定網域名稱 , 例如 mydomain.com
- 主 DNS 伺服器 IP

- 。 設定這個 網域的 NS 的 IP, 通常都是設定這機器的 對外真實 IP, 若是給僅對內的視界 則設定內部 IP
- 預設 TTL
 - 。 設定設定值的有效快取時間 單位為秒

當新增網域後系統會預先自動幫你自己幾筆預設的紀錄 , 其中有幾筆紀錄建議如果不清楚設定目的,請不要刪除或修改 , 尤其是關於 NS 相關的紀錄請務必要保留 , 錯誤的設定可能會造成 整個 DNS 服務無法啟動

紀錄管理

紀錄是轄區下的描述元素,本系統管理的紀錄有以下形態

- A
- 。 主機名稱與IP的正解設定,例如 @,www.mail
- 。 特別: @ 表示空的意思
- MX
 - 。 郵件交換設定 , 一筆名稱可以有多筆交換名稱 , 但優先權值越小表示權值越高 , 郵件遞送時會查詢最優先的 MX 設定優先傳輸
 - 。 MX 設定值並不是 IP, 需先設定一個主機名稱, 再設定該主機名稱的 A紀錄來對應
- CNAME
 - 。 跟隨設定的主機名稱的 IP
- TXT
 - 。 設定主機名稱的註解 ,通常會還會利用於域名擁有認證
- SPF
 - 。 寄件者原則架構 , 用於設定郵件主機與 IP 的綁定身分驗證
- DKIM
 - 。 域名密鑰識別郵件(DomainKeys Identified Mail, DKIM)是一套電子郵件認證機制,使用公開金鑰加密的基礎提供了數位簽章與身份验证的功能,以檢測寄件者、主旨、內文、附件等部份有否被偽冒或竄改。

DMARC

。 以網域為基礎的訊息驗證、報告和一致性 (DMARC) 是電子郵件驗證、原則和報告通訊協定。這建立在寄件者原則架構 (SPF) 和網域金鑰驗證郵件 (DKIM) 通訊協定的基礎上。若這些驗證方法均未透過,則 DMARC 原則確定如何處理訊息

- AAAA
 - 。 IPV6正解設定
- NS
 - 。 名稱伺服器記錄指定網域或子網域的授權設定

Web 伺服器

基本設定

- 啓用服務
 - 。 啟用本伺服器的 web server網頁伺服器功能
 - 。 啟動伺服器預設會使用 tcp/80 port
- 服務狀態
 - 。 顯示目前 Web 伺服器是否正確啟動 , 並列出服務 PID , PID 數量會根據服務忙碌程度 有所不同
- PHP 版本
 - 。 本系統提供多版本的 php 服務,您可以選用其中一種以符合您的網頁程式的應用
- 起始首頁
 - 。 設定網頁根目錄的起始首頁 通常是 index.html 或 index.php
- PHP 附檔名
 - 。 設定 php網頁程式的副檔名
- 用戶個人網站功能
 - 。 設定帳號個人首頁是否使用, 若開啟此功能 ,且帳號設定有勾選使用 web 功能者 則此帳號可以在自己的 home 目錄下的 www 目錄下建立網站
 - 。 例如 admin 這使用者允許建立 web功能
 - 。 此用戶可以將網站透過 ftp 上傳到自己目錄下的 www 下
 - 個人網址為 http://server IP/~admin/
 - 。 通常不建議開啟此功能
- TLS 加密層級
 - 。 設定使用加密的最低層級,
 - 。 版本 V5.34 之前的版本 ,最高的加密層級為 TLSv1.2, V5.34(含)之後版本 最高可支援 至 TLSv1.3
 - 。 通常不建議設定在最高(TLSv1.3) 可能會造成對方若系統太舊會無法與我方伺服器連線
 - 。 目前最建議的設定為 TLSv1.1 表示可以接受 TLSv1.1, TLSv1.2 及 TLSv1.3連線
 - 如來源的加密層級太低,可以調整伺服器的加密層級來協調接受,但一般都是建議請對方升級加密層級,來配合我方

進階設定

- php.ini
 - 。 設定 php.ini 整體的設定值 ,此設定會影響到所也的網站設定
- Apache 模組
 - 。 此設定可以設定 httpd.conf載入的模組
 - 。 通常不建議隨意更改設定,錯誤的設定可能會造成 web server無法啟動
 - ** 以上如果設定已經被修改到嚴重錯誤導致服務無法啟動時,可以將內容全部清除, 按確定後會回復預設的設定內容.

網站設定

列出目前所建立的網站,本系統可以建立多個網站

可以在此建立一個新的網站或修改原本網站的設定

按下 新增 按鈕可以新增一個新的網站,設定網站前請先指定好 DNS 的 A 記錄或 CNAME 記錄,以確保設定可以正確被執行

基本設定

- 啟用
 - 。 設定此網站是否啟用
- 網站網址
 - o 範例 www.mydomain.com 或 mydomain.com
- 阜號
 - 。 預設如果不使用 ssl 會使用 tcp 80 port, 自訂 port 建議使用 1024 以後的 port, 並需避免與一些常用的服務 port 衝突
 - 。 議可以用 9999,8888,7777
 - 。 使用 ssl 和不使用 ssl 不能使用同一 port
- SSL 憑證
 - 。不使用
 - 此網站不使用 SSL/TLS 加密
 - 。 啟用:使用預設 CA 憑證
 - 此網站使用 SSL/TLS 加密 , 憑證使用系統預設的憑證 ,預設憑證可以參考 系統設定/SSL 憑證管理
 - 。 啟用: 自行上傳 CA 憑證

■ 自行剪貼憑證的 憑證金鑰,憑證證書,中繼憑證/串鏈 ,本系統使用 PEM 格式 , 看起來就像是普通的文字檔案,內容類似下圖

• 帳號

- 。 設定此網站的根目錄位於那個用戶的 _www_目錄下 , 之後可以用此用戶的帳號密碼 以 FTP 或網路芳鄰方式登入並將網站上傳到用戶目錄下的 _www_ 目錄
- 。 可以設定一帳號管理一個網站 或是 一個帳號管理多個網站

• 網站根目錄

- 。網站根目錄 預設是 _www_ 目錄之下,若要在同一個用戶下建立多個網站 可以在 此建立子目錄,並設定該子目錄為網站根目錄
- 。 這個目錄必須自行建立 , 請使用 ftp 軟體或 網路硬碟 進入新增目錄 , 目錄權限請 設定為 755

進階設定

- PHP :
 - 設定此網站是否要支援 PHP 動態網站, 若開啟 php 支援後可以再設定以下幾個常用的參數,若還需設定更進階的設定,可以在 進階手動設定 或 php.ini 修改
- AllowOverride
 - 。 確定允許存在于.htaccess檔案中的指令類型.
- RewriteEngine
 - 。 允許使用語法改寫定義 url 的轉向操作
- 進階手動設定
 - 。 個別網站如果要設定獨立的參數 (php.ini) 可以在此處設定
 - 。 可以調整這個網站的 php.ini 值:
 - 。 屬於開或關的設定: php_admin_flag php 參數 On/Off,例如: php_admin_flag register_globals On
 - 屬於數值的設定: php_admin_value php 參數 值 例如: php_admin_value post_max_size 64M
 - 設定 apache 環境參數:例如:RewriteRule ^/soft/([0-9]+).html\$ /soft.php?id=\$1

FTP 伺服器

基本設定

- 用戶可以透過 Windows 的檔案總管 或是使用 FTP 用戶程式例如 filezilla (建議使用,因為可以支援 UTF8 檔案名稱).
- 通過此設定可以很容易啟動此服務
- 啓用服務
 - 。 開啟或關閉 FTP伺服器
- 服務狀態
 - 。 顯示 FTP 服務狀況 及 pid
- 同時最多可連線的客戶數
 - 。 設定同時間可以連線的用戶端數量
- 連線最大子程序數量
 - 一個用戶端可能同時使用多線程,如果發現客戶端無法出現連線數不足時可以調整此 參數
- PORT
 - o FTP 通常使用 port 21,如果有特別理由可以重新設定 port,但應該要避開已經使用或通用的 port 如 smtp 25,pop3 110
- 使用 IPV6
 - 。 設定是否允許使用 IPV6 連線 , 必須要本伺服器有開通 IPV6 網路設定才能開啟此項 目 ,通常建議關閉
- 使用 UFT8 檔名
 - 。 由於目前的主流 ftp 軟體大多支援 UTF-8 檔名格式,建議預設使用 utf-8
 - 。 但如果您的用戶端可能使用 windows 的檔案管理員直接上傳者 , 可能會因為檔案管理員的 utf8 支援度不相容造成檔名亂碼 , 此時建議 可以停用此設定 , 若要配合網路 芳鄰讀取檔案者 ,網路芳鄰設定也必須同步設定編碼格式
- SSL 憑證
 - 。 不使用
 - 此網站不使用 SSL/TLS 加密
 - 。 啟用:使用預設 CA 憑證
 - 此網站使用 SSL/TLS 加密,憑證使用系統預設的憑證,預設憑證可以參考系統設定/SSL憑證管理

- 啟用: 自行上傳 CA 憑證
 - 自行剪貼憑證的 憑證金鑰,憑證證書,中繼憑證/串鏈 ,本系統使用 PEM 格式 , 看起來就像是普通的文字檔案,內容類似下圖

❷ 憑證金鑰(key) ----BEGIN RSA PRIVATE KEY----MIIEpAlBAAKCAQEA6jAfhsvux8OTgSL2Anri0csFAVI5fgR/vj2vWfWeH4tLeCn6 24GTqZ0QlpK9RMbytcRZsnVZqc4y0dNGfg6dk7A3q4OHDN/O25lp/53npzgHs5Gm bCrEkzGw5mdc+I+B5ZWdT9cne4OCmmkkHtzOGI+Ni/DewUSOkVKY77DuL8a8SDs+ 1w1NFX4sVQNtUKoO4t5sG8ECOsWgdHskgE2H1DfG8i7+NziOajTPf14LhRuYovdl /XOda42hlWFUeaZVM3V1oY/P7L7AaAhBJaLoe8Tg9t2APlJg0vtnnie6PdngCZvT L7RIXeR6QLsXsVKycRCUqk1mGkM6iR+jG0BYWwIDAQABAoIBAFU16WK8tUdObE9i jyzb1cgMHOgcKPsnW+u2uiT7b+t+XZl9fN99yGLA2ZZQEjoCQbHNne2HMXbNpkQe odmgK8nfJoJruyn+DWBrUljHxdBcXMED0BAvh5MfU4SiO3yGX9dPlwvD94PDmDPi 6deo8/yPzysKG6Mq9Mz/xtIACMqszPqkfKGeTa/aY7O9p7YQvLig5HXCL/DNDgHp MIID/jCCAuagAwiBAgiJAlQcLmpUMTXTMA0GCSqGSib3DQEBCwUAMiGeMQswCQYD ❷ 憑證證書(crt) VOQGEwJaSDEQMA4GA1UECAwHbXkgY2l0eTEXMBUGA1UEBwwOWGlueWkgRGizdHJp Y3QxEzARBqNVBAoMCk15IENvbXBhbnkxFTATBqNVBAsMDEhiYWRxdWFydGVvczEV MBMGA1UEAwwMbXlkb21haW4uY29tMSEwHwYJKoZlhvcNAQkBFhJhZG1pbkBteWRv bWFpbi5jb20wHhcNMTkxMDIzMDQ0NDM4WhcNMjlwMTI1MDQ0NDM4WjCBnjELMAkG A1UEBhMCWkaxEDAOBqNVBAqMB215IGNpdHkxFzAVBqNVBAcMDlhpbnlpIERpc3Ry aWN0MRMwEQYDVQQKDApNeSBDb21wYW55MRUwEwYDVQQLDAxIZWFkcXVhcnRlcnMx FTATBgNVBAMMDG15ZG9tYWluLmNvbTEhMB8GCSqGSlb3DQEJARYSYWRtaW5AbXlk b21haW4uY29tMIIBIjANBqkqhkiG9w0BAQEFAAOCAQ8AMIIBCqKCAQEA6jAfhsvu

x8OTgSL2Anri0csFAVI5fgR/vj2vWfWeH4tLeCn624GTqZ0QlpK9RMbytcRZsnVZqc4y0dNGfg6dk7A3q4OHDN/O25lp/53npzgHs5GmbCrEkzGw5mdc+I+B5ZWdT9cn

- 啟用匿名 FTP 服務
 - 。 啟用匿名 ftp 登入, 匿名 ftp 可以用 ftp 或 anonymous 這帳號登入,且不需密碼
 - 。 匿名 ftp 通常用來給公眾下載檔案之使用
 - 。 請確實設定好 匿名 ftp 內的限制服務
- 匿名 FTP 管理員
 - 。 設定匿名 ftp 的實體空間位於那個用戶的空間
 - 。 指定一名已經存在的使用者,匿名 FTP 之空間將建立在該使用空間下的 "_anonymous_ftp" 目錄下 該目錄將會自動產生,您無須自行建立
- 同時最大匿名連線數
 - 。 允許同時最多匿名登入數量
- 匿名下載速度限制
 - 。 限制匿名連線可使用的連線下載速度(從伺服器下載檔案)
- 匿名上傳速度限制
 - 。 限制匿名連線可使用的連線上傳速度(上傳檔案至伺服器)
- 限制服務
 - 。 設定限制匿名使用者不能使用以下的執行動作 , 勾選的項目表示 "禁止"

虛擬使用者管理

- 本系統允許建立 除了本機的帳號可以 FTP 登入自己的家目錄之外, 還可以設定 "虛擬帳號" 讓公司以外的客戶也可以上傳或下載指定區域的檔案
- 新增的虛擬帳號只能用在 FTP 的檔案服務登入,不能用來收發本機的 Email或是其他服務
- 按下[新增]按鈕
- 啟用
 - 。 設定此虛擬帳號是否啟用
- 上層管理員
 - 。 指定一個本地帳號來管理這個虛擬帳號的檔案內容
- 虚擬帳號名稱
 - 。 一個易於辨識的名稱,例如:張三
- 虚擬帳號
 - 。 此虛擬帳號不能與本機帳號,群組帳號,群組信件發送帳號 重複
 - 。 此虛擬 FTP 帳號之空間將建立在管理員使用空間下的 "_ftp_" 目錄下 該目錄將會自動產生,您無須自行建立
- 密碼
 - 輸入密碼時不可見,若要檢視密碼可以按一下眼睛圖示



- 上傳速度限制
 - 限制虛擬使用者的連線上傳速度(上傳檔案至伺服器)
- 下載速度限制
 - 。 限制虛擬使使用的連線下載速度(從伺服器下載檔案)
- 限制服務
 - 。 設定限制虛擬使用者不能使用以下的執行動作 , 勾選的項目表示 "禁止"

❷ 限制服務 ☑ 建立目錄 ☑ 刪除目錄 ☑ 刪除檔案 ☑ 覆蓋檔案 ☑ 更改檔名 ☑ 下載檔案 □ 上傳檔案

- 傳送上傳報表
 - 當虛擬帳號上傳檔案後系統每5分鐘會自動匯集報表傳送郵件給上層管理員
 - 。 收到的報表格式如下圖:

知: Ftp伺服器上傳通知及報表

Pate: Fri, 10 Sep 2021 16:50:01 +0800

rom: <admin@localhost.localdomain> 🕮

o: <jerry@localhost.localdomain> 🕮

日期: 2021-09-10 16:46:25

使用者: ftp2(陳二)

檔案: 未命名的試算表.gsheet

大小: 176

日期: 2021-09-10 16:46:29

使用者: ftp2(陳二) 檔案: 米奇形狀.pdf

大小: 113354

日期: 2021-09-10 16:46:30

使用者: ftp2(陳二)

檔案:

大小: 176

日期: 2021-09-10 16:46:33

使用者: ftp2(陳二)

網路芳鄰伺服器

基本設定

- 網路芳鄰伺服器是模擬 Windows 的網路芳鄰檔案共用的服務 , 開啟服務可以從 Windows , MacOS 或 Linux 系統 透過 CIFS 或 SMB通訊協定服務來進行認證連線並傳輸檔案
- 網路芳鄰網路服務應該限制在區域網路內使用 , 不建議開放到網際網路上
- 啓用服務
 - 。 設定是否啟用服務
- 服務狀態
 - 。 顯示服務狀況及執行的 PID
- 工作群組名稱
 - 。 設定 群組名稱 , 請依照您的網路環境設定

• 伺服器名稱

- 。 設定此伺服器在 區域網路上的 netbios名稱
- 。 設定後您可以用 //名稱/帳號 連線

• 個人分享區

- 。 開啟這個功能,讓啟動網路芳鄰功能的用戶可以透過 CIFS/SMB 協定,存取個人空間內的 資料.
- 。 用戶必須在帳號設定設定 帳號可行使功能 必須包含 網路芳鄰功能

NTLM 使用者驗證

- 。 設定伺服器接受 NTLM 使用者驗證
- 。 某些 Windows 的電腦可能會經由防火牆或防毒軟體將 認證設定為 NTLM,必須打開 此功能,否則此類電腦無法登入連線

• 檔名字元集

- 。 一般使用建議選 UTF8,若配合 WIN 檔案管理員 FTP 上傳者,可以調成傳統編碼格式 BIG5(繁中)或 GB2312(簡中),注意:其他編碼可能會造成檔名變成亂碼
- 。 請注意:若設定為非 UTF-8 時 , 帳號的名稱不能設定非英文 ,否則會無法登入網路 芳鄰

• 允許連線 IP

- 。 設定僅允許表列的 IP 來源才能連線
- 。 可輸入完整 IP,或區段 IP(例如:192.168.) 多個設定可以用『逗號』或『空白』或『換行』 分隔

共用分享區設定

網路芳鄰除了可以設定個人登入管理自己的家目錄下的檔案,也可以由管理員設定共用區域,並設定那些來源 IP,那些人可以查看,那些人才能修改檔案

按下新增按鈕 可以新增一個分享區

- 啓用
 - 。 設定是否啟用此分享區
- 分享名稱
 - 。 例如: video, 連結分享區爲:\\IP或伺服器名稱\video
 - 。 如果非使用 UTF8 的編碼設定,強烈建議不要使用中文名稱(非英文)
- 隱藏分享區
 - 。 分享區設定隱藏,不會在搜尋分享時出現,但如果知道連線的名稱者可以設定連線
- 允許直接開啟執行檔
 - 如果分享區內放置可執行檔,通常在安全顧慮下不允許直接執行必須下載到本地硬碟 後才能執行,若勾選此選項則允許直接在原地執行此檔案

- 可讀使用者
 - 。 設定可以讀取此分享區的人員 , 需輸入本地的 帳號 , 例如 admin
 - 。 若不輸入表示所有人員 多人時可以用『逗號』或『空白』或『換行』分隔
- 可寫使用者
 - 。 設定可以寫入此分享區的人員, 需輸入本地的 帳號, 例如 admin
 - 。 若不輸入表示所有人員 多人時可以用『逗號』或『空白』或『換行』分隔
- 允許連線 IP
 - 。 設定允許連線的 IP, 若不輸入即沿用基本設定,可輸入完整 IP,或區段 IP(例如:192.168.)
 - 。 多個設定可以用『逗號』或『空白』或『換行』分隔

DHCP 伺服器

基本設定

動態主機設定協定(Dynamic Host Configuration Protocol,縮寫:DHCP),

又稱動態主機組態協定,是一個用於 IP 網路的網路協定,位於 OSI 模型的應用層,使用 UDP 協定工作,主要有兩個用途:

- 用於內部網路或網路服務供應商自動分配 IP 位址給使用者
- 用於內部網路管理員對所有電腦作中央管理
- 啓用服務
 - 。 設定是否啟用此服務
- 服務狀態
 - 。 顯示此服務狀態及執行的 PID
- 網域名稱
 - 。 設定此網路環境使用的網域名稱
- DNS 伺服器
 - 。 指定給用戶端的 DNS 伺服器, 建議可用: 8.8.8.8, 多筆可以用 逗點分隔
- 和約時效
 - 。 設定分配的 IP 有效時間, 逾時後會重新分配新的 IP
- 網路遮罩
 - 。 設定此網路遮罩, C class 設定為 255.255.255.0
- 網路閘道

- 。 設定分配給用戶端的閘道
- IP 分配範圍
 - 。 設定分配的 IP 節圍

位址綁定

如果要固定某一部電腦的 IP,可以透過 位址綁定 利用網路卡的 Mac address 與 IP 的綁定,讓 IP不會跳動

按下 +新增 按鈕

- 啟用
 - 。 設定此設定是否生效
- 機器名稱
 - 。 易於辨識的名稱,例如: 大雄的電腦
- 硬體位址
 - 。 機器的網卡硬體位址,例如: 6D:13:08:18:55:78
- 綁定位址 IP
 - 。 設定此電腦欲綁定的 IP

資料庫伺服器

本系統內建一套 MariaDB

MariaDB 是一套與 MySQL完全相容的資料庫,並且完全免費與開源的資料庫,能輕鬆成為 MySQL的 代替品,原本的程式幾乎可以不需任何修改即可操作此資料庫.詳細請參考MariaDB官方網站.

開啟此服務,可以配合 Web 伺服器内的 PHP,執行動態的網站 例如:wordpress 或是 joomla 或購物車 ...

基本設定

- 啓用服務
 - 。 設定是否啟用此服務
- 服務狀態

- 。 顯示服務狀態與執行的 PID
- 版本
 - 。 顯示目前使用的 MariaDB 的版本
- root 密碼
 - 。 若要更改 root 密碼請由此更改,
 - 。 請勿使用 phpMyAdmin 更改權限及密碼.
 - 。 建議盡量不要使用 root 權限操作資料庫.
 - 。 當使用者建立時若有勾選 SQL 功能,會自動建立一個與用戶同名的資料庫,用戶可以以自己的帳號/密碼登入並管理該資料庫.
- 強迫更改密碼
 - 。 當 root 密碼被第三方工具修改,造成密碼不同步時可以勾選此項目進行強迫更改密碼
- 開啟防火牆 port 3306
 - 。 開啟防火牆 port 3306(允許外部可以連線必須修 mysql 資料庫,請自行參考資料修改)
 - 。 除了開啟防火牆 port 外 還需要分別指定 user, db 連線的來源,可以透過 phpMyadmin 來修改 資料庫 mysql 內的 user 與 db 表格的設定

my.cnf

- 除非有特定需求,通常無須自訂,錯誤的設定可能造成服務無法啟動
- 如果設定已經被修改到嚴重錯誤導致服務無法啓動時 ,可以將內容全部清除 ,按確定後會回 復預設的設定內容.

phpMyAdmin

- phpMyAdmin 是一套開放原始碼的自由軟體,主要功能用來管理 MySQL(或相容)的資料庫,大 多數使用 PHP+MySQL 開發環境的程式設計師應該都不陌生,為了方便用戶管理資料庫已經 預先將此軟體安裝於本系統中,
- 為了系統的安全性建議僅在使用時開啟平常可保持關閉,或是設定以下允許使用的 IP,防止網路 駭客探測或盜取資料.
- 啓用服務
 - 。 設定是否要啟用此功能
- 版本
 - 。 目前 phpMyAdmin 的版本
- 自訂路徑
 - 。 設定一個只有管理員自己知道的路徑,可防止被駭客探測或掃描.
- 允許使用的 IP
 - 。 設定一個或區段的 IP,只有限定的 IP 才能操作此系統.

• 訪問連結

- 。 顯示出連接到 phpMyAdmin 的服務連接,你必須符合上述的設定條件才能連線,
- 若從內部 IP 連線 , 則需把服務的網址改為 內部 IP , 例如 : https://192.168.8.10:88/phpMyAdmin888/

LDAP 伺服器

基本設定

輕型目錄存取協定(英文: Lightweight Directory Access Protocol,縮寫: LDAP)是一個開放的,中立的,工業標準的應用協定,通過 IP 協定提供存取控制和維護分散式資訊的目錄資訊。

本系統使用 LDAP 服務 主要用於兩種服務目的:

通訊錄:

。 個人通訊錄:可在個人的 WebMail 下新增修改個人可以存取的通訊錄,在寫信時可以很方便的調用

• 共用通訊錄:

由管理員建立,並設定其讀寫權限,可設定那些人可以讀取,那些人可以編輯,同樣可以用於用戶在寫信時的調用

• 認證:

。 系統會自動同步本機的帳號/密碼到此LDAP, 其他設備可以透過LDAP服務協定來進行 設備認證

• 啟用服務

。 設定是否啟用服務

• 服務狀態

。 顯示 LDAP 服務狀況 及 pid

• Base DN:

- 。 通常依循慣例寫法將 網域名稱以 DC 分隔書寫 , 例如:ldap.mydomain.com , 可以寫成:dc=ldap,dc=mydomain,dc=com ,
- 。 不過若沒有對外服務,僅供系統內部使用可以使用預設的 dc=ldap 即可

root manager

。 這是此 ldap 服務的最高權限用戶 ,系統預設 cn=ldaproot,dc=ldap , 且不能更改

password

。 這是設定 root manager 的密碼 ,預設是空白 ,但並非沒有密碼而是使用本系統的預設 密碼 ,如果沒有必要可以不需重新設定

• SSL 憑證

。 設定是否啟用 SSL 加密服務,標準的未加密的 LDAP 服務是走 TCP/389,如果是走加密 ldaps 走 TCP/636

管理員

。 通常不建議使用 root magager 的身分去操作 ldap 服務 ,如果要在其他的機器使用本系統的內容或認證 ,建議使用這個管理員來進行資料存取的權限

連線 DN

o 如果上述的管理員設定 admin,則一般在其他系統書寫 user dn 時的寫法為: uid=admin,ou=users,o=linux,dc=ldap

• 回朔資料

。 LDAP 系統會每天備份一份完整的資料,並保留最後30天的資料可供回溯,萬一資料損害可以透過此功能回溯到前一天的資料,或指定的前今天資料

• 整修資料庫

。 當LDAP 伺服器無法啟動,資料異常或是通訊錄無法刪除或無法設定操作權限等異常狀 況時 ,可以按下此按鈕進行LDAP 資料庫自動維護,維護時間通常為幾秒鐘到幾分鐘,維 護期間LDAP 服務將會暫時停止.

共用通訊錄 / 新增編輯通訊錄

- 左邊的部分顯示為通訊錄的樹狀結構 , 通訊錄的權限會繼承給以下的子通訊錄 , 子通訊錄也可以自己設定權限
- 系統會自動產生一本或多本與本機相同名稱的通訊錄錄並以相同網域名稱建立 , 且在新增與 刪除帳號時會自動維護 ,
- 此預設的通訊錄預設權限為開放給所有使用者可以讀取,若管理員不希望讓所有用戶可以查看此通訊錄,建議可以在通訊錄設定其讀取權限
- 右邊的部分為目前打開的通訊錄的內容列表,管理員可以在此進行通訊錄資料庫的維護
- 上層目錄
 - 。 設定此通訊錄於目錄結構樹的位置

通訊錄名稱

。 名稱可以使用中文/英文或數字,但不可使用符號

• 可讀使用者

- 。 設定有那些使用者可以讀取這本通訊錄 , 預設空白為全部帳號都可以讀取內容 , 使用者可以在 WebMail 寫信時取用此共用通訊錄
- 可寫使用者

。 設定那些使用者可以編寫此通訊錄 ,預設空白為沒有人可以編輯 ,被允許編輯的用戶可以在 WebMail 的共用通訊錄內新增編寫通訊錄的內容 ,或由系統管理員於此處進行編輯

共用通訊錄 / 新增編輯聯絡人

- 先在左邊的通訊錄選擇您要新增資料的通訊錄,再按+新增 進行資料新增
- 新增時 姓名及電子信箱為必須一定要的欄位 , 且 姓名欄位在一個通訊錄內不可以重複 , 且 盡量不要使用符號

網路設定

WAN 介面設定

IPV4

如果您只有一片網卡,不管是直接連結對外(使用真實 IP)或是設定於防火牆之後(使用虛擬 IP),都請設定於 WAN 介面

• 主機名稱

- 。 設定本機器在網路上的唯一名稱,名稱以 FQDN 格式 例如: mail.mydomain.com
- 。 主機名稱必須正確設定,例如: yourdomain.com 或 mail.yourdomain.com, 設定前請先 用 ping 指令 確定你要指定的這個主機名稱,所解釋到的 IP 和你的伺服器 IP 相同,不正確的設定將會造成伺服器某些功能不正常,例如 FTP,伺服器轉寄重寄,群組帳號失效,信件遺失 ...等問題

硬體位址

。 顯示此介面網卡的硬體位址 mac address

- IP
- 。 顯示目前設定的 IP,及自動偵測出的對外真實 IP
- 。 本系統會以類似 whois 的方式 , 對外部的幾台伺服器發出"what is my ip"的詢問 , 再由外部伺服器告知從外部看到連結的 IP , 藉以確定對外連線是否正常
- 。 如果無法顯示對外真實 IP,可能是您的前方防火牆限制您對外連線的封包 , 請務必要處理好此問題 , 否則伺服器之後可能無法正確對外連線 , 或無法註冊和無法自動更新

• 網路連結方式

- 。 可分為三種方式
- 。 固定 IP 連結

- IP:設定固定 IP,若安裝於防火牆內可以設定內部虛擬 IP,之後必須使用防火牆導入服務阜(port)
- MASK:網路遮罩,通常是 255.255.255.0
- Gateway:網路閘道,請依照 ISP 給您的資料填寫,如果設定虛擬 IP,通常是設定防火牆的 LAN IP
- 主要 DNS: 設定此伺服器使用的 DNS 服務器,通常可設定 google DNS: 8.8.8.8,或 hinet: 168.95.1.1,或是內部有自己的 DNS 伺服器 也可以
- 次要 DNS: 可以設定或省略
- 。 DHCP 連結
 - 設定由 DHCP 伺服器自動配發 IP, 通常不建議使用此設定
- o PPPoe 撥接連結
 - 如果您的伺服器直接連結於ISP的的數據機之後,可以選擇此項目,並依照ISP 提供的資料填寫帳號及密碼,通常 hinet 的線路會填寫 數字@ip.hinet.net 以取 得一個固定的 IP

設定好 WAN 介面後如果正確無誤,通常會自動重新導到新 IP 的管理介面連結 ,如果沒有正確切換 ,請重新在瀏覽器上輸入新的 IP 連結

如果測試網路是否連結正確,可以到網路設定/網路測試工具使用 DNS 查詢或 PING 測試

通常公司大多已經有防火牆設置,比較建議的是將 WAN 網卡設定連結內部的交換機,並設定內部為內部固定 IP(不建議使用 DHCP),再經由防火牆設定,導入需要的服務阜(port)

建議導入的 port 如下 (請依照需要的服務導入)

- TCP+UDP 53/DNS 伺服器 (named server)
- TCP 88/管理介面
- TCP 443/WebMail
- TCP 25/SMTP, 465/SMTPs(tls), 587/SMTPs(starttls)
- TCP 110/POP3, 995/POP3s(tls)
- TCP 143/IMAP, 993/IMAPs(tls)
- TCP 80 及其他自定 網站伺服器
- TCP 21/ FTP 伺服器, TCP 60000~61000 PassivePorts (此 port 範圍導入會增加 FTP 伺服器連線的 穩定性)
- TCP 389 : LDAP , TCP 636 : LDAPs(TLS)
- TCP 3306: 資料庫開放外部連線(通常不建議開啟)
- TCP 873:備援機(主要角色),當主要與備援機分處不同地點時才需要開啟

IPV6

如果您的線路具備有 IPV6 的服務 ,可以啟動此項目 ,並依照 IPV6 的位址設定格式設定 IPV6 的地址及 Gateway

hosts

此欄位設定會增加到 /etc/hosts 檔案內,用於設定靜態的 主機名稱 -> ip 解析例如:10.1.1.1 www.mydomain.com, www.mydomain.com 將優先解析爲 10.1.1.1

LAN 介面設定

如果您的機器上有第二片網卡,可以啟動此網卡

通常會使用 2 片網卡 大多是 第一片網卡 連結 WAN 並設定對外(與 ISP 的數據機連線),第二片網卡設定 LAN 連結(與內部的交換機 Hub 連線) 指定內部虛擬 IP

可以設定 DHCP 伺服器自動分配 IP 給同樣連線在內部交換機的內部電腦提供上網服務

通常公司大多已經有防火牆設置,所以一般建議不需要安裝此網路卡,比較建議的是將 WAN 網卡設定連結內部的交換機,並設定內部為內部固定 IP(不建議使用 DHCP),再經由防火牆設定,導入需要的服務阜(port)

靜熊路由

當公司網路環境有多個路由器,並且切分為多個網段(subnet),可能會需要設定靜態路由功能來與網路環境協作

此功能通常必須具備專業的網路環境規劃,才需要設定此功能

實際設定方法需參考現場規劃的網路拓墣來制定

• 路由名稱:可以設定一個易於辨識的名稱

網路目標:設定來源網路遮罩:設定網路目標的遮罩

• 路由:指定導向的路由

• 介面:設定指定流量的介面

連接設定

設定預設的管理介面及 webmail 使用的通訊阜

管理介面服務阜: 系統預設為 88, 如要連線到管理介面可以在瀏覽器的網址列上輸入 https://xxx.xxx.xxx.xxx:88, xxx.xxx.xxx 是伺服器的 IP, 若要更改服務阜, 需要小心不要設定與其他服務衝突, 建議設定 1024 以上

TLS 加密層級: 設定 TLS 連線最低門檻,建議使用 TLS 1.2

WebMail 加密服務阜:預設為 443,若要連線到 WebMail 介面,可以在瀏覽器的網址列上輸入 https://xxx.xxx.xxx,xxx,xxx,xxx.xxx 是伺服器的 IP,

若要更改服務阜,需要小心不要設定與其他服務衝突,建議設定 1024 以上

更改其他阜號後網址後必須加入指定的:阜號

通常如果 Web 伺服器如果有需要用到標準 https (port 443), WebMail 加密 port 必須讓出占用的 443, 此設定一定需要修改為其他的 port

TLS 加密層級: 設定 TLS 連線最低門檻,建議使用 TLS 1.2

WebMail 未加密服務阜 http: 若伺服器未申請安裝 SSL 憑證, 瀏覽器在連線時會跳出警告訊息,此時可以設定一個不加密的通道(port) 避免此現象,但建議此通道僅限制於內網使用,避免網路風險,此通道預設為關閉,若無必要建議不要開啟

連線 IP 限制:設定哪些 IP 允許登入管理介面及 WebMail 介面,多個設定可用換行或逗號分隔,設定方式請參考功能頁面的說明.

此功能亦可以經由 防火牆設定/手動防禦設定 制定更安全的防禦手段(經由防火牆設定的防禦機制可以完全封鎖到網路封包),例如要防止特定的來源來進行資安掃描時可以將該 IP 封鎖

網路測試工具

此功能可以當作一個網路探測工具,不同的是其測試的角度是站在伺服器本身對外測試,因此可以 更客觀測試並找出連線上的錯誤

DNS 查詢

可以測試伺服器本身的 DNS 設定,或是其他網域的 DNS 設定是否正確,或設定後是否已經生效(站在此伺服器的角度觀察)

DNS SERVER:

設定預設即參考網路設定/WAN介面設定內的 DNS 設定

指定:可以設定其他他的共用 DNS 來進行測試,例如 hinet: 168.95.1.1,或 google: 8.8.8.8,或 CloudFlare: 1.1.1.1,若要封閉迴路來測試自己本身設定的 DNS 是否正常,可以使用 127.0.0.1 或是 伺服器本身的 IP

解析網域主機或 IP: 依照正解或反解輸入 host/domain 或 IP

解析類別:提供基本的 A, AAAA, MX, CNAME, TXT, NS 及 PTR(反解)

PING

站在伺服器本身的角度執行 ping 指令並觀察回應可以設定 PING IPV4 或 IPV6 的模式

Tracerouter

站在伺服器本身的角度執行 trace route 指令, 並觀察其回應

Web test

站在伺服器本身的角度進行對外瀏覽,以測試防火牆是否阻擋伺服器外出的封包可以輸入 https://xxx.xxx.xxx,或 http://xxx.xxx.xxx 執行回應的內容為 html 原始碼所以看來像亂碼,通常只提供觀察參可使用

前方伺服器若阻擋伺服器對外的 TCP 443(標準 https 通訊),會造成伺服器無法正常進行授權驗證,並且無法正常自動更新韌體,此時務要要找出防火牆(指的是公司所設置的防火牆,並非系統選單內的防火牆功能)阻擋的原因,自行或委請相關廠商進行正確的設定

防火牆設定

一般設定

啟用 NAT 功能:當系統有安裝第二片網路卡(LAN),此功能才能生效

WAN 端不回應 ping: 設定此功能後可以讓本機的 IP 不接受 ping 封包, 不回應外界 ping(ICMP 封包)

自動防禦阻斷

此功能伺服器的可以依照來襲的不法或是違反規則定義的來源即時主動阻擋一段時間之後再解除阻擋,若來源多次來襲,可以設定累犯機制將該來源長期阻斷,防禦阻斷的因素可以參考以下

啟用服務: 設定此自動防禦功能是否要啟用

阻斷IP數量上限:對於觸及規定的來源IP,系統會以防火牆規則將之阻斷,被阻斷的來源會完全無法與本伺服器通訊,甚至是 ping 也無回應,看似本伺服器不存在網路上,因為阻斷的IP越多系統就需要更多的效能及記憶體來處理封包,所以我們的系統會對不同程度的觸犯來源在一定的時間後進行解放,如此可以達到伺服器資源有效的運用,此設定最高為 50000 個阻斷 IP,可以由管理員自行設定

原則上防禦的規則 採用 "一段時間內" 若同一個來源 "錯誤觸發次數" 大約設定值 即對該來源 IP 進行 一定的 "阻斷時間",該時間到期後會解除該 IP 的阻斷,以釋放伺服器的資源.

防禦設定

dns-deny(DNS 干擾): 如果管理員有啟動本機的 DNS 管理系統及服務 ,系統的 DNS 服務預設是非 OpenDNS ,也就是只提供上游來查詢本機的 DNS 結果 ,如果其他來源查詢非本機的 DNS 名稱時系統會拒絕並紀錄在攻擊次數

pop-auth(收信帳號登入認證): 通常是來源端在進行帳號密碼的暴力猜測,該規則會檢查 pop3,imap,pop3s,imaps 服務進行檢查,若嘗試登入失敗一次會紀錄一次攻擊

smtp-auth(寄信登入帳號認證):通常也是來源端進行帳號密碼的暴力猜測,該規則會檢查 smtp saslauthd 服務進行檢查,若嘗試登入失敗一次會紀錄一次攻擊

smtp-connect (smtp 連線): 雖然 smtp connect 屬於正常的連線行為,但如果在很短的時間內進行很多次連線,這樣就可能是攻擊的來源,最常出現的可能是 ddos 攻擊或是故意霸佔 smtp 的連線資源的行為

webadmin-auth(管理介面登入失敗):如果管理員有將 webadmin(管理介面)開放到公共網路上(管理員方便於任何地方登入查看及管理),若來源在一定的時間內進行多次的登入失敗,系統會判斷來源為攻擊行為紀錄一次攻擊

webmail-auth(WebMail 介面登入失敗): 和上一個功能相似, 差別是監視 WebMail 登入的介面

recidivist(累犯,慣犯):當來源IP觸犯了上面的任何一項攻擊規則時達到設定的次數後會被立即阻斷,系統亦會在阻斷一段時間後將其解開阻斷,若是該來源在一段時間內多次觸犯被阻斷,系統可將之視為累犯,該IP可以將其阻斷更長的時間

白名單

對於某些 IP,可以設定特別白名單,對其觸犯的行為不理會,例如:內部的虛擬 IP,或是公司防火牆(路由器)的共同出入口 IP,或是其他特殊原因的 IP 都可以加入該白名單內,白名單可以設定完整 IP 或是子網域

已阻斷中紀錄

對於上列說明的來源若觸犯了阻斷規則而被處於阻斷中的 IP, 管理員可以在此列表中看到並可查詢,若要提早將該 IP 解除阻斷,可以先點選後後按下解除阻斷按鈕

若要查詢較之前阻斷過但已經時間過後解除的 IP,可以到系統日誌/攻擊阻斷紀錄 查詢更多的紀錄

手動防禦設定

相較於前一章節所說明的自動防禦阻斷功能 , 此章節要說明的是 管理員如何 "手動" 管理防火牆封包管理

所有手動新增的防火牆條例可以在此列表中查看 , 刪除或修改

新增防火牆規則:

啟用:設定此防火牆條例是否生效

執行順序: 防火牆的條例是有順序的關係 , 例如先關閉所有(或一段)來源 , 再下一條例開啟特地的來源 , 若順序錯誤可能會有不同的結果

通訊協定:可以設定 TCP 或 UDP 或兩者

PORT: 設定防火牆要管理的 PORT, 可以設定單一port, 多個(以逗點分隔), 連續 port: (以冒號分隔)

例如:單一 999,多 port 999,1024,777,連續 1000:1005

來源表列方式: 設定下方的來源 表示的方式

正向表列: 設定的來源 IP 即表列

反向表列:除了設定的來源以外的 IP

來源: 要被規範的來源 IP

策略動作:拒絕並丟棄(DROP),允許通過(ACCEPT)

註解:說明此條例的用途或簡述(此欄位非必要)

虛擬服務轉阜

此防火牆服務必須系統有安裝第二片網路卡,並啟動 (一般設定的 NAT)功能,設定才會生效,此功能主要設定依照 port 將外部進來的封包,轉發到內部其他伺服器的指定 PORT,與通常的防火牆的 PORT 轉發 或是 虛擬伺服器的功能類似

設定說明:

啟用:設定此轉發條例是否生效

通訊協定:設定 TCP 或 UDP 或全部

外阜:外部對應的PORT,此PORT不能是本伺服器上已經使用的PORT,若要查驗那些PORT已經占用服務,可以到系統日誌/伺服器監視的netstat功能查看

允許連線來源:可以設定外部只有指定的IP才能通過此轉發規則,例如設定 分公司的IP,若保留空白表示全部的IP

內阜:內部轉發的機器對應的 PORT,可以與外阜不同

內部 IP: 欲轉發內部(NAT下)機器的 IP

註解:說明此轉發規則的簡述(可以不寫)

系統日誌

系統日誌是會在幕後檢視系統的運行,從系統的開機過程,到每一個服務的運作與交談,分別記錄 在分類的記錄檔內.

選擇查詢區段

系統日誌記錄是以檔案方式儲存,當檔案到指定的大小時會自動分開檔案儲存(可以自訂),檔案以 日期為後綴,查詢時可以切換欲瀏覽的區段檔案

搜尋

若要在目前區段內搜尋關鍵記錄,可以在搜尋欄內輸入關鍵字,進行篩選查詢,可以直接輸入欲查詢的關鍵字,例如: error

- 複合查詢: 查詢的關鍵字可以用 逗點分隔開,代表以 AND 方式查詢,例如:system,error
- 日期查詢時若遇到個位數日期時日期需輸入兩個空白來分隔(7 的前面要多一個空白)例如: Oct 7
- 關鍵字搜尋時不區分大小寫,複合搜尋條件的記錄內 關鍵字會以醒目的底色標示

雅出

匯出日誌時, 若無輸入搜尋條件時為整段下載, 若有關鍵字時則僅會下載符合條件的記錄

設定

- 日誌檔案大小: 可以設定每個記錄區段的大小(MB),當記目前錄檔案大於此大小時,系統會自動將檔案截斷儲存,另外開啟新檔案繼續儲存記錄
- 日誌檔案數:可以設定最多可以保存多少段落的記錄,當段落大於此設定時,最早的區段 會先被刪除回收磁碟空間
- 舉例: 如果每個記錄檔記錄 20MB,保留 3 個段落,表示會用到 20x3=60MB 的磁碟空間, 當第 4 個段落形成時,最早的(第一段)會被刪除,此為先進先出的原則,好比一般的行車記錄器 的原理.

為保留正確連續性系統日誌不能被管理員主動刪除,僅能透過逾期自動刪除的機制回收空間,不同的系統服務會記錄在不同的系統日誌內,每個日誌可以個別設定不同的設定參數

事件記錄

事件記錄

記錄系統自動執行的事務及管理員在管理界面上執行的變更項目或敏感的查詢事項

系統自動執行事項記錄

• 系統定時備份, 鏡射碟 , 系統更新 , 更新病毒碼 , 網路 ups 關機或重啟動等等 的發生時間與結果記錄在此

管理員操作記錄

會將管理員在界面上執行的動作或修改進行記錄:

例如:新增/修改/刪除使用者,功能上的設定 ... 郵件記錄器 查詢動作記錄,幾乎所有的頁面變更都會被記錄下來,保留查詢

主機事件

主機事件

記錄事項包含:

- 開機硬體偵測及系統核心 kernel 所有發出的通知/警告/錯誤 的記錄
- 系統服務的 通知/警告/錯誤 的記錄
- 硬體的 通知/警告/錯誤 的記錄
- 其它未歸類的系統記錄

SMTP 郵件

SMTP 記錄

記錄所有關於電子郵件的服務記錄包含

- 內部帳號互相寄信的記錄
- 本機帳號寄給外部客戶的信件記錄
- 外部客戶寄信給本機帳號的記錄

關於查詢的技巧請參考以下幾篇查詢文件

POP IMAP

POP IMAP 記錄

記錄用戶端(例如: outlook)與伺服器收取信件時的記錄 記錄中可能會包含:

• 何時:用戶端與伺服器連線的時間

• 來源:用戶端的 IP(若是使用 webmail 一律為 127.0.0.1)

• 用戶:用戶的帳號

• 通訊協定:可能是 IMAP 或 POP

• 連線階段的代號:由系統配發

範例: Oct 28 02:53:00 imap-login: Info: Login: user=\<vvv>, method=PLAIN, rip=192.168.8.87, lip=192.168.8.150, mpid=25346, session=\<yMV5pgjs+szAqAhX>

解譯:用戶 vvv 於 10-28 02:53:00 從 192.168.8.87的 IP 以 imap 協定成功登入到伺服器

範例: Oct 28 11:00:02 imap(jerry)\<26271>\<NIusRAvsk5Jv/CAr>: Info: flag_change: box=INBOX, uid=6732, msgid=\457126614.29506691.1666912866053@email.apple.com\, size=39825, from=Apple \no_reply@email.apple.com\, subject=你的 Apple 收據

解譯: 10-28 11:00:02 用戶 jerry 以 imap 協定從信箱 INBOX(收件匣)讀取一封信, 該信的標題為 "您的 Apple 收據"

範例: Oct 28 11:08:58 imap(jerry)\<14262>\<4nbjnQ7sQJ5v/CAr>: Info: flag_change: box=Trash, uid=111390, msgid=\0L4607067dLbd7e20eL44ed647L539698eL505145aL1312L1311.0L460706@ecgenuine.com.tw\, size=12854, from="捷元 B2B 採購網 "\epaper@ecgenuine.com.tw\, subject=【新商品來襲】壁掛式充電樁!電動車住家充電解決方案...

關於其它的搜尋技巧及記錄的解讀 請參考其它相關的文件

郵件掃毒

郵件掃畫記錄

記錄本系統使用的 clamav,執行或進行郵件掃毒時的行為記錄

攻擊阻斷記錄

攻擊阻斷記錄

記錄 防火牆設定/自動防禦阻斷 功能的相關執行及偵測行為記錄

範例: Oct 28 11:27:17 UMail v5 myFail2ban: smtp-connect trigger: 45.85.190.69

解譯: log 時間 來自 45.85.190.69 與我方伺服器進行 ssmtp 連線

注意: 此記錄並非代表攻擊, 僅記錄該 IP 與我方伺服器的連線動作

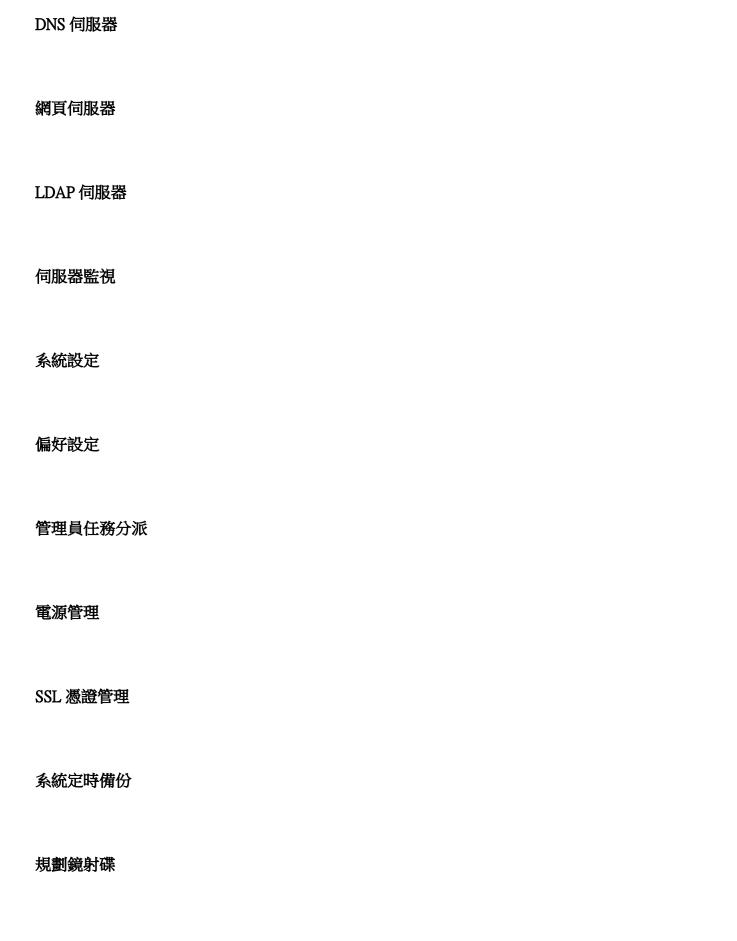
範例: Oct 27 20:55:31 UMail v5 myFail2ban: smtp-connect to block IP: 104.156.155.21: too many tries (130

times)

來自 104.156.155.21 在設定時間內連線次數超過 130 次,被伺服器判斷為攻擊行為,將該 IP 隔離一段時間

範例: Oct 27 23:17:45 UMail v5 myFail2ban: time to UNblock IP: 38.22.104.248

該 IP 已經隔離期滿,系統將該 IP 解開隔離



FTP 伺服器

磁碟管理

規劃備援機

系統更新

授權註冊

登出

有任何問題歡迎洽詢



http://line.naver.jp/ti/p/%40xat.0000132120.jmw



help@ublink.org