Horizon 7 安装

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 安裝

《Horizon 7 安裝》說明如何安裝 VMware Horizon® 7 伺服器和用戶端元件。

主要對象

此資訊適用於想要安裝 VMware Horizon 7 的任何人。這些資訊是針對熟悉虛擬機器技術及資料中心作業的資深 Windows 或 Linux 系統管理員所撰寫。

伺服器元件的系統需求

1

執行 Horizon 7 Server 元件的主機必須符合特定的硬體和軟體需求。

本章節討論下列主題：

- Horizon 連線伺服器需求
- Horizon Administrator 需求
- View Composer 需求

Horizon 連線伺服器需求

Horizon 連線伺服器會透過驗證後將傳入的使用者要求導向至適當的遠端桌面平台和應用程式，當做用戶端連線的代理使用。Horizon 連線伺服器具備特定的硬體、作業系統、安裝以及支援軟體需求。

- Horizon 連線伺服器的硬體需求

  您必須在符合特定硬體需求的專用實體或虛擬機器上安裝所有的 Horizon 連線伺服器安裝類型，包括標準、複寫、安全伺服器和註冊伺服器安裝。

- Horizon 連線伺服器支援的作業系統

  您必須在支援的 Windows Server 作業系統上安裝 Horizon 連線伺服器。

- Horizon 連線伺服器的虛擬化軟體需求

  Horizon 連線伺服器需要特定版本的 VMware 虛擬化軟體。

- 複寫 Horizon 連線伺服器執行個體的網路需求

  安裝複寫 Horizon 連線伺服器執行個體時，您通常必須在相同實體位置設定執行個體，並透過高效能 LAN 連線到這些執行個體。否則，延遲問題可能會引起 Horizon 連線伺服器執行個體上的 View LDAP 組態出現不一致。使用者連線到組態過期的 Horizon 連線伺服器執行個體時，可能會發生存取遭拒的情況。

Horizon 連線伺服器的硬體需求

您必須在符合特定硬體需求的專用實體或虛擬機器上安裝所有的 Horizon 連線伺服器安裝類型，包括標準、複寫、安全伺服器和註冊伺服器安裝。

表 1-1. Horizon 連線伺服器硬體需求

硬體元件	必要	建議
處理器	Pentium IV 2.0GHz 處理器或更快的處理器	4 顆 CPU
網路介面卡	100Mbps NIC	1Gbps NIC
記憶體 Windows Server 2008 R2 64 位元	4GB RAM 或更高容量	至少 10 GB RAM 用於 50 個以上遠端桌面平台的部署
記憶體 Windows Server 2012 R2 64 位元	4GB RAM 或更高容量	至少 10 GB RAM 用於 50 個以上遠端桌面平台的部署

這些需求也適用於您針對高可用性或外部存取安裝的複寫和安全伺服器 Horizon 連線伺服器執行個體。

重要　主控 Horizon 連線伺服器的實體或虛擬機器必須具有不會變更的 IP 位址。在 IPv4 環境中，請設定靜態 IP 位址。在 IPv6 環境中，機器會自動取得不會變更的 IP 位址。

Horizon 連線伺服器支援的作業系統

您必須在支援的 Windows Server 作業系統上安裝 Horizon 連線伺服器。

下列作業系統支援所有 Horizon 連線伺服器安裝類型，包括標準、複寫和安全伺服器安裝。

表 1-2. Horizon 連線伺服器的作業系統支援

作業系統	版本	版本
Windows Server 2008 R2 SP1	64 位元	Standard Enterprise 資料中心
Windows Server 2012 R2	64 位元	Standard 資料中心
Windows Server 2016	64 位元	Standard 資料中心
Windows Server 2019	64 位元	Standard 資料中心

備註　不再支援不含任何 Service Pack 的 Windows Server 2008 R2。

Horizon 連線伺服器的虛擬化軟體需求

Horizon 連線伺服器需要特定版本的 VMware 虛擬化軟體。

如果您要使用 vSphere，必須使用支援的 vSphere ESX/ESXi 主機和 vCenter Server 版本。

如需哪些版本的 Horizon 與哪些版本的 vCenter Server 及 ESXi 相容的詳細資訊，請參閱 VMware 產品互通性對照表，網址為：http://www.vmware.com/resources/compatibility/sim/interop_matrix.php。

複寫 Horizon 連線伺服器執行個體的網路需求

安裝複寫 Horizon 連線伺服器執行個體時，您通常必須在相同實體位置設定執行個體，並透過高效能 LAN 連線到這些執行個體。否則，延遲問題可能會引起 Horizon 連線伺服器執行個體上的 View LDAP 組態出現不一致。使用者連線到組態過期的 Horizon 連線伺服器執行個體時，可能會發生存取遭拒的情況。

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。

Horizon Administrator 需求

管理員可以使用 Horizon Administrator 設定 Horizon Connection Server、部署並管理遠端桌面平台和應用程式、控制使用者驗證、起始並檢查系統事件，以及執行分析活動。執行 Horizon Administrator 的用戶端系統必須符合特定需求。

Horizon Administrator 是一種採用 Web 介面的應用程式，當您安裝連線伺服器時，會一併安裝。您可以使用下列網頁瀏覽器存取並使用 Horizon Administrator：

- Internet Explorer 9 (不建議)
- Internet Explorer 10
- Internet Explorer 11
- Firefox (最新的支援版本)
- Chrome (最新的支援版本)
- Safari 6 和更新版本
- Microsoft Edge (Windows 10)

若要搭配您的網頁瀏覽器使用 Horizon Administrator，您必須安裝 Adobe Flash Player 10.1 或更新版本。您的用戶端系統必須能夠存取網際網路，以允許安裝 Adobe Flash Player。

啟動 Horizon Administrator 所在的電腦必須信任裝載連線伺服器之伺服器的根憑證與中繼憑證。支援的瀏覽器已經包含所有知名憑證授權機構 (CA) 的憑證。若您的憑證來自較少見的 CA，您必須按照 設定用戶端端點信任根憑證和中繼憑證 中的指示操作。

若要正常顯示文字，Horizon Administrator 需要 Microsoft 專屬的字型。如果您的網頁瀏覽器是在非 Windows 作業系統 (如 Linux、UNIX 或 Mac) 上執行，請確認您電腦上有安裝 Microsoft 專屬的字型。

目前 Microsoft 網站並未發佈 Microsoft 字型，但是您可以從獨立網站下載。

View Composer 需求

藉由 View Composer，您可以從單一的集中式基礎映像部署多個連結複製桌面平台。View Composer 具備特定的安裝與儲存需求。

- View Composer 支援的作業系統

  View Composer 支援具有特定需求和限制的 64 位元作業系統。您可以在與 vCenter Server 相同的實體或虛擬機器上，或不同的伺服器上，安裝 View Composer。

- 獨立式 View Composer 的硬體需求

  如果您在不同於 vCenter Server 使用的實體或虛擬機器上安裝 View Composer，則必須使用符合特定硬體需求的專用機器。

- View Composer 和事件資料庫的資料庫需求

  View Composer 需要 SQL 資料庫來儲存資料。View Composer 資料庫必須位於 View Composer Server 主機上或可供其使用。您可選擇性設定事件資料庫來記錄來自 Horizon Connection Server 的 Horizon 事件相關資訊。

View Composer 支援的作業系統

View Composer 支援具有特定需求和限制的 64 位元作業系統。您可以在與 vCenter Server 相同的實體或虛擬機器上，或不同的伺服器上，安裝 View Composer。

表 1-3. View Composer 的作業系統支援

作業系統	版本	版本
Windows Server 2008 R2 SP1	64 位元	Standard Enterprise 資料中心
Windows Server 2012 R2	64 位元	Standard 資料中心
Windows Server 2016	64 位元	Standard 資料中心
Windows Server 2019	64 位元	Standard 資料中心

備註 不再支援不含任何 Service Pack 的 Windows Server 2008 R2。

如果您打算在不同於 vCenter Server 的實體或虛擬機器上安裝 View Composer，請參閱獨立式 View Composer 的硬體需求。

如需在 Windows Server 2016 或 Windows Server 2019 虛擬機器上對 View Composer 安裝進行疑難排解的詳細資訊，請參閱 VMware 知識庫文章 https://kb.vmware.com/s/article/59633。

獨立式 View Composer 的硬體需求

如果您在不同於 vCenter Server 使用的實體或虛擬機器上安裝 View Composer，則必須使用符合特定硬體需求的專用機器。

獨立 View Composer 安裝可與另一台 Windows Server 機器上安裝的 vCenter Server，或 Linux 系統的 vCenter Server 應用裝置搭配使用。VMware 建議在每個 View Composer 服務與 vCenter Server 執行個體之間是一對一的對應關係。

表 1-4. View Composer 硬體需求

硬體元件	必要	建議
處理器	1.4 GHz 或更快的 Intel 64 或 AMD 64 處理器，含 2 顆 CPU	2GHz 或更快的處理器與 4 顆 CPU
網路作業	一張或多張 10/100Mbps 網路介面卡 (NIC)	1Gbps NIC
記憶體	4GB RAM 或更高容量	8GB RAM 或更高容量，用於 50 或更多個遠端桌面平台的部署
磁碟空間	40GB	60GB

重要 主控 View Composer 的實體或虛擬機器必須具有不會變更的 IP 位址。在 IPv4 環境中，請設定靜態 IP 位址。在 IPv6 環境中，機器會自動取得不會變更的 IP 位址。

View Composer 和事件資料庫的資料庫需求

View Composer 需要 SQL 資料庫來儲存資料。View Composer 資料庫必須位於 View Composer Server 主機上或可供其使用。您可選擇性設定事件資料庫來記錄來自 Horizon Connection Server 的 Horizon 事件相關資訊。

如果 vCenter Server 的資料庫伺服器執行個體已存在，則 View Composer 可使用該現有的執行個體 (如果是 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 上的《VMware 產品互通性對照表》所列出的版本)。如果資料庫伺服器執行個體尚不存在，則必須安裝一個。

View Composer 支援 vCenter Server 所支援的部分資料庫伺服器。如果您已使用 vCenter Server 搭配 View Composer 不支援的資料庫伺服器，請繼續針對 vCenter Server 使用該資料庫伺服器，並安裝另一部用於 View Composer 的資料庫伺服器。

重要 如果您在與 vCenter Server 相同的 SQL Server 執行個體上建立 View Composer 資料庫，請不要覆寫 vCenter Server 資料庫。

如需有關支援資料庫的最新資訊，請參閱《VMware 產品互通性對照表》，網址為 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php。對於**解決方案/資料庫互通性**，在為「新增資料庫」步驟選取產品和版本後，若要查看支援的資料庫版本清單，請選取**任意**，然後按一下**新增**。

客體作業系統的系統需求

2

執行 Horizon Agent 或 Horizon Persona Management 的系統必須符合特定硬體和軟體需求。

本章節討論下列主題：

Horizon Agent 支援的作業系統

Horizon Agent 元件 (舊版稱為 View Agent) 有助於工作階段管理、Single Sign-On、裝置重新導向以及其他功能。您必須將 Horizon Agent 安裝在所有虛擬機器、實體系統以及 RDS 主機上。

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。

若要搭配 Horizon Agent 使用 Horizon Persona Management 安裝選項，您必須在 Windows 10、Windows 8、Windows 8.1、Windows 7、Windows Server 2012 R2、Windows Server 2008 R2 或 Windows Server 2016 虛擬機器上安裝 Horizon Agent。此選項不會在實體電腦或 RDS 主機上運作。

您可以在實體電腦上安裝獨立版的 Horizon Persona Management。請參閱獨立 Horizon Persona Management 支援的作業系統。

備註 若要使用 VMware Blast 顯示通訊協定，您必須在單一工作階段虛擬機器或 RDS 主機上安裝 Horizon Agent。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。

為獲得增強安全性，VMware 建議您設定加密套件以移除已知弱點。如需針對執行 View Composer 或 Horizon Agent 的 Windows 機器設定加密套件網域原則的指示，請參閱 在 SSL/TLS 中停用弱加密。

獨立 Horizon Persona Management 支援的作業系統

獨立 Horizon Persona Management 軟體可為未安裝 Horizon Agent 的獨立實體電腦和虛擬機器提供角色管理。當使用者登入時，會以動態方式，將其設定檔從遠端設定檔存放庫下載到其獨立系統。

備註 若要設定 Horizon 桌面平台的角色管理，請使用**角色管理**安裝選項安裝 Horizon Agent。獨立 Persona Management 軟體僅適用於非 Horizon 系統。

若要查看支援獨立 Horizon Persona Management 軟體的作業系統清單，請參閱 VMware 知識庫 (KB) 文章 http://kb.vmware.com/kb/2150295。

在 Microsoft 遠端桌面服務上不支援獨立 Persona Management 軟體。

遠端顯示通訊協定及軟體支援

遠端顯示通訊協定及軟體提供對遠端桌面平台和應用程式的存取權。使用的遠端顯示通訊協定取決於用戶端裝置的類型 (不論您是連線到遠端桌面平台還是遠端應用程式)，以及管理員設定桌面平台或應用程式集區的方式。

- 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。

- 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。

- 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。

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。
- 支援 Windows 桌面與 Horizon Agent 支援的作業系統中所列的 Horizon Agent 作業系統版本的連線。
- 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 7 架構規劃》文件。

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。

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。

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。
- 支援 Windows 桌面與 Horizon Agent 支援的作業系統中所列的 Horizon Agent 作業系統版本的連線。
- 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。

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。

在 IPv6 環境中安裝 Horizon 7

3

Horizon 7 支援將 IPv6 做為 IPv4 的替代。環境必須僅限於 IPv6 或僅限於 IPv4。Horizon 7 不支援 IPv6 和 IPv4 混合的環境。

並非 IPv4 環境支援的所有 Horizon 7 功能均受 IPv6 環境支援。Horizon 7 不支援從 IPv4 環境升級到 IPv6 環境。此外，Horizon 7 也不支援 IPv4 與 IPv6 環境之間的移轉。

重要 若要在 IPv6 環境下執行 Horizon 7，必須在安裝所有 Horizon 7 元件時指定 IPv6。

本章節討論下列主題：

- 在 IPv6 環境中設定 Horizon 7
- IPv6 環境中支援的 vSphere 資料庫及 Active Directory 版本
- IPv6 環境下 Horizon 7 Server 支援的作業系統
- IPv6 環境中桌面平台和 RDS 主機支援的 Windows 作業系統
- IPv6 環境中支援的用戶端
- IPv6 環境中支援的遠端通訊協定
- IPv6 環境中支援的驗證類型
- IPv6 環境中的其他支援功能

在 IPv6 環境中設定 Horizon 7

若要在 IPv6 環境中執行 Horizon 7，則在執行某些管理工作時，您必須瞭解 IPv6 專屬的需求和選項。

安裝 Horizon 7 之前，您必須擁有一個運作正常的 IPv6 環境。下列 Horizon 7 管理工作擁有 IPv6 專屬的選項。

- 安裝 Horizon 連線伺服器。請參閱使用新組態安裝 Horizon 連線伺服器。
- 安裝 View 複寫伺服器。請參閱安裝 Horizon 連線伺服器的複寫執行個體。
- 安裝 View 安全伺服器。請參閱安裝安全伺服器。
- 設定 PCoIP 外部 URL。請參閱設定安全閘道和通道連線的外部 URL。
- 設定 PCoIP 外部 URL。請參閱設定連線伺服器執行個體的外部 URL。

- 修改 PCoIP 外部 URL。請參閱設定連線伺服器執行個體的外部 URL。
- 安裝 Horizon Agent。請參閱《設定桌面平台和應用程式集區》文件中的〈Horizon Agent 安裝〉主題。
- 安裝 Horizon Client。請參閱 IPv6 環境中支援的用戶端。

備註 Horizon 7 不要求您在任何管理作中輸入 IPv6 位址。如果您可以指定完整網域名稱 (FQDN) 或 IPv6 位址，強烈建議您指定 FQDN，以免出現潛在錯誤。

IPv6 環境中支援的 vSphere 資料庫及 Active Directory 版本

在 IPv6 環境中，Horizon 7 支援特定的 vSphere、資料庫伺服器以及 Active Directory 版本。

IPv6 環境支援 SQL Server 2012 和更新版本以及 Oracle 11g 和更新版本的資料庫。如需 IPv6 環境中支援的資料庫、vSphere 版本和 Active Directory 版本的最新資訊，請參閱《VMware 產品互通性對照表》，網址是 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php。

IPv6 環境下 Horizon 7 Server 支援的作業系統

在 IPv6 環境下，必須在特定 Windows Server 作業系統上安裝 Horizon 7 Server。

Horizon 7 Server 包括連線伺服器執行個體、複寫伺服器、安全伺服器以及 Horizon 7 Composer 執行個體。

作業系統	版本
Windows Server 2016	Standard, Enterprise
Windows Server 2008 R2 SP1	Standard, Enterprise
Windows Server 2012 R2	Standard

IPv6 環境中桌面平台和 RDS 主機支援的 Windows 作業系統

在 IPv6 環境中，Horizon 7 支援桌面平台機器和 RDS 主機的特定 Windows 作業系統。RDS 主機為使用者提供工作階段型桌面平台和應用程式。

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。

IPv6 環境中支援的用戶端

在 IPv6 環境中，Horizon 7 支援特定桌面平台作業系統上執行的用戶端。

表 3-1. 支援的 Windows 作業系統

作業系統	版本	版本
Windows 7 和 Windows 7 SP1	32 位元或 64 位元	Home、Enterprise、Professional 與 Ultimate
Windows 8 與 Windows 8.1	32 位元或 64 位元	專業版、企業版，以及 Industry Embedded
Windows 10	32 位元或 64 位元	家用版、專業版、工作站專業版、企業版以及 IoT 企業版

在 iOS 裝置上，iOS 9.2 或更新版本支援使用 iOS 版 Horizon Client 4.1 或更新版本。

在 macOS 裝置上，需要 Mac 版 Horizon Client 4.9 或更新版本。

在 Android 裝置上，需要 Android 版 Horizon Client 4.9 或更新版本。

在 Chromebook 裝置上，需要 Android 版 Horizon Client 5.1 或更新版本。

不支援以下用戶端。

- Linux 版 Horizon Client、Chrome 版 Horizon Client、Chrome OS 版 Horizon Client、Windows 10 UWP 版 Horizon Client，以及 Windows 市集版 Horizon Client。
- PCoIP 零用戶端

IPv6 環境中支援的遠端通訊協定

在 IPv6 環境中，Horizon 7 支援特定遠端通訊協定。

支援下列遠端通訊協定：

- RDP
- 具有安全通道的 RDP
- PCoIP
- 透過 PCoIP 安全閘道的 PCoIP
- VMware Blast
- 透過 Blast 安全閘道的 VMware Blast
- Blast Extreme Adaptive Transport (BEAT)

IPv6 環境中支援的驗證類型

在 IPv6 環境中，Horizon 7 支援特定驗證類型。

支援下列驗證類型：

- 使用 Active Directory 的密碼驗證
- 智慧卡
- Single Sign-On

不支援下列驗證類型：

- SecurID
- RADIUS
- SAML

IPv6 環境中的其他支援功能

在 IPv6 環境中，Horizon 7 支援上述主題中未涵蓋的一些功能。

支援下列功能：

- 應用程式集區
- 音訊輸出
- 完整虛擬機器、即時複製或 Horizon 7Composer 連結複製的自動桌面平台集區
- Blast Extreme Adaptive Transport (BEAT)
- 客戶經驗改進計畫 (CEIP)
- 磁碟空間回收
- 事件
- Horizon 效能追蹤程式
- HTML5 多媒體重新導向
- 即時複製桌面平台集區
- LDAP 備份
- 手動桌面平台集區，包括 vCenter Server 虛擬機器、實體電腦，以及不受 vCenter Server 管理的虛擬機器
- 原生 NFS 快照 (VAAI)
- 角色管理
- 即時音訊視訊 (RTAV)
- RDS 桌面平台集區
- RDS 主機 3D
- 角色型管理
- 工作階段協作
- Single Sign-on，包括以目前使用者身分登入功能
- 系統健全狀況儀表板
- ThinApp
- Unity Touch

- USB 重新導向
- Horizon 7Composer Agent
- Horizon 7 儲存加速器
- Horizon 7Composer 資料庫備份
- 虛擬列印
- VMware 音訊
- VMware 視訊
- 適用於商務用 Skype 的 VMware 虛擬化套件 (僅限 Windows)

不支援下列功能：

- 用戶端磁碟機重新導向
- 用戶端 IP 通透性 (僅限 64 位元)
- Cloud Pod 架構
- 裝置橋接
- 檔案關聯
- Flash URL 重新導向
- HTML Access
- Log Insight
- Lync
- 使用 PCoIP 搭配 RDSH 即時複製集區
- 掃描器重新導向
- 序列埠重新導向
- Syslog
- Teradici TERA 主機卡
- TSMMR
- URL 重新導向
- vSAN
- 虛擬磁碟區
- vRealize OperationsDesktop Agent

以 FIPS 模式安裝 Horizon 7

4

Horizon 7 可使用 FIPS (聯邦資訊處理標準) 140-2 相容演算法執行密碼編譯作業。您可透過以 FIPS 模式安裝 Horizon 7 來啟用這些演算法。

FIPS 模式中並不支援所有 Horizon 7 功能。此外，Horizon 7 也不支援從非 FIPS 安裝升級至 FIPS 安裝。

備註 為確保 Horizon 7 以 FIPS 模式執行，您必須在安裝所有 Horizon 7 元件時啟用 FIPS。

本章節討論下列主題：

以 FIPS 模式設定 Horizon 7 的概觀

若要以 FIPS 模式設定 Horizon 7，您必須先在 Windows 環境下啟用 FIPS 模式。接著，您必須以 FIPS 模式安裝所有 Horizon 7 元件。

只有在 Windows 環境中啟用 FIPS 模式時，才可選擇以 FIPS 模式安裝 Horizon 7。如需有關在 Windows 中啟用 FIPS 模式的資訊，請參閱 https://support.microsoft.com/en-us/kb/811833。

備註 Horizon Administrator 不會指出 Horizon 7 是否以 FIPS 模式執行。

若要以 FIPS 模式安裝 Horizon 7，請執行下列管理工作。

- 安裝連線伺服器時，請選取 FIPS 模式選項。請參閱使用新組態安裝 Horizon 連線伺服器。
- 安裝複寫伺服器時，請選取 FIPS 模式選項。請參閱安裝 Horizon 連線伺服器的複寫執行個體。
- 在安裝安全伺服器之前，在 Horizon Administrator 中取消選取全域設定**針對安全伺服器連線使用 IPSec**，並手動設定 IPsec。請參閱 http://kb.vmware.com/kb/2000175。
- 安裝安全伺服器時，請選取 FIPS 模式選項。請參閱安裝安全伺服器。
- 如果設定 Windows 系統以進行 FIPS 作業，並設定 Horizon 7 以使用 IPSec 進行連線伺服器與安全伺服器之間的通訊，會無法安裝安全伺服器。在 IPv4 環境中，將包含連接埠號碼 4172 的 PCoIP 外部 URL 指定為 IP 位址。在 IPv6 環境中，您可以指定 IP 位址或完整網域名稱，以及連接埠號碼 4172。無論在哪種環境下，請勿包含通訊協定名稱。

例如，在 IPv4 環境中：`10.20.30.40:4172`

用戶端必須能夠使用 URL 連線安全伺服器。

- 針對 View Composer 和 Horizon Agent 機器停用弱加密。請參閱在 SSL/TLS 中停用弱加密。
- 安裝 View Composer 時，請選取 FIPS 模式選項。請參閱第 6 章 安裝 View Composer。
- 安裝 Horizon Agent 時，請選取 FIPS 模式選項。請參閱《在 Horizon 7 中設定虛擬桌面平台》或《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件中的 Horizon Agent 安裝主題。
- 針對 Windows 用戶端，請在用戶端作業系統中啟用 FIPS 模式，然後在安裝 Windows 版 Horizon Client 時選取 FIPS 模式選項。請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。
- 針對 Linux 用戶端，請在用戶端作業系統中啟用 FIPS 模式。請參閱《Linux 版 VMware Horizon Client 安裝和設定指南》文件。

FIPS 模式的系統需求

為支援 FIPS 模式，您的 Horizon 7 部署必須符合下列需求。

vSphere	■ vCenter Server 6.0 或更新版本 ■ ESXi 6.0 或更新版本
遠端桌面平台	■ 任何具有 FIPS 憑證的 Windows 平台。如需相關資訊，請參閱 Microsoft TechNet 網站上的「FIPS 140 驗證」。 ■ View Agent 6.2 或更新版本，或 Horizon Agent 7.0 或更新版本 (僅適用於 Windows 平台)
Horizon Client	■ 任何具有 FIPS 憑證的 Windows 平台。如需相關資訊，請參閱 Microsoft TechNet 網站上的「FIPS 140 驗證」。 ■ Windows 版 Horizon Client 3.5 或更新版本
密碼編譯通訊協定	■ TLSv1.2

準備 Active Directory

5

Horizon 7 使用現有的 Microsoft Active Directory 基礎結構進行使用者驗證及管理。您必須執行某些工作來準備 Active Directory，以便與 Horizon 7 搭配使用。

Horizon 7 支援以下 Active Directory Domain Services (AD DS) 網域功能性層級：

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

本章節討論下列主題：

設定網域和信任關係

您必須將每個連線伺服器主機加入 Active Directory 網域。主機不得為網域控制站。

Active Directory 也會管理您 Horizon 7 部署中的 Horizon Agent 機器 (包括單一使用者機器和 RDS 主機) 以及使用者和群組。您可以為使用者和群組賦予使用遠端桌面平台和應用程式的權利，您也可以選取使用者和群組，作為 Horizon Administrator 中的管理員。

您可以將 Horizon Agent 機器、View Composer 伺服器以及使用者和群組放入下列 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

使用 Active Directory 針對連線伺服器網域以及與其存在信任協議的任何其他使用者網域對使用者進行驗證。

如果您的使用者和群組位於單向受信任網域中，則必須為 Horizon Administrator 中的管理員使用者提供次要認證。管理員必須擁有次要認證，才能存取單向受信任網域。單向受信任網域可以是外部網域或位於可轉移樹系信任中的網域。

只有 Horizon Administrator 工作階段才需要次要認證，使用者的桌面平台或應用程式工作階段不需要。只有管理員使用者才需要次要認證。

您可以使用 `vdmadmin -T` 命令來提供次要認證。

- 請為個別管理員使用者設定次要認證。
- 至於樹系信任，您可為樹系根網域設定次要認證。接著，連線伺服器就能列舉樹系信任中的子網域。

如需詳細資訊，請參閱《Horizon 7 管理》文件中的〈使用 -T 選項為管理員提供次要認證〉。

在單向信任的網域中不支援使用者的智慧卡和 SAML 驗證。

從 Horizon 7(7.10 版) 開始，單向信任網域已可支援 Windows 版 Horizon Client 中的「以目前使用者身分登入」功能。

備註 由於安全伺服器不會存取任何驗證存放庫 (包括 Active Directory)，因此不需要位於 Active Directory 網域內。

信任關係和網域篩選

為了判斷連線伺服器執行個體所能存取的網域，它會從本身的網域開始周遊信任關係。

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或網域間連線功能的降低而拉長。此清單可能也包含使用者連線到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。

您可以使用 `vdmadmin` 命令設定網域篩選，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。

如果樹系信任設定為名稱字尾排除項目，則設定的排除項目將用於篩選樹系子網域清單。除了套用名稱字尾排除項目篩選，還會套用 vdmadmin 命令指定的篩選。

為遠端桌面平台建立 OU

您應該為遠端桌面平台建立專屬的組織單位 (OU)。組織單位是 Active Directory 中的子分割，其中包含使用者、群組、電腦或其他組織單位。

若要防止群組原則設定套用至與桌面平台相同網域中的其他 Windows Server 或工作站，您可以為 Horizon 7 群組原則建立 GPO，並將其連結至包含您的遠端桌面平台的 OU。您也可以將組織單位的控制委派給下層群組，例如伺服器操作員或個別使用者。

如果您使用 View Composer，則應該為連結複製桌面平台建立單獨的 Active Directory 容器，該容器以您的遠端桌面平台的 OU 為基礎。在 Active Directory 中具有 OU 管理員權限的管理員無需具有網域管理員權限即可佈建連結複製桌面平台。如果您變更 Active Directory 中的管理員認證，也必須更新 View Composer 中的認證資訊。

建立 Kiosk 模式用戶端帳戶的組織單位和群組

Kiosk 模式的用戶端是精簡型用戶端或鎖定的電腦，會執行用戶端軟體以連線至連線伺服器執行個體，並啟動遠端桌面工作階段。如果您設定 Kiosk 模式的用戶端，則應該在 Active Directory 中建立 Kiosk 模式用戶端帳戶專用的組織單位和群組。

為 Kiosk 模式用戶端帳戶建立專用的組織單位和群組可對用戶端系統進行磁碟分割，避免未經保證的入侵，並且簡化用戶端組態和管理。

如需詳細資訊，請參閱《Horizon 7 管理》文件。

建立使用者的群組

您應該為 Active Directory 中各種不同類型的使用者建立群組。例如，您可以為使用者建立稱為 Horizon 7 Users 的群組，並為將要管理遠端桌面平台和應用程式的使用者建立另一個稱為 Horizon 7 Administrators 的群組。

建立 vCenter Server 的使用者帳戶

您必須在 Active Directory 中建立使用者帳戶以搭配 vCenter Server 使用。您在 Horizon Administrator 中新增 vCenter Server 執行個體時，需要指定此使用者帳戶。

您必須提供使用者帳戶在 vCenter Server 中執行特定作業的權限。您可建立擁有適當權限的 vCenter Server 角色並將該角色指派給 vCenter Server 使用者。新增至 vCenter Server 角色的權限清單視您是否搭配使用 Horizon 7 與 View Composer 而有所不同。如需設定這些權限的相關資訊，請參閱設定 vCenter Server、View Composer 和即時複製的使用者帳戶。

如果在與 vCenter Server 相同的機器上安裝 View Composer，您必須將 vCenter Server 使用者新增至 vCenter Server 機器上的本機管理員群組。此需求允許 Horizon 7 向 View Composer 服務驗證。

如果在不同於 vCenter Server 的機器上安裝 View Composer，vCenter Server 使用者無需是 vCenter Server 機器上的本機管理員。但是，您需要建立必須是 View Composer 機器上之本機管理員的獨立式 View Composer Server 使用者帳戶。

建立獨立式 View Composer Server 的使用者帳戶

如果在不同於 vCenter Server 的機器上安裝 View Composer，您必須在 Active Directory 中建立 Horizon 7 可用於向獨立式機器上的 View Composer 服務驗證的網域使用者帳戶。

使用者帳戶必須與連線伺服器主機位於相同網域，或位於信任的網域中。您必須將使用者帳戶新增至獨立式 View Composer 機器上的本機管理員群組。

您在 Horizon Administrator 中設定 View Composer 設定，並選取**獨立式 View Composer Server** 時，需要指定此使用者帳戶。請參閱設定 View Composer。

建立 View Composer AD 作業的使用者帳戶

如果使用 View Composer，您必須在 Active Directory 中建立允許 View Composer 在 Active Directory 中執行特定作業的使用者帳戶。View Composer 需要此帳戶才能將連結複製虛擬機器加入您的 Active Directory 網域中。

為確保安全性，您應該另外建立一個使用者帳戶來搭配 View Composer 使用。藉由建立另一個帳戶，就可以確保該帳戶不會具備為其他用途所定義的其他權限。您可以為帳戶提供在指定的 Active Directory 容器中建立與移除電腦物件所需的最小權限。例如，View Composer 帳戶不需要網域管理員權限。

程序

1. 在 Active Directory 中，在與連線伺服器主機相同的網域或信任網域中建立使用者帳戶。
2. 將**建立電腦物件**、**刪除電腦物件**及**寫入全部內容**權限新增至建立連結複製電腦帳戶所在或是連結複製電腦帳戶移至其中的 Active Directory 容器中的帳戶。

   下列清單顯示使用者帳戶需要的所有權限，包括預設指定的權限：

   - 列出內容
   - 讀取全部內容
   - 寫入全部內容
   - 讀取權限
   - 重設密碼
   - 建立電腦物件

- 刪除電腦物件

備註 如果為桌面平台集區選取**允許重複使用既存的電腦帳戶**設定，則需要較低的權限。確保已將下列權限指派給使用者帳戶：

- 列出內容
- 讀取全部內容
- 讀取權限
- 重設密碼

3 請確認使用者帳戶的權限套用至 Active Directory 容器及容器的所有子物件。

後續步驟

當您在「新增 vCenter Server」精靈中設定 View Composer 網域，以及設定並部署連結複製桌面平台集區時，請在 Horizon Administrator 中指定帳戶。

建立即時複製作業的使用者帳戶

在部署即時複製之前，您必須先建立有權限在 Active Directory 中執行特定作業的使用者帳戶。

當您在部署即時複製桌面平台集區之前新增即時複製網域管理員時，請選取此帳戶。如需詳細資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈新增即時複製網域管理員〉。

程序

1 在 Active Directory 中，在與連線伺服器相同的網域或信任網域中建立使用者帳戶。

2 在即時複製電腦帳戶的容器上，將**建立電腦物件**、**刪除電腦物件**和**寫入全部內容**等權限新增至帳戶。

下列清單顯示使用者帳戶的必要權限，包括依預設指派的權限：

- 列出內容
- 讀取全部內容
- 寫入全部內容
- 讀取權限
- 重設密碼
- 建立電腦物件
- 刪除電腦物件

請確定這些權限套用至正確的容器及容器的所有子物件。

設定受限群組原則

為能夠連線至遠端桌面平台，使用者必須屬於遠端桌面平台的本機遠端桌面平台使用者群組。您可以使用 Active Directory 中的受限群組原則，將使用者或群組新增到每一個加入您網域之遠端桌面平台的本機遠端桌面平台使用者群組。

受限群組原則會將網域中電腦的本機群組成員資格設定為符合受限群組原則中定義的成員資格清單設定。遠端桌面平台使用者群組的成員一律會新增到已加入您網域之每個遠端桌面平台的本機遠端桌面平台使用者群組。新增使用者時，您只需要將他們新增到您的遠端桌面平台使用者群組即可。

這些步驟適用於 Horizon 7 虛擬桌面平台或已發佈的桌面平台和應用程式所加入網域上的 Active Directory 伺服器。

必要條件

在您 Active Directory 的網域中，建立遠端桌面平台使用者的群組。例如，建立名為「Horizon 使用者」的群組。

程序

1 在 Active Directory 伺服器上，瀏覽至群組原則管理外掛程式。

AD 版本	瀏覽路徑
Windows 2003	a 選取**開始 > 所有程式 > 系統管理工具 > Active Directory 使用者和電腦**。 b 在您的網域上按一下滑鼠右鍵，然後按一下 **內容**。 c 在 **群組原則** 標籤上，按一下 **開啟** 以開啟群組原則管理外掛程式。 d 在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。
Windows 2008	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。
Windows 2012 R2	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在**預設網域原則**上按一下滑鼠右鍵，然後按一下**編輯**。
Windows 2016	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。

2 展開**電腦組態**區段，並開啟 **Windows 設定\安全性設定**。

3 以滑鼠右鍵按一下**受限群組**，選取**新增群組**，然後新增遠端桌面使用者群組。

4 在群組上按一下滑鼠右鍵，然後將新的遠端桌面平台使用者群組新增至群組成員資格清單。

例如，將「Horizon 使用者」新增至遠端桌面平台使用者。

5 按一下**確定**儲存變更。

使用 Horizon 7 群組原則管理範本檔

Horizon 7 包含數個元件專屬的群組原則管理 (ADMX) 範本檔。

為 Horizon 7 提供群組原則設定的所有 ADMX 檔案皆可從 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 中取得，其中 *x.x.x* 為版本，而 *yyyyyyy* 為組建編號。您可以從 VMware 下載網站下載此檔案，網址為 https://my.vmware.com/web/vmware/downloads。在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含 ZIP 檔案。

您可以將這些檔案中的原則設定新增至 Active Directory 中的新 GPO 或現有 GPO，然後將該 GPO 連結至包含您桌面平台的 OU，從而最佳化遠端桌面平台並保護其安全。

如需有關使用 Horizon 7 群組原則設定的相關資訊，請參閱《Horizon 7 管理》和《在 Horizon 7 中設定遠端桌面平台功能》文件。

為進行智慧卡驗證準備好 Active Directory

實作智慧卡驗證時，您可能需要在 Active Directory 中執行特定工作。

- 為智慧卡使用者新增 UPN

  智慧卡登入依賴於使用者主體名稱 (UPN)，因此，使用智慧卡在 Horizon 7 中進行驗證之使用者和管理員的 Active Directory 帳戶，都必須有一個有效的 UPN。

- 將根憑證新增至信任的根憑證授權單位

  如果您使用憑證授權單位 (CA) 核發智慧卡登入或網域控制站憑證，則必須將根憑證新增到 Active Directory 中的「受信任的根憑證授權單位」群組原則。如果 Windows 網域控制站當做根 CA，則您不需要執行此程序。

- 將中繼憑證新增至中繼憑證授權單位

  如果您使用中繼憑證授權單位 (CA) 核發智慧卡登入或網域控制站憑證，則必須將中繼憑證新增到 Active Directory 中的「中繼憑證授權單位」群組原則。

- 將根憑證新增至 Enterprise NTAuth Store

  如果您使用 CA 核發智慧卡登入或網域控制站憑證，必須將根憑證新增到 Active Directory 中的 Enterprise NTAuth 存放區。如果 Windows 網域控制站當做根 CA，則您不需要執行此程序。

為智慧卡使用者新增 UPN

智慧卡登入依賴於使用者主體名稱 (UPN)，因此，使用智慧卡在 Horizon 7 中進行驗證之使用者和管理員的 Active Directory 帳戶，都必須有一個有效的 UPN。

如果智慧卡使用者所在的網域不同於核發根憑證的來源網域，則您必須將使用者的 UPN 設定為包含在信任的 CA 的根憑證中的主體別名 (SAN)。如果您的根憑證是從智慧卡使用者目前網域中的伺服器核發，則您不需要修改使用者的 UPN。

備註 即使憑證是從相同的網域核發，您可能還是必須為內建的 Active Directory 帳戶設定 UPN。包括 Administrator 在內的內建帳戶預設都沒有設定 UPN。

必要條件

- 透過檢視憑證內容來取得包含在信任的 CA 的根憑證中的 SAN。

- 如果您的 Active Directory 伺服器上沒有出現 ADSI Edit 公用程式，請從 Microsoft 網站下載並安裝適當的 Windows 支援工具。

程序

1 在 Active Directory 伺服器上，啟動 ADSI Edit 公用程式。

2 在左窗格中，展開使用者所在的網域，然後按兩下 `CN=Users`。

3 在右窗格中，以滑鼠右鍵按一下使用者，然後按一下**內容**。

4 按兩下 `userPrincipalName` 屬性，然後輸入信任的 CA 憑證的 SAN 值。

5 按一下**確定**來儲存屬性設定。

將根憑證新增至信任的根憑證授權單位

如果您使用憑證授權單位 (CA) 核發智慧卡登入或網域控制站憑證，則必須將根憑證新增到 Active Directory 中的「受信任的根憑證授權單位」群組原則。如果 Windows 網域控制站當做根 CA，則您不需要執行此程序。

程序

1 在 Active Directory 伺服器上，瀏覽至群組原則管理外掛程式。

AD 版本	瀏覽路徑
Windows 2003	a 選取**開始 > 所有程式 > 系統管理工具 > Active Directory 使用者和電腦**。 b 在您的網域上按一下滑鼠右鍵，然後按一下 **內容**。 c 在 **群組原則** 標籤上，按一下 **開啟** 以開啟群組原則管理外掛程式。 d 在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。
Windows 2008	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。
Windows 2012 R2	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在**預設網域原則**上按一下滑鼠右鍵，然後按一下**編輯**。
Windows 2016	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。

2 展開**電腦組態**區段，並開啟 **Windows 設定\安全性設定\公開金鑰**。

3 以滑鼠右鍵按一下**受信任的根憑證授權單位**，然後選取**匯入**。

4 依照精靈中的提示，匯入根憑證 (例如，`rootCA.cer`)，然後按一下**確定**。

5 關閉「群組原則」視窗。

網域中的所有系統現在在其受信任的根存放區中都有一份根憑證的複本。

後續步驟

如果中繼憑證授權單位 (CA) 核發智慧卡登入或網域控制站憑證，請將中繼憑證新增到 Active Directory 中的「中繼憑證授權單位」群組原則。請參閱將中繼憑證新增至中繼憑證授權單位。

將中繼憑證新增至中繼憑證授權單位

如果您使用中繼憑證授權單位 (CA) 核發智慧卡登入或網域控制站憑證，則必須將中繼憑證新增到 Active Directory 中的「中繼憑證授權單位」群組原則。

程序

1 在 Active Directory 伺服器上，瀏覽至群組原則管理外掛程式。

AD 版本	瀏覽路徑
Windows 2003	a 選取**開始 > 所有程式 > 系統管理工具 > Active Directory 使用者和電腦**。 b 在您的網域上按一下滑鼠右鍵，然後按一下 **內容**。 c 在 **群組原則** 標籤上，按一下 **開啟** 以開啟群組原則管理外掛程式。 d 在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。
Windows 2008	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。
Windows 2012 R2	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在**預設網域原則**上按一下滑鼠右鍵，然後按一下**編輯**。
Windows 2016	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。

2 展開**電腦組態**區段，並開啟 **Windows 設定\安全性設定\公開金鑰**的原則。

3 以滑鼠右鍵按一下**中繼憑證授權單位**，然後選取**匯入**。

4 依照精靈中的提示，匯入中繼憑證 (例如，`intermediateCA.cer`)，然後按一下**確定**。

5 關閉「群組原則」視窗。

網域中的所有系統現在在其中繼憑證授權存放區中都有一份中繼憑證的複本。

將根憑證新增至 Enterprise NTAuth Store

如果您使用 CA 核發智慧卡登入或網域控制站憑證，必須將根憑證新增到 Active Directory 中的 Enterprise NTAuth 存放區。如果 Windows 網域控制站當做根 CA，則您不需要執行此程序。

程序

- 在 Active Directory 伺服器上，使用 `certutil` 命令將憑證發佈到 Enterprise NTAuth 存放區。

  例如：**`certutil –dspublish –f`** ***`path_to_root_CA_cert`*** **`NTAuthCA`**

CA 現在受到信任，可核發此類型的憑證。

在 SSL/TLS 中停用弱加密

為獲得更佳的安全性，您可設定網域原則 GPO (群組原則物件)，以確保 View Composer 和執行 View Agent 或 Horizon Agent 的 Windows 機器不會在使用 SSL/TLS 通訊協定通訊時使用弱加密。

程序

1 在 Active Directory 伺服器上，選取**開始 > 系統管理工具 > 群組原則管理**，並在 GPO 上按一下滑鼠右鍵，然後選取**編輯**，來編輯 GPO。

2 在群組原則管理編輯器中，瀏覽至**電腦設定 > 原則 > 系統管理範本 > 網路 > SSL 組態設定**。

3 按兩下 **SSL 加密套件順序**。

4 在 [SSL 加密套件順序] 視窗中，按一下**啟用**。

5 在 [選項] 窗格中，以下列加密清單取代 [SSL 加密套件] 文字方塊的所有內容。

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

加密套件在上方以單獨行列出以便閱讀。當您將清單貼在文字方塊內時，加密套件必須位於一行中且逗點後不含空格。

6 結束群組原則管理編輯器。

7 重新啟動 View Composer 和 View Agent 或 Horizon Agent 機器，使新的群組原則生效。

安裝 View Composer

6

若要使用 View Composer，您要建立 View Composer 資料庫、安裝 View Composer 服務，並且最佳化 View 基礎結構以支援 View Composer。您可以將 View Composer 服務與 vCenter Server 安裝在同一部主機或不同主機上。

View Composer 是選擇性的功能。如果您要部署連結複製桌面平台集區，請安裝 View Composer。

您必須擁有安裝及使用 View Composer 功能的授權。

備註 在安裝 View Composer 前，請先確認您已備妥 Active Directory。

備註 如果您將 View Composer 安裝在安裝 vCenter Server 6.5 的相同機器上，則 View Composer 在 vCenter Server 上的行為可能會有所不同。如需詳細資訊，請參閱 VMware 知識庫文章 https://kb.vmware.com/s/article/2150066。

本章節討論下列主題：

準備 View Composer 資料庫

您必須建立資料庫和資料來源名稱 (DSN) 才能儲存 View Composer 資料。

View Composer 服務不包含資料庫。如果您的網路環境中沒有資料庫執行個體，則必須安裝一個。安裝資料庫執行個體之後，請將 View Composer 資料庫新增至執行個體。

您可以將 View Composer 資料庫新增至 vCenter Server 資料庫所在的執行個體中。您可以在本機上設定資料庫，或從遠端的網路連線 Linux、UNIX 或 Windows Server 電腦進行設定。

View Composer 資料庫會儲存 View Composer 所使用之連線和元件的相關資訊：

- vCenter Server 連線

- Active Directory 連線
- View Composer 部署的連結複製桌面
- View Composer 建立的複本

View Composer 服務的每個執行個體必須有自己的 View Composer 資料庫。多個 View Composer 服務無法共用 View Composer 資料庫。

如需支援的資料庫版本清單，請參閱 View Composer 和事件資料庫的資料庫需求。

若要將 View Composer 資料庫新增至已安裝的資料庫執行個體中，請選擇這些程序中的其中一項。

- 建立 View Composer 的 SQL Server 資料庫

  View Composer 可以在 SQL Server 資料庫中儲存連結複製桌面資訊。建立 View Composer 資料庫的方式是將它新增至 SQL Server 並且設定其 ODBC 資料來源。

- 建立 View Composer 的 Oracle 資料庫

  View Composer 可以在 Oracle 12c 或 11g 資料庫中儲存連結複製桌面平台資訊。建立 View Composer 資料庫的方式是將它新增至現有的 Oracle 執行個體並且設定其 ODBC 資料來源。您可以使用 Oracle 資料庫組態助理員或執行 SQL 陳述式來新增 View Composer 資料庫。

建立 View Composer 的 SQL Server 資料庫

View Composer 可以在 SQL Server 資料庫中儲存連結複製桌面資訊。建立 View Composer 資料庫的方式是將它新增至 SQL Server 並且設定其 ODBC 資料來源。

程序

1. 將 View Composer 資料庫新增到 SQL Server 中

   您可以將新的 View Composer 資料庫新增到現有的 Microsoft SQL Server 執行個體，以儲存 View Composer 的連結複製資料。

2. (選擇性) 藉由手動建立資料庫角色來設定 SQL Server 資料庫權限

   藉由使用此建議方法，View Composer 資料庫管理員可透過 Microsoft SQL Server 資料庫角色來設定要授與 View Composer 管理員的權限。

3. 將 ODBC 資料來源新增至 SQL Server 中

   將 View Composer 資料庫新增到 SQL Server 之後，您必須設定 ODBC 與新資料庫的連線，讓 View Composer 服務可以看到這個資料來源。

將 View Composer 資料庫新增到 SQL Server 中

您可以將新的 View Composer 資料庫新增到現有的 Microsoft SQL Server 執行個體，以儲存 View Composer 的連結複製資料。

如果資料庫位於本機上將安裝 View Composer 的電腦上，您可以使用「整合式 Windows 驗證」安全性模型。如果資料庫位於遠端系統上，則無法使用此驗證方法。

必要條件

- 請確認已在您將安裝 View Composer 的電腦上或網路環境中，安裝支援的 SQL Server 版本。如需詳細資料，請參閱 View Composer 和事件資料庫的資料庫需求。
- 確認使用 SQL Server Management Studio 建立和管理資料庫。或者，可以使用 SQL Server Management Studio Express，可從下列網站下載並安裝。

  http://www.microsoft.com/en-us/download/details.aspx?id=7593

程序

1. 在 View Composer 電腦上，選取**開始 > 所有程式 > Microsoft SQL Server 2014**、**Microsoft SQL Server 2012** 或 **Microsoft SQL Server 2008**。
2. 選取 **SQL Server Management Studio** 並連線至 SQL Server 執行個體。
3. 在「物件總管」面板中，以滑鼠右鍵按一下「資料庫」項目，然後選取**新增資料庫**。

   您可以為資料庫和記錄檔使用 `Initial size` 和 `Autogrowth` 參數的預設值。
4. 在「新增資料庫」對話方塊的「資料庫名稱」文字方塊中，輸入名稱。

   例如：`ViewComposer`
5. 按一下**確定**。

   SQL Server Management Studio 會將您的資料庫新增到 [物件總管] 面板中的 [資料庫] 項目。
6. 結束 Microsoft SQL Server Management Studio。

後續步驟

選擇性地依照藉由手動建立資料庫角色來設定 SQL Server 資料庫權限中的指示進行

請依照將 ODBC 資料來源新增至 SQL Server 中中的指示進行。

藉由手動建立資料庫角色來設定 SQL Server 資料庫權限

藉由使用此建議方法，View Composer 資料庫管理員可透過 Microsoft SQL Server 資料庫角色來設定要授與 View Composer 管理員的權限。

VMware 建議使用此方法，因為它不需要為安裝和升級 View Composer 的 View Composer 管理員設定 **db_owner** 角色。

在此程序中，您可以提供自己的名稱做為資料庫登入名稱、使用者名稱和資料庫角色。使用者 **[vcmpuser]** 及資料庫角色 **VCMP_ADMIN_ROLE** 和 **VCMP_USER_ROLE** 為範例名稱。**dbo** 結構描述是在建立 View Composer 資料庫時建立的。您必須使用 **dbo** 結構描述名稱。

必要條件

- 確認已建立 View Composer 資料庫。請參閱將 View Composer 資料庫新增到 SQL Server 中。

程序

1 以 sysadmin (SA) 身分或使用具有 **sysadmin** 權限的使用者帳戶登入 Microsoft SQL Server Management Studio 工作階段。

2 建立將向其授與適當 SQL Server 資料庫權限的使用者。

```
use ViewComposer
go
CREATE LOGIN [vcmpuser] WITH PASSWORD=N'vcmpuser!0', DEFAULT_DATABASE=ViewComposer,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
use MSDB
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
```

3 在 View Composer 資料庫中，建立資料庫角色 **VCMP_ADMIN_ROLE**。

4 在 View Composer 資料庫中，將權限授與 **VCMP_ADMIN_ROLE**。

   a 授與 **dbo** 結構描述上的結構描述權限**更改**、**參考**和**插入**。

   b 授與權限**建立資料表**、**建立視圖**和**建立程序**。

5 在 View Composer 資料庫中，建立 **VCMP_USER_ROLE**。

6 在 View Composer 資料庫中，將 **dbo** 結構描述上的結構描述權限**選取**、**插入**、**刪除**、**更新**和**執行**授與 **VCMP_USER_ROLE**。

7 將 **VCMP_USER_ROLE** 授與使用者 **[vcmpuser]**。

8 將 **VCMP_ADMIN_ROLE** 授與使用者 **[vcmpuser]**。

9 在 MSDB 資料庫中，建立資料庫角色 **VCMP_ADMIN_ROLE**。

10 在 MSDB 中，將權限授與 **VCMP_ADMIN_ROLE**。

   a 在 MSDB 資料表 `syscategories`、`sysjobsteps` 和 `sysjobs` 中，將**選取**權限授與使用者 **[vcmpuser]**。

   b 在 MSDB 預存程序 `sp_add_job`、`sp_delete_job`、`sp_add_jobstep`、`sp_update_job`、`sp_add_jobserver`、`sp_add_jobschedule` 和 `sp_add_category` 中，將**執行**權限授與角色 **VCMP_ADMIN_ROLE**。

11 在 MSDB 資料庫中，將 **VCMP_ADMIN_ROLE** 授與使用者 **[vcmpuser]**。

12 使用 SQL Server 登入名稱 **vcmpuser** 建立 ODBC 系統 DSN。

   如需相關指示，請參閱 將 ODBC 資料來源新增至 SQL Server 中。

13 安裝 View Composer。

   如需相關指示，請參閱 安裝 View Composer 服務。

14 在 MSDB 資料庫中，從使用者 **[vcmpuser]** 撤銷 **VCMP_ADMIN_ROLE**。

撤銷該角色後，您可以將該角色保留為非作用中狀態或者移除該角色以提高安全性。

將 ODBC 資料來源新增至 SQL Server 中

將 View Composer 資料庫新增到 SQL Server 之後，您必須設定 ODBC 與新資料庫的連線，讓 View Composer 服務可以看到這個資料來源。

設定 View Composer 的 ODBC DSN 時，請保護適合您環境層級的基礎資料庫連線的安全。如需有關保護資料庫連線安全的相關資訊，請參閱 SQL Server 文件。

如果基礎資料庫連線使用 SSL 加密，建議您使用信任的 CA 所簽署的 SSL 憑證，設定資料庫伺服器。如果您使用自我簽署的憑證，您的資料庫連線可能會容易造成攔截式攻擊。

必要條件

完成將 View Composer 資料庫新增到 SQL Server 中中所述的步驟。

程序

1 在將安裝 View Composer 的電腦上，選取 **開始 > 系統管理工具 > 資料來源 (ODBC)**。

2 選取**系統 DSN** 索引標籤。

3 按一下**新增**，然後從清單中選取 **SQL Native Client**。

4 按一下**完成**。

5 在**建立新的資料來源至 SQL Server 安裝程式**精靈中，輸入 View Composer 資料庫的名稱和描述。

例如：`ViewComposer`

6 在「伺服器」文字方塊中，輸入 SQL Server 資料庫名稱。

請使用 *host_name\server_name* 這個格式，其中 *host_name* 是電腦的名稱，而 *server_name* 是 SQL Server 執行個體。

例如：`VCHOST1\VIM_SQLEXP`

7 按**下一步**。

8 請確認已選取**連線到 SQL Server 以獲得其他設定選項的預設設定**核取方塊，然後選取驗證選項。

選項	描述
整合 Windows 驗證	如果您要使用 SQL Server 的本機執行個體，請選取此選項。此選項也就是所謂的受信任的驗證。只有 SQL Server 在本機電腦上執行時，才支援整合 Windows 驗證。
SQL Server 驗證	如果您要使用 SQL Server 的遠端執行個體，請選取此選項。在遠端 SQL Server 上不支援 Windows NT 驗證。 如果手動設定 SQL Server 資料庫權限並已將其指派給使用者，請透過使用者進行驗證。例如，透過使用者 **vcmpuser** 進行驗證。或者，以 sysadmin (SA) 或擁有 **sysadmin** 權限的使用者帳戶驗證。

9 按**下一步**。

10 選取**變更預設資料庫為**核取方塊，然後從清單中選取 View Composer 資料庫的名稱。

例如：**ViewComposer**

11 如果 SQL Server 連線是在啟用 SSL 時設定的，請導覽至「Microsoft SQL Server DSN 組態」頁面，然後選取**使用高度加密資料**。

12 完成後，請關閉 **Microsoft ODBC 資料來源管理員**精靈。

後續步驟

安裝新的 View Composer 服務。請參閱安裝 View Composer 服務。

建立 View Composer 的 Oracle 資料庫

View Composer 可以在 Oracle 12c 或 11g 資料庫中儲存連結複製桌面平台資訊。建立 View Composer 資料庫的方式是將它新增至現有的 Oracle 執行個體並且設定其 ODBC 資料來源。您可以使用 Oracle 資料庫組態助理員或執行 SQL 陳述式來新增 View Composer 資料庫。

- 將 View Composer 資料庫新增到 Oracle 12c 或 11g 中

  您可以使用「Oracle 資料庫組態輔助程式」，將新的 View Composer 資料庫新增到現有的 Oracle 12c 或 11g 執行個體。

- 使用 SQL 陳述式將 View Composer 資料庫新增至 Oracle 執行個體

- 設定 View Composer 的 Oracle 資料庫使用者

  根據預設，執行 View Composer 資料庫的資料庫使用者擁有 Oracle 系統管理員權限。若要限制執行 View Composer 資料庫之使用者的安全性權限，您必須設定具有特定權限的 Oracle 資料庫使用者。

- 將 ODBC 資料來源新增至 Oracle 12c 或 11g 中

  將 View Composer 資料庫新增到 Oracle 12c 或 11g 執行個體之後，您必須設定 ODBC 與新資料庫的連線，讓 View Composer 服務可以看到這個資料來源。

將 View Composer 資料庫新增到 Oracle 12c 或 11g 中

您可以使用「Oracle 資料庫組態輔助程式」，將新的 View Composer 資料庫新增到現有的 Oracle 12c 或 11g 執行個體。

必要條件

請確認本機或遠端電腦上已安裝支援的 Oracle 12c 或 11g 版本。請參閱 View Composer 和事件資料庫的資料庫需求。

程序

1 在您要新增 View Composer 資料庫所在的電腦上，啟動**資料庫組態助理員**。

資料庫版本	動作
Oracle 12c	選取**開始 > 所有程式 > Oracle-OraDb12c_home > 組態設定和移轉工具 > 資料庫組態輔助程式**。
Oracle 11g	選取**開始 > 所有程式 > Oracle-OraDb11g_home > 組態設定和移轉工具 > 資料庫組態輔助程式**。

2 在「作業」頁面上，選取**建立資料庫**。

3 在「資料庫範本」頁面上，選取**一般用途或交易處理**範本。

4 在「資料庫識別碼」頁面上，輸入「全域資料庫名稱」及「Oracle 系統識別碼」(SID) 首碼。

為簡化起見，請為兩個項目使用相同的值。

5 在「管理員選項」頁面上，按**下一步**來接受預設設定。

6 在「資料庫認證」頁面上，選取**所有帳戶使用同一個管理密碼**，並輸入密碼。

7 在其餘的組態頁面上，按**下一步**來接受預設設定。

8 在「建立選項」頁面上，確認已選取**建立資料庫**，然後按一下**完成**。

9 在「確認」頁面上，檢閱選項，然後按一下**確定**。

組態工具便會建立資料庫。

10 在「資料庫建立完成」頁面上，按一下**確定**。

後續步驟

請依照將 ODBC 資料來源新增至 Oracle 12c 或 11g 中中的指示進行。

使用 SQL 陳述式將 View Composer 資料庫新增至 Oracle 執行個體

建立資料庫時，您可以自訂資料和記錄檔的位置。

必要條件

View Composer 資料庫必須有特定的表格空間和權限。您可以使用 SQL 陳述式，在 Oracle 12c 或 11g 資料庫執行個體中建立 View Composer 資料庫。

請確認本機或遠端電腦上已安裝支援的 Oracle 12c 或 11g 版本。如需詳細資料，請參閱 View Composer 和事件資料庫的資料庫需求。

程序

1 使用系統帳戶登入 SQL*Plus 工作階段。

2 執行下列 SQL 陳述式以建立資料庫。

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

在此範例中，VCMP 是 View Composer 資料庫的範例名稱，而 `vcmp01.dbf` 是資料庫檔案的名稱。

若是 Windows 安裝，請在 `vcmp01.dbf` 檔案的目錄路徑中使用 Windows 慣例。

後續步驟

如果您要使用特定的安全性權限執行 View Composer 資料庫，請依照設定 View Composer 的 Oracle 資料庫使用者中的指示進行。

請依照將 ODBC 資料來源新增至 Oracle 12c 或 11g 中中的指示進行

設定 View Composer 的 Oracle 資料庫使用者

根據預設，執行 View Composer 資料庫的資料庫使用者擁有 Oracle 系統管理員權限。若要限制執行 View Composer 資料庫之使用者的安全性權限，您必須設定具有特定權限的 Oracle 資料庫使用者。

必要條件

確認已在 Oracle 12c 或 11g 執行個體中建立 View Composer 資料庫。

程序

1 使用系統帳戶登入 SQL*Plus 工作階段。

2 執行下列 SQL 命令以建立具有正確權限的 View Composer 資料庫使用者。

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
   grant connect to VCMPADMIN;
   grant resource to VCMPADMIN;
   grant create view to VCMPADMIN;
   grant create sequence to VCMPADMIN;
   grant create table to VCMPADMIN;
   grant create materialized view to VCMPADMIN;
   grant execute on dbms_lock to VCMPADMIN;
   grant execute on dbms_job to VCMPADMIN;
   grant unlimited tablespace to VCMPADMIN;
```

在此範例中，使用者名稱為 VCMPADMIN，而 View Composer 資料庫名稱為 VCMP。

根據預設，`resource` 角色已指定了 `create procedure`、`create table` 及 `create sequence` 權限。如果 `resource` 角色沒有這些權限，請將它們明確授與 View Composer 資料庫使用者。

將 ODBC 資料來源新增至 Oracle 12c 或 11g 中

將 View Composer 資料庫新增到 Oracle 12c 或 11g 執行個體之後，您必須設定 ODBC 與新資料庫的連線，讓 View Composer 服務可以看到這個資料來源。

設定 View Composer 的 ODBC DSN 時，請保護適合您環境層級的基礎資料庫連線的安全。如需有關保護資料庫連線安全的相關資訊，請參閱 Oracle 資料庫文件。

如果基礎資料庫連線使用 SSL 加密，建議您使用信任的 CA 所簽署的 SSL 憑證，設定資料庫伺服器。如果您使用自我簽署的憑證，您的資料庫連線可能會容易造成攔截式攻擊。

必要條件

請確認您已完成將 View Composer 資料庫新增到 Oracle 12c 或 11g 中或使用 SQL 陳述式將 View Composer 資料庫新增至 Oracle 執行個體中所述的步驟。

程序

1. 在 View Composer 資料庫電腦上，選取**開始 > 系統管理工具 > 資料來源 (ODBC)**。
2. 從 **Microsoft ODBC 資料來源管理員**精靈中，選取**系統 DSN** 索引標籤。
3. 按一下**新增**，然後從清單中選取適當的 Oracle 驅動程式。

   例如：`OraDb11g_home`
4. 按一下**完成**。
5. 在「Oracle ODBC 驅動程式組態」對話方塊中，輸入要搭配 View Composer 使用的 DSN、資料來源的描述，以及要連線到資料庫的使用者識別碼。

   如果您使用特定的安全性權限設定 Oracle 資料庫使用者識別碼，請指定此使用者識別碼。

   備註 當您安裝 View Composer 服務時，請使用 DSN。
6. 從下拉式功能表中選取「全域資料庫名稱」，藉以指定 **TNS 服務名稱**。

   Oracle 資料庫組態助理員會指定「全域資料庫名稱」。
7. 若要確認資料來源，請按一下**測試連線**，然後按一下**確定**。

後續步驟

安裝新的 View Composer 服務。請參閱安裝 View Composer 服務。

設定 View Composer 的 SSL 憑證

根據預設，自我簽署憑證會與 View Composer 一起安裝。您可以使用預設的憑證進行測試，但是供生產用途的憑證應以憑證授權單位 (CA) 簽署的憑證取代。

您可以在安裝 View Composer 之前或之後設定憑證。在 View 5.1 和更新版本中，設定憑證的方式是將它匯入安裝或將安裝 View Composer 所在 Windows Server 電腦上的 Windows 本機電腦憑證存放區中。

- 如果您在安裝 View Composer 之前匯入 CA 簽署的憑證，就可以在 View Composer 安裝期間選取簽署的憑證。此方法可免除安裝後手動取代預設憑證的工作。
- 如果您要在安裝 View Composer 之後將現有憑證或預設的自我簽署憑證取代為新憑證，則必須匯入新憑證並且執行 `SviConfig ReplaceCertificate` 公用程式，將新憑證繫結至 View Composer 所使用的連接埠。

如需設定 SSL 憑證和使用 `SviConfig ReplaceCertificate` 公用程式的詳細資料，請參閱第 8 章 設定 Horizon 7 Server 的 TLS 憑證。

如果您在相同的 Windows Server 電腦上安裝 vCenter Server 和 View Composer，則它們可以使用相同的 SSL 憑證，但是您必須為每個元件個別設定憑證。

安裝 View Composer 服務

您必須安裝 View Composer 服務才能使用 View Composer。Horizon 7 會使用 View Composer 在 vCenter Server 中建立及部署連結複製桌面平台。

您可以在安裝 vCenter Server 所在的 Windows Server 電腦上，或另一部 Windows Server 電腦上安裝 View Composer 服務。獨立式 View Composer 安裝可與 Windows Server 電腦上安裝的 vCenter Server 搭配運作，以及與 Linux 型 vCenter Server Appliance 搭配運作。

View Composer 軟體無法與其他任何 Horizon 7 軟體元件 (包括複寫伺服器、安全伺服器、連線伺服器、Horizon Agent 或 Horizon Client) 共存於相同的虛擬或實體機器上。

為獲得增強安全性，我們建議您設定加密套件以移除已知弱點。如需針對執行 View Composer 或 Horizon Agent 的 Windows 機器設定加密套件網域原則的指示，請參閱 在 SSL/TLS 中停用弱加密。

必要條件

- 確認您的安裝滿足 View Composer 需求中所述的 View Composer 需求。
- 確認沒有其他 Horizon 7 元件 (包括連線伺服器、安全伺服器、Horizon Agent 或 Horizon Client) 安裝在您打算安裝 View Composer 的機器上。
- 確認您擁有安裝及使用 View Composer 的授權。
- 確認您有在「ODBC 資料來源管理員」精靈中提供的 DSN、網域管理員使用者名稱及密碼。您要在安裝 View Composer 服務時輸入這項資訊。
- 如果您打算在安裝期間為 View Composer 設定 CA 所簽署的 SSL 憑證，請確認憑證已匯入 Windows 本機電腦憑證存放區。請參閱第 8 章 設定 Horizon 7 Server 的 TLS 憑證。
- 確認 View Composer 電腦上執行的應用程式都未使用 Windows SSL 程式庫 (這些程式庫需要 Microsoft Secure Channel (Schannel) 安全性套件所提供的 SSL 2 版 (SSLv2))。View Composer 安裝程式會停用 Microsoft Schannel 上的 SSLv2。應用程式 (如 Tomcat (使用 Java SSL) 或 Apache (使用 OpenSSL)) 不受此限制影響。
- 若要執行 View Composer 安裝程式，您必須是擁有系統管理員權限的使用者。

程序

1 從位於 http://www.vmware.com/products/ 的 VMware 產品頁面，將 View Composer 安裝程式檔案下載至 Windows Server 電腦。

  安裝程式的檔案名稱為 `VMware-viewcomposer-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是組建編號，而 *y.y.y* 是版本號碼。此安裝程式檔案會在 64 位元 Windows Server 作業系統上安裝 View Composer 服務。

2 若要啟動 View Composer 安裝程式，請用滑鼠右鍵按一下安裝程式檔案，並選取**以管理員身分執行**。

3 接受 VMware 授權條款。

4 接受或變更目的地資料夾。

5 輸入您在 Microsoft 或 Oracle **ODBC 資料來源管理員**精靈中提供的 View Composer 資料庫的 DSN。

例如：**VMware View Composer**

備註 如果您未設定 View Composer 資料庫的 DSN，請按一下 **ODBC DSN 設定**立即設定名稱。

6 輸入您在 **ODBC 資料來源管理員**精靈中提供的網域管理員使用者名稱和密碼。

如果您使用特定的安全性權限設定 Oracle 資料庫使用者，請指定此使用者名稱。

7 輸入連接埠號碼或接受預設值。

View 連線伺服器會使用此連接埠與 View Composer 服務進行通訊。

8 提供 SSL 憑證。

選項	動作
建立預設 SSL 憑證	選取此選項按鈕會建立 View Composer 服務的預設 SSL 憑證。 安裝後，您可以將預設憑證取代為 CA 簽署的 SSL 憑證。
使用現有 SSL 憑證	如果您已安裝簽署的 SSL 憑證且想要用於 View Composer 服務，則選取此選項按鈕。從清單選取 SSL 憑證。

9 按一下**安裝**和**完成**，完成 View Composer 服務安裝。

VMware Horizon View Composer 服務便會啟動。

View Composer 會使用 Windows Server 作業系統提供的密碼編譯加密套件。您應該依照組織的指導方針，管理 Windows Server 系統上的加密套件。如果您的組織未提供指導方針，VMware 建議您停用 View Composer Server 上的弱式密碼編譯加密套件，以強化 Horizon 7 環境的安全性。如需管理密碼編譯加密套件的相關資訊，請參閱 Microsoft 文件。

後續步驟

如果您擁有舊版 vCenter Server，請參閱 在從 View Composer 連往 vCenter 和 ESXi 的連線上啟用 TLSv1.0。

如果手動設定 SQL Server 資料庫權限並已將其指派給使用者，您可以從該使用者撤銷資料庫管理員角色。如需詳細資訊，請參閱藉由手動建立資料庫角色來設定 SQL Server 資料庫權限的程序中的最後一步。

在從 View Composer 連往 vCenter 和 ESXi 的連線上啟用 TLSv1.0

Horizon 7 及更新版本的元件預設會停用 TLSv1.0 安全性通訊協定。如果您的部署包含僅支援 TLSv1.0 的舊版 vCenter Server，在安裝或升級至 View Composer 7.0 或更新版本後，您可能需要為 View Composer 連線啟用 TLSv1.0。

有些 vCenter Server 5.0、5.1 和 5.5 的舊維護版本只支援 TLSv1.0，但 Horizon 7 及更新版本預設已不再啟用此功能。如果無法將 vCenter Server 升級至支援 TLSv1.1 或 TLSv1.2 的版本，您可為 View Composer 連線啟用 TLSv1.0。

如果您的 ESXi 主機未執行 ESXi 6.0 U1b 或更新版本，而且無法升級，則可能也需要啟用從 View Composer 連往 ESXi 主機的 TLSv1.0 連線。

必要條件

- 確認您已安裝 View Composer 7.0 及更新版本。
- 確認您可以管理員身分登入 View Composer 機器，以使用 Windows 登錄編輯程式。

程序

1. 在主控 View Composer 的機器上，開啟 Windows 登錄編輯程式 (`regedit.exe`)。
2. 瀏覽至 `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client`

   如果此機碼尚不存在，請建立此機碼。
3. 刪除 **Enabled** 值 (如果此值存在)。
4. 建立或編輯 **DWORD** 值 **DisabledByDefault**，並將其設定為 **0**。
5. 重新啟動 VMware Horizon View Composer 服務。

   現在已啟用從 View Composer 連往 vCenter 的 TLSv1.0 連線。
6. 在 View Composer 機器的 Windows 登錄中，瀏覽至 `HKLM\SOFTWARE\VMware, Inc.\VMware View Composer`。
7. 建立或編輯字串值 **EnableTLS1.0**，並將其設定為 **1**。
8. 如果 View Composer 主機為 64 位元機器，請瀏覽至 `HKLM\SOFTWARE\WOW6432Node\VMware, Inc\VMware View Composer`。
9. 建立或編輯字串值 **EnableTLS1.0**，並將其設定為 **1**。
10. 重新啟動 VMware Horizon View Composer 服務。

    現在已啟用從 View Composer 連往 ESXi 主機的 TLSv1.0 連線。

設定 View Composer 的基礎結構

您可以利用 vSphere、vCenter Server、Active Directory 及基礎結構的其他元件中的各項功能，最佳化 View Composer 的效能、可用性及可靠性。

設定 View Composer 的 vSphere 環境

若要支援 View Composer，您應在安裝及設定 vCenter Server、ESXi 與其他 vSphere 元件時遵循特定的最佳做法。

這些最佳做法可讓 View Composer 在 vSphere 環境中有效率地運作。

- 建立連結複製虛擬機器的路徑和資料夾資訊後，請勿在 vCenter Server 中變更資訊。請改用 Horizon Administrator 變更資料夾資訊。

  如果您在 vCenter Server 中變更此資訊，Horizon 7 將無法成功查閱 vCenter Server 中的虛擬機器。
- 請確保已將 ESXi 主機上的 vSwitch 設定設為具有足夠的連接埠，以支援 ESXi 主機上所執行連結複製虛擬機器上設定的虛擬 NIC 總數。
- 當您在資源集區中部署連結複製桌面時，請確定您的 vSphere 環境擁有足夠的 CPU 和記憶體可裝載您需要的桌面數目。請使用 vSphere Client 監視資源集區中的 CPU 和記憶體使用量。
- 在 vSphere 5.1 及更新版本中，若複本磁碟儲存在 VMFS5 (或更新的資料存放區) 或 NFS 資料存放區上，則用於 View Composer 連結複製的叢集可包含超過八部 ESXi 主機。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。
- 使用 vSphere DRS。DRS 能在主機之間有效散佈連結複製虛擬機器。

  備註 連結複製桌面不支援 Storage vMotion。

View Composer 的其他最佳做法

為確保 View Composer 有效率地運作，請檢查您的動態名稱服務 (DNS) 是否正確運作，並在猶豫時執行防毒軟體掃描。

您可以透過確認 DNS 解析是否正確運作來克服因 DNS 錯誤所造成的間歇性問題。View Composer 服務依賴動態名稱解析，與其他電腦進行通訊。若要測試 DNS 運作，請透過名稱偵測 Active Directory 及 View 連線伺服器電腦。

如果您要錯開執行防毒軟體的時間，連結複製桌面的效能不會受到影響。如果防毒軟體同時在所有連結複製中執行，在儲存子系統中會發生過度的每秒的記憶體運算 (IOPS)。這個過度的活動可能會影響連結複製桌面的效能。

安裝 Horizon 連線伺服器 7

若要使用連線伺服器，您需要在支援的電腦上安裝軟體，設定必要的元件，並選擇性地最佳化元件。

本章節討論下列主題：

安裝 Horizon 連線伺服器軟體

根據您的 Horizon 7 部署的效能、可用性和安全性需要，您可以安裝連線伺服器的單一執行個體、連線伺服器的複寫執行個體，以及安全伺服器。您必須安裝至少一個連線伺服器執行個體。

安裝連線伺服器時，您要選取安裝類型。

標準安裝	使用新的 View LDAP 組態產生連線伺服器執行個體。
複寫安裝	使用從現有執行個體複製的 View LDAP 組態產生連線伺服器執行個體。

安全伺服器安裝	產生的連線伺服器執行個體會在網際網路與內部網路之間增加一層額外的安全性。
註冊伺服器安裝	安裝 True SSO (Single Sign-On) 功能所需的註冊伺服器，以讓使用者在登入 VMware Identity Manager 後，不用提供 Active Directory 認證即可連線至遠端桌面平台或應用程式。註冊伺服器會要求短期憑證以用於驗證。 **備註** 由於此功能需要同時設定憑證授權機構以及執行特定組態，因此在《Horizon 7 管理》文件的〈驗證使用者而不要求認證〉一章中提供註冊伺服器的安裝程序，而非在此安裝文件中提供。

Horizon 連線伺服器的安裝先決條件

在您安裝連線伺服器之前，必須先確認您的安裝環境符合特定先決條件。

- 您必須具有有效的 Horizon 7 授權金鑰。
- 您必須將連線伺服器主機加入 Active Directory 網域。連線伺服器支援下列 Active Directory Domain Services (AD DS) 網域功能層級：
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016

  連線伺服器主機不得為網域控制站。

  備註 連線伺服器不會也不需要對 Active Directory 進行任何結構描述或組態更新。
- 請勿在已安裝 Windows 終端機伺服器角色的系統上安裝連線伺服器。您必須從連線伺服器安裝所在的任何系統中移除 Windows 終端機伺服器角色。
- 請勿在執行任何其他功能或角色的系統上安裝連線伺服器。例如，不要使用相同的系統來裝載 vCenter Server。
- 安裝連線伺服器的系統必須具有不會變更的 IP 位址。在 IPv4 環境中，請設定靜態 IP 位址。在 IPv6 環境中，機器會自動取得不會變更的 IP 位址。
- 若要執行 Horizon 連線伺服器安裝程式，您必須使用在系統上具有管理員權限的網域使用者帳戶。
- 當您安裝連線伺服器時，系統會為 Administrators 帳戶進行授權。您可以指定本機管理員群組或是網域使用者或群組帳戶。Horizon 7 僅會將完整的管理權限 (包括安裝複寫的連線伺服器執行個體的權限) 指派給此帳戶。如果您指定網域使用者或群組，則必須先在 Active Directory 中建立帳戶，再執行安裝程式。

使用新組態安裝 Horizon 連線伺服器

若要將連線伺服器安裝為單一伺服器或複寫的連線伺服器執行個體群組中的第一個執行個體，您可以使用標準安裝選項。

當您選取標準安裝選項時，安裝會建立新的本機 View LDAP 組態。安裝會載入結構描述定義、目錄資訊樹狀結構 (DIT) 定義及 ACL，並且初始化資料。

安裝後，您可以使用 Horizon Administrator 管理多數的 View LDAP 組態資料。連線伺服器會自動維護部分 View LDAP 項目。

連線伺服器軟體無法與其他任何 Horizon 7 軟體元件 (包括複寫伺服器、安全伺服器、View Composer、Horizon Agent 或 Horizon Client) 共存於相同的虛擬或實體機器上。

當您使用新組態安裝連線伺服器時，您可以參與客戶經驗改進計劃。VMware 會收集有關部署的匿名資料，以便改進 VMware 對使用者需求的回應。不會收集任何可用於識別貴組織的資料。您可以選擇不參與，只要在安裝期間取消選取此選項即可。如果您在安裝後改變主意，可以編輯 Horizon Administrator 中的「產品授權及使用」頁面來加入或退出計劃。若要檢閱從中收集資料的欄位清單 (包括匿名欄位)，請參閱《Horizon 7 管理》文件中的〈客戶經驗改進計劃所收集的資訊〉。

依預設，HTML Access 元件會在您安裝連線伺服器時安裝在連線伺服器主機上。此元件會設定 Horizon 7 使用者入口網站頁面，除 Horizon Client 圖示外，還會顯示 HTML Access 圖示。附加的圖示可讓使用者在連線至其桌面平台時選取 HTML Access。

如需為 HTML Access 設定連線伺服器的概觀，請參閱 Horizon Client 說明文件頁面上的《VMware Horizon HTML Access 安裝和設定指南》文件。

必要條件

- 確認您能夠以具備連線伺服器安裝所在 Windows Server 電腦之管理員權限的網域使用者身分登入。
- 確認您的安裝滿足 Horizon 連線伺服器需求中所述的需求。
- 準備您的環境進行安裝。請參閱 Horizon 連線伺服器的安裝先決條件。
- 如果您想要授權網域使用者或群組作為 Administrators 帳戶，請確認您已在 Active Directory 中建立網域帳戶。
- 準備資料復原密碼。備份連線伺服器時，系統會將 View LDAP 組態匯出為加密的 LDIF 資料。若要還原加密的備份 Horizon 7 組態，您必須提供資料復原密碼。密碼必須包含 1 至 128 個字元。請遵循組織的最佳做法，產生安全密碼。

  重要 您將需要資料復原密碼來維持 Horizon 7 的運作，並避免在業務持續性與災難復原 (BCDR) 狀況下發生停機。您可以在安裝連線伺服器時，隨密碼提供密碼提醒。

- 熟悉必須在 Windows 防火牆上針對連線伺服器執行個體開放的網路連接埠。請參閱 Horizon 連線伺服器的防火牆規則。
- 如果您打算將安全伺服器與此連線伺服器執行個體配對，請確認作用中設定檔中的 [具有進階安全性的 Windows 防火牆] 設為**開啟**。建議您將所有設定檔的這個設定設為**開啟**。依預設，IPsec 規則會控管安全伺服器與連線伺服器之間的連線，且必須啟用 [具有進階安全性的 Windows 防火牆]。

- 如果您的網路拓撲中的安全伺服器與連線伺服器執行個體之間包含後端防火牆，則必須設定防火牆以支援 IPsec。請參閱設定後端防火牆支援 IPsec。

程序

1 從 VMware 下載網站下載連線伺服器安裝程式檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含連線伺服器。

安裝程式檔案名稱是 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是組建編號，而 *y.y.y* 是版本號碼。

2 若要啟動連線伺服器安裝程式，請按兩下安裝程式檔案。

3 接受 VMware 授權條款。

4 接受或變更目的地資料夾。

5 選取 **View 標準伺服器**安裝選項。

6 選取網際網路通訊協定 (IP) 版本、**IPv4** 或 **IPv6**。

您必須安裝具有相同 IP 版本的所有 Horizon 7 元件。

7 選取要啟用或停用 FIPS 模式。

只有在 Windows 中啟用 FIPS 模式時才可使用此選項。

8 如果您打算允許使用者藉由使用網頁瀏覽器連線至其桌面平台，請確保已選取**安裝 HTML Access**。

如果選取的是 **IPv4**，此設定將預設為選取。如果選取的是 **IPv6**，則不會顯示此設定，因為 HTML Access 在 IPv6 環境中不受支援。

9 輸入資料復原密碼，以及選擇性地輸入密碼提醒。

10 選擇如何設定 Windows 防火牆服務。

選項	動作
自動設定 Windows 防火牆	讓安裝程式設定 Windows 防火牆以允許必要的網路連線。
不設定 Windows 防火牆	手動設定 Windows 防火牆規則。 只有在組織使用自己預先定義的規則設定 Windows 防火牆時選取此選項。

11 授權 Horizon Administrators 帳戶。

只有此帳戶的成員才能登入 Horizon Administrator、執行完整管理權限，以及安裝複寫的連線伺服器執行個體和其他 Horizon 7 Server。

選項	說明
授權本機管理員群組	允許本機管理員群組中的使用者管理 Horizon 7。
授權特定的網域使用者或網域群組	允許指定的網域使用者或群組管理 Horizon 7。

12 如果您已指定網域 Horizon Administrators 帳戶，並且以本機管理員的身分或沒有網域帳戶存取權的另一個使用者身分執行安裝程式，請提供包含授權使用者名稱和密碼的認證來登入網域。

使用 *domain name\user name* 或使用者主體名稱 (UPN) 格式。UPN 格式可以是 *user@domain.com*。

13 選擇是否參與客戶經驗改進計劃。

如果您參與，可以選擇性地選取組織的類型、規模和位置。

14 完成安裝精靈，以完成連線伺服器的安裝。

15 檢查 Windows Server 電腦的新修補程式，並且視需要執行 Windows Update。

即使您在安裝連線伺服器之前已完整修補 Windows Server 電腦，安裝仍可能初次啟用作業系統功能。現在可能需要其他修補程式。

Horizon 7 服務會安裝在 Windows Server 電腦上：

- VMware Horizon 連線伺服器
- VMware Horizon View Framework 元件
- VMware Horizon View 訊息匯流排元件
- VMware Horizon View 指令碼主機
- VMware Horizon View 安全閘道元件
- VMware Horizon View PCoIP 安全閘道
- VMware Horizon View Blast 安全閘道
- VMware Horizon View Web 元件
- VMware VCMSDS，提供 View LDAP 目錄服務

如需這些服務的相關資訊，請參閱《Horizon 7 管理》文件。

如果已在安裝期間選取**安裝 HTML Access** 設定，則 HTML Access 元件會安裝在 Windows Server 電腦上。此元件會在 Horizon 7 使用者入口網站頁面中設定 HTML Access 圖示，並在 Windows 防火牆中啟用 **VMware Horizon View 連線伺服器 (Blast-In)** 規則。此防火牆規則允許用戶端裝置上的網頁瀏覽器在 TCP 連接埠 8443 上連線至連線伺服器。

後續步驟

設定連線伺服器的 SSL 伺服器憑證。請參閱第 8 章 設定 Horizon 7 Server 的 TLS 憑證。

如果您擁有舊版 vCenter Server，請參閱 在從連線伺服器連往 vCenter 的連線上啟用 TLSv1.0。

在連線伺服器上執行初始組態。請參閱第 9 章 初次設定 Horizon 7。

如果您打算在部署中包含複寫的連線伺服器執行個體和安全伺服器，則必須藉由執行連線伺服器安裝程式檔案來安裝每個伺服器執行個體。

如果您要重新安裝連線伺服器，且您已將資料收集器集合工具設定為監控效能資料，請停止資料收集器集合工具，然後重新將其啟動。

以無訊息方式安裝 Horizon 連線伺服器

您可以使用 Microsoft Windows Installer (MSI) 的無訊息安裝功能，在數部 Windows 電腦上執行連線伺服器的標準安裝。在無訊息安裝中，您會使用命令列，而且不必回應精靈的提示。

透過無訊息安裝，您便能有效地將 Horizon 7 元件部署在大型企業中。

必要條件

- 確認您能夠以具備連線伺服器安裝所在 Windows Server 電腦之管理員權限的網域使用者身分登入。
- 確認您的安裝滿足 Horizon 連線伺服器需求中所述的需求。
- 準備您的環境進行安裝。請參閱 Horizon 連線伺服器的安裝先決條件。
- 如果您想要授權網域使用者或群組作為 Horizon Administrators 帳戶，請確認您已在 Active Directory 中建立網域帳戶。
- 如果您使用 MIT Kerberos 驗證登入您要安裝連線伺服器的 Windows Server 2008 R2 電腦，請安裝知識庫 978116 中所述的 Microsoft Hotfix，網址為：http://support.microsoft.com/kb/978116。
- 熟悉必須在 Windows 防火牆上針對連線伺服器執行個體開放的網路連接埠。請參閱 Horizon 連線伺服器的防火牆規則。
- 如果您打算將安全伺服器與此連線伺服器執行個體配對，請確認作用中設定檔中的 [具有進階安全性的 Windows 防火牆] 設為**開啟**。建議您將所有設定檔的這個設定設為**開啟**。依預設，IPsec 規則會控管安全伺服器與連線伺服器之間的連線，且必須啟用 [具有進階安全性的 Windows 防火牆]。
- 如果您的網路拓撲中的安全伺服器與連線伺服器執行個體之間包含後端防火牆，則必須設定防火牆以支援 IPsec。請參閱設定後端防火牆支援 IPsec。
- 確認連線伺服器安裝所在的 Windows 電腦採用 MSI 執行階段引擎 2.0 版或更新版本。如需詳細資料，請參閱 Microsoft 網站。
- 自行熟悉 MSI 安裝程式命令列選項。請參閱 Microsoft Windows Installer 命令列選項。
- 熟悉連線伺服器之標準安裝提供的無訊息安裝屬性。請參閱 Horizon 連線伺服器標準安裝的無訊息安裝內容。

程序

1 從 VMware 下載網站下載連線伺服器安裝程式檔案，網址為 https://my.vmware.com/web/vmware/downloads。

  在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含連線伺服器。

  安裝程式檔案名稱是 `VMware-viewconnectionserver-x86_64-`*`y.y.y-xxxxxx`*`.exe`，其中 *xxxxxx* 是組建編號，而 *y.y.y* 是版本號碼。

2 在 Windows Server 電腦上開啟命令提示字元。

3 將安裝命令輸入成一行。

例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1 VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

重要 當您執行無訊息安裝時，包括資料復原密碼在內的整個命令列都會記錄在安裝程式的 `vminst.log` 檔案中。安裝完成後，請使用 Horizon Administrator 刪除此記錄檔或變更資料復原密碼。

4 檢查 Windows Server 電腦的新修補程式，並且視需要執行 Windows Update。

即使您在安裝連線伺服器之前已完整修補 Windows Server 電腦，安裝仍可能初次啟用作業系統功能。現在可能需要其他修補程式。

Horizon 7 服務會安裝在 Windows Server 電腦上：

- VMware Horizon 連線伺服器
- VMware Horizon View Framework 元件
- VMware Horizon View 訊息匯流排元件
- VMware Horizon View 指令碼主機
- VMware Horizon View 安全閘道元件
- VMware Horizon View PCoIP 安全閘道
- VMware Horizon View Blast 安全閘道
- VMware Horizon View Web 元件
- VMware VCMSDS，提供 View LDAP 目錄服務

如果已在安裝期間選取**安裝 HTML Access** 設定，則 HTML Access 元件會安裝在 Windows Server 電腦上。此元件會在 Horizon 7 使用者入口網站頁面中設定 HTML Access 圖示，並在 Windows 防火牆中啟用 **VMware Horizon View 連線伺服器 (Blast-In)** 規則。此防火牆規則允許用戶端裝置上的網頁瀏覽器在 TCP 連接埠 8443 上連線至連線伺服器。

如需這些服務的相關資訊，請參閱《Horizon 7 管理》文件。

後續步驟

設定連線伺服器的 SSL 伺服器憑證。請參閱第 8 章 設定 Horizon 7 Server 的 TLS 憑證。

如果您擁有舊版 vCenter Server，請參閱 在從連線伺服器連往 vCenter 的連線上啟用 TLSv1.0。

如果您是初次設定 Horizon 7，請在連線伺服器上執行初始組態。請參閱第 9 章 初次設定 Horizon 7。

Horizon 連線伺服器標準安裝的無訊息安裝內容

當您從命令列執行無訊息安裝或升級時，可以加上特定的連線伺服器內容。您必須使用 *PROPERTY=value* 格式，Microsoft Windows Installer (MSI) 才能解譯屬性和值。無訊息升級會使用相同的安裝命令。

表 7-1. 在標準安裝中，以無訊息方式安裝連線伺服器適用的 MSI 屬性

MSI 屬性	說明	預設值
INSTALLDIR	連線伺服器軟體安裝所在的路徑和資料夾。 例如：`INSTALLDIR=""D:\abc\my folder""` 括住路徑的兩組雙引號允許 MSI 安裝程式將空間轉譯為路徑的有效部分。	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	Horizon Server 安裝的類型： ■ **1**.標準安裝 ■ **2**.複寫安裝 ■ **3**.安全伺服器安裝 ■ **5**.註冊伺服器安裝 例如，若要執行標準安裝，請定義 `VDM_SERVER_INSTANCE_TYPE=1`	1
FWCHOICE	決定是否為連線伺服器執行個體設定防火牆的 MSI 屬性。 值為 1 時，設定防火牆。值為 2 時，不設定防火牆。 例如：`FWCHOICE=1`	1
VDM_INITIAL_ADMIN_SID	使用 Horizon 中的完整管理權限授權的初始 Horizon Administrator 使用者或群組的 SID。 預設值為連線伺服器電腦上的本機管理員群組的 SID。您可以指定網域使用者或群組帳戶的 SID。	`S-1-5-32-544`
VDM_SERVER_RECOVERY_PWD	資料復原密碼。如果在 Horizon LDAP 中沒有設定資料復原密碼，則此屬性為強制的。 密碼必須包含 1 至 128 個字元。請遵循組織的最佳做法，產生安全密碼。	無
VDM_SERVER_RECOVERY_PWD_REMINDER	資料復原密碼提醒。此屬性為選用。	無
VDM_IP_PROTOCOL_USAGE	指定 Horizon 元件用於通訊的 IP 版本。可能的值為 **IPv4** 和 **IPv6**。	**IPv4**
VDM_FIPS_ENABLED	指定要啟用或停用 FIPS 模式。值為 1 則啟用 FIPS 模式。值為 0 則停用 FIPS 模式。若此屬性設為 1 且 Windows 不位於 FIPS 模式，則安裝程式將中止。	0
HTMLACCESS	控制 HTML Access 附加元件的安裝。將此內容設定為 1 可設定 HTML Access 或忽略此內容 (如果不需要 HTML Access)。	1

在從連線伺服器連往 vCenter 的連線上啟用 TLSv1.0

Horizon 7 及更新版本的元件預設會停用 TLSv1.0 安全性通訊協定。如果您的部署包含僅支援 TLSv1.0 的舊版 vCenter Server，在安裝或升級至連線伺服器 7.0 或更新版本後，您可能需要為連線伺服器連線啟用 TLSv1.0。

某些 vCenter Server 5.1 和 5.5 的較舊維護版本僅支援 TLSv1.0，但 Horizon 7 和更新版本依預設已不再啟用此功能。如果無法將 vCenter Server 升級至支援 TLSv1.1 或 TLSv1.2，您可為連線伺服器連線啟用 TLSv1.0。

必要條件

- 如果您要升級至 Horizon 7，請在升級前執行此程序，以將必須重新啟動服務的次數降至最低。在升級期間，連線伺服器服務會重新啟動，並且需要重新啟動才能套用此程序中說明的組態變更。如果您尚未執行此程序就進行升級，將需要再次重新啟動服務。
- 有關如何在 Windows 作業系統版本使用 ADSI Edit 公用程式的資訊，請參閱 Microsoft TechNet 網站。

程序

1 在連線伺服器主機上啟動 ADSI Edit 公用程式。

2 在主控台樹狀結構中，選取**連線至**。

3 在**選取或輸入辨別名稱或命名內容**文字方塊中，輸入辨別名稱 **DC=vdi, DC=vmware, DC=int**。

4 在 [電腦] 窗格中選取或輸入 **localhost:389**，或連線伺服器主機的完整網域名稱 (FQDN)，後面再加上連接埠 389。

   例如：**localhost:389** 或 **mycomputer.example.com:389**

5 依序展開 ADSI Edit 樹狀結構和 **OU=Properties**、選取 **OU=Global**，然後按兩下右窗格中的 **CN=Common**。

6 在 [內容] 對話方塊中，編輯 **pae-ClientSSLSecureProtocols** 屬性以新增下列值

   \LIST:TLSv1.2,TLSv1.1,TLSv1

   請務必在該行開頭處加上反斜線。

7 按一下**確定**。

8 如果是全新安裝，若要套用組態變更，請重新啟動每個連線伺服器執行個體上的連線伺服器服務。

   如果您計劃執行升級，則不需重新啟動服務，因為升級程序會自動重新啟動服務。

安裝 Horizon 連線伺服器的複寫執行個體

為提供高可用性與負載平衡，您可以安裝一或多個額外的連線伺服器執行個體，用來複寫現有的連線伺服器執行個體。在複寫安裝之後，現有和新安裝的連線伺服器執行個體就會一致。

當您安裝複寫執行個體時，Horizon 7 會從現有的連線伺服器執行個體複製 View LDAP 組態資料。

安裝後，複寫群組中所有連線伺服器執行個體上的 View LDAP 組態資料會保持一致。在某個執行個體上進行變更時，更新的資訊會複製到其他執行個體。

如果複寫的執行個體失敗，群組中的其他執行個體會繼續運作。當失敗的執行個體恢復活動時，其組態會以中斷期間所做的變更進行更新。

備註　複寫功能是由 View LDAP 提供，它會使用與 Active Directory 相同的複寫技術。

複寫伺服器軟體無法與其他任何 Horizon 7 軟體元件 (包括安全伺服器、連線伺服器、View Composer、Horizon Agent 或 Horizon Client) 共存於相同的虛擬或實體機器上。

依預設，HTML Access 元件會在您安裝連線伺服器時安裝在連線伺服器主機上。此元件會設定 Horizon 7 使用者入口網站頁面，除 Horizon Client 圖示外，還會顯示 HTML Access 圖示。附加的圖示可讓使用者在連線至其桌面平台時選取 HTML Access。

如需為 HTML Access 設定連線伺服器的概觀，請參閱 Horizon Client 說明文件頁面上的《VMware Horizon HTML Access 安裝和設定指南》文件。

必要條件

- 確認網路上至少已安裝並設定一個連線伺服器執行個體。
- 若要安裝複寫執行個體，您必須以具有管理員角色的使用者身分登入。您可以在安裝第一個連線伺服器執行個體時，指定具備管理員角色的帳戶或群組。此角色可以指定給本機管理員群組或是網域使用者或群組。請參閱使用新組態安裝 Horizon 連線伺服器。
- 如果現有的連線伺服器執行個體與複寫執行個體位於不同的網域中，則網域使用者也必須具備現有執行個體安裝所在之 Windows Server 電腦的管理員權限。
- 如果您使用 MIT Kerberos 驗證登入您要安裝連線伺服器的 Windows Server 2008 R2 電腦，請安裝知識庫 978116 中所述的 Microsoft Hotfix，網址為：http://support.microsoft.com/kb/978116。
- 確認您的安裝滿足 Horizon 連線伺服器需求中所述的需求。
- 確認您安裝複寫的連線伺服器執行個體所在的電腦是透過高效能 LAN 連線。請參閱複寫 Horizon 連線伺服器執行個體的網路需求。
- 準備您的環境進行安裝。請參閱 Horizon 連線伺服器的安裝先決條件。
- 如果您安裝的複寫連線伺服器執行個體為 Horizon 7 5.1 或更新版本，而您要複寫的現有連線伺服器執行個體為 Horizon 7 5.0.*x* 或更早版本，請準備資料復原密碼。請參閱使用新組態安裝 Horizon 連線伺服器。
- 熟悉必須在 Windows 防火牆上針對連線伺服器執行個體開放的網路連接埠。請參閱 Horizon 連線伺服器的防火牆規則。
- 如果您打算將安全伺服器與此連線伺服器執行個體配對，請確認作用中設定檔中的 [具有進階安全性的 Windows 防火牆] 設為**開啟**。建議您將所有設定檔的這個設定設為**開啟**。依預設，IPsec 規則會控管安全伺服器與連線伺服器之間的連線，且必須啟用 [具有進階安全性的 Windows 防火牆]。
- 如果您的網路拓撲中的安全伺服器與連線伺服器執行個體之間包含後端防火牆，則必須設定防火牆以支援 IPsec。請參閱設定後端防火牆支援 IPsec。

程序

1 從 VMware 下載網站下載連線伺服器安裝程式檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含連線伺服器。

安裝程式檔案名稱是 `VMware-viewconnectionserver-x86_64-`*`y.y.y-xxxxxx`*`.exe`，其中 *xxxxxx* 是組建編號，而 *y.y.y* 是版本號碼。

2 若要啟動連線伺服器安裝程式，請按兩下安裝程式檔案。

3 接受 VMware 授權條款。

4 接受或變更目的地資料夾。

5 選取 **View 複寫伺服器**安裝選項。

6 選取網際網路通訊協定 (IP) 版本、**IPv4** 或 **IPv6**。

您必須安裝具有相同 IP 版本的所有 Horizon 7 元件。

7 選取要啟用或停用 FIPS 模式。

只有在 Windows 中啟用 FIPS 模式時才可使用此選項。

8 如果您打算允許使用者藉由使用 HTML Access 連線至其桌面平台，請確保已選取**安裝 HTML Access**。

如果選取的是 **IPv4**，此設定將預設為選取。如果選取的是 **IPv6**，則不會顯示此設定，因為 HTML Access 在 IPv6 環境中不受支援。

9 輸入您要複寫的現有連線伺服器執行個體的主機名稱或 IP 位址。

10 輸入資料復原密碼，以及選擇性地輸入密碼提醒。

只有在您要複寫的現有連線伺服器執行個體為 Horizon 7 5.0.*x* 或更早版本時，系統才會提示您輸入資料復原密碼。

11 選擇如何設定 Windows 防火牆服務。

選項	動作
自動設定 Windows 防火牆	讓安裝程式設定 Windows 防火牆以允許必要的網路連線。
不設定 Windows 防火牆	手動設定 Windows 防火牆規則。 只有在組織使用自己預先定義的規則設定 Windows 防火牆時選取此選項。

12 完成安裝精靈，以完成安裝複寫執行個體。

13 檢查 Windows Server 電腦的新修補程式，並且視需要執行 Windows Update。

即使您在安裝連線伺服器之前已完整修補 Windows Server 電腦，安裝仍可能初次啟用作業系統功能。現在可能需要其他修補程式。

Horizon 7 服務會安裝在 Windows Server 電腦上：

- VMware Horizon 連線伺服器
- VMware Horizon View Framework 元件
- VMware Horizon View 訊息匯流排元件
- VMware Horizon View 指令碼主機
- VMware Horizon View 安全閘道元件
- VMware Horizon View PCoIP 安全閘道
- VMware Horizon View Blast 安全閘道

- VMware Horizon View Web 元件
- VMware VCMSDS，提供 View LDAP 目錄服務

如需這些服務的相關資訊，請參閱《Horizon 7 管理》文件。

如果已在安裝期間選取**安裝 HTML Access** 設定，則 HTML Access 元件會安裝在 Windows Server 電腦上。此元件會在 Horizon 7 使用者入口網站頁面中設定 HTML Access 圖示，並在 Windows 防火牆中啟用 **VMware Horizon View 連線伺服器 (Blast-In)** 規則。此防火牆規則允許用戶端裝置上的網頁瀏覽器在 TCP 連接埠 8443 上連線至連線伺服器。

後續步驟

設定連線伺服器執行個體的 SSL 伺服器憑證。請參閱第 8 章 設定 Horizon 7 Server 的 TLS 憑證。

您不需要在連線伺服器的複寫執行個體上執行初始 Horizon 7 組態。複寫執行個體會從現有的連線伺服器執行個體繼承其組態。

不過，您可能需要設定此連線伺服器執行個體的用戶端連線設定，而且您可以調整 Windows Server 設定以支援大型部署。請參閱設定 Horizon Client 連線與 調整 Windows Server 設定以支援您的部署。

如果您要重新安裝連線伺服器，且您已將資料收集器集合工具設定為監控效能資料，請停止資料收集器集合工具，然後重新將其啟動。

以無訊息方式安裝 Horizon 連線伺服器的複寫執行個體

您可以使用 Microsoft Windows Installer (MSI) 的無訊息安裝功能，在數部 Windows 電腦上安裝連線伺服器的複寫執行個體。在無訊息安裝中，您會使用命令列，而且不必回應精靈的提示。

透過無訊息安裝，您便能有效地將 Horizon 7 元件部署在大型企業中。

必要條件

- 確認網路上至少已安裝並設定一個連線伺服器執行個體。
- 若要安裝複寫執行個體，您必須以有認證可存取 Administrators 帳戶的使用者身分登入。您可在安裝第一個連線伺服器執行個體時指定 Administrators 帳戶。此帳戶可以是本機管理員群組或是網域使用者或群組帳戶。請參閱使用新組態安裝 Horizon 連線伺服器。
- 如果現有的連線伺服器執行個體與複寫執行個體位於不同的網域中，則網域使用者也必須具備現有執行個體安裝所在之 Windows Server 電腦的管理員權限。
- 如果您使用 MIT Kerberos 驗證登入您要安裝連線伺服器的 Windows Server 2008 R2 電腦，請安裝知識庫 978116 中所述的 Microsoft Hotfix，網址為：http://support.microsoft.com/kb/978116。
- 確認您的安裝滿足 Horizon 連線伺服器需求中所述的需求。
- 確認您安裝複寫的連線伺服器執行個體所在的電腦是透過高效能 LAN 連線。請參閱複寫 Horizon 連線伺服器執行個體的網路需求。
- 準備您的環境進行安裝。請參閱 Horizon 連線伺服器的安裝先決條件。
- 熟悉必須在 Windows 防火牆上針對連線伺服器執行個體開放的網路連接埠。請參閱 Horizon 連線伺服器的防火牆規則。

- 如果您打算將安全伺服器與此連線伺服器執行個體配對，請確認作用中設定檔中的 [具有進階安全性的 Windows 防火牆] 設為**開啟**。建議您將所有設定檔的這個設定設為**開啟**。依預設，IPsec 規則會控管安全伺服器與連線伺服器之間的連線，且必須啟用 [具有進階安全性的 Windows 防火牆]。
- 如果您的網路拓撲中的安全伺服器與連線伺服器執行個體之間包含後端防火牆，則必須設定防火牆以支援 IPsec。請參閱設定後端防火牆支援 IPsec。
- 自行熟悉 MSI 安裝程式命令列選項。請參閱 Microsoft Windows Installer 命令列選項。
- 熟悉連線伺服器的複寫安裝提供的無訊息安裝屬性。請參閱複寫的 Horizon 連線伺服器執行個體的無訊息安裝屬性。

程序

1 從 VMware 下載網站下載連線伺服器安裝程式檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含連線伺服器。

安裝程式檔案名稱是 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是組建編號，而 *y.y.y* 是版本號碼。

2 在 Windows Server 電腦上開啟命令提示字元。

3 將安裝命令輸入成一行。

例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544"`
如果您安裝的複寫連線伺服器執行個體是 View 5.1 或更新版本，而且您要複寫的現有連線伺服器執行個體是 View 5.0.*x* 或更早版本，則必須指定資料復原密碼，而且您可以新增密碼提醒。例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

重要 當您執行無訊息安裝時，包括資料復原密碼在內的整個命令列都會記錄在安裝程式的 `vminst.log` 檔案中。安裝完成後，請使用 Horizon Administrator 刪除此記錄檔或變更資料復原密碼。

4 檢查 Windows Server 電腦的新修補程式，並且視需要執行 Windows Update。

即使您在安裝連線伺服器之前已完整修補 Windows Server 電腦，安裝仍可能初次啟用作業系統功能。現在可能需要其他修補程式。

Horizon 7 服務會安裝在 Windows Server 電腦上：

- VMware Horizon 連線伺服器
- VMware Horizon View Framework 元件
- VMware Horizon View 訊息匯流排元件
- VMware Horizon View 指令碼主機
- VMware Horizon View 安全閘道元件
- VMware Horizon View PCoIP 安全閘道

- VMware Horizon View Blast 安全閘道
- VMware Horizon View Web 元件
- VMware VCMSDS，提供 View LDAP 目錄服務

如需這些服務的相關資訊，請參閱《Horizon 7 管理》文件。

如果已在安裝期間選取**安裝 HTML Access** 設定，則 HTML Access 元件會安裝在 Windows Server 電腦上。此元件會在 Horizon 7 使用者入口網站頁面中設定 HTML Access 圖示，並在 Windows 防火牆中啟用 **VMware Horizon View 連線伺服器 (Blast-In)** 規則。此防火牆規則允許用戶端裝置上的網頁瀏覽器在 TCP 連接埠 8443 上連線至連線伺服器。

後續步驟

設定連線伺服器執行個體的 SSL 伺服器憑證。請參閱第 8 章 設定 Horizon 7 Server 的 TLS 憑證。

您不需要在連線伺服器的複寫執行個體上執行初始 Horizon 7 組態。複寫執行個體會從現有的連線伺服器執行個體繼承其組態。

不過，您可能需要設定此連線伺服器執行個體的用戶端連線設定，而且您可以調整 Windows Server 設定以支援大型部署。請參閱設定 Horizon Client 連線與 調整 Windows Server 設定以支援您的部署。

複寫的 Horizon 連線伺服器執行個體的無訊息安裝屬性

當您以無訊息方式，從命令列安裝複寫的 Horizon 連線伺服器執行個體時，您可以加入特定屬性。您必須使用 *PROPERTY*=*value* 格式，Microsoft Windows Installer (MSI) 才能解譯屬性和值。

表 7-2. 以無訊息方式安裝複寫的 Horizon 連線伺服器執行個體適用的 MSI 屬性

MSI 屬性	說明	預設值
INSTALLDIR	連線伺服器軟體安裝所在的路徑和資料夾。 例如：`INSTALLDIR=""D:\abc\my folder""` 括住路徑的兩組雙引號允許 MSI 安裝程式將空間轉譯為路徑的有效部分。 此 MSI 屬性為選用。	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	連線伺服器的安裝類型： ■ **1**.標準安裝 ■ **2**.複寫安裝 ■ **3**.安全伺服器安裝 若要安裝複寫的執行個體，請定義 `VDM_SERVER_INSTANCE_TYPE=2` 安裝複寫時，需要這個 MSI 屬性。	1
ADAM_PRIMARY_NAME	您要複寫的現有連線伺服器執行個體的主機名稱或 IP 位址。 例如：`ADAM_PRIMARY_NAME=cs1.companydomain.com` 需要此 MSI 屬性。	無
FWCHOICE	決定是否為連線伺服器執行個體設定防火牆的 MSI 屬性。 值為 1 時，設定防火牆。值為 2 時，不設定防火牆。 例如：`FWCHOICE=1` 此 MSI 屬性為選用。	1

表 7-2. 以無訊息方式安裝複寫的 Horizon 連線伺服器執行個體適用的 MSI 屬性 (續)

MSI 屬性	說明	預設值
VDM_SERVER_RECOVERY_PWD	資料復原密碼。如果在 View LDAP 中沒有設定資料復原密碼，則此屬性為強制的。 **備註** 如果您要複寫的標準連線伺服器執行個體是 View 5.0 或更早版本，則不會在 View LDAP 中設定資料復原密碼。如果您要複寫的連線伺服器執行個體是 View 5.1 或更新版本，則不需要提供此屬性。 密碼必須包含 1 至 128 個字元。請遵循組織的最佳做法，產生安全密碼。	無
VDM_SERVER_RECOVERY_PWD_REMINDER	資料復原密碼提醒。此屬性為選用。	無
VDM_IP_PROTOCOL_USAGE	指定 Horizon 7 元件用於通訊的 IP 版本。可能的值為 **IPv4** 和 **IPv6**	**IPv4**
VDM_FIPS_ENABLED	指定要啟用或停用 FIPS 模式。值為 1 則啟用 FIPS 模式。值為 0 則停用 FIPS 模式。若此屬性設為 1 且 Windows 不位於 FIPS 模式，則安裝程式將中止。	0

設定安全伺服器配對密碼

您必須先設定安全伺服器配對密碼，然後才能安裝安全伺服器。當您使用連線伺服器安裝程式安裝安全伺服器時，在安裝期間，該程式會提示您輸入密碼。

安全伺服器配對密碼是一個允許安全伺服器與連線伺服器執行個體配對的單次密碼。當您將密碼提供給連線伺服器安裝程式之後，該密碼即無效。

備註 您無法將舊版的安全伺服器與目前版本的連線伺服器進行配對。如果您在目前版本的連線伺服器上設定配對密碼，並嘗試安裝舊版安全伺服器，則配對密碼將會無效。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 伺服器**。

2 在 [連線伺服器] 索引標籤中，選取要與安全伺服器配對的連線伺服器執行個體。

3 從**更多命令**下拉式功能表中，選取**指定安全伺服器配對密碼**。

4 在「配對密碼」和「確認密碼」文字方塊中輸入密碼，並指定密碼逾時值。

   您必須在指定的逾時期間內使用密碼。

5 按一下**確定**以設定密碼。

後續步驟

安裝安全伺服器。請參閱 安裝安全伺服器。

重要 如果您在密碼逾時期間內未提供安全伺服器配對密碼給連線伺服器安裝程式，則密碼會變成無效，而必須設定新密碼。

安裝安全伺服器

安全伺服器是連線伺服器的執行個體，可為網際網路與您的內部網路之間增加一層額外的安全性。您可以安裝一或多個要連線至連線伺服器執行個體的安全伺服器。

安全伺服器軟體無法與其他任何 Horizon 7 軟體元件 (包括複寫伺服器、連線伺服器、View Composer、Horizon Agent 或 Horizon Client) 共存於相同的虛擬或實體機器上。

必要條件

- 決定要使用的拓撲類型。例如，決定要採用的負載平衡解決方案。決定與安全伺服器配對的連線伺服器執行個體是否供外部網路使用者專用。如需相關資訊，請參閱《Horizon 7 架構規劃》文件。

  重要 如果您使用負載平衡器，它必須具有不會變更的 IP 位址。在 IPv4 環境中，請設定靜態 IP 位址。在 IPv6 環境中，機器會自動取得不會變更的 IP 位址。

- 確認您的安裝滿足 Horizon 連線伺服器需求中所述的需求。
- 準備您的環境進行安裝。請參閱 Horizon 連線伺服器的安裝先決條件。
- 確認要與安全伺服器配對的連線伺服器執行個體已完成安裝和設定，並且執行與安全伺服器版本相容的連線伺服器版本。請參閱《Horizon 7 升級》文件中的〈Horizon 7 元件相容性對照表〉。
- 確認要與安全伺服器配對的連線伺服器執行個體能夠存取您要在其中安裝安全伺服器的電腦。

  備註 連線伺服器升級至 Horizon 7 (7.5 版) 後，停用 IPsec 的安全伺服器必須重新安裝。如果安全伺服器的 IP 位址發生變更，則必須重新安裝安全伺服器。如果安全伺服器位於動態 NAT 後方，則安全伺服器配對將無法正常運作。

- 設定安全伺服器配對密碼。請參閱設定安全伺服器配對密碼。
- 熟悉外部 URL 的格式。請參閱設定安全閘道和通道連線的外部 URL。
- 確認使用中設定檔中的「具有進階安全性的 Windows 防火牆」設為**開啟**。建議您將所有設定檔的這個設定設為**開啟**。根據預設，IPsec 規則控管安全伺服器與 View 連線伺服器之間的連線，而且必須啟用「具有進階安全性的 Windows 防火牆」。
- 熟悉必須在 Windows 防火牆上針對安全伺服器開放的網路連接埠。請參閱 Horizon 連線伺服器的防火牆規則。
- 如果您的網路拓撲中的安全伺服器與連線伺服器之間包含後端防火牆，則必須設定防火牆以支援 IPsec。請參閱設定後端防火牆支援 IPsec。
- 如果您要升級或重新安裝安全伺服器，請確認已移除安全伺服器的現有 IPsec 規則。請參閱移除安全伺服器的 IPsec 規則。
- 若您以 FIPS 模式安裝 Horizon 7，您必須在 Horizon Administrator 中取消選取全域設定**針對安全伺服器連線使用 IPSec**，因為在 FIPS 模式中，您必須在安裝安全伺服器之後手動設定 IPsec。

程序

1 從 VMware 下載網站下載連線伺服器安裝程式檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含連線伺服器。

安裝程式檔案名稱是 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是組建編號，而 *y.y.y* 是版本號碼。

2 若要啟動連線伺服器安裝程式，請按兩下安裝程式檔案。

3 接受 VMware 授權條款。

4 接受或變更目的地資料夾。

5 選取 **View 安全伺服器**安裝選項。

6 選取網際網路通訊協定 (IP) 版本、**IPv4** 或 **IPv6**。

您必須安裝具有相同 IP 版本的所有 Horizon 7 元件。

7 選取要啟用或停用 FIPS 模式。

只有在 Windows 中啟用 FIPS 模式時才可使用此選項。

8 在**伺服器**文字方塊中，輸入要與安全伺服器配對的連線伺服器執行個體的完整網域名稱或 IP 位址。

安全伺服器會將網路流量轉送至此連線伺服器執行個體。

9 在**密碼**文字方塊中，輸入安全伺服器配對密碼。

如果密碼已過期，您可以使用 Horizon Administrator 設定新密碼，並且在安裝程式中輸入新密碼。

10 在**外部 URL** 文字方塊中，輸入安全伺服器的外部 URL。無論用戶端使用何種顯示通訊協定，所有用戶端都需要此設定。

URL 必須包含通訊協定識別碼 (HTTPS)、用戶端可解析的安全伺服器名稱，以及連接埠號碼 (443)。

例如：`https://view.example.com:443`

您網路外部支援通道的用戶端，會使用 URL 透過安全伺服器連線到您網路內的機器。

11 在 **PCoIP 外部 URL** 文字方塊中，輸入安全伺服器的 PCoIP 閘道的外部 URL。使用 PCoIP 顯示通訊協定連線至遠端桌面平台的用戶端都需要此設定。

通訊協定相對 URL 必須包含安全伺服器 IP 位址和連接埠號碼 (4172)。在 IPv4 環境中，請使用 IPv4 位址。在 IPv6 環境中，請使用 IPv6 位址。

例如，在 IPv4 環境下，指定：`10.20.30.40:4172`

您網路外部支援 PCoIP 的用戶端，會使用 URL 透過安全伺服器連線到您網路內的機器。

備註 雖然在 IPv6 環境中必須於此處輸入 IPv6 位址，但在安裝後，即可將其取代為用戶端可解析的名稱。

12 在 **Blast 外部 URL** 文字方塊中，輸入安全伺服器的 Blast 閘道的外部 URL。使用 Blast 顯示通訊協定或 HTML Access 連線至遠端桌面平台的用戶端都需要此設定。

URL 必須包含通訊協定識別碼 (HTTPS)、用戶端可解析的安全伺服器名稱，以及連接埠號碼 (8443)。

例如：`https://myserver.example.com:8443`

您網路外部支援 Blast 的用戶端和 HTML Access 用戶端，會使用 URL 透過安全伺服器連線到您網路內的機器。

13 選擇如何設定 Windows 防火牆服務。

選項	動作
自動設定 Windows 防火牆	讓安裝程式設定 Windows 防火牆以允許必要的網路連線。
不設定 Windows 防火牆	手動設定 Windows 防火牆規則。 只有在組織使用自己預先定義的規則設定 Windows 防火牆時選取此選項。

14 完成安裝精靈，以完成安裝安全伺服器。

安全伺服器服務會安裝在 Windows Server 電腦上：

- VMware Horizon View 安全伺服器
- VMware Horizon View Framework 元件
- VMware Horizon View 安全閘道元件
- VMware Horizon View PCoIP 安全閘道
- VMware Blast 安全閘道

如需這些服務的相關資訊，請參閱《Horizon 7 管理》文件。

安全伺服器會出現在 Horizon Administrator 的 [安全伺服器] 窗格中。

已在安全伺服器上的 Windows 防火牆中啟用了 **VMware Horizon View 連線伺服器 (Blast-In)** 規則。此防火牆規則允許用戶端裝置上的網頁瀏覽器使用 HTML Access 透過 TCP 連接埠 8443 連線到安全伺服器。

備註 如果已取消或中止安裝，您可能需要先移除安全伺服器的 IPsec 規則，才能再次開始安裝。即使您已在重新安裝或升級安全伺服器之前移除 IPsec 規則，仍要執行這個步驟。如需移除 IPsec 規則的指示，請參閱移除安全伺服器的 IPsec 規則。

後續步驟

設定安全伺服器的 SSL 伺服器憑證。請參閱第 8 章 設定 Horizon 7 Server 的 TLS 憑證。

您可能需要設定安全伺服器的用戶端連線設定，而且您可以調整 Windows Server 設定以支援大型部署。請參閱設定 Horizon Client 連線與 調整 Windows Server 設定以支援您的部署。

如果您要重新安裝安全伺服器，而且您已將資料收集器集合工具設定為監控效能資料，請停止資料收集器集合工具，然後重新將其啟動。

以無訊息方式安裝安全伺服器

您可以使用 Microsoft Windows Installer (MSI) 的無訊息安裝功能，在數部 Windows 電腦上安裝安全伺服器。在無訊息安裝中，您會使用命令列，而且不必回應精靈的提示。

透過無訊息安裝，您便能有效地將 Horizon 7 元件部署在大型企業中。

必要條件

- 決定要使用的拓撲類型。例如，決定要採用的負載平衡解決方案。決定與安全伺服器配對的連線伺服器執行個體是否供外部網路使用者專用。如需相關資訊，請參閱《Horizon 7 架構規劃》文件。

  重要 如果您使用負載平衡器，它必須具有不會變更的 IP 位址。在 IPv4 環境中，請設定靜態 IP 位址。在 IPv6 環境中，機器會自動取得不會變更的 IP 位址。

- 確認您的安裝滿足 Horizon 連線伺服器需求中所述的需求。
- 準備您的環境進行安裝。請參閱 Horizon 連線伺服器的安裝先決條件。
- 確認要與安全伺服器配對的連線伺服器執行個體已完成安裝和設定，並且執行與安全伺服器版本相容的連線伺服器版本。請參閱《Horizon 7 升級》文件中的〈Horizon 7 元件相容性對照表〉。
- 確認要與安全伺服器配對的連線伺服器執行個體能夠存取您要在其中安裝安全伺服器的電腦。

  備註 連線伺服器升級至 Horizon 7 (7.5 版) 後，停用 IPsec 的安全伺服器必須重新安裝。如果安全伺服器的 IP 位址發生變更，則必須重新安裝安全伺服器。如果安全伺服器位於動態 NAT 後方，則安全伺服器配對將無法正常運作。

- 設定安全伺服器配對密碼。請參閱設定安全伺服器配對密碼。
- 熟悉外部 URL 的格式。請參閱設定安全閘道和通道連線的外部 URL。
- 確認使用中設定檔中的「具有進階安全性的 Windows 防火牆」設為**開啟**。建議您將所有設定檔的這個設定設為**開啟**。依預設，IPsec 規則會控管安全伺服器與連線伺服器之間的連線，且必須啟用 [具有進階安全性的 Windows 防火牆]。
- 熟悉必須在 Windows 防火牆上針對安全伺服器開放的網路連接埠。請參閱 Horizon 連線伺服器的防火牆規則。
- 如果您的網路拓撲中的安全伺服器與連線伺服器之間包含後端防火牆，則必須設定防火牆以支援 IPsec。請參閱設定後端防火牆支援 IPsec。
- 如果您要升級或重新安裝安全伺服器，請確認已移除安全伺服器的現有 IPsec 規則。請參閱移除安全伺服器的 IPsec 規則。
- 自行熟悉 MSI 安裝程式命令列選項。請參閱 Microsoft Windows Installer 命令列選項。
- 熟悉安全伺服器提供的無訊息安裝內容。請參閱安全伺服器的無訊息安裝內容。
- 若您以 FIPS 模式安裝 Horizon 7，您必須在 Horizon Administrator 中取消選取全域設定**針對安全伺服器連線使用 IPSec**，因為在 FIPS 模式中，您必須在安裝安全伺服器之後手動設定 IPsec。

程序

1 從 VMware 下載網站下載連線伺服器安裝程式檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含連線伺服器。

安裝程式檔案名稱是 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是組建編號，而 *y.y.y* 是版本號碼。

2 在 Windows Server 電腦上開啟命令提示字元。

3 將安裝命令輸入成一行。

例如：
```
VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3
VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://
view.companydomain.com:443 VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40
VDM_SERVER_SS_PCOIP_TCPPORT=4172 VDM_SERVER_SS_PCOIP_UDPPORT=4172
VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443 VDM_SERVER_SS_PWD=secret"
```

安全伺服器服務會安裝在 Windows Server 電腦上：

- VMware Horizon View 安全伺服器
- VMware Horizon View Framework 元件
- VMware Horizon View 安全閘道元件
- VMware Horizon View PCoIP 安全閘道
- VMware Blast 安全閘道

如需這些服務的相關資訊，請參閱《Horizon 7 管理》文件。

安全伺服器會出現在 Horizon Administrator 的 [安全伺服器] 窗格中。

已在安全伺服器上的 Windows 防火牆中啟用了 **VMware Horizon View 連線伺服器 (Blast-In)** 規則。此防火牆規則允許用戶端裝置上的網頁瀏覽器使用 HTML Access 透過 TCP 連接埠 8443 連線到安全伺服器。

備註 如果已取消或中止安裝，您可能需要先移除安全伺服器的 IPsec 規則，才能再次開始安裝。即使您已在重新安裝或升級安全伺服器之前移除 IPsec 規則，仍要執行這個步驟。如需移除 IPsec 規則的指示，請參閱移除安全伺服器的 IPsec 規則。

後續步驟

設定安全伺服器的 SSL 伺服器憑證。請參閱第 8 章 設定 Horizon 7 Server 的 TLS 憑證。

您可能需要設定安全伺服器的用戶端連線設定，而且您可以調整 Windows Server 設定以支援大型部署。請參閱設定 Horizon Client 連線與 調整 Windows Server 設定以支援您的部署。

安全伺服器的無訊息安裝內容

當您以無訊息方式，從命令列安裝安全伺服器時，可以加入特定的屬性。您必須使用 *PROPERTY=value* 格式，Microsoft Windows Installer (MSI) 才能解譯屬性和值。

表 7-3. 以無訊息方式安裝安全伺服器適用的 MSI 屬性

MSI 屬性	說明	預設值
INSTALLDIR	連線伺服器軟體安裝所在的路徑和資料夾。 例如：`INSTALLDIR=""D:\abc\my folder""` 括住路徑的兩組雙引號允許 MSI 安裝程式將空間轉譯為路徑的有效部分。 此 MSI 屬性為選用。	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	連線伺服器的安裝類型： ■ **1**.標準安裝 ■ **2**.複寫安裝 ■ **3**.安全伺服器安裝 若要安裝安全伺服器，請定義 `VDM_SERVER_INSTANCE_TYPE=3` 安裝安全伺服器時，需要這個 MSI 屬性。	1
VDM_SERVER_NAME	要與安全伺服器配對的現有連線伺服器執行個體的主機名稱或 IP 位址。 例如：`VDM_SERVER_NAME=cs1.internaldomain.com` 需要此 MSI 屬性。	無
VDM_SERVER_SS_EXTURL	安全伺服器的外部 URL。URL 必須包含通訊協定、可從外部解析的安全伺服器名稱以及連接埠號碼 例如：`VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443` 需要此 MSI 屬性。	無
VDM_SERVER_SS_PWD	安全伺服器配對密碼。 例如：`VDM_SERVER_SS_PWD=secret` 需要此 MSI 屬性。	無
FWCHOICE	決定是否為連線伺服器執行個體設定防火牆的 MSI 屬性。 值為 1 時，設定防火牆。值為 2 時，不設定防火牆。 例如：`FWCHOICE=1` 此 MSI 屬性為選用。	1
VDM_SERVER_SS_PCOIP_IPADDR	PCoIP 安全閘道外部 IP 位址。在 IPv6 環境中，此屬性還可以設為 PCoIP 安全閘道的 FQDN。只有在 Windows Server 2008 R2 或更新版本上有安裝安全伺服器時，才支援這個屬性。 例如：`VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40` 如果您打算使用 PCoIP 安全閘道元件，則需要這個屬性。	無
VDM_SERVER_SS_PCOIP_TCPPORT	PCoIP 安全閘道外部 TCP 連接埠號碼。只有在 Windows Server 2008 R2 或更新版本上有安裝安全伺服器時，才支援這個屬性。 例如：`VDM_SERVER_SS_PCOIP_TCPPORT=4172` 如果您打算使用 PCoIP 安全閘道元件，則需要這個屬性。	無
VDM_SERVER_SS_PCOIP_UDPPORT	PCoIP 安全閘道外部 UDP 連接埠號碼。只有在 Windows Server 2008 R2 或更新版本上有安裝安全伺服器時，才支援這個屬性。 例如：`VDM_SERVER_SS_PCOIP_UDPPORT=4172` 如果您打算使用 PCoIP 安全閘道元件，則需要這個屬性。	無

表 7-3. 以無訊息方式安裝安全伺服器適用的 MSI 屬性 (續)

MSI 屬性	說明	預設值
VDM_SERVER_SS_BSG_EXTURL	Blast 安全閘道外部 URL。URL 必須包含 HTTPS 通訊協定、可從外部解析的安全伺服器名稱以及連接埠號碼 例如：`VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443` 預設連接埠號碼是 8443。必須在安全伺服器上安裝 Blast 安全閘道，使用者才能建立 Horizon 7 桌面平台的網路連線。	無
VDM_SERVER_SS_FORCE_IPSEC	強制在安全伺服器與其配對的連線伺服器執行個體之間使用 IPsec。 依預設，在停用 IPsec 的情況下，自動安裝安全伺服器並將其與連線伺服器執行個體配對，可能會導致配對失敗。 預設值為 1 時，會強制 IPsec 配對。將此值設為 0 時，允許在沒有 IPsec 的情況下進行配對。	1
VDM_IP_PROTOCOL_USAGE	指定 Horizon 7 元件用於通訊的 IP 版本。可能的值為 **IPv4** 和 **IPv6**	**IPv4**
VDM_FIPS_ENABLED	指定要啟用或停用 FIPS 模式。值為 1 則啟用 FIPS 模式。值為 0 則停用 FIPS 模式。若此屬性設為 1 且 Windows 不位於 FIPS 模式，則安裝程式將中止。	0

移除安全伺服器的 IPsec 規則

您必須先移除目前對安全伺服器與其配對的連線伺服器執行個體之間的通訊進行控管的 IPsec 規則，才能升級或重新安裝安全伺服器執行個體。如果您未採取這個步驟，升級或重新安裝就會失敗。

依預設，安全伺服器與其配對的連線伺服器執行個體之間的通訊是由 IPsec 規則所控管。當您升級或重新安裝安全伺服器，並再次將其與連線伺服器執行個體配對時，必須建立一組新的 IPsec 規則。如果未在升級或重新安裝之前移除現有的 IPsec 規則，配對就會失敗。

當您升級或重新安裝安全伺服器，並使用 IPsec 保護安全伺服器與連線伺服器之間通訊的安全時，必須執行此步驟。

您可以在不使用 IPsec 規則的情況下，設定初始安全伺服器配對。在安裝安全伺服器之前，您可以開啟 Horizon Administrator，並取消選取全域設定**針對安全伺服器連線使用 IPSec** (此設定依預設為啟用)。如果 IPsec 規則未生效，則不需要移除就能進行升級或重新安裝。

備註 在升級或重新安裝安全伺服器之前，您不需要從 Horizon Administrator 移除安全伺服器。只有在您打算將安全伺服器從 Horizon 7 環境中永久移除時，才需要從 Horizon Administrator 移除安全伺服器。

使用 View 5.0.x 及較舊版本時，您可以從 Horizon Administrator 使用者介面中移除安全伺服器，或使用 `vdmadmin -S` 命令列命令來移除。在 View 5.1 和更新版本中，您必須使用 `vdmadmin -S`。請參閱《Horizon 7 管理》文件中的〈使用 -S 選項移除 Horizon 連線伺服器執行個體或安全伺服器的項目〉。

注意 如果您移除使用中安全伺服器的 IPsec 規則，與該安全伺服器的所有通訊都會遺失，直到您升級或重新安裝安全伺服器為止。因此，如果您使用負載平衡器來管理一組安全伺服器，請先在一部伺服器上執行此程序，接著升級該伺服器，之後再移除下一部伺服器的 IPsec 規則。您可以透過此方式，從生產環境逐一移除伺服器再將它們逐一新增回來，以避免對使用者造成停機時間。

程序

1 在 Horizon Administrator 中，按一下 **View 組態 > 伺服器**。

2 在**安全伺服器**索引標籤中，選取安全伺服器並按一下**更多命令 > 準備升級或重新安裝**。

如果您在安裝安全伺服器之前就已停用 IPsec 規則，則此設定為非使用中。在此情況下，您不需要移除 IPsec 規則，就能重新安裝或升級。

3 按一下**確定**。

IPsec 規則已移除且**準備升級或重新安裝**設定變成非使用中，表示您可以重新安裝或升級安全伺服器。

後續步驟

升級或重新安裝安全伺服器。

Unified Access Gateway 應用裝置相較於 VPN 的優點

Unified Access Gateway 應用裝置是用於從公司防火牆外部安全存取遠端桌面平台和應用程式的預設閘道。

如需最新版本的 Unified Access Gateway 說明文件，請參閱 https://docs.vmware.com/tw/Unified-Access-Gateway/index.html 中的《部署及設定 VMware Unified Access Gateway》文件。

Unified Access Gateway 應用裝置位於網路非軍事區 (DMZ) 內，可用作受信任網路內連線的 Proxy 主機，透過防護虛擬桌面平台、應用程式主機和伺服器不受面向公眾的網際網路所危害，以提供一層額外的安全性。

設定 Unified Access Gateway 應用裝置

Unified Access Gateway 與通用 VPN 解決方案很類似，因為它們都可確保僅在代表經過嚴格驗證的使用者時，才會將流量轉送至內部網路。

Unified Access Gateway 優於通用 VPN 的方面包括下列項目。

- Access Control Manager。Unified Access Gateway 會自動套用存取規則。Unified Access Gateway 會辨識使用者的權利和在內部連線所需的定址。VPN 也有相同的功效，因為大多數的 VPN 允許管理員分別針對每位使用者或使用者群組設定網路連線規則。剛開始，使用 VPN 可以順利運作，但需要投入大量的管理工作來維護必要規則。
- 使用者介面。Unified Access Gateway 不會變更簡潔的 Horizon Client 使用者介面。利用 Unified Access Gateway，當 Horizon Client 啟動時，經驗證的使用者會在其 View 環境中，並對其桌面平台和應用程式擁有受控制的存取權。根據 VPN 的要求，您必須先設定 VPN 軟體並分別進行驗證，然後才能啟動 Horizon Client。

- 效能。Unified Access Gateway 是專為將安全性和效能最大化而設計。有了 Unified Access Gateway，您不需要其他封裝就可以保護 PCoIP、HTML Access 及 WebSocket 通訊協定。VPN 會實作為 SSL VPN。此實作可滿足安全需求，而且在啟用傳輸層安全性 (Transport Layer Security, TLS) 的情況下，我們都會認為它們是安全的，不過使用 SSL/TLS 的基礎通訊協定只是以 TCP 為基礎。論及利用無連線 UDP 式傳輸的現代化視訊遠端通訊協定，當強制透過 TCP 型傳輸時，其效能優勢可能會大打折扣。這種說法不見得適用於所有 VPN 技術，因為能額外與 DTLS 或 IPsec (而非 SSL/TLS) 協同作業的技術也能與 Horizon 7 桌面平台通訊協定搭配運作。

使用 Unified Access Gateway 增強 Horizon 安全性

Unified Access Gateway 應用裝置利用將裝置憑證驗證分層放置在使用者驗證之上，讓您可以將存取限制為僅來自已知的良好裝置，並在虛擬桌面平台基礎結構上新增另一層的安全性，藉此增強安全性。

備註 僅在 Windows 版 Horizon Client 中支援此功能。

- 請參閱 https://docs.vmware.com/tw/Unified-Access-Gateway/index.html 之《部署及設定 VMware Unified Access Gateway》文件中的〈在 Unified Access Gateway 應用裝置上設定憑證或智慧卡驗證〉。
- 除了 Unified Access Gateway 上提供的其他使用者驗證服務之外，「端點符合性檢查」功能為存取 Horizon 桌面平台提供一層額外的安全性。請參閱《部署及設定 VMware Unified Access Gateway》文件中的〈Horizon 的端點符合性檢查〉，網址為 https://docs.vmware.com/tw/Unified-Access-Gateway/index.html。

重要 如果 Unified Access Gateway 應用裝置已設定使用雙因素驗證 (RSA SecureID 和 RADIUS) 並啟用 Windows 使用者名稱比對，且具有多個使用者網域，您應該啟用連線伺服器以傳送網域清單，讓使用者在使用 Windows 使用者名稱和密碼進行驗證時可以選取正確的網域。

雙躍點 DMZ

對於在網際網路與內部網路之間需要雙躍點 DMZ 的情況，您可以將外部 DMZ 中的 Unified Access Gateway 應用裝置部署為內部 DMZ 中 Unified Access Gateway 的 Web Reverse Proxy，以建立雙躍點 DMZ 組態。流量可透過每個 DMZ 層中的特定 Reverse Proxy 傳遞，但無法略過 DMZ 層。如需組態詳細資料，請參閱《部署及設定 VMware Unified Access Gateway》文件。

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 7-4. 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。
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。

設定後端防火牆支援 IPsec

如果您的網路拓撲中的安全伺服器與連線伺服器執行個體之間包含後端防火牆，則必須在防火牆上設定特定通訊協定和連接埠以支援 IPsec。未經過適當的組態，在安全伺服器與連線伺服器執行個體之間傳送的資料將無法通過防火牆。

依預設，IPsec 規則會控管安全伺服器與連線伺服器執行個體之間的連線。若要支援 IPsec，連線伺服器安裝程式可在 Horizon 7 Server 安裝所在的 Windows Server 主機上設定 Windows 防火牆規則。至於後端防火牆，您必須自行設定規則。

備註 強烈建議您使用 IPsec。或者，您可以停用 Horizon Administrator 全域設定**針對安全伺服器連線使用 IPsec**。

下列規則必須允許雙向流量。您可能需要在防火牆上指定不同的輸入和輸出流量規則。

不同的規則會分別套用到使用網路位址轉譯 (NAT) 和未使用 NAT 的防火牆。

表 7-5. 支援 IPsec 規則的非 NAT 防火牆需求

來源	通訊協定	連接埠	目的地	備註
安全伺服器	ISAKMP	UDP 500	Horizon 連線伺服器	安全伺服器會使用 UDP 連接埠 500 交涉 IPsec 安全性。
安全伺服器	ESP	N/A	Horizon 連線伺服器	ESP 通訊協定會封裝 IPsec 加密流量。 您不需要在規則中指定 ESP 的連接埠。如有必要，您可以指定來源及目的地 IP 位址，以縮小規則的範圍。

下列規則會套用至使用 NAT 的防火牆。

表 7-6. 支援 IPsec 規則的 NAT 防火牆需求

來源	通訊協定	連接埠	目的地	備註
安全伺服器	ISAKMP	UDP 500	Horizon 連線伺服器	安全伺服器會使用 UDP 連接埠 500 起始 IPsec 安全性交涉。
安全伺服器	NAT-T ISAKMP	UDP 4500	Horizon 連線伺服器	安全伺服器會使用 UDP 連接埠 4500 周遊 NAT 並交涉 IPsec 安全性。

使用備份組態重新安裝 Horizon 連線伺服器

在某些情況下，您可能必須重新安裝最新版的連線伺服器執行個體，並藉由匯入包含 View LDAP 組態資料的備份 LDIF 檔案來還原現有的 Horizon 7 組態。

例如，您可能需要備妥資料中心停止運作時實作的程序，做為業務持續及災難復原 (BC/DR) 計劃的一部份。此類計劃中的第一個步驟，就是確定已在其他位置備份 View LDAP 組態。第二個步驟是在新的位置安裝連線伺服器，並匯入備份組態，如此程序所說明。

當您使用現有的 Horizon 7 組態建立另一個資料中心時，也可以使用此程序。或者，如果您的 Horizon 7 部署僅包含單一連線伺服器執行個體，且該伺服器發生問題，您也可以使用此程序。

如果您在複寫的群組中有多個連線伺服器執行個體，且有單一執行個體關閉，則無須遵循此程序。您僅需重新安裝連線伺服器作為複寫的執行個體即可。在安裝期間，您需要提供連線資訊給另一個連線伺服器執行個體，而 Horizon 7 會從其他執行個體還原 View LDAP 組態。

必要條件

- 請確認已將 View LDAP 組態備份到加密的 LDIF 檔。
- 自行熟悉如何使用 `vdmimport` 命令，從 LDIF 備份檔案還原 View LDAP 組態。

  請參閱《Horizon 7 管理》文件中的〈備份與還原 Horizon 7 組態資料〉。
- 自行熟悉安裝新的連線伺服器執行個體的步驟。請參閱使用新組態安裝 Horizon 連線伺服器。

程序

1 使用新組態安裝連線伺服器。

2 將加密的 LDIF 檔案解密。

例如：

```
vdmimport –d –p mypassword
–f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

3 匯入解密的 LDIF 檔案來還原 View LDAP 組態。

例如：

```
vdmimport –f MyDecryptedexport.LDF
```

備註 在這個階段中，您仍無法存取 Horizon 7 組態。用戶端無法存取連線伺服器，也無法連線至其桌面平台。

4 使用 Windows **新增/移除程式**公用程式，從電腦解除安裝連線伺服器。

請勿解除安裝 View LDAP 組態，也就是 AD LDS Instance VMwareVDMDS 執行個體。您可以使用**新增/移除程式**公用程式，確認未從 Windows Server 電腦移除 AD LDS Instance VMwareVDMDS 執行個體。

5 解除安裝連線伺服器。

安裝程式提示時，接受現有的 View LDAP 目錄。

後續步驟

使用新的組態安裝連線伺服器執行個體之後，設定連線伺服器以及您的 Horizon 7 環境。

Microsoft Windows Installer 命令列選項

若要以無訊息方式安裝 Horizon 7 元件，必須使用 Microsoft Windows Installer (MSI) 命令列選項和內容。Horizon 7 元件安裝程式是 MSI 程式，並使用標準 MSI 功能。

如需關於 MSI 的詳細資訊，請參閱 Microsoft 網站。如需 MSI 命令列選項，請參閱 Microsoft Developer Network (MSDN) 程式庫網站並搜尋 MSI 命令列選項。若要顯示 MSI 命令列用法，您可以在 Horizon 7 元件電腦上開啟命令提示字元，並輸入 `msiexec /?`。

若要以無訊息方式執行 Horizon 7 元件安裝程式，一開始請先以無訊息方式執行啟動程序程式，此程式會將安裝程式解壓縮到暫存目錄，並啟動互動式安裝。

在命令列，您可輸入控制安裝程式 bookstrap 程式的命令列選項。

表 7-7. Horizon 7 元件啟動程序程式的命令列選項

選項	說明
/s	停用 bootstrap 啟用顯示畫面和解壓縮對話方塊，可避免顯示互動對話方塊。 例如：VMware-viewconnectionserver-*y.y.y-xxxxxx*.exe /s 必須使用 /s 選項，才可執行無訊息安裝。
/v"*MSI_command_line_options*"	指示安裝程式，傳遞在命令列中輸入為 MSI 選項組的雙引號中字串，進行解讀。您必須包含雙引號中的命令列項目。請在 /v 後和命令列結束時，放置雙引號。 例如：VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"*command_line_options*" 若要指示 MSI 安裝程式解譯包含空格的字串，請用兩組雙引號包住該字串。例如，您可能會想要在包含空格的安裝路徑名稱中安裝 Horizon 7 元件。 例如：VMware-viewconnectionserver-*y.y.y-xxxxxx*.exe /s /v"*command_line_options* INSTALLDIR=""d:\abc\my folder""" 在此範例中，MSI 安裝程式會略過安裝目錄路徑，不會嘗試將字串解譯為兩個命令列選項。請注意包住整個命令列的最後一個雙引號。 必須使用 /v"*command_line_options*" 選項，才可執行無訊息安裝。

您可以將命令列選項與 MSI 屬性值傳遞至 MSI 安裝程式，msiexec.exe，來控制無訊息安裝的其餘部分。MSI 安裝程式包含 Horizon 7 元件的安裝程式碼。安裝程式會使用您在命令列中輸入的值與選項來解譯 Horizon 7 元件專屬的安裝選擇與安裝選項。

表 7-8. MSI 命令列選項 MSI 屬性

MSI 選項或屬性	說明
/qn	指示 MSI 安裝程式，不要顯示安裝程式精靈頁。 例如，您可能想要無訊息安裝 Horizon Agent，並僅使用預設的安裝選項與功能： VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn" 或者，您可以使用 /qb 選項，在非互動式的自動安裝中顯示基本進度對話方塊。 必須使用 /qn 或 /qb 選項，才可執行無訊息安裝。 如需其他 /q 參數的相關資訊，請參閱 Microsoft 開發人員中心網站。
INSTALLDIR	指定 Horizon 7 元件的備用安裝路徑。 使用 *INSTALLDIR=path* 格式指定安裝路徑。如果您要將 Horizon 7 元件安裝在預設路徑中，則可以忽略此 MSI 屬性。 此 MSI 屬性為選用。

表 7-8. MSI 命令列選項 MSI 屬性 (續)

MSI 選項或屬性	說明
ADDLOCAL	決定要安裝的元件特定選項。 在互動式安裝中，Horizon 7 安裝程式會顯示您可以選取或取消選取的自訂安裝選項。在無訊息安裝中，您可以使用 ADDLOCAL 屬性在命令列上指定個別安裝選項來有選擇性地安裝這些選項。不會安裝您未明確指定的選項。 在互動式及無訊息安裝中，Horizon 7 安裝程式會自動安裝某些功能。您無法使用 ADDLOCAL 來控制是否安裝這些非選用功能。 輸入 ADDLOCAL=ALL 安裝可以在互動式安裝期間安裝的所有自訂安裝選項，包括預設安裝的選項以及您必須選取安裝的選項，NGVC 除外。NGVC 和 SVIAgent 互斥。 下列範例將安裝 Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG 以及客體作業系統支援的所有功能：`VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"` 如果您不使用 ADDLOCAL 屬性，將安裝預設安裝的自訂安裝選項以及自動安裝的功能。預設關閉 (未選取) 的自訂安裝選項不會加以安裝。 下列範例將安裝 Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG 以及客體作業系統支援而且預設開啟的自訂安裝選項：`VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn"` 若要指定個別安裝選項，請輸入以逗號分隔的安裝選項名稱清單。不要在名稱間使用空格。使用以下格式：ADDLOCAL=*value,value,value...*。 您使用 ADDLOCAL=*value,value,value...* 屬性時，必須包含 Core。 下列範例將安裝具有 Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG、Instant Clone Agent 和虛擬列印等功能的 Horizon Agent： `VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC,ThinPrint"` 以上範例不會安裝其他元件，即使是預設互動安裝的選項也不會加以安裝。 ADDLOCAL MSI 屬性為選用。
REBOOT	您可使用 REBOOT=ReallySuppress 選項，允許在系統重新開機前，完成系統設定工作。 此 MSI 屬性為選用。
/l*v *log_file*	使用詳細輸出，寫入記錄資訊到指定記錄檔案。 例如：`/l*v ""%TEMP%\vmmsi.log""` 此範例會產生類似互動式安裝時產生記錄的詳細記錄檔案。 您可使用此選項，記錄可能唯一套用到安裝的自訂功能。您可使用記錄的資訊，指定未來無訊息安裝時的安裝功能。 /l*v 選項為選用。

使用 MSI 命令列選項以無訊息方式解除安裝 Horizon 7 元件

您可以使用 Microsoft Windows Installer (MSI) 命令列選項解除安裝 Horizon 7 元件。

語法

```
msiexec.exe
/qb
/x
product_code
```

選項

/qb 選項會顯示解除安裝進度列。若要隱藏解除安裝進度列的顯示，請將 /qb 選項取代成 /qn 選項。

/x 選項會解除安裝 Horizon 7 元件。

product_code 字串會將 Horizon 7 元件產品檔案識別為 MSI Uninstaller。您可以在安裝期間建立的 %TEMP%\vmmsi.log 檔案中搜尋 ProductCode，以找出 *product_code* 字串。若要尋找適用於舊版 Horizon 7 元件的 *product_code* 字串，請參閱位於 http://kb.vmware.com/kb/2064845 的 VMware 知識庫 (KB) 文章。

如需 MSI 命令列選項的相關資訊，請參閱 Microsoft Windows Installer 命令列選項。

解除安裝 Horizon Agent 範例

若要解除安裝 32 位元 Horizon Agent 7.0.2 版，請輸入下命令：

```
msiexec.exe /qb /x {B23352D8-AD44-4379-A56E-0E337F9C4036}
```

若要解除安裝 64 位元 Horizon Agent 7.0.2 版，請輸入下命令：

```
msiexec.exe /qb /x {53D6EE37-6B10-4963-81B1-8E2972A1DA4D}
```

將詳細記錄新增至命令。

```
/l*v "%TEMP%\vmmsi_uninstall.log"
```

如果您不明確傳遞 /l 選項，預設的詳細記錄檔為 %TEMP%\MSI*nnnn*.log，其中 *nnnn* 為四個字元的 GUID。

Horizon Agent 解除安裝程序會保留一些登錄機碼。需要這些機碼才能保留連線伺服器組態資訊，讓遠端桌面平台即使在代理程式解除安裝再重新安裝的情況下，仍可與連線伺服器保持配對。移除這些登錄機碼會中斷該配對狀態。

下列登錄機碼會保留下來：

- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CRLs
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CTLs
- HKLM\SOFTWARE\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMwareView*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\vRealize Operations for Horizon*

- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM

設定 Horizon 7 Server 的 TLS 憑證

8

VMware 強烈建議您設定 TLS 憑證，以進行連線伺服器執行個體、安全伺服器及 View Composer 服務執行個體的驗證。

在您安裝連線伺服器執行個體、安全伺服器或 View Composer 執行個體時，系統會產生預設 TLS 伺服器憑證。您可以使用預設憑證進行測試。

用於連線伺服器之間和 Horizon Agent 與連線伺服器執行個體之間通訊的憑證，會使用自動機制取代，並且無法手動取代。如需詳細資料，請參閱《Horizon 7 安全性》文件。

重要 請盡快取代預設憑證。預設憑證未經憑證授權機構 (CA) 簽署。使用未經 CA 簽署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。

本章節討論下列主題：

瞭解 Horizon 7 Server 的 TLS 憑證

您必須遵循特定指導方針來設定 Horizon 7 Server 與相關元件的 TLS 憑證。

Horizon 連線伺服器和安全伺服器

與伺服器的用戶端連線需要使用 TLS。終止 TLS 連線的用戶端對向連線伺服器執行個體、安全伺服器以及中繼伺服器需要 TLS 伺服器憑證。

依預設，安裝連線伺服器或安全伺服器時，安裝會為伺服器產生自我簽署憑證。不過，在下列情況下，安裝會使用現有的憑證：

- 如果擁有 vdm 易記名稱的有效憑證已存在於 Windows 憑證存放區中
- 如果您從較舊的版本升級到 Horizon 7，且 Windows Server 電腦上已設定有效的金鑰儲存區檔案，則安裝會擷取金鑰和憑證，並將其匯入至 Windows 憑證存放區。

vCenter Server 與 View Composer

將 vCenter Server 與 View Composer 新增到生產環境中的 Horizon 7 之前，請確保 vCenter Server 與 View Composer 使用由 CA 簽署的憑證。

如需取代 vCenter Server 的預設憑證的相關資訊，請參閱 VMware Technical Papers 網站上的「取代 vCenter Server 憑證」，網址為：http://www.vmware.com/resources/techresources/。

如果您在相同的 Windows Server 主機上安裝 vCenter Server 和 View Composer，則它們可以使用相同的 TLS 憑證，但是您必須為每個元件個別設定憑證。

PCoIP 安全閘道

為符合產業或管轄區域安全法規，您可以將 PCoIP 安全閘道 (PSG) 服務產生的預設 TLS 憑證取代為 CA 簽署的憑證。強烈建議您設定 PSG 服務使用 CA 簽署的憑證，尤其是要求使用安全掃描程式才能通過符合性測試的部署。請參閱 設定 PCoIP 安全閘道使用新的 TLS 憑證。

Blast 安全閘道

依預設，Blast 安全閘道 (BSG) 會使用針對執行 BSG 的連線伺服器執行個體或安全伺服器而設定的 TLS 憑證。如果您使用 CA 簽署的憑證取代伺服器的預設自我簽署憑證，則 BSG 也會使用 CA 簽署的憑證。

SAML 2.0 驗證器

VMware Identity Manager 使用 SAML 2.0 驗證器提供整個安全網域的 Web 型驗證與授權。如果您希望 Horizon 7 將驗證委派給 VMware Identity Manager，可以設定 Horizon 7 接受來自 VMware Identity Manager 的 SAML 2.0 已驗證工作階段。若將 VMware Identity Manager 設定為支援 Horizon 7，則 VMware Identity Manager 使用者可以選取 Horizon 使用者入口網站上的桌面平台圖示，以連線至遠端桌面平台。

在 Horizon Administrator 中，您可以設定 SAML 2.0 驗證器與連線伺服器執行個體搭配使用。

在 Horizon Administrator 中新增 SAML 2.0 驗證器之前，請確認 SAML 2.0 驗證器使用由 CA 簽署的憑證。

其他指導方針

如需要求及使用由 CA 簽署的 TLS 憑證的一般資訊，請參閱 使用 CA 簽署的 TLS 憑證的優點。

用戶端端點連線至連線伺服器執行個體或安全伺服器時，會與伺服器的 TLS 伺服器憑證以及信任鏈結中的任何中繼憑證一起呈現。若要信任伺服器憑證，用戶端系統必須已經安裝簽署 CA 的根憑證。

當連線伺服器與 vCenter Server 和 View Composer 進行通訊時，連線伺服器會與 TLS 伺服器憑證以及這些伺服器中的中繼憑證一起呈現。若要信任 vCenter Server 與 View Composer Server，連線伺服器電腦必須已安裝簽署 CA 的根憑證。

同樣地，如果為連線伺服器設定了 SAML 2.0 驗證器，則連線伺服器電腦必須已為 SAML 2.0 伺服器憑證安裝簽署 CA 的根憑證。

設定 TLS 憑證的工作概觀

若要為 Horizon 7 Server 設定 TLS 伺服器憑證，您必須執行數項高階工作。

在複寫的連線伺服器執行個體的網繭中，您必須在網繭中的所有執行個體上執行這些工作。

執行這些工作的程序會在此概觀後續的各主題中描述。

1 判斷您是否需要向 CA 取得新簽署的 TLS 憑證。

  如果您的組織已有有效的 TLS 伺服器憑證，您可以使用該憑證取代隨連線伺服器、安全伺服器或 View Composer 提供的預設 TLS 伺服器憑證。若要使用現有的憑證，您還需要隨附的私密金鑰。

開始進行	動作
組織已提供有效的 TLS 伺服器憑證給您。	直接移至步驟 2。
您沒有 TLS 伺服器憑證。	向 CA 取得簽署的 TLS 伺服器憑證。

2 將 TLS 憑證匯入至 Horizon 7 Server 主機上的 Windows 本機電腦憑證存放區。

3 針對連線伺服器執行個體和安全伺服器，將憑證易記名稱修改為 **vdm**。

  將易記名稱 **vdm** 僅指派給每個 Horizon 7 Server 主機上的一個憑證。

4 在連線伺服器電腦上，如果 Windows Server 主機不信任根憑證，請將根憑證匯入至 Windows 本機電腦憑證存放區。

  此外，如果連線伺服器執行個體不信任為安全伺服器、View Composer 和 vCenter Server 主機設定的 TLS 伺服器憑證的根憑證，則您也必須匯入這些根憑證。您僅需要針對連線伺服器執行個體採取這些步驟。您不必將根憑證匯入至 View Composer、vCenter Server 或安全伺服器主機。

5 如果您的伺服器憑證是由中繼 CA 所簽署，請將中繼憑證匯入至 Windows 本機電腦憑證存放區。

  若要簡化用戶端組態，請將整個憑證鏈結匯入至 Windows 本機電腦憑證存放區。如果 Horizon 7 Server 中缺少中繼憑證，則必須為啟動 Horizon Administrator 的用戶端和電腦設定這些憑證。

6 針對 View Composer 執行個體，請採取下列其中一個步驟：

  - 如果您在安裝 View Composer 之前將憑證匯入至 Windows 本機電腦憑證存放區，就可以在安裝 View Composer 期間選取您的憑證。
  - 如果您要在安裝 View Composer 之後將現有憑證或預設的自我簽署憑證取代為新憑證，請執行 `SviConfig ReplaceCertificate` 公用程式，將新憑證繫結至 View Composer 所使用的連接埠。

7 如果您的 CA 並不知名，請設定用戶端信任根憑證和中繼憑證。

此外，請確定啟動 Horizon Administrator 的電腦信任根憑證和中繼憑證。

8 判斷是否要重新設定憑證撤銷檢查。

連線伺服器會在 Horizon 7 Server、View Composer 和 vCenter Server 上執行憑證撤銷檢查。CA 簽署的大部分憑證都包含憑證撤銷資訊。如果您的 CA 不包含這項資訊，您可以設定伺服器不要檢查憑證撤銷的狀況。

如果設定了 SAML 驗證器與連線伺服器執行個體搭配使用，則連線伺服器也會對 SAML 伺服器憑證執行憑證撤銷檢查。

從 CA 取得簽署的 TLS 憑證

如果組織未提供 TLS 伺服器憑證給您，則您必須要求 CA 簽署的新憑證。

您可以使用多種方法取得新簽署的憑證。例如，您可以使用 Microsoft `certreq` 公用程式產生憑證簽署要求 (CSR)，並將憑證要求提交至 CA。

請參閱《用於設定 Horizon 7 之 TLS 憑證的案例》文件中的範例，以瞭解如何使用 `certreq` 來完成這項工作。

基於測試目的，您可以向許多 CA 取得以未受信任的根憑證為基礎的免費暫時憑證。

重要 從 CA 取得簽署的 TLS 憑證時，您必須遵循特定規則和指導方針。

- 當您在電腦上產生憑證要求時，請確定也一併產生私密金鑰。當您取得 TLS 伺服器憑證並將其匯入至 Windows 本機電腦憑證存放區時，必須有與此憑證相對應的隨附私密金鑰。
- 若要符合 VMware 安全性建議，請使用用戶端裝置用於連線至主機的完整網域名稱 (FQDN)。請勿使用簡單伺服器名稱或 IP 位址，即使針對內部網域內的通訊。
- 不要使用僅與 Windows Server 2008 Enterprise CA 或更新版本相容的憑證範本來建立伺服器的憑證。
- 不要使用低於 1024 的 `KeyLength` 值，來產生伺服器的憑證。用戶端端點不會驗證在伺服器上以低於 1024 的 `KeyLength` 產生的憑證，而且用戶端將無法連線至伺服器。連線伺服器執行的憑證驗證也會失敗，導致受影響的伺服器在 Horizon Administrator 儀表板中顯示為紅色。

如需取得憑證的一般資訊，請參閱 MMC 的憑證嵌入式管理單元中提供的 Microsoft 線上說明。如果您的電腦尚未安裝憑證嵌入式管理單元，請參閱將憑證嵌入式管理單元新增到 MMC 中。

從 Windows 網域或企業 CA 取得簽署的憑證

若要從 Windows 網域或企業 CA 取得簽署的憑證，您可以使用 Windows 憑證存放區中的「Windows 憑證註冊」精靈。

如果電腦之間的通訊保持在您的內部網域內，則適合使用這種方法要求憑證。例如，伺服器對伺服器的通訊可能適合向 Windows 網域 CA 取得簽署的憑證。

如果您的用戶端從外部網路連線至 Horizon 7 Server，請要求由信任的第三方 CA 簽署的 TLS 伺服器憑證。

必要條件

- 決定用戶端裝置用於連線至主機的完整網域名稱 (FQDN)。

  若要符合 VMware 安全性建議，請使用 FQDN，而非簡單伺服器名稱或 IP 位址，即使是針對內部網域內的通訊。

- 確認憑證嵌入式管理單元已新增至 MMC。請參閱將憑證嵌入式管理單元新增到 MMC 中。
- 確認您擁有適當的認證，可要求能夠對電腦或服務核發的憑證。

程序

1. 在 Windows Server 主機的 **MMC** 視窗中，展開**憑證 (本機電腦)** 節點，並選取**個人**資料夾。
2. 從**動作**功能表前往**所有工作 > 要求新憑證**，以顯示**憑證註冊**精靈。
3. 選取憑證註冊原則。
4. 選取您想要求的憑證類型，然後選取**可匯出私密金鑰**選項，並按一下**註冊**。
5. 按一下**完成**。

新簽署的憑證會新增至 Windows 憑證存放區的**個人 > 憑證**資料夾中。

後續步驟

- 確認伺服器憑證和憑證鏈結都已匯入至 Windows 憑證存放區。
- 針對連線伺服器執行個體或安全伺服器，將憑證易記名稱修改為 **vdm**。請參閱修改憑證易記名稱。
- 針對 View Composer Server，將新憑證繫結至 View Composer 使用的連接埠。請參閱 將新的 TLS 憑證繫結至 View Composer 使用的連接埠 。

將 Horizon 連線伺服器、安全伺服器或 View Composer 設定為使用新的 TLS 憑證

若要將連線伺服器執行個體、安全伺服器或 View Composer 執行個體設定為使用 TLS 憑證，您必須將伺服器憑證和整個憑證鏈結匯入至連線伺服器、安全伺服器或 View Composer 主機上的 Windows 本機電腦憑證存放區。

在複寫的連線伺服器執行個體的網繭中，您必須在網繭中的所有執行個體上匯入伺服器憑證和憑證鏈結。

依預設，Blast 安全閘道 (BSG) 會使用針對執行 BSG 的連線伺服器執行個體或安全伺服器而設定的 TLS 憑證。如果您將 View Server 的預設自我簽署憑證取代為 CA 簽署的憑證，則 BSG 也會隨之使用 CA 簽署的憑證。

重要 若要將連線伺服器或安全伺服器設定為使用某憑證，您必須將憑證易記名稱變更為 **vdm**。此外，憑證必須具有隨附的私密金鑰。

如果您要在安裝 View Composer 之後將現有憑證或預設的自我簽署憑證取代為新憑證，則必須執行 `SviConfig ReplaceCertificate` 公用程式，將新憑證繫結至 View Composer 所使用的連接埠。

程序

1 將憑證嵌入式管理單元新增到 MMC 中

您必須將憑證嵌入式管理單元新增至 Horizon 7 Server 安裝所在之 Windows Server 主機上的 Microsoft Management Console (MMC)，才能將憑證新增至 Windows 憑證存放區。

2 將簽署的伺服器憑證匯入 Windows 憑證存放區

您必須將 TLS 伺服器憑證匯入至連線伺服器執行個體或安全伺服器服務安裝所在 Windows Server 主機上的 Windows 本機電腦憑證存放區中。

3 修改憑證易記名稱

若要設定連線伺服器執行個體或安全伺服器，使其可辨識並使用 TLS 憑證，您必須將憑證易記名稱修改為 `vdm`。

4 將根憑證和中繼憑證匯入 Windows 憑證存放區

如果連線伺服器安裝所在的 Windows Server 主機不信任簽署的 TLS 伺服器憑證的根憑證，則您必須將根憑證匯入至 Windows 本機電腦憑證存放區。此外，如果連線伺服器主機不信任為安全伺服器、View Composer 和 vCenter Server 主機設定的 TLS 伺服器憑證的根憑證，則您也必須匯入這些根憑證。

5 將新的 TLS 憑證繫結至 View Composer 使用的連接埠

如果您在安裝 View Composer 之後設定新的 TLS 憑證，則必須執行 `SviConfig ReplaceCertificate` 公用程式以取代繫結至 View Composer 使用之連接埠的憑證。此公用程式會解除現有憑證的繫結，並將新憑證繫結至連接埠。

將憑證嵌入式管理單元新增到 MMC 中

您必須將憑證嵌入式管理單元新增至 Horizon 7 Server 安裝所在之 Windows Server 主機上的 Microsoft Management Console (MMC)，才能將憑證新增至 Windows 憑證存放區。

必要條件

請確認在 Horizon 7 Server 安裝所在的 Windows Server 電腦上可以使用 MMC 和憑證嵌入式管理單元。

程序

1 在 Windows Server 電腦上，按一下**開始**，然後輸入 **mmc.exe**。

2 在 **MMC** 視窗中，移至**檔案 > 新增/移除嵌入式管理單元**。

3 在**新增或移除嵌入式管理單元**視窗中，選取**憑證**，然後按一下**新增**。

4 在**憑證嵌入式管理單元**視窗中，選取**電腦帳戶**，按**下一步**，選取**本機電腦**，然後按一下**完成**。

5 在**新增或移除嵌入式管理單元**視窗中，按一下**確定**。

後續步驟

將 TLS 伺服器憑證匯入到 Windows 憑證存放區中。

將簽署的伺服器憑證匯入 Windows 憑證存放區

您必須將 TLS 伺服器憑證匯入至連線伺服器執行個體或安全伺服器服務安裝所在 Windows Server 主機上的 Windows 本機電腦憑證存放區中。

您也可以在安裝有 View Composer 服務的 Windows Server 主機上執行此工作。

根據您的憑證檔案格式而定，包含在 keystore 檔案中的整個憑證鏈結可能會匯入至 Windows 本機電腦憑證存放區。例如，可能會匯入伺服器憑證、中繼憑證和根憑證。

對於其他類型的憑證檔案，只會將伺服器憑證匯入至 Windows 本機電腦憑證存放區。在此情況下，您必須採取額外的步驟，以匯入憑證鏈結中的根憑證和任何中繼憑證。

如需憑證的詳細資訊，請參閱 MMC 的憑證嵌入式管理單元中提供的 Microsoft 線上說明。

備註 如果您將 TLS 連線卸載至中繼伺服器，則必須將相同的 TLS 伺服器憑證同時匯入至中繼伺服器和卸載的 Horizon 7 Server。如需詳細資料，請參閱《Horizon 7 管理》文件中的〈將 TLS 連線卸載至中繼伺服器〉。

必要條件

確認憑證嵌入式管理單元已新增至 MMC。請參閱將憑證嵌入式管理單元新增到 MMC 中。

程序

1 在 Windows Server 主機的 MMC 視窗中，展開**憑證 (本機電腦)** 節點，並選取**個人**資料夾。

2 在 [動作] 窗格中，移至**更多動作 > 所有工作 > 匯入**。

3 在**憑證匯入**精靈中，按**下一步**並瀏覽至儲存憑證所在的位置。

4 選取憑證檔案，然後按一下**開啟**。

若要顯示憑證檔案類型，可以從**檔案名稱**下拉式功能表選取其檔案格式。

5 為包含在憑證檔案中的私密金鑰輸入密碼。

6 選取**將這個金鑰設成可匯出**。

7 選取**包含所有延伸內容**。

8 按**下一步**，然後再按一下**完成**。

新憑證會出現在**憑證 (本機電腦) > 個人 > 憑證**資料夾中。

9 確認新憑證包含私密金鑰。

a 在**憑證 (本機電腦) > 個人 > 憑證**資料夾中，按兩下新憑證。

b 在 [憑證資訊] 對話方塊的 [一般] 索引標籤中，確認顯示下列描述：這個憑證有一個對應的私密金鑰。

後續步驟

將憑證易記名稱修改為 **vdm**。

修改憑證易記名稱

若要設定連線伺服器執行個體或安全伺服器，使其可辨識並使用 TLS 憑證，您必須將憑證易記名稱修改為 vdm。

您不需要修改 View Composer 所使用的 TLS 憑證的易記名稱。

必要條件

確認伺服器憑證已匯入 Windows 憑證存放區的**憑證 (本機電腦) > 個人 > 憑證**資料夾中。請參閱將簽署的伺服器憑證匯入 Windows 憑證存放區。

程序

1 在 Windows Server 主機的 MMC 視窗中，展開**憑證 (本機電腦)** 節點，並選取**個人 > 憑證**資料夾。

2 以滑鼠右鍵按一下核發給 Horizon 7 Server 主機的憑證，然後按一下**內容**。

3 在「一般」索引標籤上，刪除**易記名稱**文字並輸入 **vdm**。

4 按一下**套用**，然後再按一下**確定**。

5 確認在**個人 > 憑證**資料夾中沒有其他伺服器憑證的易記名稱為 **vdm**。

a 找到任何其他伺服器憑證，在憑證上按一下滑鼠右鍵，然後按一下**內容**。

b 如果該憑證具有易記名稱 **vdm**，則將其刪除，按一下**套用**，然後按一下**確定**。

後續步驟

將根憑證和中繼憑證匯入至 Windows 本機電腦憑證存放區。

匯入鏈結中的所有憑證後，您必須重新啟動連線伺服器服務或安全伺服器服務，才能讓變更生效。

將根憑證和中繼憑證匯入 Windows 憑證存放區

如果連線伺服器安裝所在的 Windows Server 主機不信任簽署的 TLS 伺服器憑證的根憑證，則您必須將根憑證匯入至 Windows 本機電腦憑證存放區。此外，如果連線伺服器主機不信任為安全伺服器、View Composer 和 vCenter Server 主機設定的 TLS 伺服器憑證的根憑證，則您也必須匯入這些根憑證。

如果連線伺服器、安全伺服器、View Composer 和 vCenter Server 憑證是由連線伺服器主機已知且信任的根 CA 所簽署，且您的憑證鏈結中沒有中繼憑證，則可略過此工作。主機可能會信任常用的憑證授權機構。

您必須匯入網繭中所有複寫的連線伺服器執行個體上不受信任的根憑證。

備註 您不必將根憑證匯入至 View Composer、vCenter Server 或安全伺服器主機。

如果伺服器憑證是由中繼 CA 所簽署，則您也必須匯入憑證鏈結中的每個中繼憑證。為簡化用戶端組態，請將整個中繼鏈結匯入至安全伺服器、View Composer 和 vCenter Server 主機以及連線伺服器主機。如果連線伺服器或安全伺服器主機中缺少中繼憑證，則必須為啟動 Horizon Administrator 的用戶端和電腦設定這些憑證。如果 View Composer 或 vCenter Server 主機中缺少中繼憑證，則必須為每個連線伺服器執行個體設定這些憑證。

如果您確認整個憑證鏈結已匯入至 Windows 本機電腦憑證存放區，則可略過此工作。

備註 如果已設定供連線伺服器執行個體使用的 SAML 驗證器，則 SAML 2.0 驗證器適用相同的準則。如果連線伺服器主機不信任為 SAML 驗證器設定的根憑證，或 SAML 伺服器憑證是由中繼 CA 所簽署，則您必須確定憑證鏈結已匯入至 Windows 本機電腦憑證存放區。

程序

1. 在 Windows Server 主機的 MMC 主控台中，展開**憑證 (本機電腦)** 節點，然後移至**受信任的根憑證授權單位 > 憑證**資料夾。
   - 如果您的根憑證位於此資料夾中，而且憑證鏈結中沒有任何中繼憑證，請跳至步驟 7。
   - 如果您的根憑證不在此資料夾中，請繼續進行步驟 2。
2. 以滑鼠右鍵按一下**信任的根憑證授權機構 > 憑證**資料夾，然後按一下**所有工作 > 匯入**。
3. 在**憑證匯入**精靈中，按**下一步**並瀏覽至儲存根 CA 憑證所在的位置。
4. 選取根 CA 憑證檔案，然後按一下**開啟**。
5. 依序按**下一步**、**下一步**，然後按一下**完成**。
6. 如果您的伺服器憑證是由中繼 CA 所簽署，請將憑證鏈結中的所有中繼憑證匯入至 Windows 本機電腦憑證存放區。
   a 移至**憑證 (本機電腦) > 中繼憑證授權機構 > 憑證**資料夾。
   b 針對必須匯入的每個中繼憑證重複步驟 3 到 6。
7. 重新啟動連線伺服器服務、安全伺服器服務、View Composer 服務或 vCenter Server 服務以便讓變更生效。

將新的 TLS 憑證繫結至 View Composer 使用的連接埠

如果您在安裝 View Composer 之後設定新的 TLS 憑證，則必須執行 `SviConfig ReplaceCertificate` 公用程式以取代繫結至 View Composer 使用之連接埠的憑證。此公用程式會解除現有憑證的繫結，並將新憑證繫結至連接埠。

如果您在安裝 View Composer 之前，先將新憑證安裝在 Windows Server 電腦上，則無需執行 `SviConfig ReplaceCertificate` 公用程式。當您執行 View Composer 安裝程式時，可以選取 CA 簽署的憑證，而非預設的自我簽署憑證。在安裝期間，選取的憑證會繫結至 View Composer 所使用的連接埠。

如果希望以新憑證取代現有憑證或預設的自我簽署憑證，則必須使用 SviConfig ReplaceCertificate 公用程式。

必要條件

確認新憑證已匯入安裝 View Composer 之 Windows Server 電腦上的 Windows 本機電腦憑證存放區。

程序

1 停止 View Composer 服務。

2 在安裝 View Composer 的 Windows Server 主機上開啟命令提示字元。

3 導覽至 SviConfig 可執行檔。

該檔案與 View Composer 應用程式位於同一個位置。預設路徑為 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe。

4 輸入 SviConfig ReplaceCertificate 命令。

例如：

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

其中，–delete 是一個必要參數，會在要取代的憑證上運作。您必須指定 –delete=true 以便從 Windows 本機電腦憑證存放區刪除舊憑證，或指定 –delete=false 以保留 Windows 憑證存放區中的舊憑證。

此公用程式會顯示 Windows 本機電腦憑證存放區中可用之 TLS 憑證的編號清單。

5 若要選取憑證，請輸入憑證號碼，然後按下 Enter。

6 重新啟動 View Composer 服務讓變更生效。

範例： SviConfig ReplaceCertificate

下列範例會取代繫結至 View Composer 連接埠的憑證：

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

設定用戶端端點信任根憑證和中繼憑證

如果 Horizon 7 Server 憑證是由用戶端電腦和存取 Horizon Administrator 的用戶端電腦不信任的 CA 所簽署，您可以設定網域中的所有 Windows 用戶端系統信任根憑證和中繼憑證。若要這麼做，您必須將根憑證的公開金鑰新增到 Active Directory 中受信任的根憑證授權機構群組原則，並將根憑證新增到 Enterprise NTAuth 存放區。

例如，如果您的組織使用內部憑證服務，可能必須採取這些步驟。

如果 Windows 網域控制站當做根 CA，或者如果您的憑證是由知名 CA 所簽署，則無需採取這些步驟。對於知名的 CA，作業系統廠商會將根憑證預先安裝在用戶端系統上。

如果您的伺服器憑證是由不知名的中繼 CA 所簽署，則必須將中繼憑證新增到 Active Directory 中的中繼憑證授權機構群組原則。

對於使用 Windows 以外作業系統的用戶端裝置，請參閱有關散發使用者可安裝之根憑證和中繼憑證的下列指示：

- 對於 Mac 版 Horizon Client，請參閱設定 Mac 版 Horizon Client 信任根憑證與中繼憑證。
- 對於 iOS 版 Horizon Client，請參閱設定 iOS 版 Horizon Client 信任根憑證和中繼憑證。
- 對於 Android 版 Horizon Client，請參閱 Google 網站上的說明文件，例如《Android 3.0 使用者指南》
- 對於 Linux 版 Horizon Client，請參閱 Ubuntu 說明文件。

必要條件

確認伺服器憑證是以 1024 或更大的 `KeyLength` 值所產生。用戶端端點不會驗證伺服器上以低於 1024 的 `KeyLength` 產生的憑證，而且用戶端將無法連線至伺服器。

程序

1 在 Active Directory 伺服器上，使用 `certutil` 命令將憑證發佈到 Enterprise NTAuth 存放區。

例如：**`certutil –dspublish –f`** ***`path_to_root_CA_cert`*** **`NTAuthCA`**

2 在 Active Directory 伺服器上，瀏覽至群組原則管理外掛程式。

AD 版本	瀏覽路徑
Windows 2003	a 選取**開始 > 所有程式 > 系統管理工具 > Active Directory 使用者和電腦**。 b 在您的網域上按一下滑鼠右鍵，然後按一下 **內容**。 c 在 **群組原則** 標籤上，按一下 **開啟** 以開啟群組原則管理外掛程式。 d 在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。
Windows 2008	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。
Windows 2012 R2	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在**預設網域原則**上按一下滑鼠右鍵，然後按一下**編輯**。
Windows 2016	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，在 **預設網域原則** 上按一下滑鼠右鍵，然後按一下 **編輯**。

3 展開**電腦組態**區段，並移至 **Windows 設定 > 安全性設定 > 公開金鑰原則**。

4 匯入憑證。

選項	說明
根憑證	a 以滑鼠右鍵按一下**受信任的根憑證授權機構**，然後選取**匯入**。 b 依照精靈中的提示，匯入根憑證 (例如，`rootCA.cer`)，然後按一下**確定**。
中繼憑證	a 以滑鼠右鍵按一下**中繼憑證授權機構**，然後選取**匯入**。 b 依照精靈中的提示，匯入中繼憑證 (例如，`intermediateCA.cer`)，然後按一下**確定**。

5 關閉**群組原則**視窗。

現在，網域內所有系統的受信任根憑證存放區和中繼憑證存放區中皆已包含憑證資訊，可讓它們信任根憑證和中繼憑證。

設定 Mac 版 Horizon Client 信任根憑證與中繼憑證

如果伺服器憑證是由執行 Mac 版 Horizon Client 的電腦不信任的 CA 所簽署，您可以將這些電腦設定為信任根憑證和中繼憑證。您必須在用戶端電腦的信任鏈結中散發根憑證和所有中繼憑證。

程序

1 將根憑證與中繼憑證傳遞至執行 Mac 版 Horizon Client 的電腦。

2 在 Mac 電腦上開啟根憑證。

憑證會顯示下列訊息：您要讓您的電腦從現在起信任由「*CA name*」簽署的憑證嗎?

3 按一下**永遠信任**

4 輸入使用者密碼。

5 在信任鏈結中，針對所有中繼憑證重複步驟 2 至 4。

設定 iOS 版 Horizon Client 信任根憑證和中繼憑證

如果伺服器憑證是由不受執行 iOS 版 Horizon Client 之 iPad 和 iPhone 信任的 CA 所簽署，您可以將裝置設定為信任根憑證和中繼憑證。您必須將信任鏈結中的根憑證和所有中繼憑證散佈到裝置。

程序

1 將根憑證和中繼憑證當做電子郵件附件傳送到 iPad。

2 開啟電子郵件附件中的根憑證，並選取**安裝**。

憑證會顯示下列訊息：

> 無法確認的設定檔。無法確認 *Certificate name* 的真確性。安裝此設定檔將會變更您 iPad 上的設定。根憑證。安裝憑證 *Certificate name* 會將它新增到您 iPad 上的信任憑證清單。

3 請再次選取**安裝**。

4 在信任鏈結中，針對所有中繼憑證重複步驟 2 和 3。

針對伺服器憑證設定憑證撤銷檢查

每個連線伺服器執行個體都會對本身的憑證，以及與其配對之安全伺服器的憑證，執行憑證撤銷檢查。每一個執行個體也會在建立連線時，檢查 vCenter 和 View Composer Server 的憑證。根據預設，鏈結中的所有憑證都會加以檢查，但不包括根憑證。不過，您可以變更此預設值。

如果設定了 SAML 2.0 驗證器供連線伺服器執行個體使用，則連線伺服器同樣會對 SAML 2.0 伺服器憑證執行憑證撤銷檢查。

Horizon 7 支援各種不同的憑證撤銷檢查方法，例如憑證撤銷清單 (CRL) 與線上憑證狀態通訊協定 (OCSP)。CRL 是核發憑證的 CA 所發佈的撤銷憑證清單。OCSP 是用來取得 X.509 憑證的撤銷狀態的憑證驗證通訊協定。

使用 CRL 時，會從憑證中經常指定的憑證發佈點 (DP) 下載已撤銷憑證的清單。伺服器會定期連線到憑證中指定的 CRL DP URL，下載清單，然後進行查看以判斷是否已撤銷伺服器憑證。使用 OCSP 時，伺服器會將要求傳送至 OCSP 回應者，以判斷憑證的撤銷狀態。

若您從協力廠商憑證授權機構 (CA) 取得伺服器憑證，該憑證會包含一種或多種可判斷其撤銷狀態的方法，例如 CRL DP URL 或 OCSP 回應者的 URL。如果您有自己的 CA 並且產生憑證，但是憑證中不包含撤銷資訊，則憑證撤銷檢查會失敗。這類憑證的撤銷資訊範例可能包括像是裝載 CRL 所在伺服器上 Web 型 CRL DP 的 URL。

如果您有自己的 CA，但是並未或無法在憑證中包含憑證撤銷資訊，您可以選擇不要檢查憑證的撤銷情形，或是只檢查鏈結中的特定憑證。在伺服器上，您可以使用 Windows 登錄編輯程式建立字串 (REG_SZ) 值 **CertificateRevocationCheckType** (位於 `HKLM\Software\VMware, Inc.\VMware VDM\Security` 下)，然後將此值設為下列其中一個資料值。

值	說明
1	不要執行憑證撤銷檢查。
2	僅檢查伺服器憑證。不要檢查鏈結中的其他任何憑證。
3	檢查鏈結中的所有憑證。
4	(預設) 檢查根憑證以外的所有憑證。

如果未設定此登錄值，或是設定的值無效 (也就是值不是 1、2、3 或 4)，則會檢查根憑證以外的所有憑證。請在您要修改撤銷檢查的每部伺服器上設定此登錄值。設定此值之後，不需要重新啟動系統。

備註 如果組織的網際網路存取使用 Proxy 設定，您可能需要將連線伺服器電腦設定為使用 Proxy 設定，以確保可對用於安全用戶端連線的安全伺服器或連線伺服器執行個體執行憑證撤銷檢查。如果連線伺服器執行個體無法存取網際網路，憑證撤銷檢查可能會失敗，且連線伺服器執行個體或配對的安全伺服器可能會在 Horizon Administrator 儀表板上顯示為紅色。若要解決此問題，請參閱《Horizon 7 管理》文件中的〈疑難排解安全伺服器憑證撤銷檢查〉。

設定 PCoIP 安全閘道使用新的 TLS 憑證

為符合產業或管轄區域安全法規，您可以將 PCoIP 安全閘道 (PSG) 服務產生的預設 TLS 憑證取代為 CA 簽署的憑證。

在 Horizon 7 中，PSG 服務在啟動時，會建立預設的自我簽署 TLS 憑證。PSG 服務會將自我簽署憑證出示給執行 Horizon Client 2.0 (或 Horizon Client 5.2 for Windows) 或更新版本且連線至 PSG 的用戶端。

PSG 也提供預設舊版 TLS 憑證，並將其出示給執行舊版用戶端或更早版本且連線至 PSG 的用戶端。

預設憑證可提供從用戶端端點到 PSG 的安全連線，且不需要在 Horizon Administrator 中執行進一步組態。但是，強烈建議您設定 PSG 服務使用 CA 簽署的憑證，尤其是要求使用安全掃描程式才能通過符合性測試的部署。

雖然並非必要，但是您非常可能會為您的伺服器設定新的 CA 簽署的 TLS 憑證，然後再以 CA 簽署的憑證取代預設 PSG 憑證。下列程序假設您已將 CA 簽署憑證匯入 Windows 憑證存放區，供執行 PSG 的伺服器使用。

備註 如果您要使用安全掃描程式進行符合性測試，您可能需要先設定 PSG 使用與伺服器相同的憑證，然後掃描 View 連接埠，再掃描 PSG 連接埠。您可以在掃描 View 連接埠期間，解決信任或驗證問題，以確保這些問題不會導致 PSG 連接埠和憑證測試無效。接著您可以為 PSG 設定唯一憑證，然後再執行一次掃描。

程序

1 確認伺服器名稱與 PSG 憑證主體名稱相符

安裝連線伺服器執行個體或安全伺服器時，安裝程式會建立一個包含電腦 FQDN 值的登錄設定。您必須確認此值與安全掃描程式用於連線至 PSG 連接埠的 URL 的伺服器名稱部分相符。伺服器名稱也必須與您要用於 PSG 的 TLS 憑證的主體名稱或主體替代名稱 (SAN) 相符。

2 在 Windows 憑證存放區中設定 PSG 憑證

若要以 CA 簽署的憑證取代預設 PSG 憑證，您必須在執行 PSG 的連線伺服器或安全伺服器電腦上，於 Windows 本機電腦憑證存放區中設定憑證及其私密金鑰。

3 在 Windows 登錄中設定 PSG 憑證易記名稱

PSG 依伺服器名稱和憑證易記名稱識別要使用的 TLS 憑證。您必須在執行 PSG 的連線伺服器或安全伺服器電腦的 Windows 登錄中設定易記名稱值。

4 (選擇性) 強制使用 CA 簽署的憑證連線至 PSG

您可以確保用戶端與 PSG 間的所有連線，都使用 PSG 的 CA 簽署憑證，而不是使用預設舊版憑證。為 PSG 設定 CA 簽署的憑證時，不需要此程序。只有在強制使用 CA 簽署憑證適用於您的 Horizon 7 部署時，才採用這些步驟。

確認伺服器名稱與 PSG 憑證主體名稱相符

安裝連線伺服器執行個體或安全伺服器時，安裝程式會建立一個包含電腦 FQDN 值的登錄設定。您必須確認此值與安全掃描程式用於連線至 PSG 連接埠的 URL 的伺服器名稱部分相符。伺服器名稱也必須與您要用於 PSG 的 TLS 憑證的主體名稱或主體替代名稱 (SAN) 相符。

例如，如果掃描程式連線至 URL 為 `https://view.customer.com:4172` 的 PSG，則登錄設定必須包含值 `view.customer.com`。請注意，安裝期間設定的連線伺服器或安全伺服器電腦的 FQDN，可能會與此外部伺服器名稱不同。

程序

1 在執行 PCoIP 安全閘道的連線伺服器或安全伺服器主機上，啟動 Windows 登錄編輯程式。

2 導覽至 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway\SSLCertPsgSni` 登錄設定。

3 確認 SSLCertPsgSni 設定的值與掃描程式將用於連線至 PSG 的 URL 的伺服器名稱相符，也與您要為 PSG 安裝的 TLS 憑證的主體名稱或主體替代名稱相符。

如果值不相符，請換成正確的值。

4 重新啟動 VMware Horizon View PCoIP 安全閘道服務，讓您的變更生效。

後續步驟

將 CA 簽署的憑證匯入 Windows 本機電腦憑證存放區，並設定憑證易記名稱。

在 Windows 憑證存放區中設定 PSG 憑證

若要以 CA 簽署的憑證取代預設 PSG 憑證，您必須在執行 PSG 的連線伺服器或安全伺服器電腦上，於 Windows 本機電腦憑證存放區中設定憑證及其私密金鑰。

如果您想要讓 PSG 使用唯一憑證，您必須使用可匯出的私密金鑰，將憑證匯入 Windows 本機電腦憑證存放區，然後設定適當的易記名稱。

如果您想要讓 PSG 使用與伺服器相同的憑證，則不需要依照此程序進行。但是，在 Windows 登錄中，您必須設定伺服器名稱，使其與伺服器憑證主體名稱相符，然後將易記名稱設為 **vdm**。

必要條件

- 確認金鑰長度至少為 1024 位元。
- 確認 TLS 憑證有效。伺服器電腦上的目前時間必須在憑證開始日期到結束日期的範圍內。
- 確認憑證主體名稱或主體替代名稱與 Windows 登錄中的 SSLCertPsgSni 設定相符。請參閱確認伺服器名稱與 PSG 憑證主體名稱相符。
- 確認憑證嵌入式管理單元已新增至 MMC。請參閱將憑證嵌入式管理單元新增到 MMC 中。
- 自行熟悉如何將憑證匯入 Windows 憑證存放區。請參閱將簽署的伺服器憑證匯入 Windows 憑證存放區。
- 自行熟悉如何修改憑證易記名稱。請參閱修改憑證易記名稱。

程序

1 在 Windows Server 主機的 MMC 視窗中，開啟**憑證 (本機電腦) > 個人**資料夾。

2 選取**更多動作 > 所有工作 > 匯入**，以匯入核發給 PSG 的 TLS 憑證。

在**憑證匯入**精靈中，選取下列設定：

a **將這個金鑰設成可匯出**

b **包含所有可延伸的內容**

完成精靈以完成匯入憑證到**個人**資料夾

3 採取下列其中一個步驟，確認新憑證是否包含私密金鑰：

- 確認憑證圖示上出現一個黃色金鑰。
- 按兩下憑證，並確認 [憑證資訊] 對話方塊中顯示下列陳述：這個憑證有一個對應的私密金鑰。

4 在新憑證上按一下滑鼠右鍵，然後按一下**內容**。

5 在「一般」索引標籤上，刪除**易記名稱**文字，然後輸入您選擇的易記名稱。

請確定您輸入的名稱與 Windows 登錄的 `SSLCertWinCertFriendlyName` 設定中的名稱完全相同，如下一個程序所述。

6 按一下**套用**，然後再按一下**確定**。

PSG 就會將 CA 簽署憑證出示給透過 PCoIP 連線至伺服器的用戶端裝置。

備註 此程序不影響舊版用戶端裝置。PSG 會繼續將預設舊版憑證出示給透過 PCoIP 連線至此伺服器的舊版用戶端裝置。

後續步驟

在 Windows 登錄中設定憑證易記名稱。

在 Windows 登錄中設定 PSG 憑證易記名稱

PSG 依伺服器名稱和憑證易記名稱識別要使用的 TLS 憑證。您必須在執行 PSG 的連線伺服器或安全伺服器電腦的 Windows 登錄中設定易記名稱值。

所有連線伺服器執行個體和安全伺服器都使用憑證易記名稱 **vdm**。相較之下，您可以為 PSG 憑證設定自己的憑證易記名稱。您必須設定 Windows 登錄設定來啟用 PSG，使正確的名稱與您將在 Windows 憑證存放區中設定的易記名稱相符。

PSG 可使用與執行 PSG 的伺服器相同的 TLS 憑證。如果您設定 PSG 使用與伺服器相同的憑證，則易記名稱必須是 **vdm**。

無論在登錄或在 Windows 憑證存放區中，易記名稱值都要區分大小寫。

必要條件

- 確認 Window 登錄包含正確的主體名稱，可用於連線至 PSG 連接埠並且與 PSG 憑證主體名稱或主體替代名稱相符。請參閱確認伺服器名稱與 PSG 憑證主體名稱相符。
- 確認 Windows 本機電腦憑證存放區中已設定憑證易記名稱。請參閱在 Windows 憑證存放區中設定 PSG 憑證。

程序

1 在執行 PCoIP 安全閘道的連線伺服器或安全伺服器電腦上，啟動 Windows 登錄編輯程式。

2 導覽至 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` 登錄機碼。

3 新增字串 (REG_SZ) 值 `SSLCertWinCertFriendlyName` 到此登錄機碼。

4 修改 `SSLCertWinCertFriendlyName` 值，然後輸入 PSG 要使用的憑證易記名稱。

例如：**pcoip**

如果您使用與伺服器相同的憑證，則值必須是 **vdm**。

5 重新啟動 VMware Horizon View PCoIP 安全閘道服務，讓您的變更生效。

後續步驟

確認用戶端裝置是否持續連線至 PSG。

如果您使用安全掃描程式進行符合性測試，請掃描 PSG 連接埠。

強制使用 CA 簽署的憑證連線至 PSG

您可以確保用戶端與 PSG 間的所有連線，都使用 PSG 的 CA 簽署憑證，而不是使用預設舊版憑證。為 PSG 設定 CA 簽署的憑證時，不需要此程序。只有在強制使用 CA 簽署憑證適用於您的 Horizon 7 部署時，才採用這些步驟。

在某些情況下，PSG 可能向安全掃描程式出示預設的舊版憑證，而不是出示 CA 簽署的憑證，導致 PSG 連接埠的符合性測試無效。為解決此問題，您可以設定 PSG 不要將預設舊版憑證出示給任何嘗試連線的裝置。

重要 執行此程序可阻止所有舊版用戶端透過 PCoIP 連線至此伺服器。

必要條件

確認連線至此伺服器的所有用戶端裝置 (包括精簡型用戶端) 均執行適用於 Windows 的 Horizon Client 5.2 或 Horizon Client 2.0 或更新版本。您必須升級舊版用戶端。

程序

1. 在執行 PCoIP 安全閘道的連線伺服器或安全伺服器電腦上，啟動 Windows 登錄編輯程式。
2. 導覽至 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` 登錄機碼。
3. 新增字串 (REG_SZ) 值 `SSLCertPresentLegacyCertificate` 到此登錄機碼。
4. 將 `SSLCertPresentLegacyCertificate` 值設為 **0**。
5. 重新啟動 VMware Horizon View PCoIP 安全閘道服務，讓您的變更生效。

將 Horizon Administrator 設定為信任 vCenter Server 或 View Composer 憑證

在 Horizon Administrator 儀表板中，您可以將 Horizon 7 設定為信任不受信任的 vCenter Server 或 View Composer 憑證。

VMware 強烈建議您設定 vCenter Server 和 View Composer 使用由 CA 簽署的 TLS 憑證。或者，您可以為 vCenter Server 或 View Composer 接受預設憑證的指紋。

同樣地，VMware 建議您設定 SAML 2.0 驗證器使用由 CA 簽署的 TLS 憑證。或者，您可以在 Horizon Administrator 儀表板中接受預設憑證的指紋，藉以將 Horizon 7 設定為信任不受信任的 SAML 2.0 伺服器憑證。

使用 CA 簽署的 TLS 憑證的優點

CA 是一個受信任的實體，可保證憑證的身分及其建立者。當憑證是由信任的 CA 簽署時，使用者不會再收到要求他們確認憑證的訊息，而精簡型用戶端裝置可以連線，無需要求額外組態。

您可以要求專屬於某個網頁網域 (例如 `www.mycorp.com`) 的 TLS 伺服器憑證，也可以要求可供整個網域 (例如 `*.mycorp.com`) 使用的萬用字元 TLS 伺服器憑證。若要簡化管理，當您必須將憑證安裝在多部伺服器或不同的子網域時，可以選擇要求萬用字元憑證。

一般而言，網域專屬的憑證是用於安全安裝，而 CA 對於網域專屬憑證所提供免於損失的保證通常會比萬用字元憑證更多。如果使用與其他服務共用的萬用字元憑證，則 Horizon 7 產品的安全性也會視上述其他服務的安全性而定。如果您使用萬用字元憑證，則必須確定私密金鑰可以在伺服器之間傳輸。

當您以自己的憑證取代預設憑證時，用戶端會使用您的憑證來驗證伺服器。如果您的憑證是由 CA 簽署，CA 的憑證本身通常是嵌入瀏覽器中，或位於用戶端可以存取的信任資料庫中。當用戶端接受憑證後，會傳送秘密金鑰做為回應，該金鑰是以憑證中所包含的公開金鑰來加密的。秘密金鑰是用來為用戶端與伺服器之間的流量進行加密的。

對 Horizon 連線伺服器和安全伺服器的憑證問題進行疑難排解

Horizon 7 Server 上的憑證問題會使您無法連線至 Horizon Administrator，或導致伺服器的健全狀況指示器顯示為紅色。

問題

您無法在有問題的連線伺服器執行個體上連線至 Horizon Administrator。當您在相同網繭中的另一個連線伺服器執行個體上連線至 Horizon Administrator 時，您會看到有問題的連線伺服器執行個體的儀表板健全狀況指示器顯示為紅色。

從其他連線伺服器執行個體按一下紅色的健全狀況指示器，即會顯示 `SSL 憑證: 無效和狀態: (空白)`，表示找不到有效的憑證。Horizon 7 記錄檔會包含類型為「錯誤」的記錄項目以及下列錯誤文字：`No qualifying certificates in keystore`。

Horizon 7 記錄資料位於連線伺服器執行個體上的 `C:\ProgramData\VMware\VDM\logs\log-*.txt` 中。

原因

憑證可能因為下列其中一個原因而未成功安裝在 Horizon 7 server 上：

- 憑證不在 Windows 本機電腦憑證存放區的 [個人] 資料夾中。
- 憑證存放區沒有憑證的私密金鑰。
- 憑證不是使用易記名稱 **vdm** 命名。
- Windows Server 2008 或更新版本伺服器的憑證是使用 v3 憑證範本產生的。Horizon 7 無法偵測私密金鑰，但如果您使用憑證嵌入式管理單元來檢查 Windows 憑證存放區，存放區會指出存在私密金鑰。

解決方案

- 確認憑證已匯入至 Windows 本機電腦憑證存放區的 [個人] 資料夾中。

  請參閱將簽署的伺服器憑證匯入 Windows 憑證存放區。
- 確認憑證包含私密金鑰。

  請參閱將簽署的伺服器憑證匯入 Windows 憑證存放區。
- 確認憑證是以易記名稱 **vdm** 命名。

  請參閱修改憑證易記名稱。
- 如果憑證是使用 v3 憑證範本產生的，請從未使用 v3 範本的 CA 取得有效的已簽署憑證。

  請參閱從 CA 取得簽署的 TLS 憑證。

初次設定 Horizon 7

9

安裝 Horizon 7 Server 軟體並設定伺服器的 SSL 憑證之後，您必須採取幾個額外步驟來設定可運作的 Horizon 7 環境。

您要設定 vCenter Server 和 View Composer 的使用者帳戶、安裝 Horizon 7 授權金鑰、將 vCenter Server 和 View Composer 新增至您的 Horizon 7 環境、設定 PCoIP 安全閘道和安全通道，並且選擇性地調整 Windows Server 設定以支援您的 Horizon 7 環境。

本章節討論下列主題：

- 設定 vCenter Server、View Composer 和即時複製的使用者帳戶
- 初次設定 Horizon 連線伺服器
- 設定 Horizon Client 連線
- 取代 Horizon 7 服務的預設連接埠
- 調整 Windows Server 設定以支援您的部署

設定 vCenter Server、View Composer 和即時複製的使用者帳戶

若要搭配使用 vCenter Server 和 Horizon 7，必須設定擁有適當 vCenter Server 權限的使用者帳戶。您可建立擁有適當權限的 vCenter Server 角色並將該角色指派給 vCenter Server 使用者帳戶。

如果在不同於 vCenter Server 的機器上安裝 View Composer，您還必須在 Active Directory 中建立 Horizon 7 可用於向獨立式機器上的 View Composer 服務驗證的使用者帳戶。

如果使用 View Composer，您必須在 Active Directory 中建立允許 View Composer 在 Active Directory 中執行特定作業的第三個使用者帳戶。View Composer 需要此帳戶才能將連結複製虛擬機器加入您的 Active Directory 網域中。請參閱建立 View Composer AD 作業的使用者帳戶。

如果使用即時複製，您必須在 Active Directory 中建立允許連線伺服器在 Active Directory 中執行特定作業的使用者帳戶。連線伺服器需要此帳戶才能將即時複製虛擬機器加入您的 Active Directory 網域中。請參閱建立即時複製作業的使用者帳戶。

總之，在您首次設定 Horizon 7 時，需要在 Horizon Administrator 中提供這些使用者帳戶：

- vCenter Server 使用者允許 Horizon 7 和 View Composer 在 vCenter Server 中執行作業。

- 獨立式 View Composer Server 使用者允許 Horizon 7 向獨立式機器上的 View Composer 服務驗證。

  如果在與 vCenter Server 相同的機器上安裝 View Composer，vCenter Server 使用者可執行上述兩個功能，無需使用獨立式 View Composer Server 使用者。
- AD 作業的 View Composer 使用者允許 View Composer 在 Active Directory 中執行特定作業。
- AD 作業的即時複製使用者允許連線伺服器在 Active Directory 中執行特定作業。

使用 vCenter Server 使用者和 View Composer 使用者的位置

建立並設定這些使用者帳戶之後，您需要在 Horizon Administrator 中指定使用者名稱。

- 將 vCenter Server 新增至 Horizon 7 時，您要指定 vCenter Server 使用者。
- 設定 View Composer 設定並選取**獨立式 View Composer Server** 時，請指定獨立式 View Composer Server 使用者。
- 設定 View Composer 網域時指定 AD 作業的 View Composer 使用者。
- 建立連結複製集區時指定 AD 作業的 View Composer 使用者。

針對 Horizon 7 和 View Composer 設定 vCenter Server 使用者

若要設定允許 Horizon 7 在 vCenter Server 中執行作業的使用者帳戶，您必須將具備適當權限的 vCenter Server 角色指派給該使用者。

必須新增至 vCenter Server 角色的權限清單各異，視您是否搭配使用 Horizon 7 與 View Composer 而定。View Composer 服務在 vCenter Server 中執行需要除基礎權限以外之權限的作業。

如果在與 vCenter Server 相同的機器上安裝 View Composer，vCenter Server 使用者必須是 vCenter Server 機器上的本機系統管理員。此需求允許 Horizon 7 向 View Composer 服務驗證。

如果在不同於 vCenter Server 的機器上安裝 View Composer，vCenter Server 使用者無需是 vCenter Server 機器上的本機管理員。但是，您需要建立必須是 View Composer 機器上之本機管理員的獨立式 View Composer Server 使用者帳戶。

必要條件

- 在 Active Directory 中，建立連線伺服器網域或信任網域中的使用者。請參閱建立 vCenter Server 的使用者帳戶。
- 請熟悉使用者帳戶所需的 vCenter Server 權限。請參閱 vCenter Server 使用者所需權限。
- 如果您使用 View Composer，請熟悉額外的必要權限。請參閱 vCenter Server 使用者所需的 View Composer 和即時複製權限。

程序

1 在 vCenter Server 中，為使用者準備好具備必要權限的角色。

   - 您可以使用 vCenter Server 中預先定義的管理員角色。此角色可以在 vCenter Server 中執行所有作業。

- 如果您使用 View Composer，您可以建立受限角色，使其具備連線伺服器和 View Composer 執行 vCenter Server 作業所需的最低權限。

  在 vSphere Client 中，按一下**首頁 > 角色 > 新增角色**，輸入角色名稱 (例如 **View Composer Administrator**)，然後為角色選取權限。

  此角色必須具備連線伺服器和 View Composer 在 vCenter Server 中操作所需的所有權限。

- 如果您使用 Horizon 7 而不使用 View Composer，您可以建立更為受限的角色，使其具備連線伺服器執行 vCenter Server 作業所需的最低權限。

  在 vSphere Client 中，按一下**首頁 > 角色 > 新增角色**，輸入角色名稱 (例如 **View Manager Administrator**)，然後為角色選取權限。

- 如果您使用即時複製，您可以建立受限角色，使其具備連線伺服器執行 vCenter Server 作業所需的最低權限。

  在 vSphere Client 中，按一下**首頁 > 角色 > 新增角色**，輸入角色名稱 (例如 **View Manager Instant Clone Administrator**)，然後為角色選取權限。如需即時複製權限的資訊，請參閱 vCenter Server 使用者所需的 View Composer 和即時複製權限。

2 在 vSphere Client 中，以滑鼠右鍵按一下詳細目錄最上層的 vCenter Server，然後按一下**新增權限**，接著新增 vCenter Server 使用者。

備註 您必須在 vCenter Server 層級定義 vCenter Server 使用者。

3 從下拉式功能表中選取管理員角色，或您所建立的 View Composer 或 View Manager 角色，並將其指定給 vCenter Server 使用者。

4 如果在與 vCenter Server 相同的機器上安裝 View Composer，請將 vCenter Server 使用者帳戶新增為 vCenter Server 機器上的本機系統管理員群組中的成員。

如果在不同於 vCenter Server 的機器上安裝 View Composer，則不必執行該步驟。

後續步驟

在 Horizon Administrator 中，在您將 vCenter Server 新增至 Horizon 7 時指定 vCenter Server 使用者。請參閱將 vCenter Server 執行個體新增到 Horizon 7。

vCenter Server 使用者所需權限

vCenter Server 使用者必須擁有足夠的 vCenter Server 權限，才能在 vCenter Server 中啟用 Horizon 7 以執行作業。使用需要的權限，為 vCenter Server 使用者建立 View Manager 角色。

表 9-1. View Manager 角色所需權限

權限群組	要啟用的權限
資料夾	建立資料夾 刪除資料夾
資料存放區	配置空間

表 9-1. View Manager 角色所需權限 (續)

權限群組	要啟用的權限
虛擬機器	在**組態**中： ■ **新增或移除裝置** ■ **進階** ■ **修改裝置設定** 在**互動**中： ■ **關閉電源** ■ **開啟電源** ■ **重設** ■ **暫停** ■ **執行抹除或縮小作業** 在**詳細目錄**中： ■ **新建** ■ **從現有項目建立** ■ **移除** 在**佈建**中： ■ **自訂** ■ **部署範本** ■ **讀取自訂規格** ■ **複製範本** ■ **複製虛擬機器**
資源	**將虛擬機器指派給資源集區**
全域	**當做 vCenter Server 使用** 即使您不使用 View 儲存加速器，vCenter Server 使用者仍需要此權限。
主機	實作啟用 ESXi 主機快取的 View 儲存加速器需要下列**主機**權限。如果您沒有使用 View 儲存加速器，則 vCenter Server 使用者不需要此權限。 在**組態**中： ■ **進階設定**
設定檔驅動儲存區 (如果正在使用 vSAN 資料存放區或虛擬磁碟區)	(全部)

vCenter Server 使用者所需的 View Composer 和即時複製權限

若要支援 View Composer 或即時複製，vCenter Server 使用者必須具有支援 Horizon 7 所需的權限外，還需要其他權限。

View Composer 和即時複製權限會列出 View Manager、View Composer 和即時複製所需的權限超集。

表 9-2. View Composer 和即時複製權限

vCenter Server 上的權限群組	要啟用的權限
資料夾	**建立資料夾** **刪除資料夾**
資料存放區	**配置空間** **瀏覽資料存放區** **低階檔案作業**
主機	在**詳細目錄**中 ■ **修改叢集**
虛擬機器	在**組態**中 (全部) 在**互動**中： ■ **關閉電源** ■ **開啟電源** ■ **重設** ■ **暫停** ■ **執行抹除或縮小作業** ■ **裝置連線** 在**詳細目錄**中 (全部) 在**快照管理**中 (全部) 在**佈建**中： ■ **自訂** ■ **部署範本** ■ **讀取自訂規格** ■ **複製範本** ■ **複製虛擬機器** ■ **允許磁碟存取**
資源	**將虛擬機器指派給資源集區** 執行 View Composer 重新平衡作業需要下列權限。 **移轉已關閉電源的虛擬機器**
全域	**啟用方法** **停用方法** **系統標籤** **管理自訂屬性** **設定自訂屬性** 實作啟用 ESXi 主機快取的 View 儲存加速器需要下列權限。即使您不使用 View 儲存加速器，vCenter Server 使用者仍需要此權限。 **當做 vCenter Server 使用**
網路	(全部)
設定檔驅動儲存區	(所有--如果正在使用 vSAN 資料存放區或虛擬磁碟區)

表 9-2. View Composer 和即時複製權限 (續)

vCenter Server 上的權限群組	要啟用的權限
儲存區視圖	檢視
密碼編譯作業	如果您使用具備信任平台模組 (vTPM) 裝置的即時複製虛擬機器，則需要具備下列權限。 ■ 複製 ■ 解密 ■ 直接存取 ■ 加密 ■ 管理 KMS ■ 移轉 ■ 登錄主機

初次設定 Horizon 連線伺服器

安裝連線伺服器之後，您必須安裝產品授權，並將 vCenter Server 和 View Composer 服務新增至 Horizon 7。您也可以允許 ESXi 主機回收連結複製虛擬機器上的磁碟空間，以及設定 ESXi 主機快取虛擬機器磁碟資料。

如果您安裝安全伺服器，這些伺服器會自動新增至 Horizon 7 並顯示在 Horizon Administrator 中。

Horizon Administrator 和 Horizon 連線伺服器

Horizon Administrator 提供適用於 Horizon 7 的 Web 式管理介面。

Horizon 連線伺服器可以有多個執行個體，以作為複寫伺服器或安全伺服器。根據您的 Horizon 7 部署，您的每個連線伺服器執行個體可以各有一個 Horizon Administrator 介面。

請依照下列最佳做法搭配使用 Horizon Administrator 與連線伺服器：

- 使用連線伺服器的主機名稱和 IP 位址登入 Horizon Administrator。使用 Horizon Administrator 介面管理連線伺服器，以及任何相關聯的安全伺服器或複寫伺服器。
- 在網繭環境中，確認所有管理員皆使用相同連線伺服器的主機名稱和 IP 位址登入 Horizon Administrator。請勿使用負載平衡器的主機名稱和 IP 位址來存取 Horizon Administrator 網頁。
- 若要識別您正在使用的連線伺服器的 CPA 網繭或叢集名稱，您可以在 Horizon Administrator 標頭中和網頁瀏覽器索引標籤中檢視該名稱。

備註 如果使用 Unified Access Gateway 應用裝置 (而非安全伺服器)，您必須使用 Unified Access Gateway REST API 來管理 Unified Access Gateway 應用裝置。舊版的 Unified Access Gateway 名為 Access Point。如需詳細資訊，請參閱《部署及設定 Unified Access Gateway》。

登入 Horizon Administrator

若要執行初始組態工作，您必須登入 Horizon Administrator。

必要條件

確認您使用 Horizon Administrator 支援的網頁瀏覽器。請參閱 Horizon Administrator 需求。

程序

1 開啟您的網頁瀏覽器並輸入下列 URL，其中 *server* 是連線伺服器執行個體的主機名稱。

`https://server/admin`

備註 主機名稱無法解析時，如果您必須存取連線伺服器執行個體，則可以使用 IP 位址。不過，您聯繫的主機將不符合為連線伺服器執行個體設定的 TLS 憑證，因而導致存取遭封鎖，或只能在安全性降低的情況下存取。

您對 Horizon Administrator 的存取權取決於在連線伺服器電腦上設定的憑證類型。如果要在連線伺服器主機上開啟網頁瀏覽器，請使用 **`https://127.0.0.1`** 進行連線，而非 **`https://localhost`**。此方法避免了針對 `localhost` 解析的潛在 DNS 攻擊，從而提升了安全性。

選項	說明
您已為 Horizon 連線伺服器設定 CA 簽署的憑證。	當您第一次連線時，您的網頁瀏覽器會顯示**歡迎使用 VMware Horizon 7** 頁面。
系統會設定隨 Horizon 連線伺服器提供的預設自我簽署憑證。	初次連線時，您的網頁瀏覽器可能會顯示一個頁面，警告與該位址相關的安全性憑證不是由信任的憑證授權機構所核發。 按一下**忽略**，繼續使用目前的 TLS 憑證。

2 按一下 Horizon Administrator 下方的**啟動**。

3 使用具有管理員角色的帳戶登入。

您可以在安裝獨立連線伺服器執行個體或所複寫群組中的第一個連線伺服器執行個體時，對管理員角色進行初始指派。依預設會選取您用於安裝連線伺服器的帳戶，但您可以將此帳戶變更為管理員的本機群組或網域全域群組。

如果您選擇管理員本機群組，則可以使用直接或透過全域群組成員資格新增至此群組的任何網域使用者。您無法使用新增至此群組的本機使用者。

登入 Horizon Administrator 之後，您可以使用 **View 組態 > 管理員**變更擁有管理員角色的使用者和群組清單。

安裝產品授權金鑰

您必須先輸入產品授權金鑰，才能使用連線伺服器。

備註 如果您有 Horizon 7 訂閱授權，則不需要產品授權金鑰。如需關於訂閱授權的詳細資訊，請參閱 #unique_128。

初次登入時，Horizon Administrator 會顯示「產品授權及使用」頁面。

安裝授權金鑰後，Horizon Administrator 會在您登入時顯示儀表板頁面。

您不需要在安裝複寫的連線伺服器執行個體或安全伺服器時設定授權金鑰。複寫執行個體和安全伺服器會使用儲存在 View LDAP 組態中的一般授權金鑰。

備註 連線伺服器需要有效的授權金鑰。產品授權金鑰是 25 個字元的金鑰。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 產品授權及使用**。

2 在**授權**面板中，按一下**編輯授權**。

3 輸入授權序號，並按一下**確定**。

4 確認授權到期日。

5 根據產品授權賦予您使用權限的 VMware Horizon 7 版本，確認已啟用或停用桌面平台、應用程式遠端處理和 View Composer 授權。

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。

將 vCenter Server 執行個體新增到 Horizon 7

在 Horizon 7 部署中，您必須設定 Horizon 7 以連線至 vCenter Server 執行個體。vCenter Server 會建立並管理 Horizon 7 在桌面平台集區中使用的虛擬機器。

如果需在連結模式群組中執行 vCenter Server 執行個體，您必須將每個 vCenter Server 執行個體分別新增至 Horizon 7。

Horizon 7 將使用安全通道 (SSL) 連線至 vCenter Server 執行個體。

必要條件

- 安裝連線伺服器產品授權金鑰。
- 讓 vCenter Server 使用者有權執行支援 Horizon 7 所需的 vCenter Server 作業。若要使用 View Composer，您必須將其他權限授予使用者。

  請參閱針對 Horizon 7 和 View Composer 設定 vCenter Server 使用者。
- 確認在 vCenter Server 主機上安裝 TLS/SSL 伺服器憑證。在生產環境中，安裝受信任的憑證授權機構 (CA) 所簽署的有效憑證。

  在測試環境中，您可以使用與 vCenter Server 一併安裝的預設憑證，但是必須在將 vCenter Server 新增至 Horizon 7 時接受憑證指紋。
- 確認複寫的群組中所有連線伺服器執行個體皆信任 vCenter Server 主機上安裝之伺服器憑證所屬的根 CA 憑證。檢查根 CA 憑證是否出現在**受信任的根憑證授權單位 > 憑證**資料夾中；該資料夾位於連線伺服器主機的 Windows 本機電腦憑證存放區中。若未出現，請將根 CA 憑證匯入至 Windows 本機電腦憑證存放區。

  請參閱將根憑證和中繼憑證匯入 Windows 憑證存放區。

- 確認 vCenter Server 執行個體包含 ESXi 主機。如果並未在 vCenter Server 執行個體中設定任何主機，則無法將執行個體新增至 Horizon 7。
- 如果您升級到 vSphere 5.5 或更新版本，請確認您用作 vCenter Server 使用者的網域管理員帳戶已明確獲得指派 vCenter Server 本機使用者登入 vCenter Server 的權限。
- 若您計劃以 FIPS 模式使用 Horizon 7，請確認您擁有 vCenter Server 6.0 或更新版本以及 ESXi 6.0 或更新版本的主機。

  如需詳細資訊，請參閱第 4 章 以 FIPS 模式安裝 Horizon 7。
- 請自行熟悉決定 vCenter Server 及 View Composer 作業數上限的設定。請參閱 vCenter Server 和 View Composer 的並行作業限制與設定並行電源作業率以支援遠端桌面平台登入風暴。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 伺服器**。

2 在 **vCenter Server** 索引標籤上，按一下**新增**。

3 在 vCenter Server 設定**伺服器位址**文字方塊中，輸入 vCenter Server 執行個體的完整網域名稱 (FQDN)。

  FQDN 包含主機名稱及網域名稱。例如，在 FQDN ***myserverhost.companydomain.com*** 中，***myserverhost*** 是主機名稱，***companydomain.com*** 是網域。

  備註 如果使用 DNS 名稱或 URL 輸入伺服器，則 Horizon 7 將不執行 DNS 查詢來確認管理員先前是否使用此伺服器的 IP 位址，將此伺服器新增至 Horizon 7。如果使用 DNS 名稱及 IP 位址新增 vCenter Server，將發生衝突。

4 輸入 vCenter Server 使用者的名稱。

  例如：**domain\user** 或 **user@domain.com**

5 輸入 vCenter Server 使用者密碼。

6 (選擇性) 輸入此 vCenter Server 執行個體的描述。

7 輸入 TCP 連接埠號碼。

  預設連接埠為 443。

8 在「進階設定」下，設定 vCenter Server 及 View Composer 作業的並行作業限制。

9 按**下一步**將顯示「View Composer 設定」頁面。

後續步驟

設定 View Composer。

- 如果已使用簽署的 SSL 憑證設定 vCenter Server 執行個體，且連線伺服器信任根憑證，則「新增 vCenter Server」精靈將顯示「View Composer 設定」頁面。
- 如果已使用預設憑證設定 vCenter Server 執行個體，則必須先決定是否接受現有憑證的指紋。請參閱接受預設 TLS 憑證的指紋。

如果 Horizon 7 使用多個 vCenter Server 執行個體，則請重複執行此程序來新增其他 vCenter Server 執行個體。

設定 View Composer

若要使用 View Composer，您必須設定讓連線伺服器能夠連線至 View Composer 服務的設定。View Composer 可以安裝在其本身的獨立式機器上，或與 vCenter Server 相同的機器上。

VMware 建議在每個 View Composer 服務與 vCenter Server 執行個體之間是一對一的對應關係。

必要條件

- 確認您已將連線伺服器設定為連線至 vCenter Server。若要這樣做，您必須完成「新增 vCenter Server」精靈的「vCenter Server 資訊」頁面。請參閱將 vCenter Server 執行個體新增到 Horizon 7。
- 確認此 View Composer 服務尚未設定為連線至其他 vCenter Server 執行個體。
- 如果已在獨立式機器上安裝 View Composer，請確認您已建立獨立式 View Composer Server 使用者帳戶。此網域使用者帳戶必須是 View Composer 機器上本機管理員群組的成員。

程序

1 在 Horizon Administrator 中，完成「新增 vCenter Server」精靈的「vCenter Server 資訊」頁面。

   a 按一下 **View 組態 > 伺服器**。

   b 在「vCenter Server」標籤中，按一下**新增**，然後提供 vCenter Server 設定。

2 在「View Composer 設定」頁面上，如果不使用 View Composer，請選取**不使用 View Composer**。

   如果選取**不使用 View Composer**，其他 View Composer 設定就會變成非作用中。按**下一步**時，「新增 vCenter Server」精靈會顯示「儲存設定」頁面。不會顯示「View Composer 網域」頁面。

3 如果使用 View Composer，請選取 View Composer 機器的位置。

選項	說明
View Composer 安裝在與 vCenter Server 相同的機器上。	a 選取 **View Composer 與 vCenter Server 並行安裝**。 b 確認連接埠編號與當初在 vCenter Server 上安裝 View Composer 服務時所指定的連接埠相同。預設連接埠編號是 18443。
View Composer 安裝在其本身的另一個機器上。	a 選取**獨立 View Composer Server**。 b 在 [View Composer Server 位址] 文字方塊中，輸入 View Composer 機器的完整網域名稱 (FQDN)。 c 輸入可向 View Composer 服務驗證的網域使用者帳戶名稱。 此帳戶必須是獨立式 View Composer 機器上本機管理員群組的成員。 例如：`domain.com\user` 或 `user@domain.com` d 輸入此網域使用者帳戶的密碼。 e 確認連接埠編號與當初安裝 View Composer 服務時所指定的連接埠相同。預設連接埠編號是 18443。

4 按**下一步**以顯示「View Composer 網域」頁面。

後續步驟

設定 View Composer 網域。

- 如果已使用簽署的 SSL 憑證設定 View Composer 執行個體，且連線伺服器信任根憑證，「新增 vCenter Server」精靈便會顯示「View Composer 網域」頁面。
- 如果已使用預設憑證設定 View Composer 執行個體，則必須先決定是否接受現有憑證的指紋。請參閱接受預設 TLS 憑證的指紋。

設定 View Composer 網域

您必須設定 View Composer 部署連結複製桌面所在的 Active Directory 網域。您可以為 View Composer 設定多個網域。當您首次將 vCenter Server 和 View Composer 設定新增至 View 之後，您可以在 Horizon Administrator 中編輯 vCenter Server 執行個體，以新增更多 View Composer 網域。

必要條件

- Active Directory 管理員必須建立 AD 作業的 View Composer 使用者。此網域使用者必須擁有在包含連結複製的 Active Directory 網域中新增和移除虛擬機器的權限。如需此使用者所需權限的相關資訊，請參閱建立 View Composer AD 作業的使用者帳戶。
- 在 Horizon Administrator 中，確認您已完成「新增 vCenter Server」精靈中的「vCenter Server 資訊」和「View Composer 設定」頁面。

程序

1. 在 [View Composer 網域] 頁面上，按一下**新增**以新增 AD 作業的 View Composer 使用者帳戶資訊。
2. 輸入 Active Directory 網域的網域名稱。

   例如：**domain.com**
3. 輸入網域使用者名稱，包括 View Composer 使用者的網域名稱。

   例如：**domain.com\admin**
4. 輸入帳戶密碼。
5. 按一下**確定**。
6. 若要新增在您部署連結複製集區與所在其他 Active Directory 網域內具有權限的網域使用者帳戶，請重複前述步驟。
7. 按一下**下一步**以顯示「儲存設定」頁面。

後續步驟

啟用虛擬機器磁碟空間回收，並為 Horizon 7 設定 View 儲存加速器。

新增即時複製網域管理員

您必須先將即時複製網域管理員新增至 Horizon 7，才能建立即時複製桌面平台集區。

即時複製網域管理員必須具有特定的 Active Directory 網域權限。請參閱《Horizon 7 安裝》文件中的〈vCenter Server 使用者所需的 View Composer 和即時複製權限〉。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 即時複製網域管理員**。

2 按一下**新增**。

3 輸入即時複製網域管理員的登入名稱和密碼。

允許 vSphere 回收連結複製虛擬機器中的磁碟空間

在 vSphere 5.1 和更新版本中，您可以啟用 Horizon 7 的磁碟空間回收功能。在 vSphere 5.1 中啟動後，Horizon 7 會以有效磁碟格式建立連結複製虛擬機器，讓 ESXi 主機能夠回收連結複製中未使用的磁碟空間，以減少連結複製所需的總儲存空間。

當使用者與連結複製桌面互動時，複製的作業系統磁碟會增加，最後會佔用到幾乎和完整複製桌面一樣的磁碟空間。磁碟空間回收可減少作業系統磁碟的大小，使您不必重新整理或重新撰寫連結複製。只要開啟虛擬機器電源，系統就會在使用者與遠端桌面平台互動的同時回收空間。

當部署無法利用登出後重新整理之類可節省儲存空間的策略時，磁碟空間回收功能就特別有用。例如，知識工作者在專用遠端桌面平台上安裝使用者應用程式後，若重新整理或重新撰寫遠端桌面平台，可能會遺失其個人應用程式。有了磁碟空間回收功能，Horizon 7 可以將連結複製一直維持在接近第一次佈建時初始的較少空間。

此功能具有兩個元件：空間效率高的磁碟格式和空間回收作業。

在 vSphere 5.1 或更新版本的環境中，若父虛擬機器是虛擬硬體版本 9 或更新版本，則不管是否啟用空間回收作業，Horizon 7 都會以空間效率高的作業系統磁碟來建立連結複製。

若要啟用空間回收作業，您必須使用 Horizon Administrator 來啟用 vCenter Server 的空間回收功能，並回收個別桌面平台集區的虛擬機器磁碟空間。在 vCenter Server 的空間回收設定中，您可以對所有受 vCenter Server 執行個體管理的桌面平台集區選擇停用此功能。停用 vCenter Server 的該功能會覆寫桌面平台集區層級的設定。

下列指導方針適用於空間回收功能：

- 僅在連結複製中空間高效的作業系統磁碟上運作。
- 不會影響 View Composer 持續性磁碟。
- 它僅適用於 vSphere 5.1 或更新版本，且僅限虛擬硬體版本 9 或更新版本的虛擬機器。
- 不會在完整複製桌面上運作。
- 會在含 SCSI 控制器的虛擬機器上運作。不支援 IDE 控制器。

集區中包含具有空間高效磁碟的虛擬機器時，不支援 View Composer Array Integration (VCAI)。VCAI 使用 vStorage APIs for Array Integration (VAAI) 原生 NFS 快照技術，來複製虛擬機器。

必要條件

- 確認您的 vCenter Server 與 ESXi 主機 (包括叢集中的所有 ESXi 主機) 均為包含 ESXi 5.1 下載修補程式 ESXi510-201212001 的 5.1 版或更新版本。

程序

1 在 Horizon Administrator 中，請先完成「新增 vCenter Server」精靈頁面，再完成「儲存設定」頁面。

   a 選取 **View 組態 > 伺服器**。

   b 在 **vCenter Server** 索引標籤上，按一下**新增**。

   c 完成「vCenter Server 資訊」、「View Composer 設定」，以及「View Composer 網域」頁面。

2 在「儲存設定」頁面上，確認已選取**啟用空間回收**。

   如果您是在執行 Horizon 7 5.2 或更新版本的全新安裝，則依預設將選取空間回收功能。如果您是在從 Horizon 7 5.1 或更早版本升級為 Horizon 7 5.2 或更新版本，則必須選取**啟用空間回收**。

後續步驟

在「儲存設定」頁面上，設定 View 儲存加速器。

若要在 Horizon 7 中完成磁碟空間回收的設定，請為桌面平台集區設定空間回收功能。

設定 vCenter Server 的 View 儲存加速器

在 vSphere 5.1 和更新版本中，您可以設定 ESXi 主機以快取虛擬機器磁碟資料。這項稱為 View 儲存加速器的功能使用 ESXi 主機的內容型讀取快取 (CBRC) 功能。當許多虛擬機器啟動或立即執行防毒掃描時會發生 I/O 風暴，而 View 儲存加速器可提升 I/O 風暴期間的 Horizon 7 效能。管理員或使用者頻繁載入應用程式或資料時，這項功能也相當實用。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或應用程式。

View 儲存加速器會透過減少開機風暴期間的 IOPS 數目，降低儲存陣列的需要，讓您使用較少的儲存 I/O 頻寬支援您的 Horizon 7 部署。

您可以在 Horizon Administrator 的 vCenter Server 精靈中選取「View 儲存加速器」設定，以啟用 ESXi 主機上的快取，如本程序所述。

請確定也已針對個別桌面平台集區設定 View 儲存加速器。若要在桌面平台集區上運作，必須針對 vCenter Server 及個別桌面平台集區啟用 View 儲存加速器。

桌面平台集區預設啟用 View 儲存加速器。此功能可在建立或編輯集區時停用或啟用。最佳方法是在初次建立桌面平台集區時啟用此功能。如果透過編輯現有集區啟用此功能，則必須確保新複本及其摘要磁碟會在佈建連結複製之前建立。可以透過將集區重新撰寫為新的快照或將集區重新平衡為新的資料存放區來建立新複本。僅當桌面平台集區中的虛擬機器關閉電源後，才能針對這些虛擬機器設定摘要檔案。

對於包含連結複製的桌面平台集區，以及包含完整虛擬機器的集區，您可以啟用 View 儲存加速器。

針對 View 儲存加速器啟用的集區不支援原生 NFS 快照技術 (VAAI)。

現在 View 儲存加速器適用於使用 Horizon 7 複本分層的組態，也就是複本會儲存於非連結複製所在的單獨資料存放區。雖然 View 儲存加速器與 Horizon 7 複本分層搭配使用的效能優點在實質上並不顯著，但是將複本儲存於單獨資料存放區，可能會實現某些與容量相關的優點。因此，這是已經過測試且受支援的組合。

重要 若您想使用此功能，而您使用多個共用部分 ESXi 主機的 Horizon 7 網繭，則您必須針對共用 ESXi 主機上的所有集區啟用 Horizon Storage Accelerator 功能。在多個網繭中擁有不一致的設定可能導致共用 ESXi 主機上的虛擬機器不穩定。

必要條件

- 確認 vCenter Server 及 ESXi 主機為 5.1 版或更新版本。

  在 ESXi 叢集中，確認所有主機皆為 5.1 版或更新版本。
- 確認已在 vCenter Server 中將**主機 > 組態 > 進階設定**權限指派給 vCenter Server 使用者。

  請參閱設定 vCenter Server、View Composer 和即時複製的使用者帳戶。

程序

1 在 Horizon Administrator 中，請先完成「新增 vCenter Server」精靈頁面，再完成「儲存設定」頁面。

  a 選取 **View 組態 > 伺服器**。

  b 在 **vCenter Server** 索引標籤上，按一下**新增**。

  c 完成「vCenter Server 資訊」、「View Composer 設定」，以及「View Composer 網域」頁面。

2 在「儲存設定」頁面上，確認已選取**啟用 View 儲存加速器**核取方塊。

  此核取方塊預設為選取狀態。

3 指定預設的主機快取大小。

  預設快取大小會套用至此 vCenter Server 執行個體所管理的所有 ESXi 主機。

  預設值為 1,024MB。快取大小必須介於 100MB 和 2,048MB 之間。

4 若要針對個別 ESXi 主機指定不同的快取大小，請選取 ESXi 主機並按一下**編輯快取大小**。

  a 在「主機快取」對話方塊中，選取**覆寫預設的主機快取大小**。

  b 輸入**主機快取大小**值 (介於 100MB 和 2,048MB 之間) 並按一下**確定**。

5 在「儲存設定」頁面上，按**下一步**。

6 按一下**完成**以便將 vCenter Server、View Composer 及「儲存設定」新增至 Horizon 7。

後續步驟

若要設定用戶端連線的 PCoIP 安全閘道、安全通道及外部 URL，請參閱設定 Horizon Client 連線。

若要完成 Horizon 7 中的 View 儲存加速器設定，請設定桌面平台集區的 View 儲存加速器。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈設定桌面平台集區的 View 儲存加速器〉。

vCenter Server 和 View Composer 的並行作業限制

當您將 vCenter Server 新增至 Horizon 7 或編輯 vCenter Server 設定時，您可以設定數個選項以設定 vCenter Server 和 View Composer 所執行的並行作業數目上限。

您要在「vCenter Server 資訊」頁面上的「進階設定」面板中設定這些選項。

表 9-3. vCenter Server 和 View Composer 的並行作業限制

設定	說明
vCenter 並行佈建作業上限	決定連線伺服器在此 vCenter Server 執行個體中佈建和刪除完整虛擬機器所能提出的並行要求數目上限。 預設值為 20。 此設定僅適用於完整虛擬機器。
並行電源作業數量上限	決定在此 vCenter Server 執行個體中，由連線伺服器管理的虛擬機器上可執行的並行電源作業 (啟動、關閉、暫止等) 數目上限。 預設值為 50。 如需計算此設定之值的指導方針，請參閱設定並行電源作業率以支援遠端桌面平台登入風暴。 此設定適用於完整虛擬機器和連結複製。
並行 View Composer 維護作業上限	決定可在此 View Composer 執行個體管理之連結複製上執行的並行 View Composer 重新整理、重新撰寫及重新平衡作業數目上限。 預設值為 12。 必須先登出具有使用中工作階段的遠端桌面平台，才能開始維護作業。如果維護作業一開始您就強制使用者登出，則遠端桌面平台上需要登出的並行作業數目上限為設定值的一半。例如，如果您將此設定設為 24 並強制使用者登出，則遠端桌面平台上需要登出的並行作業數目上限為 12。 此設定僅適用於連結複製。
並行 View Composer 佈建作業上限	決定可在此 View Composer 執行個體管理之連結複製上執行的並行建立與刪除作業數目上限。 預設值為 8。 此設定僅適用於連結複製。

設定並行電源作業率以支援遠端桌面平台登入風暴

並行電源作業上限設定會管理可發生在 vCenter Server 執行個體中的遠端桌面平台虛擬機器上的並行電源作業上限。依預設，此限制設定為 50。您可以在多名使用者同時登入桌面時，變更此值以支援尖峰電源開啟速率。

最佳做法是採用試驗階段，確定此設定的正確值為何。如需規劃指導方針，請參閱《Horizon 7 架構規劃》文件中的〈架構設計元素和規劃指導方針〉。

所需要的並行電源作業數量，是以桌面開啟電源的尖峰速率，以及桌面開啟電源、開機、可供連線所需要的時間量為基礎。一般來說，電源作業限制的建議值是桌面啟動時所需要的總時間，乘上尖峰電源開啟速率。

例如，桌面平均需要兩到三分鐘時間來啟動。因此，並行電源作業限制應該是尖峰電源開啟速率的 3 倍。預設值 50 預計每分鐘可支援 16 個桌面的尖峰電源開啟速率。

系統最久會等候 5 分鐘讓桌面平台啟動。如果啟動時間超出此一限制，可能會發生其他錯誤。為保守起見，您可以將並行電源作業限制設定為尖峰電源開啟速率的 5 倍。依照此一保守作法，預設值 50 每分鐘可支援 10 個桌面的尖峰電源開啟速率。

登入以及後續的桌面電源開啟作業，通常會以一般分佈方式在特定的時間範圍內發生。您可以假設電源開啟發生在時間範圍中間，以大致估計尖峰電源開啟速率，在此時間範圍中，約有 40% 的電源開啟作業發生在 1/6 的時間範圍中。例如，假設使用者在上午 8:00 和上午 9:00 之間登入，時間範圍為一小時，而 40% 的登入發生在上午 8:25 和上午 8:35 的 10 分鐘之間。如果有 2,000 名使用者，其中 20% 關閉桌面電源，則 400 個桌面電源開啟作業當中，有 40% 發生在這 10 分鐘之間。尖峰電源開啟速率為每分鐘 16 個桌面。

接受預設 TLS 憑證的指紋

當您將 vCenter Server 和 View Composer 執行個體新增至 Horizon 7 時，您必須確認用於 vCenter Server 和 View Composer 執行個體的 TLS 憑證是有效的，並受到連線伺服器的信任。如果與 vCenter Server 和 View Composer 一起安裝的預設憑證仍然在適當的位置，您必須決定是否接受這些憑證的指紋。

如果使用 CA 簽署的憑證設定 vCenter Server 或 View Composer 執行個體，且根憑證受到連線伺服器的信任，則您不需要接受憑證指紋。您不需要執行任何動作。

如果您將預設憑證取代為 CA 簽署的憑證，但連線伺服器不信任根憑證，則您必須決定是否接受憑證指紋。指紋是憑證的密碼編譯雜湊。指紋用來快速判斷所呈現的憑證是否與另一個憑證 (例如先前接受的憑證) 相同。

備註 如果您在相同的 Windows Server 主機上安裝 vCenter Server 和 View Composer，則它們可以使用相同的 TLS 憑證，但是您必須為每個元件個別設定憑證。

如需關於設定 TLS 憑證的詳細資料，請參閱 第 8 章 設定 Horizon 7 Server 的 TLS 憑證。

您可以使用「新增 vCenter Server」精靈，先在 Horizon Administrator 中新增 vCenter Server 和 View Composer。如果憑證不受信任，而且您不接受指紋，您將無法新增 vCenter Server 和 View Composer。

新增這些伺服器之後，您可以在「編輯 vCenter Server」對話方塊中重新設定這些伺服器。

備註 當您從舊版升級，且 vCenter Server 或 View Composer 憑證不受信任時，或您將受信任的憑證取代成不受信任的憑證時，您也必須接受憑證指紋。

在 Horizon Administrator 儀表板上，vCenter Server 或 View Composer 圖示會變成紅色，而且會出現 [偵測到無效的憑證] 對話方塊。在 Horizon Administrator 中，按一下 **View 組態 > 伺服器**，然後編輯與 View Composer 服務相關聯的 vCenter Server 項目。然後，在 vCenter Server 設定中按一下**編輯**，並遵循提示來確認並接受自我簽署憑證。

同樣地，您可以在 Horizon Administrator 中設定由連線伺服器執行個體所使用的 SAML 驗證器。如果 SAML 伺服器憑證不受連線伺服器信任，則您必須決定是否接受憑證指紋。如果您不接受指紋，則無法在 Horizon 7 中設定 SAML 驗證器。設定 SAML 驗證器之後，您可以在 [編輯連線伺服器] 對話方塊中重新設定該驗證器。

程序

1 當 Horizon Administrator 顯示 [偵測到無效的憑證] 對話方塊時，按一下**檢視憑證**。

2 在「憑證資訊」視窗中檢查憑證指紋。

3 檢查針對 vCenter Server 或 View Composer 執行個體設定的憑證指紋。

   a 在 vCenter Server 或 View Composer 主機上，啟動 MMC 嵌入式管理單元，並開啟「Windows 憑證存放區」。

   b 導覽至 vCenter Server 或 View Composer 憑證。

   c 按一下「憑證詳細資料」索引標籤來顯示憑證指紋。

   同樣地，檢查 SAML 驗證器的憑證指紋。如果適當，請在 SAML 驗證器主機上採取上述步驟。

4 請確認「憑證資訊」視窗中的指紋符合 vCenter Server 或 View Composer 執行個體的指紋。

   同樣地，請確認 SAML 驗證器的指紋相符。

5 決定是否接受憑證指紋。

選項	說明
指紋相符。	按一下**接受**可使用預設憑證。
指紋不符。	按一下**拒絕**。 疑難排解不相符的憑證。例如，您可能已經為 vCenter Server 或 View Composer 提供不正確的 IP 位址。

設定 Horizon Client 連線

用戶端端點會透過安全的連線與連線伺服器或安全伺服器主機進行通訊。

初始用戶端連線是使用者提供網域名稱給 Horizon Client 時透過 HTTPS 所建立，用於使用者驗證、遠端桌面平台和應用程式選取。如果您的網路環境中的防火牆和負載平衡軟體均正確設定，則這個要求會送達連線伺服器或安全伺服器主機。透過這個連線即可驗證使用者並選取桌面平台或應用程式，但是使用者尚未連線到遠端桌面平台或應用程式。

當使用者連線至遠端桌面平台和應用程式時，依預設，用戶端會二次連線至連線伺服器或安全伺服器主機。此連線稱為通道連線，因為它提供了安全的通道，可透過 HTTPS 輸送 RDP 和其他資料。

當使用者透過 PCoIP 顯示通訊協定連線至遠端桌面平台和應用程式時，用戶端會進一步連線至連線伺服器或安全伺服器主機上的 PCoIP 安全閘道。PCoIP 安全閘道可確保只有經過驗證的使用者能夠透過 PCoIP 與遠端桌面平台和應用程式進行通訊。

您也可以透過 VMware Blast 顯示通訊協定讓使用者安全連線到遠端桌面平台和應用程式，以及讓使用 HTML Access 的外部使用者安全連線到遠端桌面平台。Blast 安全閘道會確保只有經過驗證的使用者能夠與遠端桌面平台通訊。

根據正在使用的用戶端裝置類型，可能會建立其他通道來載送其他流量，如流向用戶端裝置的 USB 重新導向資料。這些資料通道會透過安全通道 (如果已啟用) 來路由傳送流量。

安全通道和安全閘道停用時，將會在用戶端裝置與遠端機器之間直接建立桌面平台和應用程式工作階段，而略過連線伺服器或安全伺服器主機。這種連線類型稱為直接連線。

即使連線伺服器不再執行，使用直接連線的桌面平台和應用程式工作階段仍會保持連線。

通常，為了提供安全的連線給透過 WAN 連線至安全伺服器或連線伺服器主機的外部用戶端，您會同時啟用安全通道、PCoIP 安全閘道和 Blast 安全閘道。您可以停用安全通道和安全閘道，讓內部 LAN 連線的用戶端建立與遠端桌面平台和應用程式的直接連線。

如果僅啟用安全通道或一個安全閘道，工作階段可能會視所使用的用戶端類型，針對部分流量使用直接連線，而其他流量則透過連線伺服器或安全伺服器主機傳送。

所有連線伺服器和安全伺服器主機的用戶端連線都需要 SSL。

設定 PCoIP 安全閘道和安全通道連線

您可以使用 Horizon Administrator 設定並啟用安全通道和 PCoIP 安全閘道。這些元件可確保只有經過驗證的使用者可以與遠端桌面平台及應用程式進行通訊。

使用 PCoIP 顯示通訊協定的用戶端可以使用 PCoIP 安全閘道。使用 RDP 顯示通訊協定的用戶端可以使用安全通道。

如需設定 Blast 安全閘道的相關資訊，請參閱設定 Blast 安全閘道。

重要 對外部用戶端提供安全連線的一般網路組態包括安全伺服器。若要啟用或停用安全伺服器上的安全通道和 PCoIP 安全閘道，您必須編輯與安全伺服器配對的連線伺服器執行個體。

在外部用戶端直接連線至連線伺服器主機的網路組態中，您可以在 Horizon Administrator 中編輯該連線伺服器執行個體，以啟用或停用安全通道和 PCoIP 安全閘道。

必要條件

- 如果您打算啟用 PCoIP 安全閘道，請確認連線伺服器執行個體和配對的安全伺服器均為 View 4.6 或更新版本。
- 如果連線伺服器執行個體上已啟用 PCoIP 安全閘道，則將安全伺服器與其配對時，請確認安全伺服器為 View 4.6 或更新版本。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 伺服器**。

2 在 [連線伺服器] 面板中選取連線伺服器執行個體，然後按一下**編輯**。

3 設定如何使用安全通道。

選項	說明
停用安全通道	取消選取**使用安全通道連線到機器**。
啟用安全通道	選取**使用安全通道連線到機器**。

預設為啟用安全通道。

4 設定如何使用 PCoIP 安全閘道。

選項	說明
啟用 PCoIP 安全閘道	選取**使用 PCoIP 安全閘道與機器進行 PCoIP 連線**。
停用 PCoIP 安全閘道	取消選取**使用 PCoIP 安全閘道與機器進行 PCoIP 連線**。

預設為停用 PCoIP 安全閘道。

5 按一下**確定**儲存變更。

設定 Blast 安全閘道

在 Horizon Administrator 中，可透過 HTML Access 或使用 VMware Blast 顯示通訊協定的用戶端連線，來設定使用 Blast 安全閘道安全存取遠端桌面平台和應用程式。

Blast 安全閘道包含 Blast Extreme Adaptive Transport (BEAT) 網路功能，它會根據網路情況 (例如不同的速度和封包遺失) 進行動態調整。

- Blast 安全閘道僅在 Unified Access Gateway 應用裝置上執行時，才支援 BEAT 網路功能。
- 連線至 Unified Access Gateway 應用裝置 3.3 版或更新版本時，可以在 TCP 連接埠 8443 和 UDP 連接埠 8443 (適用於 BEAT) 上並行處理使用 IPv4 的 Horizon Client 和使用 IPv6 的 Horizon Client。
- 使用一般網路狀況的 Horizon Client，則必須連線至連線伺服器 (已停用 BSG)、安全伺服器 (已停用 BSG)，或高於 2.8 版的 Unified Access Gateway 應用裝置。如果 Horizon Client 使用一般網路狀況來連線至連線伺服器 (已啟用 BSG)、安全伺服器 (已啟用 BSG)，或低於 2.8 版的 Unified Access Gateway 應用裝置，則用戶端會自動感應網路狀況，並回復為 TCP 網路功能。
- 使用網路狀況極差的 Horizon Client 必須連線至 2.9 版或更新版本的 Unified Access Gateway 應用裝置 (已啟用 UDP 通道伺服器)。如果 Horizon Client 使用極差的網路狀況來連線至連線伺服器 (已啟用 BSG)、安全伺服器 (已啟用 BSG)，或低於 2.8 版的 Unified Access Gateway 應用裝置，則用戶端會自動感應網路狀況，並回復為 TCP 網路功能。
- 如果 Horizon Client 使用極差的網路狀況連線至連線伺服器 (BSG 已停用)、安全伺服器 (BSG 已停用)，2.9 版或更新版本的 Unified Access Gateway 應用裝置 (未啟用 UDP 通道伺服器)，或 2.8 版的 Unified Access Gateway 應用裝置，則用戶端會自動感應網路狀況，並回復為一般網路狀況。

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。

備註 您也可以使用 Unified Access Gateway 應用裝置 (而非安全伺服器) 從外部安全存取 Horizon 7 伺服器和桌面平台。如果使用 Unified Access Gateway 應用裝置，您必須停用連線伺服器執行個體上的安全閘道，並在 Unified Access Gateway 應用裝置上啟用這些閘道。如需詳細資訊，請參閱《部署及設定 Unified Access Gateway》。

當 Blast 安全閘道未啟用時，用戶端裝置和用戶端網頁瀏覽器會使用 VMware Blast Extreme 通訊協定直接連線到遠端桌面平台虛擬機器和應用程式，而略過 Blast 安全閘道。

重要 對外部使用者提供安全連線的一般網路組態包括安全伺服器。若要啟用或停用安全伺服器上的 Blast 安全閘道，您必須編輯與安全伺服器配對的連線伺服器執行個體。如果外部使用者直接連線至連線伺服器主機，那麼若要啟用或停用 Blast 安全閘道，則需編輯該連線伺服器執行個體。

必要條件

如果使用者使用 VMware Identity Manager 來選取遠端桌面平台，請確認 VMware Identity Manager 已安裝並設定為與連線伺服器搭配使用，且該連線伺服器已與 SAML 2.0 驗證伺服器配對。

程序

1. 在 Horizon Administrator 中，選取 **View 組態 > 伺服器**。
2. 在**連線伺服器**索引標籤上，選取連線伺服器執行個體，然後按一下**編輯**。
3. 設定如何使用 Blast 安全閘道。

選項	說明
啟用 Blast 安全閘道	選取**使用 Blast 安全閘道，以透過 Blast 連線至機器**
為 HTML Access 啟用 Blast 安全閘道	選取**僅將 Blast 安全閘道用於對機器的 HTML Access Blast 連線**
停用 Blast 安全閘道	選取**不使用 Blast 安全閘道**

   Blast 安全閘道預設為啟用。

4. 按一下**確定**儲存變更。

設定安全閘道和通道連線的外部 URL

若要使用安全通道，用戶端系統必須能夠存取 IP 位址，或是可解析為 IP 位址的完整網域名稱 (FQDN)，如此用戶端才能連接連線伺服器或安全伺服器主機。

若要使用 PCoIP 安全閘道，用戶端必須使用 URL 連線至連線伺服器或安全伺服器主機。在 IPv4 環境下，URL 必須依 IP 位址識別主機。在 IPv6 環境下，URL 可以依 IP 位址或 FQDN 識別主機。

若要使用 Blast 安全閘道，使用者的端點裝置必須能夠存取可解析為 IP 位址的 FQDN，讓使用者的網頁瀏覽器或電腦能夠連接連線伺服器或安全伺服器主機。

使用來自外部位置的通道連線

依預設，連線伺服器或安全伺服器主機只能由位於相同網路內、因而能夠找到所要求之主機的通道用戶端來聯繫。

許多組織會要求使用者能夠從外部位置使用特定 IP 位址或用戶端可解析的網域名稱及特定連接埠連線。這項資訊不一定類似於連線伺服器或安全伺服器主機的實際位址和連接埠號碼。這項資訊會以 URL 的形式提供給用戶端系統。例如：

- `https://view-example.com:443`
- `https://view.example.com:443`

- `https://example.com:1234`
- `https://10.20.30.40:443`

若要在 Horizon 7 中使用這類位址，您必須設定連線伺服器或安全伺服器主機，使其傳回外部 URL，而不是主機的 FQDN。

設定外部 URL

您要設定多個外部 URL。第一個 URL 可讓用戶端系統進行通道連線。第二個 URL 可讓使用 PCoIP 的用戶端透過 PCoIP 安全閘道進行安全連線。在 IPv4 環境下，URL 必須依 IP 位址識別主機。在 IPv6 環境下，URL 可以依 IP 位址或 FQDN 識別主機。URL 可讓用戶端從外部位置進行連線。

第三個 URL 可讓使用者透過 Blast 安全閘道從其用戶端裝置或網頁瀏覽器進行安全連線。

如果您的網路組態包含安全伺服器，請提供安全伺服器的外部 URL。與安全伺服器配對的連線伺服器執行個體上不需要外部 URL。

為連線伺服器執行個體和安全伺服器設定外部 URL 的程序有所不同。

- 在連線伺服器執行個體上，您需要藉由在 Horizon Administrator 中編輯連線伺服器設定來設定外部 URL。
- 在安全伺服器上，則需要在執行連線伺服器安裝程式時設定外部 URL。您可以使用 Horizon Administrator 修改安全伺服器的外部 URL。

設定連線伺服器執行個體的外部 URL

您可以使用 Horizon Administrator 設定連線伺服器執行個體的外部 URL。

安全通道外部 URL、PCoIP 外部 URL 和 Blast 外部 URL 必須是用戶端系統用來連接此連線伺服器執行個體的位址。

必要條件

- 確認已在連線伺服器執行個體上啟用安全通道連線和 PCoIP 安全閘道。請參閱設定 PCoIP 安全閘道和安全通道連線。
- 若要設定 Blast 外部 URL，請確認已在連線伺服器執行個體上啟用 Blast 安全閘道。請參閱設定 Blast 安全閘道。

程序

1. 在 Horizon Administrator 中，按一下 **View 組態 > 伺服器**。
2. 依序選取 [連線伺服器] 索引標籤和連線伺服器執行個體，然後按一下**編輯**。
3. 在**外部 URL** 文字方塊中輸入安全通道外部 URL。

   URL 必須包含通訊協定、用戶端可解析的主機名稱與連接埠號碼。

例如：**https://myserver.example.com:443**

備註 主機名稱無法解析時，如果您必須存取連線伺服器執行個體，則可以使用 IP 位址。不過，您聯繫的主機將不符合為連線伺服器執行個體設定的 TLS 憑證，因而導致存取遭封鎖，或只能在安全性降低的情況下存取。

4 在 **PCoIP 外部 URL** 文字方塊中輸入 PCoIP 安全閘道外部 URL。

在 IPv4 環境中，將包含連接埠號碼 4172 的 PCoIP 外部 URL 指定為 IP 位址。在 IPv6 環境中，您可以指定 IP 位址或完整網域名稱，以及連接埠號碼 4172。無論在哪種環境下，請勿包含通訊協定名稱。

例如，在 IPv4 環境下，指定：`10.20.30.40:4172`

用戶端必須能夠使用 URL 連線安全伺服器。

5 在 **Blast 外部 URL** 文字方塊中輸入 Blast 安全閘道外部 URL。

URL 必須包含 HTTPS 通訊協定、用戶端可解析的主機名稱，以及連接埠號碼。

例如：`https://myserver.example.com:8443`

依預設，URL 包含安全通道外部 URL 的 FQDN 和預設連接埠號碼 8443。URL 必須包含用戶端系統可用來連線此連線伺服器主機的 FQDN 和連接埠號碼。

6 確認此對話方塊中的所有位址皆允許用戶端系統連接此連線伺服器執行個體。

7 按一下**確定**。

修改安全伺服器的外部 URL

您可以使用 Horizon Administrator 修改安全伺服器的外部 URL。

這些外部 URL 是一開始您在連線伺服器安裝程式中安裝安全伺服器時所設定。

安全通道外部 URL、PCoIP 外部 URL 和 Blast 外部 URL 必須是用戶端系統用來聯繫此安全伺服器的位址。

必要條件

- 確認已在與此安全伺服器配對的連線伺服器執行個體上啟用安全通道連線和 PCoIP 安全閘道。請參閱設定 PCoIP 安全閘道和安全通道連線。
- 若要設定 Blast 外部 URL，請確認已在與此安全伺服器配對的連線伺服器執行個體上啟用 Blast 安全閘道。請參閱設定 Blast 安全閘道。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 伺服器**。

2 選取「安全伺服器」索引標籤，選取安全伺服器，然後按一下**編輯**。

3 在**外部 URL** 文字方塊中輸入安全通道外部 URL。

URL 必須包含通訊協定、用戶端可解析的安全伺服器主機名稱，以及連接埠號碼。

例如：`https://myserver.example.com:443`

備註 主機名稱無法解析時，如果您必須存取安全伺服器，可以使用 IP 位址。不過，您聯繫的主機將不符合針對安全伺服器設定的 TLS 憑證，因而導致存取遭封鎖，或只能在降低安全性的情況下存取。

4 在 **PCoIP 外部 URL** 文字方塊中輸入 PCoIP 安全閘道外部 URL。

在 IPv4 環境中，將包含連接埠號碼 4172 的 PCoIP 外部 URL 指定為 IP 位址。在 IPv6 環境下，您可以指定 IP 位址或網域名稱，以及連接埠號碼 4172。無論在哪種環境下，請勿包含通訊協定名稱。

例如，在 IPv4 環境下，指定：`10.20.30.40:4172`

用戶端必須能夠使用 URL 連線安全伺服器。

5 在 **Blast 外部 URL** 文字方塊中輸入 Blast 安全閘道外部 URL。

URL 必須包含 HTTPS 通訊協定、用戶端可解析的主機名稱，以及連接埠號碼。

例如：`https://myserver.example.com:8443`

根據預設，URL 包含安全通道外部 URL 的 FQDN 以及預設連接埠號碼 8443。URL 必須包含用戶端系統可以用來聯繫安全伺服器的 FQDN 和連接埠號碼。

6 確認此對話方塊中的所有位址皆允許用戶端系統連線此安全伺服器主機。

7 按一下**確定**儲存變更。

Horizon Administrator 會將更新的外部 URL 傳送至安全伺服器。您不需要重新啟動安全伺服器服務，變更就會生效。

當 Horizon 連線伺服器傳回位址資訊時，優先使用 DNS 名稱

依預設，將桌面平台機器和 RDS 主機的位址傳送至用戶端和閘道時，Horizon 連線伺服器會優先使用 IP 位址。您可以將此預設行為變更為 Horizon 7 LDAP 屬性，以告知 Horizon 連線伺服器優先使用 DNS 名稱。在某些環境下，讓連線伺服器將 DNS 名稱傳回到用戶端和閘道，可在設計網路基礎結構時提供更多彈性。

備註 在 Horizon 6.0.*x* 及舊版中，此 Horizon 7 LDAP 屬性將取代群組原則設定提供的每個桌面平台功能並 `Connect using DNS Name`。

Horizon 7 LDAP 屬性會影響在連線伺服器執行個體 (非安全伺服器) 上執行 Windows 版 Horizon Client 3.3 或更新版本、HTML Access 3.5 或更新版本以及安全閘道的用戶端。

必要條件

如需如何在 Windows Server 作業系統版本使用 ADSI Edit 公用程式的資訊，請參閱 Microsoft TechNet 網站。

程序

1 在連線伺服器電腦上啟動 ADSI Edit 公用程式。

2 在主控台樹狀結構中，選取**連線至**。

3 在**選取或輸入辨別名稱或命名內容**文字方塊中，輸入辨別名稱 **DC=vdi, DC=vmware, DC=int**。

4 在**選取或輸入網域或伺服器**文字方塊中，選取或輸入 **localhost:389**，或連線伺服器電腦的完整網域名稱 (FQDN) 後面再加上連接埠 389。

例如：`localhost:389` 或 `mycomputer.mydomain.com:389`

5 在物件 **CN=Common, OU=Global, OU=Properties** 中，將 **pae-PreferDNS** 屬性值設為 1。

當此屬性設為 1 時，連線伺服器會傳回 DNS 名稱 (如果 DNS 名稱可用，且接收者支援名稱解析)。如果有適合您環境的正確 IP 位址類型 (IPv4 或 IPv6) 可用，則連線伺服器會傳回 IP 位址。

當此屬性未設定或設為 0 時，連線伺服器會傳回 IP 位址 (如果有正確類型的 IP 位址可用)。否則，將傳回 IP 位址相容性錯誤。

允許透過負載平衡器進行 HTML Access

當使用者使用 HTML Access 時，直接位在負載平衡器或負載平衡閘道後方的連線伺服器執行個體和安全伺服器必須知道瀏覽器用來連線至負載平衡器的位址。

針對直接位在閘道後方的連線伺服器執行個體和安全伺服器，請執行允許透過閘道進行 HTML Access 中說明的程序。

您必須對位在負載平衡器或負載平衡閘道後方的每個 Horizon 7 Server 執行此程序。

程序

1 在連線伺服器或安全伺服器主機上的 SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 新增 `balancedHost` 內容並將它設為負載平衡器的位址。

例如，如果使用者在瀏覽器中輸入 **https://view.example.com** 以連線到任何負載平衡的 Horizon 7 Server，請將 `balancedHost=view.example.com` 新增至 `locked.properties` 檔案。

3 儲存 `locked.properties` 檔案。

4 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

允許透過閘道進行 HTML Access

當使用者使用 HTML Access 時，直接位在閘道 (例如 Access Point) 後方的連線伺服器執行個體和安全伺服器必須知道瀏覽器用來連線至閘道的位址。

針對位在負載平衡器或負載平衡閘道後方的連線伺服器執行個體和安全伺服器，請執行允許透過負載平衡器進行 HTML Access 中說明的程序。

您必須對位在閘道後方的每個 Horizon 7 Server 執行此程序。

程序

1 在連線伺服器或安全伺服器主機上的 SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties

2 新增 `portalHost` 內容並將它設為閘道的位址。

例如，如果 `https://view-gateway.example.com` 是瀏覽器用來透過閘道存取 Horizon 7 的位址，請將 `portalHost=view-gateway.example.com` 新增至 `locked.properties` 檔案。

如果連線伺服器執行個體或安全伺服器位於多個閘道的後方，您可以藉由將數字新增至 `portalHost` 屬性，來指定每個閘道，例如：

```
portalHost.1=view-gateway-1.example.com
portalHost.2=view-gateway-2.example.com
```

如果單一閘道機器已知有不只一個名稱，您也必須指定多個 `portalHost` 內容。

3 儲存 `locked.properties` 檔案。

4 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

取代 Horizon 7 服務的預設連接埠

在安裝期間，View 服務預設設為接聽特定網路連接埠。在某些組織中，必須變更這些連接埠以遵守組織政策或避免爭論。您可以變更連線伺服器、安全伺服器、PCoIP 安全閘道和 View Composer 服務所使用的預設連接埠。

變更連接埠是選用的設定工作。如果您的部署不要求您變更連接埠，請使用預設連接埠。

如需 Horizon 7 Server 所使用預設 TCP 和 UDP 連接埠的清單，請參閱《Horizon 7 安全性》文件。

取代 Horizon 連線伺服器執行個體和安全伺服器的預設 HTTP 連接埠或 NIC

您可以編輯伺服器電腦上的 `locked.properties` 檔案，以取代連線伺服器執行個體或安全伺服器的預設 HTTP 連接埠或 NIC。您的組織可能會要求您執行這些工作，以遵守組織政策或避免爭論。

預設的 SSL 連接埠為 443。預設的非 SSL 連接埠為 80。

在此程序中變更連接埠之後，安全通道外部 URL 中指定的連接埠不會變更。根據您的網路組態而定，您可能也需要變更安全通道外部 URL 連接埠。

如果伺服器電腦有多個 NIC，則電腦預設會接聽所有 NIC。您可以指定繫結至某個 NIC 的 IP 位址，藉以選取該 NIC 接聽已設定的連接埠。

在安裝期間，Horizon 7 會設定 Windows 防火牆開放所需的預設連接埠。如果您變更連接埠號碼或所接聽的 NIC，則必須手動重新設定 Windows 防火牆，開放更新的連接埠，讓用戶端裝置可以連線到伺服器。

如果變更 SSL 連接埠號碼且需要 HTTP 重新導向繼續運作，則還需要變更 HTTP 重新導向的連接埠號碼。請參閱變更連接埠號碼以讓 HTTP 重新導向至連線伺服器。

必要條件

確認在此程序中變更連接埠之後，此連線伺服器執行個體或安全伺服器的外部 URL 中指定的連接埠將繼續有效。

程序

1 在連線伺服器或安全伺服器電腦上的 SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties

`locked.properties` 檔案中的屬性區分大小寫。

2 將 `serverPort` 或 `serverPortNonSsl` 屬性或這兩個屬性新增到 `locked.properties` 檔案中。

例如：

```
serverPort=4443
serverPortNonSsl=8080
```

3 (選擇性) 如果伺服器電腦有多個 NIC，請選取一個 NIC 來接聽已設定的連接埠。

新增 `serverHost` 和 `serverHostNonSsl` 屬性，以指定繫結至指定 NIC 的 IP 位址。

例如：

```
serverHost=10.20.30.40
serverHostNonSsl=10.20.30.40
```

通常，SSL 和非 SSL 接聽程式都會設為使用相同的 NIC。不過，如果您使用 `serverProtocol=http` 屬性卸載 SSL 以進行用戶端連線，您可以將 `serverHost` 屬性設為不同的 NIC，以便為用來啟動 Horizon Administrator 的系統提供 SSL 連線。

如果您設定 SSL 和非 SSL 連線使用相同的 NIC，則 SSL 和非 SSL 連接埠不得相同。

4 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

後續步驟

必要時，請手動設定 Windows 防火牆開放更新的連接埠。

在 Horizon 連線伺服器執行個體和安全伺服器上，取代 PCoIP 安全閘道的預設連接埠或 NIC。

您可以取代在連線伺服器執行個體或安全伺服器上執行的 PCoIP 安全閘道所使用的預設連接埠或 NIC。您的組織可能會要求您執行這些工作，以遵守組織政策或避免爭論。

若是用戶端對向的 TCP 和 UDP 連線，PCoIP 安全閘道預設會接聽連接埠 4172。若是 UDP 連線至遠端桌面平台，則 PCoIP 安全閘道會預設接聽連接埠 55000。

在此程序中變更連接埠之後，PCoIP 外部 URL 中指定的連接埠不會變更。根據您的網路組態而定，您可能也需要變更 PCoIP 外部 URL 連接埠。

如果執行 PCoIP 安全閘道所在的電腦有多個 NIC，則電腦預設會接聽所有 NIC。您可以指定繫結至某個 NIC 的 IP 位址，藉以選取該 NIC 接聽已設定的連接埠。

必要條件

請確認在此程序中變更連接埠之後，連線伺服器執行個體或安全伺服器上的 PCoIP 外部 URL 中指定的連接埠將繼續有效。

程序

1 在執行 PCoIP 安全閘道的連線伺服器或安全伺服器電腦上，啟動 Windows 登錄編輯程式。

2 導覽至 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` 登錄機碼。

3 在此登錄機碼底下，使用您更新的連接埠號碼，新增下列一或多個 String (`REG_SZ`) 值。

例如：

```
ExternalTCPPort "44172"
ExternalUDPPort "44172"
InternalUDPPort "55111"
```

4 (選擇性) 如果執行 PCoIP 安全閘道所在的電腦有多個 NIC，請選取一個 NIC 接聽已設定的連接埠。

在相同的登錄機碼底下，新增下列 String (`REG_SZ`) 值，以指定繫結至指定 NIC 的 IP 位址。

例如：

```
ExternalBindIP "10.20.30.40"
InternalBindIP "172.16.17.18"
```

如果您設定外部和內部連線使用相同的 NIC，則外部和內部 UDP 連接埠不得相同。

5 重新啟動 VMware Horizon View PCoIP 安全閘道服務，讓您的變更生效。

在連線伺服器執行個體和安全伺服器上，取代 PCoIP 安全閘道的預設控制連接埠

您可以取代用來控制在連線伺服器執行個體或安全伺服器上執行之 PCoIP 安全閘道 (PSG) 服務的預設連接埠。您可能需要執行此工作以避免連接埠爭用。

PCoIP 安全閘道依預設會在本機 TCP 連接埠 50060 上接聽控制連線。

程序

1 在執行 PCoIP 安全閘道的連線伺服器或安全伺服器電腦上的 SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

`locked.properties` 檔案中的屬性區分大小寫。

2 將 psgControlPort 屬性新增至 locked.properties 檔案。

例如：

```
psgControlPort=52060
```

3 在相同機器上啟動 Windows 登錄編輯程式。

4 導覽至 HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway 登錄機碼。

5 在此登錄機碼底下，使用您更新的連接埠號碼，新增下列字串 (REG_SZ) 值。

例如：

```
TCPControlPort "52060"
```

備註 TCPControl Port 與 psgControlPort 的連接埠號碼相同。

6 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

取代 View Composer 的預設連接埠

View Composer 服務所使用的 SSL 憑證預設會繫結至特定的連接埠。您可以使用 SviConfig ChangeCertificateBindingPort 公用程式來取代預設的連接埠。

當您使用 SviConfig ChangeCertificateBindingPort 公用程式指定新的連接埠時，此公用程式會從目前的連接埠取消繫結 View Composer 憑證，然後將其繫結至新的連接埠。

在安裝期間，View Composer 會設定 Windows 防火牆開放所需的預設連接埠。如果變更連接埠，您必須手動重新設定 Windows 防火牆開放更新的連接埠，並確保與 View Composer 服務的連線。

必要條件

請確認您指定的連接埠可以使用。

程序

1 停止 View Composer 服務。

2 在安裝 View Composer 的 Windows Server 主機上開啟命令提示字元。

3 導覽至 SviConfig 可執行檔。

該檔案與 View Composer 應用程式位於同一個位置。預設路徑為 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe。

4 輸入 SviConfig ChangeCertificateBindingPort 命令。

例如：

```
sviconfig –operation=ChangeCertificateBindingPort
          –Port=連接埠編號
```

其中 –port=*port number* 是 View Composer 繫結憑證的新連接埠。需要 –port=*port number* 參數。

5 重新啟動 View Composer 服務讓變更生效。

後續步驟

必要時，請手動重新設定 View Composer Server 上的 Windows 防火牆，開放更新的連接埠。

變更連接埠號碼以讓 HTTP 重新導向至連線伺服器

如果您要取代 Horizon 7 Server 上的預設連接埠 443，並想允許嘗試連線至連接埠 80 的 Horizon Client 進行 HTTP 重新導向，您必須設定 Horizon 7 Server 上的 `locked.properties` 檔案。

備註 如果您將 SSL 卸載至中繼裝置，此程序將無作用。SSL 卸載完成後，Horizon 7 Server 上的 HTTP 連接埠便會提供服務給用戶端。

必要條件

確認您已從 443 變更預設連接埠號碼。如果您使用安裝期間設定的預設值，則不需要執行此程序來保留 HTTP 重新導向規則。

程序

1 在連線伺服器或安全伺服器電腦上的 SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties

`locked.properties` 檔案中的屬性區分大小寫。

2 將下列幾行新增到 `locked.properties` 檔案：

```
frontMappingHttpDisabled.1=5:*:moved:https::port
frontMappingHttpDisabled.2=3:/error/*:file:docroot
frontMappingHttpDisabled.3=1:/admin*:missing
frontMappingHttpDisabled.4=1:/view-vlsi*:missing
```

在前面幾行中，變數 *port* 是用戶端應連線的連接埠號碼。

如果不新增前面幾行，*port* 仍會是 443。

3 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

阻止用戶端連線的 HTTP 重新導向至連線伺服器

Horizon Client 透過 HTTP 連線至 Horizon 7 Server 的嘗試會以無訊息方式重新導向至 HTTPS。在某些部署中，您可能會想防止使用者在網頁瀏覽器中輸入 **http://**，強制他們使用 HTTPS。若要防止 Horizon Client 進行 HTTP 重新導向，您必須在 Horizon 7 Server 上設定 `locked.properties` 檔案。

備註 如果您將 SSL 卸載至中繼裝置，此程序將無作用。SSL 卸載完成後，Horizon 7 Server 上的 HTTP 連接埠便會提供服務給用戶端。

程序

1 在連線伺服器或安全伺服器電腦上的 SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties

`locked.properties` 檔案中的屬性區分大小寫。

2 將下列幾行新增到 `locked.properties` 檔案：

```
frontMappingHttpDisabled.1=5:*:missing
frontMappingHttpDisabled.2=3:/error/*:file:docroot
```

3 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

啟用對連線伺服器上 Horizon 7 效能計數器的遠端存取

Horizon 7 效能計數器在連線伺服器本機上可用，但從其他電腦存取時會傳回 0。若要啟用對連線伺服器上 Horizon 7 效能計數器的遠端存取，您必須在登錄中設定連線伺服器的架構連接埠。

程序

1 啟動 Windows 登錄編輯程式。

2 導覽至 `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager` 登錄機碼。

3 新增字串 (REG_SZ) 值 `Management Port`。

4 將 `Management Port` 值設為 **32111**。

調整 Windows Server 設定以支援您的部署

若要支援遠端桌面平台的大型部署，您可以設定連線伺服器安裝所在的 Windows Server 電腦。在每部電腦上，您可以調整 Windows 分頁檔的大小。

在 Windows Server 2008 R2 和 Windows Server 2012 R2 電腦上，暫時連接埠、TCB 雜湊資料表和 Java 虛擬機器設定都會依預設調整大小。這些調整可確保電腦擁有適當的資源，可在預期的使用者負載下正確執行。

調整 Horizon 連線伺服器的記憶體大小

在連線伺服器電腦上，部署 50 個或更多遠端桌面平台必須要有 10 GB 的記憶體。具有至少 10 GB 記憶體的 Windows Server 電腦會自動設定為支援大約 2000 個並行通道工作階段，這是連線伺服器可支援的數目上限。

僅設定 10GB 以下的記憶體，供小型的概念驗證部署使用。如果擁有 4GB 的最少必要記憶體，則組態可支援大約 500 個並行通道工作階段，這對於小型的概念驗證部署來說綽綽有餘。

但是，部署可能會由於更多的使用者被新增至環境而變大，因此，VMware 建議您始終設定至少 10GB 的記憶體。請僅在瞭解環境不會增長且無可用記憶體時允許例外情況。

如果您以小於 10 GB 的記憶體安裝連線伺服器，則 Horizon 7 將在安裝完成後產生警告訊息，以提供記憶體建議。此時會有每 12 小時觸發一次的事件，指出用來設定連線伺服器執行個體的實體記憶體數量太小。

如果將電腦的記憶體增加到 10 GB 以支援較大的部署，請重新啟動連線伺服器，並確定 JVM 堆積大小已自動增加至建議值。您不需要重新安裝連線伺服器。

重要 請勿變更 64 位元 Windows Server 電腦上的 JVM 堆積大小。變更此值可能會使連線伺服器行為變得不穩定。在 64 位元電腦上，連線伺服器服務會將 JVM 堆積大小設為符合實體記憶體的大小。

如需連線伺服器的其他硬體和記憶體需求，請參閱 Horizon 連線伺服器的硬體需求。

如需在大型部署中使用連線伺服器的硬體和記憶體建議，請參閱《Horizon 7 架構規劃》中的〈連線伺服器最大值和虛擬機器組態〉。

設定系統分頁檔設定

您可以藉由變更系統分頁檔設定，將連線伺服器執行個體安裝所在 Windows Server 電腦上的虛擬記憶體最佳化。

安裝 Windows Server 時，Windows 會根據電腦上安裝的實體記憶體來計算初始與最大分頁檔大小。即使在重新啟動電腦之後，這些預設設定仍會維持固定。

如果 Windows Server 電腦是虛擬機器，您可以透過 vCenter Server 變更記憶體大小。不過，如果 Windows 使用預設設定，系統分頁檔大小就不會調整為新的記憶體大小。

程序

1 在連線伺服器安裝所在的 Windows Server 電腦上，導覽到 [虛擬記憶體] 對話方塊。

預設會選取**自訂大小**。接著會出現初始及最大分頁檔大小。

2 按一下**系統管理大小**。

Windows 會根據目前的記憶體使用量及可用的記憶體，持續重新計算系統分頁檔大小。

設定事件報告

10

您可以建立一個事件資料庫，用於記錄 Horizon 7 事件的相關資訊。此外，如果您使用 Syslog 伺服器，則可以設定連線伺服器將事件傳送至 Syslog 伺服器，或建立以 Syslog 格式寫入之事件的一般檔案。

本章節討論下列主題：

新增 Horizon 7 事件的資料庫和資料庫使用者

您可以透過將事件資料庫新增到現有的資料庫伺服器來建立該事件資料庫。接著，您可以使用 Enterprise Reporting 軟體分析資料庫中的事件。

在專用伺服器上部署事件資料庫的資料庫伺服器，以便事件記錄活動不會影響佈建和對 Horizon 7 部署非常重要的其他活動。

備註 您不需要建立此資料庫的 ODBC 資料來源。

必要條件

- 確認您在連線伺服器執行個體可存取的系統上，具有支援的 Microsoft SQL Server 或 Oracle 資料庫伺服器。如需支援的資料庫版本清單，請參閱 View Composer 和事件資料庫的資料庫需求。
- 請確認您擁有在資料庫伺服器上建立資料庫和使用者所需的資料庫權限。
- 如果您不熟悉在 Microsoft SQL Server 資料庫伺服器上建立資料庫的程序，請檢閱將 View Composer 資料庫新增到 SQL Server 中中的步驟。
- 如果您不熟悉在 Oracle 資料庫伺服器上建立資料庫的程序，請檢閱將 View Composer 資料庫新增到 Oracle 12c 或 11g 中中的步驟。

程序

1 將新的資料庫新增至伺服器，並為其提供描述性名稱，例如 HorizonEvents。

對於 Oracle 12c 或 11g 資料庫，也請提供 Oracle 系統識別碼 (SID)，當您在 Horizon Administrator 中設定事件資料庫時將會用到此識別碼。

2 為此資料庫新增擁有建立資料表、檢視以及 (若是 Oracle) 觸發程序與序列之權限的使用者，以及從這些物件讀取或寫入這些物件之權限的使用者。

若是 Microsoft SQL Server 資料庫，請不要使用「整合式 Windows 驗證」安全性模型驗證方法。請務必使用「SQL Server 驗證」驗證方法。

系統會建立資料庫，但在 Horizon Administrator 中設定資料庫之前，並不會安裝結構描述。

後續步驟

請依照設定事件資料庫中的指示進行。

準備用於事件報告的 SQL Server 資料庫

您必須先設定正確的 TCP/IP 內容，並確認伺服器使用 SQL Server 驗證，才能使用 Horizon Administrator 在 Microsoft SQL Server 上設定事件資料庫。

必要條件

- 建立用於事件報告的 SQL Server 資料庫。請參閱 新增 Horizon 7 事件的資料庫和資料庫使用者。
- 確認您擁有設定資料庫的必要資料庫權限。
- 確認資料庫伺服器使用 SQL Server 驗證方法進行驗證。請勿使用 Windows 驗證。

程序

1 開啟「SQL Server 組態管理員」，並展開 **SQL Server *YYYY* 網路組態**。

2 選取 ***server_name* 的通訊協定**。

3 在通訊協定清單中，以滑鼠右鍵按一下 **TCP/IP** 並選取**內容**。

4 將**已啟用**內容設為**是**。

5 確認已指定連接埠，必要時請指定一個連接埠。

如需靜態和動態連接埠及如何指定連接埠的相關資訊，請參閱 SQL Server 組態管理員的線上說明。

6 確認此連接埠未遭到防火牆封鎖。

後續步驟

使用 Horizon Administrator 將資料庫連線至連線伺服器。請依照設定事件資料庫中的指示操作。

設定事件資料庫

事件資料庫會將 Horizon 7 事件的相關資訊以記錄的形式儲存在資料庫中 (而非記錄檔中)。

在安裝連線伺服器執行個體之後，您會設定事件資料庫。您只需要在連線伺服器群組中設定一個主機。系統會自動設定群組中的其餘主機。

備註 儘管事件流量受限於 Horizon 7 環境的相關健全狀況資訊，但連線伺服器執行個體與外部資料庫之間的資料庫連線安全性是管理員的責任。如果希望採取額外的預防措施，您可以透過 IPSec 或其他方式保護此通道的安全，也可以將資料庫部署在連線伺服器電腦本機上。

您可以使用 Microsoft SQL Server 或 Oracle 資料庫報告工具檢查資料庫資料表中的事件。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，讓協力廠商分析軟體可以存取事件資料。您可以將 `vdmadmin` 命令與 `-I` 選項搭配使用，將 Horizon 7 事件訊息以 `Syslog` 格式記錄在事件記錄檔中。請參閱《Horizon 7 管理》文件中的〈使用 -I 選項以 Syslog 格式產生 Horizon 7 事件記錄訊息〉。

必要條件

您需要下列資訊才能設定事件資料庫：

- 資料庫伺服器的 DNS 名稱或 IP 位址。
- 資料庫伺服器類型：Microsoft SQL Server 或 Oracle。如需所支援資料庫伺服器的詳細資訊，請參閱 IPv6 環境中支援的 vSphere 資料庫及 Active Directory 版本。
- 用來存取資料庫伺服器的連接埠號碼。Oracle 的預設值為 1521，SQL Server 的預設值為 1433。對於 SQL Server，如果資料庫伺服器是具名執行個體，或者您使用的是 SQL Server Express，則可能必須決定連接埠號碼。請參閱有關連線至 SQL Server 具名執行個體的 Microsoft 知識庫文章，網址為：http://support.microsoft.com/kb/265808。
- 您在資料庫伺服器上建立之事件資料庫的名稱。請參閱新增 Horizon 7 事件的資料庫和資料庫使用者。

  針對 Oracle 12c 或 11g 資料庫，當您在 Horizon Administrator 中設定事件資料庫時，必須使用 Oracle 系統識別碼 (SID) 作為資料庫名稱。
- 您為此資料庫建立之使用者的使用者名稱和密碼。請參閱新增 Horizon 7 事件的資料庫和資料庫使用者。

  為此使用者使用 SQL Server 驗證。不要使用整合式 Windows 驗證的安全性模型驗證方法。
- 事件資料庫中資料表的前置詞，例如 VE_。前置詞可讓資料庫在 Horizon 7 安裝期間共用。

  備註 您必須輸入對您使用之資料庫軟體有效的字元。當您完成對話方塊時，系統不會檢查前置詞的語法。如果您輸入的字元對您所使用的資料庫軟體而言無效，當連線伺服器嘗試連線至資料庫伺服器時，將會發生錯誤。如果資料庫名稱無效，記錄檔會指出所有錯誤，包括此錯誤及從資料庫伺服器傳回的其他所有錯誤。

程序

1. 在 Horizon Administrator 中，選取 **View 組態 > 事件組態**。
2. 在**事件資料庫**區段中，按一下**編輯**，在提供的欄位中輸入資訊，再按一下**確定**。

3 (選擇性) 在「事件設定」視窗中，按一下**編輯**，變更顯示事件的時間長度，以及將事件分類為新事件的天數，然後按一下**確定**。

關於事件時間長度的這些設定會在 Horizon Administrator 介面中列出。目前只有在歷史資料庫資料表中才有事件。

「資料庫組態」視窗會顯示事件資料庫的目前組態。

4 選取**監視 > 事件**以確認與事件資料庫的連線成功。

如果連線不成功，則會出現錯誤訊息。如果您使用的是 SQL Express，或者使用的是 SQL Server 的具名執行個體，則可能必須決定正確的連接埠號碼 (如先決條件所述)。

在「Horizon Administrator 儀表板」中，「系統元件狀態」的「報告資料庫」標題下會顯示事件資料庫伺服器。

設定 Syslog 伺服器的事件記錄

您可以使用 `Syslog` 格式產生 Horizon 7 事件，讓分析軟體可以存取事件資料。

您只需要在連線伺服器群組中設定一個主機。系統會自動設定群組中的其餘主機。

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，這些記錄檔會移至該共用。

- 只有在設定期間進行快速疑難排解時 (或許是在設定事件資料庫之前) 才使用本機檔案，如此才有方法可查看事件。

  刪除最舊的檔案之前，事件記錄 (包括已關閉的記錄檔) 之本機目錄的大小上限為 300MB。Syslog 輸出的預設目的地為 `%PROGRAMDATA%\VMware\VDM\events\`。

- 如果您沒有 Syslog 伺服器，或者您目前的 Syslog 伺服器不符需求，請使用 UNC 路徑儲存長期事件記錄的記錄檔。

或者，您可以使用 `vdmadmin` 命令，以 Syslog 格式設定事件的檔案式記錄。請參閱《Horizon 7 管理》文件中，關於使用 `vdmadmin` 命令的 `-I` 選項以 Syslog 格式產生 Horizon 7 事件記錄訊息的主題。

重要 Syslog 資料會以沒有軟體式加密的方式傳送到網路上，而且可能包含敏感資料，例如使用者名稱。VMware 建議使用連結層安全性 (例如 IPSEC) 以避免此資料可能在網路上遭到監視。

必要條件

您需要使用下列資訊設定連線伺服器，才能以 Syslog 格式記錄事件和/或將事件傳送至 Syslog 伺服器：

- 如果您打算使用 Syslog 伺服器在 UDP 連接埠上接聽 Horizon 7 事件，您必須具有 Syslog 伺服器的 DNS 名稱或 IP 位址以及 UDP 連接埠號碼。預設 UDP 連接埠號碼為 514。
- 如果您打算以一般檔案格式收集記錄，則必須擁有檔案共用及儲存記錄檔所在資料夾的 UNC 路徑，而且還必須擁有使用者名稱、網域名稱，以及具備寫入檔案共用之權限的帳戶密碼。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 事件組態**。

2 (選擇性) 在 **Syslog** 區域中，若要設定連線伺服器以將事件傳送到 Syslog 伺服器，請按一下**傳送到 syslog 伺服器**旁的**新增**，並提供伺服器名稱或 IP 位址以及 UDP 連接埠號碼。

3 (選擇性) 在**事件到檔案系統**區域中，選擇是否要啟用事件記錄訊息的產生，並在記錄檔中以 Syslog 格式儲存。

選項	說明
永遠	永遠產生並在記錄檔中以 Syslog 格式儲存事件記錄訊息。
發生錯誤時記錄到檔案 (預設)	寫入事件到事件資料庫或 Syslog 伺服器發生問題時，將稽核事件記錄到記錄檔。此選項依預設為啟用。
永不	永不產生並在記錄檔中以 Syslog 格式儲存事件記錄訊息。

除非您指定檔案共用的 UNC 路徑，否則記錄檔會保留在本機上。

4 (選擇性) 若要將 Horizon 7 事件記錄訊息儲存在檔案共用上，請按一下**複製到位置**旁的**新增**，並提供要用來儲存記錄檔之檔案共用和資料夾的 UNC 路徑，以及有權寫入檔案共用之帳戶的使用者名稱、網域名稱和密碼。

以下為 UNC 路徑範例：

```
\\syslog-server\folder\file
```