第 1 章
Windows Server 2016 舊系統升級實戰

每當 Microsoft 發行了新版本的 Windows Server 作業系統時，IT 部門就得開始思考是否有升級的必要性。根據筆者實際的採訪得知，絕大多數的企業 IT 單位，都會採取較保守的隔岸觀火策略，也就是即便有新功能的需求，也得先看看別人使用的情況，再來計劃未來的升級行程。

觀望固然是保險的作法，但若是觀望太久，等到幾個新版本接二連三發行之後，你才意識到有升級的必要性時，恐將讓你的企業付出可觀的 IT 成本。

1.1 簡介

如果你是一位 IT 部門的系統工程師，相信令你最害怕的工作之一就是各類「系統」的升級，尤其是會動到基礎架構的系統升級，更是會讓人覺得膽戰心驚，像是常見的作業系統就地升級、Active Directory 升級、虛擬化平台的升級以及叢集主機的升級等等。

一旦在升級或移轉的過程中處理不慎或不周全，所影響的層面肯定相當廣泛，重者造成與它有相互整合的應用服務執行失敗，輕者使得系統運行不穩定或某些功能無法正常執行。以 Microsoft 自家的產品來說，最常見的案例就是在 Active Directory 升級後，造成 Exchange Server 相關服務無法正常啟動。

為了避免上述的窘境發生在自己身上，多數負責的 IT 人員，都會選擇盡可能避開升級的計劃，只要不影響到現行應用程式或服務的正常運行，能夠不動刀就不要動，等到未來真有某個關鍵的應用程式或服務，非得相依在新版的系統中來運行時，再來進行評估也不遲啊！想想看像這樣的 IT 維運觀念是否正確呢？依照筆者多年的實務經驗，可以很肯定的告訴大家：「千萬別這麼做」。

在[功能]頁面中，基本上是不需要再勾選任何[功能]項目，除非你有其他管理功能的需求，可以在此頁面中一併加入安裝之中。點選[下一步]。在[確認安裝選項]的頁面中，可以檢視到即將安裝的網域服務以及所有與 Active Directory 相關的管理工具。

其中在管理工具部分，後續管理員也可以自行在其他的 Windows Server 2016 主機上，透過[功能]的新增再完成安裝，以利於遠端的連線管理需求。至於給予 Windows 10 的遠端伺服器管理工具，則可以到以下官方網站來下載安裝。點選[安裝]。

Windows 10 遠端伺服器管理工具：
https://www.microsoft.com/zh-TW/download/details.aspx?id=45520

完成上述的伺服器角色安裝之後，你可以直接在[結果]頁面中，點選[將此伺服器升級為網域控制站]的連結，或是後續再從如圖 10 所示的[伺服器管理員] 部署設定提示中來點選此連結。

圖 10　部署設定提示

如圖 11 所示，便是建立新網域控制站的設定精靈。首先在[部署設定]頁面中，請先選取[將網域控制站新增至現有網域]，在[網域]欄位中輸入現行的網域名稱，你可以決定是否要變更執行此操作的網域使用者，點選[下一步]。

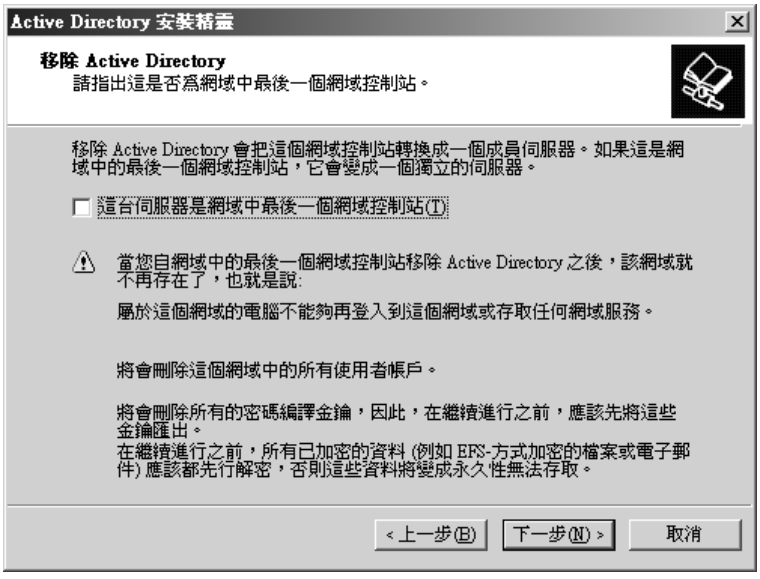

圖 25　網域控制站降級設定

1.5　升級移轉 DHCP 伺服器

DHCP Server 是目前 IT 網路中必要的基礎建設，對於許多中小企業來說，通常為了節省成本，會選擇將 DHCP Server 角色安裝在與網域控制站在同一部主機之中，在這種情境之下你就需要在舊網域控制站五大角色，初步完成移轉作業時，就一併完成移轉作業。

可是如果你的來源主機是 Windows Server 2003 R2，是無法依循接下來的操作說明來進行移轉，因為它最低的版本限制是 Window Server 2008，不過仍有替代的解決之道。先來看看標準的移轉方法。首先請如圖 26 所示在目的地的 Windows Server 2016 主機上，加裝[Windows Server 移轉工具]功能。

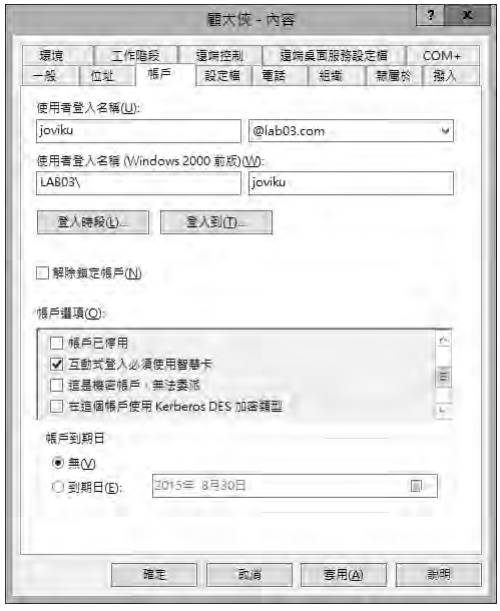

圖 28 網域帳戶設定

2.4 鎖定帳戶管理

當網域使用者登入時輸入多次的錯誤密碼，如果你是網域管理者，打算如何來管制他們呢？是任憑他們輸入幾次錯誤都沒有關係，直到輸入正確即可，還是要強制限制密碼嘗試輸入的次數，一旦超過指定的錯誤次數即進行鎖定。

基本上如果網域使用者的帳戶，只使用在內部網路電腦的登入驗證，在沒有設限嘗試次數的狀態下，可能會造成的危害相當有限。但是如果是開放了從遠端進行各種的連線服務，像是 VPN、WiFi、SMTP 以及 POP3 等等，這時候人員帳戶的安全性就可能隨時亮起紅燈了，因為只要透過最簡單的暴力式字典攻擊法，就可以輕鬆破解任一人員的帳號密碼，取得該人員所有能夠獲取得到的公司檔案資料。

Active Directory 人員帳戶自動鎖定的功能，最好能夠搭配一項名為[不要顯示上次登入的使用者名稱]的原則設定，如圖 29 所示此原則的啟用，能夠確保這一些受管制的網域電腦，在每一次開機的登入畫面之中，不會顯示最近登入的使用者名稱，以及其他曾經登入過的使用者名稱，包括了本機帳戶與網域帳戶登入記錄顯示。

圖 29　不要顯示上次登入的使用者名稱

如圖 30 所示便是一部已被套用[不要顯示上次登入的使用者名稱]原則設定的 Windows 10 登入畫面，使用者不會再像過去一樣，從左下方直接看到曾經登入的使用者名單，進而讓惡意人士有機可乘。

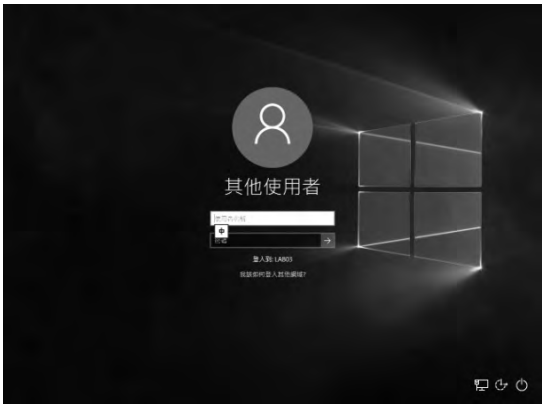

圖 30　成功套用登入原則設定

解決人員 Windows 10 電腦登入名單可能外洩的問題之後，就可以來進一步設定帳戶鎖定原則。請如圖 31 所示在開啟[群組原則管理編輯器]介面之後，展開至[電腦設定]\[原則]\[Windows 設定]\[安全性設定]\[帳戶鎖定原則]節點頁面，便可以看到三大原則項目，分別是重設帳戶鎖定計數器的時間間隔、帳戶鎖定時間、帳戶鎖定閥值。

其中後兩者的磁碟區類型是唯一具備容錯功能的選項，鏡像磁碟區需要兩個磁碟機，而 RAID-5 磁碟區則需要至少三個磁碟機，並且這一些磁碟的規格最好都能夠一樣，以避免某一些較大容量的磁碟機，浪費掉許多不必要的空間。在此我們以點選[新增 RAID-5 磁碟區]為例繼續。

圖 1 磁碟管理

在如圖 2 所示的[選取磁碟]頁面中，請將左方窗格之中所有可用的磁碟機，一一新增至右方選取的窗格之中。這時候磁碟區大小總計的結果便會立即出現。在此由於 RAID 5 的總容量計算方式是 n-1，因此範例中的三顆 20GB 的磁碟機，便是有大約 40GB（60GB-20GB）的可用空間。點選[下一步]繼續。

圖 2 新增 RAID-5 磁碟區

只是無論選擇部署在私有雲還是公有雲之中，所謂的雲端作業平台（Cloud OS）至少必須具備以下特性：

- 低耗能、可用資源最大化
- 可部署在虛擬化或實體的主機之中
- 主體就可作為虛擬化平台，包括了 Virtual Machine、Containers
- 支援軟體定義網路（SDN）、軟體定義儲存（SDS）
- 內建各類高可用性、高可靠度、高延展能力的安全機制

上述 Cloud OS 所需具備的特性，在全新的 Windows Server 2016 中皆已俱全，其中若想要達到低耗能與可用資源最大化的極致，採用以新推出的 Nano Server 來作為基礎平台絕對是不二的選擇，原因為何呢？很簡單！它只給你需要的，其餘通通拿掉，至於精簡到甚麼程度呢？

首先它比過去 Windows Server 2008/R2 以及 Windows Server 2012/R2 時期的 Server Core 更精簡，除了各項內建程式、元件以及服務大幅簡化之外，在主機端的 Console 介面上僅提供純文字的操作，就好像一個純文字介面的 Linux 作業系統一樣，可是它卻能夠提供許多企業級的伺服器角色與功能，包括了 Hyper-V 主機、容錯移轉叢集、儲存管理主機、Scale-Out File Server、DNS Server、IIS、應用程式伺服器等等。

針對極致精簡的 Nano Server 設計，在基礎的運作上主要帶來了以下效益：

- 讓需要安裝的重大更新、安全更新的次數減少許多，這意味著需要重新啟動系統的次數也隨之降低。
- 開機需要載入的驅動程式、服務以及需要開啟的連接埠口減少了，這表示可能遭受惡意攻擊的面縮小了，讓安全性將大幅提升。
- 由於精簡因而讓可用的硬體資源增加了，讓耗能相對減少了。
- 由於輕巧因而讓 IT 人員從部署、管理到維護的時間都大幅縮短了。舉例來說，若以部署單一部 Nano Server 的虛擬機器來說，過去的 Server Core 所需要的虛擬硬碟檔案大小，大約是 6.3GB。如今 Nano Server 僅需要 0.41GB。

4.2 部署 Nano Server 的注意事項

做為一個擁有最低成本效益以及最高敏捷度的 Nano Server 來說，在設計上它完全不同於過去的 Server Core 以及完整桌面體驗的 Windows Server，因此有以下幾個特性需要 IT 管理人員特別注意的：

- 沒有提供本機的登入功能以及圖形操作介面，僅有一個簡易的[Nano Server Recovery Console]功能，來管理最基本的網路設定與開關機功能等等。
- 唯一支援運行 64 位元的應用程式、工具以及代理程式。
- Nano Server 無法做為 Active Directory 網域控制站，僅能夠加入成為網域的成員主機。
- 不支援群組原則（Group Policy）的管理。
- 你無法設定 Nano Server 透過 Proxy Server 來連接 Internet。
- 不支援 NIC Teaming 功能的使用，特別是容錯負載平衡或 LBFO 機制。改由支援 Switch-embedded teaming （SET）來取而代之。
- 不支援 System Center Configuration Manager 與 System Center Data Protection Manager 的整合管理。
- 在 Windows PowerShell 的使用上也有一些限制，關於這部分我們留在後面再來詳加說明。

4.3 開始安裝 Nano Server

接下來筆者要示範的是如何安裝一部 Nano Server，在現行 Windows Server 2016 的 Hyper-V 虛擬化平台上來運行。由於需要產生 Nano Server 的虛擬硬碟檔案，在此我們以在 Windows 10 的作業環境中來完成這些步驟。如圖 1 所示，首先請在你準備好的 Windows Server 2016 安裝映像檔上，按下滑鼠右鍵點選[掛接]繼續。

圖 34　服務管理員

接下來我們可以從[工作管理員]來開啟如圖 35 所示的[資源監視器]，在[網路]的頁面中，便可以看到目前 GatewayService.exe 程式的網路連線情形，這表示此閘道主機與 Azure 上的伺服器管理工具，在網路通訊上應該是沒有問題了！

圖 35　資源監視器

如果你想要安裝 IIS 伺服器角色，在現有的 Nano Server 離線虛擬硬碟檔案（vhd 或 vhdx）之中，也就是在 Nano Server 虛擬機器關機的狀態下，便需要透過 Dism 命令來掛接相關虛擬硬碟檔案，再經由 Add-Package 參數選項，來完成 IIS 伺服器角色套件的新增即可。請參考以下命令範例。

```
mkdir mount
dism.exe /Mount-Image /ImageFile:.\NanoServer01.vhd /Index:1 /MountDir:
.\mount
dism.exe /Add-Package /PackagePath:.\packages\Microsoft-NanoServer-IIS-
Package.cab /Image:.\mount
dism.exe /Add-Package /PackagePath:.\packages\zh-tw\Microsoft-NanoServer
-IIS-Package_zh-tw.cab /Image:.\mount
dism.exe /Unmount-Image /MountDir:.\Mount /Commit
```

如果你的 Nano Server 已經在線上使用了，若還想要加裝 IIS 伺服器角色，就得先建立如圖 39 所示的以下回應檔（unattend.xml）範例，再透過 Dism 命令來完成指定線上安裝即可。

關於此回應檔的內容設定，必須與你準備安裝的套件語系相互匹配才可以。舉例來說，如果要安裝的是繁體中文版，則相關語系的設定會是 zh-tw。如果是英文版本則是 en-us。這包括了其中的套件路徑也可能需要一併修改的，否則後續的執行將會發生找不到套件的相關錯誤訊息。

```
<?xml version="1.0" encoding="utf-8"?>
    <unattend xmlns="urn:schemas-microsoft-com:unattend">
    <servicing>
        <package action="install">
            <assemblyIdentity name="Microsoft-NanoServer-IIS-Package"
version="10.0.14393.0" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" />
            <source location="c:\packages\Microsoft-NanoServer-IIS-
Package.cab" />
        </package>
        <package action="install">
            <assemblyIdentity name="Microsoft-NanoServer-IIS-Package"
version="10.0.14393.0" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="zh-TW" />
            <source location="c:\packages\zh-tw\Microsoft-NanoServer-
IIS-Package_zh-tw.cab" />
        </package>
    </servicing>
    <cpi:offlineImage cpi:source="" xmlns:cpi="urn:schemas-microsoft-
com:cpi" />
</unattend>
```

緊接著在如圖 16 所示的[系統準備工具]頁面中，請在[系統清理動作]的欄位中選取[進入系統安全新體驗 OOBE]，以及勾選[一般化]選項。在[關機選項]部分請選取[關機]。點選[確定]。執行此工具的主要目的，在於移除所有的系統特定資訊，包括電腦安全性識別碼（SID）。

圖 16 系統準備工具

完成了客體作業系統的系統準備作業之後，請在選取此虛擬機器之後按下滑鼠右鍵點選[匯出]。在如圖 17 所示的[匯出虛擬機器]頁面中，請選擇一個專門用以存放虛擬機器範本的資料夾。點選[匯出]。

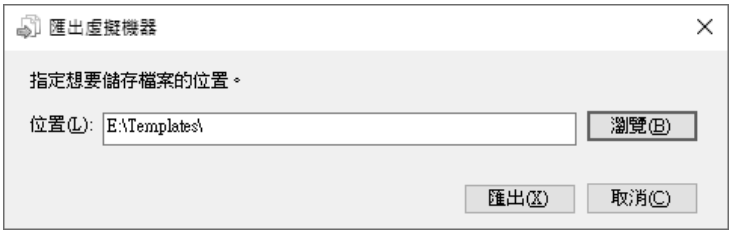

圖 17 匯出虛擬機器

成功匯出了我們所建立的虛擬機器範本之後，你就可以複製這個範本的虛擬硬碟檔案（*.vhd 或*.vhdx），分別存至新的虛擬機器存放路徑之中，例如 D:\VMs 路徑下的 VM1、VM2、VM3..等等。完成複製之後，就可以透過 PowerShell 或圖形管理介面中的[新增虛擬機器]精靈，如圖 18 所示選取[使用現有的虛擬硬碟]，挑選剛剛複製好的相對虛擬硬碟。

緊接著將會出現如圖 22 所示的[套用檢查點]提示訊息，告知我們將遺失虛擬機器的目前狀態。在此如果你非常確定現行運作中的狀態已不保留，可以直接點選[套用]即可，否則請點選[建立檢查點並套用]。此外，值得注意的是在這個右鍵選單中，還可以針對這個快照的虛擬機器，執行匯出、重新命名、刪除檢查點以及刪除檢查點樹狀子目錄等動作。

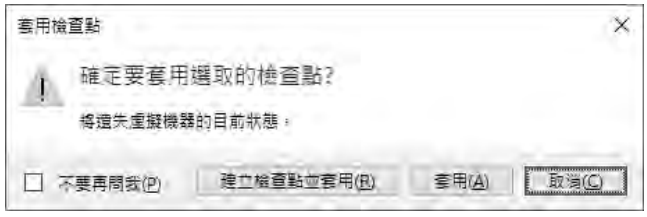

圖 22　套用檢查點

當虛擬機器的檢查點數量很多時，也會占用掉許多寶貴的硬碟空間，因此建議你最好隨時檢視一下，現行每一個虛擬機器的檢查點資訊，動手刪除一些已經不再需要保留的檢查點。現在就讓我們來學習一下，使用 PowerShell 命令管理檢查點的技巧。

首先假設我們想知道 WS2016 這個虛擬機器的檢查點資訊，只要如圖 23 所示執行 Get-VMSnapshot -VMName WS2016 命令即可。進一步，如果想要刪除在這個虛擬機器之中，所有以 WS2016 為前置字元的檢查點，只要執行 Get-VM WS2016 | Remove-VMSnapshot -Name WS2016*命令即可迅速完成。完成刪除之後可以再次進行結果查詢。

針對擁有較多檢查點的虛擬機器而言，你還可以使用更有效率的刪除方式，例如以下命令範例就是可刪除在 WS2016 虛擬機器之中，所有超過 180 天的檢查點。

```
Get-VMSnapshot -VMName WS2016 | Where-Object {$_.CreationTime -lt （Get-Date）.AddDays（-180） } | Remove-VMSnapshot
```

至於如何以 PowerShell 命令來還原虛擬機器中特定的檢查點呢？可參考以下命令範例，它便是還原了在 WS2016 虛擬機器中，一個名為'BeforeOSUpdates'的檢查點。

```
Restore-VMSnapshot -Name 'BeforeOSUpdates' -VMName WS2016
```