

## 作者序

由 OpenAI 開發的人工智慧聊天機器人 ChatGPT，從 2022 年 11 月推出以來已經席捲了整個 IT 世界，也成為了老少皆知的熱門話題。除了 ChatGPT 之外 Bing Chat 也成為了現今最火熱的聊天機器人。筆者和許多人一樣不斷嘗試與這些聊天機器人進行各種議題的交談。交談的過程中發現聊天機器人幾乎是有問必答，而給予的答案也大多是正確且通順的。

接下來有關 AI 聊天機器人的應用，業界已經有許多軟體公司開始著手發展針對在企業 IT 網路中的應用，像是建立一個 AI 聊天入口，來回答所有員工有關公司法規、人力資源、客戶管理、研發製造等等的問題，甚至於幫員工製作所需要的簡報、企劃案、電子表單、簽核流程、多媒體等草稿，來提升協同合作與專案任務的執行效率。

想要讓 AI 聊天機器人運用在企業 IT 環境之中並非難事，因為後續會有更多這方面的 API 會來提供給軟體研發的人員，透過與現行應用系統與資料庫服務的整合，來完成各種我們希望能快速達成的 IT 任務。不過請記住這一些應用的背後需要有一個龐大的資料中心。

資料中心是企業 IT 運行的核心，尤其是在未來與 AI 整合的環境之中。因此我們必須建立一個極具完善的資料中心，這個資料中心可以是來自於各個應用系統的整合結果，但它必須是穩固、安全、可靠、流暢以及持續不間斷運行，而這一切的基礎便是來自於私有雲或混合雲的虛擬化平台架構。

無論是私有雲或混合雲的部署，現今最佳的選擇就是 VMware vSphere 8，因為它提供了最佳的工作負載管理機制，讓運行於每一個虛擬機器中的應用系統與服務，能夠在持續不間斷的運行之下獲得最好的效能表現。對於 IT 管理員而言，則提供了一致性的友善操作管理介面，以及可因應各類批量與自動化管理需要的工具。

究竟 VMware vSphere 8 有哪一些優點值得我們 IT 人來發掘與學習呢？請立刻翻閱此書並且動手實戰演練吧！

顧武雄 JoviKu  
2023.09

# 04

## chapter

# vSphere Client 單一登入 與虛擬機器管理

對於中大型的組織而言，由於整體的 IT 營運相當依賴虛擬機器的使用，因此虛擬機器增加的速度往往也相當驚人。為此除了需要有更多的管理人員來分擔協助之外，懂得善用平台的工具與使用技巧也是相當重要的。今日就讓我們先解決 vSphere 帳號單一登入與權限管理的問題，再來搞定幾項 IT 人員在平日的維運中，一定要學會的虛擬機器管理技巧。



## 4.1 簡介

當企業營運中的 IT 應用需求越來越多時，在私有雲的虛擬化架構中的平台主機與虛擬機器數量，相對也需要不斷擴增才能因應各種應用系統的部署。以一個跨國多點營運的企業來說，首先勢必需要有多位的系統管理員，分散在各個分支據點來協助維運工作。

接著為了簡化多套系統帳號與密碼的管理，便必須藉由單一登入 (Single Sign-On) 的整合技術，來解決帳號與密碼集中控管的問題，以及大量用戶需要記憶多組帳號與密碼的困擾。相信許多 IT 人員都有這樣的經驗，那就是每當某個系統的密碼有效期限到來時，隔天就會陸續有許多使用者打電話進來，表示無法連線登入系統的問題，這時候 IT 人員就必須協助該用戶重置密碼設定。

在 VMware vSphere 的架構之中，vCenter Server 本身就提供了 Single Sign-On 網域的功能，因此能夠讓網域帳號管理所有與 vCenter Server 所連接的 ESXi 主機。不過這並無法滿足 IT 人員的管理需求，因為在實際運行的網路環境之中，管理員往往會希望使用現行的 Active Directory 或 Open LDAP 的帳號，來直接登入與管理 vSphere 的整體架構，而非再記憶一組新的管理員帳密。還好 vCenter Server 也早已內建了相關整合功能，可解決這一項令許多 IT 部門困擾的帳密管理問題。

緊接著您可能還必須學會如何在最新版本的 vSphere Client 中，善用內建的功能來妥善做好虛擬機器的管理以及資源的分配，以因應未來更多應用系統與服務的建置需要，這一些包含了虛擬機器範本的管理與應用、虛擬機器的複製、快照管理、資源集區配置、熱新增 CPU 與 RAM。接下來就讓筆者來一一實戰講解這一些管理祕訣吧！

## 4.2 Active Directory 單一登入配置

在以 Windows 解決方案為主的網路環境之中，相信 Active Directory 網域肯定是最常見的 IT 基礎建設，也因此讓許多第三方的應用系統都支援與它的整合，這包括了 ESXi 8.0 與 vCenter Server 8.0。筆者曾經介紹

過有關 ESXi 8.0 與 Active Directory 的整合配置，接下來讓我們來學一下 vCenter Server 8.0 與 Active Directory 的整合配置，包括了您可能會遭遇的問題。

首先請點選至[系統管理]\[Single Sign-On]\[組態]節點，然後再到[身分識別提供者]\[ Active Directory 網域]頁面中，如圖 4-1 點選[加入 AD]超連結繼續。



圖 4-1 單一登入組態管理

在如圖 4-2 的[加入 Active Directory 網域]頁面中，請依序輸入所要連接的網域、組織單位(選用)、使用者名稱以及密碼。其中網域與使用者名稱的輸入必須注意一下格式，以本範例而言網域不能夠只輸入 adlab02，使用者名稱也不能只輸入 Administrator。完成輸入之後點選[加入]。

#### 小提示



目前僅支援將 vCenter Server 加入至具有可寫入網域控制站的 Active Directory 網域，選擇加入唯讀網域控制站(RODC)的 Active Directory 網域則是不支援的。



圖 4-2 加入 Active Directory 網域

確認成功加入 Active Directory 之後，系統將會提示您將節點重新開機以套用變更，而這裡所指的 "節點" 就是 vCenter Server。在我們重新開機之前，您可以先在網域控制站(DC)的主機之中，開啟如圖 4-3 的[Active Directory Users and Computers]管理介面，便可以在[Computers]的頁面中查看到剛剛加入的 vCenter Server 主機，已成為了網域電腦的成員之一。

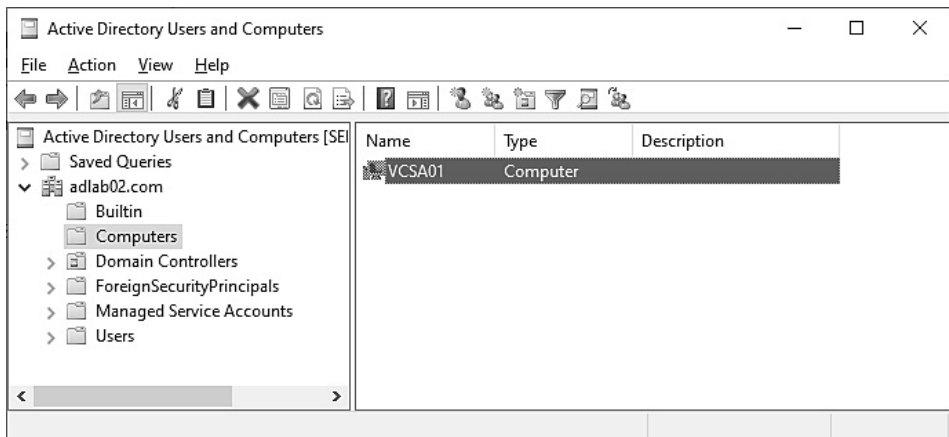


圖 4-3 Active Directory 使用者和電腦管理工具

接下來請登入 vCenter Server 管理網站。如圖 4-4 您將可以在頁面上方的[動作]選單中點選[重新開機]。請注意！在尚未完成重新開機之前，vSphere Client 網站將無法使用。成功完成重新開機之後，建議您最好再次回到 vCenter Server 管理網站的[摘要]頁面中，查看[健全狀況狀態]中的所有資源狀態是否都在正常運行中。



圖 4-4 vCenter Server 動作選單

完成了 vCenter Server 的重新開機之後，請點選至[系統管理]\[Single Sign-On]\[組態]節點，然後再到[身分識別提供者]\[身分識別來源]頁面中點選[新增]超連結。在[新增身分識別來源]頁面中，請選擇[Active Directory(整合式 Windows 驗證)]來做為身分識別來源類型，網域名稱則必須輸入前面步驟中所加入的網域。點選[新增]。如圖 4-5 便可以查看到剛新增的一筆 Active Directory 身分識別來源設定。

必須注意的是即便您在前面的步驟之中，已經完成了加入 Active Directory 網域的設定，若 Active Directory 網域與現行的 vSphere Single Sign-On 網域名稱相同，則在新增身分識別來源的過程中，將會出現 "無法設定身分識別來源" 的錯誤而無法繼續。



圖 4-5 身分識別來源管理

接下來我們只要再完成有關 Active Directory 人員帳號的授權設定，就可以使用 Active Directory 人員帳號的登入，來管理整個 vSphere 的運行。首先請點選至[系統管理]\[Single Sign On]\[使用者和群組]節點，然後在[使用者]的子頁面中，便可以在選擇 Active Directory 網域之後，如圖 4-6 查看到所有 Active Directory 的帳號清單，包含了電腦帳號。

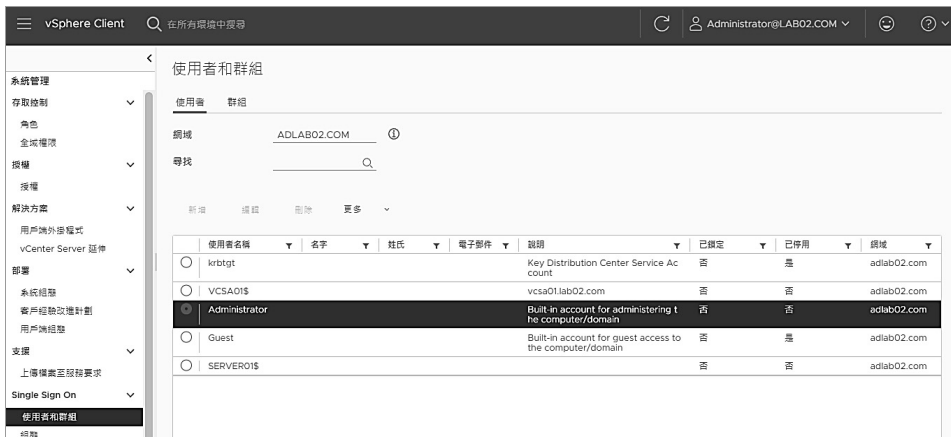


圖 4-6 使用者和群組

緊接著在[群組]的子頁面中，預設則可以查看到 vSphere SSO 網域中的所有群組清單。請在選取[Administrators]群組之後點選[編輯]超連結，然後在如圖 4-7 的[編輯群組]頁面中，先在[新增成員]欄位中選擇 Active Directory 的網域，再透過關鍵字輸入找到所有要加入此群組的帳號。一旦完成了將 Active Directory 的人員帳號，加入到 vSphere SSO

網域的 Administrators 群組之後，這一些人員便擁有了管理 vSphere 的最高權限。

編輯群組

群組名稱 \* Administrators

說明

新增成員 \* ADLAB02.COM

搜尋

- Administrator X
- vsphere-ui-c683454f-53b3-4bdb-bcc6-f64915671a06 X
- vsphere-ui-edda868b-225c-44bf-a1f0-0c12e23eab09 X
- Administrator X

Administrator@adlab02.com

圖 4-7 編輯群組

接下來筆者使用一台已經在開機時就登入 Active Directory 的 Windows 電腦，此時若開啟網頁瀏覽器來連線 vSphere Client 網站，便可以在完成 VMware 增強行插件的下載與安裝之後，直接在如圖 4-8 的登入頁面中勾選[使用 Windows 工作階段驗證]設定來完成登入，而不需要再輸入帳號與密碼。

VMware® vSphere

example@domain.local

密碼

使用 Windows 工作階段驗證

登入

圖 4-8 登入 vSphere Client



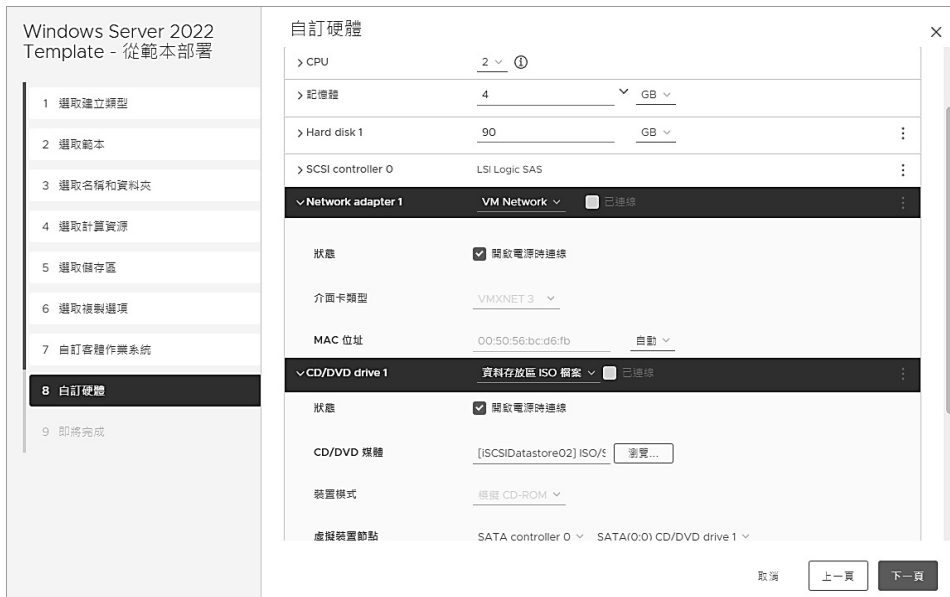


圖 4-26 自訂硬體

## 4.6 複製虛擬機器

關於虛擬機器的快速建立方法，除了可使用預先建立好的範本與規格來完成之外，也選擇直接複製現有的虛擬機器，不過若採用這種做法，您可能還需要自行修改客體作業系統的電腦名稱、IP 位址以及重置 SID 等操作。針對虛擬機器的複製功能的運用，您可能也會聯想到使用在測試用途，如此可以省去重複建立虛擬機器的時間。

具體如何快速複製一個虛擬機器，讓我們看看接下來的操作說明。請在 vSphere Client 網站中如圖 4-27 針對所要複製的虛擬機器，點選位在 [動作] 選單下的 [複製] \ [複製到虛擬機器] 繼續。

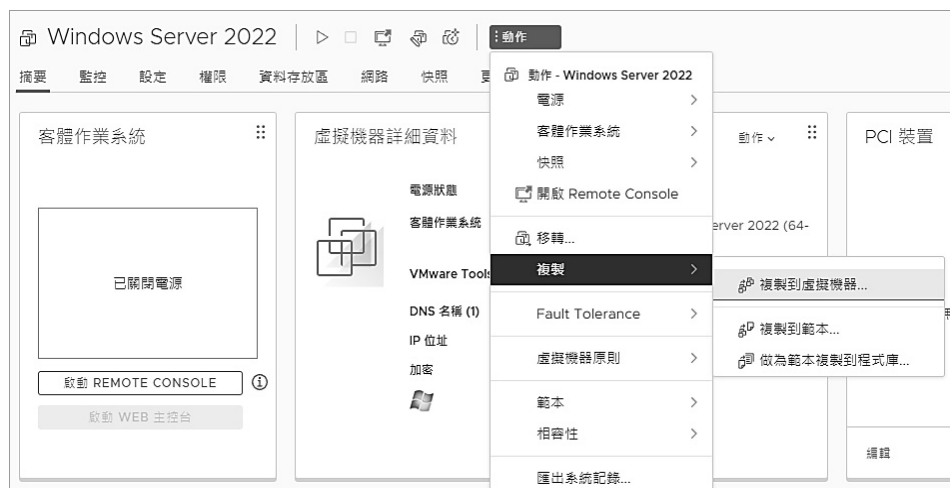


圖 4-27 虛擬機器動作選單

在的[選取儲存區]頁面中，請選取新虛擬機器檔案要存放的儲存區，若發現所選取的儲存區空間不足時，將會出現錯誤訊息而無法繼續。此外您還可以進一步針對每一個虛擬磁碟檔案設定對應的儲存區，以及可以修改虛擬磁碟格式而不必與來源虛擬機器相同。點選[下一頁]。

在如圖 4-28 的[選取計算資源]頁面中，若叢集已經啟用了 DRS 全自動化功能，您將可以透過叢集的選取，由系統自動決定負責運行的 ESXi 叢集主機，否則便需要手動選擇運行的 ESXi 主機。在此範例當中可以發現筆者所選取的 ESXi 主機，出現了有關 CD/DVD 已掛載某一個 ISO 映像的警示訊息，此類訊息是可以暫時忽略，待後續步驟中來調整設定即可。點選[下一頁]。

在如圖 4-29 的[選取儲存區]頁面中，請選取新虛擬機器檔案要存放的儲存區，若發現所選取的儲存區空間不足時，將會出現錯誤訊息而無法繼續。此外您還可以進一步針對每一個虛擬磁碟檔案設定對應的儲存區，以及可以修改虛擬磁碟格式而不必與來源虛擬機器相同，例如您可以選擇[精簡佈建]格式來因應儲存空間可能不足的問題。點選[下一頁]。



圖 4-28 選取計算資源



圖 4-29 選取儲存區

在[選取複製選項]頁面中，可以決定是否要勾選自訂作業系統、自訂此虛擬機器的硬體、建立之後開啟虛擬機器電源，在此筆者以勾選[自訂此虛擬機器的硬體]為例。點選[下一頁]。

如圖 4-30 在[自訂硬體]的[虛擬硬體]頁面之中，我們便可以修改其中的[CD/DVD drive1]的設定，以解決前面步驟中有關於選取計算資源時的警示訊息。點選[下一頁]。最後在[即將完成]的頁面中確認上述步驟設定皆無誤之後，點選[完成]。接下來便可以開始使用新複製的虛擬機器，來運行所需要的應用系統與服務。



圖 4-30 自訂硬體

## 4.7 快照虛擬機器

當有虛擬機器的 Guest OS 或應用系統需要升級時，除了要在事前做好虛擬機器的完整備份之外，通常還會建議在正式執行的一刻先進行快照，主要目的在於萬一遭遇更新任務失敗之時，能夠在第一時間迅速完成復原，這也是採用實體主機所無法享有的優勢之一。

儘管虛擬機器的快照功能如此方便與快速，但卻萬萬不可讓它與傳統的備份方式混為一談，因為快照所產生的檔案與主要虛擬機器的檔案是有相依關係的，一旦需要進行快照刪除時，便有合併處理的作業需要完成。

如圖 4-31 便是在 vSphere Client 網站上針對選定的虛擬機器，便可以在[動作][快照]選單中看到所有與快照相關的功能，包括了拍攝快照、管理快照、復原為最新快照、合併、刪除所有快照，其中對於新快照的建立請點選[拍攝快照]繼續。



圖 4-31 虛擬機器快照選單

在如圖 4-32 的[建立快照]頁面中，只要輸入新快照名稱、說明以及決定是否要勾選[包含虛擬機器的記憶體]、[靜止客體檔案系統]即可。其中[說明]欄位雖然是非必要欄位，但筆者建議您最好能夠完整描述，以利於往後大量快照時的識別管理。至於若要使用[靜止客體檔案系統]的快照功能，除了需要已完成 VMware Tools 的安裝，客體作業系統本身也需要支援此功能。點選[建立]。

#### 關於快照的使用限制


- 已開啟電源且具有獨立磁碟的虛擬機器，將無法使用記憶體快照功能
- 快照功能不支援採用匯流排共用設定的虛擬機器

## 4.9 熱新增 CPU 與 RAM

雖然說大多數的虛擬機器在運行一段時間之後，即便有擴增 CPU 或 RAM 的必要需求，也都可以安排在離峰時間完成正常停機之後，再來調整 CPU 或 RAM 的大小配置。但是相信仍然會有一些必須二十四小時持續運行的應用系統，必須在不停機的狀態下來添加 CPU 或 RAM。

在這種情境下只要虛擬機器滿足以下條件，並且 Guest OS 本身支援 CPU 或 RAM 的熱新增功能，便能夠添加現行主機中可用的 CPU 或 RAM 資源至虛擬機器的配置中，並且可讓 Guest OS 與運行中的任何應用系統以及服務，立刻使用剛才在線上所添加的資源。

- 虛擬機器硬體採用 7 或更高的版本
- 已完成 VMware Tools 的安裝
- 此虛擬機器必須尚未啟用 FT(Fault Tolerance)功能
- 必須使用 vSphere Advanced、Enterprise 或 Enterprise Plus 的合法授權

**小提示**  在 Windows 的世界中只要是 Windows Server 2012 以上的版本，無論是 Standard 或 Datacenter 授權版本，皆是支援 CPU 與 RAM 的熱新增功能。

在虛擬機器滿足了上述的條件之後，接下來就讓我們實際來為 vSphere 8.0 架構下的虛擬機器，啟用一下有關於 CPU 與 RAM 的熱新增功能。

首先請開啟虛擬機器的[編輯設定]頁面。接著請點選至[虛擬機器選項]的子頁面。如圖 4-39 便可以在展開[CPU 拓樸]設定之後，便可以將位在[CPU 熱插拔]的[啟用 CPU 熱新增]功能勾選。



圖 4-39 CPU 拓模設定

接下來是記憶體の設定部分。請切換至[虛擬硬體]的頁面中，如圖 4-40 在此便可以將位在[記憶體熱插拔]中的[啟用]勾選即可。點選[確定]。

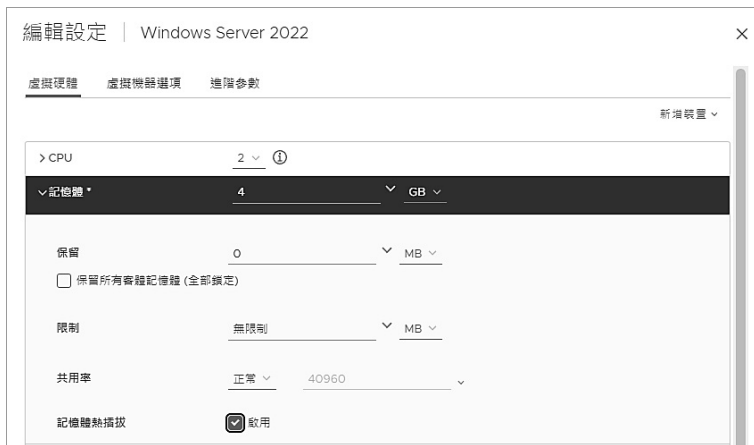


圖 4-40 記憶體配置

**小提示** 針對記憶體熱新增的大小上限，是現行的記憶體 x16 即是上限。舉例來說，如果現行的記憶體是 4GB 則最高上限便是 64GB。此外，現行的記憶體大小不可以是 3GB 或更小。



## ● 本章結語 ●

企業選擇全面部署私有雲架構方案，無非是要解決三大重點，分別是降低 IT 總體擁有成本(TCO)、簡化 IT 管理複雜度、提升應用程式與服務可靠度，然而想要真正做好企業私有雲的維運任務談何容易，還必須滿足三大基本要素才行，分別是選擇強大功能的虛擬化平台、內建完整且友善的工具、學習正確的管理方法。上述中的前兩項要素 VMware vSphere 8 已經辦到，接下來所需要的僅是 IT 人員去學習如何正確的使用它。

本章所講解的實戰內容看似簡單易懂但卻也是相當實用，未來無論面對如何更加複雜的管理需求，同樣可以有相對的進階管理技巧來因應，例如搭配 PowerCLI、ESXCLI、Script...等的自動化管理方案。請繼續閱讀其他章節內容，來學會更多實用的管理技巧。