Horizon 7 架構規劃

2019 年 12 月
VMware Horizon 7 7.11

vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

https://docs.vmware.com/tw/

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目錄

Horizon 7 架構規劃

《Horizon 7 架構規劃》提供 VMware Horizon™ 7 簡介，其中包括主要功能和部署選項的說明，以及生產環境中元件一般設定方式的概述。

本指南提供下列問題的解答：

- 本產品是否解決您要解決的問題？
- 在企業中實作此解決方案是否可行且符合成本效益？

並非所有版本均提供 VMware Horizon 7 的全部特色與功能。如需比較各版本的功能集，請參閱 http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf。

為協助您保護所安裝的產品，本指南也會討論安全功能。

主要對象

此資訊適用於 IT 決策者、架構設計人員、管理員，以及必須熟悉本產品元件與功能的其他人。架構設計人員和規劃人員可利用本指南中的資訊，判斷 Horizon 7 是否可滿足其企業以良好效率且安全方式提供 Windows 桌面和應用程式給其使用者的需求。架構範例則有助於規劃人員瞭解大規模部署的硬體需求及所需執行的設定工作。

Horizon 7 簡介

1

透過 Horizon 7，IT 部門可在資料中心執行遠端桌面平台和應用程式，並將這些桌面平台和應用程式作為受管理服務提供給員工。使用者可取得熟悉、個人化的環境，可以在企業內的任何位置或從家裡，透過任意數量的裝置進行存取。管理員則將桌面平台資料放在資料中心，可進行集中控制、並獲得效率與安全性。

本章節討論下列主題：

使用 Horizon 7 的優點

利用 Horizon 7 管理企業桌面的優點，包括可靠性、安全性、硬體獨立性和便利性等都能獲得提升。

可靠性與安全性

透過整合 VMware vSphere® 以及虛擬化伺服器、儲存區和網路資源，可以集中放置桌面平台和應用程式。將桌面平台作業系統與應用程式放在資料中心的某一部伺服器上，可提供下列優點：

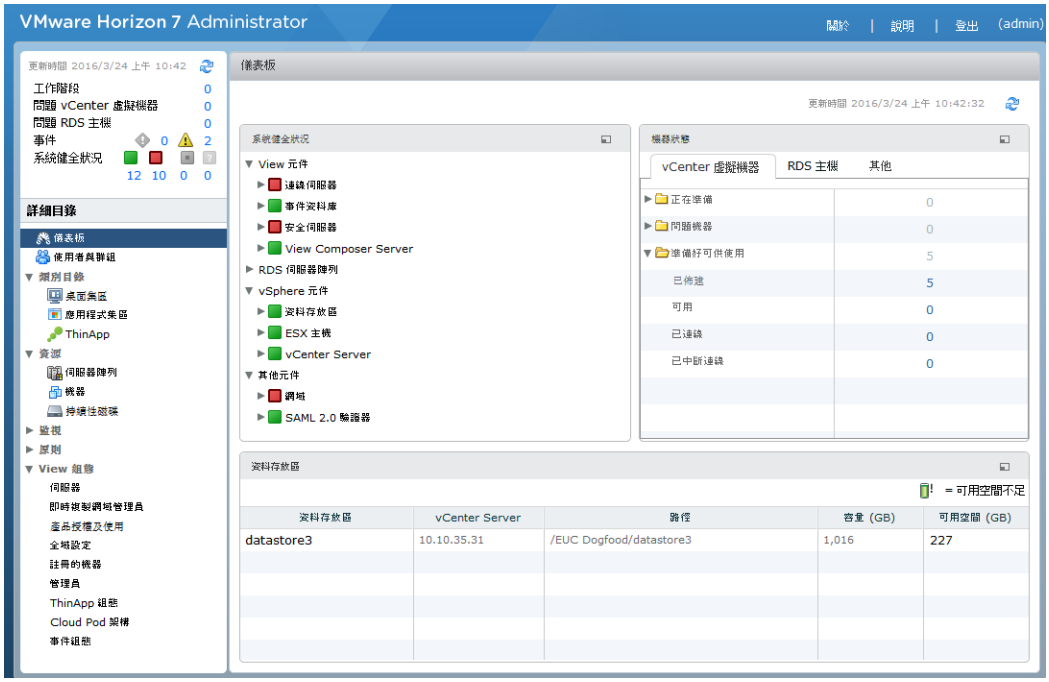
- 可以輕鬆地限制存取資料。可以防止複製機密資料到遠端員工的家用電腦。
- RADIUS 支援提供從雙因素驗證廠商當中進行選擇的彈性。支援的廠商包括 RSA SecureID、VASCO DIGIPASS、SMS Passcode 和 SafeNet 等等。
- 整合 VMware Identity Manager 意味著，使用者可以依需求透過其用於存取 SaaS、Web 和 Windows 應用程式的同一個 Web 型應用程式目錄存取遠端桌面平台。在遠端桌面平台內部，使用者還可以使用此自訂應用程式存放區來存取應用程式。
- 能夠佈建包含預先建立之 Active Directory 帳戶的遠端桌面平台，解決了具有唯讀存取權原則的鎖定 Active Directory 環境的需求。
- 可以排程資料備份，而不用考慮使用者的系統何時可能會關閉。
- 資料中心主控的遠端桌面平台和應用程式極少會發生停機狀況，甚至永遠不會停機。虛擬機器可以位於 VMware Server 的高可用性叢集上。

虛擬桌面平台也可以連線至後端實體系統和 Microsoft 遠端桌面平台服務 (RDS) 主機。

便利性

將建立統一管理主控台以提供擴充性，因此即使是最大型的 Horizon 7 部署都能從單一管理介面進行有效管理。精靈和儀表板可增強工作流程，並且有助於更深入檢視詳細資料或變更設定。圖 1-1. 顯示儀表板檢視的管理主控台 會提供 Horizon Administrator 的瀏覽器型使用者介面範例。

圖 1-1. 顯示儀表板檢視的管理主控台



可提高便利性的其他功能為 VMware 遠端顯示通訊協定、PCoIP (PC over IP) 和 Blast Extreme。這些顯示通訊協定提供相當於目前實體電腦使用經驗的使用者經驗：

- 在 LAN 上，此顯示比傳統遠端顯示更快且更順暢。
- 在 WAN 上，此顯示通訊協定可以補償延遲的增加或頻寬的減少，以確保使用者在任何網路條件下都能維持產能。

管理能力

為使用者佈建桌面平台和應用程式是一種快速程序。完全不需要使用人力在每位使用者的實體電腦上逐一安裝應用程式。使用者會連線至已發佈的應用程式或具有應用程式的遠端桌面平台。使用者可以在任何位置，從各種裝置存取其相同的遠端桌面平台或應用程式。

使用 VMware vSphere 主控虛擬桌面平台和 RDS 主機伺服器具有下列優點：

- 可減少管理工作和管理日常事務。管理員不用接觸使用者的實體電腦，即可修補及升級應用程式和作業系統。
- 整合 VMware Identity Manager 後，IT 管理員可使用 Web 型 VMware Identity Manager 管理介面監控使用者和群組使用遠端桌面平台的權利。

- 與 VMware App Volumes 整合，它是即時的應用程式提供系統，可讓企業大規模提供及管理應用程式。使用 App Volumes 將應用程式連結到使用者、群組或目標電腦 (即使使用者已登入其桌面平台)。應用程式也能夠即時佈建、提供、更新及淘汰。
- 利用 Horizon Persona Management，將可集中管理實體和虛擬桌面平台，包括使用者設定檔、應用程式權利、原則、效能及其他設定。請先將角色管理部署至實體桌面平台使用者，再轉換成虛擬桌面平台。
- 運用 VMware User Environment Manager，使用者可獲得個人化的 Windows 桌面平台以適應使用者的情況，這表示對所需 IT 資源的存取是根據角色、裝置和位置之類的層面。
- 儲存管理獲得簡化。您可以使用 VMware vSphere 虛擬化磁碟區和檔案系統，以避免管理個別的儲存裝置。
- 在 vSphere 6.0 或更新版本中，您可以使用虛擬磁碟區 (VVol)。此功能將虛擬磁碟及其衍生物、複製品、快照以及複本直接對應到儲存區系統上的物件 (稱為虛擬磁碟區)。此對應允許 vSphere 卸載密集儲存作業，例如儲存區系統的快照、複製以及複寫。例如，原先需要一小時的複製作業，現在透過虛擬磁碟區只需幾分鐘的時間。
- 運用 vSphere 5.5 Update 1 或更新版本，您可以使用 vSAN，它可將 ESXi™ 主機上提供的本機實體固態硬碟與硬碟機，虛擬化為叢集內所有主機共用的單一資料存放區。在建立桌面平台集區時僅指定一個資料存放區，各種元件 (如虛擬機器檔案、複本、使用者資料和作業系統檔案) 即會視情況放置在 SSD 磁碟或硬碟機上。

  您將以預設儲存區原則設定檔的形式管理虛擬機器儲存需求 (如容量、效能和可用性)，這些設定檔在您建立桌面平台集區時會自動建立。
- 利用 Horizon 7 儲存加速器，IOPS 儲存負載將大幅降低，進而可支援更大規模的使用者登入，而不需要任何特殊的儲存陣列技術。
- 如果遠端桌面平台使用隨 vSphere 5.1 及更新版本提供的空間效率高的磁碟格式，則會透過清除與壓縮程序，自動回收客體作業系統內過時或已刪除的資料。

硬體獨立性

遠端桌面平台和已發佈的應用程式都具有硬體獨立性。例如，由於遠端桌面平台可以在資料中心的伺服器上執行，並且只能透過用戶端裝置存取，因此遠端桌面平台可以使用可能與用戶端裝置硬體不相容的作業系統。

遠端桌面平台可以在電腦、Mac、精簡型用戶端，以及改變用途作為精簡型用戶端的電腦、平板電腦和手機上執行。已發佈的應用程式可在上述部分裝置上執行。新裝置支援將按季新增。

如果您使用 HTML Access 功能，則使用者可以在瀏覽器中開啟遠端桌面平台或應用程式，而不需要在用戶端系統或裝置安裝任何用戶端應用程式。

Horizon 7 功能

Horizon 7 的功能支援可用性、安全性、集中管理和擴充性。

下列功能提供使用者所熟悉的經驗：

- 在某些用戶端裝置上，從虛擬桌面列印至用戶端裝置上定義的任何本機或網路印表機。此虛擬印表機功能解決相容性問題，並且不需要在虛擬機器中安裝額外的驅動程式。
- 在大多數用戶端裝置上，使用隨選列印功能可對應至實體在用戶端系統附近的印表機。不必在虛擬機器中安裝列印驅動程式，即可使用隨選列印。
- 本機印表機重新導向專為下列使用案例而設計：
  - 直接連線至用戶端上 USB 或序列埠的印表機
  - 特殊印表機，例如連線至用戶端的條碼印表機和標籤印表機
  - 遠端網路上無法從虛擬工作階段定址的網路印表機。
- 使用多部監視器。利用 PCoIP 和 Blast Extreme 顯示通訊協定，多監視器支援表示您可以為每個監視器個別調整顯示解析度和旋轉。
- 存取連線至顯示虛擬桌面之本機裝置的 USB 裝置及其他週邊設備。

  您可以指定允許使用者連線的 USB 裝置類型。對於包含多種裝置 (例如視訊輸入裝置和儲存裝置) 類型的複合式裝置，您可以分割裝置，以允許使用某一種裝置 (例如視訊輸入裝置)，但不允許使用另一種裝置 (例如儲存裝置)。
- 使用 Horizon Persona Management 保留工作階段之間的使用者設定和資料，即使桌面經過重新整理或重新撰寫也可以這麼做。角色管理能夠以可設定的間隔時間，定期將使用者設定檔複寫至遠端設定檔存放區 (CIFS 共用)。

  您也可以在未由 Horizon 7 管理的實體電腦和虛擬機器上使用獨立版本的角色管理。

Horizon 7 提供下列安全功能及其他功能：

- 使用雙因素驗證登入，例如 RSA SecurID 或 RADIUS (遠端驗證撥入使用者服務)，或使用智慧卡登入。
- 在具有 Active Directory 唯讀存取原則的環境中佈建遠端桌面平台和應用程式時，使用預先建立的 Active Directory 帳戶。
- 使用 SSL/TLS 通道確保所有連線都經過完整加密。
- 使用 VMware High Availability 確保自動執行容錯移轉。

擴充性功能視管理桌面和伺服器的 VMware 虛擬化平台而定：

- 整合 VMware vSphere 以達成遠端桌面平台和應用程式符合成本效益的密度、高可用性，以及進階資源配置控制。
- 使用 Horizon 7 儲存加速器功能，以相同的儲存資源支援更大規模的使用者登入。此儲存加速器使用 vSphere 5 平台的功能來建立通用區塊讀取的主機記憶體快取。
- 設定 Horizon 連線伺服器，以便代理使用者與他們有權存取的遠端桌面平台和應用程式間的連線。
- 使用 View Composer 快速建立與主要映像共用虛擬磁碟的桌面映像。用此方式使用連結複製，可節省磁碟空間並簡化作業系統修補程式和更新的管理。

- 使用 Horizon 7 中推出的即時複製功能，快速建立與父系映像共用虛擬磁碟和記憶體的桌面平台映像。即時複製不僅具有 View Composer 連結複製的空間效率，也可以消除重新整理、重新撰寫、重新平衡的需求，進而簡化作業系統修補程式及更新的管理。即時複製可完全消除桌面平台維護時段。

下列功能提供集中管理：

- 使用 Microsoft Active Directory 管理遠端桌面平台和應用程式的存取權及管理原則。
- 使用角色管理簡化從實體移轉至虛擬桌面平台的作業。
- 使用 Web 型管理主控台從任何位置管理遠端桌面平台和應用程式。
- 您可以使用 Horizon Administrator 散佈及管理 VMware ThinApp™ 隨附的應用程式。
- 使用範本或主要映像，快速建立和佈建桌面集區。
- 在不影響使用者設定、資料或喜好設定之下，將更新和修補程式傳送至虛擬桌面。
- 與 VMware Identity Manager 整合，讓使用者可透過 Web 上的使用者入口網站存取遠端桌面平台，並透過遠端桌面平台內部的瀏覽器使用 VMware Identity Manager。
- 與 Mirage™ 及 Horizon FLEX™ 整合，以管理本機安裝的虛擬機器桌面平台，並在專用的完整複製遠端桌面平台上部署及更新應用程式，而不覆寫使用者安裝的應用程式。

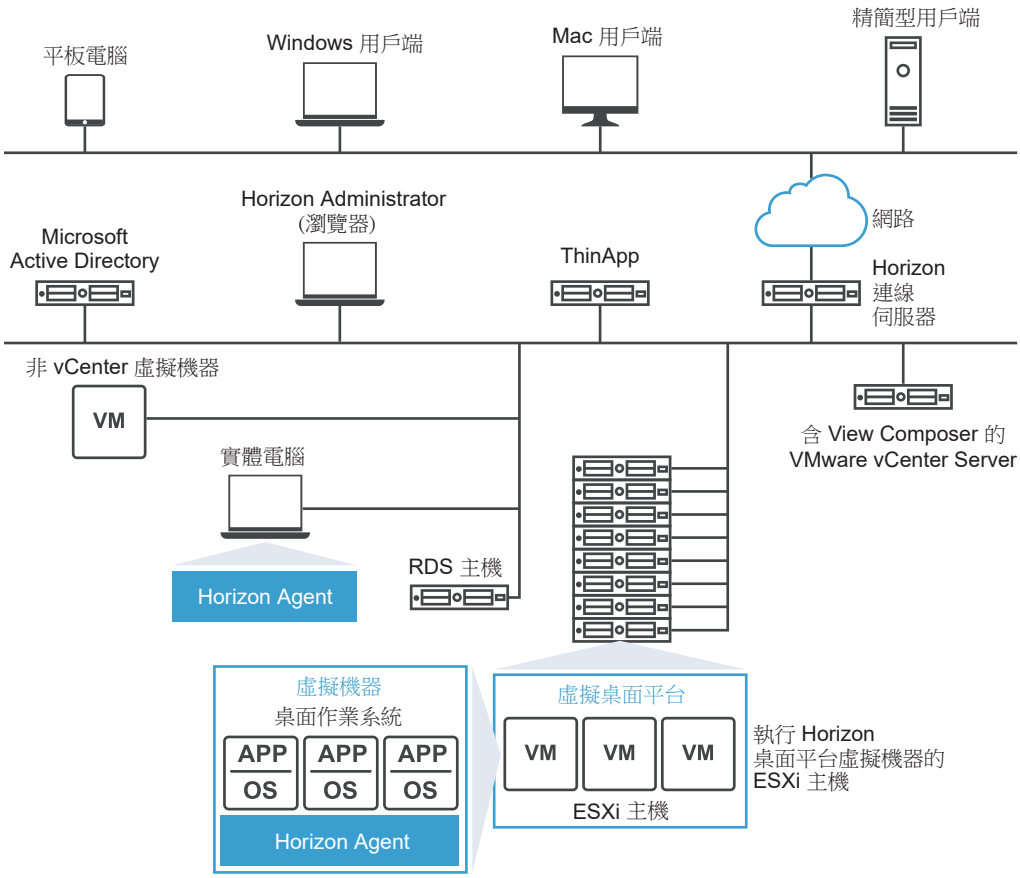
元件搭配運作的方式

使用者啟動 Horizon Client 以登入 Horizon 連線伺服器。此伺服器與 Windows Active Directory 整合，可讓您存取 VMware vSphere Server、實體電腦或 Microsoft RDS 主機上主控的遠端桌面平台。Horizon Client 也能讓您存取 Microsoft RDS 主機上已發佈的應用程式。

備註 Horizon 7 支援 Active Directory Domain Services (AD DS) 網域功能層級：如需關於受支援 AD DS 網域功能層級的詳細資訊，請參閱 VMware 知識庫 (KB) 文章 http://kb.vmware.com/kb/2150351。

圖 1-2. 高階 Horizon 7 環境範例 顯示 Horizon 7 部署中主要元件之間的關係。

圖 1-2. 高階 Horizon 7 環境範例



用戶端裝置

使用 Horizon 7 的一個重要優勢是，無論裝置或位置為何，遠端桌面平台和應用程式都會跟隨著使用者。使用者可以從公司筆記型電腦、家用電腦、精簡型用戶端裝置、Mac、平板電腦或手機，存取其個人化的虛擬桌面平台或遠端應用程式。

使用者將開啟 Horizon Client 以顯示其遠端桌面平台及應用程式。精簡型用戶端裝置會使用 Horizon 7 精簡型用戶端軟體，且可設定為使用者可在裝置上直接啟動的唯一應用程式是 Horizon 7 精簡型用戶端。將舊版電腦重新運用為精簡型用戶端桌面，可以延長硬體使用壽命三到五年。例如，藉由在精簡型桌面平台使用 Horizon 7，您可以在較舊的桌面平台硬體上使用較新的作業系統 (例如 Windows 8.x)。

如果您使用 HTML Access 功能，則使用者可以在瀏覽器中開啟遠端桌面平台，而不需要在用戶端系統或裝置安裝任何用戶端應用程式。

Horizon 連線伺服器

此軟體服務會用作用戶端連線的 Broker。Horizon 連線伺服器會透過 Windows Active Directory 驗證使用者，並將要求導向至適當的虛擬機器、實體電腦或 Microsoft RDS 主機。

連線伺服器提供下列管理功能：

- 驗證使用者

- 賦予使用者使用特定桌面和集區的權利
- 將使用 VMware ThinApp 封裝的應用程式指定給特定桌面和集區
- 管理遠端桌面平台和應用程式工作階段
- 建立使用者與遠端桌面平台及應用程式之間的安全連線
- 啟用單一登入
- 設定並套用原則

在公司防火牆內部，您可以安裝並設定一個包含兩個或更多連線伺服器執行個體的群組。其組態資料會儲存在內嵌 LDAP 目錄中，並在群組成員之間複寫。

在公司防火牆以外，您可以在 DMZ 中安裝連線伺服器，並將其設定為安全伺服器，或者您可以安裝 Unified Access Gateway 應用裝置。DMZ 中的安全伺服器和 Unified Access Gateway 應用裝置會與公司防火牆內的連線伺服器通訊。安全伺服器和 Unified Access Gateway 應用裝置可確保能夠進入公司資料中心的遠端桌面平台和應用程式流量，皆為代表經過嚴格驗證之使用者的流量。使用者只能存取其有權存取的資源。

安全伺服器提供功能子集，並不需要位於 Active Directory 網域中。您可以在 Windows Server 2008 R2 或 Windows Server 2012 R2 伺服器中安裝連線伺服器，但最好是安裝在 VMware 虛擬機器上。如需 Unified Access Gateway 應用裝置的詳細資訊，請參閱《部署及設定 Unified Access Gateway》。

重要 您可以建立不使用連線伺服器的 Horizon 7 安裝。如果您在遠端虛擬機器桌面平台上安裝 Horizon 7 Agent Direct Connect 外掛程式，則用戶端可直接連線至該虛擬機器。所有遠端桌面平台功能，包括 PCoIP、HTML Access、RDP、USB 重新導向和工作階段管理工作，都可以按此方式進行連線，如同使用者已透過連線伺服器連線一樣。如需詳細資訊，請參閱《Horizon 7 Agent Direct-Connection 外掛程式管理》。

Horizon Client

用於存取遠端桌面平台和應用程式的用戶端軟體可以執行於平板電腦、手機、Windows、Linux、Mac 電腦或筆記型電腦、精簡型用戶端等等。

登入後，使用者從有權使用的遠端桌面平台和應用程式清單中選取。授權可能會要求 Active Directory 認證、UPN、智慧卡 PIN 或 RSA SecurID，或其他雙因素驗證 Token。

管理員可以將 Horizon Client 設定為允許使用者選取顯示通訊協定。通訊協定包含適用於遠端桌面平台的 PCoIP、Blast Extreme 和 Microsoft RDP。PCoIP 和 Blast Extreme 的速度和顯示品質比得上實體電腦的速度和顯示品質。

功能因您使用的 Horizon Client 而異。本指南的重點在於 Windows 版 Horizon Client。本指南不提供下列類型用戶端的詳細說明：

- 適用於平板電腦、Linux 用戶端和 Mac 用戶端之 Horizon Client 的相關詳細資料。請參閱位於 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html 的 Horizon Client 說明文件。
- HTML Access Web client 的相關詳細資料，此用戶端可讓您在瀏覽器中開啟遠端桌面平台。用戶端系統或裝置不會安裝 Horizon Client 應用程式。請參閱位於 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html 的 Horizon Client 說明文件。

- 各種第三方精簡型用戶端和零用戶端，只能透過認證合作夥伴取得。
- 支援 VMware 合作夥伴認證計畫的 View Open Client。View Open Client 不是官方用戶端應用程式，所以本身並不受支援。

VMware Horizon 使用者入口網站

在用戶端裝置的 Web 瀏覽器上，使用者可以透過瀏覽器連線到遠端桌面平台和應用程式，自動啟動 Horizon Client (如已安裝)，或下載 Horizon Client 安裝程式。

當您開啟瀏覽器並輸入 Horizon Connection Server 執行個體的 URL 時，顯示的 Web 頁面會包含 VMware 下載網站的連結，供您下載 Horizon Client。不過，Web 頁面上的連結是可以設定的。例如，您可以設定連結指向內部 Web 伺服器，也可以限制自己專屬的連線伺服器可使用哪些用戶端版本。

若使用 HTML Access 功能，則 Web 頁面也會顯示一個連結，用於在受支援的瀏覽器內存取遠端桌面平台和應用程式。使用此功能，用戶端系統或裝置不會安裝任何 Horizon Client 應用程式。如需詳細資訊，請參閱 Horizon Client 說明文件，網址為：https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

Horizon Agent

您會將 Horizon Agent 服務安裝在所有用作遠端桌面平台和應用程式來源的虛擬機器、實體系統和 Microsoft RDS 主機上。在虛擬機器上，此代理程式會與 Horizon Client 通訊，以提供連線監控、虛擬列印、Horizon Persona Management 和存取本機連線的 USB 裝置等功能。

如果桌面平台來源是虛擬機器，則先要在該虛擬機器上安裝 Horizon Agent 服務，然後使用虛擬機器作為範本，或作為連結複製或即時複製的父系。從這個虛擬機器建立集區時，代理程式會自動安裝在每個遠端桌面平台上。

您可以安裝具有單一登入選項的代理程式。利用單一登入，系統僅在使用者連線至 Horizon 連線伺服器時才會提示使用者登入，而連線至遠端桌面平台或應用程式時，將不會再次提示使用者。

Horizon Administrator

此 Web 型應用程式可讓管理員設定 Horizon 連線伺服器、部署和管理遠端桌面平台和應用程式、控制使用者驗證，以及進行使用者問題的疑難排解。

安裝連線伺服器執行個體時，系統會一併安裝 Horizon Administrator 應用程式。此應用程式可讓管理員從任何位置管理連線伺服器執行個體，而不必在自己的本機電腦上安裝應用程式。

View Composer

您可以將這個軟體服務安裝在管理虛擬機器的 vCenter Server 執行個體上，或是安裝在別台伺服器上。然後 View Composer 可以從指定的父虛擬機器，建立連結複製集區。此策略可減少儲存成本達 90%。

每個連結複製會像獨立桌面般運作，具有唯一主機名稱和 IP 位址，連結複製需要的儲存空間極少，因為它與父系共用基礎映像。由於連結複製桌面集區會共用一個基礎映像，因此您可以只更新父虛擬機器，來快速部署更新和修補程式。使用者的設定、資料和應用程式不受影響。

您也可以使用 View Composer 建立連結複製 Microsoft RDS 主機的自動伺服器陣列，以將已發佈的應用程式提供給使用者。

雖然您可以將 View Composer 安裝在其自己專屬的伺服器主機，但是 View Composer 服務只能搭配一個 vCenter Server 執行個體運作。同樣的，vCenter Server 執行個體僅能與一個 View Composer 服務相關聯。

重要 View Composer 是選擇性的元件。如果您計劃佈建即時複製，則不需要安裝 View Composer。

vCenter Server

此服務可作為網路上已連線 VMware ESXi 伺服器的中央管理員。vCenter Server 可提供在資料中心中設定、佈建及管理虛擬機器的集中點。

除了使用這些虛擬機器作為虛擬機器桌面平台集區的來源，您還可以使用虛擬機器來主控 Horizon 7 的伺服器元件，包括 Horizon Connection Server 執行個體、Active Directory 伺服器、Microsoft RDS 主機和 vCenter Server 執行個體。

您可以將 View Composer 安裝在 vCenter Server 所在的同一部伺服器或其他伺服器上。vCenter Server 接著會管理實體伺服器的虛擬機器指派和儲存區，以及管理虛擬機器的 CPU 和記憶體資源指派。

您可以將 vCenter Server 做為 VMware 虛擬應用裝置來安裝，或在 Windows Server 2008 R2 伺服器或 Windows Server 2012 R2 伺服器上安裝 vCenter Server，最好安裝在 VMware 虛擬機器上。

整合和自訂 Horizon 7

為提高組織的 Horizon 7 效益，您可以使用數個介面，將 Horizon 7 與外部應用程式整合在一起，或者建立管理指令碼，以便從命令列執行或以批次模式執行。

與其他元件整合

Horizon 7 會與下列 VMware 產品整合。

VMware Cloud on AWS

VMware Cloud on AWS 可讓您在 Amazon Web Services 上建立 vSphere 資料中心。這些 vSphere 資料中心包含的 vCenter Server 用於管理您的資料中心、vSAN 可用於儲存，而 VMware NSX 則用於網路。您可以將內部部署資料中心連線至雲端 SDDC，並透過單一 vSphere Client 介面同時管理兩者。使用您已連線的 AWS 帳戶，您可以從 SDDC 中的虛擬機器存取 AWS 服務，例如 EC2 和 S3。如需詳細資訊，請參閱 VMware Cloud on AWS 說明文件，網址為：https://docs.vmware.com/tw/VMware-Cloud-on-AWS/index.html。

從 Horizon 7 (7.5 版) 開始，您可以在 VMware Cloud on AWS 上部署 Horizon 7 完整複製。例如，您可以部署在內部部署資料中心與 VMware Cloud on AWS 執行個體之間使用 Cloud Pod 架構的 Horizon 7 環境。這可讓 Horizon 7 輕鬆在混合雲環境上執行，並將 SDDC 基礎結構的管理外包給 VMware。

VMware Identity Manager

您可以整合 VMware Identity Manager 與 Horizon 7，為 IT 管理員和使用者提供下列好處：

- 使用者可依需求透過其用於存取 SaaS、Web 和 Windows 應用程式的網站上同一個使用者入口網站存取遠端桌面平台和應用程式，享有同樣的單一登入便利。

  利用 True SSO 功能，使用智慧卡或雙因素驗證進行驗證的使用者，可以存取其遠端桌面平台和應用程式而不需提供 Active Directory 認證。
- 使用者可以從遠端桌面平台內，存取網站上的 VMware Identity Manager，以取得所需的應用程式。
- 如果還使用 HTML Access，則使用者可以在瀏覽器中開啟遠端桌面平台，而不需要在用戶端系統或裝置上安裝任何用戶端應用程式。
- IT 管理員可以使用 VMware Identity Manager 以瀏覽器為基礎的管理主控台來監控使用者和群組的遠端桌面平台使用權利。

VMware Mirage 和 Horizon FLEX

您可以使用 Mirage 和 Horizon FLEX 在專屬的完整複製遠端桌面平台上部署和更新應用程式，無需覆寫使用者安裝的應用程式或資料。

Mirage 提供離線虛擬桌面平台解決方案，該解決方案比先前隨附於 Horizon 7 的本機模式功能更有效。Mirage 包括以下離線桌面平台的安全性和管理功能：

- 加密本機安裝的虛擬機器，從而防止使用者修改影響安全容器完整性的虛擬機器設定。
- VMware Fusion™ Professional 和 VMware®Player Plus™ 中提供原則 (包括到期日)，這些原則並不亞於隨先前本機模式功能一起提供的原則。Fusion Pro 和 Player Plus 隨附於 Mirage 。
- 使用者無需簽入或簽出其桌面平台即可接收更新。
- 使管理員能夠利用 Mirage 分層功能、備份功能和檔案入口網站。

VMware App Volumes

VMware App Volumes 是整合且統一的應用程式提供和使用者管理系統，適用於 Horizon 7 和其他虛擬環境。App Volumes 管理的應用程式和資料會保存在專屬的 VMDK 或 VHD 中 (稱為 AppStacks)，這些 AppStacks 會在登入或重新開機時連結至每個 Windows 使用者工作階段。此策略可確保將最新的應用程式和資料提供給使用者。App Volumes 也會為持續性的使用者安裝應用程式和設定提供不同的容器 (稱為可寫入磁碟區)，其也會在登入或重新

開機時載入。使用者設定檔和原則設定也可以使用 App Volumes 平台來管理。

VMware User Environment Manager

您可使用智慧原則功能來建立原則，以控制特定遠端桌面平台上 USB 重新導向、虛擬列印、剪貼簿重新導向、用戶端磁碟機重新導向以及 PCoIP 顯示通訊協定功能的行為。User Environment Manager 可讓 IT 控制允許使用者進行個人化的設定，而且也會對應環境設定，例如網路和位置特定的印表機。使用智慧原則，您可以建立只在符合特定條件時才生效的原則。例如，您可以設定一個原則，在使用者從公司網路外部連線至遠端桌面平台時，停用用戶端磁碟機重新導向功能。

VMware Unified Access Gateway

針對想從公司防火牆外部存取遠端桌面平台和應用程式的使用者，Unified Access Gateway 可做為安全閘道使用。Unified Access Gateway 是安裝在非軍事區 (DMZ) 中的應用裝置。使用 Unified Access Gateway 可確保能夠進入公司資料中心的流量，皆為代表經過嚴格驗證之遠端使用者的流量。您可以使用 Unified Access Gateway 應用裝置來取代 Horizon 7 安全伺服器。如需詳細資訊，請參閱 Unified Access Gateway 說明文件。

與常用視訊會議軟體整合

您可以使用這些音訊和視訊會議軟體搭配 Horizon 7。

Flash URL 重新導向

直接將 Flash 內容從 Adobe Media Server 串流至用戶端端點，可降低資料中心 ESXi 主機的負載，免除透過資料中心的額外路由作業，並減少將即時視訊事件同時串流至多個用戶端端點所需的頻寬。

Flash URL 重新導向功能會使用由網頁管理員嵌入到網頁的 JavaScript。不論虛擬桌面使用者何時從網頁中按一下指定的 URL 連結，JavaScript 會進行攔截，並從虛擬桌面工作階段重新導向 ShockWave File (SWF) 檔案到用戶端端點。然後端點會開啟虛擬桌面平台工作階段外的本機 VMware Flash 投影器，並在本機播放媒體串流。

備註 使用 Flash URL 重新導向時，多點傳送或單點傳送串流會重新導向到組織防火牆外的用戶端裝置。您的用戶端必須可存取主控 ShockWave Flash (SWF)（可啟動多點傳送或單點傳送串流）檔案的 Adobe 網路伺服器。如果需要，設定您的防火牆，開啟適當的連接埠，允許用戶端裝置存取此伺服器。

此功能僅適用於部分類型的用戶端。若要瞭解某個特定類型的用戶端是否支援此功能，請參閱「使用 VMware Horizon Client」文件中的功能支援對照表，是否包含該特定類型桌面或行動用戶端裝置。請前往 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

Microsoft Lync 2013

您可藉由 Lync 所認證的 USB 音訊及視訊裝置，在遠端桌面平台上利用 Microsoft Lync 2013 用戶端參與整合通訊 (UC) VoIP (IP 網路電話) 和視訊聊天通話。不再需要使用專屬 IP 電話。

要使用此架構，需要在遠端桌面平台上安裝 Microsoft Lync 2013 用戶端，並在 Windows 7 或 8 用戶端端點上安裝 Microsoft Lync VDI 外掛程式。Microsoft Lync 2013 用戶端整合了狀態資訊、即時訊息、網路會議及 Microsoft Office 功能，供客戶們使用。

每當進行 Lync VoIP 或視訊聊天通話時，Lync VDI 外掛程式會將所有媒體處理工作從資料中心伺服器卸載至用戶端端點，並將所有的媒體編碼為 Lync 最佳化的音訊與視訊轉碼器。這項最佳化的架構具有高度的延展性、能減少網路頻寬的使用，並提供點對點的媒體傳遞，而且支援高品質的即時 VoIP 與視訊。如需詳細資訊，請參閱有關 VMware Horizon 6 和 Microsoft Lync 2013 的白皮書，網址為 http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf。

備註 尚未支援音訊的錄製。只有 PCoIP 或 Blast Extreme 顯示通訊協定支援這項整合。

商務用 Skype

使用者可以使用商務用 Skype 在虛擬桌面平台內進行最佳化音訊和視訊通話，而不會影響虛擬基礎結構的效能以及使網路超載。在 Skype 語音和視訊通話期間，所有媒體處理皆會在用戶端機器上執行，而不是在虛擬桌面平台中執行。

依預設會在 Windows 版 Horizon Client (4.6 及更新版本)、Linux 版 Horizon Client (4.6 及更新版本) 以及 Mac 版 Horizon Client (4.7 及更新版本) 安裝程式的執行過程中安裝「商務用 Skype 的虛擬化套件」軟體。Horizon 管理員也必須在 Horizon Agent 安裝期間於虛擬桌面平台上安裝「商務用 Skype 的 VMware 虛擬化套件」功能。如需詳細資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件。若要設定商務用 Skype，請參閱《在 Horizon 7 中設定遠端桌面平台功能》文件。

整合 Horizon 7 與商業智慧軟體

您可以設定 Horizon 連線伺服器，將事件記錄到 Microsoft SQL Server 或 Oracle 資料庫。

- 使用者動作，例如登入和啟動桌面工作階段。
- 管理員動作，例如新增權利和建立桌面集區。
- 報告系統失敗和錯誤的警示。
- 統計抽樣，例如記錄 24 小時期間內的最高使用者人數。

您可以使用商業智慧報告引擎 (例如 Crystal Reports、IBM Cognos、MicroStrategy 9 和 Oracle Enterprise Performance Management System)，存取和分析事件資料庫。

如需詳細資訊，請參閱《Horizon 7 整合》文件。

您也可以使用 Syslog 格式產生 Horizon 7 事件，讓分析軟體可以存取事件資料。如果您啟用事件的檔案式記錄，事件會累積在本機記錄檔中。如果您指定檔案共用，記錄檔會移至該共用。如需詳細資訊，請參閱《Horizon 7 安裝》文件。

使用 Horizon PowerCLI Cmdlet 建立管理指令碼

您可以搭配使用 Horizon PowerCLI Cmdlet 與 VMware PowerCLI。您可以使用 Horizon PowerCLI Cmdlet 對 Horizon 元件執行各種管理工作。

如需關於 Horizon PowerCLI Cmdlet 的詳細資訊，請參閱《VMware PowerCLI Cmdlet 參考》。

如需用來建立進階功能和指令碼以用於 Horizon PowerCLI 之 API 規格的相關資訊，請參閱 VMware Developer Center 上的 View API 參考。

如需關於能用來建立自有 Horizon PowerCLI 指令碼之範例指令碼的詳細資訊，請參閱 GitHub 上的 Horizon PowerCLI 社群。

您可以使用 Horizon PowerCLI Cmdlet 在 Horizon 7 元件上執行各種管理工作。

- 建立和更新桌面平台集區。
- 設定多個網路標籤，以大幅擴增指定給集區中虛擬機器的 IP 位址數量。
- 將資料中心資源新增至完整的虛擬機器或連結複製集區。
- 在連結複製桌面上執行重新平衡、重新整理或重新撰寫作業。
- 抽樣檢查特定桌面或桌面平台集區長期的使用情況。
- 查詢事件資料庫。
- 查詢服務狀態。

修改 Horizon 7 中的 LDAP 組態資料

當您使用 Horizon Administrator 修改 Horizon 7 的組態時，在存放庫中適當的 LDAP 資料也會隨之更新。Horizon 連線伺服器會將其組態資訊儲存在與 LDAP 相容的存放庫。例如，如果您新增桌面平台集區，則連線伺服器會將使用者、使用者群組和權利的相關資訊儲存在 LDAP 中。

您可以使用 VMware 和 Microsoft 命令列工具，在 Horizon 7.中，匯出和匯入 LDAP 資料交換格式 (LDIF) 檔案中的 LDAP 組態資料。進階管理員想要使用指令碼更新組態資料，而不使用 Horizon Administrator 或 Horizon PowerCLI 時，可使用這些命令。

您可以使用 LDIF 檔案執行許多工作。

- 在連線伺服器執行個體之間傳輸組態資料。
- 定義大量的 Horizon 7 物件 (例如桌面平台集區)，並將其新增至連線伺服器執行個體，而不需使用 Horizon Administrator 或 Horizon PowerCLI。
- 備份組態，以便您可以還原連線伺服器執行個體的狀態。

如需詳細資訊，請參閱《Horizon 7 整合》文件。

使用 vdmadmin 命令

您可以使用 `vdmadmin` 命令列介面，在連線伺服器執行個體上執行各種管理工作。您可以使用 `vdmadmin` 執行無法從 Horizon Administrator 使用者介面中執行的管理工作，或執行必須從指令碼自動執行的管理工作。

如需詳細資訊，請參閱《Horizon 7 管理》文件。

規劃豐富的使用者經驗

2

Horizon 7 提供使用者所期待的熟悉、個人化桌面環境。例如，在某些用戶端系統上，使用者可存取連線至本機電腦的 USB 及其他裝置、將文件傳送到本機電腦可偵測到的任何一台印表機、透過智慧卡驗證，以及使用多部顯示監視器。

Horizon 7 包含許多您可能想要提供給使用者的功能。在決定要使用哪些功能之前，您必須先瞭解每項功能的限制和規定。

本章節討論下列主題：

Horizon Agent 的功能支援對照表

計畫要開放讓使用者使用哪些顯示通訊協定和功能時，請使用以下資訊判斷哪一個代理程式 (遠端桌面平台和應用程式) 作業系統支援此功能。

哪些類型和版本的客體作業系統受支援，取決於 Windows 版本。如需受支援 Windows 10 作業系統的清單更新，請參閱 VMware 知識庫 (KB) 文章 http://kb.vmware.com/kb/2149393。針對 Windows 10 以外的 Windows 作業系統，請參閱 VMware 知識庫 (KB) 文章 http://kb.vmware.com/kb/2150295。

若要檢視安裝 Horizon Agent 的 Windows 作業系統所支援的特定遠端體驗功能清單，請參閱 VMware 知識庫 (KB) 文章 http://kb.vmware.com/kb/2150305。

備註 如需有關多種不同類型的用戶端裝置所支援的功能資訊，請參閱 Horizon Client 說明文件，網址為 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

此外，還有一些 VMware 合作夥伴提供支援 Horizon 7 部署的精簡型和零用戶端裝置。每個精簡型或零用戶端裝置可用的功能，取決於企業選擇採用的廠商、機型和組態。如需精簡型和零用戶端裝置的廠商和機型相關資訊，請參閱 VMware 網站上提供的《VMware 相容性指南》。

選擇顯示通訊協定

顯示通訊協定可為使用者提供圖形化介面，來存取資料中心內的遠端桌面平台或應用程式。根據您使用的用戶端裝置類型，您可以從 VMware 提供的 Blast Extreme 和 PCoIP (PC-over-IP)，或 Microsoft RDP (遠端桌面通訊協定) 中做選擇。

您可以設定原則來控制要使用的通訊協定，或是允許使用者在登入桌面時選擇通訊協定。

備註 某些類型的用戶端既不會使用 PCoIP，也不會使用 RDP 遠端顯示通訊協定。例如，如果您使用 HTML Access 功能提供的 HTML Access 用戶端，則會使用 Blast Extreme 通訊協定，而非 PCoIP 或 RDP。同樣地，如果您使用遠端 Linux 桌面平台，則會使用 Blast Extreme。

VMware Blast Extreme

VMware Blast Extreme 已針對行動雲端最佳化，可支援最多種具有 H.264 功能的用戶端裝置。在所有顯示通訊協定中，VMware Blast 所耗用的 CPU 資源最少，因此能讓行動裝置的電池壽命延長。VMware Blast Extreme 可抵消延遲的增加或頻寬的縮減，並可同時運用 TCP 和 UDP 網路傳輸。

VMware Blast 顯示通訊協定可用於在 RDS 主機上使用虛擬機器或共用工作階段桌面平台的已發佈應用程式和遠端桌面平台。RDS 主機可以是實體機器，也可以是虛擬機器。除了 Windows 10 RS4 Enterprise 版及更新版本組建之外，VMware Blast 顯示通訊協定不會在單一使用者實體電腦上運作。

備註 執行 Windows 10 RS4 的實體電腦不支援「電影與電視」應用程式。

VMware Blast Extreme 功能

VMware Blast Extreme 的主要功能包括：

- 在公司防火牆外的使用者可使用此通訊協定搭配公司的虛擬私人網路 (VPN)，或者使用者可以在公司 DMZ 中，建立與安全伺服器或 Access Point 應用裝置間的安全加密連線。
- 支援進階加密標準 (AES) 128 位元加密，且預設為啟動狀態。不過，您可以將加密金鑰密碼變更為 AES-256。
- 來自所有用戶端裝置類型的連線。
- 在 LAN 和 WAN 減少頻寬使用量的最佳化控制。

- Windows 代理程式上使用 PerfMon 顯示的效能計數器會精準呈現系統目前的狀態，並以固定速率更新下列項目：
  - Blast 工作階段
  - 影像處理
  - 音訊
  - CDR
  - USB：如果將 USB 流量設定為使用 VMware 虛擬通道 (VVC)，則在 Windows 代理程式上使用 PerfMon 顯示的 USB 計數器為有效。
  - 商務用 Skype：計數器僅用於控制流量。
  - 剪貼簿
  - RTAV
  - 序列埠和掃描器重新導向功能
  - 虛擬列印
  - HTML5 MMR
  - Windows Media MMR：在您設定此功能以使用 VMware 虛擬通道 (VVC) 後，才會顯示效能計數器。
- Windows 用戶端上發生短暫網路中斷期間的網路持續性。
- 虛擬顯示器支援 32 位元色彩。
- 支援 ClearType 字型。
- 使用 LAN 和 WAN 的動態音訊品質調整進行的音訊重新導向。
- 在部分用戶端類型上，用於網路攝影機和麥克風的即時音訊視訊。
- 在用戶端作業系統與遠端桌面平台或已發佈的應用程式之間複製與貼上文字及映像 (適用於部分用戶端)。對於其他用戶端類型，僅支援複製與貼上純文字。您無法複製並貼上系統物件，例如系統之間的資料夾和檔案。
- 部分用戶端類型支援多部監視器。在部分用戶端上，針對停用 Aero 的 Windows 7 遠端桌面平台，您最多可使用每個顯示器解析度達 2560 x 1600 的 4 部監視器，或者最多 3 部 4K (3840 x 2160) 解析度的監視器。此外，也支援樞紐顯示與自動調整。

  啟用 3D 功能時，最多支援 2 部解析度達 1920 x 1200 的監視器，或者解析度為 4K (3840 x 2160) 的 1 部監視器。
- 部分用戶端類型支援 USB 重新導向。
- 部分 Windows 用戶端作業系統和部分遠端桌面平台作業系統 (安裝有 Horizon Agent) 支援 MMR 重新導向。
- 支援使用 NVIDIA 圖形卡連線至未連結監視器的實體機器。如需最佳效能，請使用支援 H.264 編碼的圖形卡。

如果您有擴充式分立 GPU 和內嵌 GPU，則作業系統可能會預設為使用內嵌 GPU。若要修正此問題，您可在裝置管理員中停用或移除裝置。如果問題仍存在，您可為內嵌 GPU 安裝 WDDM 圖形驅動程式，或在系統 BIOS 中停用內嵌 GPU。如需停用內嵌 GPU 方法的相關資訊，請參閱系統說明文件。

注意 停用內嵌 GPU 可能會造成未來無法使用某些功能，例如失去 BIOS 設定或 NT 開機載入器的主控台存取權。

- Blast 轉碼器透過提供更銳利的影像與字型，改善了調適性及 H.264 編碼器在桌面平台中的使用方式，且運作就像視訊轉碼器 (具有動作偵測、動作向量和畫面間預測的巨集區塊) 一樣。以下環境支援轉碼器，且依預設會停用：
  - Windows 和 Linux 代理程式。若要啟用轉碼器：
    - 在 Windows 代理程式上，設定登錄機碼：`HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderBlastCodecEnabled = 1`
    - 在 Linux 代理程式上，於 `\etc\vmware\config` 下方設定 `RemoteDisplay.allowBlastCodec=TRUE`
  - 在 Windows、Linux 和 MacOS 用戶端設定上停用 H.264。行動用戶端和 Web 用戶端不支援此功能。
- 動態編碼器切換可讓您在視訊最佳化編碼器 (H.264 4:2:0 或 H.264 4:4:4) 與文字最佳化編碼器 (Blast 轉碼器或調適性) 之間切換。此切換功能可協助維持清晰的文字和視訊，並減少頻寬使用量。若要使用此功能，請啟用編碼器切換：
  - 在 Windows 代理程式上，設定登錄機碼 `HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderSwitchEnabled = 1`
  - 在 Linux 代理程式上，於 `\etc\vmware\config` 下方設定 `RemoteDisplay.allowSwitchEncoder=TRUE`
  - 啟用 Blast 轉碼器，此依預設為停用。如果未啟用 Blast 轉碼器，則切換編碼器會使用調適性來進行文字最佳化編碼。
  - 在 Windows、Linux 和 MacOS 用戶端設定上啟用 H.264。行動用戶端和 Web 用戶端不支援此功能。

備註 編碼器切換僅會使用軟體 H.264，不支援硬體加速的圖形。

如需哪些用戶端裝置支援特定 VMware Blast Extreme 功能的相關資訊，請至 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

網路喚醒

使用 Windows 10 RS4 Enterprise 版及更新版本的實體機器支援網路喚醒。使用此功能，使用者可在與 Horizon Connection Server 連線時喚醒實體機器。網路喚醒功能具有這些先決條件：

- 僅 IPv4 環境支援網路喚醒 (WoL)。
- 在 BIOS 設定及網路卡設定中啟用網路喚醒時，必須將實體機器設定為在接收網路喚醒封包時喚醒。
- 目的地連接埠 9 會用於來自連線伺服器的 WoL 封包。

- WoL 封包是一種 IP 導向廣播封包，在從 Horizon Connection Server 傳送時必須能夠到達 Horizon Agent。這些案例中的網路喚醒功能：
  - 連線伺服器和實體機器上的 Horizon Agent 位於 LAN 環境中的相同子網路上。
  - 連線伺服器和 Horizon Agent 之間的所有路由器皆已進行設定，以允許 IP 導向廣播封包用於您要喚醒實體機器的目標子網路。

備註 網路喚醒功能不支援實體 Windows 10 代理程式的浮動指派集區。僅將 WoL 封包傳送至授權給特定使用者的專用指派集區。

建議的客體作業系統設定

以高畫質、全螢幕模式播放，或播放 720p 或更高格式的視訊時，建議使用 1GB RAM 或更高容量以及雙 CPU。若要為圖形密集的應用程式 (例如 CAD 應用程式) 使用虛擬專用圖形加速，需要 4 GB 的 RAM。

視訊品質需求

480p 格式的視訊	當遠端桌面平台具備單一虛擬 CPU 時，您可以使用 480p (含) 以下的原始解析度播放視訊。如果您要以高畫質 Flash 或全螢幕模式播放視訊，則桌面平台需要雙虛擬 CPU。即使是使用雙虛擬 CPU 桌面，低至 360p 格式的視訊以全螢幕播放時，仍可能會落後於音訊，尤其在 Windows 用戶端上更是如此。
720p 格式的視訊	如果遠端桌面平台具備雙虛擬 CPU，您可以使用 720p 的原始解析度播放視訊。如果您以 720p 的高解析度或全螢幕模式播放視訊，效能可能會受到影響。
1080p 格式的視訊	如果遠端桌面平台具備雙虛擬 CPU，您可以播放 1080p 格式的視訊，但媒體播放器可能需要調整成較小的視窗大小。
3D 轉譯	您可以設定遠端桌面平台來使用軟體或硬體加速圖形。軟體加速圖形功能可讓您在不需要實體圖形處理單元 (GPU) 的情況下，執行 DirectX 9 和 OpenGL 2.1 應用程式。硬體加速圖形功能使虛擬機器能夠在 vSphere 主機上共用實體 GPU (圖形處理單元)，或將實體 GPU 提供給單一虛擬桌面平台。 針對 3D 應用程式，最多支援 2 部監視器，而最大螢幕解析度為 1920 x 1200。遠端桌面平台上的客體作業系統必須是 Windows 7 或更新版本。 如需有關 3D 功能的詳細資訊，請參閱使用 3D 圖形應用程式。

用戶端系統的硬體需求

如需特定類型桌面平台或行動用戶端裝置之處理器與記憶體需求的相關資訊，請前往 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

PCoIP

PCoIP (PC over IP) 會透過最佳化的桌面平台體驗來提供已發佈的應用程式或整個遠端桌面平台環境，包括為 LAN 或整個 WAN 上的廣大使用者，提供應用程式、影像、音訊以及視訊內容。PCoIP 可以補償延遲的增加或頻寬的減少，以確保使用者在任何網路條件下都能維持產能。

對於已發佈的應用程式和使用虛擬機器、包含 Teradici 主機卡之實體機器的遠端桌面平台，或 RDS 主機上的共用工作階段桌面平台，可以使用 PCoIP 顯示通訊協定。

PCoIP 功能

PCoIP 的主要功能包括：

- 在公司防火牆外的使用者可使用此通訊協定搭配公司的虛擬私人網路 (VPN)，或者使用者可以在公司 DMZ 中，建立與安全伺服器或 Access Point 應用裝置間的安全加密連線。
- 支援進階加密標準 (AES) 128 位元加密，且預設為啟動狀態。不過，您可以將加密金鑰密碼變更為 AES-256。
- 來自所有用戶端裝置類型的連線。
- 在 LAN 和 WAN 減少頻寬使用量的最佳化控制。
- 虛擬顯示器支援 32 位元色彩。
- 支援 ClearType 字型。
- 使用 LAN 和 WAN 的動態音訊品質調整進行的音訊重新導向。
- 在部分用戶端類型上，用於網路攝影機和麥克風的即時音訊視訊。
- 在用戶端作業系統與遠端桌面平台或已發佈的應用程式之間複製與貼上文字及映像 (適用於部分用戶端)。對於其他用戶端類型，僅支援複製與貼上純文字。您無法複製並貼上系統物件，例如系統之間的資料夾和檔案。
- 部分用戶端類型支援多部監視器。在部分用戶端上，針對停用 Aero 的 Windows 7 遠端桌面平台，您最多可使用每個顯示器解析度達 2560 x 1600 的 4 部監視器，或者最多 3 個 4K (3840 x 2160) 解析度的監視器。此外，也支援樞紐顯示與自動調整。

  啟用 3D 功能時，最多支援 2 部解析度達 1920 x 1200 的監視器，或者解析度為 4K (3840 x 2160) 的 1 部監視器。
- 部分用戶端類型支援 USB 重新導向。
- 部分 Windows 用戶端作業系統和部分遠端桌面平台作業系統 (安裝有 Horizon Agent) 支援 MMR 重新導向。

如需支援特定 PCoIP 功能之桌面平台作業系統的相關資訊，請參閱 Horizon Agent 的功能支援對照表。

如需哪些用戶端裝置支援特定 PCoIP 功能的相關資訊，請至 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

建議的客體作業系統設定

以高畫質、全螢幕模式播放，或播放 720p 或更高格式的視訊時，建議使用 1GB RAM 或更高容量以及雙 CPU。若要為圖形密集的應用程式 (例如 CAD 應用程式) 使用虛擬專用圖形加速，需要 4 GB 的 RAM。

視訊品質需求

480p 格式的視訊

當遠端桌面平台具備單一虛擬 CPU 時，您可以使用 480p (含) 以下的原始解析度播放視訊。如果您要以高畫質 Flash 或全螢幕模式播放視訊，則桌面平台需要雙虛擬 CPU。即使是使用雙虛擬 CPU 桌面，低至 360p 格式的視訊以全螢幕播放時，仍可能會落後於音訊，尤其在 Windows 用戶端上更是如此。

720p 格式的視訊

如果遠端桌面平台具備雙虛擬 CPU，您可以使用 720p 的原始解析度播放視訊。如果您以 720p 的高解析度或全螢幕模式播放視訊，效能可能會受到影響。

1080p 格式的視訊

如果遠端桌面平台具備雙虛擬 CPU，您可以播放 1080p 格式的視訊，但媒體播放器可能需要調整成較小的視窗大小。

3D 轉譯

您可以設定遠端桌面平台來使用軟體或硬體加速圖形。軟體加速圖形功能可讓您在不需要實體圖形處理單元 (GPU) 的情況下，執行 DirectX 9 和 OpenGL 2.1 應用程式。硬體加速圖形功能使虛擬機器能夠在 vSphere 主機上共用實體 GPU (圖形處理單元)，或將實體 GPU 提供給單一虛擬機器桌面平台。

對於 3D 應用程式，最多可支援 2 部監視器，且最大螢幕解析度為 1920 x 1200。遠端桌面平台上的客體作業系統必須為 Window 7 或更新版本。

如需有關 3D 功能的詳細資訊，請參閱使用 3D 圖形應用程式。

用戶端系統的硬體需求

如需處理器與記憶體需求的相關資訊，請參閱特定類型桌面或行動用戶端裝置的「使用 VMware Horizon Client」文件。請前往 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

Microsoft RDP

遠端桌面通訊協定是許多人用來從家用電腦存取其工作電腦的相同多通道通訊協定。Microsoft 遠端桌面連線 (RDC) 使用 RDP 來傳輸資料。

Microsoft RDP 是受支援的顯示通訊協定，適用於使用虛擬機器、實體機器的遠端桌面平台，或 RDS 主機上共用工作階段的桌面平台。(已發佈的應用程式僅支援 PCoIP 顯示通訊協定和 VMware Blast 顯示通訊協定。)Microsoft RDP 提供下列功能：

- RDP 7 擁有真正的多監視器支援，最多可達 16 部監視器。
- 您可以在本機系統和遠端桌面平台之間複製並貼上文字和系統物件，例如資料夾和檔案。
- 虛擬顯示器支援 32 位元色彩。
- RDP 支援 128 位元加密。

- 在公司防火牆外的使用者可使用此通訊協定搭配公司的 Virtual Private Network (VPN)，或者使用者可以在公司 DMZ 中，建立與 View 安全伺服器間的安全加密連線。

若要支援對 Windows 7 和 Windows Server 2008 R2 的 TLSv1.1 和 TLSv1.2 連線，您必須套用 Microsoft Hotfix KB3080079。

用戶端系統的硬體需求

如需處理器與記憶體需求的相關資訊，請參閱特定類型用戶端系統的「使用 VMware Horizon Client」文件。請前往 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

備註 行動用戶端 3.x 裝置僅使用 PCoIP 顯示通訊協定。行動用戶端 4.x 用戶端僅使用 PCoIP 顯示通訊協定或 VMware Blast 顯示通訊協定。

使用已發佈的應用程式

您可以使用 Horizon Client 安全地存取已發佈的 Windows 應用程式 (遠端桌面平台除外)。

透過此功能，使用者在啟動 Horizon Client 並登入 Horizon 7 Server 之後，可以查看他們有權使用的所有已發佈應用程式 (遠端桌面平台除外)。選取應用程式可在本機用戶端裝置上為其開啟視窗，這樣該應用程式的外觀與行為就如同其安裝在本機上一樣。

例如，在 Windows 用戶端電腦上，如果您最小化應用程式視窗，該應用程式的項目會保留在工作列，並且看起來與安裝在本機 Windows 電腦上一樣。您也可以為應用程式建立一個捷徑，該捷徑會顯示在您的用戶端桌面平台上，正如本機安裝的應用程式捷徑一樣。

以這種方式部署已發佈的應用程式，可能會比在下列情況下部署完整遠端桌面平台更好：

- 如果透過多層架構設定應用程式，則使用已發佈的應用程式會是一個不錯的解決方案，因為在此架構中，如果元件在地理位置上彼此靠近，運作將更為順暢。

  例如，當使用者必須遠端存取資料庫時，如果大量資料必須透過 WAN 傳輸，效能通常會受到影響。透過已發佈的應用程式，應用程式的所有元件都可以位於與資料庫相同的資料中心中，以便隔離流量，且只有畫面更新會透過 WAN 傳送。
- 從行動裝置中，存取個別應用程式比開啟遠端 Windows 桌面平台，然後導覽至應用程式更方便。

若要使用該功能，您要在 Microsoft RDS 主機上安裝應用程式。在這方面，Horizon 7 已發佈的應用程式與其他應用程式遠端處理解決方案的運作方式相似。Horizon 7 已發佈的應用程式使用 Blast Extreme 顯示通訊協定或 PCoIP 顯示通訊協定來提供，以提供最佳使用者經驗。

使用 Horizon Persona Management 保留使用者資料和設定

您可以使用 Horizon Persona Management 搭配遠端桌面平台，以及未由 Horizon 7 管理的實體電腦和虛擬機器。角色管理會保留使用者對其設定檔所做的變更。使用者設定檔包含各種使用者產生的資訊。

- 無論使用者登入哪一個桌面，使桌面外觀維持不變的使用者專屬資料和桌面設定。
- 應用程式資料與設定。例如，這些設定可讓應用程式記住工具列位置和喜好設定。
- 由使用者應用程式設定的 Windows 登錄項目。

為有效提供這些功能，角色管理會要求 CIFS 共用儲存區大於或等於使用者本機設定檔的大小。

將登入和登出所需時間縮至最短

角色管理可盡量縮短登入與登出桌面平台所需的時間。登入期間，Horizon 7 預設只會下載 Windows 所需的檔案，例如使用者登錄檔案。Horizon 7 會記錄遠端桌面平台上設定檔的最近變更，並定期將變更複製到遠端存放庫。

您可以使用角色管理避免對 Active Directory 進行任何變更，以便讓設定檔受到管理。若要設定 Persona Management，請指定中央存放庫，但不要變更 Active Directory 中的使用者內容。您可以利用這個中央存放庫，管理某一個環境中的使用者設定檔，而不會影響到使用者可能也會登入的實體機器。

使用角色管理時，如果您佈建含有 VMware ThinApp 應用程式的桌面平台，則 ThinApp 沙箱資料也會儲存在使用者設定檔中。此資料可以隨使用者漫遊，但不會明顯影響到登入時間。此策略可以更有效地提供保護，防止資料遺失或損毀。

組態選項

您可以在數個層級設定 Horizon 7 角色：單一遠端桌面平台、桌面平台集區、OU 或您的部署中的所有遠端桌面平台。您也可以在未由 Horizon 7 管理的實體電腦和虛擬機器上使用獨立版本的角色管理。

您可以藉由設定群組原則 (GPO)，細微地控制角色中要包含的檔案和資料夾。您可以指定是否包含本機設定資料夾、登入時所要載入的檔案、在使用者登入後要在背景中下載的檔案，以及使用者角色內要使用 Windows 漫遊設定檔功能 (而非角色管理) 來管理的檔案。

對於 Windows 漫遊設定檔，您可以設定資料夾重新導向。您可以將以下的資料夾重新導向至網路共用。

連絡人	我的文件	儲存遊戲
Cookie	我的音樂	搜尋
桌面平台	我的圖片	搜尋功能表
下載	我的影片	啟動項目
我的最愛	網路上的芳鄰	範本
歷程記錄	印表機芳鄰	Temporary Internet File
連結	最近的項目	

限制

角色管理具有下列限制和規定：

- 即時複製桌面平台集區上不支援此功能。
- 您必須擁有包含角色管理元件的 Horizon 7 授權。
- 角色管理需要 CIFS (Common Internet File System) 共用。
- 不支援將此功能用於 Windows 10 連結複製桌面平台集區上的持續性磁碟。

將 USB 裝置與遠端桌面平台和應用程式搭配使用

管理員可以設定從虛擬桌面平台使用 USB 裝置的功能，例如隨身碟、相機、VoIP (voice-over-IP) 裝置和印表機。這項功能稱為 USB 重新導向。一個虛擬桌面平台最多可容納 255 部 USB 裝置。

您也可以將特定本機連接的 USB 裝置重新導向，以在已發佈桌面平台和應用程式中使用。如需支援的特定類型裝置的相關資訊，請參閱《在 Horizon 7 中設定遠端桌面平台功能》文件。

在單一使用者機器上部署的桌面平台集區中使用此功能時，連結至本機用戶端系統的大多數 USB 裝置可以在遠端桌面平台中使用。您甚至可以透過遠端桌面平台連線至 iPad 並進行管理。例如，您可以使 iPad 與遠端桌面平台安裝的 iTunes 同步。在某些用戶端裝置 (如 Windows 和 Mac 電腦) 上，USB 裝置會在 Horizon Client 的功能表中列出。您可以使用該功能表來連線與中斷連線裝置。

在大多數情況下，不能同時使用用戶端系統和遠端桌面平台中的 USB 裝置。僅幾種 USB 裝置類型可以在遠端桌面平台與本機電腦之間共用。這些裝置包括智慧卡讀卡機和人機介面裝置 (例如鍵盤和指向裝置)。

管理員可以指定允許使用者連線的 USB 裝置類型。對於包含多種裝置 (例如視訊輸入裝置和儲存裝置) 類型的複合式裝置，管理員可以在某些用戶端系統上分割裝置，以允許使用某一種裝置 (例如視訊輸入裝置)，但不允許使用另一種裝置 (例如儲存裝置)。

USB 重新導向功能僅適用於特定類型的用戶端。若要瞭解特定用戶端是否支援此功能，請參閱 Horizon Client 安裝和設定文件中所包含針對該用戶端的功能支援對照表。

使用網路攝影機和麥克風的即時音訊視訊功能

透過即時音訊視訊功能，您將可在遠端桌面平台或已發佈的應用程式中使用本機用戶端系統的網路攝影機或麥克風。即時音訊視訊功能與標準會議應用程式和瀏覽器型視訊應用程式相容。它支援標準網路攝影機、音訊 USB 裝置以及類比音訊輸入。

使用者可在遠端桌面平台中執行 Skype、Webex、Google Hangouts 及其他線上會議應用程式。此功能將視訊和音訊資料重新導向至代理程式機器時所需的頻寬，低於使用 USB 重新導向時的所需頻寬。利用即時音訊視訊，網路攝影機影像和音訊輸入會在用戶端系統上進行編碼，然後傳送至代理程式機器。在代理程式機器上，虛擬網路攝影機和虛擬麥克風可以解碼並播放可供第三方應用程式使用的串流。

此時無須進行特殊組態，但管理員可設定代理程式端的群組原則和登錄機碼，以設定畫面播放速率和影像解析度，或關閉功能。依預設，在每秒 15 個畫面時的解析度為 320 x 240 像素。如有需要，管理員也可使用用戶端組態設定來設定偏好的網路攝影機或音訊裝置。

備註 此功能僅適用於部分類型的用戶端。若要瞭解特定類型的用戶端是否支援此功能，請參閱安裝和設定文件中包含的功能支援對照表，以取得特定類型的桌面平台或行動用戶端裝置的相關資訊。

使用 3D 圖形應用程式

Blast Extreme 或 PCoIP 顯示通訊協定提供的軟體和硬體加速圖形功能，可讓遠端桌面平台使用者執行一些 3D 應用程式，例如 Google Earth、CAD 和其他需要圖形密集運算的應用程式。

NVIDIA GRID vGPU (共用的 GPU 硬體加速)	vSphere 6.0 及更新版本提供這項功能，可讓 ESXi 主機上的實體 GPU (圖形處理單元) 在虛擬機器之間共用。如果您需要高端、硬體加速的工作站圖形處理能力，請使用此功能。
使用 vDGA 的 AMD Multiuser GPU	vSphere 6.0 和更新版本有提供這項功能，其會將 GPU 當成多個 PCI 傳遞裝置，以讓多台虛擬機器共用 AMD GPU。這項功能提供靈活的硬體加速的 3D 設定檔，範圍從輕量型 3D 任務工作者到高端的工作站圖形進階使用者都有。
虛擬專用圖形加速 (vDGA)	vSphere 5.5 Update 2 及更新版本提供這項功能，可讓 ESXi 主機上的單一實體 GPU 專用於一台虛擬機器。如果您需要高端、硬體加速的工作站圖形處理能力，請使用此功能。 **備註** 有些 Intel vDGA 卡需要特定版本的 vSphere 6。請參閱 http://www.vmware.com/resources/compatibility/search.php 上的 VMware 硬體相容性清單。此外，和其他廠商一樣，Intel vDGA 使用 Intel 整合的 GPU，而非使用分立的 GPU。
虛擬共用圖形加速 (vSGA)	vSphere 5.5 Update 2 及更新版本提供這項功能，可讓多台虛擬機器共用 ESXi 主機上的實體 GPU。您可以使用 3D 應用程式進行設計以及製作模型和多媒體。
軟體 3D	vSphere 5.5 Update 2 及更新版本提供軟體加速圖形處理功能，讓您無需使用實體 GPU 就能執行 DirectX 9 和 OpenGL 2.1 應用程式。此功能適合資源需求較少的 3D 應用程式，例如 Windows Aero 主題、Microsoft Office 2010 和 Google Earth。

在 Microsoft RDS 主機上執行的已發佈應用程式現在也可支援 NVIDIA GRID vGPU 和 vDGA。

重要 如需 3D 轉譯的各種選擇和需求的詳細資訊，請參閱關於圖形加速的 VMware 白皮書、VMware Horizon 6.1 的 NVIDIA GRID vGPU 部署指南，以及 NVIDIA GRID 虛擬 GPU 使用者指南。

將多媒體串流到遠端桌面平台

適用於 Windows 7 和 Windows 8/8.1 桌面平台和用戶端的 Windows Media MMR (多媒體重新導向) 功能，在多媒體檔案以串流形式傳送至遠端桌面平台時，可在 Windows 用戶端電腦上實現完全逼真的播放。

運用 MMR，可處理多媒體串流，即在 Windows 用戶端系統上進行解碼。用戶端系統會播放媒體內容，所以可卸載 ESXi 主機的需求。Windows Media Player 支援的媒體格式均有支援；例如：M4V；MOV；MP4；WMP；MPEG-4 Part 2；WMV 7、8 和 9；WMA；AVI；ACE；MP3；WAV。

備註 您必須將 MMR 連接埠加入防火牆軟體的例外清單中。MMR 的預設連接埠為 9427。

從遠端桌面平台列印

藉由虛擬列印功能，某些用戶端系統上的使用者可以從遠端桌面平台使用本機或網路印表機，而無需在遠端桌面平台作業系統中安裝額外的列印驅動程式。藉由隨選列印功能，可以將遠端桌面平台對應至最靠近端點用戶端裝置的印表機。

使用虛擬列印時，在本機用戶端電腦上新增印表機之後，會將該印表機自動新增至遠端桌面平台上的可用印表機清單中。無需進一步進行組態設定。對於每部透過此功能而可使用的印表機，您可以設定資料壓縮、列印品質、雙面列印和顏色等項目的喜好設定。擁有管理員權限的使用者仍可在遠端桌面平台上安裝印表機驅動程式，而不會與虛擬列印元件產生衝突。

本機印表機重新導向專為下列使用案例而設計：

- 直接連線至用戶端裝置上 USB 或序列埠的印表機
- 特殊印表機，例如連線至用戶端的條碼印表機和標籤印表機
- 遠端網路上無法從虛擬工作階段定址的網路印表機。

若要將列印工作傳送至 USB 印表機，您可以使用 USB 重新導向功能或虛擬列印功能。

藉由隨選列印功能，IT 組織可以將遠端桌面平台對應至最靠近端點用戶端裝置的印表機。例如，就像醫師巡視醫院病房一樣，每當醫師列印文件時，該列印工作就會傳送至最近的印表機。若要使用此功能，必須在遠端桌面平台上安裝正確的印表機驅動程式。

備註 只有某些類型的用戶端可以使用這些列印功能。若要瞭解特定類型的用戶端是否支援列印功能，請參閱特定類型的桌面平台或行動用戶端裝置的安裝和設定指南中所包含的功能支援對照表。前往 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

使用 Single Sign-On 來登入

單一登入 (SSO) 功能讓使用者只需提供 Active Directory 登入認證一次。

如果不使用單一登入功能，則使用者必須登入兩次。系統會先提示使用者輸入 Active Directory 認證以登入 Horizon 連線伺服器，然後再提示他們登入遠端桌面平台。如果還使用了智慧卡，一般使用者必須登入三次，因為當智慧卡讀卡機提示使用者輸入 PIN 時，使用者也必須登入。

針對遠端桌面平台，此功能包含認證提供者動態連結程式庫。

True SSO

有了 True SSO 功能，使用者完全不再需要提供 Active Directory 認證。當使用者利用任何非 AD 方法 (例如，RSA SecurID 或 RADIUS 驗證) 登入 VMware Identity Manager 後，就不會再提示使用者也輸入 Active Directory 認證，以便使用遠端桌面平台或應用程式。

如果使用者利用智慧卡或 Active Directory 認證進行驗證，就不需要 True SSO 功能，但您可以設定即使在這種情況下也要使用 True SSO。如此便會忽略使用者提供的 AD 認證並使用 True SSO。

True SSO 的運作方式是透過產生獨特短期憑證來用於 Windows 登入程序。您必須設定憑證授權機構 (如果還沒有的話) 以及憑證註冊伺服器，以便代表使用者產生短期憑證。您可以藉由執行連線伺服器安裝程式並選取 [註冊伺服器] 選項來安裝註冊伺服器。

True SSO 會區隔驗證 (驗證使用者的身分識別) 與存取 (例如存取 Windows 桌面平台或應用程式)。使用者認證會使用數位憑證來保護。不會在資料中心內儲存或傳送密碼。如需詳細資訊，請參閱《Horizon 7 管理》文件。

監視器和螢幕解析度

您可以將遠端桌面平台延伸至多台監視器。若您擁有高解析度監視器，您可以使用高解析度來檢視遠端桌面平台或應用程式。

您可以選取 [所有監視器] 顯示模式，以在多台監視器上顯示遠端桌面平台。如果您正在使用 [所有監視器] 模式且按一下 [最小化] 按鈕，則當您再將視窗放到最大時，視窗將回復為 [所有監視器] 模式。同樣地，如果您正在使用 [全螢幕] 模式且將視窗最小化，則當您將視窗放到最大時，視窗將在某台監視器上回復為 [全螢幕] 模式。

在多台監視器設定中使用所有監視器

不論顯示通訊協定為何，使用遠端桌面平台時您可使用多台監視器。如果您的 Horizon Client 使用所有監視器，而且您將應用程式視窗最大化，則視窗只會展開至包含該應用程式之監視器的全螢幕。

Horizon Client 支援下列監視器組態：

- 當您使用兩台監視器時，這些監視器不必處於相同模式。例如，如果您使用的筆記型電腦與外部監視器連接，則這台外部監視器可為直向模式或橫向模式。
- 螢幕可以並排擺放、兩層各兩台的堆疊，或是當您僅使用兩台監視器、且總高度低於 4096 像素時，便可以垂直堆疊。
- 若要使用 3D 轉譯功能，您必須使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定。您最多可以使用兩台監視器，解析度可高達 1920 X 1200。若是 4K (3840 X 2160) 解析度，則僅支援一台監視器。
- 可透過 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定，支援 4K (3840 x 2160) 的遠端桌面平台畫面解析度。支援的 4K 顯示器數目取決於桌面平台虛擬機器的硬體版本以及 Windows 版本。

硬體版本	Windows 版本	支援的 4K 顯示器數目
10 (ESXi 5.5.x 相容)	7、8、8.x、10	1
11 (ESXi 6.0 相容)	7 (停用 3D 轉譯功能和 Windows Aero)	3
11	7 (啟用 3D 轉譯功能)	1
11	8、8.x、10	1
13 或 14	7、8、8.x、10 (啟用 3D 轉譯功能)	1
13 或 14	7、8、8.x、10	4

- 如果使用 Microsoft RDP 7，則可用來顯示遠端桌面平台的監視器數量上限為 16。

- 如果使用 Microsoft RDP 顯示通訊協定，則遠端桌面平台必須安裝 Microsoft 遠端桌面連線 (RDC) 6.0 或更新版本。

在多台監視器設定中使用一台監視器

如果您有多台監視器，但是只想要 Horizon Client 使用其中一台監視器，您可以選擇在 [所有監視器] 以外的任何模式中開啟遠端桌面平台視窗。依預設會在主要監視器上開啟視窗。如需詳細資訊，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。

使用高解析度模式

在某些類型的用戶端上，當您使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定時，Horizon Client 也支援極高解析度，適用於那些配備高解析度顯示器的用戶端系統。啟用高解析度模式的選項僅在用戶端系統支援高解析度顯示器時才會顯示。

依預設，硬體編碼會在您於虛擬機器中設定 vGPU 之後啟用。除了使用小於 1 GB 視訊記憶體的 vGPU 設定檔將因為 NVENC 記憶體限制而使用軟體解碼器以外，硬體編碼已針對所有支援的多台監視器組態啟用。請參閱 https://docs.nvidia.com/grid/4.3/grid-vgpu-release-notes-vmware-vsphere/index.html 中的〈NVENC 至少需要 1 GB 的框架緩衝區〉。

從中央位置管理桌面平台和應用程式集區

3

您可以建立包含一個或成百上千個遠端桌面平台的集區。虛擬機器、實體機器與 Windows 遠端桌面服務 (RDS) 主機可以用作桌面平台來源。建立一個虛擬機器做為基礎映像，Horizon 7 即可從該映像產生遠端桌面平台集區。您也可以建立能為使用者提供應用程式遠端存取權的應用程式集區。

本章節討論下列主題：

桌面平台集區的優點

Horizon 7 提供可建立和佈建桌面平台集區的功能，作為集中化管理的基礎。

您可以從下列其中一個來源建立遠端桌面平台集區：

- 實體系統，例如實體桌上型電腦。
- 在 ESXi 主機上主控並由 vCenter Server 管理的虛擬機器
- 在虛擬化平台上而不是在支援 Horizon Agent 的 vCenter Server 上執行的虛擬機器。
- RDS 主機上的工作階段型桌面平台。如需關於從 RDS 主機建立桌面平台集區的詳細資訊，請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件。

如果您使用 vSphere 虛擬機器作為桌面來源，則可以自動執行程序來建立所需數量的相同虛擬桌面。您可以設定集區要產生的虛擬桌面數目下限與上限。設定這些參數可確保您始終有足夠的遠端桌面平台可立即使用，但不會多到導致過度使用可用資源。

使用集區管理桌面平台可讓您套用設定或部署應用程式到集區中的所有遠端桌面平台。下列範例顯示部分可用的設定：

- 指定要使用哪一個遠端顯示通訊協定做為遠端桌面平台的預設值，以及是否允許使用者覆寫此預設值。

- 針對 View Composer 連結複製虛擬機器或完整複製虛擬機器，指定虛擬機器不使用時是否要關閉其電源，以及是否要一併刪除虛擬機器。即時複製虛擬機器的電源永遠會開啟。
- 針對 View Composer 連結複製虛擬機器，您可以指定是要使用 Microsoft Sysprep 自訂規格還是 VMware 的 QuickPrep。Sysprep 會為集區的每一個虛擬機器產生唯一 SID 和 GUID。即時複製需使用 VMware 的不同自訂規格 (稱為 ClonePrep)。

您也可以指定在集區中指派桌面平台給使用者的方式。

專用指派集區	會指派特定遠端桌面平台給每個使用者，使用者每次登入時都會返回同一個虛擬桌面平台。專用指派集區需要一對一的桌面平台對使用者關係。例如，100 個使用者的群組需要 100 個桌面平台的集區。
浮動指派集區	使用浮動指派集區也可以讓您建立桌面平台集區，供多組使用者使用。例如，如果使用者一次以 100 位使用者為一組輪班工作，則一個包含 100 個桌面的集區可供 300 位使用者使用。每次使用之後會選擇刪除並重新建立遠端桌面平台，以提供嚴格控制的環境。

應用程式集區的優點

使用應用程式集區，您可授與使用者存取在資料中心內的伺服器上，而非在他們個人的電腦或裝置上所執行之應用程式的權限。

應用程式集區有多項優點：

- 可存取性

  使用者可以在任何位置從網路存取應用程式。您也可以設定安全的網路存取。

- 裝置獨立性

  透過應用程式集區，您可以支援一系列用戶端裝置，例如智慧型手機、平板電腦、筆記型電腦、精簡型用戶端和個人電腦。這些用戶端裝置可在多種作業系統上執行，例如 Windows、iOS、Mac OS 或 Android。

- 存取控制

  您可以便捷地授與、移除使用者或使用者群組對應用程式的存取權。

- 加速部署

  透過應用程式集區，可加快應用程式部署的速度，因為您只需要在資料中心的伺服器上部署應用程式，而每個伺服器可支援多個使用者。

- 管理能力

  管理部署在用戶端電腦和裝置上的軟體一般需要大量資源。管理工作包含部署、設定、維護、支援和升級。透過應用程式集區，您可以簡化企業中的軟體管理，因為軟體執行於資料中心內的伺服器上，且需要較少的已安裝複本。

- 安全性與合規性

透過應用程式集區，您可以提高安全性，因為應用程式及其關聯的資料集中位於資料中心內。集中式資料可解決安全性與合規性的問題。

- 降低成本

  視軟體授權合約而定，在資料中心內主控應用程式最具成本效益。其他因素 (包含加速部署和提高管理能力) 也可以降低企業的軟體成本。

減少和管理儲存需求

部署由 vCenter Server 管理的虛擬機器上的桌面平台，可提供以往只有虛擬化伺服器才能辦到的所有儲存效率。使用即時複製或 Composer 連結複製作為桌面平台機器可節省更多的儲存空間，因為集區中的所有虛擬機器會共用具有基礎映像的虛擬磁碟。

- 透過 vSphere 管理儲存

  vSphere 可讓您虛擬化磁碟區和檔案系統，如此一來，您便可以管理和設定儲存，而不需要考量實際儲存資料的位置。

- 將 VMware vSAN 用於高效能儲存與原則式管理

  VMware VMware vSAN 是軟體定義的儲存層 (在 vSphere 5.5 Update 2 或更新版本中提供)，可虛擬化 vSphere 主機叢集上提供的本機實體儲存磁碟。建立自動桌面平台集區或自動伺服器陣列時只需指定一個資料存放區，各種元件 (例如虛擬機器檔案、複本、使用者資料及作業系統檔案) 即會放置在適當的固態硬碟 (SSD) 或直接連結硬碟 (HDD) 上。

- 將虛擬磁碟區用於以虛擬機器為中心的儲存與原則式管理

  在使用 vSphere 6.0 或更新版本隨附的虛擬磁碟區 (VVol) 的情況下，個別虛擬機器 (而非資料存放區) 會變成儲存管理單位。儲存硬體會取得虛擬磁碟內容、配置和管理的控制權。

- 透過 Composer 減少儲存需求

  由於 Composer 建立的桌面映像會與基礎映像共用虛擬磁碟，因此可以降低所需儲存容量達 50 至 90%。

- 透過即時複製減少儲存需求

  即時複製功能可利用 vSphere vmFork 技術 (隨附於 vSphere 6.0U1 和更新版本) 來靜止執行中的基礎映像或父虛擬機器，並快速建立及自訂虛擬桌面平台的集區。

透過 vSphere 管理儲存

vSphere 可讓您虛擬化磁碟區和檔案系統，如此一來，您便可以管理和設定儲存，而不需要考量實際儲存資料的位置。

光纖通道 SAN 陣列、iSCSI SAN 陣列和 NAS 陣列是廣泛使用的儲存技術，vSphere 支援這些技術以達成各種資料中心的儲存需求。儲存陣列會透過儲存區域網路，在伺服器群組間連線並共用。這樣的配置可以匯集儲存資源，並提供更多的彈性，將儲存資源佈建到虛擬機器。

相容的 vSphere 5.5 Update 2 或更新版本功能

運用 vSphere 5.5 Update 2 或更新版本，您可以使用 vSAN，它可將 ESXi 主機上提供的本機實體固態硬碟與硬碟機，虛擬化為叢集內所有主機共用的單一資料存放區。vSAN 提供高效能儲存和原則式管理，因此您可以在建立桌面平台集區時僅指定一個資料存放區，各種元件 (例如虛擬機器檔案、複本、使用者資料及作業系統檔案) 即會放置在適當的固態硬碟 (SSD) 或直接連結硬碟 (HDD) 上。

vSAN 還可讓您透過使用儲存區原則設定檔來管理虛擬機器儲存和效能。如果因為主機、磁碟、網路故障或工作負載變更而無法遵循原則，vSAN 會重新設定受影響之虛擬機器的資料，並在叢集範圍內最佳化資源的使用。您可以在包含最多 20 台 ESXi 主機的叢集上部署桌面平台集區。

vSAN 支援需要共用儲存區的 VMware 功能 (例如 HA、vMotion 與 DRS)，不再需要外部共用儲存區，並簡化了儲存區組態與虛擬機器佈建活動。

重要 vSphere 6.0 及更新版本提供的 vSAN 功能包含許多效能方面的改進。在 vSphere 6.0 中，此功能也具有更廣泛的 HCL (硬體相容性) 支援。如需 vSphere 6 或更新版本中關於 vSAN 的詳細資訊，請參閱《管理 VMware vSAN》文件。

備註 vSAN 與 View 儲存加速器功能相容，但與空間效率高的磁碟格式功能 (該功能會對磁碟進行清除與壓縮以回收磁碟空間) 不相容。

透過 vSphere 5.5 Update 2 或更新版本，您可以使用以下功能：

- 您可以使用 View 儲存加速器功能，設定 ESXi 主機快取虛擬機器磁碟資料。

  在許多機器同時啟動並執行防毒掃描的開機風暴期間，使用這個內容型讀取快取 (CBRC) 可減少 IOPS 並改善效能。主機可以從快取讀取共同的資料區塊，而不是從儲存系統一再讀取整個作業系統。
- 如果遠端桌面平台使用隨 vSphere 5.1 及更新版本提供的空間效率高的磁碟格式，則會透過清除與壓縮程序，自動回收客體作業系統內過時或已刪除的資料。
- 複本磁碟必須儲存在 VMFS5 或更新的資料存放區或 NFS 資料存放區。如果將複本儲存在比 VMFS5 還舊的 VMFS 版本上，則叢集最多只能有八個主機。作業系統磁碟和持續性磁碟可以儲存在 NFS 或 VMFS 資料存放區上。

相容的 vSphere 6.0 或更新版本功能

在 vSphere 6.0 或更新版本中，您可以使用虛擬磁碟區 (VVol)。此功能將虛擬磁碟及其衍生物、複製品、快照以及複本直接對應到儲存區系統上的物件 (稱為虛擬磁碟區)。此對應允許 vSphere 卸載密集儲存作業，例如儲存區系統的快照、複製以及複寫。

虛擬磁碟區還可讓您透過使用 vSphere 中的儲存區原則設定檔來管理虛擬機器儲存和效能。這些儲存區原則設定檔可根據每個虛擬機器控制儲存服務。這種細微佈建類型可提升容量使用率。您可以在包含最多 32 個 ESXi 主機的叢集上部署桌面平台集區。

備註 虛擬磁碟區與 View 儲存加速器功能相容，但與空間效率高的磁碟格式功能 (該功能會對磁碟進行清除與壓縮以回收磁碟空間) 不相容。

備註 即時複製不支援 Virtual Volumes。

將 VMware vSAN 用於高效能儲存與原則式管理

VMware VMware vSAN 是軟體定義的儲存層 (在 vSphere 5.5 Update 2 或更新版本中提供)，可虛擬化 vSphere 主機叢集上提供的本機實體儲存磁碟。建立自動桌面平台集區或自動伺服器陣列時只需指定一個資料存放區，各種元件 (例如虛擬機器檔案、複本、使用者資料及作業系統檔案) 即會放置在適當的固態硬碟 (SSD) 或直接連結硬碟 (HDD) 上。

vSAN 對儲存管理實作原則式方法。使用 vSAN 時，Horizon 7 會以預設儲存區原則設定檔的形式定義虛擬機器儲存區需求 (例如容量、效能和可用性)，並針對虛擬桌面平台自動將其部署至 vCenter Server 上。原則會自動針對每一磁碟 (vSAN 物件) 個別套用，且會在虛擬桌面平台的整個生命週期內進行維護。會根據指派的原則佈建和自動設定儲存區。您可以在 vCenter 中修改這些原則。Horizon 會針對連結複製桌面平台集區、即時複製桌面平台集區、完整複製桌面平台集區或每一 Horizon 叢集的自動伺服器陣列建立 vSAN 原則。

您可以為 vSAN 叢集啟用加密，以加密 vSAN 資料存放區中的所有待用資料 (支援所有的 Horizon 7 桌面平台集區類型)。vSAN 加密適用於 vSAN 6.6 或更新版本。如需有關加密 vSAN 叢集的詳細資訊，請參閱《VMware vSAN》說明文件。

每部虛擬機器都會保留其原則，不論在叢集內的實體位置如何，都是如此。如果因主機、磁碟、網路故障或工作負載變更而無法遵循原則，vSAN 會重新設定受影響虛擬機器的資料，並執行負載平衡以符合每部虛擬機器的原則。

vSAN 支援需要共用儲存區的 VMware 功能 (例如 HA、vMotion 與 DRS)，不再需要外部共用儲存區基礎結構，並簡化了儲存區組態與虛擬機器佈建活動。

重要 相較於 vSphere 5.5 Update 2，vSphere 6.0 及更新版本提供的 vSAN 功能在效能方面有許多改進。在 vSphere 6.0 中，此功能也具有更廣泛的 HCL (硬體相容性) 支援。此外，VMware vSAN6.0 也支援將 Flash 型裝置同時用於快取和永續性儲存的全 Flash 架構。

需求與限制

在 Horizon 7 部署中使用時，vSAN 功能具有以下限制：

- 此版本不支援使用 Horizon 7 空間效率高的磁碟格式功能，該功能會對磁碟進行清除與壓縮以回收磁碟空間。
- vSAN 不支援 View Composer Array Integration (VCAI) 功能，因為 vSAN 不使用 NAS 裝置。

備註 vSAN 與 View 儲存加速器功能相容。vSAN 可在 SSD 磁碟上提供快取層，而且 View 儲存加速器功能可提供內容型快取 (可在開機風暴期間降低 IOPS 並提高效能)。

vSAN 功能具有下列的需求：

- vSphere5.5 Update 2 或更新版本。
- 適當的硬體。例如，VMware 建議採用 10GB NIC，每個提供容量的節點至少使用一個 SSD 與一個 HDD。若要瞭解詳情，請參閱 VMware 相容性指南。
- 至少三部 ESXi 主機構成的叢集。您需要有足夠的 ESXi 主機來支應您的設定，即使您使用兩個具有 vSAN 延伸叢集的 ESXi 主機，仍是如此。如需詳細資訊，請參閱《vSphere 組態上限》文件。

- SSD 容量 (至少為 HDD 容量的 10%)。
- 足夠數量的 HDD (以順利完成安裝)。磁碟的使用量請勿超過 75%。

如需關於 vSAN 需求的詳細資訊，請參閱《vSphere 5.5 Update 2 儲存區》文件中的〈使用 vSAN〉。若為 vSphere 6 或更新版本，請參閱《管理 VMware vSAN》文件。如需為 VMware vSAN 調整和設計 Horizon 7 虛擬桌面平台基礎結構的關鍵元件的指導方針，請參閱位於 http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf 的白皮書。

將虛擬磁碟區用於以虛擬機器為中心的儲存與原則式管理

在使用 vSphere 6.0 或更新版本隨附的虛擬磁碟區 (VVol) 的情況下，個別虛擬機器 (而非資料存放區) 會變成儲存管理單位。儲存硬體會取得虛擬磁碟內容、配置和管理的控制權。

在使用虛擬磁碟區的情況下，抽象儲存容器取代了以 LUN 或 NFS 共用為基礎的傳統儲存磁碟區。虛擬磁碟區會將虛擬磁碟及其衍生物、複製品、快照和複本直接對應至儲存區系統上的物件 (稱為虛擬磁碟區)。透過此對應，vSphere 得以將消耗大量資源的儲存作業 (例如快照、複製和複寫) 卸載至儲存區系統。因此，舉例來說，原先需要一小時的複製作業，現在透過虛擬磁碟區只需幾分鐘的時間。

重要 虛擬磁碟區的主要好處之一，是能夠使用軟體原則式管理 (SPBM)。但就此版本而言，Horizon 7 並不會建立 vSAN 所建立的預設精細儲存區原則。您可以在 vCenter Server 中設定會套用至所有虛擬磁碟區資料存放區的全域預設儲存區原則。

虛擬磁碟區具有下列優點：

- 虛擬磁碟區支援將多項作業卸載到儲存硬體。這些作業包括建立快照、複製和 Storage DRS。
- 在使用虛擬磁碟區的情況下，您可以在個別虛擬磁碟上使用進階儲存服務，包括複寫、加密、重複資料刪除和壓縮。
- 虛擬磁碟區支援 vMotion、Storage vMotion、快照、連結複製、Flash Read Cache 和 DRS 等 vSphere 功能。
- 您可以將虛擬磁碟區搭配支援 vSphere APIs for Array Integration (VAAI) 的儲存陣列使用。

需求與限制

在 Horizon 7 部署中使用時，虛擬磁碟區功能具有以下限制：

- 此版本不支援使用 Horizon 7 空間效率高的磁碟格式功能，該功能會對磁碟進行清除與壓縮以回收磁碟空間。
- 虛擬磁碟區不支援使用 View Composer Array Integration (VCAI)。
- Virtual Volumes 資料存放區不支援用於即時複製桌面平台集區。

備註 虛擬磁碟區與 View 儲存加速器功能相容。vSAN 可在 SSD 磁碟上提供快取層，而且 View 儲存加速器功能可提供內容型快取 (可在開機風暴期間降低 IOPS 並提高效能)。

虛擬磁碟區功能的需求如下：

- vSphere 6.0 或更新版本。

- 適當的硬體。某些儲存裝置廠商會負責提供可與 vSphere 整合的儲存裝置提供者，並提供虛擬磁碟區的支援。每個儲存裝置提供者都必須經過 VMware 認證和適當部署。
- 在虛擬資料存放區上佈建的所有虛擬磁碟必須是 1 MB 的偶數倍。

虛擬磁碟區是一種 vSphere 6.0 功能。如需有關需求、功能、背景和設定需求的詳細資訊，請參閱《vSphere 儲存區》文件中有關虛擬磁碟區的主題。

透過 Composer 減少儲存需求

由於 Composer 建立的桌面映像會與基礎映像共用虛擬磁碟，因此可以降低所需儲存容量達 50 至 90%。

Composer 使用基礎映像或父虛擬機器，可建立包含多達 2,000 個連結複製虛擬機器的集區。每個連結複製會像獨立桌面般運作，具有唯一主機名稱和 IP 位址，但連結複製需要的儲存空間極少。

複本和連結複製在相同資料存放區

當您建立 Microsoft RDS 主機的連結複製桌面平台集區或伺服器陣列時，將會先從父虛擬機器進行完整複製。此完整複製 (或稱複本) 以及與其連結複製可以放在同一個資料存放區或 LUN (邏輯單元編號)。如有必要，您可以使用重新平衡功能將複本和連結複製桌面平台集區從一個 LUN 移到另一個 LUN，或者將連結複製桌面平台集區移到 vSAN 資料存放區，或從 vSAN 資料存放區移到 LUN。

複本和連結複製在不同資料存放區

您也可以將 Composer 複本和連結複製放在具有不同效能特性的單獨資料存放區。例如，您可以將複本虛擬機器儲存在固態硬碟 (SSD) 上。固態硬碟具有低儲存容量和高讀取效能，一般是每秒支援數萬個 I/O (IOPS)。您可以將連結複製儲存在搭載傳統、旋轉媒體的資料存放區。這類磁碟的效能較低，但具有價位低、儲存容量高的特色，因此很適合用來儲存大型集區中的多個連結複製。您可以使用分層儲存組態，用符合成本效益的方式處理密集 I/O 情況，例如同時重新啟動多個虛擬機器或執行排定的防毒掃描。

如需詳細資訊，請參閱標題為 VMware View 的儲存考量的最佳做法指南。

如果您使用 vSAN 資料存放區或虛擬磁碟區資料存放區，您將無法針對複本和連結複製手動選取不同的資料存放區。因為 vSAN 和虛擬磁碟區功能會將物件自動放到適當類型的磁碟和所有 I/O 作業的快取上，所以無需為 vSAN 和虛擬磁碟區的資料存放區使用複本分層。

用於分頁檔和暫存檔的可處置磁碟

建立連結複製集區或伺服器陣列時，您也可以選擇設定另外的可處置虛擬磁碟，來儲存使用者工作階段期間產生的客體作業系統分頁檔與暫存檔。關閉虛擬機器電源後，會刪除可處置的磁碟。使用可處置的磁碟會使連結複製的成長速度變慢，並減少已關閉電源之虛擬機器所用的空間，因此可節省儲存空間。

用於專用桌面的持續性磁碟

建立專用指派桌面平台集區時，Composer 也可以選擇性地為每個虛擬桌面平台建立個別的虛擬磁碟。使用者的 Windows 設定檔和應用程式資料會儲存在持續性磁碟上。重新整理、重新撰寫或重新平衡連結複製時，持續性磁碟的內容會保留下來。VMware 建議您將 Composer 持續性磁碟存放在單獨的資料存放區。然後，您可以備份保存持續性磁碟的整個 LUN。

用於浮動、無狀態桌面的本機資料存放區

連結複製桌面可以儲存在本機資料存放區，這是 ESXi 主機的內部備用磁碟。本機儲存區提供多項優點，例如便宜的硬體、快速的虛擬機器佈建、高效能電源作業，以及簡易的管理。不過，使用本機儲存區會限制可供您使用的 vSphere 基礎結構組態選項。使用本機儲存區只對特定的環境有益，其他環境則不適用。

備註 如上一節關於 vSAN 的說明，本節所述的限制不適用於同樣使用本機儲存區磁碟但需要特定硬體的 vSAN 資料存放區。

本機資料存放區可能最適合用於環境中的遠端桌面平台為無狀態的情況。例如，若您部署無狀態 kiosk 或教室和培訓站，則可使用本機資料存放區。

如果您打算利用本機儲存的優點，則必須審慎考量下列限制：

- 無法使用 VMotion、VMware High Availability (HA) 或 vSphere Distributed Resource Scheduler (DRS)。
- 無法使用 Composer 重新平衡作業，使整個資源集區中的虛擬機器負載平衡。
- 無法在個別資料存放區上儲存 Composer 複本和連結複製，且實際上，VMware 建議您將其儲存在同一個磁碟區。

若您藉由控制虛擬機器的數量和磁碟成長來管理本機磁碟使用情形，以及使用浮動指派並定期執行重新整理和刪除作業時，則可順利地將連結複製部署至本機資料存放區。

如需詳細資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中關於建立桌面平台集區的章節。

透過即時複製減少儲存需求

即時複製功能可利用 vSphere vmFork 技術 (隨附於 vSphere 6.0U1 和更新版本) 來靜止執行中的基礎映像或父虛擬機器，並快速建立及自訂虛擬桌面平台的集區。

即時複製不僅會在建立時與父虛擬機器共用虛擬磁碟，即時複製也會共用父系的記憶體。每個即時複製會像獨立桌面平台般運作，具有唯一主機名稱和 IP 位址，但即時複製需要的儲存空間極少。即時複製可將所需的儲存容量減少 50% 至 90%。在建立複製時，也會減少整體記憶體需求。如需關於儲存區需求和調整大小限制的詳細資訊，請參閱 VMware 知識庫 (KB) 文章 https://kb.vmware.com/kb/2150348。

從 Horizon 7(7.8 版) 開始，即時複製已可支援 vSAN 資料存放區的 vSphere TRIM 和 UNMAP 功能。

複本和即時複製在相同資料存放區

建立即時複製桌面平台集區時，會先從主要虛擬機器建立完整複製。此完整複製 (或稱複本) 以及與其連結複製可以放在同一個資料存放區或 LUN (邏輯單元編號)。

複本和即時複製在不同資料存放區

您也可以將即時複製複本和即時複製放在具有不同效能特性的單獨資料存放區。例如，您可以將複本虛擬機器儲存在固態硬碟 (SSD) 上。固態硬碟具有低儲存容量和高讀取效能，一般是每秒支援數萬個 I/O (IOPS)。

您可以將即時複製儲存在搭載傳統、旋轉媒體所支援的資料存放區。這類磁碟的效能較低，但具有價位低、儲存容量高的特色，因此很適合用來儲存大型集區中的多個即時複製。您可以使用分層儲存組態，用符合成本效益的方式處理密集 I/O 情況，例如同時執行排定的防毒掃描。

如果使用 vSAN 資料存放區，您將無法針對複本和即時複製手動選取不同的資料存放區。因為 vSAN 會將物件自動放到適當類型的磁碟上並快取所有 I/O 作業，所以無需為 vSAN 資料存放區使用複本分層。vSAN 資料存放區上支援即時複製集區。

在本機資料存放區上儲存即時複製

即時複製虛擬機器可儲存在本機資料存放區上，這是 ESXi 主機的內部備用磁碟。本機儲存區提供多項優點，例如便宜的硬體、快速的虛擬機器佈建、高效能電源作業，以及簡易的管理。不過，使用本機儲存區會限制可供您使用的 vSphere 基礎結構組態選項。使用本機儲存區只對特定 Horizon 7 環境有益，其他環境則不適用。

備註 本主題所述的限制不適用於同樣使用本機儲存區磁碟但需要特定硬體的 vSAN 資料存放區。

當環境中的 Horizon 7 桌面平台處於無狀態的情況下，本機資料存放區最有可能發揮良好效益。例如，若您部署無狀態 kiosk 或教室和培訓站，則可使用本機資料存放區。

如果您的虛擬機器有浮動指派、並非專屬於個別使用者，且可定期刪除或重新整理 (如使用者登出時)，則可考慮使用本機資料存放區。此方式可以讓您控制每個本機資料存放區的磁碟使用情形，而無須在資料存放區之間移動虛擬機器，或是對虛擬機器進行負載平衡。

不過，您必須考慮使用本機資料存放區對 Horizon 7 桌面平台或伺服器陣列部署所造成的限制：

- 您無法使用 VMotion 來管理虛擬磁碟區。
- 您不能使用 VMware High Availability。
- 您不能使用 vSphere Distributed Resource Scheduler (DRS)。

  如果您要將即時複製部署在使用本機資料存放區的單一 ESXi 主機上，則必須設定包含該單一 ESXi 主機的叢集。如果您的叢集具有兩個以上使用本機資料存放區的 ESXi 主機，請從叢集中的每個主機選取本機資料存放區。否則，即時複製建立會失敗。此行為不同於使用 Composer 連結複製時的本機資料存放區行為。
- 您無法將複本和即時複製儲存在不同的資料存放區上。
- 若您選取本機旋轉磁碟機，其效能可能不及市售的儲存陣列。本機旋轉磁碟機和儲存陣列的容量可能大致相同，但本機旋轉磁碟機的輸送量卻不同於儲存陣列。輸送量會隨著主軸數量的增加而提升。若您選取直接連結的固態磁碟 (SSD)，其效能可能會超越許多儲存陣列的效能。
- 若您想要利用本機儲存區的好處，您必須仔細考慮無法使用 VMotion、高可用性、DRS 及其他功能的後果。若您藉由控制虛擬機器的數量和磁碟成長來管理本機磁碟使用情形，同時使用浮動指派並定期執行重新整理和刪除作業，則可順利地將即時複製部署至本機資料存放區。
- 即時複製的本機資料存放區支援適用於虛擬桌面平台和已發佈的桌面平台。

即時複製和 Composer 連結複製之間的差異

即時複製的建立速度比連結複製快很多，因此當您在佈建即時複製集區時，將不再需要下列連結複製功能：

- 即時複製集區不支援使用可處置的個別虛擬磁碟來儲存客體作業系統的分頁和暫存檔案的組態。每次使用者登出即時複製桌面平台時，Horizon 7 都會自動刪除複製，並根據集區可用的最新作業系統映像，佈建另一個即時複製並開啟其電源。在登出作業期間將自動刪除任何客體作業系統的分頁和暫存檔案。
- 即時複製集區不支援為每個虛擬桌面平台建立個別的持續性虛擬磁碟。您可以改為將使用者的 Windows 設定檔和應用程式資料儲存在 App Volumes 的使用者可寫入磁碟上。當使用者登入時，使用者的可寫入磁碟會連結至即時複製桌面平台。此外，使用者的可寫入磁碟也可用於保存使用者安裝的應用程式。
- 由於即時複製桌面平台具有存留期短的本質，即時複製在其抹除和壓縮程序中，並不支援空間效率高的磁碟格式 (SE 疏鬆)。
- 即時複製桌面平台集區與 Storage vMotion 相容。Composer 連結複製桌面平台集區與 Storage vMotion 不相容。

應用程式佈建

Horizon 7 提供數個有關應用程式佈建的選項：您可以使用傳統的應用程式佈建技術、可以提供已發佈的應用程式而非遠端桌面平台、可以散佈使用 VMware ThinApp 建立的應用程式套件、可以將應用程式部署為 View Composer 或即時複製基礎映像的一部分，或者也可以使用 App Volumes 連結應用程式。

- 使用 RDS 主機部署個別應用程式

  您可以選擇為使用者提供已發佈的應用程式，而非遠端桌面平台。個別已發佈的應用程式可能更容易在小型行動裝置上導覽。

- 使用 View Composer 部署應用程式和系統更新

  由於連結複製桌面集區會共用一個基礎映像，因此您可以更新父虛擬機器，來快速部署更新和修補程式。

- 使用即時複製部署應用程式和系統更新

  由於即時複製桌面平台集區會共用一個基礎映像，因此您可以更新父虛擬機器，來快速部署更新和修補程式。

- 管理 Horizon Administrator 中的 VMware ThinApp 應用程式

  VMware ThinApp™ 可讓您將應用程式封裝至單一檔案，以便在虛擬化的應用程式沙箱中執行。此策略可使應用程式佈建作業具有彈性，且不會發生衝突。

- 使用 App Volumes 部署和管理應用程式

  VMware App Volumes 透過在作業系統之上虛擬化應用程式，提供另一種應用程式管理方式。藉由使用此策略，應用程式、資料檔案、設定、中介軟體和組態可作為單獨的分層式容器。

- 使用現有程序或 VMware Mirage 進行應用程式佈建

  透過 Horizon 7，您不僅可以繼續使用公司目前採用的應用程式佈建技術，還可以使用 Mirage。另有兩點需要考量：管理伺服器 CPU 使用率和儲存 I/O，以及決定是否允許使用者安裝應用程式。

使用 RDS 主機部署個別應用程式

您可以選擇為使用者提供已發佈的應用程式，而非遠端桌面平台。個別已發佈的應用程式可能更容易在小型行動裝置上導覽。

使用者可使用與之前用於存取遠端桌面平台的相同 Horizon Client 來存取遠端 Windows 系統的應用程式，並使用相同的 Blast Extreme 或 PCoIP 顯示通訊協定。

若要提供已發佈的應用程式，請在 Microsoft 遠端桌面工作階段 (RDS) 主機上安裝該應用程式。一或多個 RDS 主機構成一個伺服器陣列，而伺服器陣列管理員則從中以建立桌面平台集區類似的方式建立應用程式集區。如需調整伺服器陣列大小建議，請參閱 VMware 知識庫 (KB) 文章 http://kb.vmware.com/kb/2150348。

使用此策略可簡化新增、移除和更新應用程式；新增或移除應用程式的使用者權利；並提供可從任何裝置或網路對集中式或分散式應用程式伺服器陣列進行存取的權限。

使用 View Composer 部署應用程式和系統更新

由於連結複製桌面集區會共用一個基礎映像，因此您可以更新父虛擬機器，來快速部署更新和修補程式。

透過重新撰寫功能可以對父虛擬機器進行變更、擷取新狀態的快照，然後將新版本的映像推送至所有使用者和桌面或推送至使用者和桌面的子集。您可以將此功能用於下列工作：

- 套用作業系統及軟體修補程式和升級
- 套用 Service Pack
- 新增應用程式
- 新增虛擬裝置
- 變更其他虛擬機器設定，例如可用的記憶體

備註 由於您也可以使用 View Composer 建立連結複製 Microsoft RDS 主機的伺服器陣列，因此重新撰寫功能將可讓您更新 RDS 主機上的客體作業系統和應用程式。

您可以建立 View Composer 持續性磁碟，以包含使用者設定及其他使用者產生的資料。此持續性磁碟不會受到重新撰寫作業的影響。刪除連結複製時，可以保留使用者資料。當員工離開公司時，其他員工可以存取離職員工的使用者資料。擁有多個桌面的使用者可以在單一桌面上彙總使用者資料。

如果您想要禁止使用者新增或移除軟體或變更設定，您可以使用重新整理功能，將桌面還原成預設值。此功能也會減少連結複製的大小，連結複製往往會隨時間而不斷增大。

使用即時複製部署應用程式和系統更新

由於即時複製桌面平台集區會共用一個基礎映像，因此您可以更新父虛擬機器，來快速部署更新和修補程式。

推送映像功能可讓您對父虛擬機器進行變更、擷取新狀態的快照，然後定期將新版本的映像推送至所有使用者和桌面平台。透過滾動更新，系統可以盡量縮短與集區維護相關聯的停機時間。使用者登出即時複製虛擬桌面平台時，Horizon 7 會刪除即時複製，並從最新版的映像建立全新的即時複製，而新的複製會準備就緒而可供下一個使用者登入。

您可以將此功能用於下列工作：

- 套用作業系統及軟體修補程式和升級
- 套用 Service Pack
- 新增應用程式
- 新增虛擬裝置
- 變更其他虛擬機器設定，例如可用的記憶體

管理 Horizon Administrator 中的 VMware ThinApp 應用程式

VMware ThinApp™ 可讓您將應用程式封裝至單一檔案，以便在虛擬化的應用程式沙箱中執行。此策略可使應用程式佈建作業具有彈性，且不會發生衝突。

VMware ThinApp 會將應用程式從基礎作業系統及其程式庫和架構中解除，並且將應用程式綁定到稱為應用程式套件的單一執行檔，以進行應用程式虛擬化。您可以使用 Horizon Administrator，將 VMware ThinApp 應用程式散佈到桌面平台和集區。

重要 如果不透過指派給桌面平台和集區的方式來散佈 ThinApp，而是想要將 ThinApp 指派給 Active Directory 使用者和群組，則可以使用 VMware Identity Manager。

使用 VMware ThinApp 建立虛擬化的應用程式之後，您可以選擇從共用檔案伺服器串流應用程式，還是將應用程式安裝在虛擬桌面上。如果您設定虛擬化的應用程式進行串流處理，則必須解決下列幾個架構考量事項：

- 特定使用者群組對特定應用程式存放庫 (即儲存應用程式套件的位置) 的存取權
- 應用程式存放庫的儲存組態
- 串流產生的網路流量主要取決於應用程式的類型

對於串流的應用程式，使用者可使用桌面捷徑啟動應用程式。

如果您指定 ThinApp 套件，使其安裝在虛擬桌面上，則架構考量事項與使用傳統 MSI 型軟體佈建時要解決的考量事項相似。串流的應用程式和安裝在遠端桌面平台中的 ThinApp 套件，兩者都要考量到應用程式存放庫的儲存區組態。

使用 App Volumes 部署和管理應用程式

VMware App Volumes 透過在作業系統之上虛擬化應用程式，提供另一種應用程式管理方式。藉由使用此策略，應用程式、資料檔案、設定、中介軟體和組態可作為單獨的分層式容器。

這些容器在處於唯讀模式時稱為應用程式堆疊 (AppStacks)，在處於讀寫模式時則稱為可寫入磁碟區。管理員可以使用 App Volumes Manager 來建立 AppStacks 並指派應用程式權利，以及提供佈建的 AppStacks 給系統或是使用者或群組。App Volumes 提供之應用程式的外觀與風格就好像是原生安裝一樣，並且會跨工作階段和裝置追隨使用者。管理員可以即時更新或取代應用程式，並可立即、在使用者仍登入時，或是在下一次登入或重新開機時移除任何指派的應用程式。

如需詳細資訊，請參閱 VMware App Volumes 說明文件，網址為 https://docs.vmware.com/tw/VMware-App-Volumes/index.html。

使用現有程序或 VMware Mirage 進行應用程式佈建

透過 Horizon 7，您不僅可以繼續使用公司目前採用的應用程式佈建技術，還可以使用 Mirage。另有兩點需要考量：管理伺服器 CPU 使用率和儲存 I/O，以及決定是否允許使用者安裝應用程式。

如果您將應用程式在同一時間推送到大量的遠端桌面平台，則可能會看到 CPU 使用率和儲存 I/O 明顯突然爆增。這些尖峰工作負載對桌面平台效能有顯著的影響。最佳做法是，將應用程式更新排程在離峰時刻進行，如有可能，並且錯開桌面更新。此外，亦須確認您的儲存解決方式設計是否可支援這樣的工作負載。

如果公司允許使用者安裝應用程式，則可以繼續使用目前的原則，不過就無法利用 View Composer 功能，例如重新整理和重新撰寫桌面。使用 View Composer 時，如果有某個應用程式並未虛擬化，或者並未包含在使用者的設定檔或資料設定，只要 View Composer 執行重新整理、重新撰寫或重新平衡作業，該應用程式就會遭到捨棄。許多情況下，能夠嚴格控制要安裝的應用程式是有好處的。View Composer 桌面容易支援，因為這些桌面保持接近於已知良好的組態。

如果使用者一定要安裝自己的應用程式，並且要在遠端桌面平台使用壽命期間持續存留這些應用程式，您可以使用即時複製搭配 App Volumes，而不需使用 View Composer 佈建應用程式。另一個解決方案是建立完整複製專用的桌面平台，允許使用者安裝應用程式，然後使用 Mirage 來管理和更新桌面平台，而不覆寫使用者安裝的應用程式。

重要 另外，還可使用 Mirage 來管理本機安裝的離線桌面平台及其應用程式。如需詳細資訊，請參閱 Mirage 說明文件頁。

使用 Active Directory GPO 管理使用者和桌面

Horizon 7 包含許多群組原則管理 ADMX 範本，可用來集中管理和設定 Horizon 7 元件和遠端桌面平台。

將這些範本匯入 Active Directory 後，即可使用它們設定原則以套用至下列群組和元件：

- 所有系統，無論登入的使用者是誰
- 所有使用者，無論登入的系統為何
- 連線伺服器組態
- Horizon Client 組態
- Horizon Agent 組態

套用 GPO 之後，內容會儲存在指定元件的本機 Windows 登錄中。

您可以使用 GPO 設定所有可透過 Horizon Administrator 使用者介面 (UI) 使用的原則。您也可以使用 GPO 設定無法透過 UI 使用的原則。如需完整清單以及透過 ADMX 範本提供的設定說明，請參閱《在 Horizon 7 中設定遠端桌面平台功能》。

使用智慧原則

您也可使用智慧原則來建立原則，以控制特定遠端桌面平台上 USB 重新導向、虛擬列印、剪貼簿重新導向、用戶端磁碟機重新導向以及 PCoIP 顯示通訊協定功能的行為。此功能需要 User Environment Manager。

使用智慧原則，您可以建立只在符合特定條件時才生效的原則。例如，您可以設定一個原則，在使用者從公司網路外部連線至遠端桌面平台時，停用用戶端磁碟機重新導向功能。

一般來說，在 User Environment Manager 中為遠端桌面平台功能設定的 Horizon 原則設定，會覆寫對等的登錄機碼以及群組原則設定。

遠端桌面平台部署的架構設計元素和規劃指導方針

4

一般的 Horizon 7 架構設計會使用網繭策略。網繭 (Pod) 定義會隨使用的硬體組態、Horizon 7 和 vSphere 軟體版本，以及其他環境特定設計因素而有不同。

本文件中的範例將說明可順應您企業環境與特殊需求的可擴充設計。本章涵蓋有關記憶體、CPU、儲存容量、網路元件和硬體等需求的重要詳細資料，可讓 IT 架構設計人員和規劃人員實際瞭解部署 Horizon 7 解決方案會涉及到哪些環節。

重要 本章不包含以下主題：

主控應用程式的架構設計	Horizon 7 網繭可支援 Microsoft RDS 主機的伺服器陣列，其中，每個伺服器陣列皆包含 RDS 主機。如需更多資訊，請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》。如果計劃使用 RDS 主機的虛擬機器，另請參閱 RDS 主機虛擬機器組態。
Horizon 7 Agent Direct Connect 外掛程式的架構設計	透過在遠端虛擬機器桌面平台上執行此外掛程式，用戶端可以直接連線到該虛擬機器。所有遠端桌面平台功能，包括 PCoIP、HTML Access、RDP、USB 重新導向和工作階段管理工作，都可以按此方式進行連線，就如同使用者透過 View 連線伺服器進行連線一樣。如需詳細資訊，請參閱《Horizon 7 Agent Direct-Connection 外掛程式管理》。

本章節討論下列主題：

遠端桌面平台的虛擬機器需求

當您規劃遠端桌面平台的規格時，選擇的 RAM、CPU 和磁碟空間會明顯影響到選擇的伺服器和儲存硬體和支出。

- 根據工作者類型進行規劃

  許多組態元素 (包括 RAM、CPU 和儲存大小) 的需求主要取決於使用虛擬桌面的工作者類型，以及必須安裝的應用程式。

- 估計虛擬機器桌面平台的記憶體需求

  對伺服器而言，其 RAM 成本要比電腦的 RAM 成本高。因為 RAM 成本佔整體伺服器硬體成本和所需總儲存容量的比例很高，因此，決定正確的記憶體配置對於規劃桌面部署非常重要。

- 估計虛擬機器桌面平台的 CPU 需求

  估計 CPU 時，您必須收集有關企業中各類型工作者的平均 CPU 使用率資訊。

- 選擇適當的系統磁碟大小

  配置磁碟空間時，請提供正好足夠的空間給作業系統、應用程式以及使用者可能安裝或產生之其他內容使用。通常，這個空間會小於實體電腦配備的磁碟大小。

根據工作者類型進行規劃

許多組態元素 (包括 RAM、CPU 和儲存大小) 的需求主要取決於使用虛擬桌面的工作者類型，以及必須安裝的應用程式。

進行架構規劃時，可將工作者分成幾種類型。

任務工作者	任務工作者和管理工作者會在少數應用程式中執行重複性的工作，通常是使用固定電腦。應用程式通常不是知識工作者所用應用程式那樣需要大量的 CPU 和記憶體資源。特定班次的任務工作者可能會同時全部登入虛擬桌面。任務工作者包括客服中心分析人員、零售店員工、倉庫作業員等等。
知識工作者	知識工作者的每日工作包括存取網際網路、使用電子郵件，以及建立複雜文件、簡報和試算表。知識工作者包括會計人員、銷售經理、行銷研究分析人員等等。
進階使用者	進階使用者包括應用程式開發人員，以及使用需要密集圖形資源之應用程式的人員。
Kiosk 使用者	這些使用者需要共用位於公共區域的桌面平台。Kiosk 使用者的範例包括使用教室共用電腦的學生、護理站的護士，以及用於工作安排與人才招募的電腦。這些桌面需要自動登入。必要時，可透過某些應用程式進行驗證。

估計虛擬機器桌面平台的記憶體需求

對伺服器而言，其 RAM 成本要比電腦的 RAM 成本高。因為 RAM 成本佔整體伺服器硬體成本和所需總儲存容量的比例很高，因此，決定正確的記憶體配置對於規劃桌面部署非常重要。

如果配置的 RAM 過低，則儲存 I/O 可能會因為發生太多的 Windows 分頁而受到負面影響。如果配置的 RAM 過高，則儲存容量可能會因為客體作業系統的分頁檔和各虛擬機器的交換檔和暫停檔變得太大而受到負面影響。

RAM 大小對效能的影響

配置 RAM 時，應避免選擇過度保守的設定。請考量下列幾個事項：

- RAM 配置不足，可導致過多的 Windows 分頁，進而可產生 I/O 導致效能明顯下滑及儲存 I/O 負載增加。
- VMware ESXi 支援精密的記憶體資源管理演算法，例如透通分頁共用 (transparent page sharing) 和記憶體飄移 (memory ballooning) 等，這可明顯減少支援特定客體 RAM 配置所需的實體 RAM。例如，儘管 2GB 可能配置給虛擬桌面，但只會使用該數字之實體 RAM 的其中一小部分而已。
- 由於虛擬桌面效能易受回應時間的影響，所以在 ESXi 主機上，請將 RAM 保留設定設為非零的數值。保留一些 RAM 可確保待機但使用中的桌面決不會被完全交換出到磁碟。這也可以減少 ESXi 交換檔所使用的儲存空間。但是，偏高的保留設定值會影響到 ESXi 主機上過度認可記憶體的能力，並且可能會影響 VMotion 維護作業。

RAM 大小對儲存空間的影響

配置給虛擬機器的 RAM 大小與虛擬機器使用的特定檔案大小直接相關。若要存取下列清單中的檔案，請使用 Windows 客體作業系統尋找 Windows 分頁檔和休眠檔，並使用 ESXi 主機的檔案系統尋找 ESXi 交換檔和暫停檔。

Windows 分頁檔

此檔案的大小預設為客體 RAM 的 150%。此檔案預設位於 `C:\pagefile.sys`，會使精簡佈建的儲存空間因經常存取而變大。在 View Composer 連結複製虛擬機器上，分頁檔和暫存檔可以重新導向至個別的虛擬磁碟，並在虛擬機器關閉電源時，刪除該虛擬磁碟。可處置的分頁檔重新導向可節省空間，減慢連結複製的成長速度，所以能改善效能。雖然可以從 Windows 中調整大小，但是這樣可能會對應用程式效能造成不利影響。

針對即時複製，在登出作業期間將自動刪除任何客體作業系統的分頁和暫存檔案，因此這些檔案不會有時間增長到相當大的程度。每次使用者登出即時複製桌面平台，Horizon 會刪除複製，並根據集區可用的最新作業系統映像，佈建另一個即時複製並開啟其電源。

筆記型電腦的 Windows 休眠檔

此檔案可等於客體 RAM 的 100%。Horizon 部署中並不需要此檔案，因此，您可以安全地將其刪除。

ESXi 交換檔

此檔案的副檔名為 `.vswp`，當保留空間低於 100% 的虛擬機器 RAM 時就會建立此檔案。交換檔的大小等於客體 RAM 的未保留部分。例如，如果保留 50% 的客體 RAM，而客體 RAM 為 2GB，則 ESXi 交換檔就是 1GB。此檔案可以儲存在 ESXi 主機或叢集的本機資料存放區上。

ESXi 暫停檔

此檔案的副檔名為 `.vmss`，如果設定桌面集區登出原則，使虛擬桌面在使用者登出時暫停，便會建立此檔案。此檔案的大小等於客體 RAM 的大小。

使用 PCoIP 或 Blast Extreme 時特定監視器組態的 RAM 大小

除了系統記憶體外，虛擬機器在 ESXi 主機上也需要少量的 RAM，以支應視訊額外負荷。此一 VRAM 大小需求取決於為使用者設定的顯示器解析度和監視器數目。表 4-1. PCoIP 或 Blast Extreme 用戶端顯示額外負荷 列出各種組態所需的額外 RAM 大小。欄中所列的記憶體數量已加上其他 PCoIP 或 Blast Extreme 功能所需的記憶體數量。

表 4-1. PCoIP 或 Blast Extreme 用戶端顯示額外負荷

標準顯示解析度	寬度 (像素)	高度 (像素)	1 部監視器額外負荷	2 部監視器額外負荷	3 部監視器額外負荷	4 部監視器額外負荷
VGA	640	480	1.20MB	3.20MB	4.80MB	5.60MB
WXGA	1280	800	4.00MB	12.50MB	18.75MB	25.00MB
1080p	1920	1080	8.00MB	25.40MB	38.00MB	50.60MB
WQXGA	2560	1600	16.00MB	60.00MB	84.80MB	109.60MB
UHD (4K)	3840	2160	32.00MB	78.00MB	124.00MB	未支援

在計算系統需求時，除了虛擬機器的基本系統 RAM 以外，還要加上 VRAM 的值。當您在 Horizon Administrator 中指定監視器的數目上限並選取顯示器解析度時，會自動計算及設定額外負荷的記憶體。

如果您使用 3D 轉譯功能，並選取 Soft3D 或 vSGA，您可以在用來為 3D 客體設定 VRAM 的 Horizon Administrator 控制項中使用額外的 VRAM 值重新計算。或者，若為 Soft3D 和 vSGA 以外的其他圖形加速類型，如果您選擇使用 vSphere Client 管理 VRAM，您可以指定確切的 VRAM 數量。

根據預設，多監視器組態能夠匹配主機拓撲。此組態已針對兩部以上的監視器預先計算額外負荷，因此能夠應付其他拓撲配置。如果在啟動遠端桌面工作階段時發生螢幕變黑的情況，請確認監視器數目和顯示器解析度的值 (於 Horizon Administrator 中設定) 是否能夠匹配主機系統，或者您也可以在 Horizon Administrator 中選取**使用 vSphere Client 管理**以手動方式調整記憶體數量，然後將視訊記憶體總計值設定為最大值 128 MB。

特定工作負載和作業系統的 RAM 大小

由於所需的 RAM 大小根據工作者的類型差異甚大，因此許多公司會進行試驗階段，來確定其企業中各種工作者集區的正確設定。

配置 1 GB 給 32 位元 Windows 7 或更新版本的桌面平台，以及配置 2 GB 給 64 位元 Windows 7 或更新版本的桌面平台，是很好的起點。如果您要使用其中一個硬體加速圖形功能來完成 3D 工作負載，VMware 建議使用 2 個虛擬 CPU 和 4 GB 的 RAM。在試驗期間，請監控效能以及各種類型工作者所用的磁碟空間，並進行調整，直到找到各工作者集區的最佳設定為止。

估計虛擬機器桌面平台的 CPU 需求

估計 CPU 時，您必須收集有關企業中各類型工作者的平均 CPU 使用率資訊。

CPU 需求會隨工作者類型而有不同。在試驗階段期間，請使用效能監控工具 (例如，在虛擬機器使用 Perfmon、在 ESXi 使用 `esxtop` 或使用 vCenter Server 效能監控工具)，來瞭解這些工作者群組的平均和尖峰 CPU 使用量。另外，請使用下列指導方針：

- 軟體開發人員或其他有高效能需求的進階使用者，在 CPU 的需求上可能比知識工作者和任務工作者要高出許多。如果是 64 位元 Windows 7 虛擬機器，且執行需要大量運算的工作 (例如使用 CAD 應用程式、播放 HD 視訊或驅動 4K 顯示器解析度)，建議使用雙核心或四核心的虛擬 CPU。
- 其他情況通常則建議使用單一虛擬 CPU。

由於許多虛擬機器會在一部伺服器上執行，如果所有代理程式 (例如防毒代理程式) 在同一時間都檢查更新，則 CPU 可能會用量突然爆增。請判斷哪些代理程式以及有多少個代理程式可能引起效能問題，並採用策略解決這些問題。例如，下列策略可能對您的企業所有幫助：

- 使用即時複製或 View Composer 連結複製來更新映像，而不要讓軟體管理代理程式下載軟體更新到各個虛擬桌面。
- 將防毒和軟體更新排在非尖峰時段執行，此時登入的使用者可能較少。
- 錯開或隨機安排執行更新的時間。
- 使用與 VMware vShield API 相容的防毒產品。例如，此 API 已整合至 VMware vCloud® Networking and Security 5.1 及更新版本。

非正式的起始大小規劃方法是，開始時，假設每個虛擬機器需要 1/8 至 1/10 的 CPU 核心作為最低保證運算能力。亦即，規劃使用每一核心 8 至 10 個虛擬機器的試驗。例如，如果您假設每一核心 8 個虛擬機器，並且有 2 個通訊端 8 核心的 ESXi 主機，則可以在試驗期間，於伺服器上託管 128 個虛擬機器。在這段期間，請監控主機的整體 CPU 使用率，並確保其很少超過安全界線 (如 80%)，以提供充分的餘裕空間來因應用量突然爆增情況。

選擇適當的系統磁碟大小

配置磁碟空間時，請提供正好足夠的空間給作業系統、應用程式以及使用者可能安裝或產生之其他內容使用。通常，這個空間會小於實體電腦配備的磁碟大小。

由於資料中心磁碟空間相較於傳統電腦部署的桌上型電腦或筆記型電腦磁碟空間，每一 GB 的成本通常較高，所以請最佳化作業系統映像大小。下列建議可能有助於最佳化映像大小：

- 移除不需要的檔案。例如，減少 Temporary Internet File 的配額。
- 關閉 Windows 服務，例如索引工具服務、磁碟重組工具服務和還原點。如需詳細資料，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件。
- 選擇足以容納未來成長的虛擬磁碟大小，但不宜大到不切實際。
- 使用集中式檔案共用或 View Composer 持續性磁碟或 App Volumes，來儲存使用者產生的內容和使用者安裝的應用程式。
- 如果使用的是 vSphere 5.1 或更新版本，請啟用 vCenter Server 和連結複製桌面平台集區的空間回收。

  如果虛擬機器桌面平台使用隨 vSphere 5.1 或更新版本提供的空間效率高的磁碟格式，則會透過清除與壓縮程序，自動回收客體作業系統內過時或已刪除的資料。

每個虛擬桌面必須考量下列檔案所需的儲存空間大小：

- ESXi 暫停檔等於配置給虛擬機器的 RAM 大小。
- Windows 分頁檔預設等於 150% 的 RAM。
- 每個虛擬機器的記錄檔最多占用 100MB。
- 虛擬磁碟或 .vmdk 檔案必須能容納作業系統、應用程式和未來的應用程式與軟體更新。虛擬磁碟還必須能容納本機使用者資料和使用者安裝的應用程式，如果這些位於虛擬桌面而不是位於檔案共用。

  如果您使用 View Composer，則 .vmdk 檔案會隨時間而增長，但是您可以藉由排程 View Composer 重新整理作業、設定虛擬機器桌面平台集區的儲存過度認可原則，以及將 Windows 分頁檔和暫存檔重新導向到非持續性的獨立磁碟，來控制增長量。

  如果您使用即時複製，.vmdk 檔案會在登入工作階段內隨著時間增長。每當使用者登出時，便會自動刪除即時複製桌面平台，且隨即會建立新的即時複製並準備就緒可供下一個使用者登入。利用此程序，就能夠有效地重新整理桌面平台，使其回到原始大小。

您也可以將這個估計值增加 15%，以確保使用者不會耗盡磁碟空間。

Horizon 7 ESXi 節點

節點即單一 VMware ESXi 主機，用於主控 Horizon 7 部署中的虛擬機器桌面。

當您最大化合併率，即 ESXi 主機主控的桌面數量，Horizon 7 最具成本效益。雖然有許多因素會影響伺服器選擇，但是如果您只要獲得最佳的採購價格，則必須找出處理能力與成本之間能取得適當平衡的伺服器組態。

沒有其他方法西可取代在實際、真正環境的情況下 (例如試驗) 測量效能，以判斷環境和硬體組態的適當合併率。合併率會根據使用模式和環境因素而有很大的差異。請使用下列指導方針：

- 一般來說，請考慮每個 CPU 核心 8 至 10 個虛擬桌面的運算能力。如需瞭解如何計算各虛擬機器的 CPU 需求，請參閱估計虛擬機器桌面平台的 CPU 需求。
- 以虛擬桌面平台 RAM、主機 RAM 和過度認可比率來思考記憶體容量。雖然每個 CPU 核心有 8 到 10 個虛擬桌面平台，但是如果虛擬桌面平台有 1 GB 或更多的 RAM，則必須也審慎考量實體 RAM 需求。如需計算每個虛擬機器所需之 RAM 容量的相關資訊，請參閱估計虛擬機器桌面平台的記憶體需求。

  請注意，實體 RAM 的成本並不是線性的，在某些情況下，採購不使用昂貴 DIMM 晶片的更小伺服器可能符合成本效益。在其他情況下，機架密度、儲存連線能力、管理能力及其他考量都可能讓部署中盡量減少伺服器數量成為較好的選擇。
- 在 Horizon 7 中，依預設會開啟 View 儲存加速器功能，這可讓 ESXi 5.5 Update 2 及更新版本的主機快取通用的虛擬機器磁碟資料。View 儲存加速器可以改善效能並降低額外儲存 I/O 頻寬的需要，以管理開機風暴和防毒掃描 I/O 風暴。使用此功能需要每個 ESXi 主機 1GB 的 RAM。
- 最後，請考量叢集需求及任何容錯移轉需求。如需詳細資訊，請參閱 確定高可用性的需求。

如需 vSphere 中 ESXi 主機規格的相關資訊，請參閱《VMware vSphere 組態上限》文件。

適用於特定類型工作者的桌面平台集區

Horizon 7 提供許多功能，來協助您節省儲存空間，並減少各種使用案例所需的處理電源。其中的許多功能可當成集區設定使用。

需要考量的最基本問題是，某種類型的使用者需要可設定狀態的桌面平台映像，還是需要無狀態的桌面平台映像。需要可設定狀態的桌面平台映像的使用者會將必須保留、維護及備份的資料放在作業系統映像本身。例如，這些使用者安裝部分自己專屬的應用程式，或是有資料無法儲存在虛擬機器本身之外 (例如檔案伺服器或應用程式資料庫)。

無狀態的桌面平台映像	無狀態架構也稱為非持續性桌面平台，其具有許多優勢，像是更易於支援，以及所需儲存成本較低。其他優點包括，不太需要備份虛擬機器，以及更簡易、成本較低的災難復原與業務持續性選項。
可設定狀態的桌面平台映像	這些映像也稱為持續性桌面平台，其可能需要傳統的映像管理技術。可設定狀態的映像結合某些儲存系統技術，可實現低儲存成本。考量備份、災難復原和業務持續性等策略時，備份和復原技術 (例如 VMware Site Recovery Manager) 很重要。

有兩種方式可在 Horizon 7 中建立無狀態的桌面平台映像：

- 您可以建立即時複製虛擬機器的浮動指派集區或專用指派集區。資料夾重新導向和漫遊設定檔可選擇性地用來儲存使用者資料。
- 您可以使用 View Composer 來建立連結複製虛擬機器的浮動或專用指派集區。您可以選擇性地使用資料夾重新導向和漫遊設定檔來儲存使用者資料，或設定用來持續保存使用者資料的持續性磁碟。

有數種方式可在 Horizon 7 中建立可設定狀態的桌面平台映像：

- 您可以建立完整複製或完整虛擬機器。有些儲存裝置廠商提供符合成本效益的完整複製儲存解決方案。這些廠商通常有自己專屬的最佳做法和佈建公用程式。使用這些廠商之一可能會要求您建立手動專用指派集區。
- 您可以建立即時複製或連結複製虛擬機器的集區，並使用 App Volumes 使用者可寫入磁碟區來連結使用者資料和使用者安裝的應用程式。

要使用無狀態還是可設定狀態的桌面平台取決於特定的工作者類型。

- 適用於任務工作者的集區

  您可以對任務工作者的無狀態桌面映像進行標準化，如此映像始終會在已知可輕易支援的組態中，使用者也可以登入任何可用的桌面。

- 適用於知識工作者和進階使用者的集區

  知識工作者必須能夠建立複雜文件，並使文件存留在桌面上。進階使用者必須能夠安裝自己的應用程式，並使應用程式存留下來。視必須保留的個人資料的性質和多寡，桌面可以是可設定狀態或無狀態。

- 適用於 Kiosk 使用者的集區

  Kiosk 使用者可能包括在航空公司驗票處的客戶、身在教室或圖書館的學生、位於病歷登錄工作站的醫護人員或自助服務點的客戶。與用戶端裝置 (而不是與使用者) 相關聯的帳戶有權使用這些桌面平台集區，因為使用者無需登入即可使用用戶端裝置或遠端桌面平台。對於部分應用程式，使用者仍必須提供驗證認證資訊。

適用於任務工作者的集區

您可以對任務工作者的無狀態桌面映像進行標準化，如此映像始終會在已知可輕易支援的組態中，使用者也可以登入任何可用的桌面。

由於任務工作者會在少數應用程式中執行重複性的工作，所以您可以建立無狀態的桌面映像，這有助於節省儲存空間和處理需求。

請針對即時複製桌面平台集區使用下列集區設定：

- 對於即時複製集區，若要最佳化資源使用量，請使用隨選佈建，根據使用量擴大或縮小集區。務必指定足夠的備用桌面平台以滿足登入率。
- 針對即時複製桌面平台集區，每當使用者登出時，Horizon 7 會自動刪除即時複製。隨即會建立新的即時複製並準備就緒可供下一個使用者登入，因此能在每次登出時有效地重新整理桌面平台。

請針對 View Composer 連結複製桌面平台集區使用下列集區設定：

- 針對 View Composer 桌面平台集區，決定使用者登出時要執行的動作 (若有的話)。磁碟會隨時間不斷增長。您可以在使用者登出時重新整理桌面以回到原始狀態，藉此節省磁碟空間。您也可以設定排程以定期重新整理桌面。例如，您可以排程每日、每週或每月重新整理桌面。
- 如果適用，並且如果您使用 View Composer 連結複製集區，請考慮將桌面平台儲存在本機 ESXi 資料存放區。此策略可提供多項優點，例如便宜的硬體、快速的虛擬機器佈建、高效能電源作業，以及簡易的管理。如需限制清單，請參閱用於浮動、無狀態桌面的本機資料存放區。本機資料存放區上不支援即時複製集區。

  備註 如需其他類型儲存選項的相關資訊，請參閱減少和管理儲存需求。

- 使用 Persona Management 功能，讓使用者永遠有自己偏好的桌面外觀和應用程式設定，就像 Windows 使用者設定檔一樣。如果您沒有將桌面設定為登出時重新整理或刪除，您可以設定登出時要移除的角色。

  重要 角色管理可協助您針對要在工作階段之間保留設定的使用者，實作浮動指派集區。過去浮動指派桌面平台的其中一項限制是，使用者登出時，會遺失儲存在遠端桌面平台的所有組態設定與任何資料。

  使用者每次登入時，桌面背景會設為預設桌布，使用者必須再次設定每個應用程式的喜好設定。透過角色管理，浮動指派桌面平台的使用者將看不出其工作階段與專用指派桌面平台上的工作階段之間有何不同。

請針對所有桌面平台集區使用下列一般集區設定：

- 建立自動集區，以便在集區建立時建立桌面，或根據集區使用量，在需要時產生桌面。

- 使用浮動指派，讓使用者可登入任何可用的桌面。如果沒有人必須同時登入時，此設定可減少所需的桌面數量。
- 建立即時複製或 View Composer 連結複製桌面平台，使桌面平台共用相同的基礎映像，並讓使用的資料中心儲存空間比完整的虛擬機器還少。

適用於知識工作者和進階使用者的集區

知識工作者必須能夠建立複雜文件，並使文件存留在桌面上。進階使用者必須能夠安裝自己的應用程式，並使應用程式存留下來。視必須保留的個人資料的性質和多寡，桌面可以是可設定狀態或無狀態。

至於不需要使用者安裝應用程式 (短暫使用時除外) 的知識工作者，您可以建立無狀態的桌面映像，並將它們所有的個人資料儲存在虛擬機器、檔案伺服器或應用程式資料庫之外。對於其他知識工作者和進階使用者，您可以建立可設定狀態的桌面映像。

請針對即時複製桌面平台集區使用下列集區設定：

- 如果您使用即時複製桌面平台，請實作檔案共用、漫遊設定檔或其他設定檔管理解決方案。

請針對 View Composer 連結複製桌面平台集區使用下列集區設定：

- 如果您使用 View Composer 搭配 vSphere 虛擬桌面，請啟用 vCenter Server 和桌面平台集區的空間回收功能。利用空間回收功能，就會透過清除與壓縮程序，自動回收客體作業系統內過時或已刪除的資料。
- 如果您使用 View Composer 連結複製桌面平台，請實作角色管理、漫遊設定檔或其他設定檔管理解決方案。您也可以設定持續性磁碟，以便可以重新整理和重新撰寫連結複製作業系統磁碟，同時在持續性磁碟上保留使用者設定檔的複本。
- 使用 Persona Management 功能，讓使用者永遠有自己偏好的桌面外觀和應用程式設定，就像 Windows 使用者設定檔一樣。

請針對所有桌面平台集區使用下列一般集區設定：

- 一些進階使用者和知識工作者 (例如會計人員、銷售經理、行銷研究分析人員) 可能需要每次都登入相同的桌面平台。請為他們建立專用指派集區。
- 使用 vStorage Thin Provisioning，如此一開始，每個桌面就只會使用磁碟進行初始作業時所需的儲存空間大小。
- 對於必須安裝自己的應用程式以新增資料至作業系統磁碟的進階使用者和知識工作者，有兩個選項。其中一個選項是建立完整的虛擬機器桌面平台。

  另一個選項是建立連結複製或即時複製的集區，並使用 App Volumes 在各登入中保存使用者安裝的應用程式和使用者資料。
- 如果知識工作者不需要使用者安裝的應用程式 (短暫使用時除外)，您可以建立 View Composer 連結複製桌面平台或即時複製桌面平台。桌面映像會共用相同的基礎映像，且使用的儲存空間比完整的虛擬機器還少。

適用於 Kiosk 使用者的集區

Kiosk 使用者可能包括在航空公司驗票處的客戶、身在教室或圖書館的學生、位於病歷登錄工作站的醫護人員或自助服務點的客戶。與用戶端裝置 (而不是與使用者) 相關聯的帳戶有權使用這些桌面平台集區，因為使用者無需登入即可使用用戶端裝置或遠端桌面平台。對於部分應用程式，使用者仍必須提供驗證認證資訊。

設定為以 Kiosk 模式執行的虛擬機器桌面平台使用無狀態的桌面平台映像，因為使用者資料無需保留在作業系統磁碟中。Kiosk 模式桌面會與精簡型用戶端裝置或鎖定的電腦搭配使用。您應確保桌面應用程式會實施驗證機制以進行安全交易、實體網路能防止竄改和窺探，以及和連線至網路的所有裝置均受信任。

最佳做法是使用專用連線伺服器執行個體來處理 Kiosk 模式下的用戶端，並在 Active Directory 中為這些用戶端的帳戶建立專用的組織單位和群組。此做法不僅能隔開這些系統，避免未經授權的入侵，也能更方便設定和管理用戶端。

若要設定 Kiosk 模式，您必須使用 `vdmadmin` 命令列介面，並執行《Horizon 7 管理》文件中關於 Kiosk 模式的主題所說明的幾個程序。

在此設定過程中，您可以使用下列即時複製桌面平台集區設定。

- 如果您使用的是即時複製桌面平台集區，每當使用者登出時，Horizon 7 會自動刪除即時複製。隨即會建立新的即時複製並準備就緒可供下一個使用者登入，因此能在每次登出時有效地重新整理桌面平台。

在此設定過程中，您可以使用下列 View Composer 連結複製桌面平台集區設定。

- 如果您要使用 View Composer 連結複製桌面平台，請制定重新整理原則，使桌面平台經常進行重新整理，例如，在使用者每次登出後執行。
- 如果適用，請考量將桌面儲存在本機 ESXi 資料庫上。此策略可提供多項優點，例如便宜的硬體、快速的虛擬機器佈建、高效能電源作業，以及簡易的管理。如需限制清單，請參閱用於浮動、無狀態桌面的本機資料存放區。本機資料存放區上不支援即時複製集區。

  備註 如需其他類型儲存選項的相關資訊，請參閱減少和管理儲存需求。

在此設定過程中，您可以針對所有桌面平台集區使用下列一般設定。

- 建立自動集區，以便在集區建立時建立桌面，或根據集區使用量，在需要時產生桌面。
- 使用浮動指派，讓使用者可以存取集區中任何可用的桌面。
- 建立即時複製或 View Composer 連結複製桌面平台，使桌面平台共用相同的基礎映像，並讓使用的資料中心儲存空間比完整的虛擬機器還少。
- 使用 Active Directory GPO (群組原則物件) 設定隨選列印，使桌面使用最近的印表機。如需完整清單以及透過群組原則系統管理範本 (ADMX) 提供的設定說明，請參閱《在 Horizon 7 中設定遠端桌面平台功能》。
- 使用 GPO 或智慧原則來控制當桌面平台啟動或 USB 裝置插入用戶端電腦時，本機 USB 裝置是否要連線到桌面平台。

桌面虛擬機器組態

記憶體、虛擬處理器數目和磁碟空間等項目的範例設定是 Horizon 7 特有的設定。

所需的系統磁碟空間大小取決於基礎映像所需的應用程式數目。VMware 已驗證包含 8GB 磁碟空間的安裝。應用程式包括 Microsoft Word、Excel、PowerPoint、Adobe Reader、Internet Explorer、McAfee Antivirus 和 PKZIP。

使用者資料所需的磁碟空間大小取決於使用者的角色和資料儲存的組織原則。如果您使用 View Composer，此資料會保留在持續性磁碟上。

下表所列的指導方針適用於標準 Windows 7 或更新版本的虛擬機器桌面平台。

表 4-2. Windows 7 或 Windows 8 的桌面虛擬機器範例

項目	範例
作業系統	32 位元或 64 位元 Windows 7 或更新版本 (含最新的 Service Pack)
RAM	1GB (如果使用者必須安裝用於 3D 轉譯的硬體加速圖形，則為 4GB)
虛擬 CPU	1 (如果是 64 位元系統，或者使用者必須播放高畫質或全螢幕視訊，則為 2)
系統磁碟容量	24GB (略低於標準值)
使用者資料容量 (作為持續性磁碟)	5GB (起點)
虛擬 SCSI 介面卡類型	LSI Logic SAS (預設值)
虛擬網路介面卡	VMXNET 3

RDS 主機虛擬機器組態

使用 RDS (遠端桌面服務) 主機，為使用者提供已發佈的應用程式與工作階段型遠端桌面平台。

RDS 主機可以是實體機器，也可以是虛擬機器。本範例使用虛擬機器，其規格列在下表中。此虛擬機器的 ESXi 主機可以屬於 VMware HA 叢集，以防範實體伺服器故障。

表 4-3. RDS 主機虛擬機器範例

項目	範例
作業系統	64 位元 Windows Server 2008 R2 或 Windows Server 2012 R2
RAM	24GB
虛擬 CPU	4
系統磁碟容量	40GB
虛擬 SCSI 介面卡類型	LSI Logic SAS (Windows Server 2008 的預設值)
虛擬網路介面卡	VMXNET 3

表 4-3. RDS 主機虛擬機器範例 (續)

項目	範例
1 個 NIC	1 GB
用戶端連線總數上限 (包括工作階段型遠端桌面平台連線與已發佈的應用程式連線)	50

備註 如果您以較低的資源規格來設定 RDS 主機，且不使用預設安裝而是使用所有功能，則可能會遇到資源限制。

如需 RDS 主機組態和測試之工作負載的詳細資訊，請參閱《VMware Horizon 6 參考架構》白皮書，網址為：http://www.vmware.com/files/pdf/techpaper/VMware-Reference-Architecture-Horizon-6-View-Mirage-Workspace.pdf。

vCenter Server 和 View Composer 虛擬機器組態

您可以將 vCenter Server 和 View Composer 安裝在同一台虛擬機器上，或是安裝在個別伺服器上。這些伺服器比桌面虛擬機器需要更多的記憶體和處理能力。

VMware 已測試使用 vSphere 5.1 或更新版本，由 View Composer 建立和佈建每個集區各 2,000 個桌面。VMware 也測試了由 View Composer 在 2,000 個桌面上同次執行重新撰寫作業。這些測試的 vCenter Server 和 View Composer 安裝在個別虛擬機器上。

桌面集區大小受限於下列因素：

- 每個桌面平台集區只能包含一個 vSphere 叢集。
- 在某些設定中，叢集最多可包含 32 台主機。在其他設定中，叢集限有 8 台主機。如需更多資訊，請參閱 vSphere 叢集。
- 每個 CPU 核心具有 8 至 10 個虛擬桌面的運算能力。
- 子網路的可用 IP 位址數量會限制集區的桌面數量。例如，如果網路設定為集區的子網路只包含 256 個可用的 IP 位址，則集區大小限制為 256 個桌面。或者，您可以設定多個網路標籤，以大幅擴增指派給集區中虛擬機器的 IP 位址數量。

雖然可以在實體機器上安裝 vCenter Server 和 View Composer，但是此範例是使用個別虛擬機器，且規格如下表所列。這些虛擬機器的 ESXi 主機可以屬於 VMware HA 叢集，以防範實體伺服器故障。

此範例假設您使用 Horizon 7 搭配 vSphere 5.1 或更新版本和 vCenter Server 5.1 或更新版本。

重要 此範例也假設 View Composer 和 vCenter Server 安裝在個別虛擬機器上。

表 4-4. vCenter Server 虛擬機器範例

項目	管理 10,000 個桌面的 vCenter Server 範例	管理 2,000 個桌面的 vCenter Server 範例
作業系統	64 位元 Windows Server 2008 R2 Enterprise	64 位元 Windows Server 2008 R2 Enterprise
RAM	48GB	10-24 GB，視 vSphere 的版本而定

表 4-4. vCenter Server 虛擬機器範例 (續)

項目	管理 10,000 個桌面的 vCenter Server 範例	管理 2,000 個桌面的 vCenter Server 範例
虛擬 CPU	16	2-8，視 vSphere 的版本而定
系統磁碟容量	180GB	40GB
虛擬 SCSI 介面卡類型	LSI Logic SAS (Windows Server 2008 的預設值)	LSI Logic SAS (Windows Server 2008 的預設值)
虛擬網路介面卡	E1000 (預設值)	VMXNET 3 (雖然使用預設值 E1000 也行)
vCenter 並行佈建作業上限	20	20
並行電源作業數量上限	50	50

表 4-5. View Composer 虛擬機器範例

項目	管理 10,000 個桌面的 View Composer 範例	管理 2,000 個桌面的 View Composer 範例
作業系統	64 位元 Windows Server 2008 R2 Enterprise	64 位元 Windows Server 2008 R2 Enterprise
RAM	10 GB 或更多，視 vSphere 的版本而定	4-10 GB，視 vSphere 的版本而定
虛擬 CPU	4 個或更多，視 vSphere 的版本而定	2-4，視 vSphere 的版本而定
系統磁碟容量	50GB	40GB
虛擬 SCSI 介面卡類型	LSI Logic SAS (Windows Server 2008 的預設值)	LSI Logic SAS (Windows Server 2008 的預設值)
虛擬網路介面卡	VMXNET 3	VMXNET 3
View Composer 集區大小上限	2,000 個桌面	1,000 個桌面
並行 View Composer 維護作業上限	12	12
並行 View Composer 佈建作業上限	8	8

重要　VMware 建議您將 vCenter Server 和 View Composer 連線的資料庫放在個別虛擬機器上。

Horizon 連線伺服器最大值和虛擬機器組態

安裝 Horizon 連線伺服器時，系統會一併安裝 Horizon Administrator 使用者介面。

連線伺服器組態

您可以將連線伺服器安裝在實體機器上，不過，此範例使用的是虛擬機器，其規格如「連線伺服器虛擬機器範例」所列。此虛擬機器的 ESXi 主機可以屬於 VMware HA 叢集，以防範實體伺服器故障。

表 4-6. 連線伺服器虛擬機器範例

項目	範例
作業系統	請參閱《Horizon 7 安裝》文件中支援的作業系統。
RAM	10GB

表 4-6. 連線伺服器虛擬機器範例 (續)

項目	範例
虛擬 CPU	4
系統磁碟容量	70GB
虛擬 SCSI 介面卡類型	LSI Logic SAS (Windows Server 2008 的預設值)
虛擬網路介面卡	VMXNET 3
網路介面卡	1Gbps NIC

連線伺服器叢集設計考量

您可以在群組中部署多個複寫的連線伺服器執行個體，以支援負載平衡和高可用性。複寫的執行個體群組設計為支援 LAN 連線的單一資料中心環境內的叢集。

重要　在 Horizon 部署需要跨越資料中心的案例中，若要跨 WAN、MAN (都會區網路) 或其他非 LAN 使用複寫的連線伺服器執行個體群組，您必須使用 Cloud Pod 架構功能。如需詳細資訊，請參閱《在 Horizon 7 中管理 Cloud Pod 架構》文件。

連線伺服器的連線數目上限

「遠端桌面平台連線」提供與 Horizon 7 部署可容納同時連線數目相關的已測試限制資訊。

表 4-7. 遠端桌面平台連線

每個部署的連線伺服器	連線類型	同時連線數目上限
1 部連線伺服器	直接連線、RDP、Blast Extreme 或 PCoIP	4,000 (已測試的組態)
1 部連線伺服器	通道連線、RDP	2,000 (預設組態) 4,000 (已測試的組態)
1 部連線伺服器	PCoIP 安全閘道連線	2,000 (預設組態) 4,000 (已測試的組態)
1 部連線伺服器	Blast 安全閘道連線	2,000 (預設組態) 4,000 (已測試的組態)
1 部連線伺服器	與實體電腦間的 Unified Access	2,000 (已測試的組態)

表 4-7. 遠端桌面平台連線 (續)

每個部署的連線伺服器	連線類型	同時連線數目上限
1 部連線伺服器	與 RDS 主機間的 Unified Access	2,000 (已測試的組態)
7 部連線伺服器	直接連線、RDP、Blast Extreme 或 PCoIP	RDS 主機 ■ 10,000 (預設組態) ■ 20,000 (已測試的組態) 虛擬桌面平台 ■ 12,000 (已測試的組態)

備註 完全支援已測試的組態。若要使用已測試的組態，在單一連線伺服器上將上限 4,000 個同時連線用於通道連線、PCoIP 安全閘道和 Blast 安全閘道，請在安裝連線伺服器的虛擬機器上建立 `locked.properties` 檔案：`C:\Program Files\VMware\VMware View\Server\sslgateway\conf`。然後，在 `locked.properties` 檔案中設定 `maxConnections=4000`，並重新啟動連線伺服器。Unified Access Gateway 目前支援 2,000 個工作階段，因此在測試 20,000 個工作階段時使用了 14 個 Unified Access Gateway 應用裝置。

如果將安全伺服器或 Unified Access Gateway 應用裝置用於來自公司網路外部的 PCoIP 連線，則需要 PCoIP 安全閘道連線。如果將安全伺服器或 Unified Access Gateway 應用裝置用於來自公司網路外部的 Blast Extreme 或 HTML Access 連線，則需要 Blast 安全閘道連線。如果將安全伺服器或 Unified Access Gateway 應用裝置用於來自公司網路外部的 RDP 連線，以及用於透過 PCoIP 或 Blast 安全閘道連線的 USB 和多媒體重新導向 (MMR) 加速，則需要通道連線。您可以將多個安全伺服器與單一連線伺服器執行個體配對。

雖然單一安全伺服器或 Unified Access Gateway 應用裝置可以支援最多 2,000 個同時連線，但您可能不會讓每個連線伺服器執行個體 (具有 2,000 個工作階段) 只使用一個安全伺服器，而會選擇使用 2 或 4 個。安全伺服器的監控作業可能會指出 2,000 個使用者的活動過多。所需的記憶體數量和 CPU 使用率可能會指示您為每個連線伺服器執行個體新增更多安全伺服器，以分散負載。例如，您可以使用 2 部安全伺服器，每部處理 1,000 個連線，或可以使用 4 部安全伺服器，每部處理 500 個連線。安全伺服器與連線伺服器執行個體的比例取決於特定環境的需求。

每一 Unified Access Gateway 應用裝置的連線數目與安全伺服器的差不多。如需 Unified Access Gateway 應用裝置的詳細資訊，請參閱《部署及設定 Unified Access Gateway》。

備註 在此範例中，雖然 5 個連線伺服器執行個體 (已適當設定) 可以處理 20,000 個連線，但資料表中顯示的數目 7 是作為可用性規劃之用，以容納同時來自公司網路內部和外部的連線。

例如，如果您有 20,000 個使用者，其中 16,000 個使用者在公司網路內部，則您需要在公司網路內部部署 5 個連線伺服器執行個體。如此，萬一其中一個執行個體失效，其餘 4 個執行個體仍足以處理負載。同樣地，如果有 4,000 個連線來自公司網路外部，則您需要 2 個連線伺服器執行個體，當其中一個失效時，您還有一個執行個體可以處理負載。

這些數字假設外部連線會透過閘道呈現。在此範例中，每個處理外部連線的連線伺服器執行個體會與 3 個安全伺服器配對，以便在其中一個變得無法使用時，剩餘 2 個安全伺服器仍可處理負載。如果使用 Unified Access Gateway 應用裝置而非安全伺服器，則您需要總計 3 個應用裝置在兩個連線伺服器執行個體之間平衡負載，以便在其中一個變得無法使用時，剩餘 2 個應用裝置仍可處理負載。

在所有情況下，如果使用者使用的連線伺服器或閘道變得無法使用，則需要重新連線。

Unified Access Gateway 搭配使用 Horizon 7 的硬體需求

VMware 建議使用 2 個 vCPU 和 4GB 的 RAM，讓 Unified Access Gateway 應用裝置在搭配 Horizon 7 使用時可支援最大的連線數量。

表 4-8. Unified Access Gateway 的硬體需求

項目	範例
作業系統	OVA
RAM	4GB
虛擬 CPU	2
系統磁碟容量	20 GB (變更預設記錄層級需要額外的空間)
虛擬 SCSI 介面卡類型	LSI Logic Parallel (OVA 的預設值)
虛擬網路介面卡	VMXNET 3
網路介面卡	1Gbps NIC
網路對應	單一 NIC 選項

vSphere 叢集

Horizon 7 部署可使用 VMware HA 叢集來防範實體伺服器失敗。視您的設定而定，叢集可包含多達 32 個節點。

vSphere 和 vCenter Server 提供一套豐富的功能，來管理主控虛擬機器桌面平台的伺服器叢集。叢集組態也很重要，因為每個虛擬機器桌面平台集區都必須與 vCenter Server 資源集區相關聯。所以，每個集區的桌面數量上限與每個叢集計劃要執行的伺服器和虛擬機器數目有關。

在極大型的 Horizon 7 部署中，透過讓每個資料中心物件只有一個叢集物件，vCenter Server 的效能與回應性就能獲得改善，不過這不是預設的運作方式。依預設，vCenter Server 會在同一個資料中心物件內建立新叢集。

備註 如需 Horizon 7 的調整大小限制和建議的最新更新，請參閱 VMware 知識庫 (KB) 文章 https://kb.vmware.com/s/article/2150348。

在下列情況下，vSphere 叢集可包含多達 32 台 ESXi 主機或節點：

- vSphere 5.1 及更新版本，具備 View Composer 連結複製集區，並將複本磁碟儲存在 NFS 資料存放區或 VMFS5 或者更新版的資料存放區上
- vSphere 6.0 及更新版本，並將集區儲存在虛擬磁碟區資料存放區上

如果您具有 vSphere 5.5 Update 1 及更新版本，並將集區儲存在 vSAN 資料存放區上，則 vSphere 叢集最多可包含 20 台 ESXi 主機。

如果您將 View Composer 複本儲存在早於 VMFS5 的 VMFS 版本上，則叢集最多可擁有八台主機。作業系統磁碟和持續性磁碟可以儲存在 NFS 或 VMFS 資料存放區上。

如需詳細資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中關於建立桌面平台集區的章節。網路需求取決於伺服器類型、網路介面卡數量，以及 VMotion 的設定方式。

確定高可用性的需求

vSphere 透過其效率與資源管理，可讓每個伺服器的虛擬機器數量達成領先業界的等級。但是達到每個伺服器更高的虛擬機器密度意味著，如果某一部伺服器故障，會有更多的使用者受到影響。

對高可用性的需求會根據桌面集區的用途而有很大的不同。例如，無狀態桌面映像 (浮動指定) 集區的復原點目標 (RPO) 需求可能就跟可設定狀態的桌面映像 (專用指定) 集區不同。若是浮動指定集區，可接受的解決方案可能是，如果使用者所用的桌面無法使用時，則讓使用者登入其他桌面。

在具有高可用性需求的情況下，適當的 VMware HA 組態不可或缺。如果使用 VMware HA 並且規劃每個伺服器包含固定數量的桌面，請以減少容量的方式執行每個伺服器。如果有一部伺服器故障，當桌面在其他主機上重新啟動時，就不會超過每個伺服器的桌面容量。

例如，在一個包含 8 個主機的叢集中，其中各個主機能夠執行 128 個桌面，而目標是容許單一伺服器故障時，請確定該叢集上執行的桌面不會超過 128 * (8 - 1) = 896 個。您也可以使用 VMware DRS (Distributed Resource Scheduler) 協助平衡所有 8 個主機中的桌面。這樣就能充分使用額外的伺服器容量，不讓任何熱備援資源閒置。此外，DRS 也可以在故障的伺服器恢復服務時，協助重新平衡叢集。

您也必須確定有適當設定儲存空間，以支援多部虛擬機器因伺服器故障而同時重新啟動所產生的 I/O 負載。儲存 IOPS 對桌面從伺服器故障復原的速度影響最大。

範例： 叢集組態範例

下列表格所列的設定是 Horizon 7 特定的設定。如需 vSphere 中 HA 叢集限制的相關資訊，請參閱《VMware vSphere 組態上限》文件。

備註 下列基礎結構範例已使用 View 5.2 和 vSphere 5.1 進行測試。範例會使用 View Composer 連結複製而非即時複製，因為測試是使用 View 5.2 來執行。即時複製功能是在 Horizon 7 推出。View 5.2 無法使用的其他功能包括 vSAN 和虛擬磁碟區。

表 4-9. Horizon 7 基礎結構叢集範例

項目	範例
虛擬機器	用作桌面平台集區來源的 vCenter Server 執行個體、Active Directory、SQL 資料庫伺服器、View Composer、連線伺服器執行個體、安全伺服器和父虛擬機器
節點 (ESXi 主機)	6 部 Dell PowerEdge R720 伺服器 (16 核心 * 2 GHz；各主機 192GB RAM)
SSD 儲存	用於 vCenter Server、View Composer、SQL 資料庫伺服器和父虛擬機器的虛擬機器
非 SSD 儲存	用於 Active Directory、連線伺服器和安全伺服器的虛擬機器
叢集類型	DRS (Distributed Resource Scheduler)/HA

表 4-10. 虛擬機器桌面平台叢集範例

項目	範例
叢集數目	5
每個叢集的桌面和集區數目	每個叢集 1 個包含 2,000 個桌面 (虛擬機器) 的集區
節點 (ESXi 主機)	下列是可用於各叢集的各種伺服器範例： ■ 12 部 Dell PowerEdge R720 (16 核心 * 2 GHz；以及各主機 192GB RAM) ■ 16 部 Dell PowerEdge R710 (12 核心 * 2.526 GHz；以及各主機 144GB RAM) ■ 8 部 Dell PowerEdge R810 (24 核心 * 2 GHz；以及各主機 256GB RAM) ■ 6 部 Dell PowerEdge R810 + 3 部 PowerEdge R720
SSD 儲存	複本虛擬機器
非 SSD 儲存	32 個非 SSD 資料庫用於複製 (各資料存放區 450 GB)
叢集類型	DRS (Distributed Resource Scheduler)/HA

儲存和頻寬需求

規劃虛擬機器桌面平台的共用儲存區、規劃有關 I/O 風暴的儲存頻寬需求，以及規劃網路頻寬需求時，必須考量幾個事項。

下列主題提供 VMware 測試設定所使用的儲存和網路元件相關詳細資料。

- 共用儲存範例

  在 View 5.2 測試環境中，View Composer 複本虛擬機器會放在高讀取效能的固態硬碟 (SSD)，所支援的每秒 I/O 次數 (IOPS) 高達數萬個。連結複製則放在較低效能的傳統旋轉媒體所支援的資料存放區，這樣成本較低，並可提供較高的儲量容量。範例會使用 View Composer 連結複製而非即時複製，因為測試是使用 View 5.2 來執行。即時複製功能是在 Horizon 7 推出。

- 儲存頻寬考量事項

  在 Horizon 7 環境中，決定頻寬需求的主要考量因素是登入風暴。

- 網路頻寬考量事項

  若要容納一般的工作負載，需要某些虛擬和實體網路元件。

- View Composer 效能測試結果

  這些測試結果說明包含 10,000 個桌面平台的 View 5.2 設定，其中由一個 vCenter Server 5.1 執行個體管理 5 個集區，每個集區有 2,000 個虛擬機器桌面平台。佈建新集區或重新撰寫、重新整理或重新平衡包含 2,000 個虛擬機器的現有集區，只需要一個維護期間。10,000 位使用者的登入風暴也已經過測試。

- WAN 支援

  對於廣域網路 (WAN)，您必須考量頻寬限制和延遲問題。VMware 提供的 PCoIP 和 Blast Extreme 顯示通訊協定可順應各種延遲和頻寬條件。

共用儲存範例

在 View 5.2 測試環境中，View Composer 複本虛擬機器會放在高讀取效能的固態硬碟 (SSD)，所支援的每秒 I/O 次數 (IOPS) 高達數萬個。連結複製則放在較低效能的傳統旋轉媒體所支援的資料存放區，這樣成本較低，並可提供較高的儲量容量。範例會使用 View Composer 連結複製而非即時複製，因為測試是使用 View 5.2 來執行。即時複製功能是在 Horizon 7 推出。

儲存設計考量是建立成功的 Horizon 7 架構的最重要元素之一。對架構影響最大的是，決定是否採用 View Composer 桌面以使用連結複製技術。ESXi 二進位檔、虛擬機器分頁檔及父虛擬機器的 View Composer 複本都會儲存在共用儲存區系統。

vSphere 使用的外部儲存區系統可以是光纖通道、iSCSI SAN (儲存區域網路) 或 NFS (網路檔案系統) NAS (網路連接儲存)。透過 vSphere 5.5 Update 1 或更新版本提供的 vSAN 功能，儲存區系統也可以是彙總的本機伺服器連結儲存區。

下列範例說明 View 5.2 測試設定所用的分層儲存策略，其中由一個 vCenter Server 管理 10,000 個桌面平台。

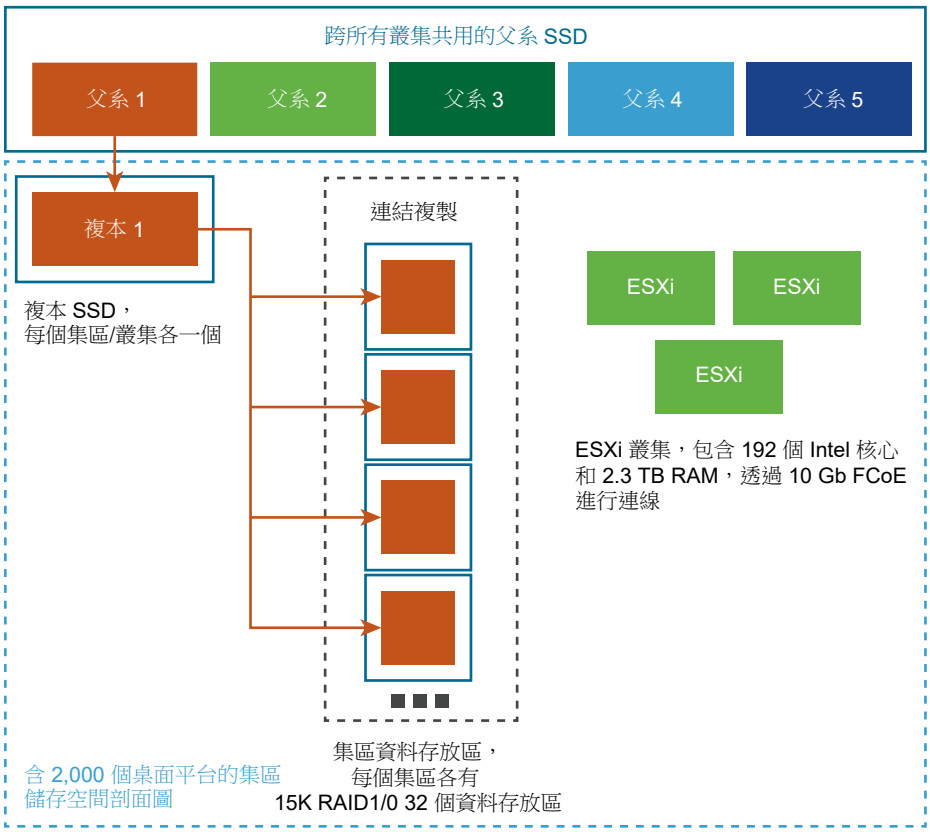
備註 此範例在發行 VMware vSAN 之前執行的 View 5.2 設定中使用過。如需為 VMware vSAN 調整和設計 View 虛擬桌面平台基礎結構的關鍵元件的指導方針，請參閱位於 http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf 的白皮書。

相較於 vSphere 5.5 Update 1，vSphere 6.0 及更新版本提供的 vSAN 功能在效能方面有許多改進。在 vSphere 6.0 中，此功能也具有更廣泛的 HCL (硬體相容性) 支援。如需 vSphere 6 或更新版本中關於 vSAN 的詳細資訊，請參閱《管理 VMware vSAN》文件。

實體儲存	■ 僅限 EMC VNX7500 區塊 ■ 1.8TB 快速快取 (SSD) ■ 八個 10Gbit FCoE 前端連線 (每個控制器各 4 個)。
SSD 儲存裝置層	單一 RAID5 儲存集區： ■ 12 * 200GB EFD ■ 250GB LUN 供父系映像使用 ■ 500GB LUN 供基礎結構使用 ■ 75GB LUN 供複本存放區使用 (每個桌面集區叢集各 1 個)
虛擬機器桌面平台儲存區層	兩個 RAID 1/0 儲存集區： 集區 1： ■ 360 15K 300GB HDD (可用 47TB) ■ 97 個 450GB LUN 供桌面使用 集區 2： ■ 296 15K 300GB HDD (可用 39TB) ■ 7 個 450GB LUN 供基礎結構使用 ■ 85 個 450GB LUN 供桌面平台使用

下圖說明這個儲存策略。

圖 4-1. 大型桌面集區的分層儲存範例



從架構的觀點來看，View Composer 會建立共用基礎映像的桌面映像，這可減少儲存需求達 50% 以上。您可以進一步減少儲存需求，方法是設定重新整理原則以定期將桌面還原成原始狀態，以及回收用於追蹤上次重新整理作業以來變更的空間。

如果您使用 View Composer 搭配 vSphere 5.1 或更新版本的虛擬機器桌面平台，即可使用空間回收功能。利用這個功能，當未使用的磁碟空間量達到特定臨界值時，就會透過清除與壓縮程序，自動回收客體作業系統內過時或已刪除的資料。請注意，如果使用 vSAN 資料存放區，空間回收功能將不受支援。

您也可以縮減作業系統磁碟空間，方法是使用 View Composer 持續性磁碟或共用檔案伺服器作為主要存放庫，來儲存使用者設定檔和使用者文件。由於 View Composer 可讓您將使用者資料與作業系統隔開，因此，您可能會發現，只有持續性磁碟才需要備份或複寫，這可進一步減少儲存需求。如需詳細資訊，請參閱透過 Composer 減少儲存需求。

備註 至於專用儲存元件，最好在試驗階段期間做出決定。主要的考量是每秒 I/O 數 (IOPS)。您可以嘗試使用分層儲存策略或 vSAN 儲存區，以獲得最佳效能和最大的成本節省。

如需詳細資訊，請參閱標題為 VMware View 的儲存考量的最佳做法指南。

儲存頻寬考量事項

在 Horizon 7 環境中，決定頻寬需求的主要考量因素是登入風暴。

雖然有許多元素對於設計儲存系統以支援 Horizon 7 環境都很重要，但是從伺服器組態的觀點來看，最不可或缺的是規劃適當的儲存頻寬。您還必須考量連接埠合併硬體的影響。

Horizon 7 環境有時會在所有虛擬機器同時執行活動的期間，發生 I/O 風暴負載。客體型代理程式可以觸發 I/O 風暴，例如防毒軟體或軟體更新代理程式。像是所有員工幾乎同時在早上登入等人員行為，也可以觸發 I/O 風暴。VMware 已針對 10,000 個桌面進行登入風暴案例測試。如需詳細資訊，請參閱 View Composer 效能測試結果。

您可以透過作業面的最佳做法，例如交錯執行不同虛擬機器的更新等，讓這些風暴工作負載降至最低。您也可以在試驗階段期間測試各種登出原則，決定使用者登出造成 I/O 風暴時是否暫停虛擬機器、還是關閉虛擬機器電源。將 View Composer 複本儲存在個別的高效能資料存放區，可以加速密集的並行讀取作業，以應付 I/O 風暴負載。例如，您可以使用下列其中一種儲存策略：

- 手動設定集區，讓複本儲存在不同的高效能資料存放區中。
- 使用 vSphere 5.5 Update 1 或更新版本提供的 vSAN，其會使用軟體原則式管理來決定要用於複本的磁碟種類。
- 使用 vSphere 6.0 或更新版本提供的虛擬磁碟區，其會使用軟體原則式管理來決定要用於複本的磁碟種類。

除了決定最佳做法之外，VMware 也建議您提供每 100 個虛擬機器 1Gbps 的頻寬，即使平均頻寬可能低於該值的 10 倍。這種保守規劃可確保有足夠的儲存連線能力來處理尖峰負載。

網路頻寬考量事項

若要容納一般的工作負載，需要某些虛擬和實體網路元件。

對顯示流量而言，有許多元素可能影響網路頻寬，例如，所用的通訊協定、監視器解析度和組態，以及工作負載中的多媒體內容量。同時啟動串流的應用程式也會造成使用量突然爆增。

由於這些問題的影響差異甚大，許多公司會透過試驗專案來監控頻寬用量。請針對一般知識工作者容量為 150 至 200Kbps 進行規劃，作為試驗的起點。

使用 PCoIP 或 Blast Extreme 顯示通訊協定時，如果企業 LAN 採用 100 Mb 或 1 Gb 交換網路，則使用者可預期在下列情況下擁有優異的效能：

- 兩部監視器 (1920 x 1080)
- 重度使用 Microsoft Office 應用程式
- 重度使用內嵌 Flash 的網頁瀏覽
- 頻繁使用多媒體，但限制使用全螢幕模式
- 頻繁使用 USB 型週邊設備
- 透過網路列印

如需詳細資訊，請參閱稱為《PCoIP 顯示通訊協定：資訊和情景網路規模指南》的資訊指南。

隨附於 PCoIP 和 Blast Extreme 的最佳化控制項

如果您使用 VMware 的 PCoIP 或 Blast Extreme 顯示通訊協定，則可以調整幾個會影響頻寬使用的元素。

- 您可以設定網路壅塞期間使用的映像畫質等級和畫面播放速率。畫質等級設定可以限制顯示映像區域變更後的初始畫質。您也可以調整畫面播放速率。

  此控制對於不需更新的靜態畫面內容，或只有一小部分需要重新整理的情況很有效用。

- 至於工作階段頻寬，您可以根據網路連線類型 (例如 4Mbit/s 網際網路連線)，設定最大頻寬 (每秒 kb)。頻寬包括所有映像處理、音訊、虛擬通道、USB 和 PCoIP 或 Blast 控制流量。

  您也可以設定要保留給工作階段使用的頻寬下限 (每秒 kb)，使用者就不必等待可用的頻寬。您可以針對工作階段的 UDP 封包，指定傳輸單元最大值 (MTU) 大小，範圍從 500 到 1500 位元組。

如需詳細資訊，請參閱《在 Horizon 7 中設定遠端桌面平台功能》中的〈PCoIP 一般設定〉和〈VMware Blast 原則設定〉小節。

網路組態範例

在由一個 vCenter Server 5.1 執行個體管理 5 個集區 (各集區有 2,000 個虛擬機器) 的 View 5.2 測試網繭中，每個 ESXi 主機配備下列硬體和軟體以滿足網路需求。

備註 此範例在發行 VMware vSAN 之前執行的 View 5.2 設定中使用過。如需為 VMware vSAN 調整和設計 View 虛擬桌面平台基礎結構的關鍵元件的指導方針，請參閱位於 http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf 的白皮書。此外，範例會使用 View Composer 連結複製而非即時複製，因為測試是使用 View 5.2 來執行。即時複製功能是在 Horizon 7 推出。

每個主機的實體元件	■ 使用 10Gig 乙太網路和 FCoE 分別處理網路和儲存流量的 Brocade 1860 Fabric Adapter。 ■ 與 Brocade VCS 乙太網路光纖 (包含 6 個 VDX6720-60 交換器) 連線。這些交換器使用與 Juniper J6350 路由器的兩個 1GB 連線上行連結至網路的其餘部分。
vLAN 摘要	■ 每個桌面集區各一個 10Gb vLAN (共 5 個集區) ■ 一個 1Gb vLAN 用於管理網路 ■ 一個 1Gb vLAN 用於 VMotion 網路 ■ 一個 10Gb vLAN 用於基礎結構網路
虛擬 VMotion-dvswitch (每個主機各 1 個上行連結)	基礎結構、父系和桌面虛擬機器的 ESXi 主機使用此交換器。 ■ Jumbo 框架 (9000 MTU) ■ 1 個暫時分散式連接埠群組 ■ 私人 VLAN 和 192.168.x.x 定址

Infra-dvswitch (每個主機各 2 個上行連結)	基礎結構虛擬機器的 ESXi 主機使用此交換器。 ■ Jumbo 框架 (9000 MTU) ■ 1 個暫時分散式連接埠群組 ■ 基礎結構 VLAN /24 (256 個位址)
Desktop-dvswitch (每個主機各 2 個上行連結)	父系和桌面虛擬機器的 ESXi 主機使用此交換器。 ■ Jumbo 框架 (9000 MTU) ■ 6 個暫時分散式連接埠群組 ■ 5 個桌面連接埠群組 (每個集區各 1 個) ■ 每個網路為 /21，2048 個位址

View Composer 效能測試結果

這些測試結果說明包含 10,000 個桌面平台的 View 5.2 設定，其中由一個 vCenter Server 5.1 執行個體管理 5 個集區，每個集區有 2,000 個虛擬機器桌面平台。佈建新集區或重新撰寫、重新整理或重新平衡包含 2,000 個虛擬機器的現有集區，只需要一個維護期間。10,000 位使用者的登入風暴也已經過測試。

本處提供的測試結果是採用下列主題所說明的軟體、硬體和組態設定完成的：

- Horizon 連線伺服器最大值和虛擬機器組態中說明的桌面和集區組態
- 共用儲存範例中說明的分層儲存元件
- 網路頻寬考量事項中說明的網路元件

處理 10,000 位使用者一小時登入風暴的功能

備註 此範例在發行 VMware vSAN 之前執行的 View 5.2 設定中使用過。如需為 VMware vSAN 調整和設計 View 虛擬桌面平台基礎結構的關鍵元件的指導方針，請參閱位於 http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf 的白皮書。如需各種工作負載的測試結果和使用 vSAN 時的 View 作業，請參閱位於 http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-virtual-san-reference-architecture.pdf 的參考架構白皮書。

相較於 vSphere 5.5 Update 1，vSphere 6.0 及更新版本提供的 vSAN 功能在效能方面有許多改進。在 vSphere 6.0 中，此功能也具有更廣泛的 HCL (硬體相容性) 支援。如需 vSphere 6 或更新版本中關於 vSAN 的詳細資訊，請參閱《管理 VMware vSAN》文件。

在測試設定中，下列桌面和集區組態會用於 10,000 個桌面的登入風暴案例。桌面的電源原則已設為「永遠開啟」。

對於 10,000 個桌面，登入風暴會發生超過 60 分鐘的時間，此使用常態分佈的登入時間。虛擬機器會在登入風暴開始前開啟電源並提供使用。登入後，包括下列應用程式在內的工作負載即開始：Adobe Reader、Microsoft Outlook、Internet Explorer、Microsoft Word 和記事本。

下列是測試期間遭受之登入風暴的額外詳細資料：

- 95% 的登入發生在 +/- 2 標準誤差時段 (40 分鐘) 的範圍內。

- 68% 的登入發生在 +/- 1 標準誤差時段 (20 分鐘) 的範圍內。
- 尖峰登入率為每分鐘 400 個或每秒 6.67 個。

佈建集區所需時間

您可以在建立集區時預先佈建集區，或在將使用者指定至集區時，依需要佈建集區。佈建是指，建立虛擬機器，然後將其設定為使用正確的作業系統映像和網路設定。

在測試設定中，其中已包含 4 個集區，且各集區包含 2,000 個虛擬機器，佈建包含 2,000 個虛擬機器的第五個集區需要 4 小時。所有虛擬機器會預先佈建。

重新撰寫集區所需時間

您可以使用重新撰寫作業，來提供作業系統修補程式、安裝或更新應用程式，或是修改集區中虛擬機器的桌面硬體設定。重新撰寫集區之前，您要擷取具有新組態之虛擬機器的快照。重新撰寫作業會使用該快照，來更新集區中的所有虛擬機器。

在包含 5 個集區 (各集區有 2,000 個虛擬機器) 的測試設定中，重新撰寫一個包含 2,000 個虛擬機器的集區需要 6 小時 40 分鐘的時間。在重新撰寫作業開始前，所有虛擬機器的電源會開啟並可供使用。

重新整理集區所需時間

由於磁碟會隨時間不斷增長，您可以使用以下方式來節省磁碟空間：在使用者登出時重新整理桌面至原始狀態，或者也可以設定定期重新整理桌面的排程。例如，您可以排程每日、每週或每月重新整理桌面。

在包含 5 個集區 (各集區有 2,000 個虛擬機器) 的測試設定中，重新整理一個包含 2,000 個虛擬機器的集區需要 2 小時 40 分鐘的時間。在重新整理作業開始前，所有虛擬機器的電源會開啟並可供使用。

重新平衡集區所需時間

桌面重新平衡作業會將連結複製桌面重新散佈在可用邏輯磁碟機之間，重新平衡作業可節省超載磁碟機上的儲存空間，並確保不會有磁碟機未充分利用。您也可以使用重新平衡作業，將桌面平台集區中的所有虛擬機器移轉到 vSAN 資料存放區或從其中轉出。

在包含 5 個集區 (各集區包含 2,000 個虛擬機器) 的測試網繭 (pod) 中，會將 2 個資料中心新增至網繭 (pod) 來進行一項測試。在另一項測試中，則會從網繭 (pod) 中移除 2 個資料中心。新增或移除資料存放區後，對其中一個集區執行重新平衡作業。重新平衡一個包含 2,000 個虛擬機器的集區需要 9 小時。在重新平衡作業開始前，所有虛擬機器的電源會開啟並可供使用。

WAN 支援

對於廣域網路 (WAN)，您必須考量頻寬限制和延遲問題。VMware 提供的 PCoIP 和 Blast Extreme 顯示通訊協定可順應各種延遲和頻寬條件。

如果使用 RDP 顯示通訊協定，則必須具備 WAN 最佳化產品，以加速分支辦公室或小型辦公室中使用者的應用程式。透過 PCoIP 和 Blast Extreme，許多 WAN 最佳化技術都會內建於基礎通訊協定。

- WAN 最佳化對於 TCP 型通訊協定 (例如 RDP) 很重要，因為這些通訊協定需要在用戶端和伺服器之間進行許多信號交換。這些信號交換的延遲情況可能極大。WAN 加速器會偽裝回覆信號交換，所以會向通訊協定隱藏網路延遲。由於 PCoIP 和 Blast Extreme 以 UDP 為基礎，因此不需要這種形式的 WAN 加速。

- WAN 加速器也會壓縮用戶端和伺服器之間的網路流量，但是此壓縮通常限制在 2:1 的壓縮比率。PCoIP 和 Blast Extreme 具有相當高的壓縮率。

如需您可以用來調整 PCoIP 和 Blast Extreme 耗用頻寬方式的控制項的相關資訊，請參閱隨附於 PCoIP 和 Blast Extreme 的最佳化控制項。

各種類型使用者的頻寬需求

決定 PCoIP 的最低頻寬需求時，請採用下列估計值來規劃：

- 基本辦公室生產力桌面的平均頻寬為 100 至 150Kbps：不含視訊、3D 圖形且使用預設 Windows 和 Horizon 7 設定的一般辦公室應用程式。
- 最佳化辦公室生產力桌面的平均頻寬為 50 至 100Kbps：不含視訊、3D 圖形且 Windows 桌面設定已最佳化和 Horizon 7 已最佳化的一般辦公室應用程式。
- 利用多部監視器、3D、Aero 和 Microsoft Office 之虛擬桌面的平均頻寬為 400 至 600 Kbps。
- 500Kbps 至 1Mbps 最低尖峰頻寬用於提供餘裕空間因應突增的顯示變更。一般而言，請使用平均頻寬來規劃您的網路大小，但應考慮尖峰頻寬，以便能容納與大量螢幕變更相關的突增映像流量。
- 每個同時執行 480p 視訊的使用者 2Mbps，實際取決於設定的畫面播放速率限制和視訊類型。

備註 每個一般使用者 50 至 150Kbps 的估計值採用這個假設為基礎：所有使用者在一天 8 至 10 小時內持續操作及執行類似的工作。50Kbps 頻寬使用圖的資料來源是，在停用無失真建置功能情況下，對 LAN 所做的 View Planner 測試。情況可能各有不同，某些使用者可能極不活躍，幾乎不會用到頻寬，進而可讓每個連結有更多使用者。所以，這些指導方針主要用作更詳細的頻寬規劃和測試的起點。

下列範例顯示在使用 1.5Mbps T1 專線的分支或遠端辦公室中，如何計算並行使用者人數。

分支或遠端辦公室案例

- 使用者有基本的 Microsoft Office 生產力應用程式，無視訊、無 3D 圖形，以及具有 USB 鍵盤和滑鼠裝置。
- Horizon 7 中每個一般辦公室使用者所需的頻寬，是 50 至 150Kbps 之間。
- T1 網路容量為 1.5Mbps。
- 頻寬使用率是 80% (.8 使用係數)。

決定支援的使用者人數的公式

- 最差情況下，使用者需要 150Kbps：(1.5Mbps*.8)/150Kbps = (1500*.8)/150 = 8 位使用者
- 最佳情況下，使用者需要 50Kbps：(1.5Mbps*.8)/50Kbps = (1500*.8)/50 = 24 位使用者

結果

此遠端辦公室可支援每個 T1 專線 (容量為 1.5Mbps) 可有 8 到 24 位並行使用者。

重要 您可能需要同時最佳化 Horizon 7 和 Windows 桌面設定，才能達到此一使用者密度。

Horizon 7 建置區塊

一個建置區塊由多個實體伺服器、vSphere 基礎結構、多個 Horizon 7 Server、共用儲存及提供給使用者的虛擬機器桌面所組成。建置區塊是邏輯建構，且其規模不應超過 2,000 個 Horizon 桌面平台。客戶一般會在 Horizon 7 網繭中包含最多五個建置區塊，不過理論上，您可以使用多於五個區塊，只要此網繭不超過 10,000 個工作階段和 7 個 Horizon 連線伺服器執行個體。

表 4-11. 2,000 個虛擬機器桌面平台的 LAN 型 Horizon 建置區塊範例

項目	範例
vSphere 叢集	1 (含) 以上
80 連接埠網路交換器	1
共用儲存系統	1
vCenter Server 與 View Composer 位於同一個主機	1 (可在區塊本身中執行)
資料庫	MS SQL Server 或 Oracle 資料庫伺服器 (可在區塊本身中執行)
VLAN	3 (下列網路各有一個 1Gbit 乙太網路：管理網路、儲存網路和 VMotion 網路)

每台 vCenter Server 最多可支援 10,000 個虛擬機器。此支援可讓您有包含超過 2,000 個虛擬機器桌面平台的建置區塊。但是，實際區塊大小也會受制於其他 Horizon 7 特有的限制。

如果網繭中只有一個建置區塊，請使用兩個連線伺服器執行個體以提供備援。

Horizon 7 網繭 (Pod)

網繭 (Pod) 是由 Horizon 7 擴充性限制決定的組織單位。

使用五個建置區塊的網繭 (Pod) 範例

傳統的 Horizon 7 網繭會整合五個有 2,000 位使用者的建置區塊，讓您可以視為一個實體來管理。

表 4-12. 由 5 個建置區塊構成的 LAN 型 Horizon 7 網繭 (Pod) 範例

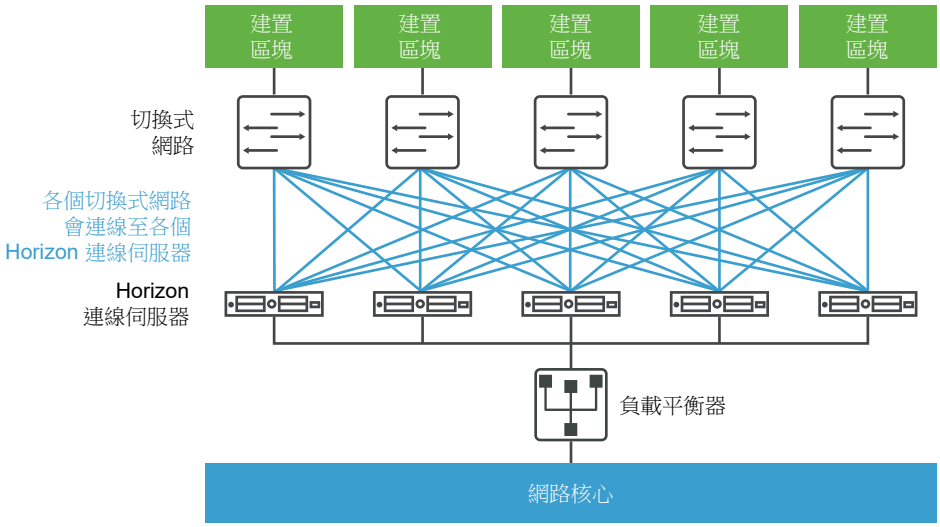
項目	數量
Horizon 7 網繭的建置區塊	5
vCenter Server 與 View Composer	5 (1 個虛擬機器主控各建置區塊中的兩者)
資料庫伺服器	5 (每個建置區塊各 1 部獨立資料庫伺服器) MS SQL Server 或 Oracle 資料庫伺服器
連線伺服器	7 (5 個用於來自企業網路內部的連線，2 個用於來自外部的連線)
vLAN	請參閱表 4-11. 2,000 個虛擬機器桌面平台的 LAN 型 Horizon 建置區塊範例。
10Gb 乙太網路模組	1
模組化網路交換器	1

每台 vCenter Server 最多可支援 35,000 個登錄的虛擬機器。此支援可讓您有包含超過 2,000 個虛擬機器桌面平台的建置區塊。但是，實際區塊大小也會受制於其他 Horizon 7 特有的限制。

對於此處說明的兩個範例，網路核心可以平衡各連線伺服器執行個體間的傳入要求負載。通常在網路層級支援備援和容錯移轉機制，可以防止負載平衡器變成單一失敗點。例如，虛擬路由器備援通訊協定 (VRRP) 可與負載平衡器通訊，以加入備援和容錯移轉功能。

如果連線伺服器執行個體在使用中的工作階段期間失敗或無法回應，使用者並不會遺失資料。桌面平台狀態會保留在虛擬機器桌面平台中，所以使用者可以連線至其他的連線伺服器執行個體，而桌面工作階段會從失敗發生點的位置繼續。

圖 4-2. 10,000 個虛擬機器桌面平台的網繭圖



使用一個 vCenter Server 的網繭 (Pod) 範例

在上一節，Horizon 7 網繭 (Pod) 由多個建置區塊所組成。每個建置區塊使用單一 vCenter Server 支援 2,000 個虛擬機器。VMware 收到客戶與合作夥伴提出的許多要求，他們希望使用單一 vCenter Server 來管理 Horizon 7 網繭 (Pod)。此要求源於單一 vCenter Server 執行個體可支援 10,000 個虛擬機器的事實。客戶可以使用單一 vCenter Server 來管理具有 10,000 個桌面平台的環境。本主題說明以使用單一 vCenter Server 管理 10,000 個桌面平台為基礎的架構。

雖然將一個 vCenter Server 和一個 View Composer 用於 10,000 個桌面是可能的，但是這樣會產生單一失敗點的情況。若遺失該單一 vCenter Server，整個桌面部署就無法進行電源、佈建和重新調整作業。基於這個原因，請選擇符合所需整體元件復原能力的部署架構。

在此範例中，包含 10,000 位使用者的網繭 (Pod) 包含實體伺服器、vSphere 基礎結構、Horizon 7 伺服器、共用儲存，以及 5 個叢集 (每個叢集各有 2,000 個虛擬桌面)。

表 4-13. 使用一個 vCenter Server 的 LAN 型 Horizon 7 網繭 (Pod) 範例

項目	範例
vSphere 叢集	6 (5 個叢集，每個叢集各有一個連結複製即區，以及 1 個基礎結構叢集)
vCenter Server	1

表 4-13. 使用一個 vCenter Server 的 LAN 型 Horizon 7 網繭 (Pod) 範例 (續)

項目	範例
View Composer	1 (獨立式)
資料庫伺服器	1 (獨立式) MS SQL Server 或 Oracle 資料庫伺服器
Active Directory 伺服器	1 或 2
連線伺服器執行個體	5
安全伺服器	5
vLAN	8 (5 個用於桌面集區叢集，管理、VMotion 和基礎結構叢集各使用 1 個)

Cloud Pod 架構概觀

在需要跨越資料中心部署 Horizon 的案例中，若要跨 WAN、MAN (都會區域網路) 或其他非 LAN 使用複寫的連線伺服器執行個體群組，您必須使用 Cloud Pod 架構功能。

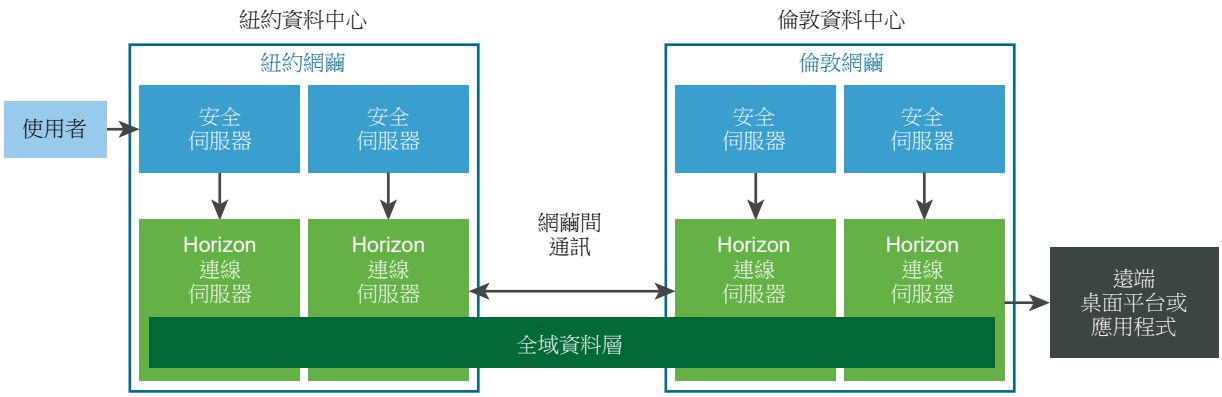
此功能使用標準 Horizon 元件提供跨資料中心管理、全域和彈性的使用者至桌面平台的對應、高可用性桌面平台，以及災難復原功能。

一般的 Cloud Pod 架構拓撲由兩個或多個網繭組成，這些網繭在網繭聯盟中會連結在一起。網繭聯盟受到某些限制。

表 4-14. 網繭聯盟限制

物件	限制
工作階段總計	250,000
網繭 (Pod)	50
每一網繭的工作階段	12,000
站台	15
每個網繭的連線伺服器執行個體	7
連線伺服器執行個體總計	350

下圖為基本 Cloud Pod 架構 拓撲範例。



在拓撲範例中，先前在不同資料中心的兩個獨立網繭聯結在一起，形成單一網繭聯盟。在此環境下，使用者可以連線至紐約資料中心的連線伺服器執行個體，並接收倫敦資料中心的桌面平台或應用程式。

IPv6 環境中不支援 Cloud Pod 架構 功能。

如需詳細資訊，請參閱《在 Horizon 7 中管理 Cloud Pod 架構》文件。

使用網繭 (Pod) 中多個 vCenter Server 的優點

當您建立 Horizon 7 生產環境的設計，而該環境可容納超過 500 個桌面時，有幾個考量事項會影響到是否使用一個 vCenter Server 執行個體，而不使用多個執行個體。

從 View 5.2 開始，VMware 支援使用單一 vCenter 5.1 或更新伺服器管理單一 Horizon 7 網繭內多達 10,000 個桌面平台虛擬機器。在您嘗試使用單一 vCenter Server 執行個體管理 10,000 個虛擬機器之前，請考量下列幾個事項：

- 公司的維護時段長度
- 能容許 Horizon 7 元件失敗的功能
- 電源、佈建和重新調整作業的頻率
- 基礎結構的簡化度

維護時段長度

虛擬機器電源、佈建和維護作業的並行設定，會依每個 vCenter Server 執行個體而定。

包含一個 vCenter Server 執行個體的網繭 (Pod) 設計	並行設定會決定整個 Horizon 7 網繭 (Pod) 一次最多可佇列多少個作業。 例如，如果您將並行佈建作業設為 20，而網繭 (Pod) 中只有一個 vCenter Server 執行個體，則桌面集區超過 20 個作業時，將會導致佈建作業序列化。在同時佇列 20 個並行作業之後，必須先完成一個作業，然後再開始下一個作業。在大規模的 Horizon 7 部署中，此佈建作業可能需要很長的時間才能完成。
包含多個 vCenter Server 執行個體的網繭 (Pod) 設計	每個執行個體可同時佈建 20 個虛擬機器。

為確保能在某個維護時段內同時完成更多個作業，您可以將多個 vCenter Server 執行個體 (最多五個) 新增至網繭 (Pod)，然後將多個桌面平台集區部署在使用個別 vCenter Server 執行個體所管理的 vSphere 叢集中。一個 vSphere 叢集一次只能使用一個 vCenter Server 執行個體來管理。為達成跨 vCenter Server 執行個體的並行作業，您也必須隨之部署桌面平台集區。

能容許元件失敗的功能

vCenter Server 在 Horizon 7 網繭 (Pod) 中的角色是提供電源、佈建和重新調整 (重新整理、重新撰寫和重新平衡) 作業。在虛擬機器桌面平台已部署且開啟電源後，Horizon 7 不會依賴 vCenter Server 進行一般程序的作業。

因為每個 vSphere 叢集都必須透過單一 vCenter Server 執行個體來管理，所以此伺服器代表著每個 Horizon 7 設計中的單一失敗點。此風險也同樣存在於每個 View Composer 執行個體。(每個 View Composer 執行個體和 vCenter Server 執行個體之間是一對一的對應關係)。 使用下列其中一項產品可減緩 vCenter Server 或 View Composer 中斷所產生的衝擊：

- VMware vSphere High Availability (HA)
- 相容的第三方容錯移轉產品

重要 若要使用其中一項容錯移轉策略，vCenter Server 執行個體必須安裝在屬於叢集的虛擬機器中，且該叢集必須由 vCenter Server 執行個體所管理。

除了 vCenter Server 容錯移轉的這些自動化選項外，您也可以選擇在新的虛擬機器或實體伺服器上重建故障的伺服器。大多數的重要資訊均儲存在 vCenter Server 資料庫。

風險承受度是決定網繭 (Pod) 設計中要使用一個、還是多個 vCenter Server 執行個體的重要因素。如果您的作業需要執行桌面管理工作的能力，例如同時執行所有桌面的電源和重新調整作業，則您應該藉由部署多個 vCenter Server 執行個體，將中斷的影響一次分散在較少的桌面中。如果您可以容許桌面環境長期無法進行管理或佈建作業，或是您選擇使用手動重建程序，則可以為網繭 (Pod) 部署單一 vCenter Server 執行個體。

電源、佈建和重新調整作業的頻率

有些虛擬機器桌面平台的電源、佈建和重新調整作業只透過管理員動作來起始，通常可以預測且可以控制，並且可以限制在所設定的維護時段內。有些虛擬機器桌面平台的電源和重新調整作業則透過使用者行為來觸發，例如使用「登出後重新整理」或「登出時暫停」設定，或使用指令碼動作來觸發，例如在使用者閒置期間使用 Distributed Power Management (DPM) 關閉閒置的 ESXi 主機。

如果 Horizon 7 設計不需要使用者觸發電源和重新調整作業，則單一 vCenter Server 執行個體也許就能符合您的需求。在沒有極頻繁的使用者觸發電源和重新調整作業之下，不會累積冗長的作業佇列，因此可能導致 Horizon 連線伺服器等待 vCenter Server 在定義的並行設定限制內完成所要求的作業時發生逾時。

許多客戶會選擇部署浮動集區，並使用「登出時重新整理」設定，以一律提供沒有來自先前工作階段之過時資料的桌面。過時資料的範例包括 `pagefile.sys` 或 Windows `temp` 檔案中未要求的記憶體分頁。浮動集區還可以透過經常重設桌面至已知的清潔狀態，將惡意程式碼的影響降至最低。

有些客戶會設定 Horizon 7 關閉未使用之桌面的電源，以降低用電量，如此一來，vSphere DRS (Distributed Resources Scheduler) 便可以將執行中的虛擬機器合併到最少數的 ESXi 主機上。VMware Distributed Power Management 接著關閉閒置主機的電源。在類似上述的案例中，多個 vCenter Server 執行個體更能顧及避免作業逾時所需的較頻繁電源和重新調整作業。

基礎結構的簡化度

大規模 Horizon 7 設計中的單一 vCenter Server 執行個體提供了一些吸引人的優點，例如，提供單一位置來管理最佳配置的主要映像和父虛擬機器、提供與 Horizon Administrator 主控台檢視一致的單一 vCenter Server 檢視，以及較少的生產後端資料庫和資料庫伺服器。相較於多個執行個體，一個 vCenter Server 的災難復原規劃比較容易。請確定您已權衡多個 vCenter Server 執行個體的利弊得失，例如，優點有維護時段長度與電源和重新調整作業的頻率等，而缺點有管理父虛擬機器映像的額外管理負荷和需要增加基礎結構元件數等。

混合式方法可能對您的設計有益。您可以選擇由一個 vCenter Server 執行個體管理相當靜態的極大集區，以及由多個 vCenter Server 執行個體管理較動態的較小桌面平台集區。升級現有大規模網繭 (Pod) 的最佳策略是，先升級現有網繭 (Pod) 中的 VMware 軟體元件。變更您的網繭設計之前，請衡量最新版本的電源、佈建和重新調整作業改善後的影響，然後實驗增加桌面平台集區的大小，以找出增加大型桌面平台集區與減少 vCenter Server 執行個體間的最佳平衡。

規劃安全功能

5

Horizon 7 提供強大的網路安全性，來保護機密的公司資料。若要更安全，您可以整合 Horizon 7 與特定第三方使用者驗證解決方案、使用安全伺服器，以及實作受限制權利功能。

重要 Horizon 6 (6.2 版) 及更新版本可使用 FIPS (聯邦資訊處理標準) 140-2 相容演算法來執行密碼編譯作業。您可透過以 FIPS 模式安裝 Horizon 7 來啟用這些演算法。並非所有功能在 FIPS 模式中皆受到支援。如需詳細資訊，請參閱《Horizon 7 安裝》文件。

本章節討論下列主題：

瞭解用戶端連線

Horizon Client 和 Horizon Administrator 可透過安全的 HTTPS 連線與 Horizon 連線伺服器主機進行通訊。在用戶端與伺服器之間進行 TLS 信號交換的過程中，系統會將連線伺服器上的伺服器憑證資訊傳達給用戶端。

當使用者開啟 Horizon Client 並提供連線伺服器、安全伺服器或 Unified Access Gateway 主機的完整網域名稱時，系統會建立初始 Horizon Client 連線，以用於使用者驗證以及遠端桌面平台和應用程式選取。當管理員在網頁瀏覽器中輸入 Horizon Administrator URL 時，系統會建立 Horizon Administrator 連線。

連線伺服器安裝期間，系統會產生預設的 TLS 伺服器憑證。依預設，當 TLS 用戶端造訪安全網頁 (如 Horizon Administrator) 時，便會向用戶端顯示此憑證。

您可以使用預設憑證進行測試，但應該盡可能換成自己的憑證。預設憑證未經商業憑證授權機構 (CA) 簽署。使用未經認證的憑證可能會讓不受信任者偽裝成您的伺服器來攔截流量。

- 使用 PCoIP 和 Blast 安全閘道進行用戶端連線

  當用戶端使用 VMware 的 PCoIP 或 Blast Extreme 顯示通訊協定連線至遠端桌面平台或應用程式時，Horizon Client 可進一步連線至 Horizon 連線伺服器執行個體、安全伺服器或 Unified Access Gateway 應用裝置上適用的安全閘道元件。此連線會提供從網際網路存取遠端桌面平台和應用程式時所需的安全層級和連線能力。

- 使用 Microsoft RDP 的通道用戶端連線

  當使用者使用 Microsoft RDP 顯示通訊協定連線至遠端桌面平台時，Horizon Client 可以透過 HTTPS 再次連線至 Horizon 連線伺服器主機。此連線稱為通道連線，因為這提供通道來載送 RDP 資料。

- 直接用戶端連線

  管理員可以設定 Horizon 連線伺服器設定，讓用戶端系統與已發佈的應用程式或桌面平台虛擬機器之間直接建立遠端桌面平台和已發佈的應用程式工作階段，以略過連線伺服器主機。這種連線類型稱為直接用戶端連線。

使用 PCoIP 和 Blast 安全閘道進行用戶端連線

當用戶端使用 VMware 的 PCoIP 或 Blast Extreme 顯示通訊協定連線至遠端桌面平台或應用程式時，Horizon Client 可進一步連線至 Horizon 連線伺服器執行個體、安全伺服器或 Unified Access Gateway 應用裝置上適用的安全閘道元件。此連線會提供從網際網路存取遠端桌面平台和應用程式時所需的安全層級和連線能力。

安全伺服器和 Unified Access Gateway 應用裝置包含 PCoIP 安全閘道元件和 Blast 安全閘道元件，這些元件提供下列優點：

- 唯一可進入公司資料中心的遠端桌面平台和應用程式流量是代表經過嚴格驗證之使用者的流量。
- 使用者只能存取其有權存取的資源。
- PCoIP 安全閘道連線支援 PCoIP，而 Blast 安全閘道連線支援 Blast Extreme。兩者都是進階遠端顯示通訊協定，能夠藉由封裝 UDP (而不是 TCP) 的視訊顯示封包，讓網路獲得更有效的使用。
- PCoIP 和 Blast Extreme 預設採用 AES-128 加密來保護其安全。不過，您可以將加密密碼變更為 AES-256。
- 只要顯示通訊協定沒有被任何網路元件封鎖，就不需要 VPN。例如，當某人嘗試從飯店房間內存取其遠端桌面平台或應用程式時，可能會發現飯店使用的 Proxy 並未設定為傳遞 UDP 封包。

  如需詳細資訊，請參閱 DMZ 型安全伺服器的防火牆規則。

安全伺服器可以在 Windows Server 2008 R2 及 Windows Server 2012 R2 作業系統上執行，並充分利用 64 位元架構。安全伺服器也可以利用支援進階加密標準新增指令 (AES New Instructions，AESNI) 的 Intel 處理器，以獲得高度最佳化的加密和解密效能。

如需 Unified Access Gateway 虛擬應用裝置的詳細資訊，請參閱《部署及設定 Unified Access Gateway》。

使用 Microsoft RDP 的通道用戶端連線

當使用者使用 Microsoft RDP 顯示通訊協定連線至遠端桌面平台時，Horizon Client 可以透過 HTTPS 再次連線至 Horizon 連線伺服器主機。此連線稱為通道連線，因為這提供通道來載送 RDP 資料。

通道連線提供下列優點：

- RDP 資料會通過 HTTPS，並使用 SSL 來加密。這個功能強大的安全性通訊協定與其他安全網站提供的安全性相同，例如，網路銀行和信用卡支付所使用的安全性。
- 用戶端可以透過單一 HTTPS 連線存取多個桌面，這可降低整體通訊協定的額外負荷。
- 由於 Horizon 7 會管理 HTTPS 連線，因此基礎通訊協定的可靠性可獲得明顯提升。如果使用者暫時中斷網路連線，在恢復網路連線時會重新建立 HTTP 連線，且 RDP 連線會自動恢復，所以使用者無須重新連線和重新登入。

在連線伺服器執行個體標準部署中，HTTPS 安全連線會終止於連線伺服器。在 DMZ 部署中，HTTPS 安全連線則終止於安全伺服器或 Unified Access Gateway 應用裝置。請參閱準備使用安全伺服器，以取得 DMZ 部署和安全伺服器的相關資訊。

使用 PCoIP 或 Blast Extreme 顯示通訊協定的用戶端可以使用通道連線進行 USB 重新導向和多媒體重新導向 (MMR) 加速，但對於所有其他資料，在安全伺服器或 Unified Access Gateway 應用裝置上，PCoIP 會使用 PCoIP 安全閘道，而 Blast Extreme 則使用 Blast 安全閘道。如需詳細資訊，請參閱 使用 PCoIP 和 Blast 安全閘道進行用戶端連線 。

如需 Unified Access Gateway 虛擬應用裝置的詳細資訊，請參閱《部署及設定 Unified Access Gateway》。

直接用戶端連線

管理員可以設定 Horizon 連線伺服器設定，讓用戶端系統與已發佈的應用程式或桌面平台虛擬機器之間直接建立遠端桌面平台和已發佈的應用程式工作階段，以略過連線伺服器主機。這種連線類型稱為直接用戶端連線。

使用直接用戶端連線時，用戶端與連線伺服器主機之間仍會建立 HTTPS 連線，以便使用者驗證並選取遠端桌面平台和已發佈的應用程式，但不會使用第二個 HTTPS 連線 (通道連線)。

直接 PCoIP 和 Blast Extreme 連線包括下列內建的安全功能：

- 支援進階加密標準 (AES) 加密 (預設為開啟) 以及 IP 安全性 (IPsec)
- 支援第三方 VPN 用戶端

用戶端使用 Microsoft RDP 顯示通訊協定時，只有在您的部署是位於公司網路內時，與遠端桌面平台的直接用戶端連線才適用。使用直接用戶端連線時，RDP 流量會透過用戶端與桌面平台虛擬機器間的連線，以未加密的方式傳送。

選擇使用者驗證方法

Horizon 7 使用您現有的 Active Directory 基礎結構進行使用者驗證和管理。若要更安全，您可以將 Horizon 7 與雙因素驗證解決方案 (例如 RSA SecurID 和 RADIUS) 及智慧卡驗證解決方案整合在一起。

- Active Directory 驗證

  所有 Horizon 連線伺服器執行個體都會加入 Active Directory 網域，並且會根據已加入網域的 Active Directory，對使用者進行驗證。此外，也會根據存在信任協議的其他任何使用者網域，對使用者進行驗證。

- 使用雙因素驗證

  您可以將 Horizon 連線伺服器執行個體設定成使用者必須使用 RSA SecurID 驗證或 RADIUS (遠端驗證撥入使用者服務) 驗證。

- 智慧卡驗證

  智慧卡是一張內嵌電腦晶片的小塑膠卡。許多政府機關及大型企業均採用智慧卡，來驗證存取其電腦網路的使用者。美國國防部使用的一種智慧卡稱為「通用存取卡」(CAC)。

- 使用隨 Windows 系統的 Horizon Client 提供的以目前使用者身分登入功能

  透過 Windows 版 Horizon Client，當使用者選取**選項**功能表中的**以目前使用者身分登入**時，就會使用他們在登入用戶端系統時提供的認證，對 Horizon 連線伺服器執行個體與遠端桌面平台進行驗證。不需要進一步驗證使用者。

Active Directory 驗證

所有 Horizon 連線伺服器執行個體都會加入 Active Directory 網域，並且會根據已加入網域的 Active Directory，對使用者進行驗證。此外，也會根據存在信任協議的其他任何使用者網域，對使用者進行驗證。

例如，如果連線伺服器執行個體是網域 A 的成員，且網域 A 和網域 B 之間存在信任協議，則來自網域 A 和網域 B 的使用者都可以使用 Horizon Client 連線至連線伺服器執行個體。

同樣地，如果在混合型網域環境中，網域 A 和 MIT Kerberos 領域之間存在信任協議，則來自 Kerberos 領域的使用者在使用 Horizon Client 連線至連線伺服器執行個體時，可以選取 Kerberos 領域名稱。

您可以將使用者和群組放在下列 Active Directory 網域中：

- 連線伺服器網域
- 與連線伺服器網域具有雙向信任關係的不同網域
- 位在與連線伺服器網域不同的樹系中，且由連線伺服器網域透過單向外部或領域信任關係而信任的網域
- 位在與連線伺服器網域不同的樹系中，且由連線伺服器網域透過單向或雙向可轉移樹系信任關係而信任的網域

連線伺服器會從主機所在的網域開始周遊信任關係，來判定可以存取哪些網域。若是一組連線良好的小型網域，連線伺服器可以快速判斷完整的網域清單，但所需的時間會隨著網域數目的增加以及網域間連線的減少而增加。此清單可能也包含使用者登入其遠端桌面平台和應用程式時，您希望不要提供給使用者的網域。

管理員可以使用 vdmadmin 命令列介面設定網域篩選，以限制連線伺服器執行個體搜尋並向使用者顯示的網域。如需詳細資訊，請參閱《Horizon 7 管理》文件。

如限制允許的登入時數和設定密碼到期日之類的原則，也會透過既有的 Active Directory 作業程序進行處理。

使用雙因素驗證

您可以將 Horizon 連線伺服器執行個體設定成使用者必須使用 RSA SecurID 驗證或 RADIUS (遠端驗證撥入使用者服務) 驗證。

- RADIUS 支援提供範圍廣泛的替代式雙因素 Token 型驗證選項。
- Horizon 7 也提供開放式標準擴充介面，讓協力廠商解決方案提供者將先進的驗證擴充整合至 Horizon 7。

由於雙因素驗證解決方案 (例如 RSA SecurID 和 RADIUS) 是與個別伺服器上安裝的驗證管理員搭配運作的，因此您必須先設定好這些伺服器，並使其可供連線伺服器主機存取。例如，如果使用 RSA SecurID，驗證管理員即為「RSA 驗證管理員」。如果使用 RADIUS，驗證管理員則為 RADIUS 伺服器。

若要使用雙因素驗證，每位使用者都必須擁有已向其驗證管理員註冊的 Token (例如 RSA SecurID Token)。雙因素驗證 Token 是一種硬體或軟體，會在固定的時間間隔內產生驗證碼。通常，驗證需要知道 PIN 和驗證碼。

如果您擁有多個連線伺服器執行個體，您可以在某些執行個體上設定雙因素驗證，並在其他執行個體上設定不同的使用者驗證方法。例如，您可以僅針對透過網際網路從公司網路外部存取遠端桌面平台和應用程式的使用者，設定雙因素驗證。

Horizon 7 是透過 RSA SecurID Ready 程式認證，且支援完整的 SecurID 功能，包括「新 PIN 模式」、「下一個 Token 碼模式」、「RSA 驗證管理員」及負載平衡。

智慧卡驗證

智慧卡是一張內嵌電腦晶片的小塑膠卡。許多政府機關及大型企業均採用智慧卡，來驗證存取其電腦網路的使用者。美國國防部使用的一種智慧卡稱為「通用存取卡」(CAC)。

管理員可啟用個別的連線伺服器執行個體進行智慧卡驗證。若要讓連線伺服器執行個體使用智慧卡驗證，則通常需要將根憑證新增至信任存放區檔案，然後修改連線伺服器設定。

所有用戶端連線 (包括使用智慧卡驗證的用戶端連線) 都會啟用 TLS/SSL。

若要使用智慧卡，用戶端機器必須有智慧卡中介軟體和智慧卡讀卡機。若要在智慧卡上安裝憑證，您必須設定電腦作為註冊站。如需特定類型 Horizon Client 是否支援智慧卡的相關資訊，請參閱 Horizon Client 說明文件，網址：https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

使用隨 Windows 系統的 Horizon Client 提供的以目前使用者身分登入功能

透過 Windows 版 Horizon Client，當使用者選取**選項**功能表中的**以目前使用者身分登入**時，就會使用他們在登入用戶端系統時提供的認證，對 Horizon 連線伺服器執行個體與遠端桌面平台進行驗證。不需要進一步驗證使用者。

為了支援此功能，使用者認證會儲存在連線伺服器執行個體與用戶端系統上。

- 在連線伺服器執行個體上，使用者認證會進行加密，並連同使用者名稱、網域與選用 UPN 一起儲存在使用者工作階段中。進行驗證時，認證會新增；工作階段物件毀損時，認證會清除。當使用者登出、工作階段逾時或驗證失敗時，工作階段物件即毀損。工作階段物件位於動態記憶體中，而未儲存在 Horizon LDAP 或磁碟檔案中。
- 在連線伺服器執行個體上啟用**接受以目前使用者身分登入**設定，可讓連線伺服器執行個體接受使用者在 Horizon Client 的**選項**功能表中選取**以目前使用者身分登入**時所傳遞的使用者身分識別和認證資訊。

  重要 在啟用此設定之前，必須先瞭解安全性風險。請參閱《Horizon 7 安全性》文件中的〈使用者驗證的安全性相關伺服器設定〉。

- 在用戶端系統上，使用者認證已加密並儲存在 Authentication Package (Horizon Client 的元件) 的資料表中。當使用者登入時，會新增認證，當使用者登出時，會將認證從資料表中移除。資料表位在動態記憶體中。

管理員可以使用 Horizon Client 群組原則設定，控制**選項**功能表中的**以目前使用者身分登入**設定的可用性，及指定其預設值。管理員也可以使用群組原則，指定哪些連線伺服器執行個體會接受使用者在 Horizon Client 中選取**以目前使用者身分登入**時傳遞的使用者身分識別與認證資訊。

在使用者透過「以目前使用者身分登入」功能登入連線伺服器後，會啟用遞迴解除鎖定功能。遞迴解除鎖定功能可在用戶端機器解除鎖定之後才解除鎖定所有遠端工作階段。管理員可透過 Horizon Client 中的**用戶端機器解除鎖定時，解除鎖定遠端工作階段**全域原則設定，來控制遞迴解除鎖定功能。如需 Horizon Client 之全域原則設定的詳細資訊，請參閱 VMware Horizon Client 說明文件網頁上的 Horizon Client 說明文件。

「以目前使用者身分登入」功能的限制與需求如下：

- 當連線伺服器執行個體上的智慧卡驗證設為「必要」時，連線至連線伺服器執行個體時選取**以目前使用者身分登入**的使用者將會驗證失敗。這些使用者必須在登入連線伺服器時，以其智慧卡和 PIN 碼重新驗證。
- 用戶端登入系統的時間，必須與連線伺服器主機的時間同步。
- 如果在用戶端系統上修改預設的**從網路存取此電腦**使用者權限指派，則必須依照 VMware 知識庫 (KB) 文章 1025691 所述進行修改。
- 用戶端機器必須能夠與企業的 Active Directory 伺服器通訊，且不使用快取的認證進行驗證。例如，如果使用者從企業網路外登入其用戶端機器，則會使用快取的認證進行驗證。如果使用者接著嘗試連線至安全伺服器或連線伺服器執行個體，而未先建立 VPN 連線，則系統會提示使用者提供認證，且「以目前使用者身分登入」功能將無法運作。

限制遠端桌面平台存取權

您可以使用受限制權利功能，根據使用者所連線的 Horizon 連線伺服器執行個體，來限制遠端桌面平台存取。

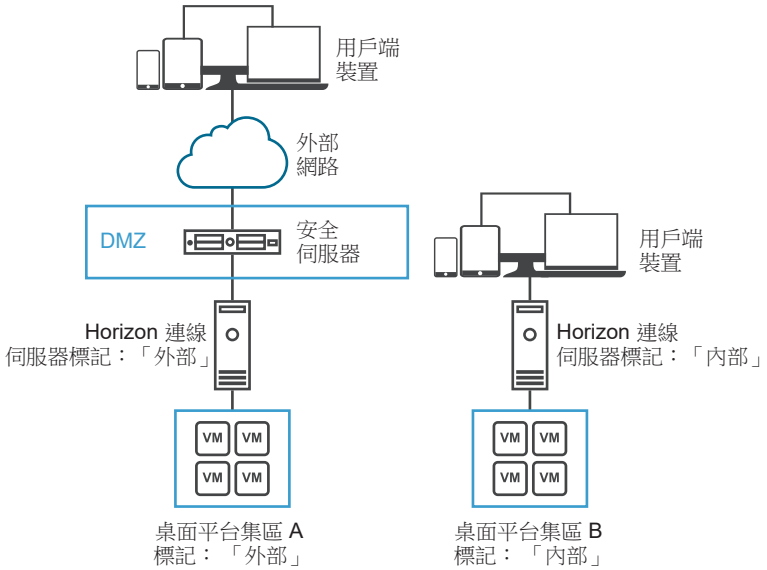
透過受限制權利，您可將一或多個標記指派給連線伺服器執行個體。接著當設定桌面平台集區時，您選取您要能夠存取桌面平台集區的連線伺服器執行個體其標記。使用者透過標記的連線伺服器執行個體登入時，只能存取至少有一個相符標記或沒有任何標記的桌面平台集區。

例如，Horizon 7 部署可能包含兩個連線伺服器執行個體。第一個執行個體支援內部使用者。第二個執行個體與安全伺服器配對，支援外部使用者。為防止外部使用者存取某些桌面，您可以設定受限制權利，如下所示：

- 將「內部」標記指派給支援您內部使用者的連線伺服器執行個體。
- 將「外部」標記指派給與安全伺服器配對並支援您外部使用者的連線伺服器執行個體。
- 將「內部」標記指派給應僅供內部使用者存取的桌面平台集區。
- 將「外部」標記指派給應僅供外部使用者存取的桌面平台集區。

外部使用者看不見標記為「內部」的桌面平台集區，因為他們是透過標記為「外部」的連線伺服器登入的，而內部使用者看不見標記為「外部」的桌面平台集區，因為他們是透過標記為「內部」的連線伺服器登入的。圖 5-1. 受限制的權利範例 會圖解此組態。

圖 5-1. 受限制的權利範例



您也可以使用受限制權利，以根據您為特定連線伺服器執行個體設定的使用者驗證方法，控制桌面平台存取權。例如，您可以讓某些桌面平台集區僅供已透過智慧卡驗證的使用者使用。

限制權利功能只會執行標記比對。您必須設計您的網路拓撲，強制讓某些用戶端透過特定的連線伺服器執行個體來連線。

使用群組原則設定保護遠端桌面平台和應用程式的安全

Horizon 7 包含群組原則管理 ADMX 範本，這些範本包含與安全性相關的群組原則設定，供您用於保護遠端桌面平台和應用程式的安全。

例如，您可以使用群組原則設定執行下列工作。

- 指定使用者在 Windows 版 Horizon Client 中選取**以目前使用者身分登入**核取方塊時，可接受使用者識別碼和認證資訊的連線伺服器執行個體。
- 在 Horizon Client 中為智慧卡驗證啟用 Single Sign-On。
- 在 Horizon Client 中設定伺服器 TLS 憑證檢查。
- 阻止使用者使用 Horizon Client 命令列選項提供認證資訊。
- 阻止非 Horizon Client 系統使用 RDP 連線至遠端桌面平台。您可以設定此原則，讓連線必須由 Horizon Client 管理，也就是說，使用者必須使用 Horizon 7 連線至遠端桌面平台。

如需使用遠端桌面平台和 Horizon Client 群組原則設定的相關資訊，請參閱《在 Horizon 7 中設定遠端桌面平台功能》文件。

使用 智慧原則

您可以將 智慧原則 用於已發佈的桌面平台或應用程式中的使用者環境設定，也可以用於在電腦開機或工作階段重新連線期間套用的電腦環境設定。

您可以為使用者環境設定建立原則，以控制 USB 重新導向、虛擬列印、剪貼簿重新導向、用戶端磁碟機重新導向、Web 和 Chrome 檔案傳輸功能，以及頻寬設定檔在已發佈的桌面平台或應用程式中的行為。使用者環境設定的 Horizon 智慧型原則會在登入期間套用，且可在工作階段重新連線期間重新整理。若要在使用者重新連線至工作階段時重新套用 Horizon 智慧型原則，您可以設定觸發的工作。

您可以為 Dynamic Environment Manager 在使用者電腦開機時套用的電腦環境設定建立原則。這些 Horizon 智慧型原則會控制 Flash 多媒體重新導向、Integrated Printing 和 USB 重新導向的行為。電腦環境設定的 Horizon 智慧型原則會在電腦開機期間套用，且可在工作階段重新連線期間重新整理。

使用智慧原則，您可以建立只在符合特定條件時才生效的原則。例如，您可以設定一個原則，在使用者從公司網路外部連線至遠端桌面平台時，停用用戶端磁碟機重新導向功能。

智慧原則 功能需要 Dynamic Environment Manager。如需更多資訊，請參閱《在 Horizon 7 中設定遠端桌面平台功能》中關於智慧原則的主題。

實施最佳做法來保護用戶端系統

實施這些最佳做法來保護用戶端系統。

- 請確定已設定用戶端系統在閒置一段時間後會進入睡眠狀態，使用者必須輸入密碼才能喚醒電腦。
- 要求使用者在啟動用戶端系統時，輸入使用者名稱和密碼。請勿設定用戶端系統允許自動登入。
- 若是 Mac 用戶端系統，請考慮對金鑰鏈和使用者帳戶設定不同的密碼。密碼不同時，在系統代替使用者輸入任何密碼之前，會顯示提示。此外，也請考量開啟 FileVault 防護。

如需 Horizon 7 提供的所有安全功能的簡要參考資料，請參閱 Horizon 7 安全性文件。

指定管理員角色

Horizon 7 環境中的一個金鑰管理工作會用來決定誰可以使用 Horizon Administrator，以及這些使用者有權執行哪些工作。

在 Horizon Administrator 中執行工作的授權，是由包含管理員角色和權限的存取控制系統所管理。一個角色是多個權限的集合。權限可授予執行特定動作的能力，例如將桌面集區的權限授予使用者或變更組態設定。權限也能控制管理員可在 Horizon Administrator 看到哪些內容。

管理員可以建立資料夾以細分桌面平台集區，然後將特定桌面平台集區的管理委派給 Horizon Administrator 中的不同管理員。管理員可以藉由將角色指定給資料夾的使用者，設定管理員對資料夾中資源的存取權。管理員僅能存取位於已指定角色的資料夾中的資源。管理員對資料夾所具備的角色會決定管理員對該資料夾中資源所擁有的存取層級。

Horizon Administrator 包含一組預先定義的角色。管理員也可以組合所選取的權限來建立自訂角色。

準備使用安全伺服器

安全伺服器是 Horizon 連線伺服器的一個特殊執行個體，可執行一部分的連線伺服器功能。您可以使用安全伺服器，為網際網路和內部網路之間提供多一層的安全性。

重要 透過 Horizon 6 (6.2 版) 及更新版本，您可以使用 Unified Access Gateway 應用裝置來取代安全伺服器。Unified Access Gateway 應用裝置會部署為強化的虛擬應用裝置，以 Linux 型應用裝置為基礎，並經過自訂以提供安全存取。如需 Unified Access Gateway 虛擬應用裝置的詳細資訊，請參閱《部署及設定 Unified Access Gateway》。

安全伺服器位於 DMZ 內，可用作 Proxy 主機以在受信任網路內進行連線。每個安全伺服器都會與一個連線伺服器執行個體配對，並將所有流量轉送至該執行個體。您可以將多個安全伺服器與單一連線伺服器配對。此設計會阻擋面向公眾的網際網路來保護連線伺服器執行個體，以及強制所有為受保護的工作階段通過安全伺服器，因此可提供多一層的安全性。

DMZ 型安全伺服器部署需要在防火牆上開啟幾個連接埠，以允許用戶端連線至 DMZ 內的安全伺服器。您也必須在內部網路中，設定安全伺服器和連線伺服器執行個體之間的通訊連接埠。請參閱 DMZ 型安全伺服器的防火牆規則，以取得特定連接埠的相關資訊。

由於使用者可以從內部網路直接與任何連線伺服器執行個體連線，所以不必在 LAN 型部署中實作安全伺服器。

備註 安全伺服器包括一個 PCoIP 安全閘道元件和一個 Blast 安全閘道元件，以便於使用 PCoIP 或 Blast Extreme 顯示通訊協定的用戶端可使用安全伺服器而不是 VPN。

如需設定 VPN 以使用 PCoIP 的相關資訊，請參閱 VPN 解決方案總覽，您可在 http://www.vmware.com/products/view/resources.html 的技術資源中心的「技術合作夥伴資源」一節取得。

部署安全伺服器的最佳做法

操作 DMZ 中的安全伺服器時，請遵循最佳做法安全性原則與程序。

DMZ Virtualization with VMware Infrastructure 白皮書提供虛擬化 DMZ 的最佳做法範例。這份白皮書中的許多建議也適用於實體 DMZ。

若要限制框架廣播的範圍，與安全伺服器配對的 Horizon 連線伺服器執行個體應部署於隔離的網路上。此拓撲有助於防止內部網路上的惡意使用者監控安全伺服器與連線伺服器執行個體之間的通訊。

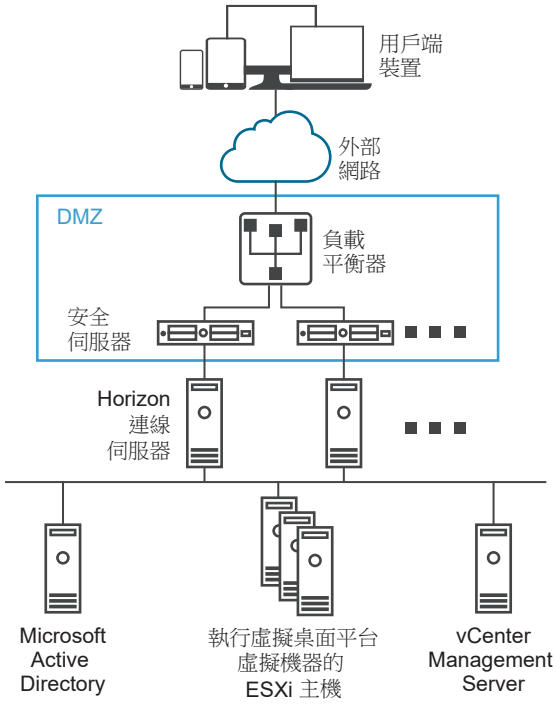
或者，您也可以使用網路交換器上的進階安全功能，防止惡意監控安全伺服器與連線伺服器間的通訊，並遏止監控攻擊，例如 ARP 快取毒害。請參閱您網路設備的管理文件，以取得詳細資訊。

安全伺服器拓撲

您可以實作幾種不同的安全伺服器拓撲。

圖 5-2. DMZ 中經過負載平衡的安全伺服器 所示拓撲顯示高可用性的環境，包括 DMZ 中兩個經過負載平衡的安全伺服器。安全伺服器會與內部網路中的兩個 Horizon 連線伺服器執行個體進行通訊。

圖 5-2. DMZ 中經過負載平衡的安全伺服器

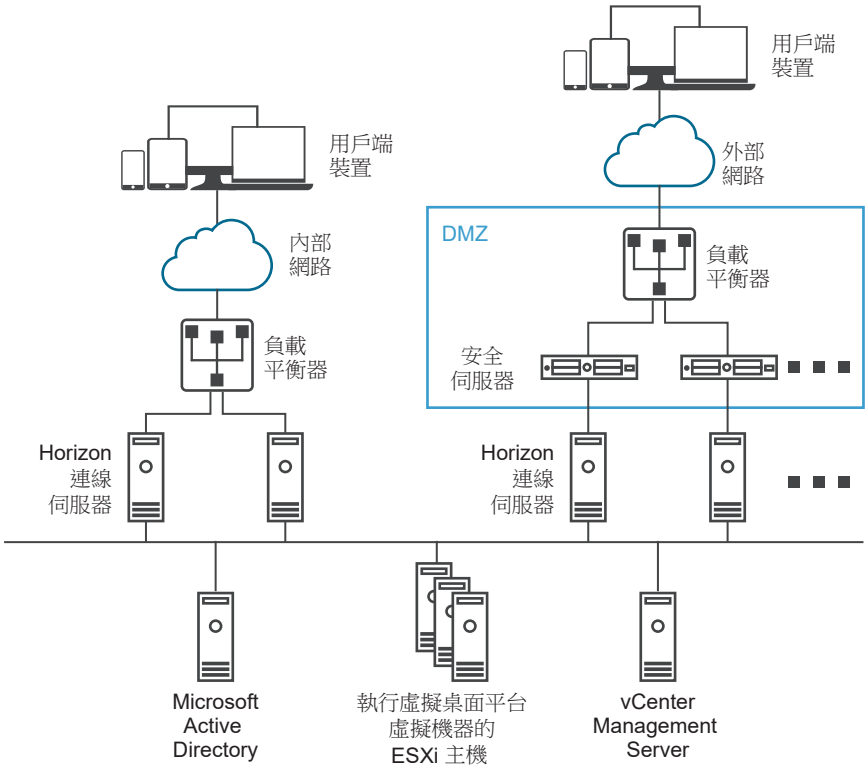


當企業網路以外的使用者連線至安全伺服器時，必須通過驗證，才能存取遠端桌面平台和應用程式。DMZ 兩端設有適當防火牆規則時，此拓撲適用於透過網際網路上的用戶端裝置存取遠端桌面平台和應用程式。

您可以將多個安全伺服器連線至各個連線伺服器執行個體。您也可以結合 DMZ 部署與標準部署，以提供存取權給內部使用者和外部使用者。

圖 5-3. 多個安全伺服器 中所示的拓撲，顯示四個連線伺服器執行個體用作一個群組的環境。內部網路中的執行個體會由內部網路使用者專用，而外部網路中的執行個體則由外部網路的使用者專用。如果啟用與安全伺服器配對的連線伺服器執行個體進行 RSA SecurID 驗證，則所有外部網路使用者都必須使用 RSA SecurID Token 進行驗證。

圖 5-3. 多個安全伺服器



如果安裝多個安全伺服器，將必須實作硬體或軟體負載平衡解決方案。連線伺服器未提供專屬的負載平衡功能。連線伺服器可與標準第三方負載平衡解決方案搭配運作。

DMZ 型安全伺服器的防火牆

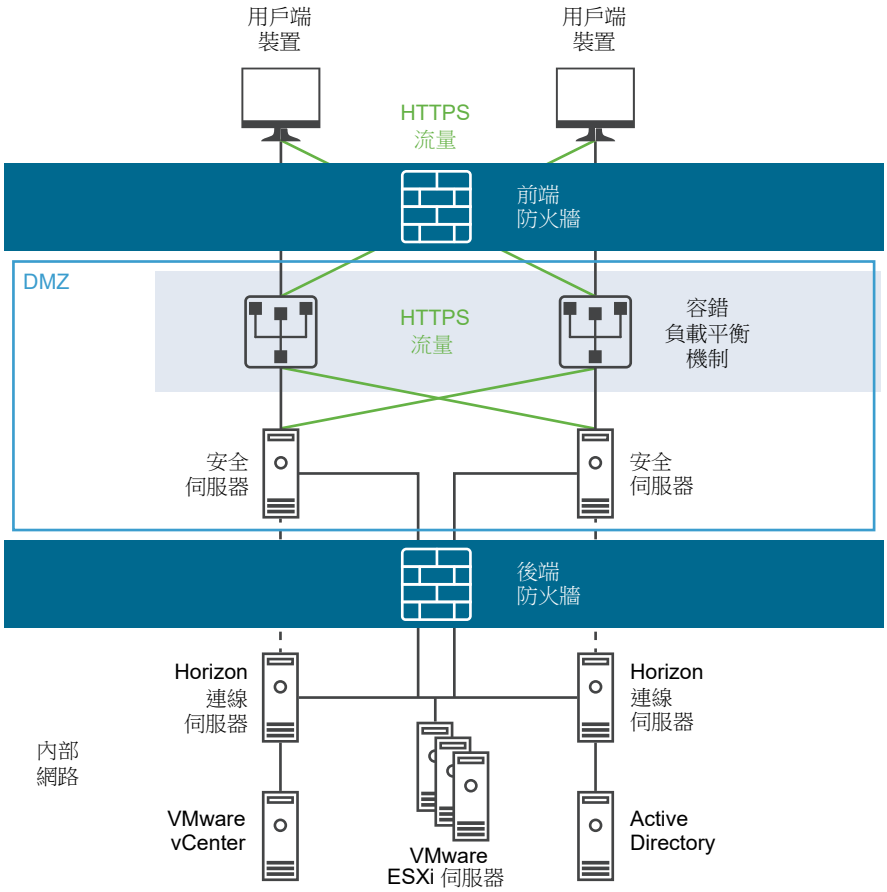
DMZ 型安全伺服器部署必須包含兩個防火牆。

- 保護 DMZ 和內部網路需要面向外部網路的前端防火牆。您可以設定此防火牆允許外部網路流量到達 DMZ。
- 提供第二層安全性則需要位於 DMZ 與內部網路之間的後端防火牆。您可以設定此防火牆僅接受發自 DMZ 內服務的流量。

防火牆原則可嚴格控制來自 DMZ 服務的輸入通訊，進而大幅降低內部網路出現漏洞的風險。如需關於設定安全伺服器所需連接埠的詳細資訊，請參閱《Horizon 7 安全性》文件。

下圖顯示包含前端和後端防火牆的組態範例。

圖 5-4. 雙防火牆拓撲



DMZ 型安全伺服器的防火牆規則

DMZ 型安全伺服器需要在前端和後端防火牆設定某些防火牆規則。在安裝期間，Horizon 7 服務預設設為接聽特定網路連接埠。必要時，您可以變更使用的連接埠號碼，以遵守組織政策或避免發生爭用情況。

重要 如需其他詳細資料和安全建議事項，請參閱《Horizon 7 安全性》文件。

前端防火牆規則

若要允許外部用戶端裝置連線至 DMZ 內的安全伺服器，前端防火牆必須允許特定 TCP 和 UDP 連接埠的流量。表 5-1. 前端防火牆規則 摘要了前端防火牆規則。

表 5-1. 前端防火牆規則

來源	預設連接埠	通訊協定	目的地	預設連接埠	備註
Horizon Client	TCP 任何連接埠	HTTP	安全伺服器	TCP 80	(選用) 外部用戶端裝置會在 TCP 連接埠 80 連線至 DMZ 內的安全伺服器，然後自動導向至 HTTPS。如需瞭解允許使用者使用 HTTP (而不是 HTTPS) 進行連線的相關安全考量，請參閱《Horizon 7 安全性》指南。
Horizon Client	TCP 任何連接埠	HTTPS	安全伺服器	TCP 443	外部用戶端裝置會在 TCP 連接埠 443 連線至 DMZ 內的安全伺服器，以便與連線伺服器執行個體、遠端桌面平台和應用程式進行通訊。

表 5-1. 前端防火牆規則 (續)

來源	預設連接埠	通訊協定	目的地	預設連接埠	備註
Horizon Client	TCP 任何連接埠 UDP 任何連接埠	PCoIP	安全伺服器	TCP 4172 UDP 4172	外部用戶端裝置會在 TCP 連接埠 4172 和 UDP 連接埠 4172 連線至 DMZ 內的安全伺服器，以便透過 PCoIP 與遠端桌面平台或應用程式進行通訊。
安全伺服器	UDP 4172	PCoIP	Horizon Client	UDP 任何連接埠	安全伺服器會從 UDP 連接埠 4172 將 PCoIP 資料傳回至外部用戶端裝置。目的地 UDP 連接埠將是所接收 UDP 封包的來源連接埠。由於這些封包包含回覆資料，所以通常不需要為此流量新增明確防火牆規則。
Horizon Client 或用戶端網頁瀏覽器	TCP 任何連接埠	HTTPS	安全伺服器	TCP 8443 UDP 8443	外部用戶端裝置和外部 Web 用戶端 (HTML Access) 會透過 HTTPS 連接埠 8443 連線至 DMZ 內的安全伺服器，以便與遠端桌面平台進行通訊。

後端防火牆規則

若要允許安全伺服器與內部網路中的所有 View 連線伺服器執行個體進行通訊，後端防火牆將必須允許特定 TCP 連接埠的傳入流量。在後端防火牆的後方，必須以類似方式設定內部防火牆，以允許遠端桌面平台應用程式與連線伺服器執行個體互相進行通訊。表 5-2. 後端防火牆規則 會摘要後端防火牆規則。

表 5-2. 後端防火牆規則

來源	預設連接埠	通訊協定	目的地	預設連接埠	備註
安全伺服器	UDP 500	IPSec	連線伺服器	UDP 500	安全伺服器會在 UDP 連接埠 500 與連線伺服器執行個體交涉 IPsec。
連線伺服器	UDP 500	IPSec	安全伺服器	UDP 500	連線伺服器執行個體會在 UDP 連接埠 500 回應安全伺服器。
安全伺服器	UDP 4500	NAT-T ISAKMP	連線伺服器	UDP 4500	如果在安全伺服器及其配對的連線伺服器執行個體之間使用 NAT，則需要此項目。安全伺服器會使用 UDP 連接埠 4500 周遊 NAT 並交涉 IPsec 安全性。
連線伺服器	UDP 4500	NAT-T ISAKMP	安全伺服器	UDP 4500	如果使用 NAT，則連線伺服器執行個體會在 UDP 連接埠 4500 回應安全伺服器。
安全伺服器	TCP 任何連接埠	AJP13	連線伺服器	TCP 8009	安全伺服器會在 TCP 連接埠 8009 連線至連線伺服器執行個體，以轉送來自外部用戶端裝置的 Web 流量。 如果您啟用 IPSec，則 AJP13 流量在配對之後不會使用 TCP 連接埠 8009。而是會透過 NAT-T (UDP 連接埠 4500) 或 ESP 傳送流量。
安全伺服器	TCP 任何連接埠	JMS	連線伺服器	TCP 4001	安全伺服器會在 TCP 連接埠 4001 連線至連線伺服器執行個體，以交換 Java Message Service (JMS) 流量。
安全伺服器	TCP 任何連接埠	JMS	連線伺服器	TCP 4002	安全伺服器會在 TCP 連接埠 4002 連線至連線伺服器執行個體，以交換安全 Java Message Service (JMS) 流量。
安全伺服器	TCP 任何連接埠	RDP	遠端桌面平台	TCP 3389	安全伺服器會在 TCP 連接埠 3389 連線至遠端桌面平台，以交換 RDP 流量。

表 5-2. 後端防火牆規則 (續)

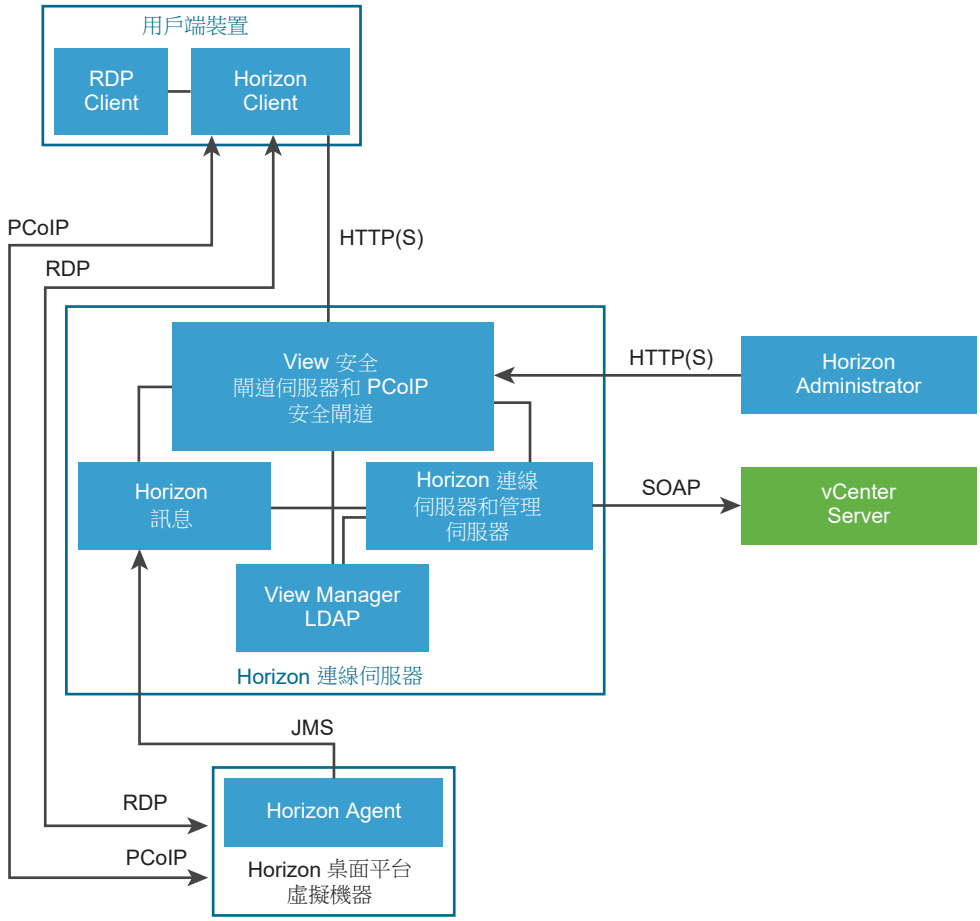
來源	預設連接埠	通訊協定	目的地	預設連接埠	備註
安全伺服器	TCP 任何連接埠	MMR	遠端桌面平台	TCP 9427	安全伺服器會在 TCP 連接埠 9427 連線至遠端桌面平台，以接收與多媒體重新導向 (MMR) 和用戶端磁碟機重新導向有關的流量。
安全伺服器	TCP 任何連接埠 UDP 55000	PCoIP	遠端桌面平台或應用程式	TCP 4172 UDP 4172	安全伺服器會在 TCP 連接埠 4172 和 UDP 連接埠 4172 連線至遠端桌面平台和應用程式，以交換 PCoIP 流量。
遠端桌面平台或應用程式	UDP 4172	PCoIP	安全伺服器	UDP 55000	遠端桌面平台和應用程式會從 UDP 連接埠 4172 將 PCoIP 資料回傳至安全伺服器。 目的地 UDP 連接埠將會是所接收 UDP 封包中的來源連接埠，由於這是回覆資料，所以通常不需要為此新增明確防火牆規則。
安全伺服器	TCP 任何連接埠	USB-R	遠端桌面平台	TCP 32111	安全伺服器在 TCP 連接埠 32111 連線至遠端桌面平台，以便在外部用戶端裝置與遠端桌面平台之間交換 USB 重新導向流量。
安全伺服器	TCP 或 UDP 任何連接埠	Blast Extreme	遠端桌面平台或應用程式	TCP 或 UDP 22443	安全伺服器會在 TCP 和 UDP 連接埠 22443 連線至遠端桌面平台和應用程式，以交換 Blast Extreme 流量。
安全伺服器	TCP 任何連接埠	HTTPS	遠端桌面平台	TCP 22443	如果您使用 HTML Access，安全伺服器會在 HTTPS 連接埠 22443 連線至遠端桌面平台，以便與 Blast Extreme 代理程式進行通訊。
安全伺服器		ESP	連線伺服器		無需 NAT 穿越時封裝的 AJP13 流量。ESP 為 IP 通訊協定 50。未指定連接埠號碼。
連線伺服器		ESP	安全伺服器		無需 NAT 穿越時封裝的 AJP13 流量。ESP 為 IP 通訊協定 50。未指定連接埠號碼。

瞭解通訊協定

Horizon 6 和 Horizon 7 元件會使用幾種不同的通訊協定來交換訊息。

圖 5-5. 沒有安全伺服器的 Horizon 6 和 Horizon 7 元件以及通訊協定 說明未設定安全伺服器時，各元件用於通訊的通訊協定。亦即，未開啟 RDP 安全通道、Blast 安全閘道和 PCoIP 安全閘道。一般 LAN 部署可能使用這種組態。

圖 5-5. 沒有安全伺服器的 Horizon 6 和 Horizon 7 元件以及通訊協定



備註 此圖顯示用戶端使用 PCoIP 或 RDP 進行直接連線。但預設設定是使用 PCoIP 直接連線和 RDP 通道連線。

請參閱表 5-3. 預設連接埠，瞭解各通訊協定所用的預設連接埠。

圖 5-6. 具有安全伺服器的 Horizon 6 和 Horizon 7 元件以及通訊協定 說明設定安全伺服器時，各元件用於通訊的通訊協定。一般 WAN 部署可能使用這種組態。

圖 5-6. 具有安全伺服器的 Horizon 6 和 Horizon 7 元件以及通訊協定

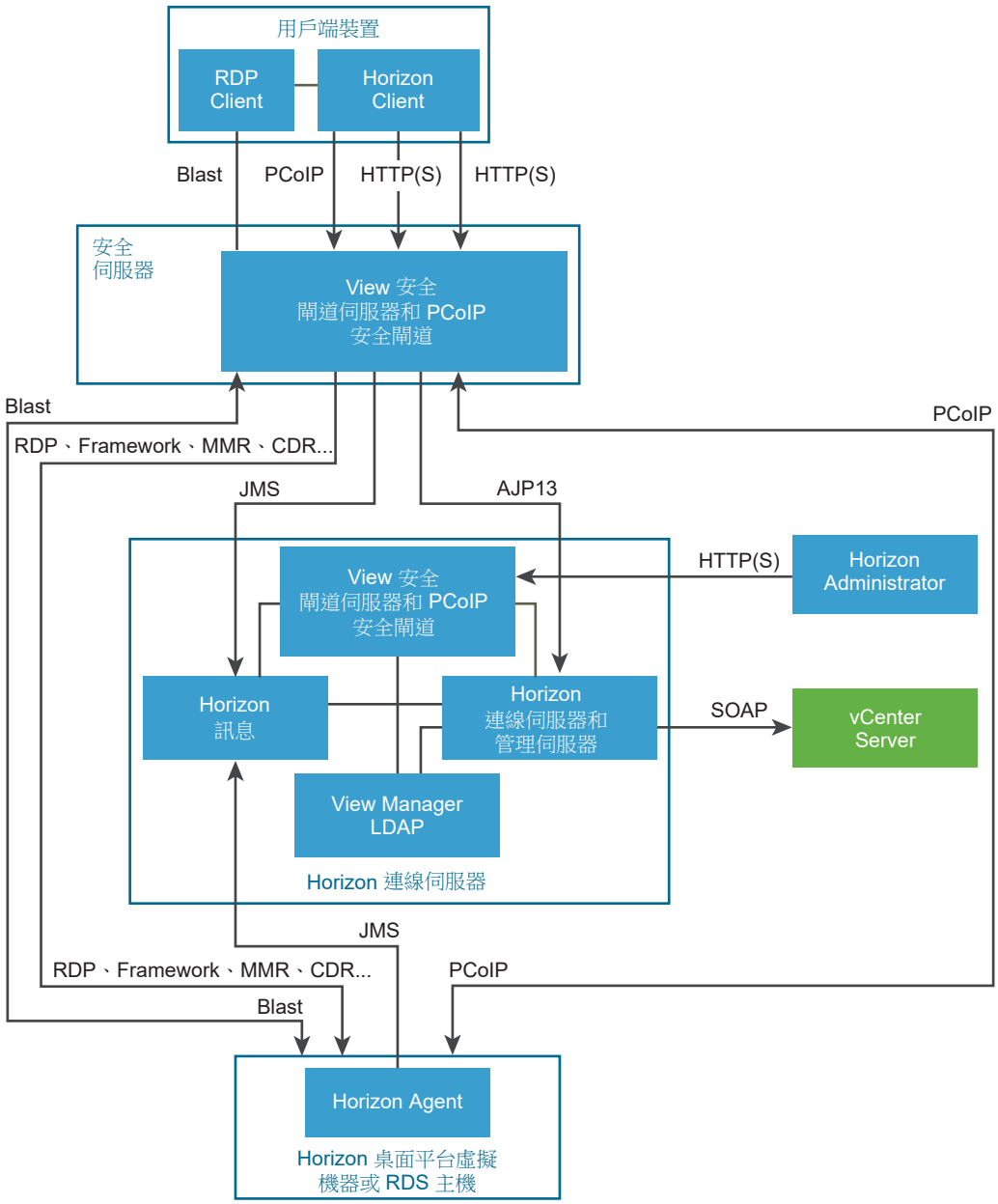


表 5-3. 預設連接埠 列出各通訊協定所用的預設連接埠。必要時，您可以變更使用的連接埠號碼，以遵守組織政策或避免發生爭用情況。

表 5-3. 預設連接埠

通訊協定	連接埠
JMS	TCP 連接埠 4001 TCP 連接埠 4002
AJP13	TCP 連接埠 8009 **備註** AJP13 只會用於安全伺服器組態。

表 5-3. 預設連接埠 (續)

通訊協定	連接埠
HTTP	TCP 連接埠 80
HTTPS	TCP 連接埠 443
MMR/CDR	針對多媒體重新導向和用戶端磁碟機重新導向，TCP 連接埠 9427
RDP	TCP 連接埠 3389 **備註** 如果設定連線伺服器執行個體以進行直接用戶端連線，則這些通訊協定會直接從用戶端連線至遠端桌面平台，而不會透過 View 安全閘道伺服器元件通道連線。
SOAP	TCP 連接埠 80 或 443
PCoIP	TCP 連接埠 4172 UDP 連接埠 4172、50002、55000
USB 重新導向	TCP 連接埠 32111。此連接埠也用於時區同步化。
VMware Blast Extreme	TCP 連接埠 8443、22443 UDP 連接埠 443、8443、22443
HTML Access	TCP 連接埠 8443、22443

用於連線伺服器互相通訊的 TCP 連接埠

群組中的連線伺服器執行個體會使用其他 TCP 連接埠互相通訊。例如，連線伺服器執行個體會使用連接埠 4100 或 4101 互相傳輸 JMS 路由器間 (JMSIR) 流量。群組中的連線伺服器執行個體之間通常不會使用防火牆。

View 安全閘道伺服器

View 安全閘道伺服器是伺服器端元件，用於在用戶端系統與安全伺服器、Unified Access Gateway 應用裝置或 View 連線伺服器執行個體之間建立安全的 HTTPS 連線。

當您設定連線伺服器的通道連線時，RDP、USB 和多媒體重新導向 (MMR) 流量會經由 View 安全閘道元件通道傳送。當您設定直接用戶端連線時，這些通訊協定會從用戶端直接連線至遠端桌面平台，不會經由 View 安全閘道伺服器元件通道連線。

備註 使用 PCoIP 或 Blast Extreme 顯示通訊協定的用戶端可以使用通道連線進行 USB 重新導向和多媒體重新導向 (MMR) 加速，但對於所有其他資料，在安全伺服器或 Unified Access Gateway 應用裝置上，PCoIP 會使用 PCoIP 安全閘道，而 Blast Extreme 則使用 Blast 安全閘道。

View 安全閘道伺服器也負責從用戶端轉送其他 Web 流量到連線伺服器，其中包括使用者驗證及桌面平台和應用程式選擇流量。View 安全閘道伺服器也會將 Horizon Administrator 用戶端 Web 流量傳遞到管理伺服器元件。

Blast 安全閘道

安全伺服器和 Unified Access Gateway 應用裝置包含 Blast 安全閘道元件。Blast 安全閘道啟用時，在驗證之後，使用 Blast Extreme 或 HTML Access 的用戶端可以進一步與安全伺服器或 Unified Access Gateway 應用裝置建立安全連線。此連線可讓用戶端從網際網路存取遠端桌面平台和應用程式。

啟用 Blast 安全閘道元件時，安全伺服器或 Unified Access Gateway 應用裝置會將 Blast Extreme 流量轉送至遠端桌面平台和應用程式。如果使用 Blast Extreme 的用戶端也使用 USB 重新導向功能或多媒體重新導向 (MMR) 加速，則可以啟用 View 安全閘道元件以轉送該資料。

設定直接用戶端連線時，Blast Extreme 流量及其他流量會直接從用戶端傳送到遠端桌面平台或應用程式。

當家庭或行動工作者之類的使用者從網際網路存取桌面平台時，安全伺服器或 Unified Access Gateway 應用裝置會提供所需等級的安全性和連線能力，所以不需要使用 VPN 連線。Blast 安全閘道元件可確保，唯一可進入公司資料中心的遠端流量是代表經過嚴格驗證之使用者的流量。使用者只能存取其有權存取的資源。

透過 Blast 安全閘道運作的 Blast 原生用戶端預期有其 Blast 工作階段 TLS 連線，而該連線由 Blast 安全閘道上設定的 TLS 憑證加以驗證。如果用戶端的 Blast 連線看到某些其他 TLS 憑證，則連線將會遭到捨棄，且用戶端將會報告憑證指紋不相符。

如果您選擇將用戶端連線至放置在該用戶端與 Blast 安全閘道之間的 TLS 終止 Proxy，則可以透過安排 Proxy 來提供 Blast 安全閘道憑證 (以及私密金鑰) 的複本，以滿足用戶端憑證需求，以及避免指紋不相符錯誤，從而可讓用戶端成功進行 Blast 連線。

將 Blast 安全閘道的憑證複製至 Proxy 的替代方法是提供 Proxy 其本身的 TLS 憑證，然後將 Blast 安全閘道設定為建議用戶端預期並接受 Proxy 的憑證，而非 Blast 安全閘道的憑證。

您可以在 Unified Access Gateway 中設定 Blast 安全閘道，方法是在 Unified Access Gateway Horizon 設定的 **Blast Proxy 憑證**中上傳 Proxy 的憑證。請參閱位於 https://docs.vmware.com/tw/Unified-Access-Gateway/index.html 中的《部署及設定 VMware Unified Access Gateway》文件。

備註 系統僅會上傳 Proxy 憑證。系統不會對 Unified Access Gateway 揭露對應的私密金鑰。

PCoIP 安全閘道

安全伺服器和 Unified Access Gateway 應用裝置包含 PCoIP 安全閘道元件。PCoIP 安全閘道啟用時，在驗證之後，使用 PCoIP 的用戶端可以進一步與安全伺服器或 Unified Access Gateway 應用裝置建立安全連線。此連線可讓用戶端從網際網路存取遠端桌面平台和應用程式。

啟用 PCoIP 安全閘道元件時，安全伺服器或 Unified Access Gateway 應用裝置會將 PCoIP 流量轉送至遠端桌面平台和應用程式。如果使用 PCoIP 的用戶端也使用 USB 重新導向功能或多媒體重新導向 (MMR) 加速，則可以啟用 View 安全閘道元件以轉送該資料。

設定直接用戶端連線時，PCoIP 流量及其他流量會直接從用戶端傳送到遠端桌面平台或應用程式。

當家庭或行動工作者之類的使用者從網際網路存取桌面平台時，安全伺服器或 Unified Access Gateway 應用裝置會提供所需等級的安全性和連線能力，所以不需要使用 VPN 連線。PCoIP 安全閘道元件可確保，唯一可進入公司資料中心的遠端流量是代表經過嚴格驗證之使用者的流量。使用者只能存取其有權存取的資源。

View LDAP

View LDAP 是 View 連線伺服器中的內嵌 LDAP 目錄，也是所有 Horizon 7 組態資料的組態存放庫。

View LDAP 包含代表每個遠端桌面平台和應用程式、每個可存取的遠端桌面平台、多個集中管理的遠端桌面平台以及 Horizon 7 元件組態設定的項目。

View LDAP 還包含一組 Horizon 7 外掛程式 DLL，可為其他 Horizon 7 元件提供自動化服務和通知服務。

Horizon 訊息

Horizon 訊息元件提供訊息路由器，以繞送 Horizon Connection Server 元件之間的通訊，以及 Horizon Agent 與連線伺服器之間的通訊。

此元件支援 Java Message Service (JMS) API，其用於 Horizon 7 的訊息。

元件間訊息驗證會使用 DSA 金鑰。依預設，金鑰大小為 512 個位元，但 FIPS 模式除外，其金鑰大小為 2048 個位元。

備註　將訊息安全模式設定為**增強**時，將使用 SSL/TLS 而非使用每則訊息加密來確保 JMS 連線的安全。在增強訊息安全模式中，驗證僅適用於一個訊息類型。針對增強訊息模式，VMware 建議將金鑰大小增加為 2048 個位元。如果您未使用增強訊息安全模式，VMware 建議不要變更 512 個位元的預設值，因為增加金鑰大小會影響效能和擴充性。

如果您希望所有金鑰都是 1024 位元，則必須在安裝第一個連線伺服器執行個體之後，以及在建立其他伺服器和桌面平台之前，立即變更 RSA 金鑰大小。如需詳細資訊，請參閱 VMware 知識庫 (KB) 文章 1024431。

Horizon 連線伺服器的防火牆規則

防火牆上必須為連線伺服器執行個體和安全伺服器開放特定的連接埠。

當您安裝連線伺服器時，安裝程式可為您選擇性地設定必要的 Windows 防火牆規則。這些規則會開放預設使用的連接埠。如果您在安裝後變更預設連接埠，則必須手動設定 Windows 防火牆，以允許 Horizon Client 裝置透過更新的連接埠連線至 Horizon 7。

下表列出了可在安裝期間自動開啟的預設連接埠。這些是傳入連接埠，除非另有說明。

表 5-4. Horizon 連線伺服器安裝期間開放的連接埠

通訊協定	連接埠	Horizon 連線伺服器執行個體類型
JMS	TCP 4001	標準和複寫
JMS	TCP 4002	標準和複寫
JMSIR	TCP 4100	標準和複寫
JMSIR	TCP 4101	標準和複寫
AJP13	TCP 8009	標準和複寫
HTTP	TCP 80	標準、複寫和安全伺服器
HTTPS	TCP 443	標準、複寫和安全伺服器
PCoIP	TCP 4172 傳入； UDP 4172 雙向	標準、複寫和安全伺服器
HTTPS	TCP 8443 UDP 8443	標準、複本和安全伺服器。 與 Horizon 7 進行初始連線之後，網頁瀏覽器或用戶端裝置會連線至 TCP 連接埠 8443 上的 Blast 安全閘道。必須在安全伺服器或 View 連線伺服器執行個體上啟用 Blast 安全閘道，才能允許進行此第二個連線。

表 5-4. Horizon 連線伺服器安裝期間開放的連接埠 (續)

通訊協定	連接埠	Horizon 連線伺服器執行個體類型
HTTPS	TCP 8472	標準和複寫 對於 Cloud Pod 架構功能：用於網繭間的通訊。
HTTP	TCP 22389	標準和複寫 對於 Cloud Pod 架構功能：用於全域 LDAP 複寫。
HTTPS	TCP 22636	標準和複寫 對於 Cloud Pod 架構功能：用於安全的全域 LDAP 複寫。

View Agent 或 Horizon Agent 的防火牆規則

View Agent 和 Horizon Agent 安裝程式會選擇性地在遠端桌面平台和 RDS 主機上設定 Windows 防火牆規則，以開啟預設的網路連接埠。這些是傳入連接埠，除非另有說明。

View Agent 和 Horizon Agent 安裝程式會設定輸入 RDP 連線的本機防火牆規則，以符合主機作業系統目前的 RDP 連接埠，通常是 3389。

如果您指示 View Agent 或 Horizon Agent 安裝程式不要啟用遠端桌面支援，則程式不會開啟連接埠 3389 和 32111，此時您必須手動開啟這些連接埠。

如果您在安裝之後變更 RDP 連接埠號碼，您必須變更相關聯的防火牆規則。如果您在安裝後變更預設連接埠，則必須手動重新設定 Windows 防火牆規則，以便允許在更新的連接埠上進行存取。請參閱《Horizon 7 安裝》文件中的〈取代 View 服務的預設連接埠〉。

在 RDS 主機的 View Agent 或 Horizon Agent 上，Windows 防火牆規則會將由 256 個連續 UDP 連接埠組成的區塊顯示為開啟，以供輸入流量使用。此連接埠的區塊可供 VMware Blast 內部用於 View Agent 或 Horizon Agent 中。RDS 主機上有一個特殊的 Microsoft 簽署驅動程式，可封鎖從外部來源輸入至這些連接埠的流量。此驅動程式會造成 Windows 防火牆將連接埠視為已關閉。

如果您使用虛擬機器範本作為桌面來源，則只有在範本屬於桌面網域成員時，防火牆例外才能執行於已部署的桌面。您可以使用 Microsoft 群組原則設定，來管理本機防火牆例外。如需詳細資訊，請參閱 Microsoft 知識庫 (KB) 文章 875357。

表 5-5. View Agent 或 Horizon Agent 安裝期間開啟的 TCP 與 UDP 連接埠

通訊協定	連接埠
RDP	TCP 連接埠 3389
USB 重新導向和時區同步化	TCP 連接埠 32111
MMR (多媒體重新導向) 和 CDR (用戶端磁碟機重新導向)	TCP 連接埠 9427
PCoIP	針對 RDS 主機，PCoIP 會使用下列連接埠號碼：TCP 連接埠 4172 和 UDP 連接埠 4172 (雙向)。 針對桌面平台，PCoIP 會使用從可設定範圍中選擇的連接埠號碼。依預設，TCP 連接埠為 4172 至 4173，而 UDP 連接埠為 4172 至 4182。針對這些連接埠的防火牆規則不會指定連接埠號碼，但會動態地遵循每個 PCoIP Server 所開啟的連接埠。所選的連接埠號碼會透過連線伺服器傳達給用戶端。

表 5-5. View Agent 或 Horizon Agent 安裝期間開啟的 TCP 與 UDP 連接埠 (續)

通訊協定	連接埠
VMware Blast	TCP 連接埠 22443 UDP 連接埠 22443 (雙向) **備註** Linux 桌面平台上未使用 UDP。
HTML Access	TCP 連接埠 22443
XDMCP	UDP 177 **備註** 此連接埠只會對執行 Ubuntu 18.04 的 Linux 桌面平台中開啟，以進行 XDMCP 存取。防火牆規則會封鎖對此連接埠的所有外部主機存取。
X11	TCP 6100 **備註** 此連接埠只會對執行 Ubuntu 18.04 的 Linux 桌面平台中開啟，以進行 XServer 存取。防火牆規則會封鎖對此連接埠的所有外部主機存取。

Active Directory 的防火牆規則

如果您的 Horizon 7 環境與 Active Directory 伺服器之間有防火牆，則必須確定所有必要的連接埠都已經開啟。

例如，View 連線伺服器必須能存取 Active Directory 通用類別目錄和輕量型目錄存取通訊協定 (LDAP) 伺服器。如果通用類別目錄和 LDAP 連接埠被您的防火牆軟體封鎖，則管理員將無法順利設定使用者權利。

請參閱您的 Active Directory 伺服器版本的 Microsoft 文件，以瞭解必須開啟哪些連接埠，才能使 Active Directory 透過防火牆正確運作的相關資訊。

設定 Horizon 7 環境的步驟概觀

6

請完成下列高階工作以安裝 Horizon 7 並設定初始部署。

表 6-1. Horizon 7 安裝與設定檢查清單

步驟	工作
1	在 Active Directory 中設定所需的管理員使用者和群組。 指示：《Horizon 7 安裝》和 vSphere 說明文件。
2	如果您尚未執行，請安裝並設定 ESXi 主機和 vCenter Server。 指示：VMware vSphere 說明文件。
3	(選用) 如果您要部署連結複製桌面，請在 vCenter Server 系統或在單獨伺服器上安裝 View Composer。同時要安裝 View Composer 資料庫。 指示：《Horizon 7 安裝》文件。
4	安裝並設定 Horizon 連線伺服器。同時要安裝事件資料庫。 指示：《Horizon 7 安裝》文件。
5	建立一或多個虛擬機器，以作為全複製桌面平台集區的範本或作為連結複製桌面平台集區或即時複製桌面平台集區的父系。 指示：《在 Horizon 7 中設定虛擬桌面平台》。
6	(選用) 為使用者設定 RDS 主機並安裝遠端應用程式。 指示：《在 Horizon 7 中設定已發佈的桌面平台和應用程式》。
7	建立桌面平台集區、應用程式集區，或兩者。 指示：《在 Horizon 7 中設定虛擬桌面平台》和《在 Horizon 7 中設定已發佈的桌面平台和應用程式》。
8	控制使用者對桌面的存取權。 指示：《在 Horizon 7 中設定遠端桌面平台功能》。
9	在使用者的機器上安裝 Horizon Client，並讓使用者擁有其遠端桌面平台和應用程式的存取權。 指示：Horizon Client 說明文件，網址：https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。
10	(選用) 建立並設定其他管理員，賦予其特定詳細目錄物件和設定的不同存取層級。 指示：《Horizon 7 管理》文件。
11	(選用) 設定原則來控制 Horizon 7 元件、桌面平台和應用程式集區，以及使用者之行為。 指示：《在 Horizon 7 中設定遠端桌面平台功能》。

表 6-1. Horizon 7 安裝與設定檢查清單 (續)

步驟	工作
12	(選用) 設定 Horizon Persona Management，讓使用者在登入桌面平台時可存取個人化資料和設定。 指示：《在 Horizon 7 中設定虛擬桌面平台》。
13	(選用) 若要更安全，可整合智慧卡驗證或 RADIUS 雙因素驗證解決方案。 指示：《Horizon 7 管理》文件。