

# 部署 Exchange Server 2019



**過**去 Exchange Server 總是被拿來和 Linux 下的 Mail Server 方案來進行比較，並且指出它在效能的表現方面不及開源的郵件系統，且又是一個狂吃資源的大怪物。如今 Microsoft 所推出的最新 Exchange Server 2019，不僅速度超快且支援部署在極簡的 Server Core 架構下，讓整體的運行不只有更充分的資源可以被利用，對於安全管理層面而言也將更加堅固。今日就讓我們透過本章節一同來學習，如何將最新 Exchange Server 2019，建置在 Windows Server 2019 的 Server Core 作業環境之中。

## 2.1 簡介

筆者早在 Exchange Server 5.5 版本時期，就已經開始接觸了 Microsoft 在協同合作方面的應用了，記得當時所使用的作業系統還是 Windows NT 4.0，並且也還沒有任何虛擬化平台可以使用，完全得部署在實體的主機之中，對於 IT 人員來可說是大挑戰，因為無論是平時的維護任務還是升級、移轉、修復、備份、還原，皆需要投入許多的時間來執行。

時間飛逝！如今已是 Exchange Server 2019 搭配 Windows Server 2019 的年代，對於上述所提到的各項任務之執行，IT 人員已不再需要心驚膽跳，因為在結合虛擬化平台架構的部署之下，可以說大幅縮短了測試、部署、升級以及移轉的時間。

更重要的是 Exchange Server 2019 本身的設計不僅在功能、效能以及安全性更加完善，對於 IT 人員來說在全新以 Web-based 設計的 Exchange Administration Center (EAC) 介面，搭配 Exchange Management Shell 命令管理的使用之下，讓原本許多看似複雜的管理任務都簡化了許多，且可以讓更多平日常用的維護操作，透過 PowerShell Cmdlet 的 Script 設計，達成自動化的管理需求。

進步也可以在結合 Office 365 的使用之下，輕鬆建構出堪稱是對企業最好的 IT 策略，那就是所謂的混合雲 (Hybrid Cloud) 運行架構，讓組織可以更加彈性的對於不同角色或不同需求的人員信箱，來加以分散存放。如此將可以一方面提升用戶端存取的效能，另一方面又能降低私有雲伺服器與網路的負載，最重要的是肯定也可以減輕 IT 人員的負擔。

## 2.2 新功能介紹

相較於前版的 Exchange Server 2016，全新的 Exchange Server 2019 從伺服器端到用戶端，主要增加了哪些令人關注的新功能呢，分別說明如下：

- 支援部署在 Windows Server Core：這項支援意味著不僅可以讓 Exchange Server 獲得更多可用資源，同時也大幅減少可能的攻擊面。
- 提供用戶端存取規則 (Client Access Rule) 管理機制，讓管理者可以預先配置好對於 Exchange 系統管理中心 (EAC) 以及 Exchange 管理命令介面的存取權限，也就是僅開放給特定的內部或外部來源網路，才能夠進行連線管理。

- 磁碟空間：在準備安裝 Exchange 的磁碟機上至少必須剩餘 30 GB 的可用空間。系統磁碟必須至少剩餘 200MB，對於準備存放訊息佇列（queue）資料庫的磁碟至少必須剩餘 500 MB。
- 螢幕解析必須至少在 1024 x 768 pixels 以上
- 檔案系統：無論是系統磁碟分割、Exchange 二進位檔案、Exchange 診斷記錄所產生的檔案、傳輸資料庫檔案（如郵件佇列資料庫）皆需要採用 NTFS 檔案系統的分割區。至於信箱資料庫與交易記錄檔，則可以選擇存放在更先進的 ReFS 檔案系統的分割區之中。

如果在您現行的網路環境之中已經有 Active Directory，甚至於已經有舊版的 Exchange Server 正在運行，那麼在您準備部署最新的 Exchange Server 2019 之前，必須優先注意以下相容性的要求。

▼ 表 2-2 新舊版本 Exchange 共存相容性

現行 Exchange 版本	共存支援
Exchange 2010 或更舊版本	不支援
Exchange 2013	只要是 Exchange 2013 累計更新 21（CU21）或更新版本皆支援（包含 Edge Transport Server）
Exchange 2016	只要是 Exchange 2016 累計更新 11（CU11）或更新版本皆支援（包含 Edge Transport Server）

在 Active Directory 的需求部分，首先樹系中的所有網域控制站都必須執行 Windows Server 2012 R2 Standard（含 Datacenter）或以上版本，樹系功能層級則必為 Windows Server 2012 R2 以上版本。

至於部署 Exchange Server 所在的 Active Directory 站台，必須包含至少一個可寫入的網域控制站（DC），而且也同時必須是全域目錄伺服器（GC），否則安裝過程中將會發生失敗，必須注意的是基於安全性

如表 3-1 所示便是一個典型 Exchange Server 的外部 DNS 記錄設定範例，您必須在內部與外部的 DNS 伺服器都有相同的記錄設定，這包括了網域的 MX 記錄、Exchange Server 的 A 記錄、OWA 的別名設定、自動探索（Autodiscover）的別名設定，只是 組是對應內部 IP 位址，組則是對應外部的 IP 位址。

其中 MX 記錄在外部 DNS 伺服器中 定要有，尤其是在對外的 SMTP 服務有兩台以上時，可以設定優先權來決定其先後順序。至於 Autodiscover 的記錄，便是用來方便用戶端，在無需輸入 Exchange Server 位址的設定之下，改由根據 Email 地址的尾碼即可找到伺服器的連線位址。

▼ 表 3-1 DNS 記錄參考設定

完整網域名稱 ( FQDN )	DNS 記錄類型	值
EX01.lab04.com	A	140.1.1.100
lab04.com	MX	EX01.lab04.com
mail.lab04.com	CNAME	EX01.lab04.com
owa.lab04.com	CNAME	EX01.lab04.com
Autodiscover.lab04.com	CNAME	EX01.lab04.com

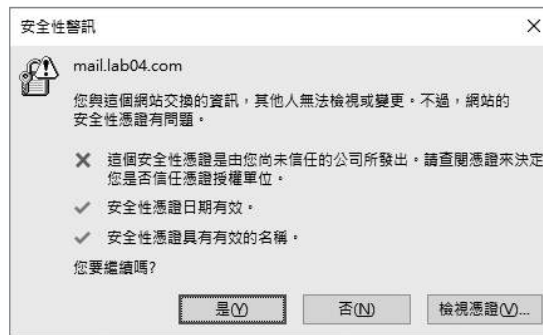
如圖 3-3 所示便是自動探索的別名新增設定範例，請在 [Alias] 的欄位中輸入 Autodiscover，再點選 [Browse] 按鈕來選取相對應的 Exchange Server 記錄即可。點選 [OK]。



▲ 圖 3-3 新增別名記錄

### 3.3 伺服器憑證申請

無論用戶端是使用 Outlook、OWA 還是行動裝置的 ActiveSync 連線方式，Exchange Server 對於連線的建立，皆是採用 SSL 加密安全通道來完成，如此可以有效避免傳送中的帳號、密碼以及各類訊息遭到網路封包分析工具的側錄。為此我們必須為 Exchange Server 建立專屬的伺服器憑證，才能啟用 SSL 安全通道功能。否則當使用者的 Outlook 或 OWA 在進行連線 Exchange Server 信箱時，將會出現類似如圖 3-4 所示的憑證安全警示。



▲ 圖 3-4 證安全警示

請連線登入 [Exchange 系統管理中心] 網站，然後點選至 [伺服器] 節點的 [憑證] 頁面中，如圖 3-5 所示在預設的狀態下還不會有正式使用的憑證，只會有供測試用途的自我簽署憑證。點選新增的圖示之後將會開啟 [新增 Exchange 憑證] 頁面，請選取 [建立向憑證授權單位索取憑證的要求]。點選 [下一步] 繼續。

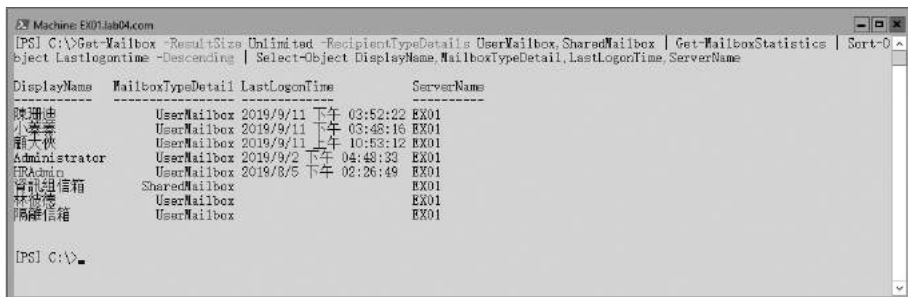
除了人員信箱之外，您也可以透過命令參數方式，來建立可讓多位人員一起存取的共用信箱。在以下的範例中，便是新增一個名為”IT Department”的共用信箱，並且將 [ 傳送為 ] 以及 [ 完整存取權 ] 的成員，分別選定為現行的 IT 以及 SI 安全性群組。如此一來這個群組的所有人員，便可以對於此共用信箱進行完整權限的存取，並且可以使用 IT 部門的名義來傳遞、轉寄或回覆 Email。

```
New-Mailbox -Shared -Name "IT Department" -DisplayName "資訊組" -Alias IT
| Set-Mailbox -GrantSendOnBehalfTo IT | Add-MailboxPermission -User SI
-AccessRights FullAccess -InheritanceType All
```

## 4.4 查詢信箱最近登入的時間

相信無論是在 Compliance 還是 Security 層面的管理需求，常會聽到 IT 人員在詢問如何得知所有人員或選定的人員，最近一次登入的時間以及所登入的 Exchange Server 是哪一台。如圖 4-5 所示便是一個典型的 PowerShell 命令查詢範例，其執行結果將會顯示所有人員信箱與共用信箱的最近一次登入時間，以及所登入的 Exchange Server，並且依照降冪排序方式來加以呈現。

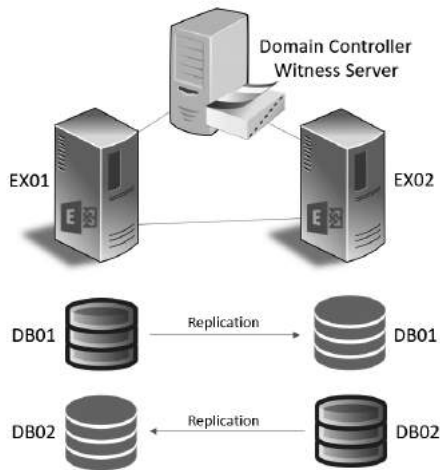
```
Get-Mailbox -ResultSize Unlimited -RecipientTypeDetails UserMailbox,
SharedMailbox | Get-MailboxStatistics | Sort-Object Lastlogontime
-Descending | Select-Object DisplayName,MailboxTypeDetail,LastLogonTime,Se
rverName
```



DisplayName	MailboxTypeDetail	LastLogonTime	ServerName
陳淑迪	UserMailbox	2019/9/11 下午 03:52:22	EX01
小麥	UserMailbox	2019/9/11 下午 03:48:16	EX01
蕭大猷	UserMailbox	2019/9/11 上午 10:53:12	EX01
Administrator	UserMailbox	2019/9/2 下午 04:49:33	EX01
HRAdmin	UserMailbox	2019/8/5 下午 02:26:49	EX01
資訊組信箱	SharedMailbox		EX01
林政德	UserMailbox		EX01
簡維信箱	UserMailbox		EX01

▲ 圖 4-5 查看最後登入時間

如圖 5-1 所示便是雙成員伺服器 DAG 架構的設計範例，其中我可以將位在 EX01 中的主要 DB01 信箱資料庫，設定複寫至 EX02 的 DB01 副本資料庫，針對 DB02 信箱資料庫的做法則為相反。必須特別注意的是無論您選擇 DAG 架構為何，除了必須在相同的 Active Directory 樹系之中之外，負責用來存放仲裁資料的見證主機也是必要的，在此我們直接使用網域控制站（DC）來充當這個角色。



▲ 圖 5-1 雙成員伺服器 DAG 架構

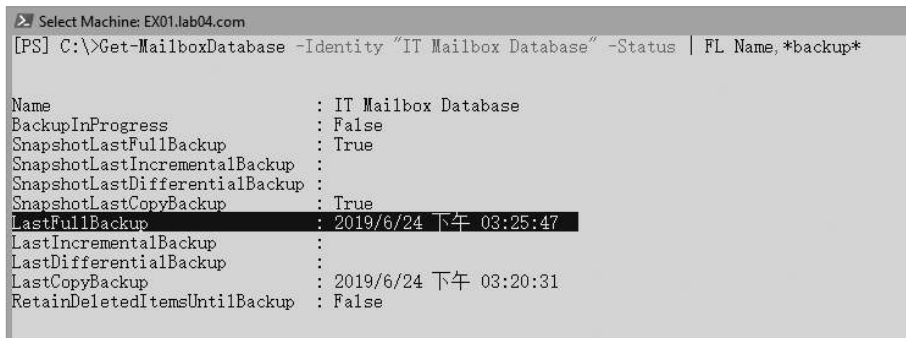
## 5.3 安裝第二台信箱伺服器

目前在筆者實驗室環境之中已經有一台名為 EX01 的 Exchange Server 2019 伺服器，部署在 LAB04 的 Active Directory 網域之中。接下來將準備部署第二台名為 EX02 的 Exchange Server 2019 伺服器於相同的網域之中。

在完成電腦名稱以及網卡 IP 位址的設定之後，請完成 Microsoft Visual C++ 2013 可轉發套件的下載與安裝。緊接著請開啟 Exchange Server

關於 Exchange Server 信箱資料庫是否有備份成功，除了可以從 Windows Server Backup 來查看相關記錄之外，也可以從 PowerShell 的連線或 EMS 命令介面之中，如圖 6-17 所示執行以下命令參數來取得 "LastFullBackup" 狀態資訊，即是此信箱資料庫最新一次完整備份的日期與時間。

```
Get-MailboxDatabase -Name "IT Mailbox Database" -Status | FL Name,*backup*
```



```
Select Machine: EX01.lab04.com
[PS] C:\>Get-MailboxDatabase -Identity "IT Mailbox Database" -Status | FL Name,*backup*

Name                : IT Mailbox Database
BackupInProgress    : False
SnapshotLastFullBackup : True
SnapshotLastIncrementalBackup :
SnapshotLastDifferentialBackup :
SnapshotLastCopyBackup : True
LastFullBackup      : 2019/6/24 下午 03:25:47
LastIncrementalBackup :
LastDifferentialBackup :
LastCopyBackup      : 2019/6/24 下午 03:20:31
RetainDeletedItemsUntilBackup : False
```

▲ 圖 6-17 查看最新完整備份記錄

請注意！當您在 Windows Server Backup 的進階設定中，沒有選擇採用 VSS Full Backup 配置時，在信箱資料庫的備份狀態資訊中，便只會顯示備份的日期與時間於 LastCopyBackup 欄位之中。

## 6.5 命令備份工具的使用

在前面的示範當中我們看到了使用 PowerShell 命令，來查看信箱資料庫的備份狀態。其實就連 Windows Server Backup 所有的操作管理，都是可以經由執行 PowerShell 命令參數來完成。首先您必須知道目前有哪些與 Windows Server Backup 相關的命令。請如圖 6-18 所示執行 Get-Command \*wb\* -commandtype cmdlet 命令參數便可以一目了然。



```

Machine: EK01.lab04.com
[PS] C:\>Get-Command *wb* -commandtype cmdlet

CommandType      Name                                     Version      Source
-----
Cmdlet           Add-WBBackupTarget                    1.0.0.0     WindowsServerBackup
Cmdlet           Add-WBbareMetalRecovery               1.0.0.0     WindowsServerBackup
Cmdlet           Add-WBFileSpec                        1.0.0.0     WindowsServerBackup
Cmdlet           Add-WBSystemState                     1.0.0.0     WindowsServerBackup
Cmdlet           Add-WBVirtualMachine                  1.0.0.0     WindowsServerBackup
Cmdlet           Add-WBVolume                           1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBBackupSet                       1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBBackupTarget                    1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBBackupVolumeBrowsePath          1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBbareMetalRecovery               1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBDisk                             1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBFileSpec                        1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBJob                             1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBPerformanceConfiguration       1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBPolicy                           1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBSchedule                         1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBSummary                          1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBSystemState                     1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBVirtualMachine                  1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBVolume                           1.0.0.0     WindowsServerBackup
Cmdlet           Get-WBvssBackupOption                 1.0.0.0     WindowsServerBackup

```

▲ 圖 6-18 查詢可用的備份命令

在得知了 Windows Server Backup 有哪些可用的命令之後，若想要知道某一個命令（例如：Add-WBBackupTarget）的完整使用說明，可以如圖 6-19 所示執行 `Get-Help Add-WBBackupTarget -full` 命令參數，如果只是要查看這個命令的使用範例，則可以執行 `Get-Help Add-WBBackupTarget -examples` 命令參數即可。

```

Machine: EK01.lab04.com
[PS] C:\>Get-Help Add-WBBackupTarget -full

Do you want to run Update-Help?
The Update-Help cmdlet downloads the most current Help files for Windows PowerShell modules, and installs them on your computer. For more information about the Update-Help cmdlet, see
https://go.microsoft.com/fwlink/?LinkId=210614.
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"):

NAME
    Add-WBBackupTarget

SYNOPSIS
    Adds a backup target to a backup policy.

SYNTAX
    Add-WBBackupTarget [-Policy] <WBPolicy> [-Target] <WBBackupTarget> [[-Force]] [<CommonParameters>]

DESCRIPTION
    The Add-WBBackupTarget cmdlet adds a WBBackupTarget object, which specifies backup storage locations, to a WBPolicy object that contains a backup policy. To use this cmdlet, you must first use the New-WBBackupTarget cmdlet to create a WBBackupTarget object. You can then use the Add-WBBackupTarget cmdlet to specify the storage location by using a disk, a volume, or a remote shared folder (network) location.

```

▲ 圖 6-19 查詢備份命令用法

## 9.2 Edge Transport 硬體需求

Exchange Server 2019 支援了與舊版 Exchange Server，在相同 Active Directory 的架構中共存運行，這些版本包括了 Exchange Server 2013 累計更新 21（CU21）以及 Exchange Server 2016 累計更新 11（CU11）或更新版本，並且也相容於其中現行的 Edge Transport Server 部署。

關於部署 Edge Transport Server 所採用的作業系統，必須是 Windows Server 2019 Standard 或 Datacenter 版本，並且可選擇安裝在 Server Core 或完整的桌面環境之中，而它所需要的硬體需求可參考表 9-1。

請注意！Edge Transport Server 不支援安裝與執行在 Nano 伺服器的運作模式下。

▼ 表 9-1 Edge Transport Server 硬體需求

元件	需求	附註
CPU	支援 Intel 64 與 AMD64 架構的處理器	不支援 Intel Itanium IA64 處理器
RAM	建議至少 64B 記憶體	Exchange 2019 支援最多 256GB 記憶體
分頁檔案大小	建議設定成已安裝記憶體大小的 25%，並將分頁檔案最小值和最大值設定成同樣大小。	無
磁碟空間	系統磁碟機至少剩下 200 MB 的可用空間。對於 Exchange 程式安裝的目標磁碟，請提供 30GB 以上的可用空間，對於包含訊息佇列資料庫的磁碟機則至少 500 MB 以上的可用空間。	無

元件	需求	附註
螢幕解析度	建議至少設定成 1024 x 768 以上像素	無
檔案系統	NTFS：建議將系統磁碟以及 Exchange 的二進位檔案、診斷記錄檔案、郵件佇列資料庫所需要使用到的磁碟分割區，採用此類型的檔案系統。 ReFS：適合用以存放 Exchange 信箱資料庫以及交易記錄檔案。	無

在網路和目錄伺服器需求部分可以參考表 9-2 說明。

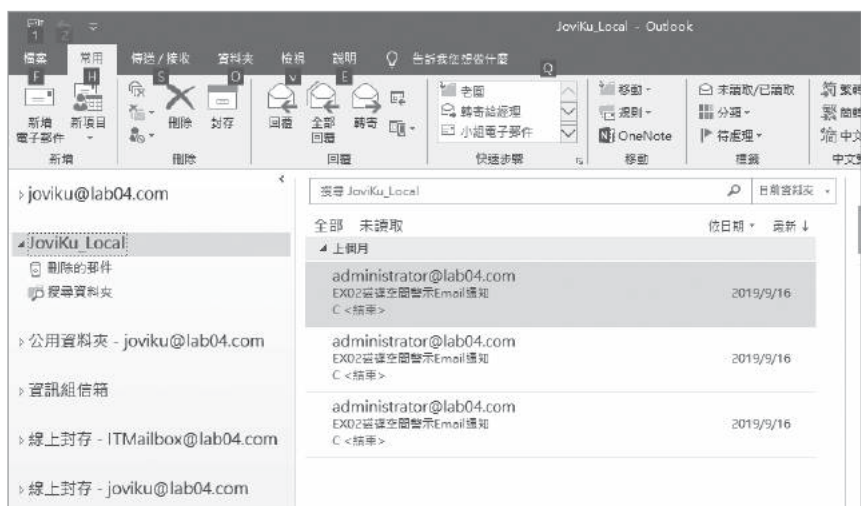
▼ 表 9-2 網路和目錄伺服器需求

元件	需求
網域控制站 (DC)	作業系統必須是 Windows Server 2012 R2 以上版本。
Active Directory 樹系	樹系功能層級必須至少是 Windows Server 2012 R2。
Active Directory 站台	站台中必須包含至少一個可寫入的網域控制站 (DC)，且同時也是全域類別伺服器 (GC)。
DNS 命名空間	支援了連續、不連續、單標籤網域以及斷續四種 DNS 命名空間。
IPv6	只有在現行網路支援 IPv4 與 IPv6，並且在 Exchange Server 的網路設定也已經啟用了 IPv4，才能支援 IPv6 的使用。



如果想要針對選定的組織單位人員，來批次啟用線上封存功能（例如：業務部），可以透過執行 `Get-User -Filter "Department -eq '業務部'" | Enable-Mailbox -Archive` 命令參數來一次完成設定。

完成了就地封存信箱的建立之後，用戶就可以在 Outlook 或 OWA 中看 [線上封存] 的信箱，對於想要封存的郵件可以隨時拖曳過去即可。在如圖 11-10 所示的範例中，則可以同時分別看到存放在本機的封存（JoviKu\_Local）、共用信箱的線上封存以及用戶自己的線上封存。



▲ 圖 11-10 Outlook 信箱

## 11.5 管理郵件保留原則

當在人員的主要信箱上又多了 一個線上封存信箱之後，除了可以讓用戶隨時將郵件拖曳至線上封存信箱來進行保存之外，也可透過管理員預先幫我們建立好的封存原則或保留標籤，像如圖 11-11 所示 樣來自由套用在選定的郵件或郵件資料夾設定中。