

6.6 整合檔案型防毒軟體之注意事項

檔案型的防毒軟體在排程定時的掃描作業中，有可能會造成 Exchange Server 資料庫或記錄檔遭到鎖住或隔離的問題，因而產生編號為 1018 的事件，進而造成用戶端使用者存取失敗的問題。

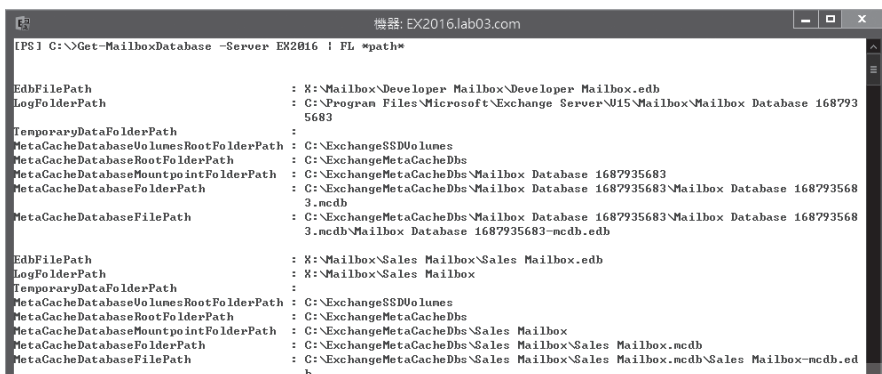
由此可見當我們準備將檔案型的防毒軟體安裝在 Exchange Server 2013 主機上時，便需要分別將特定的資料夾、執行程式、副檔名排除在掃描的名列中，如此一來才能夠讓 Exchange Server 的運行得以順暢。分別說明如下：

請注意！在接下來有關於命令主控台的範例中，凡是出現「EX2016」的字眼，即表示所要連線的 Exchange Server 主機名稱，因此你必須正確輸入實際的名稱。

需要排除掃描的資料夾：

- 信箱資料庫資料夾

Exchange Server 2016 中的信箱資料庫、檢查點檔案、記錄檔在預設中階會存放在 %ExchangeInstallPath%Mailbox 路徑之中，透過 Get-MailboxDatabase -Server EX2016 | FL *path* 即可查詢到。而有關於資料庫相關的索引檔預設也將會儲存在相同路徑之中。至於與群組檢測有關的檔案預設則會儲存在 %ExchangeInstallPath%GroupMetrics 路徑之中。



```
機器: EX2016.lab03.com
[PS] C:\>Get-MailboxDatabase -Server EX2016 | FL *path*

EdbFilePath           : X:\Mailbox\Developer Mailbox\Developer Mailbox.edb
LogFolderPath         : C:\Program Files\Microsoft\Exchange Server\15\Mailbox\Mailbox Database 1687935683
TemporaryDataFolderPath :
MetaCacheDatabase\0\LunesRootFolderPath : C:\ExchangeSSD\0\Lunes
MetaCacheDatabaseRootFolderPath : C:\ExchangeMetaCacheDbs
MetaCacheDatabaseMountPointFolderPath : C:\ExchangeMetaCacheDbs\Mailbox Database 1687935683
MetaCacheDatabaseFolderPath : C:\ExchangeMetaCacheDbs\Mailbox Database 1687935683\3.ncdb
MetaCacheDatabaseFilePath : C:\ExchangeMetaCacheDbs\Mailbox Database 1687935683\Mailbox Database 1687935683\3.ncdb\Mailbox Database 1687935683-ncdb.edb

EdbFilePath           : X:\Mailbox\Sales Mailbox\Sales Mailbox.edb
LogFolderPath         : X:\Mailbox\Sales Mailbox
TemporaryDataFolderPath :
MetaCacheDatabase\0\LunesRootFolderPath : C:\ExchangeSSD\0\Lunes
MetaCacheDatabaseRootFolderPath : C:\ExchangeMetaCacheDbs
MetaCacheDatabaseMountPointFolderPath : C:\ExchangeMetaCacheDbs\Sales Mailbox
MetaCacheDatabaseFolderPath : C:\ExchangeMetaCacheDbs\Sales Mailbox\Sales Mailbox.ncdb
MetaCacheDatabaseFilePath : C:\ExchangeMetaCacheDbs\Sales Mailbox\Sales Mailbox.ncdb\Sales Mailbox-ncdb.edb
```

↑ 圖 6-26 信箱資料庫路徑

有關於信箱伺服器的一般性記錄檔，這包含了訊息追蹤記錄檔以及行事曆修復記錄檔等等，預設皆會儲存在 %ExchangeInstallPath%TransportRoles\Logs 與 %ExchangeInstallPath%Logging 路徑中，可以透過以下命令參數來進行查詢。

```
Get-MailboxServer EX2016 | FL *path*
```

關於離線通訊錄的記錄檔預設則會儲存在 %ExchangeInstallPath%ClientAccess\OAB 路徑中，IIS 網站的系統檔案則預設會儲存在 %SystemRoot%\System32\Inetsrv 路徑中。至於信箱資料庫的暫時存放資料夾預設則是在 %ExchangeInstallPath\Mailbox\MDBTEMP 路徑中。



```

機器: EX2016.lab03.com
[PS] C:\>Get-MailboxServer EX2016 | FL *path*

DataPath                : C:\Program Files\Microsoft\Exchange Server\N15\Mailbox
CalendarRepairLogPath   : C:\Program Files\Microsoft\Exchange Server\N15\Logging\Calendar Repair Assistant
LogPathForManagedFolders : C:\Program Files\Microsoft\Exchange Server\N15\Logging\Managed Folder Assistant
MigrationLogFilePath    :
TransportSyncLogFilePath :
TransportSyncMailboxHealthLogFilePath :
  
```

↑ 圖 6-27 信箱伺服器相關記錄檔路徑

- 資料庫可用性（DAG）群組成員資料夾

叢集仲裁資料庫檔案預設會儲存在 %Windir%\Cluster 路徑之中，而在資料庫可用性（DAG）群組的架構中，典型的作法不會將用戶端存取伺服器與信箱伺服器安裝在同一部主機之中，因此預設作為存放監看的共用資料夾會是在 %SystemDrive%:\DAGFileShareWitnesses\

- 傳輸服務資料夾

針對傳輸服務記錄檔的儲存部分，例如訊息追蹤與連線記錄檔案皆會存放在 %ExchangeInstallPath%TransportRoles\Logs 的路徑之中，你可以下達 Get-TransportService EX2016 | FL *logpath*,*tracingpath* 命令參數來取得完整記錄檔路徑資訊。

7.4 復原信箱資料庫

有了針對 Exchange Server 2016 資料庫資料夾的排程備份，以及整部伺服器的完整排程備份之後，就可以在面對不同災害的情境下，來進行資料的復原作業。其中對於特定信箱資料庫的復原方式，管理人員可以自由選擇從完整的備份位置，或僅從資料庫資料夾的備份位置中來進行復原。請從 Windows Server Backup 介面的 [動作] 窗格中點選 [復原] 繼續。在 [開始使用] 的頁面中，便可以看到系統會讓你選擇，是要從這台伺服器還是其他位置的備份來進行接下來的資料庫復原作業。點選 [下一步]。

在 [選取備份日期] 的頁面中，可從行事曆的圖示中先挑選備份的日期，其中標示為粗體字的日期，即是有建立備份的日期。接著再挑選要還原的時間點，這時候系統便會列出可復原的資訊連結。確認後請點選 [下一步]。在 [選取復原類型] 頁面中，在此由於筆者是載入了完整伺服器的備份資料，應該也可以選取 [應用程式]。點選 [下一步] 繼續。




↑ 圖 7-19 選取還原類型

7.5 活用ESEUTIL重整與修復信箱資料庫

在完成了 Exchange Server 2016 所備份的資料庫相關檔案，到指定的路徑下之後，先不用急著將它復原至線上資料庫的路徑之中。因為你需要先為它進行一些健康檢查之後，才可以開始執行最後的復原作業，否則你將可能遭遇到無法復原或復原後的資料庫無法掛載的問題。在此假設我準備要復原一個名為「Developer Mailbox.edb」的信箱資料庫，這時候我就可以在命令提示列中，切換到這個剛復原的資料庫路徑下，然後下達以下命令檢查這個資料庫檔案的狀態。

```
Eseutil /mh"Developer Mailbox.edb"
```



```
選擇 機器: EX2016.lab03.com
[PS] C:\Program Files\Microsoft\Exchange Server\N15\Mailbox\RDB01>Eseutil /mh "Developer Mailbox.edb"
Extensible Storage Engine Utilities for Microsoft(R) Exchange Server
Version 15.01
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating FILE DUMP mode...
    Database: Developer Mailbox.edb

DATABASE HEADER:
Checksum Information:
Expected Checksum: 0xa1102d21
Actual Checksum: 0xa1102d21

Fields:
    File Type: Database
    Checksum: 0xa1102d21
    Format ulMagic: 0x89abcdef
    Engine ulMagic: 0x89abcdef
    Format ulVersion: 0x620,20
    Engine ulVersion: 0x620,20
Created ulVersion: 0x620,20
    DB Signature: Create time:01/29/2016 14:49:39.620 Rand:1913875683 Computer:
    chDbPage: 32768
    dbtime: 2747405 (0x29ec0d)
    State: Dirty Shutdown
    Log Required: 1864-1865 (0x748-0x749)
    Log Committed: 0-1866 (0x0-0x74a)
    Log Recovering: 1864 (0x748)
    Log Consistent: 1864 (0x748)
GenMax Creation: 05/31/2016 11:01:22.460
    Shadowed: Yes
    Last Objid: 5085
    Scrub Dbtime: 0 (0x0)
    Scrub Date: 00/00/1900 00:00:00
    Repair Count: 0
```

↑ 圖 7-24 下達 Eseutil /mh"Developer Mailbox.edb" 命令檢查復原後的資料庫狀態

如果 Status=Dirty Shutdown，則必須優先使用 Eseutil /R E01 /I /D 命令來將 Log 檔 Commit 到信箱資料庫。當再檢查一次之後如果發現 Status=Clean Shutdown 則表示沒有問題。

而當復原信箱的設定越來越多時，你可能會想要清除所已完成作業的復原信箱設定，這時候下達以下命令參數即可搞定！

```
Get-MailboxRestoreRequest | Where Status -eq Completed | Remove-MailboxRestoreRequest
```

```

機器: EX2016.lab03.com

[PS] C:\>Get-MailboxRestoreRequest

Name                                     TargetMailbox                           Status
----                                     -
趙雲 Recovery                          lab03.com\業務部\趙雲                   Completed
趙雲 Recovery02                         lab03.com\業務部\趙雲                   Completed

[PS] C:\>Get-MailboxRestoreRequest | Where Status -eq Completed | Remove-MailboxRestoreRequest
確認
確定要執行此動作?
正在移除完成的要求 'lab03.com\業務部\趙雲\趙雲 Recovery'。
[Y] 是(Y)  [A] 全部皆是(A)  [N] 否(N)  [L] 全部皆否(L)  [?] 說明 (預設值為 "Y"): A
[PS] C:\>Get-MailboxRestoreRequest
[PS] C:\>

```

↑ 圖 7-38 刪除所有已完成的復原要求設定項

7.8 裸機快速復原法

「天有不測風雲，人有旦夕禍福」。機器也是一樣的，無論你再如何用心維護它，它仍會有故障損毀的一天。因此萬一我們的整部伺服器主機板或硬碟全故障時，當硬體零件更換新品之後，如何進行裸機的復原作業呢？首先，你需要有最重要的完整伺服器備份磁碟，然後就可以透過 Windows Server 2012 R2 的開機安裝媒體，在啟動 [安裝程式] 頁面中時，點選左下方 [修復您的電腦] 連結繼續。

- 四成員的 DAG 設計：適合針對單一資料中心的規劃，藉由將所有 DAG 成員伺服器集中部署在相同的地理位置中，來達成高可用性的部署需求，適合在 Intranet 中所有主要伺服器都集中在企業總部的資訊網路設計。
- 四成員或以上的 DAG 設計（跨異地）：可以將 DAG 架構中的兩部成員伺服器部署在主要的資料中心（Data Center），而將其他兩部的 DAG 成員伺服器部署在次要的資料中心。如此一來，不僅達到本地端高可性的需求，也同時達成了異地備援的建構需求。這種情境很適合擁有多點營運中心，以及多點獨立的資料控管中心。

8.2 雙主機 DAG 安裝設定

在 DAG 中的成員伺服器的最佳配置，是讓每一部 DAG 的成員伺服器採用兩張網路卡（使用不同子網路），一張網路卡可以負責處理資料複寫的流量，另一張網路卡僅負責處理來自用戶端的 MAPI 流量。這種架構的運行方式，將有助於提升大流量 Email 的傳輸效能。

在此我們假設你已經有了一部現行的 Exchange Server 2016 Mailbox 伺服器，目前正準備要安裝第二部同等的 Mailbox 伺服器，建議你可以試試下列的命令安裝法，一道命令參數就能夠搞定整個安裝流程。整個安裝過程中一樣會做整備檢查，基本上只要通過檢查，安裝就能夠順利完成。

```
Setup.exe /Mode:Install /Role:Mailbox /IAcceptExchangeServerLicenseTerms
```

```
New-MailboxSearch -Name "PF Search 1" -AllSourceMailboxes $False  
-AllPublicFolderSources $True -SearchQuery "安全" -InPlaceHoldEnabled $True  
-TargetMailbox "Discovery Search Mailbox"
```

```
Start-MailboxSearch "PF Search 1"
```

9.6 善用法規遵循搜尋功能

儘管在 Exchange Server 2016 中新加入的法規遵循搜尋 (Compliance Search) 功能，沒有像就地探索 (In-Place eDiscovery) 有這麼多的限制，但它只能夠使用在搜尋這項任務上，而無法將搜尋到的郵件項目進行就地保留或是彙整到指定的信箱之中，這表示 Compliance Search 與 In-Place eDiscovery 必須相互搭配使用，才能解決大量信箱的內容搜尋與就地保留管理需求，也就是說一個負責搜尋任務，另一個負責將搜尋結果，選擇性的套用就地保留或匯出滿足條件的郵件項目至指定的信箱之中。

關於法規遵循搜尋功能的使用，必須透過 Exchange Management Shell 的命令工具來管理，而它的相關命令分別有 Get-ComplianceSearch、New-ComplianceSearch、Remove-ComplianceSearch、Set-ComplianceSearch、Start-ComplianceSearch、Stop-ComplianceSearch。想要執行上述命令必須至少擁有 Discovery Management 角色群組的權限，你可以在開啟該角色頁面中完成設定。

在我們開始動手實作範例之前，請先到以下網址下載 SourceMailboxes.ps1 與 MBSearchFromComplianceSearch.ps1 手稿程式碼。你只需要由上而下依序複製程式碼範例，並將它們依序儲存成上述的兩個 .ps1 檔案即可。

[https://technet.microsoft.com/zh-tw/library/mt607080\(v=exchg.160\).aspx](https://technet.microsoft.com/zh-tw/library/mt607080(v=exchg.160).aspx)

9.8 資料外洩防護（DLP）實作

為了監視與防止某一些特定敏感的 Email 內容被寄送到組織內的某些特定人士或是組織外的收件者，在 Exchange Server 2010 版本時期，我們通常都會盡可能善用傳輸規則的制訂來解決這一方面的管理問題。然而問題來了，因為有許多的敏感資訊，單單依賴主旨與內文關鍵字的檢測，是無法真正百分百判斷成功的，這包括了像是護照號碼、信用卡號碼、身分證字號、銀行戶頭帳號…等等。因為諸如這一類的資訊，大多有它們各自的編碼規則，因此我們就必須要有一套能夠自動辨別這一類資訊的元件加入，才能夠真正完全掌控它們是否被夾帶在 Email 內文之中。

其實打從 Exchange Server 2013 版本開始，Microsoft 便已經加入了一個名為資料遺失防護（DLP，Data Loss Prevention）的功能，透過它與傳輸規則的結合使用，便可以決定針對哪一種的敏感資訊所要執行的處理動作。在最新 Exchange Server 2016 中你可以擁有更完善的 DLP 功能，來管理各類敏感資訊的流通，只要透過三種方式來建立資料外洩防護（DLP）原則，分別是從內建的 80 個範本中來快速建立新防護原則，以及結合第三方的 DLP 整合軟體，來匯入滿足企業 IT 管理需要的原則，或是在 DLP 管理介面中自訂新的防護原則，然後設定新原則所需要的條件、規則以及處理動作。

想要使用這項功能請先開啟 [Exchange 系統管理中心]，然後開啟 [法規遵循管理] 節點中的 [資料外洩防護] 頁面。在預設的狀態下並沒有任何 DLP 原則，你可以在新增的下拉選單中來挑選新增設定的方式。在此我們點選 [新增自訂 DLP 原則] 繼續。

10.4 結合 Exchange 傳輸規則的使用

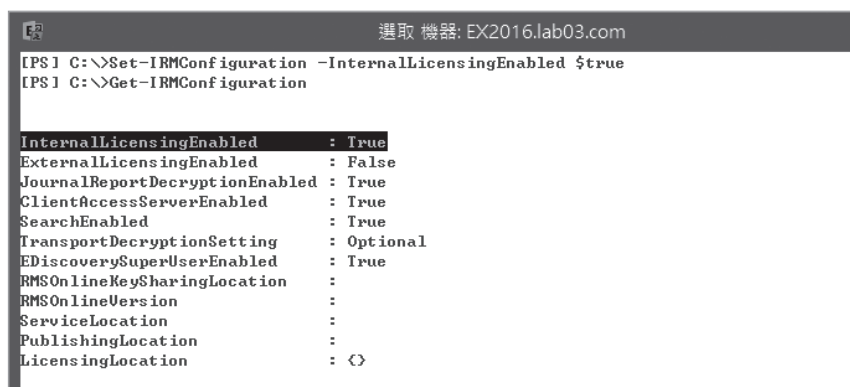
關於 AD RMS 伺服器角色整合 Exchange Server 2016 的應用方式，主要可以從兩個面向來看。第一種是從 Exchange 伺服端的傳輸規則，來配置所要自動以 AD RMS 進行加密的郵件條件。第二種則是由用戶端 Outlook 或 Outlook 網頁版的使用者，來隨時自行決定哪一些郵件的寄送所需要套用的 AD RMS 權限範本。針對第一種方式的整合需求，我們必須先在 Exchange Management Shell 介面之中下達以下命令來完成連接設定。

```
Set-IRMConfiguration -InternalLicensingEnabled $true
```

若想要查看設定結果是否成功，可以緊接著下達以下命令來得知。

```
Get-IRMConfiguration
```

你可能會覺得奇怪：我們又沒有設定 AD RMS 伺服器的連線位址，為何 Exchange Server 會知道要連線哪一台主機呢？其實原因簡單，那就是我們有登錄了 [AD RMS 服務連線點 (SCP)] 設定，而這項設定就是記錄在 Active Directory 資料庫之中。換句話說，如果你尚未登錄此設定，那麼在你後續下達 Get-RMSTemplate 命令時，便無法查詢到任何可用的 AD RMS 範本。



```
選取 機器: EX2016.lab03.com
[PS] C:\>Set-IRMConfiguration -InternalLicensingEnabled $true
[PS] C:\>Get-IRMConfiguration

InternalLicensingEnabled      : True
ExternalLicensingEnabled     : False
JournalReportDecryptionEnabled : True
ClientAccessServerEnabled    : True
SearchEnabled                 : True
TransportDecryptionSetting    : Optional
EDiscoverySuperUserEnabled    : True
RMSONlineKeySharingLocation   :
RMSONlineVersion              :
ServiceLocation               :
PublishingLocation            :
LicensingLocation             : <>
```

↑ 圖 10-20 啟用內部數位版權控管功能

關於這些已建立的範本清單，必須在完成 Set-IRMConfiguration 設定後才會顯示出來。AD RMS 使用了 XML 的標準格式原則範本，讓相容的 IRM 應用程式可以去套用一致性的保護原則，而在 Windows Server 2012 R2 裡所內建的 AD RMS 伺服器角色中，便提供了以 Web 服務的加密連線方式，提供前端的應用程式或系統服務列舉以及要求原則範本。以下是預設使用在整合 Exchange Server 2016 中的原則範本，你可以透過下達 Get-RMSTemplate 命令來查詢：

實戰範例 禁止轉寄

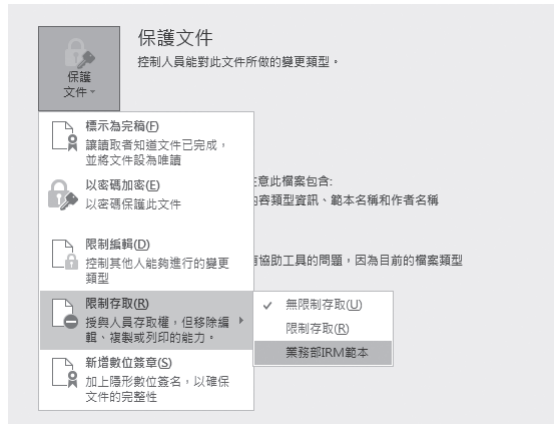
當收件者收到一封經由不要轉寄（Do Not Forward）原則範本所加密的郵件訊息時，收件者只能看到其內容，但是無法對於這一封郵件訊息進行轉寄、複製、列印或是螢幕的硬拷貝功能。



Name	Description	TemplateGuid
不要轉寄	收件者可以讀取這封郵件，但是無法轉寄...	cf5cf348-a8d7-40d5-91e

↑ 圖 10-21 查詢可用權限範本

完成了 AD RMS 與 Exchange Server 2016 的整合設定之後，接下來我們就可以嘗試建立傳輸規則，看看系統是否會自動加密特定條件的郵件內容。請開啟 [Exchange 系統管理中心] 網站，然後在 [郵件流程] \ [規則] 頁面中，點選新增小圖示就可以看到各種可用的規則範本，其中 [套用權限保護至郵件] 就是我們需要的，然而其實你也可以選擇 [建立新的規則]。



↑ 圖 10-40 Word 2016 權限範本選擇

POINT

AD RMS 結合日誌規則的使用會有問題嗎？

如果透過日誌規則封存的郵件，是經由 AD RMS 範本的加密處理，那麼負責稽核的人員可能會遇到無法開啟這些郵件訊息的問題。還好在系統預設的狀態下，Exchange Server 2016 會針對日誌規則所封存的郵件進行自動解密，不過前提是你必須預先將 Exchange Server 的電腦，加入到 AD RMS 管理介面中的 [安全性原則] [進階使用者] 啟用設定才可以，否則將會導致因系統無法進行郵件的解密處理，而使得將準備進行封存的郵件無法傳遞。而這一項自動解密設定，也可以經由 Set-IRMConfiguration 命令，來將 JournalReportDecryptionEnabled 參數值修改成 True 或 False。

AD RMS 所提供的數位版權保護機制，只能用在保護 Exchange Server 的敏感訊息內容嗎？當然不是，因為在以 Microsoft 系統為基礎的 IT 環境之中，敏感的資訊不會只存放在 Email 訊息之中。有許多只允許在企業內流通的文件檔案，甚至於只被允許在特定部門之間流通的檔案，通常會被存放在 Windows 檔案伺服器，或是集中儲存在以 ISO 文件管理為基礎的 SharePoint Server 伺服器之中。而在混合雲的架構之中，則可能被上傳至 Azure 上的

11.6 搶救誤刪的重要郵件

有時我們刪除一些當下認為不重要的 Email，但有可能後來又發現需要這一封 Email 才能夠處理接下來的任務，這時你可以到 [刪除的郵件] 資料夾中，將還沒有被清除的已刪除郵件移動到收件匣或其他自訂的資料夾之中。



↑ 圖 11-32 刪除的郵件

但如果在 [刪除的郵件] 資料夾中已經找不到該郵件時，怎麼辦呢？很簡單！只要在上一步驟的頁面提示中，點選 [擷取最近從此資料夾刪除或清空的郵件] 提示訊息，即可開啟管理頁面，來讓使用者還有一次機會自己復原已清除的郵件。然而無論是在 [刪除的郵件] 資料夾中的郵件，還是已經被清除的郵件，管理員都能夠設定它的最長保留期限。

一旦上述兩個位置的保留期限皆到期而找不到郵件時，怎麼辦呢？這時候就得依靠管理人員平日所做的備份，來協助還原使用者指定的郵件了，關於這方面的實戰講解，可以參考其它相關的章節內容。