

序

儘管 VMware vSphere 7.0 已經發行，但如今以實體主機為主的資訊環境仍有不少。筆者近期就曾經拜訪過營業規模不小，且頗有知名度的一家企業。正準備為這家公司導入一套先進的 HR 管理系統，結果竟發現在這家公司的資訊環境中，所有伺服端的應用系統皆是運行在獨立的實體主機。後來在會議中深入了解之後，發現資訊部門的人員並非不知道有虛擬化平台，而是不知道它能夠帶來什麼樣顯著的效益，還是覺得繼續使用傳統實體主機架構比較安心。

類似的情況，筆者還真遇過不少，其中大多數的情況都是資訊部門對於虛擬化平台技術的一知半解，以至於不知道若轉換成虛擬化平台的運行架構，能夠為現行的用戶、資訊部門以及公司帶來什麼好處。面對這種情況，以資訊服務廠商的角度來說，就必須在專案會議之中簡單扼要的說明幾項重點，包括了像是熱備援機制、快速備份與還原、簡化 IT 管理、降低維護成本…等等。

上述所提到的幾項關於虛擬化平台的重點效益，對於已經熟悉這項技術應用的 IT 人士來說似乎是老掉牙的概念了，但對於一些還沒有實際導入的用戶來說，如果能夠讓他們感受到現行實體架構的痛點，且明白到虛擬化架構相對的解決方案與效益，相信從此刻開始便是協助它們踏入私有雲部署的第一步。這個第一步對於資訊服務廠商而言也相當重要，因為它也同時降低了遠端故障排除時的風險。

想想看在這世界上有哪一些 IT 任務的執行，可以同時利人、利己又利群生的呢？其實只要做到能為公司營運帶來效益，接著還夠同時解決客戶、廠商以及合作夥伴的問題，最後又能夠因節能減碳來延續地球的生命，相信這就是最好的 IT 解決方案，而在現今虛擬化平台解決方案中，能夠做到最完善的就 VMWare，不僅如此它已是全球企業、政府單位以及非營利組織的首選。

最後祝福每一位 IT 先進，能夠從本書之中獲得美好的學習經驗！

顧武雄 Jovi Ku

第 1 章

VMware vSphere 7.0 全面 火速部署實戰

一個強大的雲端平台不僅在功能面的提供要完整，對於部署與管理的設計還得做到簡單與友善，如此才能受到廣泛 IT 人員的青睞。全新 VMware vSphere 7.0 完全滿足了這項需求，它所提供的基礎元件 vCenter Server 與 ESXi，不僅易於部署與管理，更有完善的諸多功能可以確保虛擬機器與應用程式，獲得更安全的保護以及更流暢的執行效能，且不間斷的持續運行。本章將引領讀者一同來學習如何從零開始，完整部署 vCenter Server 與 ESXi 主機的基礎架構，讓後續虛擬機器與應用程式的運行更快、更安穩。

小提示 如果你需要在 Guest OS 操作中按下 [Ctrl] + [Alt] + [Del] 鍵，請在 [動作] 選單中點選 [客體作業系統] [傳送按鍵] \[Ctrl-Alt-Delete] 即可。



1.8 vCenter Server 7.0 系統需求

在完成了多部 ESXi 7.0 主機的安裝與配置之後，後續若要進行集中管理以及使用進階的運行功能，就必須進一步部署 vCenter Server 7.0 並完成與所有 ESXi 主機的連線配置。在開始講解部署步驟之前，同樣的請先來了解一下部署 vCenter Server 的系統需求與注意事項。首先是如表 1-2 所示的五種部署規模大小的資源需求說明。

表 1-2 不同部署規模的系統需求

部署大小	vCPUs	記憶體大小	儲存區大小	主機數量	虛擬機器數量
Tiny	2	12GB	415GB	10	100
Small	4	19GB	480GB	100	1000
Medium	8	28GB	700GB	400	4000
Large	16	37GB	1065GB	1000	10000
X-Large	24	57GB	1805GB	2000	35000

在完成了 vCenter Server 的部署之後，便可以使用它內建的 vSphere Client 網站，來集中管理 vCenter Server、ESXi 主機、虛擬機器等各項功能配置，不過必須注意連線此網站所相容的網頁瀏覽器，在 Windows 作業系統（32bit 與 64bit）部分有 Microsoft Edge 38 以上版本、Mozilla Firefox 45 以上版本、Google Chrome 50 以上版本。在 Mac OS 作業系則有 Mozilla Firefox 45 以上版本、Google Chrome 50 以上版本。

請注意！如果你的 vCenter Server 選擇部署在有相隔防火牆的網路位置之中，則必須特別留意所需要開啟的連接埠有哪些。關於這方面的資訊可以參考以下的官網說明。

- vCenter Server 所需的連接埠：

<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.upgrade.doc/GUID-925370DD-E3D1-455B-81C7-CB28AAF20617.html>

Kubernetes Service，只不過當時透過附加於虛擬機器中的運行來完成，而不像現在是直接內建原生的 Kubernetes，讓開發人員可以透過介面並使用命令或 Script 的方式，來建立專屬的 K8s 叢集、節點、應用程式以及調配所需要的虛擬化資源，並同時享有 vSphere 各項高可用性、高可靠度、高擴充性、高延展性的防護機制。

除了內建原生的 Kubernetes 之外，還提供了在雲端基礎服務以及混合架構服務下的 vSphere Pod Service、Storage Service、Network Service 以及 Registry Service，這一些都是在前一版本（6.7）中所沒有的強大功能。

而在各項資源管理數量上的最大支援限制上，ESXi 7.0 相較於前一版 ESXi 6.7 是一樣的，像是對於每一台主機所支援的邏輯 CPU 數量上限皆是 768、支援的虛擬機器數量皆是 1024 等等。不過若是在 vCenter Server 6.7 與最新 7.0 的比較上，則是有所增長的，這部分可以參考表 2-1 說明。此外必須要注意的是在前一版本的 vCenter Server 6.7 所提供的 vSphere Client，還同時支援 Flash-based 的舊版 Web Client 與新版的 HTML5 Client 設計介面，但在新版的 vCenter Server 7.0 中僅支援純 HTML5 Client 的設計介面。

表 2-1 vCenter Server 相關連接管理數量比較

功能	vSphere 6.7	vSphere 7.0
每一 vCenter Server 的主機上限	2000	2500
每一 vCenter Server 已開機的虛擬機器上限	25000	40000
每一 vCenter Server 已註冊的虛擬機器上限	35000	45000
已連結的 vCenter Server 系統上限	15	15
在已連結的 vCenter Server 中的主機數量	5000	15000
在已連結 vCenter Server 中的已開機虛擬機器上限	50000	135000
在已連結 vCenter Server 中註冊的虛擬機器上限	70000	150000
每一 vCenter Server 中 Lifecycle Manager 可管理的主機數量	N/A	150

2.3 vSphere 7.0 注意事項

vSphere 7.0 除了新增了上述主要功能之外，在部署前與未來的維運管理上還有哪一些需要特別注意的呢？筆者特別整理如下：

- TLS Protocol 預設將是啟用 1.2 版本，至於 TLS 1.0 與 TLS 1.1 版本預設則是關閉的。如果需要啟用舊版 TLS Protocol，可透過 TLS Configurator 工具來啟用。
- 為簡化管理已移除外部的 PSC (Platform Services Controller)。在 vSphere 7.0 中的 vCenter Server 已包含了所有 PSC 服務，保留了所有的功能包括了流程、身分驗證、憑證管理以及授權管理，因此不再需要提供外部 PSC 的部署選項。
- 已移除了 vCenter Server for Windows 的部署支援。關於這點其實早在前一版的發行說明中已有預告。
- ESXi 7.0 主機中已移除了舊版所內建的 VNC Server 功能。換句話，你無法再透過虛擬機器進階配置中的 RemoteDisplay.vnc.enable=true 設定，來讓 VNC Client 可以來進行遠端操作 Guest OS。取而代之的是改透過 vSphere Client、ESXi Host Client 或 VMware Remote Console 來完成相同任務。
- 用以進行更新管理的 Update Manager 附加程式 (plugin)，已由 Lifecycle Manager 所取代，如此除了可繼續管理旗下的 Update Manager，也可以使用新增加的功能。
- 整合 Windows 驗證 (IWA) 的功能在 vSphere 7.0 中已被取代，並且將在未來版本中移除。
- Direct Console 使用者介面 (DCUI) 在未來的版本中，將不再支援智慧卡的驗證功能。

2.4 vSphere 7.0 升級前的準備

你可以選擇將 vSphere 6.5 或 6.7 直接升級至 7.0 版本，筆者將以 6.5 版本為升級來源的系統。想要將舊版的 vSphere 6.5 架構升級至 vSphere 7.0，則升級的四大標準程序請依序為：(1) 備份 vCenter 與 ESXi 伺服器、(2) 升

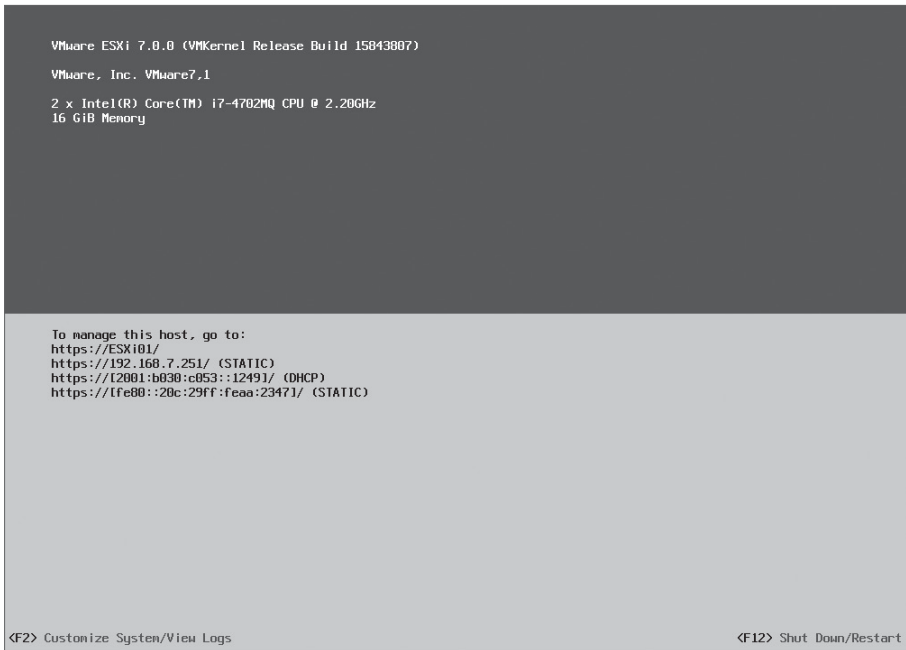


圖 2-22 主機 DCUI 管理介面

2.9 使用 ESXCLI 升級 ESXi 主機

緊接著要講解的第二種就地升級法，就是透過 ESXCLI 命令工具來完成。首先請到 ESXi 伺服器端的主控制台，按下 [F2] 鍵開啟系統設定頁面，進入之前將需要輸入此主機系統管理員的帳戶密碼。接著請點選進入 [Troubleshooting Options] 頁面，分別將 [ESXi Shell] 與 [SSH] 兩項功能設定啟用 (Enable)。如此一來後續所要執行的命令參數，便可以自由選擇經由本機的 Shell 或遠端的 SSH 連線來進行。在此筆者建議採用後者的連線方式。

升級之前請確認已經在官網上下載好了升級封裝檔案 (例如：VMware-ESXi-7.0.0-15843807-depot.zip)。接下來請將所下載的 depot 封裝檔案，如圖 2-23 所示透過 vSphere Client 的連線上傳到儲存區之中，必須注意的是在叢集 (Cluster) 的架構之中，由於我們可能會陸續升級多部的 ESXi 主機，因此這個 depot 封裝檔案就必須上傳至叢集共用的資料儲存區之中。如果只是升級單一 ESXi 主機，只需連線登入 ESXi Host Client 並將封裝檔案上傳至本機的資料存放區即可。

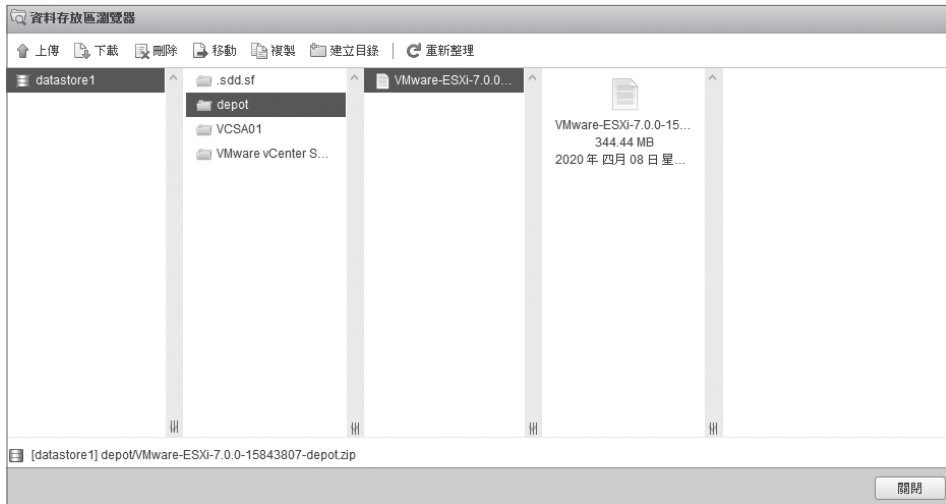


圖 2-23 上傳 depot 檔案至本機

接下來便可以將準備升級的 ESXi 主機上的所有虛擬機器關機，或移轉至其他 ESXi 主機中來運行。然後再使用 SSH 工具連線至 ESXi 主機，如圖 2-24 所示執行以下命令參數來查看目前這個 depot 檔案的封裝內容，其中資料夾的所在路徑，必須輸入你實際的存放路徑。內容中可以發現有兩個檔案，其中 ESXi-7.0.0-15843807-standard 就是我們接下來會使用到的檔案。

```
esxcli software sources profile list -d=/vmfs/volumes/datastore1/  
depot/VMware-ESXi-7.0.0-15843807-depot.zip
```

最請執行以下命令參數，以完成 ESXi 主機系統的更新任務，操作也會把升級結果輸出到一個名為 output.txt 文件之中。

```
esxcli software profile update -d=/vmfs/volumes/datastore1/depot/  
VMware-ESXi-7.0.0-15843807-depot.zip -p=ESXi-7.0.0-15843807-  
standard > /tmp/output.txt
```

3.1 簡介

通常我們在買一台標準伺服器的主機時，在選購上除了 CPU 與 RAM 的規格之外，對於硬碟的規格選擇會特別講究，因為除了儲存容量大小與 I/O 讀寫的速度之外，還需要搭配磁碟陣列控制卡（RAID controller）的配置，來預防發生單一磁碟故障時的容錯機制。舉例來說，你可以選定兩顆磁碟配置為 RAID 1 來做為系統磁碟，接著再選定四顆磁碟配置為 RAID 6 來做為資料磁碟，最後再配置一顆純熱備援（Host Spare）用途的磁碟。

關於上述常見的磁碟陣列規劃方式，無非是要確保資料儲存的基本安全，以便在發生磁碟故障時主機仍可繼續維持正常運作。如果想要更加保障主機的可用性，可以考慮再添加電源供應器的熱備援。上述這些做法僅是針對單一實體主機在硬體故障時的容錯機制，然而當有多個虛擬機器需要在這一台主機來運行時，如何預防主機在發生硬體故障、斷電或網路無法連線時，仍可繼續運行提供服務的可用性狀態呢？

答案其實很簡單，只要再多準備一台以上的主機並且建立叢集（Cluster）架構，便可以啟用這個虛擬化平台所支援的 HA 機制，來讓叢集中所有連接共用儲存區的虛擬機器，都享有容錯移轉的熱備援能力，如此一來便可以讓所有運行於這一些虛擬機器之中的應用程式、服務以及資料庫等系統，同時獲得硬體架構與虛擬化架構的雙重保護。如今像這樣的基礎私有雲的架構部署，早已成為了許多組織在新一代 IT 基礎建設的規劃重點，並且絕大多數都是選擇以 VMware vSphere 為主 HA 方案。

關於 vSphere HA 的運作方式並沒有很複雜，簡單來說是在它叢集中啟用 HA 功能時，系統會自動完成叢集中每台主機代理程式的部署，接著它會監視叢集中所有的 ESXi 主機，並自動選擇一台 ESXi 主機來作為主要主機（Master Host），讓它負責去監視所有受保護虛擬機器以及次要主機的狀態。

之後一旦有主機發生故障時，將會藉由資料存放區活動訊號來確認故障的類型，如果發現主機故障而必須重新啟動運行中的虛擬機器之時，將會立即在叢集中其他備用的主機上來重新啟動，至於虛擬機器重新啟動的優先順序則是可以由管理員預先配置好的。

3.7 測試虛擬機器故障備援

一旦完成了 vSphere HA 功能的啟用之後，接著就可以來進行容錯移轉的測試，不過必須注意的是你必須針對已經運行在叢集中的虛擬機器來進行測試，而不是針對叢集以外的虛擬機器，或是使用 ESXi 本機儲存區的虛擬機器來進行測試。為此筆者會建議管理人員對於虛擬機器的 [摘要] 資訊檢視，可以透過點選 [切換到新視圖] 按鈕來開啟如圖 3-23 所示的檢視頁面，這個新的視圖設計除了可以讓我們迅速查看到此虛擬機器對於各項資源的容量與使用量、硬體規格以及快照資訊之外，更重要的是能夠直接得知虛擬機器所在的叢集、主機、網路以及儲存區。

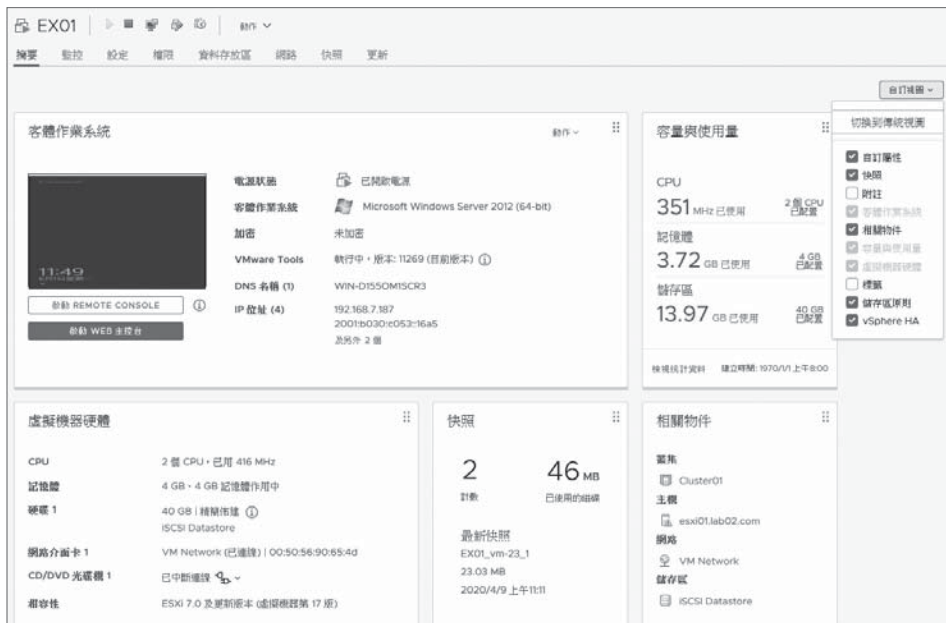


圖 3-23 虛擬機器新視圖

如果你想要將現行運行於 ESXi 本機儲存區的虛擬機器，移轉至叢集所連接的共用儲存區之中，只要在選取虛擬機器之後，點選位在 [動作] 選單中的 [移轉]，然後 [選取移轉類型] 頁面中選擇 [僅變更儲存區] 的選項，即可開始進行虛擬機器儲存區的移轉任務。

4.2 安裝 VMware Converter Standalone

VMware vCenter Converter Standalone 是一套 VMware 發行的免費工具，可以讓 IT 人員以很簡單的精靈介面操作方式，從實體主機或其他虛擬機器來源完成 VMware 虛擬機器的移轉，也就是所謂的 P2V 以及 V2V。

VMware vCenter Converter Standalone 目前最新的版本是 6.2，用戶可以自行在 my.vmware.com 網站來進行搜尋與下載。目前僅提供英文版本。你可以選擇將它安裝在目前所相容的用戶端作業系統，包括了 Windows Vista SP2 至最新版本的 Windows 10。若是選擇安裝在相容的伺服器作業系統，則目前支援的有 Windows Server 2008 SP2 至 Windows Server 2016。

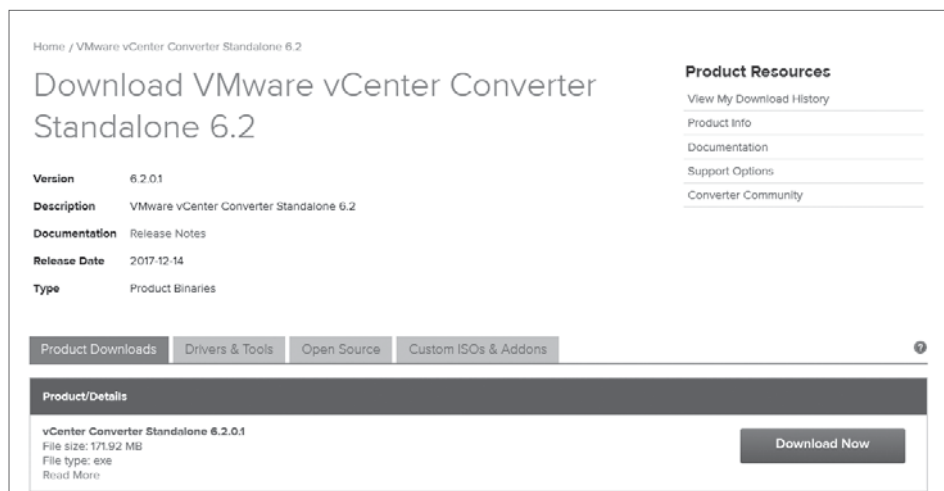


圖 4-1 下載 VMware vCenter Converter Standalone 6.2

如果你準備移轉的離線虛擬機器是來自 Hyper-V，則相容的 Hyper-V 作業系統有 Windows Server 2008 R2、Windows Server 2012/R2、Windows Server 2016 以及 Windows 10。值得注意的是官方雖沒有公布相容於最新的 Windows Server 2019，但根據筆者的實測也是可以成功相容與移轉的。

至於在移轉來源所相容的 Guest OS 部分，則支援的有 Windows Vista SP2 至最新版本的 Windows 10、Windows Server 2008 SP2 至 Windows Server 2016、CentOS 6.x 至 7.5、Red Hat Enterprise Linux 4.x 至 7.5、SUSE Linux Enterprise Server 10.x 至 11.x、Ubuntu 12.04 LTS 至 16.04 LTS。

行高可用性。整體而言 VMware vSAN 對於檔案資料的存放與虛擬機器的運行，不僅大幅提升了執行性能與安全性，也同時簡化了管理複雜度與降低總體持有成本（TCO）。

8.2 VMware vSAN 7.0 新功能

對於超大型的架構需求而言可以部署具備 64 個節點的 vSAN 叢集，但其實對於小型架構需求的 IT 環境來說，VMware 打從 vSAN 6.1 版本開始，便已經提供了支援雙節點的 vSAN 運作架構來因應。接著從 vSAN 6.5 版本開始，規格要求上也不再強制需要搭配昂貴的 10Gbps 網路交換器，且支援了分離見證網路流量的配置。

上述這一些改變對於中小型企業的 IT 環境來說，不僅可大幅降低 vSAN 部署的成本，也提升了整體運行與管理上的彈性與效率。然而整體而言相較於前一版的 vSAN 6.7 來說，vSAN 7.0 究竟新增與改善了哪一些關鍵功能的設計呢？

- **簡化管理：**有別於舊版的 vSphere Update Manager（VUM）的更新管理設計，全新 vSphere Lifecycle Manager（vLCM）不僅可以一致性管理 vSphere 架構下的所有 vCenter Server、ESXi、虛擬機器的版本更新之外，也能夠針對儲存相關的控制器、模組、韌體進行相符性掃描與矯正，簡單做好統一的生命週期管理。
- **原生檔案服務：**vSAN 7.0 叢集的原生檔案服務（Native File Services）已提供可建立和提供 NFS v4.1 和 v3 檔案共用的功能，如此一來 IT 部門對於任何應用系統所需要連接 NFS 儲存區的需求，就可以直接由 vSAN 來提供而無須另尋其他解決方案了。不過此新功能並不支援本章所要講解的雙節點延伸叢集架構之中，而是必須運行在已部署 3 至 8 台 vSAN 節點主機的環境之中。只要完成相關配置與功能啟用，後續便可以從 vSAN Skyline Health Services 頁面中的 [The File Service - Infrastructure health] 選項來監視它運行的健康狀態了。
- **增強雲端原生儲存：**早在 vSAN 6.7 U3 版本時期，VMware 就已經引進了雲端原生儲存，這讓管理人員可以直接在 vSphere Client 網站上來運行、監視以及管理容器（Container）與虛擬機器（VM）在相同的平

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

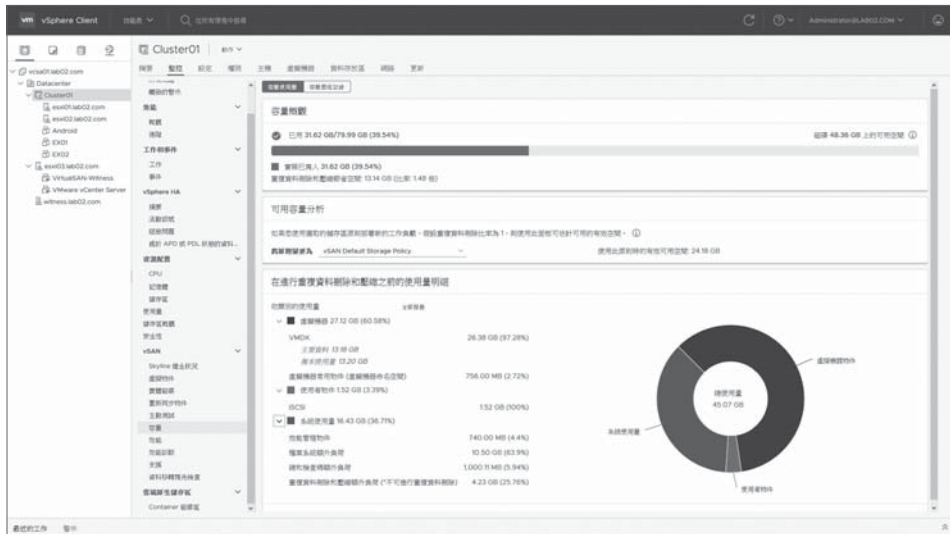


圖 8-22 容量使用分析與記錄

針對許多 IT 人員關心的 vSAN 運行的效能表現問題，可以如圖 8-23 所示在 [監控] \ [vSAN] \ [效能] 頁面中，分別查看到虛擬機器、後端以及 iSCSI 運行的效能分析，管理員可以根據選定的時間範圍，來檢視包括了 IOPS、輸送量、延遲時間、頻寬以及壅塞的分析圖。



圖 8-23 vSAN 效能分析

為了避免未來 vSAN 叢集之中會有主機故障或是停機維護的需求，最好能夠預先在 [監控] \ [vSAN] \ [資料移轉預先檢查] 頁面中，如圖 8-24 所示來針對選定的 ESXi 主機執行 [確保可存取性] 的測試。藉此可以讓管理人員得