

# VMware Horizon 7 (7.11 版) 版本說明

2019 年 12 月 12 日發行

這些版本說明包含以下主題：

- [此版本的新增功能](#)
- [開始之前](#)
- [國際化](#)
- [相容性注意事項](#)
- [支援的 Windows 10 作業系統](#)
- [支援 Red Hat Enterprise Linux Workstation](#)
- [舊版的 Horizon 7](#)
- [已知問題](#)
- [已解決的問題](#)

## 此版本的新增功能

VMware Horizon 7 (7.11 版) 提供下列新功能和增強功能。本資訊依可安裝的元件進行分類。

- [產品增強功能](#)
- [Horizon Connection Server 內部部署](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon GPO 服務包](#)
- [Horizon Client](#)
- [Horizon 7 Cloud Connector](#)
- [在 VMware Cloud on AWS 上部署的 Horizon 7](#)

如需此版本中已解決問題的相關資訊，請參閱[已解決的問題](#)。

### 產品增強功能

VMware Horizon 7 (7.11 版) 版本包含 Horizon Connection Server 和 Horizon Agent 的許多新功能和增強功能，包括繼續建置 Horizon Console 的功能同位，即最終將取代 Horizon Administrator (將於 2020 年初淘汰) 的 HTML5 Web 主控台。

### Horizon Connection Server 內部部署

- [Horizon Console \(以 HTML5 為基礎的 Web 介面\)](#)  
Horizon Console 有數項增強功能。其中包括：
  - Horizon Console 現在是 Horizon 7 的主要和建議的 Web 介面。現有的 Flash 型 Horizon Administrator Web 介面仍受支援，但將在 2020 年初淘汰。請參閱《VMware Horizon Console 管理》文件中的[登入 Horizon Console](#) 主題。
  - Horizon Help Desk Tool 已整合至 Horizon Console，且更易於檢視。在 Horizon Console 中，按一下 [監視] > [服務台] 即可開啟 Horizon Help Desk Tool。請參閱《VMware Horizon Console 管理》文件中的[在 Horizon Console 中啟動 Horizon Help Desk Tool](#) 主題。

- 您可以自訂顯示在 RADIUS 雙因素驗證登入對話方塊中的使用者名稱和密碼標籤。請參閱《VMware Horizon Console 管理》文件中的[在 Horizon Console 中啟用雙因素驗證](#)主題。
- 您可以設定全域用戶端限制設定，以針對不受支援的 Horizon Client 版本，限制對桌面平台和已發佈應用程式的用戶端工作階段連線。請參閱《VMware Horizon Console 管理》文件中的[Horizon Console 中的用戶端工作階段的全域用戶端限制設定](#)主題。
- 您可以在 Horizon Console 中檢視每個連線伺服器的 CPU 和記憶體耗用量。請參閱《VMware Horizon Console 管理》文件中的[監視 Horizon Connection Server 的負載狀態](#)主題。
- 「管理 Composer 桌面平台集區映像」權限已重新命名為「管理自動桌面平台和伺服器陣列上的維護作業」權限。您可以使用此權限，在即時複製桌面平台集區或伺服器陣列上執行推送映像作業。請參閱《VMware Horizon Console 管理》文件中的[物件特定的權限](#)。
- 當您檢視伺服器陣列的工作階段資訊時，您可以檢視與工作階段相關聯的已發佈應用程式名稱。請參閱《VMware Horizon Console 管理》文件中的[在 Horizon Console 中管理已發佈的桌面平台和應用程式工作階段](#)主題。
- Cloud Pod 架構
  - 已確認在 Horizon 7 (7.11 版) 中，每個網繭可以有 12,000 個工作階段。
  - 若要查看包含特定桌面平台集區的全域桌面平台權利，您可以選取詳細目錄，>桌面平台 (在 Horizon Console 中)。包含桌面平台集區之全域桌面平台權利的名稱會顯示在 [桌面平台集區] 頁面上該桌面平台集區的 [全域權利] 欄中。您也可以按 [桌面平台集區] 頁面上按一下桌面平台集區名稱，然後在摘要索引標籤上檢視全域桌面平台權利的名稱。
  - 您可以設定備份全域權利。當主要全域權利因集區容量不足或網繭無法使用等問題而無法啟動工作階段時，備份全域權利可提供遠端桌面平台或已發佈的應用程式。備份全域權利可包含來自網繭聯盟中任何網繭的集區。請參閱《在 Horizon 7 中管理 Cloud Pod 架構》文件中的[實作備份全域權利](#)主題。
- 已發佈的桌面平台和應用程式
  - Horizon 7 支援在 Windows 10 虛擬桌面平台 (WVD) 主機或桌面平台集區上執行的通用 Windows 平台 (UWP) 應用程式。請參閱《在 Horizon Console 中設定已發佈的桌面平台和應用程式》文件中的[遠端桌面平台服務主機](#)主題。
- 虛擬桌面平台
  - 進度列會指出第一次為即時複製集區發佈的主要虛擬機器和快照的擱置中映像狀態。
- True SSO
  - 您可以使用搭配使用 Unified Access Gateway 應用裝置與 True SSO 功能的第三方身分識別提供者。請參閱《Horizon 7 管理》文件中的[設定 True SSO](#)主題。
- 負載平衡
  - VMware Avi Networks 支援連線伺服器、Unified Access Gateway 應用裝置和 App Volumes Manager 的負載平衡。

## Horizon Agent for Linux

- 支援的發行版
 

Horizon Agent for Linux 現在支援下列 Linux 遠端桌面平台的作業系統。如需詳細資訊，請參閱《設定 Horizon 7 for Linux 桌面平台》文件中的[Horizon 7 for Linux 的系統需求](#)主題。

  - RHEL 7.7
  - CentOS 7.7
  - CentOS 8.0
- RHEL/CentOS 8 桌面平台上的 True SSO
 

在執行 RHEL/CentOS 8 發行版的手動和自動完整複製桌面平台上，支援 True SSO 功能。即時複製 RHEL 8 桌面平台不支援 True SSO。請參閱《設定 Horizon 7 for Linux 桌面平台》文件中的[在 RHEL/CentOS 8 桌面上設定 True SSO](#)主題。

## Horizon Agent

- 遠端處理通訊協定
  - 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。請參閱

《Horizon 7 架構規劃》文件中的 [VMware Blast Extreme](#) 主題。

- HW 編碼器支援五個或更多監視器。
- 擱置中的訊息會分批處理並以較大的封包傳送，以減少資料傳輸的頻寬使用量。

- **遠端體驗**

- 管理員可以使用登錄機碼字串，或設定應用程式和程序的 GPO 設定 VMware AppTap 組態，以便在使用者登出遠端工作階段時，會忽略使遠端工作階段無法結束的應用程式和程序。GPO 設定列於《在 Horizon 7 中設定遠端桌面平台功能》文件中的 [VMware View Agent 組態的 ADMX 範本設定](#) 主題中。
- 準備在內嵌模式中使用桌面平台或 RDSH 映像時，您可以按任意順序安裝 Horizon Agent 和 Horizon Client。
- Horizon Agent 安裝程式支援已啟用 LSA 的機器。請參閱《在 Horizon Console 中設定虛擬桌面平台》文件中的[在虛擬機器上安裝 Horizon Agent](#) 主題。

## Horizon GPO 服務包

- VMware View Agent 組態 ADMX 範本檔 vdm\_agent.admx 包含下列新設定：
  - 啟用電池狀態重新導向
  - 在 RDSH 平台上啟用 UWP 支援
  - VMware AppTap 組態
- VMware Horizon Client 組態 ADMX 範本檔 vdm\_client.admx 包含下列新設定：
  - 將解析度和 DPI 儲存到伺服器

## Horizon Client

如需 Horizon Client 5.3 中各項新功能 (包括 HTML Access 5.3) 的相關資訊，請參閱 [Horizon Client 說明文件](#) 頁面上的版本說明。

## Horizon 7 Cloud Connector

適用於 VMware Horizon 全域授權客戶。Horizon 7 (7.6 版) 及更新版本必須要有 Horizon Cloud Connector 虛擬應用裝置這項元件，才能支援以 Horizon Cloud Service 來管理 Horizon 7 網繭。

## 在 VMware Cloud on AWS 上部署的 Horizon 7

如需 VMware Cloud on AWS 可支援的 Horizon 7 功能清單，請參閱 [VMware 知識庫文章 58539](#)。

## 開始之前

- **關於安裝 VMware View Composer 的重要注意事項**

如果您計劃要安裝或升級至 View Composer 7.2 或更新版本，您必須將 Microsoft .NET Framework 升級至 4.6.1 版。否則，安裝就會失敗。

- **關於安裝 VMware Tools 的重要注意事項**

如果您計劃安裝下載自「VMware 產品下載」的某個版本 VMware Tools，而不是隨著 vSphere 提供的預設版本，請確定該 VMware Tools 版本受支援。若要判斷支援的 VMware Tools 版本，請前往 [VMware 產品互通性對照表](#)，選取解決方案 VMware Horizon View 及版本，然後選取 VMware Tools (僅可下載項目)。

- 如果您想要以無訊息方式安裝 View Composer，請參閱 VMware 知識庫 (KB) 文章 2148204 [Microsoft Windows Installer Command-Line Options for Horizon Composer \(適用於 Horizon Composer 的 Microsoft Windows Installer 命令列選項\)](#)。
- 此 Horizon 7 版本包含有別於某些較舊版本的新組態需求。請參閱《Horizon 7 升級》文件以取得升級指示。
- 如果您想要升級 View 6.2 版本之前的 Horizon 7 安裝，以及使用依預設安裝之自我簽署憑證的連線伺服器、安全伺服器或 View Composer Server，您必須在執行升級之前移除現有的自我簽署憑證。如果現有的自我簽署憑證依然存在，連線可能會無法作用。在升級期間，安裝程式不會取代任何現有的憑證。移除舊的自我簽署憑證可確保會安裝新憑證。相較於 6.2 之前的版本，此版本的自我簽署憑證的 RSA 金鑰較長 (2048 位元，而非 1024 位元)，使用的簽章也較強大 (SHA-256 搭配 RSA，而非 SHA-1 搭配 RSA)。請注意，自我簽署憑證

不安全，應該盡快以 CA 簽署的憑證取代，而 SHA-1 憑證也不再被視為安全，應該以 SHA-2 憑證取代。VMware 的建議是不要移除為生產用途而安裝的 CA 簽署憑證。升級至此版本後，CA 簽署憑證仍可持續運作。

- 在您執行全新安裝，或將所有連線伺服器執行個體升級至 Horizon 7 (7.2 版) 或更新版本之後，即無法將連線伺服器執行個體降級至 Horizon 7 (7.2 版) 以前的版本，因為用來保護 LDAP 資料的金鑰已變更。在規劃升級至 Horizon 7 (7.2 版) 或更新版本的作業時若想保有降級連線伺服器執行個體的可能性，您必須在開始升級之前執行 LDAP 備份。如果需要降級連線伺服器執行個體，您必須降級所有的連線伺服器執行個體，然後將 LDAP 備份套用至降級的最後一個連線伺服器。
- 安裝 Horizon Agent 時選取 [掃描器重新導向] 安裝選項可能會明顯影響到主機合併率。為確保最佳的主機合併率，請確定只為那些需要它的使用者選取 [掃描器重新導向] 安裝選項。(依預設，安裝 Horizon Agent 時不會選取 [掃描器重新導向] 選項。)針對需要掃描器重新導向功能的使用者，設定獨立的桌面平台集區，並只在該集區中選取安裝選項。
- Horizon 7 僅使用 TLSv1.1 和 TLSv1.2。在 FIPS 模式中，則僅使用 TLSv1.2。您可能無法連線至 vSphere，除非您套用 vSphere 修補程式。如需重新啟用 TLSv1.0 的相關資訊，請參閱《Horizon 7 升級》文件中的[在從連線伺服器連往 vCenter 的連線上啟用 TLSv1](#) 和 [在從 View Composer 連往 vCenter 和 ESXi 的連線上啟用 TLSv1](#)。
- 6.2 之前的版本不支援 FIPS 模式。如果您在 Windows 中啟用 FIPS 模式，並將 Horizon Composer 或 Horizon Agent 從早於 Horizon View 6.2 的版本升級至 Horizon 7 (7.2 版) 或更新版本，則不會顯示 FIPS 模式選項。您必須執行全新安裝，而不是在 FIPS 模式中安裝 Horizon 7 (7.2 版) 或更新版本。
- Linux 桌面平台針對 VMware Blast 顯示通訊協定使用連接埠 22443。
- 從 Horizon 7 (7.2 版) 開始，您可以透過連線伺服器來對加密套件強制執行排序。如需詳細資訊，請參閱《Horizon 7 安全性》文件。
- 從 Horizon 7 (7.2 版) 開始，連線伺服器必須能夠在連接埠 32111 上與相同網蔴中的其他連線伺服器進行通訊。如果在安裝或升級期間封鎖此流量，則安裝將不會成功。
- 從 Horizon 7 (7.3.2 版) 開始，連接埠 443 上的 TLS 信號交換必須在 10 秒內完成，如果已啟用智慧卡驗證，則必須在 100 秒內完成。先前的 Horizon 7 版本則允許連接埠 443 上的 TLS 信號交換在 100 秒內完成，不論是哪种情況都一樣。您可以設定 `handshakeLifetime` 組態內容，以調整連接埠 443 上的 TLS 信號交換時間。您也可以選擇將負責處理過度執行 TLS 信號交換的用戶端自動新增到黑名單。來自黑名單用戶端的新連線在處理之前會先延遲一段可設定期間，讓來自其他用戶端的連線能夠優先受到處理。您可以設定 `secureHandshakeDelay` 組態內容來啟用此功能。如需關於設定組態內容的詳細資訊，請參閱《Horizon 7 安全性》文件。
- 當遠端桌面服務角色不存在時，Horizon Agent 安裝程式會提示您以 RDS 模式或桌面平台模式安裝 Horizon Agent。

## 國際化

Horizon Administrator 和 Horizon Console 使用者介面、Horizon Administrator 和 Horizon Console 線上說明以及 Horizon 7 產品說明文件提供日文、法文、德文、西班牙文、簡體中文、繁體中文及韓文版本。如需說明文件，請參閱 [VMware Horizon 7 說明文件中心](#)。

## 相容性注意事項

- 若是單一使用者機器和 RDS 主機上 Horizon Agent 所支援的客體作業系統，請參閱 VMware 知識庫 (KB) 文章 2150295：[Supported Windows Versions for Remote Desktop Systems for Horizon Agent \(Horizon Agent 的遠端桌面系統所支援的 Windows 版本\)](#)。
- 若您使用 Horizon 7 伺服器搭配 View Agent 6.2 之前的版本，則您將需要啟用 PCoIP 連線的 TLSv1.0。6.2 之前版本的 View Agent 僅針對 PCoIP 支援安全性通訊協定 TLSv1.0。Horizon 7 伺服器 (包含連線伺服器和安全伺服器) 皆會依預設停用 TLSv1.0。您可依照 VMware 知識庫 (KB) 文章 2130798 中的指示，在這些伺服器上為 PCoIP 連線啟用 TLSv1.0：[Configure security protocols for PCoIP for Horizon 6 version 6.2 and later, and Horizon Client 3.5 and later](#) (為 Horizon 6 (6.2 版) 及更新版本，以及 Horizon Client 3.5 及更新版本設定 PCoIP 的安全性通訊協定)。
- 如需 Horizon Agent 支援的 Linux 客體作業系統，請參閱《設定 Horizon 7 for Linux 桌面平台》文件中的



## Horizon 7 for Linux 的系統需求。

- 如需連線伺服器、安全伺服器和 View Composer 支援的作業系統，請參閱《Horizon 7 安裝》文件中的[伺服器元件的系統需求](#)。
- Horizon 7 功能已透過本版本隨附的一組更新的 Horizon Client 進行增強。例如，使用 VMware Blast Extreme 連線需要 Horizon Client 4.0 或更新版本。如需受支援的 Horizon Client 的相關資訊，請參閱 [VMware Horizon Client 說明文件](#) 頁面。
- 即時複製功能需要 vSphere 6.0 Update 1 或更新版本。
- Windows 7 和 Windows 10 支援即時複製，但 Windows 8 或 Windows 8.1 則不支援。
- 請參閱 [VMware 產品互通性對照表](#)，取得 Horizon 7 與 vSphere 目前版本和舊版之間相容性的資訊。
- 如需受支援的 Active Directory Domain Services (AD DS) 網域功能等級，請參閱《Horizon 7 安裝》文件中的[準備 Active Directory](#)。
- 如需更多系統需求 (例如 Horizon Administrator 支援的瀏覽器)，請參閱《Horizon 7 安裝》文件。
- 根據 RFC 7465「禁止 RC4 加密套件」、RFC 7568「取代安全通訊端層 3.0 版」、PCI-DSS 3.1「支付卡產業 (PCI) 資料安全標準」，以及 SP800-52r1「選取、組態和使用傳輸層安全性 (TLS) 實作的準則」，Horizon 7 元件中的 RC4、SSLv3 和 TLSv1.0 會依預設停用。如果您需要在連線伺服器、安全伺服器、View Composer 或 Horizon Agent 機器上重新啟用 RC4、SSLv3 或 TLSv1.0，請參閱《Horizon 7 安全性》文件中的[View 中已停用的舊版通訊協定和加密](#)。
- 如果已為 PCoIP 連線部署 PCoIP 安全閘道 (PSG)，則零用戶端軟體必須是 4.0 版或更新版本。
- 使用用戶端磁碟機重新導向 (CDR) 時，部署 Horizon Client 3.5 或更新版本以及 View Agent 6.2 或更新版本，可以確保 CDR 資料在從外部用戶端裝置傳送至 PCoIP 安全伺服器以及從安全伺服器傳送至遠端桌面平台時，都是透過加密虛擬通道來進行。如果您部署較舊版本的 Horizon Client 或 Horizon Agent，則連往 PCoIP 安全伺服器的外部連線會加密，但在公司網路內從安全伺服器傳送至遠端桌面平台的資料則不會加密。您可以在 Active Directory 中設定 Microsoft 遠端桌面平台服務群組原則設定，以停用 CDR。如需詳細資料，請參閱《在 Horizon 7 中設定遠端桌面平台功能》文件中的〈[管理用戶端磁碟機重新導向的存取](#)〉。
- Horizon Agent 安裝程式中的 [USB 重新導向] 安裝選項依預設會取消選取。您必須選取此選項才能安裝 USB 重新導向功能。如需安全使用 USB 重新導向的指引，請參閱《Horizon 7 安全性》文件中的[在安全 View 環境中部署 USB 裝置](#)。
- 全域原則、多媒體重新導向 (MMR) 預設為拒絕。若要使用 MMR，必須開啟 Horizon Administrator、編輯全域原則，以及明確地將此值設定為允許。若要控制 MMR 的存取，您可以全域啟用或停用多媒體重新導向 (MMR) 原則，或針對個別集區或使用者加以啟用或停用。會在沒有進行應用程式加密時，在網路傳送多媒體重新導向 (MMR) 資料，依據重新導向的內容，可能會包含敏感資料。請僅在安全網路上使用 MMR，以確保該資料在網路上不會被監控。
- 在 Horizon Administrator 中設定透明分頁共用 (TPS) 的層級之前，VMware 建議您瞭解安全性含意。如需準則，請參閱 VMware 知識庫 (KB) 文章 2080735 [Security considerations and disallowing inter-Virtual Machine Transparent Page Sharing \(安全考量以及不允許在虛擬機器間使用透明分頁共用\)](#)。
- 若要在 vSphere 5.5 或更新版本的環境中使用 View 儲存加速器，則桌面平台虛擬機器必須為 512 GB 或更小。在大於 512 GB 的虛擬機器上將停用 View 儲存加速器。將由 VMDK 總容量定義虛擬機器大小。例如，一個 VMDK 檔案可能為 512 GB 或一組 VMDK 檔案總大小為 512 GB。此需求也適用於使用較舊 vSphere 版本並升級至 vSphere 5.5 版所建立的虛擬機器。
- Horizon 7 不支援 vSphere Flash Read Cache (以前稱為 vFlash)。
- 在 Horizon (隨附 View) 6.0 版及更新版本中，View PowerCLI Cmdlet Get-TerminalServer、Add-TerminalServerPool 和 Update-TerminalServerPool 已過時。
- 在 vSphere 6.0 和更新版本中所建立之虛擬機器中的畫面 DMA 會依預設停用。View 需要啟用畫面 DMA。若畫面 DMA 停用，則使用者會在連線至遠端桌面平台時看到黑色畫面。當 Horizon 7 佈建桌面平台集區時，它會針對集區中 vCenter Server 管理的所有虛擬機器自動啟用畫面 DMA。不過，若 Horizon Agent 以未受管理模式 (VDM\_VC\_MANAGED\_AGENT=0) 安裝於虛擬機器中，則畫面 DMA 不會啟用。如需關於手動啟用畫面 DMA 的資訊，請參閱 VMware 知識庫 (KB) 文章 2144475 [Manually enabling screen DMA in a virtual machine \(在虛擬機器中手動啟用畫面 DMA\)](#)。
- vSphere 2016 和更新版本支援啟用 vGPU 的即時複製桌面平台集區。
- Microsoft Windows Server 需要在 Horizon 7 環境中的所有連線伺服器之間開放某個動態範圍的連接埠。Microsoft Windows 需要這些連接埠來進行遠端程序呼叫 (RPC) 和 Active Directory 複寫的一般作業。如需動態範圍連接埠的詳細資訊，請參閱 Microsoft Windows Server 說明文件。
- 在 Horizon 7 (7.2 版) 或更新版本中，viewDBChk 工具將無法存取 vCenter 或 View Composer 的認證。如有

需要，系統會提示您提供此資訊。

- 在此版本中，連線伺服器執行個體和安全伺服器所接收 HTTP 要求的轉送規則已變更。如果您已在 `locked.properties` 中定義自訂的 `frontMapping` 項目，則應先將其移除然後再升級。如果您想要禁止管理員連線至特定的連線伺服器執行個體，請將此項目新增至 `locked.properties`，而非定義自訂的 `frontMapping` 項目：

```
frontServiceWhitelist =  
tunnel|ajp:broker|ajp:portal|ajp:misc|moved:*|file:docroot
```

在安全伺服器上，系統會自動套用此項目，因此不需要在 `locked.properties` 中進行設定。

- Horizon Persona Management 與使用 UIA + 設定檔範本建立的使用者可寫入磁碟區不相容。
- 在 Horizon 7 (7.0.3 版) 或更新版本中，內部驗證會檢查並判斷即時複製和內部範本是否具有有效的 IP 位址和網路連線。如果虛擬機器的 NIC 在佈建期間無法獲指派 IP 位址，則即時複製佈建會失敗。
- 如需 Horizon 7 所支援的 NVIDIA GPU 卡型號的相關資訊，請參閱 <https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html>。
- 支援 AMD v340 圖形卡。
- 在 IPv6 環境中支援即時音訊視訊 (RTAV)。
- 如需 Horizon 7 與最新版本的 VMware Unified Access Gateway、VMware Identity Manager、VMware App Volumes、VMware User Environment Manager 和 VMware Tools 之間相容性的相關資訊，請參閱 [VMware 產品互通性對照表](#)。
- JMP Server 支援 VMware App Volumes 2.14 或更新版本，但不支援 App Volumes 4.0。若要使用 JMP Server，您必須安裝 2.14 或更新版本的 App Volumes 2.xx 版。
- 在 VMware Cloud on AWS 上，由於邏輯交換器的 NSX-t 限制，即時複製桌面平台集區和包含完整虛擬機器的桌面平台集區限制為 1000 個桌面平台。
- IPv6 環境中的 RDSH 即時複製集區不支援 PCoIP。在 IPv6 環境中的遠端桌面平台支援 PCoIP。
- 從 18.2.7 版開始，Avi 網路 (VMware NSX Advanced Load Balancer) 針對連線伺服器、Unified Access Gateway 應用裝置和 App Volumes Manager 支援負載平衡。

## 支援的 Windows 10 作業系統

如需受支援 Windows 10 作業系統的更新清單，請參閱 VMware 知識庫 (KB) 文章 2149393 [Supported Versions of Windows 10 on Horizon 7 \(Horizon 7 上受支援的 Windows 10 版本\)](#)。

如需 Windows 10 作業系統之升級需求的詳細資訊，請在此處參閱 VMware 知識庫 (KB) 文章 2148176 [Upgrade Requirements for Windows 10 Operating Systems \(Windows 10 作業系統的升級需求\)](#)。

## 支援 Red Hat Enterprise Linux Workstation

Horizon Agent for Linux 支援在執行 Red Hat Enterprise Linux Workstation 的系統上進行安裝。不支援 Red Hat Enterprise Linux Server。

在設定 [Horizon 7 for Linux 桌面平台](#) 文件中，所有的「Red Hat Enterprise Linux」和「RHEL」皆僅表示 Red Hat Enterprise Linux Workstation。

如需 Red Hat Enterprise Linux Workstation 的支援版本清單，請參閱 [Horizon 7 for Linux 的系統需求](#)。

## 舊版的 Horizon 7

舊版所包含的功能和存在的已知問題會在各版本的版本說明中說明。

## 已解決的問題

- 1864296：如果您最初是以使用者名稱和密碼進行登入，接著嘗試使用智慧卡驗證來登入已啟用「用戶端機器解除鎖定時，解除鎖定遠端工作階段」群組原則設定的本機機器，以便進行遞迴方式解除鎖定，然後又從 Horizon Client 啟用「以目前使用者身分登入」時，系統會出現 GSSAPI\_ERROR 訊息。
- 2260206：因為沒有對角色的驅動程式卸載回撥呼叫，Windows 虛擬機器未關閉。
- 2344754：由於拒絕權限，角色管理同步會按複寫間隔時間發生失敗。
- 2373674：當使用者登入啟用了深度安全性的遠端桌面平台時，機器將會在角色複製大型檔案時停滯。
- 2414242：啟用深度安全性之後，無法刪除從檔案共用複製到本機磁碟的檔案。
- 2403057：結合角色和深度安全性時，會發生 BSOD REGISTRY\_FILTER\_DRIVER\_EXCEPTION (135)。
- 2373808：安裝 Adobe Acrobat Reader 時，已啟用角色的 Windows 機器會當機，並出現 BSOD (檢查錯誤 3B)。
- 2403061：對於以日文文字處理器 Ichitaro 撰寫的文件，無法正常執行使用者設定檔同步化。
- 2292092：當桌面平台進行登出程序時，已登出的使用者可以登入相同的桌面平台。
- 2412281：使用 Blast 或 PCoIP 連線至 Windows 2016 發佈的桌面平台時，使用者無法儲存「在桌面語言列可用時使用它」設定。

## 已知問題

已知問題分類如下。

- [Horizon Persona Management](#)
- [View Composer](#)
- [Horizon Connection Server](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon GPO 服務包](#)
- [Horizon Client](#)
- [Horizon JMP Server 和 JMP Integrated Workflow](#)
- [Horizon Cloud Connector](#)

### Horizon Persona Management

- 在每次登入後，角色管理都會花費很長時間，在使用「v6」版使用者設定檔的客體作業系統上複製第一個使用者角色。
- 當您使用角色設定檔登入 Windows 10 LTSC 機器，並嘗試從 [快速存取] (例如 [下載] 或 [我的文件]) 存取重新導向的資料夾時，您會收到此錯誤：

無法使用 C:\Users\vdiuser7\Downloads。Microsoft 未提供可將資料夾或檔案新增至 [快速存取] 的 API。  
因應措施：無

- 當您第二次登入設定了角色管理的虛擬機器時，Microsoft Edge 瀏覽器會當機並出現錯誤訊息，指出先前未曾使用 OneDrive 應用程式。此外，檔案和資料夾皆無法正確複製。此問題發生於 Windows 10 組建編號 1703 及更新版本。

因應措施：停用角色管理設定漫遊本機設定資料夾。停用此設定時，Microsoft Edge 瀏覽器仍可正常運作，但只有在您首次登入時才可使用 OneDrive 應用程式。

- 在啟用了 Horizon Persona Management 設定的 Windows Server 2012 虛擬機器上，不會為檔案顯示「離線」圖示。  
因應措施：未知。

- 初次成功登入至 Horizon Agent 安裝在 Windows 10 (1703 版) CBB 系統上並啟用角色管理的虛擬機器之後，在後續登入嘗試期間顯示「OneDrive -不正確的映像錯誤」訊息。

**因應措施：** 請勿在 Windows 10 (1703 版) CBB 系統上使用 OneDrive。在群組原則管理編輯器中，於電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > 角色管理 > 漫遊與同步資料夾中停用「漫遊本機設定資料夾」設定。

## View Composer

- 在具有最新的 Windows 更新的 Windows Server 2016 上，從命令列執行 View Composer 安裝程式時，您會遇到 Microsoft .NET 4.6 架構錯誤。此問題發生的原因為 CLI 安裝程式無法識別最新版本的 Microsoft .NET 4.7。  
**因應措施：** 使用 View Composer 安裝程式使用者介面來執行安裝程式。
- 在將父系虛擬機器從 Windows 10 作業系統的組建編號 1511 升級為組建編號 1607 之後，建立或重新撰寫桌面平台集區失敗。組建編號 1607 為 Windows 10 年度更新版作業系統。  
**因應措施：**
  - 選項 1：在父系虛擬機器上執行 Windows 10 組建編號 1607 的全新安裝。
  - 選項 2：請勿在桌面平台集區建立精靈中選取「重新導向可處置的檔案」。
- 當您執行下列命令時，並無法連線到 View Composer：viewdbchk.cmd -findMachine  
**因應措施：** 將 View Composer 的自我簽署憑證匯入連線伺服器的金鑰儲存區中，或使用自訂的 CA 憑證。
- 由於 vSphere 6.7 上的「客體自訂」公用程式最近有所變更，在 Horizon 7 升級為 7.5 版期間，您無法將 View Composer 7.5 與舊版 Horizon Agent 搭配使用，以透過 Sysprep 自訂方法佈建和重新撰寫連結複製集區。在佈建或重新撰寫作業的期間，連結複製桌面平台和伺服器陣列會無限期地卡在自訂狀態中。  
**因應措施：** 在父虛擬機器上將 VMware Tools 升級至最新版並將 Horizon Agent 升級至 7.5 版，並對升級後的父虛擬機器建立快照。然後，在 vSphere 6.7 上使用 Sysprep 自訂方法來佈建或重新撰寫連結複製桌面平台集區。
- Win2k12 Standard 和 Datacenter 版的連結複製會停滯於自訂中狀態下。  
**因應措施：** 如需關於如何修正此問題的詳細資訊，請參閱 VMware 知識庫文章 <https://kb.vmware.com/s/article/57348>。

## Horizon Connection Server

- 佈建即時複製桌面平台集區期間，若資料存放區上沒有足夠的空間，Horizon Administrator 中顯示的錯誤訊息是「複製虛擬機器 <虛擬機器名稱> 失敗 - VC\_FAULT\_FATAL: 無法將分頁檔從 0 KB 交換到 2097152 KB。」此訊息未清楚指出問題的根本原因。  
**因應措施：** 非必要。
- 在 Horizon Administrator 中，若您移至類別目錄 > 桌面平台集區、按兩下即時複製桌面平台集區、移至詳細目錄索引標籤並按一下機器 (即時複製詳細資料)，則視窗會顯示即時複製的詳細資料。不過，作業系統磁碟資料存放區資料行不會顯示任何資訊。  
**因應措施：** 無
- 在大型環境中，即時複製桌面平台集區中的部分桌面平台可能會進入「無效的 IP」狀態。  
**因應措施：** 在 Horizon Administrator 中，移至集區詳細目錄，選取處於無效的 IP 狀態的桌面平台，然後按一下復原。
- 當您從 vCenter Server 或從 Windows 作業系統功能表重新啟動或重設桌面平台集區中已存在使用者工作階段的虛擬機器時，虛擬機器會重新啟動，但 Horizon Administrator 中虛擬機器的狀態可能會顯示為「已使用」狀態。  
下列集區類型可能會發生此問題：
  - 即時複製桌面平台集區。
  - 已啟用「登出時刪除」的連結複製浮動桌面平台集區。
  - 已啟用「登出時重新整理」的連結複製浮動桌面平台集區。
  - 已啟用「登出時刪除」的完整複製浮動桌面平台集區。**因應措施：** 使用 Horizon Administrator 或 Horizon Client 來重新啟動或重設即時複製桌面平台集區中的虛



擬機器。若虛擬機器已經是「已使用」狀態，請移除虛擬機器。此動作會根據集區佈建設定自動建立新的虛擬機器。

- 在本機資料存放區上佈建即時複製時，對應的主機無法進入維護模式。發生此狀況的原因是內部虛擬機器和即時複製儲存在本機資料存放區上，而使其無法進行移轉。

**因應措施：**刪除即時複製桌面平台集區。這會刪除相關的虛擬機器，並讓相應的主機可以進入維護模式。

- 如果主機上的即時複製父虛擬機器處於已開啟電源的狀態，則使用 VUM 進行 ESXi 主機修復會失敗。  
**因應措施：**如需詳細資訊，請參閱 VMware 知識庫 (KB) 文章 2144808：[Entering and exiting maintenance mode for an ESXi host that has Horizon instant clones](#) (讓具有 Horizon 即時複製的 ESXi 主機進入或退出維護模式)。
- 在 Windows Server 2016 和 Windows Server 2019 RDS 主機上，不支援以通用 Windows 平台 (UWP) 應用程式作為已發佈的應用程式。
- 針對 True SSO，對於您用來存取 Horizon Administrator 的連線伺服器，連線伺服器執行個體與註冊伺服器之間的連線狀態僅會顯示在 [系統健全狀況狀態] 儀表板上。例如，若您針對 Horizon Administrator 使用 `https://server1.example.com/admin`，則僅會針對 `server1.example.com` 連線伺服器收集註冊伺服器的連線狀態。您可能會看到下列一個或兩個訊息：
  - 無法連絡主要註冊伺服器以管理此連線伺服器上的工作階段。
  - 無法連絡次要註冊伺服器以管理此連線伺服器上的工作階段。

您必須將一個註冊伺服器設定為主要註冊伺服器。設定次要註冊伺服器則為選用。若您只有一個註冊伺服器，則只會看到第一個訊息 (在發生錯誤時)。若您有主要和次要註冊伺服器，且皆發生連線問題，則會看到兩個訊息。

- 當您在環境中設定 True SSO 時，若使用具有不同範本設定的 CA 和 SubCA，將可以使用 CA 或 SubCA 與另一個 CA 或 SubCA 的範本組合來設定 True SSO。因此，儀表板可能會將 True SSO 的狀態顯示為綠色。不過，當您嘗試使用 True SSO 時則會失敗。
- 在 Horizon Help Desk Tool 中，如果工作階段是本機工作階段或執行於本機網繭中的工作階段，則不會顯示網繭名稱。  
**因應措施：**設定 Cloud Pod 架構環境，以便在 Horizon Help Desk Tool 中檢視網繭名稱。
- Workspace ONE 模式的設定不會從 Workspace ONE 反映到複寫伺服器中。  
**因應措施：**在連線伺服器中設定 Workspace ONE 模式。
- 當您建立完整複製桌面平台集區時，有時會顯示錯誤的範本，並會因快取問題而使有效範本遭隱藏。  
**因應措施：**重新啟動連線伺服器。
- 當您嘗試在 Horizon Administrator 中新增 SAML 驗證器時，[管理 SAML 驗證器] 頁面上的新增按鈕會停用。  
**因應措施：**以具有管理員或本機管理員角色的使用者身分登入 Horizon Administrator。
- 在 Cloud Pod 架構環境中，從全域應用程式權利預先啟動的應用程式工作階段不會顯示在 Horizon Administrator 的詳細目錄 > 搜尋工作階段中。  
**因應措施：**登入主控網繭中連線伺服器執行個體的 Horizon Administrator 使用者介面，並選取監控 > 事件以檢視預先啟動的工作階段資訊。

- 獲指派 20 至 50 個 Cloud Pod 架構全域應用程式權利的使用者，在透過任何版本的 Horizon Client 進行連線而向 Horizon 7 驗證時，會延遲 20 至 30 秒。

**注意：**在 Horizon 7 (7.2 版) 中，此連線時間已有些許改善。

**因應措施：**無。

- 針對 Intel vDGA，僅支援 Haswell 和 Broadwell 系列的 Intel 整合式 GPU。僅 vSphere 6 Update 1b 和更新版本支援 Broadwell 整合式 GPU。vSphere 5.5 和更新版本支援 Haswell 整合式 GPU。必須先在 BIOS 中啟用 GPU 後，ESXi 才能加以識別。如需詳細資訊，請參閱特定 ESXi 主機的說明文件。Intel 建議將 BIOS 中的圖形記憶體設定保留為預設值。若您選擇變更設定，請將 Aperture 設定保留為預設值 (256M)。
- 根據設定要使用 NVIDIA GRID vGPU 之 View Composer 桌面平台集區的虛擬機器佈建失敗，發生下列錯誤：父資源集區中可用圖形資源的數量對此作業而言不足。  
**因應措施：**對叢集中設定要進行 3D 轉譯的所有虛擬桌面平台使用單一 vGPU 設定檔。

- 針對 vCenter Server 6.0 U3 或更新版本 (包括 vCenter Server 6.5)，內部的父虛擬機器會在故障期間移轉至另一台主機。由於目的地主機上有不必要的父虛擬機器，此移轉會導致問題。  
**因應措施：**將這些父虛擬機器手動移除。如需詳細資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件。
- 為了降低記憶體耗盡的可能性，具有 512 MB (或以下) 框架緩衝區的 vGPU 設定檔在 Windows 10 客體作業系統上僅支援一個虛擬顯示螢幕。

下列 vGPU 設定檔具有 512 MB (或以下) 的框架緩衝區：

- Tesla M6-0B、M6-0Q
- Tesla M10-0B、M10-0Q
- Tesla M60-0B、M60-0Q
- GRID K100、K120Q
- GRID K200、K220Q

**因應措施：**使用支援多個虛擬顯示螢幕，且至少具有 1 GB 框架緩衝區的設定檔。

- 已發佈的桌面平台和應用程式集區若已啟用用戶端限制功能，且有權使用已設定了單向 AD 信任的網域，就無法啟動。  
**因應措施：**無
- 升級之後，如果您的角色具有「管理伺服器陣列及桌面平台和應用程式集區」(物件特定權限)，則新增伺服器陣列的選項將呈現為灰色。  
**因應措施：**使用「管理伺服器陣列及桌面平台和應用程式集區」權限編輯角色或再次建立角色時，系統也會新增「管理全域組態和原則」權限。
- 升級之後，書籤並未顯示在 Workspace ONE 中。  
**因應措施：**請再次從 Workspace ONE 中的類別目錄新增書籤。
- 如果您拔除並重新接上網路線，然後在用戶端機器上按一下 [中斷連線並登出]，遠端桌面平台並不會中斷連線並登出。  
**因應措施：**手動關閉遠端桌面平台的視窗，然後中斷遠端工作階段的連線。
- 在 Horizon Administrator 中，為包含完整虛擬機器的自動集區進行複製程序時，即將完成步驟不會顯示多個欄位的值。不過，複製作業仍會成功完成。  
**因應措施：**無。
- 使用 Sysprep 自訂方法建立連結複製和完整複製時，在 Windows 10 客體作業系統上自訂和網域加入有時會失敗。  
**因應措施：**這是由於 Microsoft Windows 的問題導致。若要解決此問題，請依照 Microsoft 知識庫 (KB) 文章中的步驟：<https://support.microsoft.com/en-us/help/2769827>。
- 如果沒有已設定的 Horizon 7 授權，就無法在 Horizon Console 中建立連結複製桌面平台集區或伺服器陣列。  
**因應措施：**在沒有 Horizon 7 授權的情況下，請使用 Horizon Administrator 來建立連結複製桌面平台集區或伺服器陣列。
- 從 Internet Explorer 瀏覽器登入 Horizon Console 時，只會顯示關鍵字，而不會顯示圖示。當您使用 IP 位址而非 DNS 名稱連線至連線伺服器或安全伺服器時，即會發生此問題。  
**因應措施：**連線時請使用 DNS 名稱而非 IP 位址。如需詳細資訊，請參閱 VMware 知識庫 (KB) 文章 <https://kb.vmware.com/s/article/2150307>。
- 當您使用 Safari 10.1.1 版作為網頁瀏覽器來登入使用完整網域名稱的 Horizon Console 時，可能會發生底部面板出現空白之類的使用者介面問題。  
**因應措施：**Safari 10.1.1 版並非 Horizon Console 支援的網頁瀏覽器版本。請使用 Safari 版本早於 10.1.1 版或 11.0.2 版及更新版本來登入 Horizon Console。

- Cloud Pod 架構部署之全域 Linux 工作階段中的 Horizon Help Desk Tool 發生下列使用者介面問題：
  - 當您在 [詳細資料] 索引標籤上按一下工作階段詳細資料時，顯示發生內部錯誤的訊息、商務用 Skype 狀態未顯示，且作業系統版本顯示為「-」。
  - 當您按一下 [遠端協助] 時，顯示 [無法取得遠端協助票證] 訊息。
  - 當您按一下 [應用程式] 索引標籤時，顯示發生內部錯誤的訊息。

**因應措施：**無。Horizon Help Desk 不支援 Linux 桌面平台的下列使用者介面功能：商務用 Skype 狀態、遠端協助、[應用程式] 索引標籤和工作階段閒置狀態。
- 針對使用 VMFS6 搭配自動「取消對應」功能之 vSphere 6.7 版上的 vCenter Server，Horizon Administrator 不會更新空間回收資訊。
 

**因應措施：**無。
- 升級至 Horizon 7 (7.5 版) 之後，僅第一個安裝的連線伺服器可以連線至註冊伺服器。
 

**因應措施：**停止 Horizon Connection Server 服務，從 VMware Horizon View 憑證存放區中移除易記名為「vdm.ec」的憑證，然後重新啟動 Horizon Connection Server 服務。
- 如果您在逾時的 Horizon Console 索引標籤中存取 Horizon Administrator，然後從 Horizon Administrator 按一下 Horizon Console 連結，則 Single Sign-On 會無法運作。
 

**因應措施：**清除瀏覽器中的網站資料並重新啟動瀏覽器。
- 如果您在 Firefox、Google Chrome、Microsoft Edge、Firefox 或 Safari 網頁瀏覽器上使用 IP 位址來登入 Horizon Console，則登入 Horizon Console 會失敗。
 

**因應措施：**請使用完整網域名稱 (FQDN) 來登入 Horizon Console。如需有關使用 FQDN 登入 Web 應用程式的詳細資訊，請參閱《Horizon 7 安全性》文件。
- Horizon Administrator 會對下列使用者在 [使用者與群組] 頁面的使用者名稱欄中顯示空值/空值：帳戶操作員、傳入樹系信任建置器、終端機伺服器授權伺服器、Windows 授權存取群組、伺服器操作員以及 Pre-Windows 2000 Compatible Access。
 

**因應措施：**無。
- 升級至 vSphere 6.7 之後，您無法使用以 vSphere 早於 6.7 版本所建立的自訂規格。
 

**因應措施：**升級至 vSphere 6.7 之後，請建立新的自訂規格，並使用此規格進行集區佈建。
- Horizon Help Desk Tool 會一併顯示代理網繭和主控網繭的登入時間，但不會顯示非代理網繭亦非主控網繭的網繭的登入時間。如果代理網繭為遠端網繭，則 Horizon Help Desk Tool 會在幾分鐘後顯示主控網繭的登入時間。
 

**因應措施：**如果 Horizon Help Desk Tool 未顯示主控網繭的登入時間，請關閉顯示工作階段詳細資料的頁面，接著等待 7 - 8 分鐘，然後導覽至 [詳細資料] 索引標籤再次檢視工作階段詳細資料。
- VMware Identity Manager 有時無法啟動桌面平台。第一次在連線伺服器上已啟用 SAML 的 VMware Identity Manager 中儲存 SAML 組態詳細資料時，桌面平台不會啟動。
 

**因應措施：**再次儲存該設定檔，並對新設定檔執行同步作業。同步作業根據管理員所設定可能為每小時或每天進行。
- 當您嘗試以 CSV 格式匯出表格的內容時，處於匿名模式之 Chrome 上的 Horizon Administrator 會顯示錯誤：目前已開啟相同名稱的檔案，因此無法匯出該檔案。請關閉檔案然後再試一次，或使用不同的檔案名稱。
 

**因應措施：**請在 Chrome 的一般模式中使用 Horizon Administrator 來匯出表格。
- 當您使用 Sysprep 在 vCenter Server 6.7 上自訂 Windows 10 連結複製時，於佈建或重新撰寫作業期間，連結複製桌面平台會無限期卡在自訂狀態中。
 

**因應措施：**請使用 vCenter Server 6.5 U2 或更早版本。如果您必須使用 vCenter Server 6.7，則請使用 QuickPrep 自訂方法。

- 在 Horizon Administrator 中，您可以利用未驗證存取使用者身分來新增遠端存取使用者。不過，未驗證存取使用者無法從外部網路取得遠端存取權。使用者將無法存取虛擬桌面平台，且僅能以未驗證存取使用者身分來啟動應用程式。如果使用者嘗試使用一般存取權來登入，則會出現「要求的驗證類型不正確」錯誤訊息。  
**因應措施：**無。

- 當信任驗證設定的範圍設定為 [選擇性驗證] 時，Horizon Single Sign On 會失敗。

**因應措施：**使用以下其中一個因應措施來解決此問題。

- 使用全網域驗證。
- 繼續使用 [選擇性驗證] 安全性設定，但對每個 Horizon Connection Server 主機 (本機系統) 帳戶明確授與信任網域或樹系中電腦物件 (資源電腦) 所有網域控制站的 [允許驗證] 權限。如需如何授與 [允許驗證] 權限的資訊，請參閱 Microsoft 文章 Grant the Allowed to Authenticate permission on computers in the trusting domain or forest (授與信任網域或樹系電腦上的允許驗證權限)。

- 使用 Cloud Pod 架構功能時，在某些情況下，RDS 授權伺服器會對混合模式授權環境中的相同用戶端簽發多個永久授權。

**因應措施：**無。此問題是第三方問題，且即便沒有 Horizon 7，仍符合 Microsoft RDS 授權伺服器簽發授權的方式。

- 在 Horizon Administrator 中，針對 vSAN 資料存放區上所建立包含完整虛擬機器的連結複製集區或自動集區，在複製期間的「儲存空間最佳化」步驟中選取 [使用 VMware Virtual vSAN] 時，該選項並不會顯示。不過，複製作業仍會成功。

**因應措施：**無。

- 如果您在編輯包含完整虛擬機器的自動桌面平台集區時瀏覽資料存放區，將會發生下列問題：

- 在 [vCenter 設定] 索引標籤上按一下 [瀏覽資料存放區]，即會顯示建議的 GB 值下限。
- 在 [佈建設定] 索引標籤上增加機器數目上限，接著選取 [vCenter 設定] 索引標籤，然後按一下 [瀏覽資料存放區]。建議的 GB 值下限會增加，但會新增至現有的值。
- 對於包含三個機器，而其中一個可供使用，另一個仍處於自訂或佈建階段的桌面平台集區，編輯桌面平台集區並選取 [vCenter 設定] 索引標籤，然後按一下 [瀏覽資料存放區]。系統會顯示三個機器總計的建議 GB 值下限。

**因應措施：**在編輯包含完整虛擬機器的自動桌面平台集區時，使用 Horizon Administrator 瀏覽資料存放區，以檢視正確的建議 GB 儲存區下限。

- 如果您在編輯即時複製桌面平台集區時瀏覽資料存放區，將會發生下列問題：

- 在即時複製桌面平台集區的所有機器皆處於可用狀態後，編輯桌面平台集區，然後在 [vCenter 設定] 索引標籤上按一下 [瀏覽資料存放區]。[建議的最小值 (GB)]、[建議的最大值 (GB)] 和 [50% 使用量] 的值皆為正值。
- 在即時複製桌面平台集區的所有機器皆處於可用狀態後，編輯桌面平台集區，然後在 [佈建設定] 索引標籤上增加機器數目上限，接著在 [vCenter 設定] 索引標籤上按一下 [瀏覽資料存放區]。[建議的最小值 (GB)]、[建議的最大值 (GB)] 和 [50% 使用量] 的值皆會增加，但會新增至現有的值。
- 對於包含三個機器，而其中一個可供使用，另一個仍處於自訂或佈建階段的桌面平台集區，編輯桌面平台集區並選取 [vCenter 設定] 索引標籤，然後按一下 [瀏覽資料存放區]。系統會顯示所有三個機器的 [建議的最小值 (GB)]、[建議的最大值 (GB)] 和 [50% 使用量] 值。

**因應措施：**在編輯即時複製桌面平台集區時使用 Horizon Administrator 瀏覽資料存放區，以檢視正確的 [建議的最小值 (GB)]、[建議的最大值 (GB)] 和 [50% 使用量] 值。

- 如果您以兩個或多個名稱建立了包含完整虛擬機器的自動桌面平台集區，且 [保持開啟電源狀態的未指定機器數目] 值小於指定的實際名稱數，則在後續編輯集區時，[保持開啟電源狀態的未指定機器數目] 欄位將不會接受與集區建立程序期間所指定名稱總數相等的值，且會顯示不正確的錯誤訊息。

**因應措施：**使用 Horizon Administrator，以兩個或多個名稱編輯包含完整虛擬機器的自動桌面平台集區，以正確更新 [保持開啟電源狀態的未指定機器數目] 欄位值。



- 針對未進行其他組態的多數瀏覽器，使用 IP 位址或 CNAME 嘗試連線至 HTML Access 入口網站或其中一個管理主控台皆會失敗。在這種情況下大多會報告錯誤，但有時會顯示空白的錯誤訊息。  
因應措施：若要解決此問題，請參閱《Horizon 7 安全性》文件中的〈來源檢查〉。
- 設定商務用 Skype 時，[媒體旁路] 是一項啟用後會略過中繼伺服器的選用功能。  
為了讓 PSTN 使用者享有最佳化的商務用 Skype 往來通話，無論 [媒體旁路] 是否啟用，媒體將一律透過中繼伺服器進行路由。  
因應措施：無。商務用 Skype 的虛擬化套件不支援 [媒體旁路]。請參閱 <https://kb.vmware.com/s/article/56977>
- 如果同一使用者存在於需要在 Cloud Pod 架構環境中進行配對的兩個連線伺服器網繭中，Horizon Administrator 會將「來源網繭」的值顯示為 2，然後從兩個網繭找出使用者來源。管理員可以從兩個網繭編輯使用者，這可能會造成混合登入期間使用者組態不一致。此外，無法停用使用者的混合登入。  
因應措施：您必須從兩個網繭刪除使用者，然後重新建立使用者，並為使用者設定混合登入。
- 在 Horizon Administrator 中，對於從 vCenter Server 啟動的遠端工作階段，不會停用 [登出工作階段] 和 [中斷工作階段連線] 按鈕。  
因應措施：對於從 vCenter Server 啟動的遠端工作階段，使用 Horizon Console 取得已停用的 [登出工作階段] 和 [中斷工作階段連線] 按鈕功能。但是，當您導覽到 [詳細目錄] > [桌面平台]、選取桌面平台集區，並按一下 [機器] 索引標籤、[機器 (即時複製詳細資料)] 索引標籤或 [機器 (View Composer 詳細資料)] 索引標籤時，此功能無法運作。
- 在巢狀 ESXi 或巢狀虛擬 ESXi 上新增虛擬磁碟區資料存放區時，會產生核心傾印錯誤訊息。  
因應措施：無。
- 當您瀏覽 vSAN 資料存放區以匯入持續性磁碟時，Horizon Administrator 和 Horizon Console 都顯示內部資料夾名稱，而不是實際資料夾名稱。  
因應措施：無。
- 在 Horizon Administrator 和 Horizon Console 中，具有「管理服務台 (唯讀)」權限的自訂角色會顯示為適用於存取群組。  
因應措施：無。
- 具有管理員 (唯讀) 角色的使用者在 Horizon Administrator 中看不到 View 組態 > Cloud Pod 架構。  
因應措施：使用 Horizon Console。
- 在 Horizon Administrator 中，新增或編輯使用 vSAN 資料存放區的連結複製伺服器陣列時，[停機時間] 會停用。  
因應措施：使用 Horizon Console 為使用 vSAN 資料存放區的連結複製伺服器陣列設定停機時間。
- 在 Horizon Administrator 中，包含完整虛擬機器的自動桌面平台集區，其機器摘要中的 [重建] 按鈕無法運作。  
因應措施：在 Horizon Administrator 中，使用 [機器] > [vCenter Server] 中的重建功能。
- 使用現有的 PowerShell 指令碼向連線伺服器新增 vCenter Server 時，會顯示下列錯誤訊息：無法新增 VC 執行個體：沒有列舉常數 com.vmware.vdi.commonutils.ThumbprintAlgorithm.SHA-1。此問題發生的原因為，在 Horizon 7 (7.8 版) 新增針對自我簽署憑證指示憑證覆寫的 certificateEncoding 內容所導致。因此，具有不正確值 SHA-1 的舊版 VMware PowerCLI 指令碼無法成功執行。  
因應措施：更新 PowerShell 指令碼，使用內容值 DER\_BASE64\_PEM 取代 SHA-1。例如，設定為 \$certificate\_override.sslCertThumbprintAlgorithm = 'DER\_BASE64\_PEM'。
- 升級通用 Windows 平台 (UWP) 應用程式後，包含版本的路徑會發生變更，而無法以原始路徑存取應用程式。應用程式在 Horizon Administrator 中的狀態為無法使用，且使用者無法啟動應用程式。  
因應措施：升級之後，請在 Horizon Administrator 中更新應用程式路徑，並確認應用程式狀態為可用。或者，請不要升級應用程式。

- 如果為用戶端磁碟機重新導向功能設定了應用裝置篩選，當使用者使用 RDP 顯示通訊協定進行連線時，裝置篩選將無法正常運作。

**因應措施：**為用戶端磁碟機重新導向設定了裝置篩選時，請將連線伺服器設定為不允許 RDP 連線。

- True SSO 桌面平台解除鎖定功能在 PCoIP 和 Blast 通訊協定中受支援，但在遠端桌面平台通訊協定 (RDP) 中不受支援。
- 在 Horizon Console 中，使用者或群組摘要在下列情況下會因為網域信任問題而無法載入：
  - 使用者和群組屬於單向信任網域，且已登入的管理員具有單向信任網域中的必要權限。
  - 使用者和群組屬於雙向信任網域，且已登入的管理員具有雙向信任網域中的必要權限。
  - 使用者和群組屬於單向或雙向信任網域，且已登入的管理員來自於子網域，並且具有必要權限。

**因應措施：**使用 Horizon Administrator 存取使用者或群組摘要。

- 在 Horizon Console 中，可能會因為連線伺服器時間未按照連線伺服器時區正確設定，而未列出部分事件。  
**因應措施：**使用 Horizon Administrator 檢視所有事件。
- 您可以復原具有作用中工作階段的即時複製虛擬機器。Horizon Administrator 和 Horizon Console 皆會發生此問題。  
**因應措施：**無。

- 在 Horizon Administrator 和 Horizon Console 中，當您移除具有中斷連結的持續性磁碟的 vCenter Server 時，Horizon Administrator 仍會顯示該 vCenter 中的磁碟，但無法對這些磁碟進行操作。Horizon Console 不會顯示任何已中斷連結的磁碟，但會顯示內部錯誤橫幅。

**因應措施：**沒有已知的因應措施。在移除之前，請先確認 vCenter Server 中沒有已中斷連結的磁碟。

- 在 Horizon Console 中，當您建立手動桌面平台集區時，若 [工作階段類型] 選項為 [應用程式] 或 [桌面平台與應用程式]，則 [空白工作階段逾時 (僅限應用程式)] 欄位將不會更新。  
**因應措施：**編輯手動桌面平台集區，以更新 [空白工作階段逾時 (僅限應用程式)] 欄位。

- 使用 Windows 2019 安裝，且藉由在 vSphere 7 的 vSphere Client 中選取 Windows 2019 作業系統而建立的虛擬機器，在 Horizon 7 中不會列出或不受支援。  
**因應措施：**藉由在 vSphere Client 中選取 Windows 2016 作業系統版本，在虛擬機器上安裝 Windows 2019。

- 當您為即時複製桌面平台集區或伺服器陣列選取網路時，如果在 VMware Cloud on AWS 主控台中變更了區段名稱，Horizon Console 並不會反映連接埠群組或區段的新名稱。  
**因應措施：**無。

- 當您透過 Horizon 7 Administrator 主控台圖示，或藉由在瀏覽器的網址列中輸入 `https://localhost/admin` 或 `https://localhost/newadmin` 來啟動 Horizon Administrator 時，系統會將您重新導向至 `https://127.0.0.1/admin`。重新導向至 IP 位址可能會導致驗證失敗，如 VMware 知識庫 (KB) 文章 2150307 所述：[Cannot login to a VMware Web application such as Horizon Administrator or Horizon Help Desk Tool \(無法登入 VMware Web 應用程式，例如 Horizon Administrator 或 Horizon Help Desk Tool\)](#)。

**因應措施：**若要防止重新導向至 IP 位址，請在瀏覽器的網址列中輸入 `https://localhost/admin/` (請務必在 URL 的結尾處附加「/」)。

## Horizon Agent for Linux

本節說明在使用 Horizon Agent for Linux 或設定 Linux 桌面平台時可能會發生的問題。

- 有時在您連線至遠端桌面平台，並按一下 [協作 UI] 圖示後，[協作] 視窗可能不會顯示。

**因應措施：**調整桌面平台視窗的大小，或者重新連線至遠端桌面平台。

- 不支援在 vSphere 6.0 中於 RHEL 6.6 或 CentOS 6.6 虛擬機器上設定四部解析度為 2560x1600 的監視器。  
因應措施：使用 2048x1536 解析度或在 vSphere 5.5 中部署該組態。
- 如果鍵盤輸入法系統設為 `fcitx`，則 Linux 代理程式的鍵盤配置和地區設定不會與用戶端同步。  
因應措施：將鍵盤輸入法系統設定為 `iBus`。
- 使用系統安全服務精靈 (SSSD) 新增網域時，Single Sign On (SSO) 無法在 RHEL/CentOS 7.2 桌面平台上順利運作。  
因應措施：使用 SSSD 新增網域之後，請使用 VMware 知識庫文章 2150330 [SSO configuration changes required when using SSSD to join AD on RHEL/CentOS 7.2 Desktops](#) (使用 SSSD 在 RHEL/CentOS 7.2 桌面上加入 AD 時所需的 SSO 組態變更) 中的資訊修改 `/etc/pam.d/password-auth` 檔案。
- 如果使用智慧卡重新導向進行驗證的用戶端使用者連線至 Ubuntu 18.04/16.04 或 SLES/SLED 12 SP3 桌面平台，並在輸入 PIN 碼之前移除或重新插入智慧卡，桌面平台可能無法辨識所做的變更。  
必須在使用者關閉輸入 PIN 碼的提示後，桌面平台才會偵測到智慧卡狀態的變更。  
因應措施：在出現提示時，輸入智慧卡 PIN 碼，然後按一下 [確定]。或者，按一下 [取消] 以關閉提示而不輸入 PIN 碼。
- 當用戶端使用者連線至 Ubuntu 18.04/16.04 或 SLED/SLES 12 SP 3 桌面平台時，登入畫面會出現「錯誤 2306：沒有適用的權杖」會出現在登入畫面。  
此錯誤訊息表示智慧卡已從用戶端系統中移除。使用者可藉由輸入使用者密碼或重新插入智慧卡來登入桌面平台。
- 在 Ubuntu 16.04 上，如果管理員嘗試藉由在 `/etc/vmware/config` 組態檔中將 `WC.ScRedir.Enable` 設為「FALSE」來停用智慧卡重新導向，桌面平台將會停滯在登入畫面上。
- 在連線至 Ubuntu 16.04 桌面平台後，如果在進行智慧卡驗證時輸入了錯誤的 PIN 碼，用戶端使用者將會看見要求使用者輸入密碼的登入提示，而非輸入智慧卡 PIN 碼。  
用戶端使用者可以按一下 [確定] 以關閉該使用者密碼提示。此時會出現新的提示，要求使用者輸入智慧卡 PIN 碼。
- 在 Ubuntu 18.04/16.04 和 SLED/SLES 12 SP3 上，當使用者從用戶端系統中移除智慧卡時，桌面平台螢幕保護程式不會如預期鎖定。  
依預設，即使用戶端使用者移除了登入桌面平台的驗證所使用的智慧卡，桌面平台螢幕保護程式也不會鎖定。若要在這些情況下鎖定螢幕保護程式，您必須在桌面平台上設定 `pkcs11_eventmgr`。  
因應措施：設定 `pkcs11_eventmgr`，以指定正確的螢幕保護程式行為來回應智慧卡事件。
- 在 RHEL 7.0 桌面平台上安裝已啟用智慧卡重新導向 (`-m` 參數設定為「是」) 的 Horizon Agent 之後，Horizon Administrator、Horizon Console 或 vSphere 可能會顯示黑色畫面。執行 RHEL 7.1 或更新版本的桌面平台支援智慧卡重新導向。RHEL 7.0 桌面平台不支援此功能。  
因應措施：在執行 RHEL 7.1 或更新版本的桌面平台上，安裝已啟用智慧卡重新導向的 Horizon Agent。
- 如果將兩部監視器設定為不同的解析度，而主要螢幕的解析度低於次要螢幕的解析度，您可能會無法移動滑鼠或拖曳應用程式視窗至螢幕的某些區域。  
因應措施：確定主要監視器的解析度至少與次要監視器的解析度一樣高。
- 如果您在 RHEL 7 桌面平台上使用智慧卡，並啟用在移除智慧卡時鎖定畫面的選項，當您使用智慧卡登入後，畫面可能會立即鎖定。這是 RHEL 7 的已知問題。  
因應措施：若要存取桌面平台，請在使用智慧卡登入後將畫面解除鎖定。

- 在 FIPS 模式中，Horizon Agent 無法與連線伺服器配對，且在 Horizon Agent 安裝到非 C 磁碟機的其他磁碟機時，集區狀態無法使用。

**因應措施：**在 FIPS 模式中作業時，請在 C 磁碟機上安裝 Horizon Agent。

- 在 Windows Server 2016 上解除安裝 Horizon Agent 時，顯示關於應用程式目前使用中的警告訊息。  
**因應措施：**使用 Windows 的 [新增或移除程式] 來解除安裝 Horizon Agent 時，按一下出現之對話方塊中的 [忽略]。如果是從命令列解除安裝 Horizon Agent，請使用命令 `msiexec /x /qn {代理程式的 GUID}` 而非命令 `msiexec /x {代理程式的 GUID}`。

- 當您解除安裝 Horizon Agent 時，滑鼠速度會變慢且不順暢。解除安裝 Horizon Agent 時，系統也會解除安裝 vmkbd.sys 驅動程式。

**因應措施：**修復 Horizon Agent 虛擬機器上的 VMware Tools。

- 在 Windows 7 客體作業系統上，從 Horizon Agent 7.1 升級至 Horizon Agent 7.2 時，系統會顯示 [檔案使用中] 對話方塊。此對話方塊指出 VMware Horizon Agent 應用程式正在使用需要由安裝程式更新的檔案。  
**因應措施：**按一下「忽略」繼續執行升級。

- 如果登出時重新整理或刪除原則已啟用，在「設定檔管理」完成使用者資料的同步之前，桌面平台就會重新整理或刪除。

**因應措施：**無

- Windows 10 32 位元 Horizon Agent 安裝擲回「引數無效」例外狀況，而安裝在您按一下 [確定] 之後繼續。發生此錯誤是因為已停用列印多工緩衝處理器服務。  
**因應措施：**啟用列印多工緩衝處理器服務，安裝才能如預期般運作。
- 如果工作階段擁有者在協作工作階段期間觀看已使用 MMR 加速的視訊，協作者將會看見黑色畫面，而不是視訊。

**因應措施：**身為工作階段擁有者，如果您需要在協作工作階段期間播放視訊，請不要使用 Windows Media Player 或 Internet Explorer 播放視訊，或是應在啟用協作功能的集區上停用 MMR。

- 如果協作者加入了多監視器工作階段，並在其用戶端上啟用相對滑鼠模式，則滑鼠有可能會移至協作者看不見的次要監視器。

**因應措施：**將滑鼠移回畫面上。或者，不要在多監視器工作階段中使用相對滑鼠模式。

- 如果您使用 Chrome 搭配 URL 內容重新導向，且在篩選規則中針對 https 通訊協定設定「\*.google.\*」，並在 Chrome 中將 Google 設定為首頁，則每次開啟新索引標籤時皆會重新導向至 google.com。

**因應措施：**變更首頁或篩選規則。

- 設定協作工作階段時，從雙向信任的網域依電子郵件地址新增協作者會失敗。

**因應措施：**請使用「網域\使用者」的格式新增協作者。

- HTML5 多媒體重新導向對早於 1803 版之 Windows 10 虛擬桌面平台中的 Edge 可正常運作，但更新至最新的 Windows 10 1803 版本 (例如 17133) 之後，重新導向會無法運作，特別是針對使用自動播放的網站，例如 youtube.com。

**因應措施：**強制重新啟動 Windows 10 虛擬桌面平台。

- 當用戶端工作階段閒置時，即便使用 GPO 或非 GPO 方法為 [閒置工作階段逾時] 設定了 MaxIdleTime，已發佈的應用程式仍不會中斷連線。此時會出現中斷連線警告訊息，但應用程式不會中斷連線。

- 使用多媒體重新導向執行串流媒體的搜尋作業後，音訊和視訊會變得不穩定。

**因應措施：**等待數分鐘，或重新開啟目前的串流媒體。

- 有時，使用者在 Edge 瀏覽器中使用 HTML5 多媒體重新導向功能播放 YouTube 視訊時，視訊會一直緩衝處理，且沒有任何影像或聲音。



**因應措施：**重新整理頁面。

- 在連線至啟用了即時音訊視訊功能的遠端桌面平台後，您可能會看到下列訊息：「您的電腦需要重新啟動以完成此裝置的設定：*devicename* (VDI)。」

**因應措施：**您可以忽略此訊息，因為該裝置可在遠端桌面平台中使用。或者，您可以關閉 Windows 設定通知，以防止顯示該訊息。

- 如果您連線至使用多個高解析度監視器 (4K) 的桌面平台，並使用新的 Blast 轉碼器以全螢幕模式播放視訊，播放效能可能會很差 (畫面播放速率偏低)。

**因應措施：**使用 H.264 以全螢幕模式播放視訊。

- 將 Horizon Agent 安裝在 RDS 主機時，如果代理程式群組原則設定 **COM 連接埠隔離模式** 設為 **完全隔離** (預設設定)，使用者將無法使用具有序列埠重新導向功能的序列印表機。此問題對 Windows 和 Linux 用戶端都有影響。虛擬桌面平台不會發生此問題。

**因應措施：**編輯 **COM 連接埠隔離模式** 群組原則設置，將模式變更為 **隔離已停用**，然後重新啟動 Horizon Agent。如需詳細資訊，請參閱《在 Horizon 7 中設定遠端桌面平台功能》文件中的〈序列埠重新導向群組原則設定〉。

- 使用 VMware Integrated Printing 功能時，如果您從 Windows 7 用戶端機器連線至 Windows 10 代理程式機器，並從重新導向的印表機列印包含 Delta 字型的文件，這些字型將不會正確顯示。

**因應措施：**無。這是第三方問題。

## Horizon GPO 服務包

- 即時複製上不會套用需要重新開機才能生效的電腦全域原則物件 (GPO)。

**因應措施：**請參閱 VMware 知識庫 (KB) 文章 [2150495](#)。

- 在第一層級桌面平台 (已安裝 Horizon Client 和 Horizon Agent 的機器) 為虛擬桌面平台，第二層級桌面平台是已發佈桌面平台的巢狀模式組態中，如果您在第一層級虛擬桌面平台中設定了「重新導向用戶端印表機時指定篩選器」群組原則設定，該設定不會影響第二層級桌面平台。

**因應措施：**如果您想要篩選第二層級桌面平台的印表機，請在第二層級桌面平台中設定「重新導向用戶端印表機時指定篩選器」群組原則。

## Horizon Client

本節說明使用者在使用 Horizon Client 或 HTML Access 連線至遠端桌面平台和應用程式時，可能會遇到的問題。若要了解只會在特定 Horizon Client 平台發生的問題，請參閱 [Horizon Client 說明文件頁面](#) 上的 Horizon Client 版本說明。

- RDS 主機上的多個使用者工作階段遺漏設定檔資料。當工作階段處於中斷連線狀態，但 RDS 主機上的工作管理員仍顯示這些工作階段時，則會發生此問題。

**因應措施：**從 RDS 主機刪除工作階段，或將使用者登出已發佈的桌面平台或應用程式。

- 當您登入 Workspace ONE 時，系統不會觸發預先啟動的應用程式工作階段。僅在從 Horizon Client 成功登入至連線伺服器時才會觸發預先啟動的工作階段。

**因應措施：**從 Workspace ONE 手動啟動應用程式或桌面平台，以觸發啟用了預先啟動之應用程式的啟動作業。

- 使用 VMware Blast 顯示通訊協定並停用 Blast 安全閘道 (BSG) 時，Horizon Client 有時會無法從短暫的 (約 1 分鐘) 網路中斷復原，而使桌面平台的連線中斷。在啟用 BSG 時不會發生此問題。

**因應措施：**重新連線工作階段。

- RDS 主機只會儲存工作階段中第一次啟動應用程式時的一組應用程式資料。任何後續的應用程式啟動資料都會遺失。  
**因應措施：**登出工作階段，並啟動另一個應用程式以儲存該資料。
- 當您從 Internet Explorer 或 Microsoft Edge 網頁瀏覽器使用 HTML Access 連線至 Windows 10 用戶端作業系統上的連線伺服器、安全伺服器或複寫伺服器時，無法啟動桌面平台。此問題會影響使用 Windows 10 N、Windows 10 KN、Windows 7 N 以及 Windows 7 KN 客體作業系統的桌面平台。  
**因應措施：**透過 Firefox 或 Google Chrome 網頁瀏覽器使用 HTML Access。
- 針對 Intel vDGA，多台監視器支援僅限於 3 台監視器以內。Intel 驅動程式僅支援最多 3 台監視器，解析度可高達 3840 X 2160。若您嘗試連線 4 台監視器，則連線會顯示 3 個黑色畫面，僅一個畫面能夠正常運作。
- 如果 VDI 桌面平台位於遠端位置，且具有高度網路延遲狀況，則使用智慧卡驗證的遞迴解除鎖定可能無法正常運作。  
**因應措施：**手動將桌面平台解除鎖定。
- 如果 Windows 8 遠端桌面的使用者使用 Kerberos 驗證登入，而桌面已鎖定，則 Windows 8 依預設顯示給使用者用來解除鎖定桌面的使用者帳戶是相關的 Windows Active Directory 帳戶，而不是來自 Kerberos 網域的原始帳戶。使用者看不到其用於登入的帳戶。這是 Windows 8 的問題，不是 Horizon 7 本身的問題。可能但通常 Windows 7 中不會發生此問題。  
**因應措施：**使用者必須選取「其他使用者」來解除鎖定桌面。然後 Windows 會顯示正確的 Kerberos 網域，使用者即可使用 Kerberos 身分登入。
- 當您使用 Ambir Image Scan Pro 490i 在遠端桌面平台或應用程式上執行掃描時，對話方塊一律會顯示「掃描中...」，且不會完成。  
**因應措施：**在用戶端上執行掃描。用戶端掃描會校準掃描器。校準作業完成後，請儲存校準檔案，並將其部署至 ProgramData\AmbirTechnology\ImageScanPro490i
- 在 Horizon 7 for Linux 桌面平台中，Unicode 鍵盤輸入搭配 HTML Access 時無法正常運作。
- 連線至 Linux 桌面平台時，某些鍵盤輸入無法正常運作。例如，如果您在用戶端裝置和遠端桌面平台上都使用非英文 IME，有些非英文按鍵將無法正確顯示。  
**因應措施：**在用戶端裝置上設定英文 IME，並在遠端桌面平台上設定非英文 IME。
- Skype 對商務用 Skype 的語音通話有時候無法正確啟動。在商務用 Skype 用戶端上，通話狀態會顯示為「電話正在連線...」。  
**因應措施：**無。
- 如果您在非持續性桌面平台內使用商務用 Skype，可能會達到 16 個裝置憑證的商務用 Skype 限制。達到此限制時，商務用 Skype 會嘗試使用新登入，且在新憑證核發後，將會撤銷最舊的已指派憑證。
- 如果您啟動已啟用 FIPS 模式的 Linux 版 Horizon Client 4.8 或更早版本，且嘗試連線至已啟用 FIPS 模式的 Horizon Agent 7.6 或 Horizon 連線伺服器 7.6 (或更新版本)，則會顯示錯誤訊息「rds-license 的授權資訊無效：遺失用戶端識別碼」。  
**因應措施：**若要使用已啟用 FIPS 模式的 Linux 版 Horizon Client 連線至已啟用 FIPS 模式的 Horizon Agent 7.6 (或更新版本) 或 Horizon 連線伺服器 7.6 (或更新版本)，請使用 Linux 版 Horizon Client 4.9 或更新版本。
- 在 macOS 10.15、iOS 13 和 Chrome OS 76 上執行的 Chrome 瀏覽器、Safari 瀏覽器或 VMware Horizon Client，可能無法使用在 Unified Access Gateway、Horizon Connection Server 和安全伺服器上產生的預設自我簽署 TLS 伺服器憑證。出現此問題的原因可能是，上述作業系統版本的 Apple 變更了受信任 TLS 伺服器憑證的需求。預設的自我簽署憑證目前不符合這些新需求。如果從用戶端到 Horizon 的連線通過終止了 TLS 的中繼負載平衡器或 Proxy，則在這些裝置上也必須符合新的憑證需求。在 macOS 10.15 上的 Mac 版 Horizon Client 中，若未驗證自我簽署憑證，「在連線至未受信任的伺服器前提出警告」模式可能無法繼續，並彈出「不受信任的伺服器連線」對話方塊，其中顯示錯誤訊息「VMware Horizon Client 無法驗證您的連線。請連絡您的管理員」，且只有「顯示憑證」和「不要連線」按鈕可供使用。

**因應措施：**VMware 通常會建議將這些產品上的預設自我簽署 TLS 伺服器憑證，取代為由受信任的 CA 為環境簽署的憑證。此建議無論何時都是一個很好的安全準則。在此情況下，只要受信任的 CA 簽署的憑證符合新的 Apple 需求，就不會發生此問題。針對 macOS 和 iOS Horizon 用戶端，替代的因應措施是將 SSL 組態設為不驗證伺服器憑證。如需 Apple 憑證需求的詳細資訊，請參閱 <https://support.apple.com/zh-tw/HT210176>

## Horizon JMP Server 和 JMP Integrated Workflow

- 在已安裝多個 JMP Server 的環境中，如果一個以上的 JMP 伺服器參照相同的 User Environment Manager 組態共用，則在建立或刪除 JMP 指派時可能會發生衝突。

**因應措施：**無。

- 如果您設定了 JMP 設定為僅使用一個 VMware App Volumes Manager，且如果您在 JMP 指派建立期間所選取桌面平台集區之 Horizon Agent 未指向該設定的 App Volumes Manager，您仍可從桌面平台集區之 Horizon Agent 所指向的 App Volumes Manager 執行個體選取 AppStack。此外，如果您將 [JMP 設定] 設定為使用多個 App Volumes Manager 執行個體，即便您所選取桌面平台集區的 Horizon Agent 指向這其中一個 App Volumes Manager 執行個體，您仍可從 JMP 設定中設定的其他 App Volumes Manager 執行個體選取 AppStack。不過，當桌面平台集區啟動時，從那些其他 App Volumes Manager 選取的 AppStack 將無法使用。

**因應措施：**無。

- 如果現有 JMP 指派所使用的 AppStack 是使用 App Volumes Manager 或藉由編輯 JMP 指派來重新命名，則現有 JMP 指派的摘要頁面並不會更新為新的 AppStack 名稱。

**因應措施：**無。

- 如果您有已向相同 JMP Server 執行個體登錄並使用相同 App Volumes Manager 的兩個 Horizon 7 執行個體，則從其中一個 Horizon 7 執行個體刪除 JMP 指派時，可能會刪除另一個 Horizon 7 執行個體中其他 JMP 指派所使用的 AppStack 指派。

**因應措施：**無。

- 在 [JMP 設定] 頁面中新增或編輯 Active Directory 資訊時，如果針對繫結使用者名稱輸入的值包含一或多個 30 個三位元組範圍內的中文字元 (例如「試」字元)，則作業會失敗並導致 Active Directory 驗證失敗。

**因應措施：**請使用來自具有管理權限，且不包含任何 30 個三位元組中文字元 (例如「試」字元) 之 Active Directory 的另一個繫結使用者名稱。

- 在 [JMP 設定] 頁面中新增或編輯 App Volumes Manager 執行個體資訊時，如果針對服務帳戶使用者名稱輸入的值包含一或多個 30 個三位元組範圍內的中文字元 (例如「試」字元)，則作業會失敗並導致 App Volumes Manager 執行個體驗證失敗。

**因應措施：**請使用來自具有管理權限，且不包含任何 30 個三位元組中文字元 (例如「試」字元) 之 App Volumes Manager 執行個體的另一個繫結使用者名稱。

- 啟動 Windows 10 1703 桌面平台集區時，不會顯示使用 VMware Dynamic Environment Manager 9.2.1 版對應的磁碟機對應設定。

**因應措施：**請在啟動 Windows 10 1703 桌面平台集區後，執行下列命令。

```
C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe -UemRefreshDrives
```

如需其他資訊，請參閱 VMware 知識庫 (KB) 文章 <https://kb.vmware.com/s/article/2113657>。

- 如果您使用 localhost 來存取 Horizon Console，則在 Horizon Console 的 [JMP 設定] 窗格中會顯示錯誤訊息「目前無法連線到 JMP Server。」。

**因應措施：**請僅使用完整網域名稱 (FQDN)，而非使用 localhost 來存取 Horizon Console。

- 建立新 JMP 指派時，應用程式索引標籤中可能會出現下列警告訊息：「與選取的桌面平台集區相關聯的 App Volumes 執行個體不符合任何已登錄的 App Volumes 執行個體。」當下列其中一項成立時，即會發生此問題：

- 桌面平台集區中使用的 App Volumes Agent 是使用 IP 位址而非完整網域名稱 (FQDN) 安裝
- 桌面平台集區中使用的 App Volumes Agent 是使用 FQDN 安裝，但 JMP 設定中登錄的卻是 App Volumes Manager 執行個體的 IP 位址。

**因應措施：**請使用 FQDN 重新安裝 App Volumes Agent，並在設定 (JMP) > App Volumes 索引標籤中登錄 App Volumes Manager 執行個體時使用 FQDN。

- 安裝 VMware Horizon JMP Server 時，因為 McAfee Antivirus 偵測到 NSSM.EXE 為威脅，導致 JMP Server 安裝程式無法繼續。

**因應措施：**重新安裝 JMP Server 之前，請將下列檔案新增至 McAfee Antivirus 排除清單。

C:\Program Files (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe

C:\Program Files (x86)\VMware\JMP\com\xmp\node\_modules\winser\bin\nssm.exe

- 如果您在 Horizon 7 連線伺服器安裝期間選取會建立 BUILTIN\Administrators 群組而非 <domainName>\Administrator 的授權本機管理員群組選項，則使用 Horizon Console 新增 JMP Server 資訊的作業會失敗並顯示錯誤訊息「Horizon 權限不足」。

**因應措施：**請使用 Horizon Administrator，並以完整管理員存取權來登錄

<domainName>/administrator。重新登入 Horizon Console，並新增 JMP Server 資訊。

- 當您要建立 JMP 指派並將游標懸停在即時複製桌面平台集區時，針對 [3D 轉譯器] 選項所顯示的值為已停用而非使用 vSphere Client 管理。

**因應措施：**無。

- 當信任驗證設定的範圍設定為 [選擇性驗證] 時，JMP Server 登錄會失敗。

**因應措施：**使用以下其中一個因應措施來解決此問題。

- 使用全網域驗證。
- 繼續使用 [選擇性驗證] 安全性設定，但對每個 Horizon Connection Server 主機 (本機系統) 帳戶明確授與信任網域或樹系中電腦物件 (資源電腦) 所有網域控制站的 [允許驗證] 權限。如需如何授與 [允許驗證] 權限的資訊，請參閱 Microsoft 文章 [Grant the Allowed to Authenticate permission on computers in the trusting domain or forest](#) (授與信任網域或樹系電腦上的允許驗證權限)。

- 因為無法判定桌面平台集區所使用的 App Volumes Manager 和 JMP Server 所使用的 User Environment Manager 版本相關資訊，JMP 指派並未如預期般正常運作。

**因應措施：**設定桌面平台集區時，在 [佈建設定] 窗格的 [調整桌面平台集區大小] 區段中，將備用 (開啟電源) 機器數目值設為 1 或以上。此外，如果您在 [佈建時機] 區段中選取隨選佈建機器選項，請將機器的最小數目值設為 1 或以上。

- 當 JMP Server 1.0.2.x 版安裝程式檔案在目前已安裝 JMP Server 1.0.0.516 版的主機上執行時，無法繼續安裝程序。

**因應措施：**使用控制台來解除安裝 JMP Server 1.0.0.516 版。執行 JMP Server 1.0.2.x 版的安裝檔案，並遵循精靈以完成安裝。在安裝程序期間提供相同的 SQL Server 資料庫資訊，以保留 JMP Server 1.0.0.516 版安裝中既有的任何資料。

- 在下列情況下，當您嘗試使用 JMP Server 安裝程式 1.1.0.xxx 版升級目前的安裝後，升級會失敗且安裝會回復，而您的 JMP Server 執行個體會變得無法使用。

- 在升級期間，您 JMP Server 安裝中的 SQL Server 資料庫憑證會遺失，且會選取啟用 SSL 核取方塊。



- 透過選擇「Windows 驗證」連線模式完成 JMP Server 升級，但並未建立 JMP Server 主機系統的 SQL Server 登入帳戶。
- 您已透過按一下取消來取消升級作業。

**因應措施：**重新執行 JMP Server 安裝程式 1.1.0.xxx 版，以重新嘗試升級。您必須重新輸入先前用來安裝舊版 JMP Server 的相同 SQL Server 資料庫資訊。成功升級後，請確認已為 JMP Server 設定的所有憑證仍保持原狀。根據安裝失敗或取消作業的發生時間，憑證可能已有所變更。

- 嘗試新增 Dynamic Environment Manager (DEM) 組態共用時，可能會出現下列錯誤：runOne] 執行 file\_share.createFileShare 時發生錯誤 { code: 400,\n took: 221,\n data: {},\n 錯誤：「無法建立檔案共用 <fileshare-unc-path>。」

DEM 組態共用的密碼包含下列任一字元時，新增 DEM 組態共用的作業將會失敗：“#+,;<>=\~

**因應措施：**使用不同密碼，其中包含下列允許的字元之一：!\$%&'()\*-./:~@[]^\_`{|}

## Horizon Cloud Connector

- 使用以 HTML5 為基礎的 vSphere Web Client 來部署 Horizon Cloud Connector 虛擬應用裝置 OVA 檔案時，會發生下列錯誤：「為內容 proxySsl 指定的「false」值無效。無法部署 OVF 套件。」  
**因應措施：**使用 Flex 型或 Flash 型的 vSphere Web Client 來部署 Horizon Cloud Connector 虛擬應用裝置 OVA 檔案。
- 啟動 Horizon Cloud Connector 時，您會看到下列訊息：「[失敗] 無法啟動，請等待網路完成設定。請參閱「systemctl status systemd-networkd-wait-online.service」以取得詳細資料。」  
此訊息未正確顯示，且未指出網路實際發生的問題。您可以忽略此訊息，並如常繼續使用 Horizon Cloud Connector。