Horizon 架構規劃

VMware Horizon 2103

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/

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

目錄

Horizon 架構規劃

《Horizon 架構規劃》提供 VMware Horizon™ 的簡介，其中包括主要功能和部署選項的說明，並概述在生產環境中設定元件的一般方式。

本指南提供下列問題的解答：

- 本產品是否解決您要解決的問題？

VMware Horizon 的所有功能和特性並非在所有授權版本中均可用。如需比較各版本的功能集，請參閱 https://www.vmware.com/products/horizon.html。

為協助您保護所安裝的產品，本指南也會討論安全功能。

主要對象

此資訊適用於 IT 決策者、架構設計人員、管理員，以及必須熟悉本產品元件與功能的其他人。架構設計人員和規劃人員可利用本指南中的資訊，判斷 VMware Horizon 是否可滿足其企業的需求，能夠以有效且安全的方式提供虛擬桌面平台和應用程式給其使用者。

VMware Horizon 簡介

1

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

本章節討論下列主題：

使用 VMware Horizon 的優點

VMware Horizon 的優點包括能夠利用類似於雲端的經濟效益和彈性，簡單、安全、快速且靈活地提供虛擬桌面平台和應用程式。

彈性的 VMware Horizon 部署

VMware Horizon 可讓您靈活地在內部部署、雲端主控環境，或兩者的混合環境中部署虛擬桌面平台和應用程式。不同的部署環境可能需要不同的授權。

您可以在下列環境中部署 VMware Horizon。

內部部署

VMware Horizon 可部署在內部部署的基礎結構或私有雲上。您可以對內部部署使用永久授權。您可以選擇性地購買可讓您存取 Horizon Control Plane 與相關聯服務的 Horizon 訂閱授權。

雲端主控部署

VMware Horizon 可部署在公有雲 (例如 VMware Cloud on AWS)，或 Azure VMware Solutions 中。對於公有雲中的部署，您必須使用訂閱授權。透過訂閱授權，您將可選擇存取 Horizon Control Plane 與相關聯的服務。

混合部署

您可以同時在內部部署和雲端主控環境中部署 VMware Horizon。您可以在聯盟中連結這些部署。在此混合部署案例中，您可以進行下列部署：

- 對內部部署使用永久授權，並且對雲端主控部署使用訂閱授權。
- 同時對內部部署和雲端主控部署使用訂閱授權。

將您的 Horizon 部署連線至 Horizon Control Plane

若要使用訂閱授權並存取 Horizon Control Plane，您必須使用 Horizon Cloud Connector 虛擬應用裝置，以使用 Horizon 控制平面來連線 Horizon 部署。

Horizon Control Plane (由訂閱授權啟用) 可在連線至您的 Horizon 部署時提供下列優點：

- Horizon 通用主控台在內部部署和多雲端部署間提供單一的整合主控台，可與承租人的雲端連線網繭機群搭配運作。
- 混合多雲端協調提供單一工作流程來啟用 VMware JMP 技術。
- Horizon Universal Broker 是雲端式代理技術，用來管理混合多雲端指派的虛擬資源並將其配置給您的使用者。
- 雲端監控服務 (CMS) 是 Horizon 控制平面中提供的一項中心服務。CMS 可讓您監控雲端連線網繭機群內和其間的容量、使用量和健全狀況，無論個別網繭所在的部署環境為何。
- Horizon 映像管理服務是一項雲端式服務，可讓您以簡便且自動化的方式管理雲端連線 Horizon 網繭中的桌面平台指派 (例如桌面平台集區和伺服器陣列) 所使用的系統映像。
- 《Horizon 架構規劃》文件提供部署 VMware Horizon 的概觀和需求。如需 Horizon Control Plane 的相關資訊，請參閱 VMware Horizon Cloud Service 說明文件中的 Horizon Cloud 簡介。

Just-in-Time Management Platform (JMP)

JMP 提供彈性、快速且個人化的 VMware Horizon 功能，可用來提供即時虛擬桌面平台和應用程式。JMP 包含下列 VMware 技術。

即時複製

即時複製是一種以 vSphere 為基礎的複製技術，可用來從單一最佳配置映像佈建數千個非持續性虛擬桌面平台。即時複製桌面平台提供下列優點：

- 快速的佈建速度，平均只需 1-2 秒即可建立新的桌面平台。
- 在每次使用者登入時提供全新、高效能的桌面平台。
- 在每次使用者登出時終結桌面平台，藉以提高安全性。
- 不需為每個單一使用者提供專用的桌面平台。
- 修補桌面平台集區時完全不需中斷運作。
- VMware App Volumes 和 VMware Dynamic Environment Manager 可以與即時複製搭配使用，以提供完整的個人化桌面平台。

VMware App Volumes

VMware App Volumes 是整合且統一的應用程式提供和使用者管理系統，適用於 VMware Horizon 和其他虛擬環境。VMware App Volumes 提供下列優點：

- 快速佈建大規模的應用程式。
- 即便使用者已登入其桌面平台，仍可將應用程式動態連結至使用者、群組或裝置。
- 即時佈建、提供、更新和淘汰應用程式。
- 為使用者提供可寫入的磁碟區，讓其能夠在桌面平台上安裝後續的應用程式。

VMware Dynamic Environment Manager

VMware Dynamic Environment Manager 提供跨任何虛擬、實體和雲端式環境的個人化設定和動態原則組態。VMware Dynamic Environment Manager 提供下列優點：

- 讓使用者快速存取 Windows 工作區和應用程式，同時在不同的裝置和位置之間維持個人化的一致體驗。
- 為組織提供利用單一、可擴充且利用現有基礎結構的解決方案，以簡化使用者設定檔管理。
- 藉由以非同步程序套用組態和環境設定 (而非全都在登入時套用)，加快登入程序的執行速度。
- 在使用者啟動應用程式時提供動態環境組態，例如磁碟機或印表機對應。

除了使用三項基礎 JMP 技術以外，您也可以透過 Horizon 控制平面中的「指派」精靈，在單一工作流程中加以協調運用。

可靠性與安全性

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

- 可以輕鬆地限制存取資料。可以防止複製機密資料到遠端員工的家用電腦。
- RADIUS 支援提供從雙因素驗證廠商當中進行選擇的彈性。支援的廠商包括 RSA SecureID、VASCO DIGIPASS、SMS Passcode 和 SafeNet 等等。
- 整合 VMware Workspace ONE Access 意味著，使用者可以依需求透過其用於存取 SaaS、Web 和 Windows 應用程式的同一個 Web 型應用程式目錄存取遠端桌面平台。在遠端桌面平台內部，使用者還可以使用此自訂應用程式存放區來存取應用程式。利用 True SSO 功能，使用智慧卡或雙因素驗證進行驗證的使用者，可以存取其遠端桌面平台和應用程式而不需提供 Active Directory 認證。
- 針對想從公司防火牆外部存取遠端桌面平台和應用程式的使用者，Unified Access Gateway 可做為安全閘道使用。Unified Access Gateway 是安裝在非軍事區 (DMZ) 中的應用裝置。使用 Unified Access Gateway 可確保能夠進入公司資料中心的流量，皆為代表經過嚴格驗證之遠端使用者的流量。
- 能夠佈建包含預先建立之 Active Directory 帳戶的遠端桌面平台，解決了具有唯讀存取權原則的鎖定 Active Directory 環境的需求。
- 可以排程資料備份，而不用考慮使用者的系統何時可能會關閉。
- 資料中心主控的遠端桌面平台和應用程式極少會發生停機狀況，甚至永遠不會停機。虛擬機器可以位於 VMware Server 的高可用性叢集上。

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

與 VMware 生態系統緊密整合

您可以使用 VMware Horizon 搭配 VMware vSphere、vSAN、NSX，以透過虛擬計算、虛擬儲存、虛擬網路與安全性來擴充虛擬化功能，以降低成本、增強使用者體驗，並提供更高的業務靈活性。您可以在公有雲上執行部署，例如 VMware Cloud on AWS 或 VMware Azure 解決方案。

您也可以利用其他管理軟體，例如 vRealize、Avi Networks 和 Carbon Black。

豐富的使用者體驗

VMware Horizon 提供使用者預期且熟悉的個人化桌面平台環境，其中包括下列使用者體驗：

- 多樣化的顯示通訊協定選項。
- 能夠存取 USB 和其他連線至其本機電腦的裝置。
- 將文件傳送至其本機電腦可偵測到的任何印表機。
- 即時音訊/視訊功能。
- 使用智慧卡進行驗證。
- 使用多台顯示器監視器。
- 3D 圖形支援。

REST 式 API

針對 VMware Horizon 基礎結構、工作負載以及與第三方產品的整合，VMware Horizon REST 式 API 可自動化其部署、作業、管理、監控、報告和分析。您可以使用這些 API 執行下列功能：

- 桌面平台集區管理
- 虛擬機器和伺服器陣列管理
- 發佈應用程式
- 授權已發佈的應用程式
- 基礎結構探索
- 監控和疑難排解

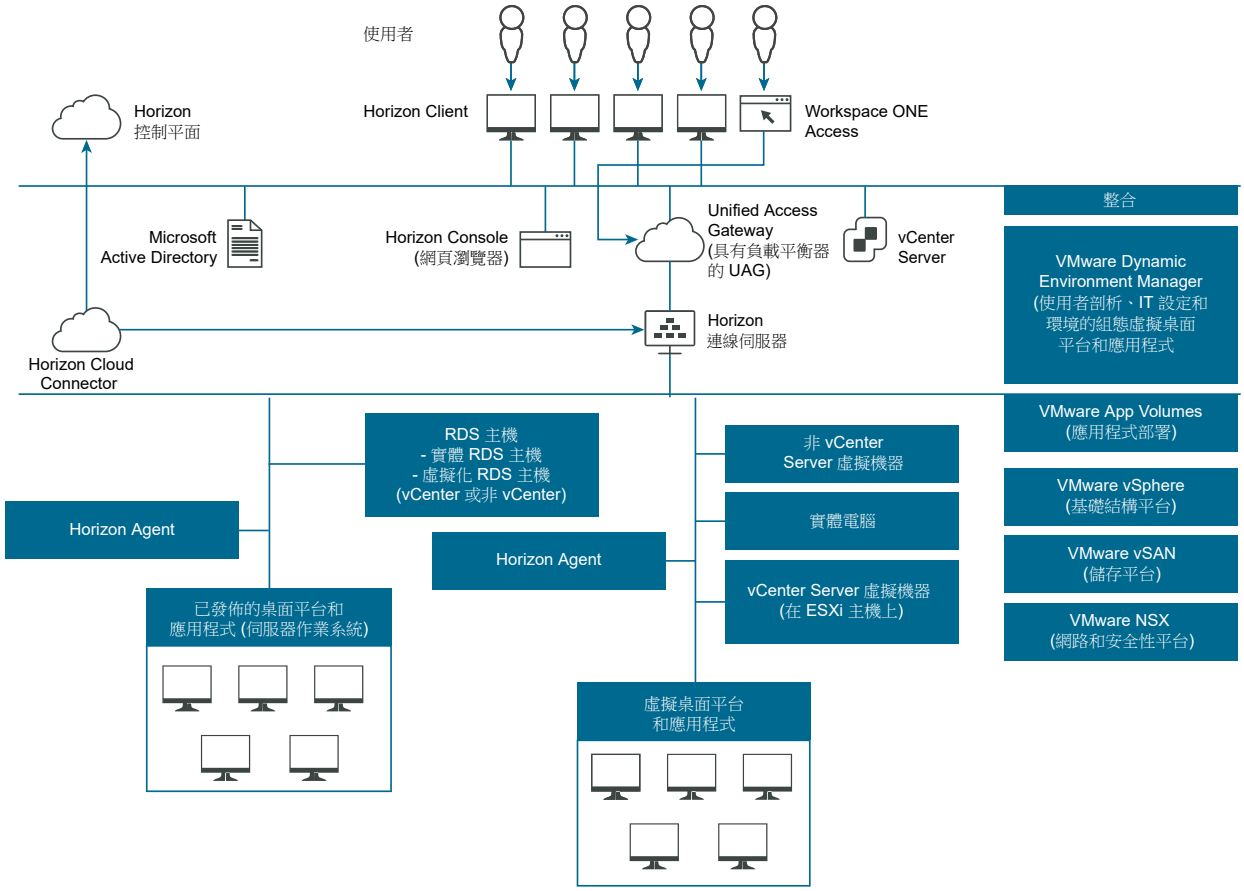
如需關於 VMware Horizon REST 式 API 的詳細資訊，請參閱 https://code.vmware.com 中提供的 REST 式 API。

元件搭配運作的方式

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

VMware Horizon 環境的高階範例顯示 VMware Horizon 部署的主要元件之間的關係。

圖 1-1. VMware Horizon 環境的高階範例



用戶端裝置

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

使用者將開啟 Horizon Client 以顯示其遠端桌面平台及應用程式。精簡型用戶端裝置會使用 VMware Horizon 精簡型用戶端軟體，且可設定為使用者可在裝置上直接啟動的唯一應用程式是 VMware Horizon 精簡型用戶端。將舊版電腦重新運用為精簡型用戶端桌面，可以延長硬體使用壽命三到五年。例如，藉由在精簡型桌面使用 VMware Horizon，您可以在較舊的桌面硬體上使用較新的作業系統 (例如 Windows 10)。

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

Horizon 連線伺服器

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

連線伺服器提供下列管理功能：

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

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

在公司防火牆外部，您可以在 DMZ 中安裝 Unified Access Gateway 應用裝置。DMZ 中的 Unified Access Gateway 應用裝置會與公司防火牆內的連線伺服器通訊。Unified Access Gateway 應用裝置可確保唯一可進入公司資料中心的遠端桌面平台和應用程式流量是代表經過嚴格驗證之使用者的流量。使用者只能存取其有權存取的資源。

如需關於 Unified Access Gateway 應用裝置的詳細資訊，請參閱 Unified Access Gateway 說明文件，網址為 https://docs.vmware.com/tw/Unified-Access-Gateway/index.html。

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

Horizon Client

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

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

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

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

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

- 各種第三方精簡型用戶端和零用戶端，只能透過認證合作夥伴取得。

VMware Horizon 使用者入口網站

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

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

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

Horizon Agent

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

如果桌面來源是虛擬機器，則應先在該虛擬機器上安裝 Horizon Agent 服務，然後使用虛擬機器作為範本或作為即時複製的最佳配置映像。從這個虛擬機器建立集區時，代理程式會自動安裝在每個遠端桌面平台上。

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

Horizon Console

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

當您安裝連線伺服器執行個體時，您也會取得 Horizon Console Web 介面的 URL。此 Web 介面可讓管理員從任何位置管理連線伺服器執行個體，而不必在自己的本機電腦上安裝應用程式。

vCenter Server

如果您要在 vSphere 上部署 Horizon，則 vCenter Server 可作為已連接網路之 VMware ESXi 伺服器的中央管理員。vCenter Server 可提供在資料中心中設定、佈建及管理虛擬機器的集中點。

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

整合 VMware Horizon

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

整合 VMware Horizon 與商業智慧軟體

您可以設定 Horizon Connection Server，將事件記錄到 Microsoft SQL Server、Oracle 或 PostgreSQL 資料庫。

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

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

如需詳細資訊，請參閱《Horizon 管理》文件。

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

使用 Horizon PowerCLI Cmdlet 建立管理指令碼

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

如需關於 Horizon PowerCLI Cmdlet 的詳細資訊，請參閱 https://code.vmware.com/docs/6978/cmdlet-reference 中提供的《VMware PowerCLI Cmdlet 參考》。

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

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

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

- 建立和更新桌面平台集區。
- 設定多個網路標籤，以大幅擴增指定給集區中虛擬機器的 IP 位址數量。
- 將資料中心資源新增至完整的虛擬機器。
- 抽樣檢查特定桌面或桌面平台集區長期的使用情況。
- 查詢事件資料庫。
- 查詢服務狀態。

修改 VMware Horizon 中的 LDAP 組態資料

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

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

您可以使用 LDIF 檔案執行許多工作。

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

如需詳細資訊，請參閱《Horizon 管理》文件。

使用 vdmadmin 命令

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

如需詳細資訊，請參閱《Horizon 管理》文件。

規劃豐富的使用者經驗

2

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

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

本章節討論下列主題：

Horizon Agent 的功能支援對照表

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

哪些類型和版本的客體作業系統受支援，取決於 Windows 版本。

如需 Windows 10 客體作業系統的清單，請參閱 VMware 知識庫 (KB) 文章 https://kb.vmware.com/s/article/78714。

針對 Windows 10 以外的 Windows 作業系統，請參閱 VMware 知識庫 (KB) 文章 https://kb.vmware.com/s/article/78715。

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

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

選擇顯示通訊協定

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

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

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

VMware Blast Extreme

VMware Blast Extreme 已針對行動雲端進行最佳化，可支援最範圍廣泛、且具備 H.264、HEVC、JPEG、PNG 和專屬 Blast 轉碼器功能的用戶端裝置。在所有顯示通訊協定中，VMware Blast Extreme 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 Extreme 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 Virtual Private Network (VPN)，或者使用者可以在公司 DMZ 中，建立與 Unified Access Gateway 應用裝置間的安全加密連線。

  備註 不建議使用 VPN，因為 Blast 連線已加密。為獲得更理想的使用者體驗，請改用 Unified Access Gateway 應用裝置。

- 支援進階加密標準 (AES) 128 位元加密，且預設為啟動狀態。不過，您可以將加密金鑰密碼變更為 AES-256。
- 來自所有用戶端裝置類型的連線。

- 在 LAN 和 WAN 減少頻寬使用量的最佳化控制。
- Windows 代理程式上使用 PerfMon 顯示的效能計數器會精準呈現系統目前的狀態，並以固定速率更新下列項目：
  - Blast 工作階段
  - 影像處理
  - 音訊
  - CDR
  - USB：如果將 USB 流量設定為使用 VMware 虛擬通道 (VVC)，則在 Windows 代理程式上使用 PerfMon 顯示的 USB 計數器為有效。
  - 商務用 Skype：計數器僅用於控制流量。
  - 剪貼簿
  - RTAV
  - 序列埠和掃描器重新導向功能
  - 虛擬列印
  - HTML5 MMR
  - Windows Media MMR：在您設定此功能以使用 VMware 虛擬通道 (VVC) 後，才會顯示效能計數器。
- Windows 用戶端上發生短暫網路中斷期間的網路持續性。
- 虛擬顯示器支援 32 位元色彩。
- 支援 ClearType 字型。
- 使用 LAN 和 WAN 的動態音訊品質調整進行的音訊重新導向。
- 在部分用戶端類型上，用於網路攝影機和麥克風的即時音訊視訊。
- 在用戶端作業系統與遠端桌面平台或已發佈的應用程式之間複製與貼上文字及映像 (適用於部分用戶端)。對於其他用戶端類型，僅支援複製與貼上純文字。您無法複製並貼上系統物件，例如系統之間的資料夾和檔案。
- 部分用戶端類型支援多部監視器。在部分用戶端上，針對 Windows 桌面平台，您最多可使用每個顯示器解析度達 2560 x 1600 的四部監視器，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 和 HEVC。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。

如需有關 3D 功能的詳細資訊，請參閱使用 3D 圖形應用程式。

用戶端系統的硬體需求

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

PCoIP

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

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

PCoIP 功能

PCoIP 的主要功能包括：

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

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

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

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

建議的客體作業系統設定

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

視訊品質需求

480p 格式的視訊

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

720p 格式的視訊

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

1080p 格式的視訊

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

3D 轉譯

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

如需有關 3D 功能的詳細資訊，請參閱使用 3D 圖形應用程式。

用戶端系統的硬體需求

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

使用已發佈的應用程式

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

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

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

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

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

  例如，當使用者必須遠端存取資料庫時，如果大量資料必須透過 WAN 傳輸，效能通常會受到影響。透過已發佈的應用程式，應用程式的所有元件都可以位於與資料庫相同的資料中心中，以便隔離流量，且只有畫面更新會透過 WAN 傳送。

- 從行動裝置中，存取個別應用程式比開啟遠端 Windows 桌面平台，然後導覽至應用程式更方便。

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

將 USB 裝置與遠端桌面平台和應用程式搭配使用

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

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

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

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

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

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

使用網路攝影機和麥克風

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

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

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

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

使用 3D 圖形應用程式

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

NVIDIA GRID vGPU (共用的 GPU 硬體加速)

vSphere 提供這項功能，可讓 ESXi 主機上的實體 GPU (圖形處理單元) 在虛擬機器之間共用。如果您需要高端、硬體加速的工作站圖形處理能力，請使用此功能。

AMD MxGPU

vSphere 提供這項功能，它會將 GPU 當成多個 PCI 傳遞裝置，以讓多部虛擬機器共用 AMD GPU。這項功能提供靈活的硬體加速的 3D 設定檔，範圍從輕量型 3D 任務工作者到高端的工作站圖形進階使用者都有。

虛擬專用圖形加速 (vDGA)

vSphere 提供這項功能，它可讓 ESXi 主機上的單一實體 GPU 專用於單一虛擬機器。如果您需要高端、硬體加速的工作站圖形處理能力，請使用此功能。

備註 請參閱 http://www.vmware.com/resources/compatibility/search.php 上的 VMware 硬體相容性清單。和其他廠商一樣，Intel vDGA 使用 Intel 整合的 GPU，而非使用分立的 GPU。

虛擬共用圖形加速 (vSGA)

vSphere 提供這項功能，可讓多部虛擬機器共用 ESXi 主機上的實體 GPU。您可以使用 3D 應用程式進行設計以及製作模型和多媒體。

軟體 3D

vSphere 提供軟體加速圖形，讓您不需使用實體 GPU，即可執行 DirectX 9 和 OpenGL 2.1 應用程式。此功能適合資源需求較少的 3D 應用程式，例如 Windows Aero 主題、Microsoft Office 2010 和 Google Earth。

重要 請參閱 VMware 白皮書，瞭解 vSphere 的圖形加速相關資訊。轉譯選項會隨著環境 (vSphere、非 vSphere 和實體電腦) 與使用案例 (虛擬桌面平台與已發佈的桌面平台) 而有所不同。若要瞭解您的環境和使用案例專用的 3D 選項，請參閱《在 Horizon 中設定虛擬桌面平台》文件和《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。如需各種 3D 轉譯選項的詳細資訊，請參閱 VMware Horizon 6.1 的 NVIDIA GRID vGPU 部署指南和 NVIDIA GRID 虛擬 GPU 使用者指南。

將多媒體串流到遠端桌面平台

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

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

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

從遠端桌面平台列印

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

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

本機印表機重新導向專為下列使用案例而設計：

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

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

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

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

使用 Single Sign-On 來登入

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

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

針對遠端桌面平台，此功能包含認證提供者動態連結程式庫。

True SSO

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

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

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

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

監視器和螢幕解析度

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

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

在多台監視器設定中使用所有監視器

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

Horizon Client 支援下列監視器組態：

- 當您使用兩台監視器時，這些監視器不必處於相同模式。例如，如果您使用的筆記型電腦與外部監視器連接，則這台外部監視器可為直向模式或橫向模式。
- 螢幕可以並排擺放、兩層各兩台的堆疊，或是當您僅使用兩台監視器、且總高度低於 4096 像素時，便可以垂直堆疊。
- 若要使用 3D 轉譯功能，您必須使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定。您最多可以使用兩台監視器，解析度可高達 1920 x 1200。若是 4K (3840 x 2160) 解析度，則僅支援一台監視器。
- - Windows Server 2019 虛擬桌面平台需要 Horizon Agent 7.7 或更新版本。
  - Horizon Agent 2006 及更新版本不支援 Windows 7 和 Windows 8.x 虛擬桌面平台。

- 使用 VMware Blast 顯示通訊協定時，支援 8K (7680 x 4320) 的遠端桌面平台螢幕解析度。支援兩個 8K 顯示器。桌面平台虛擬機器的硬體版本必須為 14 (ESXi 6.7 或更新版本)。您必須在虛擬機器中配置足夠的系統資源，才能支援 8K 顯示。如需適用於 GRID 型桌面平台和適用於 NVIDIA vGPU 設定檔之所支援監視器組態的相關資訊，請參閱 NVIDIA 網站上的《虛擬 GPU 軟體使用者指南》。只有 Windows 用戶端支援此功能。
- 可透過 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定，支援 4K (3840 x 2160) 的遠端桌面平台畫面解析度。支援的 4K 顯示器數目取決於桌面平台虛擬機器的硬體版本以及 Windows 10 版本。

硬體版本	支援的 4K 顯示器數目
10 (ESXi 5.5.x 相容)	1
11 (ESXi 6.0 相容)	3
11	1
13、14 或更新版本	1 (啟用 3D 轉譯功能) 4 (停用 3D 轉譯功能)

  為了達到最佳效能，虛擬機器應具備至少 2 GB RAM 和 2 個 vCPU。此功能可能需要良好的網路條件，例如 1000Mbps 頻寬與低網路延遲，以及低封包遺失率。

  備註 遠端桌面平台螢幕解析度設定為 3840 x 2160 (4K) 時，螢幕上的項目可能會顯得比較小，您也無法使用遠端桌面平台中的 [螢幕解析度] 對話方塊讓文字和其他項目變大。在 Windows 用戶端上，您可以將用戶端機器的 DPI 設定為適當設定，並啟用 DPI 同步功能，將用戶端機器的 DPI 設定重新導向至遠端桌面平台。

- 如果使用 Microsoft RDP 7，則可用來顯示遠端桌面平台的監視器數量上限為 16。
- 如果使用 Microsoft RDP 顯示通訊協定，則遠端桌面平台必須安裝 Microsoft 遠端桌面連線 (RDC) 6.0 或更新版本。

在多台監視器設定中使用一台監視器

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

使用高解析度模式

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

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

從中央位置管理桌面平台和應用程式集區

3

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

本章節討論下列主題：

桌面平台集區

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

您可以從下列其中一個來源建立桌面平台集區：

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

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

使用集區管理桌面平台可讓您套用設定或部署應用程式到集區中的所有遠端桌面平台。若要進一步瞭解虛擬機器或未受管理機器的桌面平台集區，請參閱《在 Horizon 中設定虛擬桌面平台》文件。若要進一步瞭解以 RDS 主機上工作階段為基礎的桌面平台集區，請參閱《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

應用程式集區

透過在 RDS 主機之伺服器陣列上執行的應用程式集區，讓使用者可以存取在資料中心的伺服器 (而非其個人電腦或裝置) 上執行的已發佈應用程式。

應用程式集區有多項優點：

- 可存取性

  使用者可以在任何位置從網路存取應用程式。您也可以設定安全的網路存取。

- 裝置獨立性

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

- 存取控制

  您可以便捷地授與、移除使用者或使用者群組對應用程式的存取權。

- 加速部署

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

- 管理能力

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

- 安全性與合規性

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

- 降低成本

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

應用程式佈建

VMware Horizon 提供數個有關應用程式佈建的選項。

- 使用 RDS 主機部署已發佈的應用程式。請參閱使用 RDS 主機部署已發佈的應用程式。
- 在具有虛擬機器主控應用程式的桌面平台集區上，部署在其中執行的已發佈應用程式。請參閱在具有虛擬機器主控應用程式的桌面平台集區上，部署在其中執行的已發佈應用程式。
- 在虛擬桌面平台內部署應用程式。請參閱在虛擬桌面平台中部署應用程式。

- 使用 VMware App Volumes 部署應用程式。您可以使用 VMware App Volumes 封裝應用程式，並將其提供給使用者。當您的使用者登入其遠端桌面平台時，其應用程式將會連結至桌面平台，如需詳細資訊，請參閱 VMware App Volumes 說明文件，網址為 https://docs.vmware.com/tw/VMware-App-Volumes/index.html。
- 散佈使用 VMware ThinApp 建立的應用程式套件。若要進一步瞭解如何散佈使用 VMware ThinApp 建立的應用程式套件，請參閱 VMware ThinApp 說明文件，網址為 https://docs.vmware.com/tw/VMware-ThinApp/index.html。
- 使用 RDS 主機部署已發佈的應用程式

  您可以選擇為使用者提供已發佈的應用程式，而非遠端桌面平台。個別已發佈的應用程式可能更容易在小型行動裝置上導覽。
- 在具有虛擬機器主控應用程式的桌面平台集區上，部署在其中執行的已發佈應用程式

  您可以將一或多個已發佈的應用程式提供給使用者，而不需建立 RDS 主機的伺服器陣列。您可以建立虛擬機器桌面平台的集區來主控應用程式，然後僅對使用者公開已發佈的應用程式。
- 在虛擬桌面平台中部署應用程式

  您可以將應用程式部署至最佳配置映像中，然後建立相同桌面平台的集區，讓每個桌面平台都有完全相同的應用程式複本。

使用 RDS 主機部署已發佈的應用程式

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

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

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

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

在具有虛擬機器主控應用程式的桌面平台集區上，部署在其中執行的已發佈應用程式

您可以將一或多個已發佈的應用程式提供給使用者，而不需建立 RDS 主機的伺服器陣列。您可以建立虛擬機器桌面平台的集區來主控應用程式，然後僅對使用者公開已發佈的應用程式。

下列應用程式類型可因此方法而獲益。

此策略可簡化下列應用程式類型的使用方式。

- 需要 .NET Framework 版本相容性的應用程式。
- 驅動程式在 RDS 主機上可能無法執行或不受支援，而需要特殊裝置支援的應用程式。

- 僅在 Windows 10 上經過測試和認證的應用程式。
- 需要獨立軟體廠商提供安裝授權和使用量報告的應用程式。

如需詳細資訊，請參閱《VMware Horizon 和 VMware Horizon Apps 中已發佈的應用程式和桌面平台的最佳做法》文件，網址為 https://techzone.vmware.com。

在虛擬桌面平台中部署應用程式

您可以將應用程式部署至最佳配置映像中，然後建立相同桌面平台的集區，讓每個桌面平台都有完全相同的應用程式複本。

如果您部署即時複製桌面平台集區，則在修補所有桌面平台的應用程式時，您僅需更新最佳配置映像，然後使用推送映像功能，以輪替的方式將變更快速散佈至集區中的所有桌面平台即可。當使用者登出即時複製虛擬桌面平台時，VMware Horizon 會刪除即時複製，並從最新版本的最佳配置映像建立全新的即時複製。這個新的複製已準備就緒，可供後續使用者登入。透過滾動更新，系統可以盡量縮短與集區維護相關聯的停機時間。

您可以將此功能用於下列工作：

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

使用 Active Directory GPO 管理使用者和桌面

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

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

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

套用 GPO 之後，內容會儲存在指定元件的本機 Windows 登錄中。

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

使用 Dynamic Environment Manager 搭配智慧型原則

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

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

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

遠端桌面平台部署的架構設計元素和規劃指導方針

4

本章討論架構設計元素和規劃指導方針，包括有關記憶體、CPU、儲存容量、網路元件和硬體等需求的重要詳細資料，可讓 IT 架構設計人員和規劃人員實際瞭解部署 VMware Horizon 解決方案會涉及到哪些環節。

如需關於如何設計 VMware Horizon 部署架構的詳細資料，請參閱《VMware Workspace ONE 和 VMware Horizon 參考架構》文件，網址為 https://techzone.vmware.com。

重要 本章不包含以下主題：

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

本章節討論下列主題：

- 遠端桌面平台的客體作業系統需求
- ESXi 節點
- vCenter Server 虛擬機器組態
- Horizon 連線伺服器最大值和組態
- vSphere 叢集
- 儲存區和頻寬設計的考量事項
- VMware Horizon 建置區塊
- Horizon 網繭 (Pod)
- 使用網繭 (Pod) 中多個 vCenter Server 的優點
- Cloud Pod 架構概觀

遠端桌面平台的客體作業系統需求

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

- 根據工作者類型進行規劃

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

- 桌面平台類型

  需要考量的最基本問題是，某種類型的使用者需要可設定狀態的桌面平台映像，還是需要無狀態的桌面平台映像。應使用持續性還是持續性桌面平台，取決於特定工作者類型。

- 估計虛擬機器桌面平台的記憶體需求

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

- 估計虛擬機器桌面平台的 CPU 需求

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

- 選擇適當的系統磁碟大小

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

- 桌面虛擬機器組態

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

- RDS 主機虛擬機器組態

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

根據工作者類型進行規劃

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

進行架構規劃時，可將工作者分成幾種類型。

任務工作者

任務工作者和管理工作者會在少數應用程式中執行重複性的工作，通常是使用固定電腦。應用程式通常不是知識工作者所用應用程式那樣需要大量的 CPU 和記憶體資源。特定班次的任務工作者可能會同時全部登入虛擬桌面。任務工作者包括客服中心分析人員、零售店員工、倉庫作業員等等。

知識工作者

知識工作者的每日工作包括存取網際網路、使用電子郵件，以及建立複雜文件、簡報和試算表。知識工作者包括會計人員、銷售經理、行銷研究分析人員等等。

進階使用者

進階使用者包括應用程式開發人員，以及使用需要密集圖形資源之應用程式的人員。這些使用者和應用程式往往會佔用大量的 CPU 和記憶體，因此在設計架構的過程中需考量這些事項。

Kiosk 使用者

這些使用者需要共用位於公共區域的桌面平台。Kiosk 使用者的範例包括使用教室共用電腦的學生、護理站的護士，以及用於工作安排與人才招募的電腦。這些桌面需要自動登入。必要時，可透過某些應用程式進行驗證。

桌面平台類型

需要考量的最基本問題是，某種類型的使用者需要可設定狀態的桌面平台映像，還是需要無狀態的桌面平台映像。應使用持續性還是持續性桌面平台，取決於特定工作者類型。

持續性桌面平台

持續性桌面平台會將必須保留、維護和備份的資料存放在作業系統映像本身。例如，使用者若需要安裝部分自己專屬的應用程式，或是有資料無法儲存在虛擬機器本身以外 (例如檔案伺服器或應用程式資料庫)，則需要持續性桌面平台。

有多種方式可在 VMware Horizon 中建立持續性桌面平台：

您可以建立完整複製虛擬機器的自動集區。

如果您已建立虛擬桌面平台或實體桌面 (vCenter 虛擬機器、非 vCenter 虛擬機器或實體電腦)，則可以使用具有專用指派的手動桌面平台集區，將其匯入至 VMware Horizon 作為持續性桌面平台。

持續性桌面平台可為使用者提供最高的彈性，並且讓他們控制本身的桌面平台。但此類桌面平台會耗用較多計算資源，且 IT 人員較難加以管理。這些桌面平台可能需要傳統的映像管理技術。持續性桌面平台可結合某些儲存系統技術，實現低儲存成本。由於每個持續性桌面平台都是唯一的，且必須保留，因此在考量業務持續性的策略時，備份及復原技術相當重要。

非持續性桌面平台

非持續性桌面平台是彼此相同的無狀態映像。此類桌面平台主要供不需要安裝或保留其應用程式的使用者使用。非持續性桌面平台有許多優勢，像是更易於支援，以及所需儲存成本較低。其他優點包括，不太需要備份虛擬機器，以及更簡易、成本較低的災難復原與業務持續性選項。由於未儲存唯一的使用者資料，虛擬桌面平台本身不需受到保護。在虛擬桌面平台終結的情況下，您可以直接從最佳配置映像重新建立虛擬桌面平台。此外，也可以選擇性地使用資料夾重新導向和各種設定檔技術，來處理儲存區使用者設定檔和使用者資料。

在 VMware Horizon 中，您可以利用即時複製來建立非持續性桌面平台。如需即時複製的詳細資訊，請參閱《在 Horizon 中設定虛擬桌面平台》文件。

適用於任務工作者的桌面平台

由於任務工作者會在少部分的應用程式中執行重複性的工作，因此，您可以利用非持續性桌面平台來節省儲存區的計算成本，並簡化桌面平台管理。

適用於知識工作者和進階使用者的桌面平台

知識工作者常需要建立複雜的文件，並持續加以保存。進階使用者常需安裝自己的應用程式，並加以持續保存。根據須保留之個人資料的性質和數量，他們將需要非持續性桌面平台或持續性桌面平台。

若工作者必須安裝其本身的應用程式，且這些應用程式會將資料新增至作業系統磁碟，則最佳選擇是使用完整複製虛擬機器建立持續性桌面平台。

適用於 Kiosk 使用者的桌面平台

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

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

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

如需關於為特定類型的工作者建立桌面平台集區的詳細資訊，請參閱《在 Horizon 中設定虛擬桌面平台》文件。

估計虛擬機器桌面平台的記憶體需求

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

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

RAM 大小對效能的影響

配置 RAM 時，應避免選擇過度保守的設定。請考量下列幾個事項：

- RAM 配置不足，可導致過多的 Windows 分頁，進而可產生 I/O 導致效能明顯下滑及儲存 I/O 負載增加。
- 由於虛擬桌面平台的效能對回應時間非常敏感，因此 VMware 建議保留所有記憶體。

RAM 大小對儲存空間的影響

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

Windows 分頁檔

此檔案的大小預設為客體 RAM 的 150%。此檔案預設位於 `C:\pagefile.sys`，會使精簡佈建的儲存空間因經常存取而變大。

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

筆記型電腦的 Windows 休眠檔

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

ESXi 交換檔

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

ESXi 暫停檔

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

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

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

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

標準顯示解析度	寬度 (像素)	高度 (像素)	1 部監視器額外負荷	2 部監視器額外負荷	3 部監視器額外負荷	4 部監視器額外負荷
VGA	640	480	1.20MB	3.20MB	4.80MB	5.60MB
WXGA	1280	800	4.00MB	12.50MB	18.75MB	25.00MB
1080p	1920	1080	8.00MB	25.40MB	38.00MB	50.60MB
WQXGA	2560	1600	16.00MB	60.00MB	84.80MB	109.60MB
UHD (4K)	3840	2160	32.00MB	78.00MB	124.00MB	170.00 MB

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

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

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

特定工作負載和作業系統的 RAM 大小

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

為 Windows 10 或更新版本的桌面平台配置 2 GB 是很好的起點。如果您要使用其中一個硬體加速圖形功能來完成 3D 工作負載，VMware 建議使用 2 個虛擬 CPU 和 4 GB 的 RAM。在試驗期間，請監控效能以及各種類型工作者所用的磁碟空間，並進行調整，直到找到各工作者集區的最佳設定為止。

估計虛擬機器桌面平台的 CPU 需求

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

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

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

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

- 對您的虛擬桌面平台使用即時複製桌面平台集區，而非完整虛擬機器的桌面平台集區。透過即時複製，您可以對最佳配置映像進行修補，然後使用推送映像以輪替方式將修補散佈至各個桌面平台集區。這可消除通常與傳統修補程式管理軟體相關聯的軟體更新瓶頸，因為此軟體會直接在每個虛擬桌面平台上個別下載和更新修補程式。
- 將防毒和軟體更新排程在非尖峰時段執行，此時登入的使用者可能較少。
- 錯開或隨機安排執行更新的時間。
- 使用與 VMware NSX 客體自我檢查功能相容的無代理程式防毒軟體。

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

選擇適當的系統磁碟大小

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

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

- 移除不需要的檔案。例如，減少 Temporary Internet Files 的配額。

- 關閉 Windows 服務，例如索引工具服務、磁碟重組工具服務和還原點。如需詳細資料，請參閱《在 Horizon 中設定虛擬桌面平台》文件。
- 選擇足以容納未來成長的虛擬磁碟大小，但不宜大到不切實際。
- 使用集中式檔案共用或 App Volumes 處理使用者產生的內容和使用者安裝的應用程式。
- 為 vCenter Server 啟用空間回收，以自動回收客體作業系統內過時或已刪除資料所使用的空間。

每個虛擬桌面必須考量下列檔案所需的儲存空間大小：

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

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

您也可以將這個估計值增加 15%，以確保使用者不會耗盡磁碟空間。

桌面虛擬機器組態

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

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

使用者資料所需的磁碟空間大小取決於使用者的角色和資料儲存的組織原則。

下表所列的指導方針適用於標準 Windows 10 虛擬機器桌面平台。

表 4-2. Windows 10 的桌面虛擬機器範例

項目	範例
作業系統	Windows 10 (含最新的 Service Pack)
RAM	4GB
虛擬 CPU	2
系統磁碟容量	24GB (略低於標準值)
虛擬 SCSI 介面卡類型	LSI Logic SAS (預設值)
虛擬網路介面卡	VMXNET 3

RDS 主機虛擬機器組態

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

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

表 4-3. RDS 主機虛擬機器範例

項目	範例
作業系統	64 位元 Windows Server 2012 R2
RAM	24GB
虛擬 CPU	4
系統磁碟容量	40GB
虛擬 SCSI 介面卡類型	LSI Logic SAS (Windows Server 2008 的預設值)
虛擬網路介面卡	VMXNET 3
1 個 NIC	1 GB
用戶端連線總數上限 (包括工作階段型遠端桌面平台連線與已發佈的應用程式連線)	50

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

ESXi 節點

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

VMware Horizon 在您最大化合併率時最具成本效益，而合併率是指在 ESXi 主機上主控的虛擬機器數目 (也用作桌面平台或 RDS 主機)。合併率通常取決於 ESXi 主機可用的 CPU、RAM 和儲存區數量，以及為了因應基礎結構元件所需的額外負荷資源時，每部虛擬機器所需的數量。雖然有許多因素會影響伺服器選擇，但是如果您只要獲得最佳的採購價格，則必須找出處理能力、記憶體與儲存裝置之間能取得適當平衡的伺服器組態。使用下列指導方針：

- 一般來說，請考慮每個 CPU 核心 8 至 10 個虛擬桌面的運算能力。如需計算每部虛擬機器之 CPU 需求的相關資訊，請參閱估計虛擬機器桌面平台的 CPU 需求。
- 請以虛擬桌面平台 RAM 和主機 RAM 為依據考量記憶體容量。如需計算每部虛擬機器所需之 RAM 數量的相關資訊，請參閱估計虛擬機器桌面平台的記憶體需求。

  請注意，實體 RAM 的成本並不是線性的，在某些情況下，採購不使用昂貴 DIMM 晶片的更小伺服器可能符合成本效益。在其他情況下，機架密度、儲存連線能力、管理能力及其他考量都可能讓部署中盡量減少伺服器數量成為較好的選擇。
- 在 VMware Horizon 中，依預設會開啟 View 儲存加速器功能，這可讓 ESXi 主機快取通用的虛擬機器磁碟資料。View 儲存加速器可以改善效能並降低額外儲存 I/O 頻寬的需要，以管理開機風暴和防毒掃描 I/O 風暴。使用此功能時，每個 ESXi 主機需要最多 32 GB 的 RAM。如需關於 View 儲存加速器的詳細資訊，請參閱《Horizon 安裝》文件中的〈設定 vCenter Server 的 View 儲存加速器〉。
- 最後，請考量叢集需求及任何容錯移轉需求。若要進一步瞭解如何判斷 vSphere 叢集上的高可用性需求，請參閱 確定高可用性的需求。

沒有其他方法西可取代在實際、真正環境的情況下 (例如試驗) 測量效能，以判斷環境和硬體組態的適當合併率。合併率會根據使用模式和環境因素而有很大的差異。如需 vSphere 中 ESXi 主機規格的相關資訊，請參閱《VMware vSphere 組態上限》文件。

vCenter Server 虛擬機器組態

當您在 vSphere 環境中部署 VMware Horizon 時，您將需要必須部署和設定 vCenter Server。您可以將 vCenter Server 安裝在與虛擬桌面平台或 RDS 主機相同的伺服器上，或安裝在不同的伺服器上。執行 vCenter Server 的虛擬機器需要比桌面平台虛擬機器更多的記憶體和處理能力。

vCenter 虛擬機器範例表顯示包含 vCenter Server 之虛擬機器的大小範例。

表 4-4. vCenter Server 虛擬機器範例

項目	管理 10,000 個桌面的 vCenter Server 範例	管理 2,000 個桌面的 vCenter Server 範例
作業系統	64 位元 Windows Server 2012 R2 Enterprise	64 位元 Windows Server 2012 R2 Enterprise
RAM	48GB	10-24 GB，視 vSphere 的版本而定
虛擬 CPU	16	2-8，視 vSphere 的版本而定
系統磁碟容量	180GB	40GB
虛擬 SCSI 介面卡類型	LSI Logic SAS (Windows Server 2008 的預設值)	LSI Logic SAS (Windows Server 2008 的預設值)
虛擬網路介面卡	E1000 (預設值)	VMXNET 3 (雖然使用預設值 E1000 也行)
vCenter 並行佈建作業上限	20	20
並行電源作業數量上限	50	50

Horizon 連線伺服器最大值和組態

Horizon 連線伺服器可安裝在實體伺服器或虛擬機器中。

連線伺服器組態範例

此範例使用的虛擬機器具有連線伺服器虛擬機器範例中所列出的規格。此虛擬機器的 ESXi 主機可以屬於 VMware HA 叢集，以防範實體伺服器故障。

表 4-5. 連線伺服器虛擬機器範例

項目	範例
作業系統	請參閱《Horizon 安裝》文件中支援的作業系統。
RAM	10GB
虛擬 CPU	4
系統磁碟容量	70GB
虛擬 SCSI 介面卡類型	LSI Logic SAS

表 4-5. 連線伺服器虛擬機器範例 (續)

項目	範例
虛擬網路介面卡	VMXNET 3
網路介面卡	1Gbps NIC

連線伺服器叢集設計考量

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

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

連線伺服器的連線數目上限

VMware 知識庫 (KB) 文章 https://kb.vmware.com/s/article/2150348 提供在 VMware Horizon 部署可同時容納的連線數目方面經過測試之限制的相關資訊。

如果將 Unified Access Gateway 應用裝置用於來自公司網路外部的 PCoIP 連線，則需要 PCoIP 安全閘道連線。如果將 Unified Access Gateway 應用裝置用於來自公司網路外部的 Blast Extreme 或 HTML Access 連線，則需要 Blast 安全閘道連線。如果將 Unified Access Gateway 應用裝置用於來自公司網路外部的 RDP 連線，以及用於透過 PCoIP 或 Blast 安全閘道連線的 USB 和多媒體重新導向 (MMR) 加速，則需要通道連線。

雖然 Unified Access Gateway 應用裝置最多同時可支援 2,000 個連線，但您可以選擇使用 2 或 4 個。所需的記憶體數量和 CPU 使用率可能會指示您為每個連線伺服器執行個體新增更多 Unified Access Gateway 應用裝置，以分散負載。

雖然 5 個連線伺服器執行個體 (已適當設定) 可以處理 20,000 個連線，但基於可用性規劃，您可以考慮使用 6 或 7 個連線伺服器，以及因應來自公司網路內部和外部的連線。

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

這些數字假設外部連線會透過閘道呈現。在此範例中，處理外部連線的每個連線伺服器執行個體將與 3 個 Unified Access Gateway 應用裝置配對，並且在兩個連線伺服器執行個體之間進行負載平衡，以便在其中一個無法使用時，由剩餘 2 個應用裝置處理負載。

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

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

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

表 4-6. Unified Access Gateway 的硬體需求

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

vSphere 叢集

VMware Horizon 部署可使用 VMware HA 叢集來防範實體伺服器失敗。

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

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

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

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

確定高可用性的需求

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

對高可用性的需求會根據桌面集區的用途而有很大的不同。例如，非持續性桌面平台集區可能具有與持續性桌面平台集區不同的復原點目標 (RPO) 需求。對於非持續性集區，如果使用者使用的桌面平台變得無法使用時，我們建議讓使用者登入其他桌面平台。

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

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

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

儲存區和頻寬設計的考量事項

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

- 共用儲存區的考量事項

  儲存設計考量是建立成功的 VMware Horizon 架構的最重要元素之一。

- 儲存頻寬考量事項

  在 VMware Horizon 環境中，決定頻寬需求的主要考量因素是登入風暴。

- 網路頻寬考量事項

  若要容納一般的工作負載，需要某些虛擬和實體網路元件。

共用儲存區的考量事項

儲存設計考量是建立成功的 VMware Horizon 架構的最重要元素之一。

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

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

您可以使用 VMware vSAN，它可將 ESXi 主機上提供的本機實體固態硬碟與硬碟機，虛擬化為叢集內所有主機共用的單一資料存放區。vSAN 提供高效能儲存和原則式管理，因此您可以在建立桌面平台集區時僅指定一個資料存放區，各種元件 (例如虛擬機器檔案、複本、使用者資料及作業系統檔案) 即會放置在適當的固態硬碟 (SSD) 或直接連結硬碟 (HDD) 上。如需關於 vSAN 的詳細資訊，請參閱 vSphere 說明文件，網址為 https://docs.vmware.com/tw/VMware-vSphere/index.html。如需最佳做法的相關資訊，請參閱技術白皮書 VMware Horizon on VMware vSAN 最佳做法。

如需關於 Horizon 儲存區組態的詳細資訊，請參閱《在 Horizon 中設定虛擬桌面平台》文件中的〈管理虛擬桌面平台的儲存區〉。

儲存頻寬考量事項

在 VMware Horizon 環境中，決定頻寬需求的主要考量因素是登入風暴。

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

VMware Horizon 環境有時會在所有虛擬機器同時執行活動的期間，發生 I/O 風暴負載。客體型代理程式可以觸發 I/O 風暴，例如防毒軟體或軟體更新代理程式。像是所有員工幾乎同時在早上登入等人員行為，也可以觸發 I/O 風暴。

您可以透過作業面的最佳做法，例如交錯執行不同虛擬機器的更新等，讓這些風暴工作負載降至最低。您也可以在試驗階段期間測試各種登出原則，決定使用者登出造成 I/O 風暴時是否暫停虛擬機器、還是關閉虛擬機器電源。

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

網路頻寬考量事項

若要容納一般的工作負載，需要某些虛擬和實體網路元件。

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

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

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

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

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

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

隨附於 PCoIP 和 Blast Extreme 的最佳化控制項

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

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

  此控制對於不需更新的靜態畫面內容，或只有一小部分需要重新整理的情況很有效用。
- 至於工作階段頻寬，您可以根據網路連線類型 (例如 4Mbit/s 網際網路連線)，設定最大頻寬 (每秒 kb)。頻寬包括所有映像處理、音訊、虛擬通道、USB 和 PCoIP 或 Blast 控制流量。

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

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

VMware Horizon 建置區塊

建置區塊是一種邏輯結構，可包含特定數目的虛擬機器。一個建置區塊由多個實體伺服器、vSphere 基礎結構、多個 VMware Horizon Server、共用儲存及提供給使用者的虛擬機器桌面所組成。每個區塊的延展性取決於您為每個 vCenter Server 部署的虛擬機器數量。

表 4-7. 4,000 部虛擬機器桌面平台的 LAN 型 Horizon 建置區塊範例

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

如果網繭中只有一個建置區塊，請使用兩個連線伺服器執行個體以提供備援。

Horizon 網繭 (Pod)

Horizon 網繭是由 VMware Horizon 延展性限制所決定的組織單位。您可以用多個建置區塊建立 Horizon 網繭。每個 Horizon 網繭都是一個管理單元，具有個別的 Horizon Console 管理使用者介面。

使用兩個建置區塊的網繭範例

表 4-8. 由 2 個建置區塊構成的 LAN 型 Horizon 網繭 (Pod) 範例

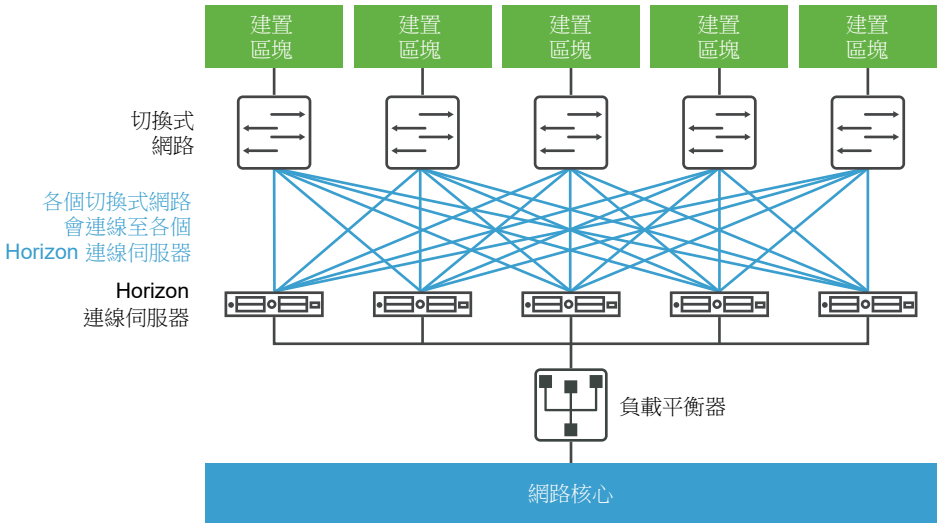
項目	數量
Horizon 網繭的建置區塊	2
vCenter Server	2
資料庫伺服器	2 (每個建置區塊各 1 部獨立資料庫伺服器) MS SQL Server、Oracle 或 PostgreSQL 資料庫伺服器
連線伺服器	7 (5 個用於來自企業網路內部的連線，2 個用於來自外部的連線)
vLAN	請參閱表 4-7. 4,000 部虛擬機器桌面平台的 LAN 型 Horizon 建置區塊範例。
10Gb 乙太網路模組	1
模組化網路交換器	1

取決於特定的組態，每個 vCenter Server 可支援大量虛擬機器。此支援可讓您擁有虛擬機器桌面平台的大型建置區塊。但是，實際區塊大小也會受制於其他 VMware Horizon 特有的限制。

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

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

圖 4-1. 虛擬機器桌面平台的網繭圖



使用一個 vCenter Server 的網繭 (Pod) 範例

在上一節，Horizon 網繭 (Pod) 由多個建置區塊所組成。每個建置區塊使用單一 vCenter Server 支援 5,000 部虛擬機器。本主題說明以使用單一 vCenter Server 管理 10,000 個桌面平台為基礎的架構。

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

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

表 4-9. 使用一個 vCenter Server 的 LAN 型 Horizon 網繭 (Pod) 範例

項目	範例
vSphere 叢集	6 (5 個叢集，每個叢集各有一個即時複製集區，以及 1 個基礎結構叢集)
vCenter Server	1
資料庫伺服器	1 (獨立式) MS SQL Server、Oracle 或 PostgreSQL 資料庫伺服器
Active Directory 伺服器	1 或 2

表 4-9. 使用一個 vCenter Server 的 LAN 型 Horizon 網繭 (Pod) 範例 (續)

項目	範例
連線伺服器執行個體	5
Unified Access Gateway 應用裝置	5
vLAN	8 (5 個用於桌面集區叢集，管理、VMotion 和基礎結構叢集各使用 1 個)

使用網繭 (Pod) 中多個 vCenter Server 的優點

在您嘗試使用單一 vCenter Server 執行個體管理許多虛擬機器之前，您必須考量下列幾個事項：

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

維護時段長度

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

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

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

能容許元件失敗的功能

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

因為每個 vSphere 叢集都必須透過單一 vCenter Server 執行個體來管理，所以此伺服器代表著每個 VMware Horizon 設計中的單一失敗點。

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

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

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

電源、佈建和重新調整作業的頻率

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

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

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

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

基礎結構的簡化度

大規模 VMware Horizon 設計中的單一 vCenter Server 執行個體提供了一些吸引人的優點，例如，提供單一位置來管理最佳配置映像虛擬機器、提供與 Horizon Console 視圖一致的單一 vCenter Server 視圖，以及較少的生產後端資料庫和資料庫伺服器。相較於多個執行個體，一個 vCenter Server 的災難復原規劃比較容易。請確定您已權衡多個 vCenter Server 執行個體的利弊得失，例如，優點有維護時段長度與電源和重新調整作業的頻率等，而缺點有管理最佳配置映像虛擬機器映像的額外管理負荷和需要增加基礎結構元件數等。

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

Cloud Pod 架構概觀

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

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

一般的 Cloud Pod 架構拓撲由兩個或多個網繭組成，這些網繭在網繭聯盟中會連結在一起。網繭聯盟受到某些限制。Cloud Pod 架構功能可用來連線在內部部署、公有雲或兩者混合環境中執行的網繭。如需詳細資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

規劃安全功能

5

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

重要 VMware Horizon 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 VMware Horizon 來啟用這些演算法。並非所有功能在 FIPS 模式中皆受到支援。如需詳細資訊，請參閱《Horizon 安裝》文件。

本章節討論下列主題：

瞭解用戶端連線

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

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

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

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

- 使用 PCoIP 和 Blast 安全閘道進行用戶端連線

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

- 使用 Microsoft RDP 的通道用戶端連線

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

- 直接用戶端連線

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

使用 PCoIP 和 Blast 安全閘道進行用戶端連線

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

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

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

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

使用 Microsoft RDP 的通道用戶端連線

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

通道連線提供下列優點：

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

在連線伺服器執行個體標準部署中，HTTPS 安全連線會終止於連線伺服器。在 DMZ 部署中，HTTPS 安全連線則終止於 Unified Access Gateway 應用裝置。

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

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

直接用戶端連線

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

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

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

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

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

選擇使用者驗證方法

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

- Active Directory 驗證

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

- 使用雙因素驗證

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

- 智慧卡驗證

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

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

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

Active Directory 驗證

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

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

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

您可以將使用者和群組放在下列 Active Directory 網域中：

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

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

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

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

使用雙因素驗證

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

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

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

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

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

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

智慧卡驗證

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

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

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

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

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

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

為了支援此功能，使用者認證會儲存在連線伺服器執行個體與用戶端系統上。

- 在連線伺服器執行個體上，使用者認證會進行加密，並連同使用者名稱、網域與選用 UPN 一起儲存在使用者工作階段中。進行驗證時，認證會新增；工作階段物件毀損時，認證會清除。當使用者登出、工作階段逾時或驗證失敗時，工作階段物件即毀損。工作階段物件位於動態記憶體中，而未儲存在 Horizon LDAP 或磁碟檔案中。

- 在連線伺服器執行個體上啟用**接受以目前使用者身分登入**設定，可讓連線伺服器執行個體接受使用者在 Horizon Client 的**選項**功能表中選取**以目前使用者身分登入**時所傳遞的使用者身分識別和認證資訊。

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

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

  當您選取**接受以目前使用者身分登入**時，您可以啟用下列使用者設定：

  - 允許舊版用戶端：支援舊版用戶端。Horizon Client 2006 版和 5.4 版及更早版本均被視為較舊的用戶端。
  - 允許 NTLM 後援：如果無法存取網域控制站，系統會使用 NTLM 驗證而非 Kerberos。必須在 Horizon Client 組態中啟用 NTLM 群組原則設定。
  - 停用通道繫結：用來保護 NTLM 驗證的額外一層安全防護層。依預設，用戶端上會啟用通道繫結。
  - True SSO 整合：在連線伺服器上啟用此設定，以允許使用 True SSO 對桌面平台進行 SSO。例如，在巢狀模式下，系統會使用 True SSO 登入巢狀用戶端，然後執行第二次桌面平台登入。如需巢狀模式的相關資訊，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》。
    - 已停用：如果用戶端未收到登入認證，則使用者必須輸入登入資訊。
    - 選用：系統將使用用戶端認證 (如果有的話)，否則將使用 True SSO。如果已啟用 True SSO 和以目前使用者身分登入，則建議使用此設定。
    - 已啟用：系統將使用 True SSO 來登入桌面平台。

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

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

備註 如果 Horizon Client 無法存取網域控制站，則在使用以目前使用者身分登入搭配 NTLM 驗證時，遞迴解除鎖定功能可能會變慢。若要緩解此問題，請在群組原則管理編輯器中，啟用 **VMware Horizon Client 組態 > 安全性設定 > NTLM 設定**資料夾中的群組原則設定**一律對伺服器使用 NTLM**。

「以目前使用者身分登入」功能的限制與需求如下：

- 當連線伺服器執行個體上的智慧卡驗證設為「必要」時，連線至連線伺服器執行個體時選取**以目前使用者身分登入**的使用者將會驗證失敗。這些使用者必須在登入連線伺服器時，以其智慧卡和 PIN 碼重新驗證。

- 用戶端登入系統的時間，必須與連線伺服器主機的時間同步。
- 如果在用戶端系統上修改預設的**從網路存取此電腦**使用者權限指派，則必須依照 VMware 知識庫 (KB) 文章 1025691 所述進行修改。

限制遠端桌面平台存取權

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

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

例如，VMware Horizon 部署可能包含兩個連線伺服器執行個體。第一個執行個體支援內部使用者。第二個執行個體與 Unified Access Gateway 應用裝置配對，並支援外部使用者。為防止外部使用者存取某些桌面，您可以設定受限制的權利，如下所示：

- 將「內部」標記指派給支援您內部使用者的連線伺服器執行個體。
- 將「外部」標記指派給與 Unified Access Gateway 應用裝置配對，並支援您外部使用者的連線伺服器執行個體。
- 將「內部」標記指派給應僅供內部使用者存取的桌面平台集區。
- 將「外部」標記指派給應僅供外部使用者存取的桌面平台集區。

外部使用者看不見標記為「內部」的桌面平台集區，因為他們是透過標記為「外部」的連線伺服器登入的，而內部使用者看不見標記為「外部」的桌面平台集區，因為他們是透過標記為「內部」的連線伺服器登入的。

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

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

使用群組原則設定保護遠端桌面平台和應用程式的安全

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

例如，您可以使用群組原則設定執行下列工作。

- 指定使用者在 Windows 版 Horizon Client 中選取**以目前使用者身分登入**核取方塊時，可接受使用者識別碼和認證資訊的連線伺服器執行個體。
- 在 Horizon Client 中為智慧卡驗證啟用 Single Sign-On。
- 在 Horizon Client 中設定伺服器 TLS 憑證檢查。
- 阻止使用者使用 Horizon Client 命令列選項提供認證資訊。

- 阻止非 Horizon Client 系統使用 RDP 連線至遠端桌面平台。您可以設定此原則，讓連線必須由 Horizon Client 管理，也就是說，使用者必須使用 VMware Horizon 連線至遠端桌面平台。

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

使用 智慧原則

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

您可以為控制行為範圍的使用者環境設定建立原則。使用者環境設定的 Horizon 智慧型原則會在登入期間套用，且可在工作階段重新連線期間重新整理。若要在使用者重新連線至工作階段時重新套用 Horizon 智慧型原則，您可以設定觸發的工作。

您可以為 Dynamic Environment Manager 在使用者電腦開機時套用的電腦環境設定建立原則。電腦環境設定的 Horizon 智慧型原則會在電腦開機期間套用，且可在工作階段重新連線期間重新整理。

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

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

若要瞭解如何使用智慧原則來控制遠端 Linux 桌面平台上功能的行為，請參閱《在 Horizon 中設定 Linux 桌面平台》。

實施最佳做法來保護用戶端系統

實施這些最佳做法來保護用戶端系統。

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

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

指定管理員角色

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

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

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

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

瞭解通訊協定

VMware Horizon 元件會使用數個不同的通訊協定來交換訊息。

下表列出每個通訊協定使用的預設連接埠。您可以變更連接埠號碼。例如，您可能需要變更連接埠號碼以符合組織原則，或避免爭用。

表 5-1. 預設連接埠

通訊協定	連接埠
JMS	TCP 連接埠 4001 TCP 連接埠 4002
HTTP	TCP 連接埠 80
HTTPS	TCP 連接埠 443
MMR/CDR	TCP 連接埠 9427 下列功能會使用此連接埠。 ■ Windows 多媒體重新導向 ■ 用戶端磁碟機重新導向 ■ Microsoft Teams 最佳化 ■ HTML 多媒體重新導向 ■ VMware 印表機重新導向 ■ USB 重新導向
RDP	TCP 連接埠 3389 **備註** 如果設定連線伺服器執行個體以進行直接用戶端連線，則這些通訊協定會直接從用戶端連線至遠端桌面平台，而不會透過 Horizon 安全閘道伺服器元件通道連線。
SOAP	TCP 連接埠 80 或 443
PCoIP	TCP 連接埠 4172 UDP 連接埠 4172、50002、55000
USB 重新導向	TCP 連接埠 32111。此連接埠也用於時區同步化。
VMware Blast Extreme	TCP 連接埠 8443、22443 UDP 連接埠 443、8443、22443
HTML Access	TCP 連接埠 8443、22443

用於連線伺服器互相通訊的 TCP 連接埠

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

Horizon 安全閘道

Horizon 安全閘道是伺服器端元件，用於在用戶端系統與 Unified Access Gateway 應用裝置或連線伺服器執行個體之間的安全 HTTPS 連線。

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

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

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

Blast 安全閘道

Unified Access Gateway 應用裝置包含一個 Blast 安全閘道元件。Blast 安全閘道啟用時，在驗證之後，使用 Blast Extreme 或 HTML Access 的用戶端可以進一步與 Unified Access Gateway 應用裝置建立安全連線。此連線可讓用戶端從網際網路存取遠端桌面平台和應用程式。

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

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

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

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

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

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

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

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

PCoIP 安全閘道

Unified Access Gateway 應用裝置包含一個 PCoIP 安全閘道元件。PCoIP 安全閘道啟用時，在驗證之後，使用 PCoIP 的用戶端可以進一步與 Unified Access Gateway 應用裝置建立安全連線。此連線可讓用戶端從網際網路存取遠端桌面平台和應用程式。

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

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

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

Horizon LDAP

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

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

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

Horizon 訊息

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

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

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

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 VMware Horizon。

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

表 5-2. 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、複本
HTTPS	TCP 443	標準、複本
PCoIP	TCP 4172 傳入； UDP 4172 雙向	標準、複本
HTTPS	TCP 8443 UDP 8443	標準、複本 與 VMware Horizon 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。

Horizon Agent 的防火牆規則

若要開啟預設的網路連接埠，Horizon Agent 安裝程式會選擇性地在虛擬桌面平台和 RDS 主機上設定 Windows 防火牆規則。

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

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

如果您在安裝之後變更 RDP 連接埠號碼，您必須變更相關聯的防火牆規則。如果您在安裝後變更預設連接埠，則必須手動重新設定防火牆規則，以便允許在更新的連接埠上進行存取。如需詳細資訊，請參閱《Horizon 安裝》文件。

在 RDS 主機上，Horizon Agent 的 Windows 防火牆規則會將 256 個連續的 UDP 連接埠顯示為對輸入流量開啟的連接埠。此連接埠的區塊可供 VMware Blast 內部用於 Horizon Agent 中。RDS 主機上有一個特殊的 Microsoft 簽署驅動程式，可封鎖從外部來源輸入至這些連接埠的流量。此驅動程式會造成 Windows 防火牆將連接埠視為已關閉。

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

下表列出在 Horizon Agent 安裝期間開啟的 TCP 和 UDP 連接埠。這些是傳入連接埠，除非另有說明。

表 5-3. Horizon Agent 安裝期間會開啟的 TCP 與 UDP 連接埠

通訊協定	連接埠
RDP	TCP 連接埠 3389
USB 重新導向和時區同步化	TCP 連接埠 32111
多媒體重新導向 (MMR) 和用戶端磁碟機重新導向 (CDR)	TCP 連接埠 9427 下列功能會使用此連接埠： ■ Windows 多媒體重新導向 ■ 用戶端磁碟機重新導向 ■ Microsoft Teams 最佳化 ■ HTML 多媒體重新導向 ■ VMware 印表機重新導向 ■ USB 重新導向
PCoIP	對於 RDS 主機，PCoIP 會使用 TCP 連接埠 4172 和 UDP 連接埠 4172 (雙向)。 針對虛擬桌面平台，PCoIP 會使用從可設定範圍中選取的連接埠號碼。依預設，PCoIP 會使用 TCP 連接埠 4172 至 4173，以及 UDP 連接埠 4172 至 4182。防火牆規則不會指定連接埠號碼，而是會動態遵循每個 PCoIP 伺服器所開啟的連接埠。選取的連接埠號碼會透過連線伺服器執行個體傳達給用戶端。
VMware Blast	TCP 連接埠 22443 UDP 連接埠 22443 (雙向) **備註** Linux 桌面平台上未使用 UDP。
HTML Access	TCP 連接埠 22443
XDMCP	UDP 177 **備註** 此連接埠只會對執行 Ubuntu 18.04 的 Linux 桌面平台中開啟，以進行 XDMCP 存取。防火牆規則會封鎖對此連接埠的所有外部主機存取。
X11	TCP 6100 **備註** 此連接埠只會對執行 Ubuntu 18.04 的 Linux 桌面平台中開啟，以進行 XServer 存取。防火牆規則會封鎖對此連接埠的所有外部主機存取。

Active Directory 的防火牆規則

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

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

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

設定 VMware Horizon 環境的步驟概觀

6

請完成下列高階工作以安裝 VMware Horizon 並設定初始部署。

表 6-1. VMware Horizon 安裝與設定檢查清單

步驟	工作
1	在 Active Directory 中設定所需的管理員使用者和群組。 指示：《Horizon 安裝》和 vSphere 說明文件。
2	如果您尚未執行，請安裝並設定 ESXi 主機和 vCenter Server。 指示：VMware vSphere 說明文件。
4	安裝並設定 Horizon 連線伺服器。同時要安裝事件資料庫。 指示：《Horizon 安裝》文件。
5	建立一或多部虛擬機器，以作為全複製桌面平台集區的範本或作為即時複製桌面平台集區的父系。 指示：《在 Horizon 中設定虛擬桌面平台》。
6	(選用) 為使用者設定 RDS 主機並安裝遠端應用程式。 指示：《在 Horizon 中設定已發佈的桌面平台和應用程式》。
7	建立虛擬和已發佈的桌面平台集區和/或應用程式集區。 指示：《在 Horizon 中設定虛擬桌面平台》和《在 Horizon 中設定已發佈的桌面平台和應用程式》。
8	控制使用者對桌面的存取權。 指示：《在 Horizon 中設定遠端桌面平台功能》。
9	在使用者的機器上安裝 Horizon Client，並讓使用者擁有其遠端桌面平台和應用程式的存取權。 指示：Horizon Client 說明文件，網址：https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。
10	(選用) 建立並設定其他管理員，賦予其特定詳細目錄物件和設定的不同存取層級。 指示：《Horizon 管理》文件。
11	(選用) 設定原則來控制 VMware Horizon 元件、桌面平台和應用程式集區，以及使用者之行為。 指示：《在 Horizon 中設定遠端桌面平台功能》。
13	(選用) 若要更安全，可整合智慧卡驗證或 RADIUS 雙因素驗證解決方案。 指示：《Horizon 管理》文件。