在 Horizon 7 中設定遠端桌面平台功能

2019 年 12 月

VMware Horizon 7 7.11

vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

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

目錄

在 Horizon 7 中設定遠端桌面平台功能

1

《在 Horizon 7 中設定遠端桌面平台功能》說明如何設定隨著 Horizon Agent 安裝在虛擬桌面平台或 RDS 主機上的遠端桌面平台功能。您也可以設定原則來控制桌面平台與應用程式集區、機器以及使用者的行為。

主要對象

這項資訊適用於任何想要在虛擬桌面平台或 RDS 主機上設定遠端桌面平台功能或原則的人員。這項資訊是針對熟悉虛擬機器技術及資料中心作業的 Windows 系統管理員所撰寫的。

設定遠端桌面平台功能

2

與 Horizon Agent 一起安裝的某些遠端桌面平台功能可以在 Horizon 7 版本中更新。您可以設定這些功能，以提升使用者的遠端桌面平台體驗。

這些功能包括 HTML Access、Unity Touch、Flash URL 重新導向、HTML5 多媒體重新導向、地理位置重新導向、即時音訊視訊、Windows Media 多媒體重新導向 (MMR)、USB 重新導向、掃描器重新導向、序列埠重新導向、指紋掃描器重新導向、工作階段協作、商務用 Skype，以及 URL 內容重新導向。

如需 HTML Access 的相關資訊，請參閱《VMware Horizon HTML Access 安裝和設定指南》文件。如需 USB 重新導向的相關資訊，請參閱第 4 章 將 USB 裝置與遠端桌面平台和應用程式搭配使用。如需 URL 內容重新導向的相關資訊，請參閱第 3 章 設定 URL 內容重新導向。

本章節討論下列主題：

設定 Unity Touch

使用 Unity Touch 時，您可在平板電腦和智慧型手機輕鬆瀏覽、搜尋並開啟 Windows 應用程式和檔案、選擇最愛的應用程式和檔案，且不需使用 [開始] 功能表或 [工具列]，就可輕鬆在執行的應用程式間切換。您可以設定將在 Unity Touch 側邊列中顯示的最愛應用程式的預設清單。

您可以在 Horizon Agent 安裝後停用或啟用 Unity Touch 功能，只要設定 Horizon Agent 組態 ADMX 範本檔 (vdm_agent.admx) 中的**啟用 Unity Touch** 群組原則設定即可。

iOS、Android 和 Chrome OS 裝置的 VMware Horizon Client 文件會提供關於 Unity Touch 所提供之使用者功能的詳細資訊。請參閱 https://docs.vmware.com/tw/VMware-Horizon-Client/index.html。

Unity Touch 系統需求

Horizon Client 軟體和安裝 Horizon Client 的行動裝置必須符合特定版本需求，才可支援 Unity Touch。

遠端桌面平台

若要支援 Unity Touch，必須在使用者存取的虛擬機器上安裝以下軟體：

- 透過安裝 View Agent 6.0 或更新版本，或 Horizon Agent 7.0 或更新版本來安裝 Unity Touch 功能。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈在虛擬機器上安裝 Horizon Agent〉。
- 作業系統：Windows 7 (32 位元或 64 位元)、Windows 8 (32 位元或 64 位元)、Windows 8.1 (32 位元或 64 位元)、Windows Server 2008 R2 或 Windows Server 2012 R2、Windows 10 (32 位元或 64 位元)

Horizon Client 軟體

以下 Horizon Client 版本支援 Unity Touch：

- iOS 版 Horizon Client
- Android 版 Horizon Client
- Chrome OS 版 Horizon Client

設定 Unity Touch 顯示的最愛應用程式

具備 Unity Touch 功能時，平板電腦和智慧型手機使用者能迅速地從 Unity Touch 側邊列，導覽至遠端桌面平台應用程式或檔案。雖然為了方便起見，使用者可指定要在側邊欄顯示的最愛應用程式，管理員可設定最愛的應用程式預設清單。

如果您使用浮動指派桌面平台集區，除非您在 Active Directory 中啟用漫遊使用者設定檔，否則從桌面平台中斷連線時，將會遺失使用者指定的最愛應用程式和最愛檔案。

使用者先連線到啟用 Unity Touch 時，最愛應用程式的預設清單仍會持續開啟。但是，如果使用者設定他自己的最愛應用程式清單，則系統會忽視預設清單。使用者連線到浮動或專用集區中的不同機器時，使用者最愛應用程式清單仍會在使用者的漫遊設定檔中顯示且仍可使用。

如果建立最愛應用程式的預設清單，且在遠端桌面平台作業系統上沒有安裝一或多個應用程式，或在 [開始] 功能表找不到這些應用程式的路徑時，不會在最愛的清單顯示應用程式。您可使用此行為設定套用至多個虛擬機器映像（使用不同組的安全應用程式）的一個最愛應用程式主預設清單。

例如，如果在第一台虛擬機器上安裝 Microsoft Office 和 Microsoft Visio，在第二台虛擬機器上安裝 Windows Powershell 和 VMware vSphere Client，則您可以建立包含所有四種應用程式的清單。只有已經安裝的應用程式會在各個桌面平台上顯示為預設最愛的應用程式。

您可使用不同的方式，指定最愛應用程式的預設清單：

- 在桌面平台集區中的虛擬機器上新增 Windows 登錄值
- 從 Horizon Agent 安裝程式建立管理安裝套件，並將套件散佈到虛擬機器
- 從虛擬機器上的命令列執行 Horizon Agent 安裝程式

備註 Unity Touch 假設應用程式的捷徑位於**開始**功能表的 Program 資料夾。如果任何捷徑不在 Programs 資料夾，連接前置詞 **Programs** 到捷徑路徑。例如：位在 `ProgramData\Microsoft\Windows\Start Menu` 資料夾的 `Windows Update.lnk`。若要公布此捷徑為預設最愛的應用程式，新增前置詞 **Programs** 到捷徑路徑。例如：`"Programs/Windows Update.lnk"`。

必要條件

- 確認已在虛擬機器上安裝 Horizon Agent。
- 確認您在虛擬機器上具有管理員權限。為了執行此程序，您需要編輯登錄設定。
- 如果您有浮動指派桌面平台集區，請使用 Active Directory 設定漫遊使用者設定檔。請遵循 Microsoft 提供的指示。

  每次登入時，浮動指派桌面平台集區的使用者都可以看見最愛的應用程式和檔案清單。

程序

◆ (選擇性) 新增 Windows 登錄值，建立最愛應用程式的預設清單。

a 開啟 `regedit` 並導覽至 `HKLM\Software\VMware, Inc.\VMware Unity` 登錄設定。

在 64 位元虛擬機器上，導覽到 `HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity` 目錄。

b 建立稱為 `FavAppList` 的字串值。

c 指定預設最愛的應用程式。

使用以下格式，指定在**開始**功能表中使用之應用程式的捷徑路徑。

```
path-to-app-1|path-to-app-2|path-to-app-3|…
```

例如：

```
Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere
Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010
Language Preferences.lnk
```

- (選擇性) 透過從 Horizon Agent 安裝程式建立管理安裝套件，建立最愛應用程式的預設清單。
  a 從命令列，使用以下格式建立管理安裝封裝。

  ```
  VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""用來儲存管理安裝套件的網路共用
  "" UNITY_DEFAULT_APPS=""應設定於登錄中的預設最愛應用程式清單"""
  ```

  例如：

  ```
  VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share
  \ViewFeaturePack\"" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of
  Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows
  PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|Programs/Google
  Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft
  SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/
  WebEx/Productivity Tools/WebEx Settings.lnk|"""
  ```

  b 使用組織採用的標準 Microsoft Windows Installer (MSI) 部署方式，從網路共用區分發管理安裝套件到桌面平台虛擬機器。
- (選擇性) 透過直接從虛擬機器的命令列執行 Horizon Agent 安裝程式，建立最愛應用程式的預設清單。

  使用以下格式。

  ```
  VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS=""應設定於登錄中的預設最愛應用
  程式清單"""
  ```

  備註 前述的命令會結合安裝 Horizon Agent 與指定最愛應用程式預設清單的作業。執行此命令前，您不需安裝 Horizon Agent。

後續步驟

如果在虛擬機器上直接執行此工作 (編輯 Windows 登錄或從命令列安裝 Horizon Agent)，您必須部署新設定的虛擬機器。您可以建立快照或範本、建立桌面平台集區或重新撰寫現有集區。或您可建立 Active Directory 群組原則，部署新的設定。

設定多點傳送或單點傳送串流的 Flash URL 重新導向

客戶現在可使用 Adobe Media Server 和多點傳送或單點傳送，在虛擬桌面平台基礎架構 (VDI) 環境中傳送即時視訊事件。若要在 VDI 環境內提供多點傳送或單點傳送即時視訊串流，應略過遠端桌面平台，直接從媒體來源將媒體串流傳送至端點。Flash URL 重新導向功能透過從遠端桌面平台攔截和重新導向 ShockWave Flash (SWF) 檔案至用戶端端點，支援此功能。

接著會使用用戶端本機 Flash 媒體播放器，顯示 Flash 內容。

直接從 Adobe Media Server 串流 Flash 內容到用戶端端點，可降低資料中心 ESXi 主機的負載，免除透過資料中心額外的路由作業並減少同時串流 Flash 內容到多個用戶端端點所需的頻寬。

Flash URL 重新導向功能會使用由網頁管理員嵌入到 HTML 網頁的 JavaScript。不論遠端桌面平台使用者何時從網頁中按一下指定的 URL 連結，JavaScript 都會進行攔截並從遠端桌面工作階段重新導向 SWF 檔案到用戶端端點。然後端點會開啟遠端桌面工作階段外的本機 Flash 放映檔，並在本機播放媒體串流。

若要設定 Flash URL 重新導向，您必須設定 HTML 網頁以及用戶端裝置。

程序

1 Flash URL 重新導向系統需求

若要支援 Flash URL 重新導向，您的 Horizon 7 部署必須符合特定軟體和硬體需求。

2 確認已安裝 Flash URL 重新導向功能

使用此功能前，確認 Flash URL 重新導向功能已安裝，且正在虛擬桌面平台上執行。

3 設定 Flash URL 重新導向的網頁

要允許使用 Flash URL 重新導向，您必須在提供多點傳送或單點傳送串流連結的 MIME HTML (MHTML) 網頁，嵌入 JavaScript 指令。使用者在其遠端桌面平台上的瀏覽器中顯示這些網頁，來存取視訊串流。

4 設定 Flash URL 重新導向的用戶端裝置

Flash URL 重新導向功能會從遠端桌面平台重新導向 SWF 檔案到用戶端裝置。若要允許用戶端裝置從多點傳送或單點傳送串流播放 Flash 視訊，您必須確認在用戶端裝置已安裝適當的 Adobe Flash Player。用戶端同時也必須具備媒體來源的 IP 連線。

5 停用或啟用 Flash URL 重新導向

當您以 `VDM_FLASH_URL_REDIRECTION=1` 內容來執行 Horizon Agent 的無訊息安裝時，將會啟用 Flash URL 重新導向。您可以透過對那些虛擬機器上的 Windows 登錄機碼設定值，在選取的遠端桌面平台上停用或重新啟用 Flash URL 重新導向功能。

Flash URL 重新導向系統需求

若要支援 Flash URL 重新導向，您的 Horizon 7 部署必須符合特定軟體和硬體需求。

遠端桌面平台	■ 在 View Agent 6.0 或更新版本，或 Horizon Agent 7.0 或更新版本的無訊息安裝期間，您可以在命令列上輸入 `VDM_FLASH_URL_REDIRECTION` 內容，以安裝 Flash URL 重新導向。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈Horizon Agent 的無訊息安裝屬性〉。 ■ 桌面平台必須執行 Windows 7 64 位元或 32 位元作業系統。 ■ 支援的桌面平台瀏覽器包含 Internet Explorer 8、9 和 10、Chrome 29.*x* 以及 Firefox 20.*x*。
Flash 媒體播放器和 ShockWave Flash (SWF)	您必須整合如 Strobe 媒體播放等適當的 Flash 媒體播放器到網站。要串流多點傳送內容，您可在網頁使用 `multicastplayer.swf` 或 `StrobeMediaPlayback.swf`。要串流即時單點傳送內容，您必須使用 `StrobeMediaPlayback.swf`。您也可針對其他支援的功能（如 RTMP 串流和 HTTP 動態串流），使用 `StrobeMediaPlayback.swf`。
Horizon Client 軟體	以下 Horizon Client 版本支援多點傳送和單點傳送： ■ Linux 版 Horizon Client 2.2 或更新版本

	■ Windows 版 Horizon Client 2.2 或更新版本 以下 Horizon Client 版本僅支援多點傳送（不支援單點傳送）： ■ Horizon Client 2.0 或 2.1 for Linux ■ Horizon Client 5.4 for Windows
Horizon Client 電腦或用戶端存取裝置	■ 在 x86 精簡型用戶端裝置執行 Linux 版 Horizon Client 的所有作業系統均支援 Flash URL 重新導向。在 ARM 處理器上不支援此功能。 ■ 執行 Windows 版 Horizon Client 的所有作業系統均支援 Flash URL 重新導向。如需詳細資訊，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。 ■ 在 Windows 用戶端裝置上，您必須安裝 Internet Explorer 的 Adobe Flash Player 10.1 或更新版本。 ■ 在 Linux 精簡型用戶端裝置，您必須安裝 `libexpat.so.0` 和 `libflashplayer.so` 檔案。請參閱設定 Flash URL 重新導向的用戶端裝置。 **備註** 使用 Flash URL 重新導向時，多點傳送或單點傳送串流會重新導向到組織防火牆外的用戶端裝置。您的用戶端必須可存取託管 ShockWave Flash (SWF)（可啟動多點傳送或單點傳送串流）檔案的 Adobe 網路伺服器。如果需要，設定您的防火牆，開啟適當的連接埠，允許用戶端裝置存取此伺服器。

確認已安裝 Flash URL 重新導向功能

使用此功能前，確認 Flash URL 重新導向功能已安裝，且正在虛擬桌面平台上執行。

必須在每台要支援多點傳送或單點傳送重新導向的桌面平台上都安裝 Flash URL 重新導向功能。如需 Horizon Agent 安裝指示，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈Horizon Agent 的無訊息安裝屬性〉。

程序

1 啟動使用 PCoIP 的遠端桌面工作階段。

2 開啟工作管理員。

3 確認在桌面平台上正在執行 `ViewMPServer.exe` 程序。

設定 Flash URL 重新導向的網頁

要允許使用 Flash URL 重新導向，您必須在提供多點傳送或單點傳送串流連結的 MIME HTML (MHTML) 網頁，嵌入 JavaScript 指令。使用者在其遠端桌面平台上的瀏覽器中顯示這些網頁，來存取視訊串流。

此外，您可自訂 Flash URL 重新導向發生問題時，向使用者顯示的英文錯誤訊息。如果您想要向使用者顯示本地語系的錯誤訊息，則執行選用步驟。您必須在 MHTML 網頁嵌入 `var vmwareScriptErroMessage` 組態以及本地語系的文字字串。

必要條件

驗證 `swfobject.js` 程式庫是否匯入 MHTML 網頁。

程序

1 在 MHTML 網頁 `viewmp.js` JavaScript 指令。

例如：`<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`

2 (選擇性) 自訂傳送給使用者的 Flash URL 重新導向錯誤訊息。

例如：「`var vmwareScriptErroMessage=`*當地語系化的錯誤訊息*」

3 確定在 ShockWave Flash (SWF) 檔案匯入至 MHTML 網頁前，嵌入 `viewmp.js` JavaScript 命令，並選擇是否自訂 Flash URL 重新導向錯誤訊息。

當使用者在遠端桌面平台中顯示網頁時，`viewmp.js` JavaScript 命令會叫用遠端桌面平台上的 Flash URL 重新導向機制，將 SWF 檔案從桌面平台重新導向到主控用戶端裝置。

設定 Flash URL 重新導向的用戶端裝置

Flash URL 重新導向功能會從遠端桌面平台重新導向 SWF 檔案到用戶端裝置。若要允許用戶端裝置從多點傳送或單點傳送串流播放 Flash 視訊，您必須確認在用戶端裝置已安裝適當的 Adobe Flash Player。用戶端同時也必須具備媒體來源的 IP 連線。

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

程序

- 在用戶端裝置上安裝 Adobe Flash Player。

作業系統	動作
Windows	安裝 Internet Explorer 的 Adobe Flash Player 10.1 或更新版本。
Linux	a 安裝 `libexpat.so.0` 檔案，或確認已安裝此檔案。 確認檔案安裝位置為 `/usr/lib` 或 `/usr/local/lib` 目錄。 b 安裝 `libflashplayer.so` 檔案，或確認已安裝此檔案。 確認在 Linux 作業系統的適當 Flash 外掛程式目錄中已安裝檔案。 c 安裝 `wget` 程式，或確認已安裝程式檔案。

停用或啟用 Flash URL 重新導向

當您以 VDM_FLASH_URL_REDIRECTION=1 內容來執行 Horizon Agent 的無訊息安裝時，將會啟用 Flash URL 重新導向。您可以透過對那些虛擬機器上的 Windows 登錄機碼設定值，在選取的遠端桌面平台上停用或重新啟用 Flash URL 重新導向功能。

程序

1 在虛擬機器上啟動 Windows 登錄編輯程式。

2 導覽至控制 Flash URL 重新導向的 Windows 登錄機碼。

選項	描述
Windows 7 64 位元	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware ViewMP\enabled = value`
Windows 7 32 位元	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware ViewMP\enabled = value`

3 設定值以停用或啟用 Flash URL 重新導向。

選項	值
已停用	`0`
已啟用	`1`

依預設，此值設定為 1。

設定 Flash 重新導向

透過 Flash 重新導向，如果使用者使用 Internet Explorer 9、10 或 11，會將 Flash 內容傳送至用戶端系統，進而降低 ESXi 主機上的負載。用戶端系統會使用 Flash Player ActiveX 版本，在 Flash 容器視窗中播放媒體內容。

雖然此功能的名稱類似稱為 Flash URL 重新導向的功能，但如下表所述，兩者有很大的不同。

表 2-1. Flash 重新導向功能和 Flash URL 重新導向的比較

差異項目	Flash 重新導向	Flash URL 重新導向
支援此功能的 Horizon Client 類型	僅限 Windows 用戶端	Windows 用戶端和 Linux 用戶端
顯示通訊協定	PCoIP 和 VMware Blast。	PCoIP
瀏覽器	適用於遠端桌面平台的 Internet Explorer 9、10 或 11	Horizon Client 和 Horizon Agent 目前支援的所有瀏覽器
組態機制	使用 Horizon Agent 群組原則設定，指定可使用或無法使用 Flash 重新導向的網站白名單或黑名單	若要嵌入必要的 JavaScript，請修改網頁上的原始程式碼。

功能限制

Flash 重新導向功能有以下限制：

- 按一下 Flash Player 視窗內的 URL 連結，將會在用戶端開啟瀏覽器，而不會在遠端桌面平台 (代理程式端) 開啟。
- 有些網站在部分瀏覽器版本上無法使用 Flash 重新導向。例如，如果您使用 Internet Explorer 11，則 vimeo.com 不會運作。
- Flash 和 Java 指令碼可能不會如預期般運作。
- Horizon Client 視窗在播放 Flash 內容時可能會凍結，但是您可以設定 Windows 登錄機碼來解決此問題。

  在 32 位元用戶端上，請將 `HKLM\Software\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` 值設為「FALSE」，在 64 位元用戶端上，請將 `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` 設為「FALSE」。
- YouTube 不再支援 Flash 媒體。
- 對於 redbox.com，Flash 重新導向會無法運作。
- Flash 快顯功能表 (藉由點按滑鼠右鍵啟動) 會停用。
- 如果 Horizon Client 4.1 連線至使用 PCoIP 的遠端桌面平台，Flash 重新導向將會失敗。Horizon Client 會以遠端桌面平台的原生播放程式播放 Flash 內容，或是使用者會看到白色畫面。

Flash 重新導向的系統需求

Horizon Agent 和 Horizon Client 以及安裝代理程式與用戶端軟體的遠端桌面平台和用戶端系統都必須符合特定需求，才能支援 Flash 重新導向功能。

遠端桌面平台	■ 必須在選取 [Flash 重新導向] 自訂安裝選項的情況下，在虛擬桌面平台中安裝 Horizon Agent 7.0 或更新版本。依預設不會選取 [Flash 重新導向] 自訂安裝選項。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中關於安裝 Horizon Agent 的主題。 ■ 必須設定適當的群組原則設定。請參閱安裝和設定 Flash 重新導向。 ■ Windows 7、Windows 8、Windows 8.1 和 Windows 10 虛擬桌面平台可支援 Flash 重新導向。 ■ 必須安裝 Internet Explorer 9、10 或 11 並搭配相對應的 Flash ActiveX 外掛程式。 ■ 安裝之後，必須在 Internet Explorer 中啟用 VMware View FlashMMR Server 附加元件。
Horizon Client 電腦或用戶端存取裝置	■ 必須安裝 Horizon Client 4.0 或更新版本。依預設會啟用 [Flash 重新導向] 選項。請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件中關於安裝 Horizon Client 的主題。

- Windows 7、Windows 8、Windows 8.1 和 Windows 10 可支援 Flash 重新導向。
- 必須已安裝並啟用 Flash ActiveX 外掛程式

適用於遠端工作階段的顯示通訊協定

- PCoIP
- VMware Blast (需要 Horizon Agent 7.0 或更新版本)

安裝和設定 Flash 重新導向

若要將遠端桌面平台的 Flash 內容重新導向至本機用戶端系統上的 Flash Player 視窗，必須在遠端桌面平台與用戶端系統上安裝 Flash 重新導向功能以及 Internet Explorer，並指定使用此功能的網站。

若要啟用此功能並指定使用此功能的網站，您可以設定群組原則設定。或者，您可以使用遠端桌面平台上的 Windows 登錄設定，來設定用於 Flash 重新導向的網站白名單。請參閱使用 Windows 登錄設定來設定 Flash 重新導向。

必要條件

- 在用戶端系統上安裝 Horizon Client，並在已啟用 Flash 重新導向功能的遠端桌面平台上安裝 Horizon Agent。如需必要的版本、安裝選項和完整系統需求，請參閱 Flash 重新導向的系統需求。
- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。
- 將 Horizon Agent 組態 ADMX 範本檔 `vdm_agent.admx` 新增至遠端桌面平台的 OU。如需安裝指示，請參閱將 ADMX 範本檔新增至 Active Directory。
- 編譯可以 (白名單) 或不可 (黑名單) 重新導向 Flash 內容的網站清單。
- 確認 Flash ActiveX 已安裝並正常運作。若要確認安裝，請執行 Internet Explorer，並移至 https://helpx.adobe.com/flash-player.html。

程序

1. 如有必要，請在用戶端系統上安裝 ActiveX 版的 Flash Player (而非 NPAPI 版本)。

   Internet Explorer 10 和 11 中依預設已安裝 Flash Player。若是 Internet Explorer 9，您可能需要在 https://get.adobe.com/flashplayer/ 下載並安裝 Flash Player。

2. 在遠端桌面平台上，執行下列安裝步驟。

   a 安裝 Internet Explorer 9、10 或 11。

   b 如有必要，請安裝 ActiveX 版的 Flash Player (而非 NPAPI 版本)。

   Internet Explorer 10 和 11 中依預設已安裝 Flash Player。若是 Internet Explorer 9，您可能需要在 https://get.adobe.com/flashplayer/ 下載並安裝 Flash Player。

3. 在遠端桌面平台上，於 Internet Explorer 的功能表列中選取**工具 > 管理附加元件**，並確認其中有列出 **VMware View FlashMMR Server** 並已啟用。

4 在 Active Directory 伺服器上開啟群組原則管理編輯器，並在**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware FlashMMR** 資料夾中設定 Flash 重新導向原則設定。

設定	說明
啟用 Flash 多媒體重新導向	指定是否在遠端桌面平台 (代理程式端) 上啟用 Flash 重新導向 (FlashMMR)。若啟用，此功能會將所指定 URL 中的 Flash 多媒體資料透過 TCP 通道轉送給用戶端，並叫用用戶端系統上的本機 Flash Player。此功能可大幅降低對代理程式端 CPU 與網路頻寬的需求。
啟用 FlashMMR 的矩形大小下限	指定用來播放 Flash 內容之矩形的最小寬度和高度 (以像素為單位)。例如，**400,300** 指定寬度 400 像素與高度 300 像素。只有在 Flash 內容等於或大於此原則中指定的值時，才會使用 Flash 重新導向。如果未設定此 GPO，則使用的預設值為 **320,200**。

5 在 Active Directory 伺服器上開啟群組原則管理編輯器，並在**使用者設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware FlashMMR** 資料夾中設定 Flash 重新導向原則設定。

a 若要定義用於 Flash 重新導向的主機 URL 清單，請開啟 **FlashMMR URL 清單使用定義**設定，然後選取**已啟用**。

b 在 **FlashMMR URL 清單使用定義**下拉式功能表中，選取**啟用白名單**或**啟用黑名單**，然後按一下**確定**。

依預設會啟用白名單。

c 若要新增使用或不使用 Flash 重新導向的主機 URL 清單，請開啟**啟用 FlashMMR 的主機 URL 清單**設定，然後選取**已啟用**。

d 按一下**顯示**，然後在 [值名稱] 欄中輸入您為白名單或黑名單編譯的完整 URL。

請在 URL 中加入 `http://` 或 `https://` 前置詞。您可以使用規則運算式。例如，您可以指定 `https://*.google.com` 和 `http://www.cnn.com/*`。

在 [值] 欄中，您可以選擇性地指定 `requireIECompatibility=true` 和 (或) `appMode=0`。請使用逗號分隔兩個字串。

依預設，在 Flash 重新導向執行時會啟用外部介面支援，因而可能降低效能。在特定情況下，設定 `appMode=0` 將可改善效能，並帶來較佳的使用者體驗。

e 按一下**確定**以儲存 URL 清單，然後再次按一下**確定**以儲存原則設定。

6 若要將白名單或黑名單新增至 Internet Explorer，請開啟命令提示字元，並執行 `cscript "%ProgramFiles%\Common Files\VMware\Remote Experience\mergeflashmmrwhitelist.vbs"` 命令。

7 重新啟動 Internet Explorer。

使用 `requireIECompatibility=true` 參數設定的網站，會新增至 Internet Explorer 的相容性檢視。若要確認相容性檢視中的網站，請從功能表列中選取**工具 > 相容性檢視設定**。

這些網站也會新增至 Internet Explorer 的信任網站清單中。若要確認信任的網站，請從 Internet Explorer 功能表列中選取**工具 > 網際網路選項**，然後按一下**安全性**索引標籤上的**網站**。

使用 Windows 登錄設定來設定 Flash 重新導向

如果您在 Active Directory 伺服器上是不具管理員權限的網域使用者，則也可以透過在遠端桌面平台的 Windows 登錄機碼中設定適當值來設定 Flash 重新導向。

您可以將此程序作為使用群組原則設定來設定 Flash 重新導向的替代方法。

必要條件

- 若要確保只有清單中指定的 URL 可以重新導向 Flash 內容，請編譯網站的白名單。您無法使用 Windows 登錄設定來啟用黑名單。若要啟用黑名單，請使用 Flash 重新導向的群組原則設定。
- 確認已在遠端桌面平台上安裝 Horizon Agent 7.0 或更新版本、Flash Player 和 Internet Explorer 9、10 或 11。請參閱 Flash 重新導向的系統需求。
- 確認已在用戶端系統中安裝 Horizon Client 4.0 或更新版本和 Flash Player ActiveX 版本。

程序

1 使用 Horizon Client 存取遠端桌面平台。

2 在遠端桌面平台上開啟 Windows 登錄編輯程式 (`regedit.exe`)、導覽至 `HKLM\Software\VMware, Inc.\VMware FlashMMR` 資料夾，然後將 **FlashRedirection** 設為 **1**。

> **備註** 此設定會啟用 Flash 重新導向功能。如果在 `HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR` 中停用此設定 (設為 0)，則會在整個網域停用 Flash 重新導向，且只有網域管理員可加以啟用。

3 導覽至 `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR` 資料夾。

如果此資料夾不存在，請加以建立。

4 在 `VMware FlashMMR` 資料夾中，建立名為 **UrlWhiteList** 的子機碼。

5 以滑鼠右鍵按一下 **UrlWhiteList** 機碼、選取**新增 > 字串值**，然後輸入使用 Flash 重新導向之網站的 URL 作為名稱。

您可以使用規則運算式。例如，您可以指定 **`https://*.google.com`**。讓**資料**值保持空白。

6 (選擇性) 在新登錄值的資料欄位中，新增資料 **`requireIECompatibility=true`** 和 (或) **`appMode=0`**。

請使用逗號分隔兩個字串。依預設，在 Flash 重新導向執行時會啟用外部介面支援，因而可能降低效能。在特定情況下，設定 **`appMode=0`** 可改善效能，而設定 **`appMode=1`** 則可帶來較佳的使用者體驗。

7 若要新增其他 URL，請重複前述步驟，然後關閉登錄編輯程式。

8 在遠端桌面平台上開啟命令提示字元，並導覽至 `%Program Files%\Common Files\VMware\Remote Experience` 目錄。

9 若要將白名單新增至 Internet Explorer，請執行 `cscript mergeflashmmrwhitelist.vbs` 命令。

10 重新啟動 Internet Explorer。

使用參數 **`requireIECompatibility=true`** 設定的網站，會新增至 Internet Explorer 的相容性檢視。若要確認相容性檢視中的網站，請從功能表列中選取**工具 > 相容性檢視設定**。

這些網站也會新增至 Internet Explorer 的信任網站清單中。若要確認信任的網站，請從 Internet Explorer 功能表列中選取**工具 > 網際網路選項**，然後按一下**安全性**索引標籤上的**網站**。

設定 HTML5 多媒體重新導向

使用 HTML5 多媒體重新導向時，如果使用者在遠端桌面平台中使用 Google Chrome 或 Microsoft Edge 瀏覽器，HTML5 多媒體內容將會傳送至用戶端系統，而降低 ESXi 主機上的負載。用戶端系統會播放多媒體內容，而使用者會有更理想的音訊和視訊體驗。

HTML5 多媒體重新導向的系統需求

Horizon Agent 和 Horizon Client 以及安裝代理程式與用戶端軟體的遠端桌面平台和用戶端系統都必須符合特定需求，才能支援 HTML5 多媒體重新導向功能。

遠端桌面平台

- 虛擬桌面平台必須選取 HTML5 多媒體重新導向自訂安裝選項，並安裝 Horizon Agent7.3.2 或更新版本 (適用於 Chrome) 或 Horizon Agent 7.5 或更新版本 (適用於 Edge)。此選項依預設為未選取狀態。從 Horizon Agent7.10 開始，HTML5 多媒體重新導向自訂安裝選項已移除，且依預設會安裝 HTML5 多媒體重新導向。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中關於安裝 Horizon Agent 的主題。
- 已發佈桌面平台的 RDS 主機必須在選取 HTML5 多媒體重新導向自訂安裝選項的情況下，安裝 Horizon Agent7.3.2 或更新版本。此選項依預設為未選取狀態。從 Horizon Agent7.10 開始，HTML5 多媒體重新導向自訂安裝選項已移除，且依預設會安裝 HTML5 多媒體重新導向。請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件中關於安裝 Horizon Agent 的主題。
- 必須在 Active Directory 伺服器上設定 HTML5 多媒體重新導向群組原則設定。請參閱安裝和設定 HTML5 多媒體重新導向。
- 必須安裝 Chrome 或 Edge 瀏覽器。
- 必須在 Chrome 或 Edge 瀏覽器中安裝 VMware Horizon HTML5 多媒體重新導向延伸。請參閱安裝適用於 Chrome 的 VMware Horizon HTML5 重新導向延伸或安裝適用於 Edge 的 VMware Horizon HTML5 重新導向延伸。

用戶端系統

- 針對 Windows 用戶端系統，必須安裝 Horizon Client4.6 或更新版本 (適用於 Chrome) 或 Horizon Client 4.8 或更新版本 (適用於 Edge)，且須選取「支援 HTML5 多媒體重新導向和瀏覽器重新導向」自訂安裝選項。預設為選取此選項。請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件中關於安裝 Horizon Client 的主題。

- 針對 Linux 用戶端系統，必須在選取 HTML5 多媒體重新導向支援自訂安裝選項的情況下，安裝 Horizon Client5.1 或更新版本。預設為選取此選項。請參閱《Linux 版 VMware Horizon Client 安裝和設定指南》中關於安裝 Horizon Client 的主題。

適用於遠端工作階段的顯示通訊協定

- PCoIP
- VMware Blast

限制

HTML5 多媒體重新導向功能有下列限制。

- 不支援 Horizon Client 相對滑鼠功能。
- 您無法使用**靜音網站** (Chrome 瀏覽器) 或**靜音索引標籤** (Edge 瀏覽器) 將重新導向的視訊內容靜音。
- 若要從 Linux 用戶端系統上的 Chrome 使用 HTML5 多媒體重新導向，請開啟 RDS 主機所發佈的單一 Chrome 瀏覽器。如果您額外開啟其他 RDS 主機所發佈的 Chrome 瀏覽器，HTML5 多媒體重新導向將無法正常運作。
- 如果您在使用低容量精簡型用戶端硬體的 Linux 用戶端系統上播放重新導向的多媒體內容時遇到效能偏低的狀況，您可以依照此處的說明將系統效能最佳化。請將 `disableGPU.html5mmr=true` 項目新增至下列三個組態檔之一。這些組態檔將依照下列順序進行處理：

  a `/usr/lib/vmware/config`

  b `/etc/vmware/config`

  c `~/.vmware/config`

安裝和設定 HTML5 多媒體重新導向

若要將遠端桌面平台的 HTML5 多媒體內容重新導向至本機用戶端系統，必須在遠端桌面平台上安裝 HTML5 多媒體重新導向功能以及 Chrome 或 Edge 瀏覽器、啟用 HTML5 多媒體重新導向功能，並指定要使用此功能的網站。

若要啟用 HTML5 多媒體重新導向並指定要使用此功能的網站，您可以在 Active Directory 伺服器上設定群組原則設定。您必須編譯可重新導向 HTML5 多媒體內容之網站的 URL 清單。請在 URL 中加入 `http://` 或 `https://` 前置詞。您可以在 URL 中使用比對模式。

例如，若要重新導向 YouTube 上的所有視訊，請指定 `https://www.youtube.com/*`。若要重新導向 Vimeo 上的所有視訊，請指定 `https://www.vimeo.com/*`。如需詳細資訊，請參閱 https://developer.chrome.com/extensions/match_patterns。

必要條件

- 在用戶端系統上安裝 Horizon Client，並在已啟用 HTML5 多媒體重新導向功能的遠端桌面平台上安裝 Horizon Agent。如需必要的版本、安裝選項和完整系統需求，請參閱 HTML5 多媒體重新導向的系統需求。

- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。
- 將 VMware View Agent 組態 ADMX 範本檔 `vdm_agent.admx` 新增至與虛擬桌面平台的 OU 連結的 GPO，或新增至與已發佈桌面平台的 RDS 主機連結的 GPO。如需安裝指示，請參閱將 ADMX 範本檔新增至 Active Directory。
- 編譯可重新導向 HTML5 多媒體內容之網站的 URL 清單。

程序

1 在遠端桌面平台上安裝 Chrome 或 Edge 瀏覽器。

2 在您的 Active Directory 伺服器上，開啟群組原則管理編輯器。

3 導覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能**資料夾。

4 開啟**啟用 VMware HTML5 功能**設定，選取**已啟用**，然後按一下**確定**。

5 導覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能 > VMware HTML5 多媒體重新導向**資料夾。

6 開啟**啟用 VMware HTML5 多媒體重新導向**設定、選取**已啟用**，然後按一下**確定**。

7 若要使用 Chrome 瀏覽器，請執行這些步驟。

   a 瀏覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能 > VMware HTML5 多媒體重新導向**資料夾。

   b 開啟**針對 VMware HTML5 多媒體重新導向啟用 Chrome 瀏覽器**、選取**已啟用**，然後按一下**確定**。

8 若要使用 Edge 瀏覽器，請執行這些步驟。

   a 導覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能 > VMware HTML5 多媒體重新導向**資料夾。

   b 開啟**針對 VMware HTML5 多媒體重新導向啟用 Edge 瀏覽器**設定、選取**已啟用**，然後按一下**確定**。

   c 瀏覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能**資料夾。

   d 開啟**停用自動偵測內部網路**設定、選取**已啟用**，然後按一下**確定**。

9 指定哪些網站將使用 HTML5 多媒體重新導向功能。

   a 導覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能 > VMware HTML5 多媒體重新導向**資料夾。

   b 開啟**啟用 VMware HTML5 多媒體重新導向的 URL 清單**設定，然後選取**已啟用**。

c 按一下**顯示**，然後輸入您在 [值名稱] 欄中編譯的 URL。

只有您指定的 URL 才可重新導向 HTML5 多媒體內容。依預設不會新增任何 URL。讓 [值] 欄保持空白。

d 按一下**確定**以儲存 URL 清單，然後按一下**確定**以儲存原則設定。

後續步驟

若要使用 Chrome 瀏覽器，請在遠端桌面平台上的 Chrome 瀏覽器中安裝適用於 Chrome 的 VMware Horizon HTML5 重新導向延伸。請參閱安裝適用於 Chrome 的 VMware Horizon HTML5 重新導向延伸。

若要使用 Edge 瀏覽器，請在遠端桌面平台上的 Edge 瀏覽器中安裝適用於 Edge 的 VMware Horizon HTML5 重新導向延伸。請參閱安裝適用於 Edge 的 VMware Horizon HTML5 重新導向延伸。

安裝適用於 Chrome 的 VMware Horizon HTML5 重新導向延伸

若要使用「HTML5 多媒體重新導向」功能搭配 Chrome 瀏覽器，您必須在遠端桌面平台上強制安裝「VMware Horizon HTML5 重新導向延伸」。您可以藉由在 Active Directory 伺服器上設定 Google Chrome 群組原則設定，來強制安裝此延伸。

若要將 Chrome 群組原則設定套用至遠端桌面平台，您必須將 ADMX 範本檔新增至 Active Directory 伺服器上的 GPO。對於虛擬桌面平台，GPO 必須連結至包含虛擬桌面平台的 OU。對於已發佈的桌面平台，GPO 必須連結至包含 RDS 主機的 OU。

必要條件

- 設定 HTML5 多媒體重新導向功能。請參閱安裝和設定 HTML5 多媒體重新導向。
- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。

程序

1 從 https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip 下載 Google Chrome `policy_templates.zip` 檔案。

2 解壓縮 `policy_templates.zip` 檔案，並將 `chrome.admx` 和 `chrome.adml` 檔案複製到 Active Directory 伺服器上。

`chrome.admx` 檔案位於 `policy_templates.zip` 檔案的 `\windows\admx` 資料夾中，`chrome.adml` 檔案則位於 `\windows\admx\`*`language`* 資料夾中。

a 將 `chrome.admx` 檔案複製到 Active Directory 伺服器上的 `%systemroot%\PolicyDefinitions` 資料夾。

b 將 `chrome.adml` 語言資源檔案複製到 Active Directory 伺服器的 `%systemroot%\PolicyDefinitions` 下適當的語言子資料夾中。

例如，將 `en_us` 版的 `chrome.adml` 檔案複製到 Active Directory 伺服器上的 `%systemroot%\PolicyDefinitions\en_us` 子資料夾。

3 在您的 Active Directory 伺服器上開啟群組原則管理編輯器，並導覽至**電腦設定 > 原則 > 系統管理範本 > Google Chrome > 延伸**資料夾。

4 開啟**設定強制安裝的應用程式和延伸清單**原則設定，然後按一下**已啟用**。

5 按一下**顯示**，然後在 [值] 欄中輸入 **`ljmaegmnepbgjekghdfkgegbckolmcok;https://clients2.google.com/service/update2/crx`**。

6 按一下**確定**以儲存延伸識別碼/更新 URL，然後按一下**確定**以儲存原則設定。

7 確認 HTML5 多媒體重新導向延伸已安裝在遠端桌面平台上。

   a 連線至遠端桌面平台，然後啟動 Chrome。

   b 在 Chrome 位址列中輸入 **`chrome://extensions`**。

   VMware Horizon HTML5 重新導向延伸會出現在 [延伸] 清單中。

安裝適用於 Edge 的 VMware Horizon HTML5 重新導向延伸

若要使用「HTML5 多媒體重新導向」功能搭配 Edge 瀏覽器，您必須在遠端桌面平台上透過 Microsoft Store 安裝「適用於 Edge 擴充功能的 VMware Horizon HTML5 重新導向延伸」。

必要條件

設定 HTML5 多媒體重新導向功能。請參閱安裝和設定 HTML5 多媒體重新導向。

程序

1 連線至遠端桌面平台。

2 透過 Microsoft Store 下載並安裝**適用於 Edge 的 VMware Horizon HTML5 重新導向延伸**。

安裝延伸之後，Edge 瀏覽器視窗右上角即會出現 **VMware HTML5 多媒體重新導向**圖示。當 HTML5 多媒體重新導向功能運作中時，圖示上會顯示字母 REDR。

HTML5 多媒體重新導向限制

HTML5 多媒體重新導向功能有某些限制。

- HTML5 多媒體重新導向不支援 360 視訊。即使視訊不受支援，HTML5 多媒體重新導向延伸圖示仍標有 REDR 徽章。
- HTML5 多媒體重新導向功能無法從 `http://huffingtonpost.com` 重新導向 HTML 多媒體內容。HTML5 多媒體重新導向功能可以從 `http://www.yahoo.com` 重新導向 HTML5 多媒體內容，但您可能會看見「頁面沒有回應」訊息。
- 如果您在**啟用 VMware HTML5 多媒體重新導向的 URL 清單**群組原則設定的網站清單中包含 Microsoft Edge 受信任網站的 URL，HTML5 多媒體重新導向將無法用於該 URL。您可以降低主機的安全性以避免受到此限制，只要執行下列命令即可：**`CheckNetIsolation LoopbackExempt –a –n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"`**。

- 使用 Microsoft Edge 瀏覽器時，HTML5 多媒體重新導向功能無法重新導向使用 m3u8 視訊格式的網站 (例如 `ted.com`) 所傳送的 HTML 多媒體內容。
- 如果遠端桌面平台的 Horizon Agent 中啟用了**掃描器重新導向**安裝選項，在遠端桌面平台中啟動 Microsoft Edge 瀏覽器之後，適用於 Edge 的 VMware Horizon HTML5 重新導向延伸有時會當機。此問題通常發生在大型監視環境的壓力下。
- 如果使用者在遠端桌面平台中播放使用靜態視訊 URL 的 HTML5 視訊，其用戶端機器將無法存取該靜態 URL，且播放會回復到遠端桌面平台。

設定瀏覽器重導向

使用瀏覽器重新導向時，如果使用者在遠端桌面平台中使用 Google Chrome 瀏覽器，網站將會呈現在用戶端系統上，而非代理程式系統上，且會透過遠端瀏覽器的檢視區來顯示。檢視區是瀏覽器視窗中顯示網頁內容的部分。

瀏覽器重新導向的系統需求

安裝代理程式與用戶端軟體的遠端桌面平台和用戶端系統都必須符合特定需求，才能支援瀏覽器重新導向功能。

遠端桌面平台	■ 虛擬桌面平台必須已安裝 Horizon Agent7.10 或更新版本。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中關於安裝 Horizon Agent 的主題。 ■ 已發佈桌面平台的 RDS 主機必須已安裝 Horizon Agent7.10 或更新版本。請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件中關於安裝 Horizon Agent 的主題。 ■ 必須在 Active Directory 伺服器上設定 VMware Browser 重新導向群組原則設定。請參閱安裝和設定瀏覽器重新導向。 ■ 必須安裝 Chrome 瀏覽器。 ■ 必須在 Chrome 瀏覽器中安裝 VMware Horizon 瀏覽器重新導向延伸。請參閱安裝適用於 Chrome 的 VMware Horizon 瀏覽器重新導向延伸。
用戶端系統	必須安裝 Windows 版 Horizon Client5.2 或更新版本，且須選取「支援 HTML5 多媒體重新導向和瀏覽器重新導向」自訂安裝選項。預設為選取此選項。請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件中關於安裝 Horizon Client 的主題。僅支援 Windows 用戶端系統。
適用於遠端工作階段的顯示通訊協定	■ PCoIP ■ VMware Blast

安裝和設定瀏覽器重新導向

要安裝和設定瀏覽器重新導向功能，則必須安裝 Chrome 瀏覽器、在代理程式機器上啟用瀏覽器重新導向功能，以及指定要進行重新導向的 URL。

您可以選擇性地指定使用者可從重新導向的 URL 導覽至的 URL，並自訂在出現白名單違規時的後援行為。您還可以針對麥克風和相機使用、憑證錯誤處理和瀏覽器快取儲存，設定用戶端群組原則設定。

若要啟用瀏覽器重新導向並指定用於重新導向的 URL，您必須在 Active Directory 伺服器上設定代理程式端群組原則設定。編譯可重新導向的網站 URL 清單，以及使用者可選擇性地從重新導向的 URL 導覽至的網站 URL 清單。請在 URL 中加入 **`http://`** 或 **`https://`** 前置詞。您可以在 URL 中使用比對模式。例如，若要重新導向所有的 Yahoo 內容，請輸入 **`https://www.yahoo.com/*`**。如需詳細資訊，請參閱 https://developer.chrome.com/extensions/match_patterns。

必要條件

- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。
- 將 VMware View Agent 組態 ADMX 範本檔 (`vdm_agent.admx`) 新增至與虛擬桌面平台的 OU 連結的 GPO，或新增至與已發佈桌面平台的 RDS 主機連結的 GPO。如果您計劃設定任何選用的用戶端群組原則設定，還需要新增 Horizon Client 組態 ADMX 範本檔案 (`vdm_client.admx`)。如需安裝指示，請參閱 將 ADMX 範本檔新增至 Active Directory。
- 編譯可使用瀏覽器重新導向功能之網站的 URL 清單。

程序

1. 在遠端桌面平台上安裝 Chrome 瀏覽器。
2. 在您的 Active Directory 伺服器上，開啟群組原則管理編輯器。
3. 導覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能**資料夾。
4. 開啟**啟用 VMware HTML5 功能**設定，選取**已啟用**，然後按一下**確定**。
5. 導覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能 > VMware Browser 重新導向**資料夾。
6. 開啟**啟用 VMware Browser 重新導向**設定，選取**已啟用**，然後按一下**確定**。
7. 指定瀏覽器重新導向功能的 URL。

   使用者可以透過在 Chrome 網址列或自訂網址列中輸入這些 URL 來造訪這些 URL。使用者也可以從清單中的其他 URL 開始導覽或從任何代理程式端轉譯的頁面來造訪這些 URL。只有您指定的 URL 才會重新導向。依預設不會新增任何 URL。

   a 開啟**啟用 VMware Browser 重新導向的 URL 清單**設定，然後選取**已啟用**。

   b 按一下**顯示**，在 [值名稱] 欄中輸入 URL，然後按一下**確定**。

   讓 [值] 欄保持空白。

   c 若要儲存原則設定，請按一下**確定**。

8 (選擇性) 設定一或多個選用的代理程式端群組原則設定。

下表說明選用的代理程式端群組原則設定。

選項	敘述
啟用 VMware Browser 重新導向的導覽 URL 清單	您可以使用此設定來指定允許使用者從**啟用 VMware Browser 重新導向的 URL 清單**白名單中指定的 URL 導覽的目的 URL，可以透過在自訂網址列中直接輸入 URL，或者從白名單中指定的 URL 開始導覽至該 URL。 使用者無法透過在 Chrome 網址列中輸入 URL 或從代理程式端呈現的頁面導覽至 URL 來直接造訪這些 URL。 若要指定 URL，請按一下**顯示**，在 [值名稱] 欄中輸入 URL，然後按一下**確定**。讓 [值] 欄保持空白。
Enable automatic fallback after a whitelist violation	如果啟用此設定，如果使用者導覽至未在任何瀏覽器重新導向白名單中指定的 URL，無論是在自訂網址列中輸入 URL 或者透過從白名單中的任一 URL 開始導覽，則重新導向將針對該索引標籤停止，並改為在代理程式上擷取和顯示該 URL。 **備註** 如果使用者嘗試導覽至未在**啟用 VMware Browser 重新導向的 URL 清單**設定中指定的 URL，則無論是否啟用此設定，該索引標籤一律會回復為在代理程式上擷取和呈現該 URL。
Show a page with error information before automatic fallback	如果啟用此設定，則發生白名單違規時，系統會出現一個顯示倒數計時五秒的頁面。經過五秒後，該索引標籤將回復為在代理程式上擷取和呈現導致違規的 URL。如果停用此設定，則不會顯示五秒的警告頁面。僅當同時啟用了**啟用白名單違規後的自動後援**設定時，此設定才會生效。

9 (選擇性) 若要設定一或多個選用的用戶端群組原則設定，請導覽至**電腦組態 > 原則 > 管理範本 > VMware Horizon Client 組態 > VMware Browser 重新導向**。

下表說明用戶端群組原則設定。

選項	敘述
啟用瀏覽器重新導向的 WebRTC 相機和麥克風存取	如果啟用此設定，則使用 WebRTC 的重新導向頁面就可以存取用戶端系統的相機和麥克風。此設定依預設為啟用。
忽略瀏覽器重新導向的憑證錯誤	如果啟用此設定，系統將會忽略重新導向的頁面中發生的憑證錯誤，並繼續瀏覽。此設定依預設為停用。
啟用瀏覽器重新導向的快取	如果啟用此設定，則會將瀏覽歷程記錄 (包括 Cookie) 儲存在用戶端系統上。此設定依預設為啟用。 **備註** 停用此設定不會清除快取。如果先停用然後重新啟用此設定，那麼將重複使用快取。

範例

`https://play.google.com` 和 `https://news.google.com` 具有通用的登入頁面，`https://accounts.google.com`。

在以下範例中，`https://play.google.com/*` 和 `https://accounts.google.com/*` 包含在**啟用 VMware Browser 重新導向的 URL 清單**中。下表說明此案例中發生的行為。

使用者造訪 https://play.google.com	■ 將 https://play.google.com 重新導向至用戶端電腦。 ■ 當使用者登入時，用戶端電腦上會開啟 https://accounts.google.com，且使用者在用戶端電腦上進行驗證。 ■ 成功完成驗證後，網站在用戶端電腦上重新導向回 https://play.google.com，且使用者已正確登入。
使用者造訪 https://news.google.com	■ 在代理程式機器上呈現 https://news.google.com。 ■ 當使用者登入時，系統會將 https://accounts.google.com 重新導向至用戶端電腦，且使用者在用戶端電腦上進行驗證。 ■ 成功完成驗證後，使用者未正確登入，這是因為 https://news.google.com 是在代理程式機器上呈現，但驗證卻是在用戶端電腦上發生。
使用者在網址列中直接開啟 https://accounts.google.com	https://accounts.google.com 會重新導向至用戶端電腦。

在下一個範例中，https://play.google.com/* 包含在**啟用 VMware Browser 重新導向的 URL 清單**中，而 https://accounts.google.com/* 包含在**啟用 VMware Browser 重新導向的導覽 URL 清單**中。下表說明此案例中發生的行為。

使用者造訪 https://play.google.com	■ 將 https://play.google.com 重新導向至用戶端電腦。 ■ 當使用者登入時，用戶端電腦上會開啟 https://accounts.google.com，且使用者在用戶端電腦上進行驗證。 ■ 成功完成驗證後，網站在用戶端電腦上重新導向回 https://play.google.com，且使用者已正確登入。
使用者造訪 https://news.google.com	■ 在代理程式機器上呈現 https://news.google.com。 ■ 當使用者登入時，代理程式機器上會呈現 https://accounts.google.com，且使用者在代理程式機器上進行驗證。 ■ 成功完成驗證後，網站在代理程式機器上重新導向回 https://news.google.com，且使用者已正確登入。
使用者在網址列中直接開啟 https://accounts.google.com	https://accounts.google.com 會在代理程式機器上呈現。

後續步驟

安裝適用於 Chrome 的 VMware Horizon 瀏覽器重新導向延伸。

安裝適用於 Chrome 的 VMware Horizon 瀏覽器重新導向延伸

若要將瀏覽器重新導向功能與 Chrome 瀏覽器搭配使用，您必須在遠端桌面平台上強制安裝 VMware Horizon 瀏覽器重新導向延伸。您可以藉由在 Active Directory 伺服器上設定 Google Chrome 群組原則設定，來強制安裝此延伸。

若要將 Chrome 群組原則設定套用至遠端桌面平台，您必須將 ADMX 範本檔新增至 Active Directory 伺服器上的 GPO。對於虛擬桌面平台，GPO 必須連結至包含虛擬桌面平台的 OU。對於已發佈的桌面平台，GPO 必須連結至包含 RDS 主機的 OU。

必要條件

- 設定瀏覽器重新導向功能。請參閱安裝和設定瀏覽器重新導向。
- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。

程序

1 從 https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip 下載 Google Chrome `policy_templates.zip` 檔案。

2 解壓縮 `policy_templates.zip` 檔案，並將 `chrome.admx` 和 `chrome.adml` 檔案複製到 Active Directory 伺服器上。

`chrome.admx` 檔案位於 `policy_templates.zip` 檔案的 `\windows\admx` 資料夾中，`chrome.adml` 檔案則位於 `\windows\admx\`*`language`* 資料夾中。

a 將 `chrome.admx` 檔案複製到 Active Directory 伺服器上的 `%systemroot%\PolicyDefinitions` 資料夾。

b 將 `chrome.adml` 語言資源檔案複製到 Active Directory 伺服器的 `%systemroot%\PolicyDefinitions` 下適當的語言子資料夾中。

例如，將 `en_us` 版的 `chrome.adml` 檔案複製到 Active Directory 伺服器上的 `%systemroot%\PolicyDefinitions\en_us` 子資料夾。

3 在您的 Active Directory 伺服器上開啟群組原則管理編輯器，並導覽至**電腦設定 > 原則 > 系統管理範本 > Google Chrome > 延伸**資料夾。

4 開啟**設定強制安裝的應用程式和延伸清單**原則設定，然後按一下**已啟用**。

5 按一下**顯示**，然後在 [值] 欄中輸入 **`demgbalbngngkkgjcofhdiiipjblblob;https://clients2.google.com/service/update2/crx`**。

6 按一下**確定**以儲存延伸識別碼/更新 URL，然後按一下**確定**以儲存原則設定。

7 確認 VMware Horizon 瀏覽器重新導向延伸已安裝在遠端桌面平台上。

a 連線至遠端桌面平台，然後啟動 Chrome。

b 在 Chrome 位址列中輸入 **`chrome://extensions`**。

VMware Horizon 瀏覽器延伸會出現在 [延伸] 清單中。

瀏覽器重新導向限制

瀏覽器重新導向功能有某些限制。

- 只有 Windows 用戶端支援此功能。
- 僅支援 VMware Blast 和 PCoIP 顯示通訊協定。RDP 通訊協定不受支援。

- 瀏覽器重新導向無法與下列 Horizon 7 重新導向功能搭配使用：
  - URL 內容重新導向。
  - Chrome 中的 HTML5 多媒體重新導向功能。如果在 Chrome 中同時安裝了 VMware Horizon 瀏覽器重新導向延伸和 HTML5 多媒體重新導向延伸，且已這兩項功能均已正確設定群組原則設定，將只有瀏覽器重新導向可運作。
  - 地理位置重新導向。如果同時設定了這兩個功能，將會優先採用瀏覽器重新導向。
- 不支援 HTTP 和 HTTPS 以外的通訊協定，例如 mailto。
- 只有 Chrome 瀏覽器支援此功能。
- 如果您使用執行命令 (例如 **chrome *url***) 啟動 Chrome，瀏覽器重新導向將無法運作；請在編輯器內按一下 URL，或將書籤項目從 Chrome 的**書籤**功能表拖曳到遠端桌面平台，然後按兩下捷徑圖示。
- 在 Chrome 瀏覽器中使用瀏覽器重新導向功能時，可能會有下列與瀏覽器有關的限制。
  - 快顯視窗在新的索引標籤中持續保持開啟。
  - 與權限有關的快顯視窗不會顯示。
  - 您無法將重新導向檢視區上的連結拖曳到位址列。
  - 您無法下載檔案或儲存影像。
  - 您無法為需要驗證的網站儲存密碼。
  - 若要關閉索引標籤，請將焦點移至瀏覽器的索引標籤上。在焦點位於檢視區時按 Alt+F4、Ctrl+F4 或 Ctrl+W，可能會導致非預期的行為。
  - 清除瀏覽器資料 (包括 Cookie) 沒有作用。
  - 有時，您會無法回到前一頁或前往到上一頁。

設定地理位置重新導向

透過地理位置重新導向功能，遠端桌面平台和已發佈的應用程式可以使用用戶端裝置的地理位置資訊。

地理位置重新導向的系統需求

Horizon Agent 和 Horizon Client 以及安裝代理程式與用戶端軟體的虛擬桌面平台或 RDS 主機和用戶端機器都必須符合特定需求，才能支援地理位置重新導向功能。

虛擬桌面平台或 RDS 主機	■ 必須在**設定 > 隱私權 > 位置**中**開啟** Windows **位置服務**設定。

- 地理位置重新導向功能支援下列遠端桌面平台應用程式。

應用程式	平台
Google Chrome (最新版本)	所有虛擬桌面平台或 RDS 主機
Internet Explorer 11	所有虛擬桌面平台或 RDS 主機
Edge、Maps、Weather 以及其他 Win32 和 UWP 應用程式	Windows 8.1 與 Windows 10

  必須在每個支援的瀏覽器中個別啟用**位置**權限設定 (如果有的話)。

- 必須在選取地理位置重新導向自訂安裝選項的情況下，安裝 Horizon Agent 7.6 或更新版本。此選項依預設為未選取狀態。請參閱《在 Horizon 7 中設定虛擬桌面平台》和《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件中關於安裝 Horizon Agent 的主題。
- 必須在 Active Directory 伺服器上設定 VMware 地理位置重新導向群組原則設定。請參閱安裝和設定地理位置重新導向。
- 針對 Internet Explorer 11，必須為 Windows 7 虛擬桌面平台和 RDS 主機啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。請參閱啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。您不需要為 Windows 8.1 和 Windows 10 虛擬桌面平台啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。具有 VMware 地理位置重新導向驅動程式的 Windows 8.1 和 Windows 10 虛擬桌面平台可支援 Internet Explorer。
- 針對 Chrome，必須啟用 VMware Horizon 地理位置重新導向 Chrome 外掛程式。請參閱啟用 VMware Horizon 地理位置重新導向 Chrome 外掛程式。

用戶端系統

- 針對 Windows 8.1 和 Windows 10 用戶端系統，必須在**設定 > 隱私權 > 位置**中將 Windows **位置服務**設定為**開啟**，Horizon 才能存取您的所在位置。
- 您必須在用戶端系統上安裝 Windows 版 Horizon Client 4.9 或更新版本，並在 Windows 版 Horizon Client 中設定**地理位置**設定以共用用戶端系統的位置資訊。不支援非 Windows 用戶端。如需相關資訊，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。

適用於遠端工作階段的顯示通訊協定

- PCoIP
- VMware Blast

安裝和設定地理位置重新導向

若要將用戶端裝置的地理位置資訊重新導向至遠端桌面平台或已發佈的應用程式，則必須在代理程式機器上啟用地理位置重新導向功能、設定 Active Directory 伺服器的群組原則設定，並指定要使用此功能的網站。

若要啟用地理位置重新導向並指定要使用此功能的網站，您可以在 Active Directory 伺服器上設定群組原則設定。您必須編譯可使用已重新導向地理位置資訊的網站 URL 清單。請在 URL 中加入 `http://` 或 `https://` 前置詞。您可以在 URL 中使用比對模式。

必要條件

- 在用戶端系統上安裝 Horizon Client，並在已啟用地理位置重新導向功能的虛擬桌面平台或 RDS 主機上安裝 Horizon Agent。如需必要的版本、安裝選項和完整系統需求，請參閱地理位置重新導向的系統需求。
- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。
- 將 VMware View Agent 組態 ADMX 範本檔 (`vdm_agent.admx`) 新增至與虛擬桌面平台的 OU 或 RDS 主機連結的 GPO。如需安裝指示，請參閱將 ADMX 範本檔新增至 Active Directory。
- 編譯可使用已重新導向地理位置資訊的網站 URL 清單。
- 在代理程式機器上安裝 Internet Explorer 11 或 Chrome。

程序

1. 在您的 Active Directory 伺服器上，開啟群組原則管理編輯器。
2. 瀏覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能**資料夾。
3. 開啟**停用自動偵測內部網路**設定、選取**已啟用**，然後按一下**確定**。
4. 開啟**啟用 VMware HTML5 功能**設定，選取**已啟用**，然後按一下**確定**。
5. 瀏覽至**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能 > VMware 地理位置重新導向**資料夾。
6. 開啟**啟用 VMware 地理位置重新導向**設定，選取**已啟用**，然後按一下**確定**。
7. 指定哪些網站可以使用地理位置重新導向功能。

   VMware Horizon 地理位置重新導向 Chrome 外掛程式會在所有 RDS 主機和虛擬桌面平台環境中使用此網站清單。VMware Horizon 地理位置重新導向 IE 外掛程式會在 RDS 主機和 Windows 7 虛擬桌面平台環境中使用此網站清單。

   a 開啟**啟用 VMware 地理位置重新導向的 URL 清單**設定，然後選取**已啟用**。

   b 按一下**顯示**，然後輸入您在 [值名稱] 欄中編譯的 URL。

   僅您指定的 URL 可以使用重新導向的地理位置資訊。依預設不會新增任何 URL。讓 [值] 欄保持空白。

   c 按一下**確定**以儲存 URL 清單，然後按一下**確定**以儲存原則設定。
8. 開啟**設定要報告位置更新的最小距離**設定、選取**已啟用**，並指定用戶端中位置更新和上次向代理程式報告的更新 (必須更新新位置) 之間的最小距離 (以公尺為單位)。

   依預設，最小距離為 75 公尺。

後續步驟

如果您在 Windows 7 虛擬桌面平台或 RDS 主機代理程式機器上安裝了 Internet Explorer，則也必須啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。如需相關資訊，請參閱啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。

備註 具有 VMware 地理位置重新導向驅動程式的 Windows 8.1 和 Windows 10 虛擬桌面平台可支援 Internet Explorer。您不需要為 Windows 8.1 和 Windows 10 虛擬桌面平台啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。

如果您在代理程式機器上安裝了 Chrome，則也必須啟用 VMware Horizon 地理位置重新導向 Chrome 外掛程式。如需相關資訊，請參閱啟用 VMware Horizon 地理位置重新導向 Chrome 外掛程式。

啟用 VMware Horizon 地理位置重新導向 IE 外掛程式

若要搭配地理位置重新導向功能使用 Windows 7 虛擬桌面平台或已發佈桌面平台上的 Internet Explorer，您必須在虛擬桌面平台或 RDS 主機上啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。

具有 VMware 地理位置重新導向驅動程式的 Windows 8.1 和 Windows 10 虛擬桌面平台可支援 Internet Explorer。您不需要為 Windows 8.1 和 Windows 10 虛擬桌面平台啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。

必要條件

- 安裝和設定地理位置重新導向。
- 確認已關閉 Internet Explorer 11 中的**增強保護模式**。外掛程式無法使用此功能。
- 針對 Windows Server 作業系統，請確認 **Internet Explorer 增強式安全性設定**已關閉。外掛程式無法使用此功能。

程序

1. 在已啟用地理位置重新導向功能的虛擬桌面平台或 RDS 主機上，開啟 Internet Explorer 11。
2. 按一下瀏覽器視窗右上角的**工具**圖示，然後選取**管理附加元件**。
3. 向下捲動至 VMware, Inc. 區段，選取 **VMware Horizon 地理位置重新導向 IE 外掛程式**，然後按一下**啟用**。
4. 重新啟動 Internet Explorer 11。

啟用 VMware Horizon 地理位置重新導向 Chrome 外掛程式

若要透過 Chrome 使用地理位置重新導向功能，您必須啟用 VMware Horizon 地理位置重新導向 Chrome 外掛程式。

必要條件

安裝和設定地理位置重新導向。

程序

1 在 Active Directory 伺服器上，下載 `https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip` 檔案。

2 解壓縮 `chrome.admx` 檔案，然後將其複製到 Active Directory 伺服器上的 `%systemroot%\PolicyDefinitions` 資料夾。

3 解壓縮 `chrome.adml` 語言資源檔案，然後將其複製到 Active Directory 伺服器上 `%systemroot%\PolicyDefinitions\` 資料夾中的適當語言子資料夾。

例如，將 `en_us` 版的 `chrome.adml` 檔案複製到 Active Directory 伺服器上的 `%systemroot%\PolicyDefinitions\en_us` 子資料夾。

4 在您的 Active Directory 伺服器上開啟群組原則管理編輯器，並導覽至**電腦設定 > 原則 > 系統管理範本 > Google Chrome > 延伸**資料夾。

5 開啟**設定強制安裝的應用程式和延伸清單**群組原則設定，然後按一下**已啟用**。

6 按一下**顯示**，在**值**文字方塊中輸入 **`lndponbebpocehnoblfgdfeiegeaokcf;https://clients2.google.com/service/update2/crx`**，然後按一下**確定**。

7 若要儲存變更，請按一下**確定**。

8 若要確認遠端桌面平台上已安裝 VMware Horizon 地理位置重新導向擴充功能，請執行下列步驟。

a 連線至遠端桌面平台，然後啟動 Chrome。

b 在 Chrome 位址列中輸入 **`chrome://extensions`**。

c 確認 VMware Horizon 地理位置重新導向出現在 [擴充功能] 清單中。

設定即時音訊視訊

即時音訊視訊允許 Horizon 7 使用者在其遠端工作階段中執行 Skype、Webex、Google Hangouts、Microsoft Teams 以及其他線上會議應用程式。有了即時音訊視訊功能，將可重新導向連線至本機用戶端系統的網路攝影機和音訊裝置到遠端工作階段。此功能所需使用的頻寬較 USB 重新導向大幅減少，就可重新導向視訊和音訊資料。

即時音訊視訊與標準會議應用程式及以瀏覽器執行的視訊應用程式相容，且支援標準網路攝影機、音訊 USB 裝置和類比音訊輸入。

在設定應用程式 (如 Skype、Webex、Google Hangouts 或 Microsoft Teams) 時，使用者可從應用程式的功能表中選擇輸入和輸出裝置。

- 對於虛擬桌面平台，如果使用 Windows 5.2 版 Horizon Client 及更新版本，即時音訊視訊將可重新導向多個音訊和視訊裝置。虛擬桌面平台中重新導向的裝置名稱為實際的裝置名稱，但附加了 (VDI)，例如，C670i FHD 網路攝影機 (VDI)。
- 對於虛擬桌面平台，如果使用 Windows 5.1 版 Horizon Client 及更新版本，或使用非 Windows 用戶端，則即時音訊視訊只能將一個音訊裝置和一個視訊裝置重新導向至虛擬桌面平台。裝置名稱為虛擬桌面平台中的 VMware 虛擬麥克風和 VMware 虛擬網路攝影機。

- 對於已發佈的桌面平台和已發佈的應用程式，即時音訊視訊只能重新導向一個音訊裝置和一個視訊裝置。裝置名稱為遠端工作階段中的遠端音訊裝置和 VMware 虛擬網路攝影機。

VMware 虛擬網路攝影機使用核心模式網路攝影機驅動程式，該驅動程式可針對以瀏覽器執行的視訊應用程式和其他第三方會議軟體提供進階相容性。

啟動會議應用程式或視訊應用程式時，將顯示並使用 VMware 虛擬裝置，這些裝置會處理連接到用戶端本機裝置的音訊視訊重新導向。

Horizon Client 系統上必須安裝音訊和網路攝影機裝置的驅動程式，才能啟用重新導向。

即時音訊視訊的組態選擇

在 Horizon Agent 中安裝即時音訊視訊後，在不需進行進一步組態的情況下，該功能可在遠端工作階段運作。網路攝影機的畫面播放速率以及映像解析度的預設值是依據多數標準裝置和應用程式提出的建議。

您可設定群組原則設定，變更這些預設值，以適用於特定的應用程式、網路攝影機或環境。您也可以設定原則來停用或啟用功能。ADMX 範本檔可讓您在 Active Directory 伺服器或個別的桌面平台上安裝即時音訊視訊群組原則設定。請參閱設定即時音訊視訊群組原則設定。

如果使用者有多個內建於或連接到用戶端電腦的網路攝影機和音訊輸入裝置，您可能需要設定要重新導向的偏好網路攝影機和音訊輸入裝置。請參閱選取偏好的網路攝影機和麥克風。

備註 您可選取想要使用的音訊裝置，但將沒有可使用的其他音訊設定選項。

重新導向網路攝影機映像和音訊輸入到遠端工作階段時，您無法存取本機電腦上的網路攝影機和音訊裝置。反過來說，在本機電腦上使用這些裝置時，您也無法在遠端工作階段存取這些裝置。

即時音訊視訊系統需求

即時音訊視訊功能可與標準網路攝影機、USB 音訊和類比音訊裝置搭配使用。此功能也可與標準會議應用程式搭配使用。若要支援即時音訊視訊，您的 Horizon 部署必須符合特定軟體和硬體需求。

虛擬桌面平台	將 Microsoft Teams 與即時音訊視訊搭配使用時，VMware 建議虛擬桌面平台至少要有 4 個 vCPU 和 4 GB 的 RAM。
Horizon Client 軟體	■ Windows 版 Horizon Client2.2 或更新版本。若要在虛擬桌面平台中使用多個網路攝影機或麥克風，必須安裝 Windows 版 Horizon Client5.2 或更新版本。 ■ Linux 版 Horizon Client2.2 或更新版本。對於 3.1 版或更早版本，只有第三方廠商提供的 Linux 版 Horizon Client 才可使用該功能。對於 3.2 版及更新版本，VMware 提供的用戶端版本也可使用該功能。 ■ Mac 版 Horizon Client2.3 或更新版本。 ■ iOS 版 Horizon Client4.0 或更新版本。 ■ Android 版 Horizon Client4.0 或更新版本。 ■ Chrome OS 版 Horizon Client4.3 或更新版本。

	■ Chrome 版 Horizon Client4.8 或更新版本。 ■ Windows 10 UWP 版 Horizon Client5.2 或更新版本。
Horizon Client 電腦或用戶端存取裝置	■ 所有執行 Windows、iOS、Android、Chrome OS、Chrome 和 Windows 10 UWP 版 Horizon Client 的作業系統。 ■ 在 x86 裝置上執行 Linux 版 Horizon Client 的所有作業系統。在 ARM 處理器上不支援此功能。 ■ Mac OS X Mountain Lion (10.8) 及更新版本。在所有之前的 Mac OS X 作業系統上已停用此功能。 ■ 如需支援的用戶端作業系統的相關資訊，請參閱相應系統或裝置的 Horizon Client 安裝和設定文件。 ■ 必須安裝網路攝影機和音訊裝置驅動程式，且在用戶端電腦上網路攝影機和音訊裝置必須可使用。您不需在安裝代理程式的機器上安裝裝置驅動程式。
顯示通訊協定	■ PCoIP **備註** Windows 10 UWP 版 Horizon Client 不支援即時音訊視訊與 PCoIP 的搭配使用。 ■ VMware Blast (需要 Horizon Agent7.0 或更新版本)

確認使用即時音訊視訊，而非 USB 重新導向

即時音訊視訊支援用於會議應用程式的網路攝影機和音訊輸入重新導向。隨附 Horizon Agent 一起安裝的 USB 重新導向功能不支援網路攝影機重新導向。如果透過 USB 重新導向來重新導向音訊輸入裝置，則音訊串流不會在即時音訊視訊工作階段期間與視訊正確同步，並且您會失去降低網路頻寬需求的好處。您可以採取步驟確保網路攝影機和音訊輸入裝置會透過即時音訊視訊，而非 USB 重新導向，重新導向至桌面平台。

如果您的桌面平台設定了 USB 重新導向，則使用者可透過選取 Windows 用戶端功能表列中的**連線 USB 裝置**選項或 Mac 用戶端中的**桌面平台 > USB** 功能表，來連線並顯示其本機連線的 USB 裝置。依預設，Linux 用戶端會封鎖音訊和視訊裝置的 USB 重新導向，並且不會為使用者提供 USB 裝置選項。

如果使用者從**連線 USB 裝置**或**桌面平台 > USB** 清單中選取某個 USB 裝置，則該裝置無法用來進行視訊或音訊會議。例如，如果使用者進行 Skype 通話，則視訊映像可能不會顯示，或者音訊串流可能會降級。如果使用者在某個會議工作階段期間選取裝置，則網路攝影機或音訊重新導向會中斷。

若要針對使用者隱藏這些裝置並避免發生潛在的中斷，請設定 USB 重新導向群組原則設定，以在 VMware Horizon Client 中停用顯示網路攝影機和音訊輸入裝置。

尤其是，您可以針對 Horizon Agent 建立 USB 重新導向篩選規則，並指定要停用的 `audio-in` 和 `video` 裝置系列名稱。如需設定群組原則和指定 USB 重新導向篩選規則的相關資訊，請參閱使用原則來控制 USB 重新導向。

注意　如果未設定用於停用 USB 裝置系列的 USB 重新導向篩選規則，請通知您的使用者，無法從 VMware Horizon Client 功能表列中的**連線 USB 裝置**或**桌面平台 > USB** 清單中選取網路攝影機或音訊裝置。

選取偏好的網路攝影機和麥克風

如果用戶端電腦有多個網路攝影機和麥克風，您可以設定偏好的網路攝影機和麥克風，即時音訊視訊會將其重新導向至遠端桌面平台或已發佈的應用程式。這些裝置可以是內建裝置，或連接到用戶端電腦的外接裝置。

如果可用，即時音訊視訊將重新導向想要使用的網路攝影機。如果偏好的網路攝影機無法使用，則即時音訊視訊會使用系統列舉所提供的第一個網路攝影機。

Windows 用戶端電腦	對於已發佈的桌面平台或已發佈的應用程式，如果用戶端電腦已安裝 Windows 版 Horizon Client4.2 或更新版本，您可以藉由在 Horizon Client 的 [設定] 對話方塊中設定 [即時音訊視訊] 設定，來選取偏好的網路攝影機或麥克風。 對於虛擬桌面平台，如果用戶端電腦已安裝 Windows 版 Horizon Client4.2 到 5.1，您可以藉由在 Horizon Client 的 [設定] 對話方塊中設定 [即時音訊視訊] 設定，來選取偏好的網路攝影機或麥克風。從 Windows 版 Horizon Client 5.2 和 Horizon Agent 7.10 開始，即時音訊視訊功能已可將多個網路攝影機和麥克風重新導向至虛擬桌面平台，且您無須選取偏好的網路攝影機或麥克風。 使用 4.2 版之前的 Windows 版 Horizon Client 時，您必須修改登錄設定以選取偏好的網路攝影機，並使用 Windows 作業系統中的 [音效] 控制項來選取預設的麥克風。 如需詳細資訊，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。
Mac 用戶端電腦	您可以使用 Mac 預設系統來指定偏好的網路攝影機或麥克風。如需詳細資訊，請參閱《Mac 版 VMware Horizon Client 安裝和設定指南》文件。
Linux 用戶端電腦	您可藉由編輯組態檔來指定偏好的網路攝影機。若要選取預設麥克風，可以在用戶端電腦上設定 Linux 作業系統的 [音效] 控制。如需詳細資訊，請參閱《Linux 版 VMware Horizon Client 安裝和設定指南》文件。
Chromebook 用戶端電腦	如果 Chromebook 已安裝 Chrome 版 Horizon Client4.8 或更新版本，您可以藉由在 Horizon Client 的 [設定] 對話方塊中設定 [即時音訊視訊] 設定，以

	選取偏好的網路攝影機或麥克風。如需詳細資訊，請參閱《Chrome 版 VMware Horizon Client 安裝和設定指南》文件。
Windows 10 UWP 用戶端電腦	如果使用已安裝 Windows 10 UWP 版 Horizon Client5.2 或更新版本的 Windows 10 UWP 電腦，您可以藉由在 Horizon Client 的 [設定] 對話方塊中設定 [即時音訊視訊] 設定，以選取偏好的網路攝影機或麥克風。如需詳細資訊，請參閱《Windows 10 UWP 版 VMware Horizon Client 安裝和設定指南》文件。

設定即時音訊視訊群組原則設定

您可設定控制遠端桌面平台上即時音訊視訊 (RTAV) 行為的群組原則設定。這些設定會決定虛擬網路攝影機的最大畫面播放速率和影像解析度。該設定允許您管理使用者可使用的最大頻寬。另有額外設定可停用或啟用 RTAV 功能。

您不需設定這些原則設定。即時音訊視訊可與用戶端系統中網路攝影機的設定畫面播放速率和影像解析度搭配使用。建議使用適用多數網路攝影機和音訊應用程式的預設設定。

如需即時音訊視訊期間使用的頻寬範例，請參閱 即時音訊視訊頻寬。

這些原則設定會影響遠端桌面平台，而非實體裝置連接的用戶端系統。若要在桌面平台上進行這些設定，請在 Active Directory 中新增 RTAV 群組原則系統管理範本 (ADMX) 檔案。

如需在用戶端系統設定這些設定的資訊，請參閱 VMware 知識庫文章：Setting Frame Rates and Resolution for Real-Time Audio-Video on Horizon View Clients (在 Horizon View Client 上設定即時音訊視訊的畫面播放速率和解析度)，網址 http://kb.vmware.com/kb/2053644。

在 Active Directory 新增 RTAV ADMX 範本和進行設定

您可以將 RTAV ADMX 檔案 (`vdm_agent_rtav.admx`) 中的原則設定新增至 Active Directory 中的群組原則物件 (GPO)，並在群組原則物件編輯器中進行設定。

必要條件

- 確認已在虛擬機器桌面平台和 RDS 主機上安裝 RTAV 安裝選項。依預設會安裝此安裝選項，但也可以在安裝期間取消選取。如果未安裝 RTAV，則設定沒有任何作用。如需安裝 Horizon Agent 的相關資訊，請參閱您的《設定》文件。
- 確認已為 RTAV 群組原則設定建立 Active Directory GPO。GPO 必須連結至包含虛擬機器桌面平台或 RDS 主機的 OU。請參閱 Active Directory 群組原則範例。
- 確認 Microsoft MMC 和群組原則物件編輯器的嵌入式管理單元可在 Active Directory 伺服器上使用。
- 熟悉 RTAV 群組原則設定。請參閱即時音訊視訊群組原則設定 。

程序

1 從 VMware 下載網站下載 Horizon 7 GPO 服務包 `.zip` 檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在「桌面平台及使用者運算」下，選取 VMware Horizon 7 下載，其中包含 GPO 服務包。

該檔案名為 VMware-Horizon-Extras-Bundle-*x.x.x*-*yyyyyyy*.zip，其中 *x.x.x* 為版本，而 *yyyyyyy* 為組建編號。為 Horizon 7 提供群組原則設定的所有 ADMX 檔案皆可從此檔案取得。

2 解壓縮 VMware-Horizon-Extras-Bundle-*x.x.x*-*yyyyyyy*.zip 檔案，並將 ADMX 檔案複製到您的 Active Directory 伺服器。

a 將 vdm_agent_rtav.admx 檔案和 en-US 資料夾複製到 Active Directory 伺服器上的 C:\Windows\PolicyDefinitions 資料夾。

b (選擇性) 將語言資源檔案 (vdm_agent_rtav.adml) 複製到 Active Directory 伺服器上 C:\Windows\PolicyDefinitions\ 下的適當子資料夾中。

3 在 Active Directory 伺服器上開啟群組原則管理編輯器，然後在編輯器中輸入範本檔的路徑。

這些設定位於**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > View RTAV 組態**資料夾中。

後續步驟

設定群組原則設定。

即時音訊視訊群組原則設定

即時音訊視訊 (RTAV) 群組原則設定控制虛擬網路攝影機的最大畫面播放速率和最大映像解析度。其他設定可讓您停用或啟用 RTAV 功能。這些原則設定會影響遠端桌面平台，而不是與實體裝置連線的用戶端系統。

如果未設定 RTAV 群組原則設定，RTAV 將使用用戶端系統中設定的值。在用戶端系統上，預設網路攝影機畫面播放速率為每秒 15 個畫面。預設網路攝影機映像解析度為 320x240 像素。

解析度群組原則設定會決定可使用的最大值。用戶端系統上設定的畫面播放速率和解析度為絕對值。例如，如果將 RTAV 設定的最大映像解析度設定為 640x480 像素，則網路攝影機會顯示用戶端上設定為最高達 640x480 像素的任何解析度。如果將用戶端的映像解析度設為高於 640x480 像素的值，則用戶端解析度將限定為 640x480 像素。

並非所有組態均可達到每秒 25 個畫面時解析度為 1920x1080 像素的最大群組原則設定。對於指定解析度，您的組態可達到的最大畫面播放速率取決於所使用的網路攝影機、用戶端系統硬體、Horizon Agent 虛擬硬體以及可用頻寬。

解析度群組原則設定會決定使用者未設定解析度值時所使用的預設值。

群組原則設定	說明
Disable RTAV	啟用此設定時，會停用即時音訊視訊功能。 未設定或停用此設定時，會啟用即時音訊視訊。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > View RTAV 組態**資料夾中。
Max frames per second	決定網路攝影機每秒可擷取的最大畫面數。您可使用此設定來限制低頻寬網路環境下網路攝影機的畫面播放速率。 最小值為每秒一個畫面。最大值為每秒 25 個畫面。 未設定或停用此設定時，不會設定最大畫面播放速率。即時音訊視訊將使用在用戶端系統上為網路攝影機選取的畫面播放速率。 依預設，用戶端網路攝影機的畫面播放速率為每秒 15 個畫面。如果用戶端系統中未設定任何設定，且未設定或停用**每秒的最大畫面數**設定，則網路攝影機會每秒擷取 15 個畫面。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > View RTAV 組態 > View RTAV 網路攝影機設定**資料夾中。
Resolution – Max image width in pixels	決定網路攝影機擷取之映像畫面的最大寬度 (以像素為單位)。透過設定一個低最大映像寬度，您可以降低擷取畫面的解析度，這樣可改善低頻寬網路環境下的映像擷取體驗。 未設定或停用此設定時，不會設定最大映像寬度。RTAV 將使用用戶端系統上設定的映像寬度。用戶端系統上網路攝影機映像的預設寬度為 320 像素。 任何網路攝影機映像的解析度上限為 1920x1080 像素。如果將此設定設定為一個高於 1920 像素的值，則有效的最大映像寬度為 1920 像素。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > View RTAV 組態 > View RTAV 網路攝影機設定**資料夾中。
Resolution – Max image height in pixels	決定網路攝影機擷取之映像畫面的最大高度 (以像素為單位)。透過設定一個低最大映像高度，您可以降低擷取畫面的解析度，這樣可改善低頻寬網路環境下的映像擷取體驗。 未設定或停用此設定時，不會設定最大映像高度。RTAV 將使用用戶端系統上設定的映像高度。用戶端系統上網路攝影機映像的預設高度為 240 像素。 任何網路攝影機映像的解析度上限為 1920x1080 像素。如果將此設定設定為一個高於 1080 像素的值，則有效的最大映像高度為 1080 像素。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > View RTAV 組態 > View RTAV 網路攝影機設定**資料夾中。
Resolution – Default image resolution width in pixels	決定網路攝影機擷取之映像畫面的預設解析度寬度 (以像素為單位)。在使用者未定義解析度值的情況下使用此設定。 未設定或停用此設定時，預設映像寬度為 320 像素。 只有在同時使用 View Agent 6.0 或更新版本和 Horizon Client 3.0 或更新版本時，此原則設定所設定的值才會生效。對於舊版 View Agent 和 Horizon Client，此原則設定沒有作用，且預設映像寬度為 320 像素。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > View RTAV 組態 > View RTAV 網路攝影機設定**資料夾中。
Resolution – Default image resolution height in pixels	決定網路攝影機擷取之映像畫面的預設解析度高度 (以像素為單位)。在使用者未定義解析度值的情況下使用此設定。 未設定或停用此設定時，預設映像高度為 240 像素。 只有在同時使用 View Agent 6.0 或更新版本和 Horizon Client 3.0 或更新版本時，此原則設定所設定的值才會生效。對於舊版 View Agent 和 Horizon Client，此原則設定沒有作用，且預設映像高度為 240 像素。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > View RTAV 組態 > View RTAV 網路攝影機設定**資料夾中。

即時音訊視訊頻寬

即時音訊視訊頻寬會根據網路攝影機的映像解析度和畫面播放速率，以及正在擷取的映像和音訊資料而有所不同。

表 2-2. 從 Horizon Client 傳送即時音訊視訊資料至 Horizon Agent 的頻寬結果範例中顯示的範例測試使用標準網路攝影機和音訊輸入裝置測量即時音訊視訊在 Horizon 7 環境中使用的頻寬。該測試測量將視訊和音訊資料從 Horizon Client 傳送至 Horizon Agent 的頻寬。從 Horizon Client 執行桌面平台工作階段所需的總頻寬可能比這些數字更高。在這些測試中，網路攝影機會針對每種映像解析度以每秒 15 個畫面的速度擷取映像。

表 2-2. 從 Horizon Client 傳送即時音訊視訊資料至 Horizon Agent 的頻寬結果範例

映像解析度 (寬度 x 高度)	使用的頻寬 (Kbps)
160 x 120	225
320 x 240	320
640 x 480	600

為 Microsoft Teams 設定即時音訊視訊

透過即時音訊視訊，使用者將可在其遠端工作階段中執行 Microsoft Teams。

連線至本機用戶端系統的網路攝影機和音訊裝置會重新導向至遠端工作階段，且所需使用的頻寬較 USB 重新導向大幅減少。

當您在遠端桌面平台中啟動 Microsoft Teams 應用程式時，您可以從應用程式中的功能表選取 VMware 虛擬輸入和輸出裝置。VMware 虛擬裝置會重新導向連線至用戶端機器的音訊和視訊裝置。

- 對於虛擬桌面平台，如果使用 Windows 5.2 版 Horizon Client 及更新版本，即時音訊視訊將可重新導向多個音訊和視訊裝置。虛擬桌面平台中重新導向的裝置名稱為實際的裝置名稱，但附加了 (VDI)，例如，C670i FHD 網路攝影機 (VDI)。
- 對於虛擬桌面平台，如果使用 Windows 5.1 版 Horizon Client 及更新版本，或使用非 Windows 用戶端，則即時音訊視訊只能將一個音訊裝置和一個視訊裝置重新導向至虛擬桌面平台。裝置名稱為虛擬桌面平台中的 VMware 虛擬麥克風和 VMware 虛擬網路攝影機。
- 對於已發佈的桌面平台和已發佈的應用程式，即時音訊視訊只能重新導向一個音訊裝置和一個視訊裝置。裝置名稱為遠端工作階段中的遠端音訊裝置和 VMware 虛擬網路攝影機。

若要搭配使用即時音訊視訊與 Microsoft Teams，您必須在 Horizon Client 系統上安裝音訊和網路攝影機裝置驅動程式。

在 Horizon Agent 中安裝即時音訊視訊後，不需要進行進一步組態，Microsoft Teams 即可在遠端工作階段上運作。請參閱設定即時音訊視訊。

搭配使用 Microsoft Teams 與即時音訊視訊時的建議

若要搭配使用 Microsoft Teams 與即時音訊視訊，請遵循以下建議：

- Windows、Linux 和 Mac 用戶端上的 Horizon Agent7.9 版及更新版本支援 Microsoft Teams 與即時音訊視訊的搭配使用。
- 要搭配使用 Microsoft Teams 與即時音訊視訊，至少需要 4 個 vCPU、4 GB RAM 的組態，以及 640 x 480 像素的最大視訊解析度。額外的 vCPU 和記憶體組態可提供更卓越的體驗。
- 即時音訊視訊的預設視訊解析度為 320 x 240 像素。您可以在群組原則管理編輯器中變更 **VMware View Agent 組態 > View RTAV 組態**資料夾中的設定，藉以變更解析度。

設定掃描器重新導向

如果掃描和影像裝置已本機連線至用戶端電腦，則使用者可以透過使用掃描器重新導向掃描其遠端桌面平台或已發佈應用程式中的資訊。

掃描器重新導向支援與 TWAIN 和 WIA 格式和 Linux 用戶端上的 SANE 相容的標準掃描和影像裝置。

使用掃描器重新導向安裝選項安裝 Horizon Agent 後，無需進行進一步組態，該功能即可在遠端桌面平台和應用程式中正常運作。您不必在遠端桌面平台或應用程式上設定掃描器特定的驅動程式。

您可設定群組原則設定，變更這些預設值，以適用於特定的掃描和影像應用程式或環境。您也可以設定原則來一起停用或啟用功能。透過 ADMX 範本檔，您可以您的在 Active Directory 伺服器或個別的桌面平台上安裝掃描器重新導向群組原則設定。請參閱設定掃描器重新導向群組原則設定。

將掃描資料重新導向到遠端桌面平台或應用程式時，您無法在本機電腦上存取掃描或影像裝置。反過來說，在本機電腦上使用某個裝置時，您也無法在遠端桌面平台或應用程式上存取該裝置。

掃描器重新導向的系統需求

若要支援掃描器重新導向，您的 Horizon 7 部署必須符合特定軟體和硬體需求。

遠端桌面平台或已發佈的應用程式	已發佈桌面平台和 RDS 主機上已發佈應用程式，以及部署在單一使用者虛擬機器上的虛擬桌面平台上皆支援此功能。 您必須在父系或範本虛擬機器或 RDS 主機上安裝 Horizon Agent 7.0 或更新版本，並選取 [掃描器重新導向設定] 選項。 在 Windows 桌面平台和 Windows Server 客體作業系統上，Horizon Agent [掃描器重新導向] 安裝選項預設為取消選取。 單一使用者虛擬機器以及以上所述的 RDS 主機上支援下列客體作業系統： ■ 32 位元或 64 位元的 Windows 7 ■ 32 位元或 64 位元的 Windows 8。*x* ■ 32 位元或 64 位元的 Windows 10 ■ 設定為桌面平台或 RDS 主機的 Windows Server 2008 R2

	■ 設定為桌面平台或 RDS 主機的 Windows Server 2012 R2 **重要** Windows Server 客體作業系統上必須安裝了桌面平台體驗功能，無論設定為桌面平台還是 RDS 主機。 您不需在安裝 Horizon Agent 的桌面平台作業系統上安裝掃描器裝置驅動程式。
Windows 版 Horizon Client 軟體	Horizon Client 4.0 或更新版本
Horizon Client 電腦或用戶端存取裝置	支援的作業系統： ■ 32 位元或 64 位元的 Windows 7 ■ 32 位元或 64 位元的 Windows 8。*x* ■ 32 位元或 64 位元的 Windows 10 必須安裝掃描器裝置驅動程式，且在用戶端電腦上必須可執行掃描器。
掃描裝置標準	TWAIN 或 WIA
顯示通訊協定	PCoIP VMware Blast (需要 Horizon Client 4.0 或更新版本，以及 Horizon Agent 7.0 或更新版本) RDP 桌面平台工作階段不支援掃描器重新導向。

掃描器重新導向的使用者作業

透過掃描器重新導向，使用者可以操作以虛擬裝置連線至其用戶端電腦的實體掃描器與影像裝置，從而在其遠端桌面平台與應用程式中執行掃描作業。

使用者可以使用與在其本機連線的用戶端電腦上使用掃描器非常相似的方法，操作其虛擬掃描器。

- 對於 Horizon Agent 安裝「掃描器重新導向」選項後，掃描器工具匣圖示 ( ) 便會新增到桌面平台。在已發佈的應用程式上，工具匣圖示將重新導向至本機用戶端電腦。

  您無需使用掃描器工具匣圖示。在不需進行任何進一步設定的情況下，掃描重新導向即可運作。如果有多個裝置連線至用戶端電腦，您可以使用圖示來設定選項，例如變更要使用的裝置。
- 按一下掃描器圖示，即會顯示 [VMware Horizon 的掃描器重新導向] 功能表。如果連線至用戶端電腦的掃描器不相容，功能表中不會出現任何掃描器。
- 依預設，系統會自動選取掃描裝置。會分別選取 TWAIN 與 WIA 掃描器。您可以同時選取一部 TWAIN 掃描器與一部 WIA 掃描器。
- 如果已設定多部本機連線的掃描器，您可以選取與預設選取的掃描器不同的掃描器。
- WIA 掃描器顯示在遠端桌面平台之 [裝置管理員] 功能表的**影像裝置**下方。WIA 掃描器命名為 **VMware Virtual WIA Scanner**。

- 在 [VMware Horizon 的掃描器重新導向] 功能表中，您可以按一下**喜好設定**選項並從掃描器重新導向功能表中選取選項 (例如隱藏網路攝影機)，然後判定如何選取預設掃描器。

  您還可以藉由在 Active Directory 中設定掃描器重新導向群組原則設定來控制這些功能。請參閱掃描器重新導向群組原則設定。

- 操作 TWAIN 掃描器時，[VMware Horizon 的 TWAIN 掃描器重新導向] 功能表會提供其他選項，用於選取影像區域、按彩色、黑白或灰階進行掃描，以及選擇其他常用功能。

- 若要顯示 TWAIN 掃描軟體的 TWAIN 使用者介面視窗 (依預設不會顯示此視窗)，您可以在 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中選取**總是顯示 [掃描器設定] 對話方塊**選項。

  請注意，依預設大多數 TWAIN 掃描軟體會顯示 TWAIN 使用者介面視窗。對於此軟體，不論您是否選取**總是顯示 [掃描器設定] 對話方塊**選項，此視窗會始終顯示。

備註 如果您執行在不同伺服器陣列上主控的兩個已發佈應用程式，則用戶端電腦上會出現兩個掃描器重新導向工具匣圖示。通常，僅有一部掃描器會連線至用戶端電腦。在此情況下，不論您選取哪個圖示，兩個圖示均指向同一個裝置。在某些情況下，您可能會有兩部本機連線的掃描器，並且執行兩個在其他伺服器陣列上執行的已發佈應用程式。在該情況下，您必須開啟每個圖示，才能查看每個掃描器重新導向功能表分別控制哪個已發佈應用程式。

如需操作重新導向之掃描器的使用者指示，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。

設定掃描器重新導向群組原則設定

您可以設定群組原則設定，用於控制遠端桌面平台和應用程式上掃描器重新導向的行為。使用這些原則設定，您可以從 Active Directory 集中控制使用者桌面平台和應用程式上的 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊提供的選項。

您不需設定這些原則設定。掃描器重新導向與遠端桌面平台和用戶端系統上掃描裝置的預設設定搭配使用。

這些原則設定會影響遠端桌面平台和應用程式，而不是與實體掃描器連線的用戶端系統。若要在桌面平台和應用程式上進行上述設定，請在 Active Directory 中新增掃描器重新導向群組原則系統管理範本 (ADMX) 檔案。

在 Active Directory 中新增掃描器重新導向 ADMX 範本

您可以將掃描器重新導向 ADMX 範本檔 (`vdm_agent_scanner.admx`) 中的原則設定新增至 Active Directory 中的群組原則物件 (GPO)，並在群組原則物件編輯器中進行設定。

必要條件

- 確認已在虛擬機器桌面平台或 RDS 主機上安裝掃描器重新導向安裝選項。如果未安裝掃描器重新導向，則群組原則設定沒有任何作用。如需安裝 Horizon Agent 的相關資訊，請參閱您的《設定》文件。
- 確認已為掃描器重新導向群組原則設定建立 Active Directory GPO。GPO 必須連結至包含虛擬桌面平台或 RDS 主機的 OU。請參閱 Active Directory 群組原則範例。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。

- 請自行熟悉掃描器重新導向群組原則設定。請參閱掃描器重新導向群組原則設定。

程序

1. 從 VMware 下載網站下載 Horizon 7 GPO 服務包 `.zip` 檔案，網址為 https://my.vmware.com/web/vmware/downloads。

   在「桌面平台及使用者運算」下，選取 VMware Horizon 7 下載，其中包含 GPO 服務包。

   該檔案名為 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`，其中 *x.x.x* 為版本，而 *yyyyyyy* 為組建編號。為 Horizon 7 提供群組原則設定的所有 ADMX 檔案皆可從此檔案取得。

2. 解壓縮 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 檔案，並將 ADMX 檔案複製到您的 Active Directory 伺服器。

   a. 將 `vdm_agent_scanner.admx` 檔案和 `en-US` 資料夾複製到 Active Directory 伺服器上的 `C:\Windows\PolicyDefinitions` 資料夾。

   b. (選擇性) 將語言資源檔案 (`vdm_agent_scanner.adml`) 複製到 Active Directory 伺服器上 `C:\Windows\PolicyDefinitions\` 下的適當子資料夾中。

3. 在 Active Directory 伺服器上開啟群組原則管理編輯器，然後在編輯器中輸入範本檔的路徑。

   這些設定位於**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > 掃描器重新導向**資料夾中。

   大部分的設定也會新增至**使用者設定**資料夾，位於**使用者設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > 掃描器重新導向**資料夾中。

後續步驟

設定群組原則設定。

掃描器重新導向群組原則設定

掃描器重新導向群組原則設定控制使用者之桌面平台和應用程式上 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中可用的選項。

掃描器重新導向 ADMX 範本檔包含「電腦組態」與「使用者組態」原則。「使用者組態」原則允許您為虛擬桌面平台、已發佈桌面平台和已發佈應用程式使用者設定不同的組態。即使使用者之桌面平台工作階段和應用程式在同一 RDS 主機上執行，不同的「使用者組態」原則也會生效。所有設定皆位於群組原則管理編輯器的 **VMware Horizon Agent 組態 > 掃描器重新導向**資料夾中。

表 2-3. 掃描器重新導向群組原則設定

設定	電腦	使用者	說明
BandwidthLimit		X	指定將掃描的資料傳輸至使用者工作階段時允許的最大頻寬 (以每秒 KB 為單位)。 如果您指定 0 或不指定任何值，則頻寬將不受限制。
Compression		X	指定將在影像傳輸到遠端桌面平台或已發佈應用程式期間使用的影像壓縮率。 您可選取以下其中一個壓縮模式： ■ **停用** - 影像壓縮會停用。 ■ **不失真** - 使用不失真 (zlib) 壓縮時，影像品質不會下降。 ■ **JPEG** - 使用 JPEG 壓縮時品質會下降。您可以從 **JPEG 壓縮品質**下拉式功能表中選取影像品質等級。JPEG 壓縮品質必須為 0 到 100 之間的值。 啟用該設定時，將為受該原則影響之所有使用者設定所選壓縮模式。使用者可在 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中變更**壓縮**選項，從而覆寫原則設定。 停用該原則設定或未設定該設定時，將使用 JPEG 壓縮模式。
Default Color Mode			啟用此設定時，您可以設定預設色彩模式：黑白、灰階或彩色。Windows XP Professional 或 Windows Server 2003 或更高版本上支援此設定。
Default Duplex			啟用此設定時，您可以設定預設掃描模式：單面或雙面。在雙面模式下，掃描應用程式必須支援雙面掃描，並向掃描器要求兩個頁面。Windows XP Professional 或 Windows Server 2003 或更高版本上支援此設定。
Default Scanner	X	X	提供對掃描器自動選取的集中化管理。 您可以分別為 TWAIN 和 WIA 掃描器選取掃描器自動選取選項。您可選取下列其中一個自動選取選項： ■ **無**。請勿自動選取掃描器。 ■ **自動選取** 自動選取本機連線的掃描器。 ■ **最近使用** 自動選取上次使用的掃描器。 ■ **指定** 選取在**指定的掃描器**文字方塊中輸入的掃描器名稱。 將該設定做為「電腦組態」原則啟用時，設定會決定適用於受影響電腦之所有使用者的掃描器自動選取模式。使用者無法在 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中變更**預設掃描器**選項。 將該設定做為「使用者組態」原則啟用時，設定會決定適用於所有受影響使用者的掃描器自動選取模式。但是，使用者可以在 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中變更**預設掃描器**選項。 在「電腦組態」和「使用者組態」中同時啟用該設定時，「電腦組態」中的掃描器自動選取模式將針對受影響電腦之所有使用者覆寫「使用者組態」中的對應原則設定。 在任一原則組態中停用該設定或未設定該設定時，掃描器自動選取模式由對應的原則設定 (「使用者組態」或「電腦組態」) 或 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中的使用者選取決定。
Disable functionality	X		停用掃描器重新導向功能。 啟用該設定時，無法重新導向掃描器且掃描器不會顯示在使用者之桌面平台和應用程式的掃描器功能表上。 停用該設定或未設定該設定時，掃描器重新導向將運作且掃描器會顯示在掃描器功能表中。
Force the TWAIN Scanning Properties dialog		X	此設定啟用時，[TWAIN 掃描內容] 對話方塊一律會顯示，即使掃描應用程式未顯示掃描對話方塊，也是如此。

表 2-3. 掃描器重新導向群組原則設定 (續)

設定	電腦	使用者	說明
Hide Webcam	X	X	防止網路攝影機顯示在 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊的掃描器選取功能表中。 依預設，網路攝影機可重新導向到桌面平台和應用程式。使用者可選取網路攝影機並將其用作擷取影像的虛擬掃描器。 將該設定做為「電腦組態」原則啟用時，受影響電腦的所有使用者將無法看到網路攝影機。使用者無法在 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中變更**隱藏網路攝影機**選項。 將該設定做為「使用者組態」原則啟用時，所有受影響的使用者將無法看到網路攝影機。但是，使用者可以在 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中變更**隱藏網路攝影機**選項。 在「電腦組態」和「使用者組態」中同時啟用該設定時，「電腦組態」中的**隱藏網路攝影機**設定將針對受影響電腦之所有使用者覆寫「使用者組態」中的對應原則設定。 在任一原則組態中停用該設定或未設定該設定時，**隱藏網路攝影機**設定由對應的原則設定 (「使用者組態」或「電腦組態」) 或 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中的使用者選取決定。
Lock config	X		鎖定掃描器重新導向使用者介面，防止使用者變更其桌面平台和應用程式中的組態選項。 啟用該設定時，使用者無法設定其桌面平台和應用程式的 [系統匣] 功能表中的可用選項。使用者可顯示 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊，但選項已停用且無法變更。 停用該設定或未設定該設定時，使用者可在 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中設定選項。
TWAIN Scanner Properties dialog location		X	指定 [TWAIN 掃描內容] 對話方塊的顯示位置。您可選取下列其中一個選項： ■ **代理程式** - 在代理程式端上顯示 [VMware 掃描器內容] 對話方塊。 ■ **用戶端** - 在用戶端上顯示原生的廠商掃描器 TWAIN 對話方塊。(Linux 用戶端不支援此選項。)

設定序列埠重新導向

藉由序列埠重新導向，使用者可以連接本機連接的序列 (COM) 連接埠 (例如內建 RS232 連接埠或 USB 轉序列介面卡)。印表機、條碼讀取器及其他序列裝置之類的裝置可連接到這些連接埠，並且在遠端桌面平台和已發佈應用程式中使用。

您安裝 Horizon Agent 並設定序列埠重新導向功能後，不需要再進行組態即可在遠端桌面平台和已發佈應用程式中使用該功能。例如，本機用戶端系統上的 COM1 將在遠端桌面平台重新導向為 COM1，COM2 將重新導向為 COM2，除非遠端桌面平台已經有 COM 連接埠。若是如此，將對應 COM 連接埠以避免衝突。例如，如果遠端桌面平台已經有 COM1 及 COM2，用戶端的 COM1 將預設對應至 COM3。您不需要設定 COM 連接埠，也不需要在遠端桌面平台安裝裝置驅動程式。

若要啟動重新導向的 COM 連接埠，使用者可以在桌面平台工作階段期間從序列連接埠工具的功能表選取**連線**選項。使用者也可以設定 COM 連接埠裝置在使用者連線至遠端桌面平台或已發佈應用程式時自動連線。請參閱序列埠重新導向的使用者作業。

您可以設定群組原則設定來變更預設設定。例如，您可以鎖定設定，讓使用者無法變更 COM 連接埠對應或屬性。您也可以設定原則來一起停用或啟用功能。使用 ADMX 範本檔，您可以在 Active Directory 或個別的機器上安裝序列埠重新導向群組原則設定。請參閱設定序列埠重新導向群組原則設定。

在遠端桌面平台或已發佈應用程式開啟並使用重新導向的 COM 連接埠時，您無法存取本機電腦的連接埠。另一方面，在本機電腦使用 COM 連接埠時，您無法存取遠端桌面平台或已發佈應用程式上的連接埠。

序列埠重新導向的系統需求

透過序列埠重新導向功能，使用者可以將本機連接的序列 (COM) 埠 (例如內建 RS232 連接埠或 USB 轉序列介面卡) 重新導向至其遠端桌面平台和已發佈的應用程式。若要支援序列埠重新導向，您的 Horizon 部署必須符合特定軟體和硬體需求。

虛擬桌面平台

虛擬桌面平台 (單一工作階段虛擬機器) 必須安裝 View Agent 6.2.x 或更新版本，或 Horizon Agent 7.0 或更新版本，並選取序列埠重新導向安裝選項。此安裝選項預設為取消選取狀態。

虛擬桌面平台支援下列作業系統。

- 32 位元或 64 位元的 Windows 7
- 32 位元或 64 位元的 Windows 8.x
- 32 位元或 64 位元的 Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

在虛擬桌面平台中不需要安裝序列埠裝置驅動程式。

已發佈的桌面平台和已發佈的應用程式

RDS 主機必須選取序列埠重新導向安裝選項，並安裝 Horizon Agent 7.6 或更新版本。此安裝選項預設為取消選取狀態。

已發佈的桌面平台和已發佈的應用程式支援下列作業系統。

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

在 RDS 主機中不需要安裝序列埠裝置驅動程式。

Horizon Client 電腦或用戶端存取裝置	Windows 7、Windows 8.x 和 Windows 10 用戶端系統支援序列埠重新導向。必須安裝任何必要的序列埠裝置驅動程式，且序列埠必須可供使用。序列埠重新導向適用於 Windows 版 Horizon Client 3.4 及更新版本。
顯示通訊協定	■ PCoIP ■ VMware Blast (需要 Horizon Agent 7.0 或更新版本) RDP 桌面平台工作階段不支援序列埠重新導向。

序列埠重新導向的使用者作業

使用者可以操作連接到用戶端電腦的實體 COM 連接埠裝置，並使用序列連接埠虛擬化，將裝置連線至第三方應用程式可存取裝置的遠端桌面平台。

- 使用 Horizon Agent 安裝 [序列埠重新導向] 選項後，序列埠工具匣圖示 ( ) 便會新增到遠端桌面平台。針對已發佈的應用程式，其圖示會重新導向至本機用戶端電腦。

  只有在您使用所需的 Horizon Agent 及 Windows 版 Horizon Client，而且透過 PCoIP 連接時，圖示才會出現。如果您從 Mac、Linux 或行動用戶端連線至遠端桌面平台時，圖示不會出現。

  您可以圖示設定連線、中斷連線及自訂對應的 COM 連接埠所用的選項。
- 按一下序列連接埠圖示，會顯示 **VMware Horizon 的序列 COM 重新導向**功能表。
- 依預設，本機連線的 COM 連接埠將對應到遠端桌面平台的相對應 COM 連接埠。例如：**COM1 對應於 COM3**。對應的連接埠預設為未連線。
- 使用對應的 COM 連接埠時，您必須手動選取 **VMware Horizon 的序列 COM 重新導向**功能表中的**連線**選項，或者必須在上一個桌面工作階段期間或設定群組原則設定來設定**自動連線**選項。**自動連線**會設定對應的連接埠在遠端桌面工作階段啟動時自動連線。
- 您選取**連線**選項時，重新導向的連接埠將啟動。在遠端桌面的客體作業系統中出現的裝置管理員中，重新導向的連接埠將顯示為 **VMware Horizon 的序列埠重新導向 (COM*n*)**。

  連接 COM 連接埠時，您可以在第三方應用程式中開啟該連接埠，如此即可與連線至用戶端機器的 COM 連接埠裝置交換資料。在應用程式中開啟連接埠時，您無法在 **VMware Horizon 的序列 COM 重新導向**功能表中斷連接埠的連線。

  您中斷 COM 連接埠的連線前，必須先在應用程式中關閉連接埠或關閉應用程式。之後，您可以選取**中斷連線**選項來中斷連接埠的連線，並設定用戶端機器上的實體 COM 連接埠可供使用。
- 在 **VMware Horizon 的序列 COM 重新導向**功能表中，您能夠以滑鼠右鍵按一下重新導向的連接埠，以選取**連接埠屬性**命令。

  在 [COM 屬性] 對話方塊中，您可以設定連接埠在遠端桌面工作階段啟動時自動連線、忽略資料集備妥 (DSR) 訊號、讓連接埠成為永久連接埠，並選取**自訂連接埠名稱**下拉式功能表中的連接埠，將用戶端上的本機連接埠對應於遠端桌面平台的不同 COM 連接埠。

遠端桌面平台連接埠可能會顯示為重疊。例如，您可能會看見 **COM1 (重疊)**。在此情況下，將使用 ESXi 主機的虛擬硬體中出現的 COM 連接埠設定虛擬機器。即使重新導向的連接埠對應到虛擬機器上重疊的連接埠，您仍然可以使用重新導向的連接埠。虛擬機器將透過連接埠接收來自 ESXi 主機或用戶端系統的資料。

- 在客體作業系統的裝置管理員中，您可以使用**內容 > 連接埠設定**索引標籤設定重新導向的 COM 連接埠所用的設定。例如，您可以設定預設傳輸速率及資料位元。不過，如果應用程式指定連接埠設定，則將忽略您在裝置管理員中的設定。

如需操作重新導向的序列 COM 連接埠相關的使用者指示，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。

設定序列埠重新導向的準則

透過群組原則設定，您可以設定序列埠重新導向，並控制使用者能夠對於重新導向的 COM 連接埠進行自訂的程度。您的選擇將取決於組織中的使用者角色及第三方應用程式。

如需群組原則設定的相關資訊，請參閱序列埠重新導向群組原則設定。

- 如果使用者執行相同的第三方應用程式及 COM 連接埠裝置，請確定以相同的方式設定重新導向的連接埠。例如，在使用銷售點裝置的銀行或零售商店中，確定所有 COM 連接埠裝置均連接到用戶端終端的相同連接埠，而且所有連接埠均對應到遠端桌面平台上相同的重新導向 COM 連接埠。

  進行 **PortSettings** 原則設定，將用戶端連接埠對應到重新導向的連接埠。選取 **PortSettings** 中的 **Autoconnect** 項目，確定每個桌面平台工作階段開始時均已連接重新導向的連接埠。啟用 **Lock Configuration** 原則設定，避免使用者變更連接埠對應或自訂連接埠組態。在此情況下，使用者不需要手動進行連線或中斷連線，而且不會不慎造成重新導向的 COM 連接埠無法供第三方應用程式存取。

- 如果使用者是使用各種第三方應用程式的知識工作者，而且可能使用本身用戶端機器的本機 COM 連接埠，請確定使用者可以從重新導向的 COM 連接埠連線和中斷連線。

  如果預設連接埠對應不正確，您可以進行 **PortSettings** 原則設定。您也可以選擇是否設定 **Autoconnect** 項目，端視使用者的需求而定。請勿啟用 **Lock Configuration** 原則設定。

- 確定第三方應用程式開啟對應到遠端桌面平台的 COM 連接埠。
- 確定裝置所用的傳輸速率符合第三方應用程式嘗試使用的傳輸速率。
- 您最多可以從用戶端系統重新導向 5 個 COM 連接埠到遠端桌面。

設定序列埠重新導向群組原則設定

您可以設定控制遠端工作階段中序列埠重新導向行為的群組原則設定。透過這些原則設定，您可以從 Active Directory 集中控制遠端桌面平台之 **VMware Horizon 的序列 COM 重新導向**功能表中提供的選項。

您不需設定這些原則設定。序列埠重新導向與遠端工作階段和用戶端系統中對於重新導向的 COM 連接埠設定的預設設定搭配使用。

這些原則設定會影響遠端工作階段，而不是與實體 COM 連接埠裝置連線的用戶端系統。若要針對遠端桌面平台和已發佈的應用程式進行這些設定，請在 Active Directory 中新增序列埠重新導向群組原則系統管理範本 (ADMX) 檔案。

在 Active Directory 中新增序列埠重新導向 ADMX 範本

您可以將序列 COM (序列埠重新導向) ADMX 檔案 (`vdm_agent_serialport.admx`) 中的原則設定新增至 Active Directory 中的群組原則物件 (GPO)，並在群組原則物件編輯器中進行設定。

必要條件

- 確認已在虛擬桌面平台或 RDS 主機上安裝序列埠重新導向設定選項。如果未安裝序列埠重新導向，則群組原則設定沒有任何作用。如需安裝 Horizon Agent 的相關資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》或《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件。
- 確認已為序列埠重新導向群組原則設定建立 Active Directory GPO。GPO 必須連結至包含虛擬桌面平台或 RDS 主機的 OU。請參閱 Active Directory 群組原則範例。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。
- 請熟悉序列埠重新導向群組原則設定。請參閱序列埠重新導向群組原則設定。

程序

1 從 VMware 下載網站下載 Horizon 7 GPO 服務包 `.zip` 檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在「桌面平台及使用者運算」下，選取 VMware Horizon 7 下載，其中包含 GPO 服務包。

該檔案名為 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`，其中 *x.x.x* 為版本，而 *yyyyyyy* 為組建編號。為 Horizon 7 提供群組原則設定的所有 ADMX 檔案皆可從此檔案取得。

2 解壓縮 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` 檔案，並將 ADMX 檔案複製到您的 Active Directory 伺服器。

a 將 `vdm_agent_serialport.admx` 檔案和 `en-US` 資料夾複製到 Active Directory 伺服器上的 `C:\Windows\PolicyDefinitions` 資料夾。

b (選擇性) 將語言資源檔案 (`vdm_agent_serialport.adml`) 複製到 Active Directory 伺服器上 `C:\Windows\PolicyDefinitions\` 下的適當子資料夾中。

3 在 Active Directory 伺服器上開啟群組原則管理編輯器，然後在編輯器中輸入範本檔的路徑。

這些設定位於**電腦設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > 序列 COM** 資料夾中。

大部分的設定也會新增至**使用者設定**資料夾，這些設定位於**使用者設定 > 原則 > 系統管理範本 > VMware View Agent 組態 > 序列 COM** 中。

後續步驟

設定群組原則設定。

序列埠重新導向群組原則設定

序列埠重新導向群組原則設定可控制重新導向的 COM 連接埠組態，包括遠端桌面平台之 **VMware Horizon 的序列 COM 重新導向**功能表中提供的選項。

序列埠重新導向 ADMX 檔案包含「電腦組態」與「使用者組態」原則。「使用者組態」原則能夠讓您對於指定的遠端桌面平台使用者設定不同的組態。在「電腦組態」中設定的原則設定優先於在「使用者組態」中設定的相對應設定。

表 2-4. 序列埠原則設定

設定	電腦	使用者	說明
PortSettings1 PortSettings2 PortSettings3 PortSettings4 PortSettings5	X	X	連接埠設定會決定用戶端系統的 COM 連接埠與遠端桌面平台的重新導向 COM 連接埠之間的對應，並決定影響重新導向 COM 連接埠的其他設定。您可以個別設定各個重新導向的 COM 連接埠。 有五個「連接埠設定」原則設定可供使用，因此最多可以有五個 COM 連接埠從用戶端對應至遠端桌面平台。請為您想要設定的各個 COM 連接埠，分別選取一個「連接埠設定」原則設定。啟用「連接埠設定」原則設定時，您可以設定下列會對重新導向的 COM 連接埠產生影響的項目： ■ **來源連接埠號碼**設定會指定連線到用戶端系統的實體 COM 連接埠號碼。 ■ **目的地虛擬連接埠號碼**設定會指定遠端桌面平台的重新導向虛擬 COM 連接埠號碼。 ■ **自動連線**設定會在各個桌面平台工作階段開始時自動將 COM 連接埠連線到重新導向的 COM 連接埠。 ■ 藉由 **IgnoreDSR** 設定，重新導向的 COM 連接埠裝置將忽略資料集備妥 (DSR) 訊號。 ■ **關閉連接埠前暫停 (毫秒數)** 設定會指定使用者關閉重新導向的連接埠之後連接埠實際關閉之前須等待的時間 (毫秒數)。某些 USB 轉序列介面卡需要延遲，才能確保傳輸的資料獲得保留。此設定適用於疑難排解的用途。 ■ **Serial2USBModeChangeEnabled** 設定可解決使用 Prolific 晶片組的 USB 轉序列介面卡的問題，包括 GlobalSat BU353 GPS 介面卡。如果您不針對 Prolific 晶片組介面卡啟用此設定，連線的裝置只能傳輸資料，而無法接收資料。 ■ **停用等候遮罩的錯誤**設定會停用 COM 連接埠遮罩中的錯誤值。某些應用程式需要此疑難排解設定。如需詳細資料，請參閱 Microsoft 的 WaitCommEvent 功能文件，網址為 http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx`WaitCommEvent`。 ■ **HandleBtDisappear** 設定可支援 BlueTooth COM 連接埠行為。此設定適用於疑難排解的用途。 ■ **UsbToComTroubleShooting** 設定可解決 USB 轉序列連接埠介面卡的一些問題。此設定適用於疑難排解的用途。 ■ **永久**設定會將重新導向的 COM 連接埠狀態保持在遠端工作階段中，即便用戶端中斷連線仍是如此。 為特定 COM 連接埠啟用「連接埠設定」原則設定時，使用者可以連線重新導向的連接埠及中斷其連線，但使用者無法在遠端桌面平台上設定連接埠的內容。例如，使用者無法設定在使用者登入桌面平台時自動重新導向連接埠，而且無法忽略 DSR 訊號。這些屬性由群組原則設定控制。 **備註** 只有在本機將實體 COM 連接埠連接到用戶端系統時，才能連接和啟動重新導向的 COM 連接埠。如果您對應用戶端不存在的 COM 連接埠，重新導向的連接埠將在遠端桌面平台的工具匣功能表顯示為停用，而且無法使用。 停用或未設定「連接埠設定」原則設定時，重新導向的 COM 連接埠將使用由使用者在遠端桌面平台上進行的設定。**VMware Horizon 的序列 COM 重新導向**功能表選項將啟用，而且可供使用者使用。 這些設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 序列 COM > PortSettings** 資料夾中。
Bandwidth limit	X		設定重新導向的序列連接埠與用戶端系統之間的資料傳輸速度限制 (以 KBps 為單位)。

表 2-4. 序列埠原則設定 (續)

設定	電腦	使用者	說明
			您啟用此設定時，可以在 **頻寬限制 (以 KBps 為單位)** 方塊中設定值，決定重新導向的序列連接埠與用戶端之間的資料傳輸速度上限。值 0 將停用頻寬限制。 停用此設定時，不會設定任何頻寬限制。 未設定此設定時，遠端桌面平台的本機程式設定將決定是否設定頻寬限制。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 序列 COM** 資料夾中。
`Disable functionality`	X		停用序列埠重新導向功能。 您啟用此設定時，COM 連接埠不會重新導向至遠端桌面平台。遠端桌面平台的序列連接埠工具匣圖示不會顯示。 停用此設定時，序列埠重新導向將產生作用，序列連接埠工具匣圖示將顯示，而且 COM 連接埠將出現在 **VMware Horizon 的序列 COM 重新導向**功能表。 未設定此設定時，遠端桌面平台的本機設定將決定序列埠重新導向為停用或啟用。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 序列 COM** 資料夾中。
`Local settings priority`	X	X	對於在遠端桌面平台設定的設定賦予優先順序。 您啟用此原則時，使用者在遠端桌面平台設定的序列埠重新導向設定將優先於群組原則設定。只有在遠端桌面平台未設定任何設定時，群組原則設定才會生效。 停用或未設定此設定時，群組原則設定將優先於在遠端桌面平台設定的設定。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 序列 COM** 資料夾中。
`Lock configuration`	X	X	鎖定序列埠重新導向使用者介面，並避免使用者變更遠端桌面平台的組態選項。 啟用該設定時，使用者無法設定其桌面平台的 [工具匣] 功能表中的可用選項。使用者可以顯示 **VMware Horizon 的序列 COM 重新導向**功能表，但是選項將停用，而且無法加以變更。 停用此設定時，使用者可以設定 **VMware Horizon 的序列 COM 重新導向**功能表中的選項。 未設定此設定時，遠端桌面平台的本機程式設定將決定使用者能否設定 COM 連接埠重新導向設定。 此設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 序列 COM** 資料夾中。
`COM Port Isolation Mode`			指定 COM 連接埠的隔離模式。如果啟用此設定，可以選取下列其中一個隔離模式： ■ **完全隔離 -** 虛擬序列埠僅在使用者工作階段內可看見且可供存取。COM 連接埠名稱可以在不同的使用者工作階段中具有相同的名稱。系統服務 (如 `spoolsrv.exe`) 無法在此模式中存取隔離的序列埠。 ■ **隔離已停用 -** 虛擬序列埠在全域範圍內可見。任何連接埠皆可從任何工作階段存取。由於連接埠無法在不同使用者工作階段中具有相同的名稱，因此每個使用者的連接埠名稱必須是唯一的。系統服務 (如 `spoolsrv.exe`) 可以存取任何序列埠。 如果未設定此設定，則序列埠重新導向會在**完全隔離**模式中運作。

設定 USB 轉序列介面卡

您可以設定使用 Prolific 晶片組的 USB 轉序列介面卡由序列埠重新導向功能重新導向至遠端工作階段。

若要確定 Prolific 晶片組介面卡確實傳輸資料，您可以在 Active Directory 或個別虛擬機器桌面平台或 RDS 主機上啟用序列埠重新導向群組原則設定。

如果您不設定群組原則設定來解決 Prolific 晶片組介面卡的問題，連線的裝置只能傳輸資料，而無法接收資料。

您不需要在用戶端系統設定原則設定或登錄機碼。

必要條件

- 確認已在虛擬機器桌面平台或 RDS 主機上安裝序列埠重新導向設定選項。如果未安裝序列埠重新導向，則群組原則設定沒有任何作用。如需安裝 Horizon Agent 的相關資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》或《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件。
- 確認已在 Active Directory 中新增序列埠重新導向 ADMX 範本檔。
- 熟悉 **PortSettings** 群組原則設定中的 **Serial2USBModeChangeEnabled** 項目。請參閱序列埠重新導向群組原則設定。

程序

1. 在 Active Directory 伺服器上，開啟群組原則管理物件編輯器。
2. 導覽至**電腦組態 > 原則 > 系統管理範本 > VMware View Agent 組態 > 序列 COM** 資料夾。
3. 選取 **PortSettings** 資料夾。
4. 選取並啟用 **PortSettings** 群組原則設定。
5. 指定來源及目的地 COM 連接埠號碼來對應 COM 連接埠。
6. 選取 **Serial2USBModeChangeEnabled** 核取方塊。
7. 視需要設定 **PortSettings** 原則設定中的其他項目。
8. 按一下**確定**並關閉群組原則管理物件編輯器。

使用者開始其後續的工作階段時，USB 轉序列介面卡可重新導向至遠端工作階段，而且可成功接收資料。

管理 Windows Media 多媒體重新導向 (MMR) 的存取權

Horizon 7 為單一使用者機器上所執行虛擬桌面平台和 RDS 主機上已發佈桌面平台提供 Windows Media MMR 功能。

MMR 直接傳遞多媒體串流到用戶端電腦。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。

依據重新導向的內容，可能包含敏感資料的 MMR 資料會在網路傳送，而且未進行應用程式級的加密。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。

如果安全通道已啟用，則用戶端與 View 安全閘道之間的 MMR 連線安全無虞，不過從 View 安全閘道到桌面平台機器的連線不會加密。如果安全通道已停用，則從用戶端到桌面平台機器的 MMR 連線不會加密。

啟用 Horizon 7 中的多媒體重新導向

您可以採取適當步驟，確保僅有足夠資源處理本機多媒體解碼且在安全網路上連接到 Horizon 7 的 Horizon Client 系統可使用 MMR。

依預設，Horizon Administrator 中的全域原則，**多媒體重新導向 (MMR)** 設定為**拒絕**。

若要使用 MMR，您必須將此值明確設定為**允許**。

若要控制 MMR 的存取，您可對個別桌面平台集區或特定使用者，全域啟用或停用**多媒體重新導向 (MMR)** 原則。

如需在 Horizon Administrator 中設定全域原則的指示，請參閱 Horizon 7 原則。

Windows Media MMR 的系統需求

若要支援 Windows Media 多媒體重新導向 (MMR)，您的 Horizon 7 部署必須符合特定軟體和硬體需求。Horizon 6.0.2 及更新版本中提供了 Windows Media MMR。

遠端桌面平台

- 部署於單一使用者虛擬機器及 RDS 主機上已發佈桌面平台的虛擬機器桌面平台支援此功能。

  需要 View Agent 6.1.1 或更新版本，或是 Horizon Agent 7.0 或更新版本，才能在已發佈的桌面平台上支援此功能。

  需要 View Agent 6.0.2 或更新版本，或是 Horizon Agent 7.0 或更新版本，才能在單一使用者機器上支援此功能。
- 必須具備 Horizon 7 (7.9 版) 或更新版本，才可支援 Microsoft 媒體伺服器 (MMS) 和即時串流通訊協定 (RTSP)。
- 支援下列客體作業系統：
  - 64 位元或 32 位元的 Windows 10。支援 Windows Media Player。不支援預設播放程式「電影與電視」。
  - Windows Server 2016 為一項技術預覽功能。支援 Windows Media Player。不支援預設播放程式「電影與電視」。
  - 64 位元或 32 位元 Windows 7 SP1 Enterprise 或 Ultimate (單一使用者機器)。不支援 Windows 7 Professional。
  - 64 位元或 32 位元 Windows 8/8.1 Professional 或 Enterprise (單一使用者機器)
  - 設定為 RDS 主機的 Windows Server 2008 R2
  - 設定為 RDS 主機的 Windows Server 2012 及 2012 R2
- 可在桌面平台集區上啟用或停用 **3D 呈現**。

	■ 使用者必須在 Windows Media Player 12 或更新版本，或者在 Internet Explorer 8 或更新版本中播放視訊。
Horizon Client 軟體	需要 Horizon Client 3.2 Windows 版或更新版本才能在單一使用者機器支援 Windows Media MMR。
Horizon Client 電腦或用戶端存取裝置	用戶端必須執行 64 位元或 32 位元 Windows 7、Windows 8/8.1 或 Windows 10 作業系統。
支援的媒體格式	Windows Media Player 支援的媒體格式，例如：M4V；MOV；MP4；WMP；MPEG-4 Part 2；WMV 7、8 和 9；WMA；AVI；ACE；MP3；WAV。 Horizon 7 (7.9 版) 及更新版本支援 MMS 和 RTSP。 使用 MMS 與 RTSP 時不支援 MP3。 **備註** DRM 受保護的內容不會透過 Windows Media MMR 重新導向。
Horizon 原則	在 Horizon Administrator 中，將**多媒體重新導向 (MMR)** 原則設定為**允許**。預設值為**拒絕**。
後端防火牆	如果您的 Horizon 7 部署包含 DMZ 安全伺服器和內部網路間的後端防火牆，確認後端防火牆是否允許桌面平台上至 9427 連接埠的通訊。

根據網路延遲使用 Windows Media MMR

依預設，Windows Media MMR 會按照 Windows 8 或更新版本上執行的單一使用者桌面平台或 Windows Server 2012 或 2012 R2 或更新版本上執行的已發佈桌面平台的網路情況進行調整。如果 Horizon Client 和遠端桌面平台之間的網路延遲為 29 毫秒或以下，則會透過 Windows Media MMR 重新導向視訊。如果網路延遲為 30 毫秒或以上，則不會重新導向視訊。相反地，會在 ESXi 主機上轉譯並透過 PCoIP 傳送至用戶端。

此功能適用於 Windows 8 或更新版本單一使用者桌面平台及 Windows Server 2012 或 2012 R2 或更新版本已發佈桌面平台。使用者可以執行任何支援的用戶端系統，Windows 7 或 Windows 8/8.1。

此功能不適用於 Windows 7 單一使用者桌面平台或 Windows Server 2008 R2 已發佈桌面平台。在這些客體作業系統上，無論網路延遲如何，Windows Media MMR 都會執行多媒體重新導向。

您可以覆寫此功能，強制 Windows Media MMR 執行多媒體重新導向 (無論網路延遲如何)，其方法是在桌面平台上設定 `RedirectionPolicy` 登錄設定。

程序

1 在遠端桌面平台上啟動 Windows 登錄編輯程式。

2 導覽至控制重新導向原則的 Windows 登錄機碼。

您為遠端桌面平台設定的登錄機碼取決於 Windows Media Player 的位元版本。

選項	說明
64 位元 Windows Media Player	■ 若為 64 位元桌面平台，請使用登錄機碼：`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr`
32 位元 Windows Media Player	■ 若為 32 位元桌面平台，請使用登錄機碼：`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr` ■ 若為 64 位元桌面平台，請使用登錄機碼：`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware tsmmr`

3 將 `RedirectionPolicy` 值設為 `always`。

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

4 重新啟動桌面平台上的 Windows Media Player 以允許更新的值生效。

管理用戶端磁碟機重新導向的存取

當您部署具有用戶端磁碟機重新導向功能的 Horizon Client 和 Horizon Agent 時，資料夾和檔案會以加密形式透過網路傳送。

用戶端和 View 安全閘道之間的用戶端磁碟機重新導向連線，以及 View 安全閘道至桌面平台機器的連線皆安全無虞。如果啟用了 VMware Blast，則會以加密形式透過虛擬通道傳輸檔案和資料夾。

需要 9427 連接埠上的 TCP 連線，才能支援用戶端磁碟機重新導向。如果您的 Horizon 7 部署在 DMZ 型安全伺服器與內部網路之間有後端防火牆，該後端防火牆必須允許流量進入遠端桌面平台上的連接埠 9427。如果啟用了 VMware Blast，則不需要開啟 TCP 連接埠 9427，因為用戶端磁碟機重新導向會透過虛擬通道進行資料傳輸。

依預設會選取 Horizon Agent 安裝程式中的**用戶端磁碟機重新導向**自訂安裝選項。最佳做法是，在使用者需要**用戶端磁碟機重新導向**功能的遠端桌面平台上，才啟用此自訂安裝選項。

使用早於 3.5 版的 Horizon Client 版本，或早於 6.2 版的 Horizon Agent 版本時，用戶端磁碟機重新導向資料夾和檔案會以未加密的形式透過網路傳送，且可能包含敏感資料，視重新導向的內容而定。如果已啟用安全通道，Horizon Client 與 View 安全閘道之間的用戶端磁碟機重新導向連線安全無虞，不過從 View 安全閘道至桌面平台機器的連線不會予以加密。如果停用安全通道，從 Horizon Client 到桌面平台機器的用戶端磁碟機重新導向連線不會予以加密。對於較早版本的用戶端和代理程式，請僅在安全網路上使用用戶端磁碟機重新導向，以確保該資料不會在網路上遭到監控。

在 Horizon Agent 7.7 或更新版本上啟用用戶端磁碟機重新導向之後，您可以在 Horizon Client 4.10 或更新版本和遠端桌面平台與已發佈的應用程式之間拖放檔案和資料夾。請參閱設定拖放功能。

在 Unified Access Gateway 實作中使用用戶端磁碟機重新導向

如果您的 Horizon 7 實作使用 Unified Access Gateway 應用裝置而非安全伺服器，而使用者使用用戶端磁碟機重新導向搭配 PCoIP 顯示通訊協定，且 Horizon Client 和 Horizon Agent 機器位於不同網路上，則必須為 Unified Access Gateway 應用裝置啟用 UDP 通道伺服器。

若要啟用 UDP 通道伺服器，請在 Unified Access Gateway 管理員 UI 中，將 **UDP 通道伺服器已啟用**設定設為**是**。

如果您並未啟用 UDP 通道伺服器，則使用者無法使用用戶端磁碟機重新導向功能搭配 PCoIP 顯示通訊協定。無論是否已啟用 UDP 通道伺服器，用戶端磁碟機重新導向可與 VMware Blast 顯示通訊協定搭配使用。

如需詳細資訊，請參閱 Unified Access Gateway 說明文件。

使用群組原則來停用用戶端磁碟機重新導向

您可以在 Active Directory 伺服器上設定遠端桌面平台的群組原則設定，以停用用戶端磁碟機重新導向。

此群組原則設定會覆寫啟用用戶端磁碟機重新導向功能的本機登錄和智慧原則設定。

必要條件

- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。
- 將遠端桌面服務 ADMX 範本檔 `vmware_rdsh_server.admx` 新增至與您虛擬桌面平台的 OU 連結的 GPO，或新增至與已發佈桌面平台的 RDS 主機連結的 GPO。如需安裝指示，請參閱將 ADMX 範本檔新增至 Active Directory。

程序

1. 在您的 Active Directory 伺服器上開啟群組原則管理編輯器，並導覽至**電腦設定\原則\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\裝置及資源重新導向**。
2. 開啟**不允許磁碟重新導向**群組原則設定、選取**已啟用**，然後按一下**確定**。

使用群組原則來設定磁碟機代號行為

您可以使用代理程式群組原則設定，為使用用戶端磁碟機重新導向功能重新導向的磁碟機設定磁碟機代號行為。

必要條件

- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。
- 將 VMware Horizon 用戶端磁碟機重新導向 ADMX 範本檔 (`vdm_agent_cdr.admx`) 新增至與您虛擬桌面平台的 OU 連結的 GPO，或新增至與已發佈桌面平台的 RDS 主機連結的 GPO。如需安裝指示，請參閱將 ADMX 範本檔新增至 Active Directory。

程序

1 在您的 Active Directory 伺服器上開啟群組原則管理編輯器，並導覽至**電腦設定 > 系統管理範本 > VMware View Agent 組態 > VMware Horizon 用戶端磁碟機重新導向**。

2 若要設定是否為重新導向的磁碟機顯示磁碟機代號，請設定**顯示含有磁碟機代號的重新導向裝置**群組原則設定。

此設定依預設為啟用。

3 若要針對重新導向的磁碟機指定等待 Windows 檔案總管初始化並顯示磁碟機代號的時間長度 (以毫秒為單位)，請設定**磁碟機代號組態的逾時**群組原則設定。

停用或未設定此設定時，預設值為 5000 毫秒。

4 若要設定磁碟機代號對應模式，請設定**設定磁碟機代號對應模式**群組原則設定。

您可選取下列其中一個選項。

選項	敘述
一對一對應	將用戶端機器上的磁碟機代號對應至代理程式機器上的相同磁碟機代號。例如，用戶端機器上的磁碟機 X 會對應至代理程式機器上的磁碟機 X。
定義的對應	根據在**定義磁碟機代號對應表**群組原則設定中定義的對應表，將用戶端機器上的磁碟機代號對應至代理程式機器上的特定磁碟機代號。

5 若要對應磁碟機代號，請設定**定義磁碟機代號對應表**群組原則設定。

您可以按一下**顯示**以定義磁碟機代號對應表。**值名稱**欄指定用戶端機器上的磁碟機代號，而對應的**值**欄指定要在代理程式機器上使用的磁碟機代號。

使用登錄設定來設定用戶端磁碟機重新導向

您可使用 Windows 登錄機碼設定來控制遠端桌面平台上的用戶端磁碟機重新導向行為。此功能需要 Horizon Agent 7.0 或更新版本，以及 Horizon Client 4.0 或更新版本。

控制遠端桌面平台上之用戶端磁碟機重新導向行為的 Windows 登錄設定位於下列路徑：

```
HKLM\Software\VMware, Inc.\VMware TSDR
```

您可使用遠端桌面平台上的 Windows 登錄編輯程式來編輯本機登錄設定。

備註 使用智慧原則設定的用戶端磁碟機重新導向原則將優先於本機登錄設定。

停用用戶端磁碟機重新導向

若要停用用戶端磁碟機重新導向，請建立名為 `disabled` 的新字串值並將其值設為 `true`。

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

此值預設為 `false` (啟用)。

防止對共用資料夾的寫入權限

若要防止對與遠端桌面平台共用之所有資料夾的寫入權限，請建立名為 `permissions` 的新字串值，並將其值設為以 `r` 開頭，但 `rw` 除外的任何字串。

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

此值預設為 `rw` (所有共用資料夾皆可讀取也可寫入)。

共用特定的資料夾

若要與遠端桌面平台共用特定的資料夾，請建立名為 `default shares` 的新機碼，並為每個要與遠端桌面平台共用的資料夾各建立一個新的子機碼。對於每個子機碼，建立名為 `name` 的新字串值，並將其值設為要共用之資料夾的路徑。下列範例會共用資料夾 `C:\ebooks` 和 `C:\spreadsheets`。

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

如果將 `name` 設定為 `*all`，則所有用戶端磁碟機都會與遠端桌面平台共用。只有 Windows 用戶端系統才支援 `*all` 設定。

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

若要防止用戶端共用其他資料夾 (亦即未以 `default shares` 機碼指定的資料夾)，請建立名為 `ForcedByAdmin` 的字串值，並將其值設為 `true`。

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

值是 `true` 時，當使用者連線至 Horizon Client 中的遠端桌面平台，[共用] 對話方塊不會顯示出來。此值預設為 `false` (用戶端可以共用其他資料夾)。

下列範例會共用資料夾 `C:\ebooks` 和 `C:\spreadsheets`、將這兩個資料夾設為唯讀，並防止用戶端共用其他資料夾。

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

備註 請不要以 `ForcedByAdmin` 功能作為安全功能或共用控制。使用者可建立現有共用的連結，並使其指向並非以 `default shares` 機碼指定的資料夾，藉以規避 `ForcedByAdmin=true` 設定。

設定拖放功能

使用者可以在用戶端系統與遠端桌面平台和已發佈的應用程式之間拖放資料。

拖放的用戶端需求

- 僅支援 Windows 用戶端和 Mac 用戶端系統。不支援其他類型的用戶端系統。

- 使用者必須使用 VMware Blast 或 PCoIP 顯示通訊協定。
- 若要拖放檔案和資料夾，必須在 Windows 版 Horizon Client 上啟用用戶端磁碟機重新導向功能。
- 若要使用最新的拖放功能，使用者必須擁有 Windows 版 Horizon Client (5.1 或更新版本) 或 Mac 版 Horizon Client (5.1 或更新版本)。舊版的用戶端僅提供部分拖放功能。

如需在 Windows 用戶端上使用拖放功能的相關資訊，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。如需在 Mac 用戶端上使用拖放功能的相關資訊，請參閱《Mac 版 VMware Horizon Client 安裝和設定指南》文件。

拖放的代理程式需求

若要對檔案和資料夾使用拖放功能，您必須在安裝 Horizon Agent 時啟用**用戶端磁碟機重新導向**選項。

使用群組原則設定來設定拖放

您可以藉由編輯 VMware Blast 和 PCoIP 顯示通訊協定的群組原則設定，來設定拖放方向、允許的拖放格式，以及拖放大小限制。請參閱 VMware Blast 原則設定與 PCoIP 剪貼簿和拖放設定。

使用 Dynamic Environment Manager 設定拖放

透過 Dynamic Environment Manager 9.8 或更新版本和 Horizon Client 5.1 或更新版本，您可以使用智慧原則來設定拖放行為，包括完全停用拖放功能。請參閱 Horizon 智慧型原則設定。

設定簡易裝置方向 (SDO) 感應器重新導向

簡易裝置方向 (SDO) 感應器重新導向功能可以感應用戶端裝置上螢幕方向的變更，並相應地在裝置上顯示不同視圖。

SDO 感應器重新導向會與 Horizon Agent 上的軟體應用程式整合。如果您的應用程式使用 SimpleOrientationSensor 類別 https://docs.microsoft.com/en-us/uwp/api/windows.devices.sensors.simpleorientationsensor，則應用程式可以根據用戶端裝置上目前的象限方向來顯示內容。

SDO 感應器重新導向的系統需求

支援這些裝置：

表 2-5. 支援 SDO 感應器重新導向的裝置

裝置	用戶端作業系統	Windows 作業系統伺服器	通訊協定
Surface Book	Windows 10 1709	Windows 10 1709 (64 位元、32 位元)	PCoIP、Blast
Surface Pro	Windows 10 1709 Windows 8.1	Windows 10 1709 (64 位元、32 位元)	PCoIP、Blast

對於 Horizon Agent 作業系統，僅支援 Windows 10 32 位元和 64 位元。

安裝 SDO 感應器

SDO 感應器重新導向是 Horizon Agent 安裝程式中的自訂安裝選項。依預設為未選取狀態。您必須選取 SDO 感應器重新導向來加以安裝。針對 SDO 感應器重新導向的靜默安裝內容，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件。

必須啟用本機系統上的感應器服務，SDO 驅動程式才能正常運作。必須在用戶端裝置上啟用 SDO 感應器。

記錄

SDO 感應器重新導向的 Horizon Client 記錄檔會記錄在 rdeSvc 記錄檔 `%TEMP%\vmware-%USERNAME%\vmware-rdeSvc-x-xxxxx.log` 中。

SDO 感應器重新導向的 Horizon Agent 記錄檔會記錄在 rdeSvc 記錄檔 `C:\Windows\Temp\vmware-SYSTEM*\vmware-rdeSvc-x-xxxx.log` 中。

設定工作階段協作

透過工作階段協作功能，使用者可以邀請其他使用者加入現有的 Windows 遠端桌面工作階段。若要設定 Linux 桌面平台上的工作階段協作，請參閱《設定 Horizon 7 for Linux 桌面平台》文件。

工作階段協作的系統需求

若要支援工作階段協作功能，您的 Horizon 部署必須符合特定需求。

表 2-6. 工作階段協作的系統需求

元件	需求
用戶端系統	工作階段擁有者和協作者必須已在用戶端系統上安裝 Windows、Mac 或 Linux 版 Horizon Client 4.7 或更新版本，或必須使用 HTML Access 4.7 或更新版本。
Windows 遠端桌面	必須在虛擬桌面平台或在已發佈應用程式的 RDS 主機上安裝 Horizon Agent 7.4 或更新版本。必須在桌面平台集區或伺服器陣列層級上啟用工作階段協作功能。如需為桌面平台集區啟用工作階段協作功能的相關資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件。如需為伺服器陣列啟用工作階段協作功能的相關資訊，請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件。
Linux 遠端桌面平台	如需 Linux 遠端桌面平台需求，請參閱《設定 Horizon 7 for Linux 桌面平台》文件。
連線伺服器	連線伺服器執行個體會使用 Enterprise 授權。
顯示通訊協定	VMware Blast

如需如何使用工作階段協作功能的相關資訊，請參閱 Horizon Client 說明文件。

設定工作階段協作群組原則設定

使用 VMware View Agent 組態 ADMX 範本檔 (`vdm_agent.admx`) 中的協作群組原則設定，可設定工作階段協作。請參閱工作階段協作原則設定。

工作階段協作功能限制

使用者無法在協作工作階段中使用下列遠端桌面平台功能。

- USB 重新導向
- 即時音訊視訊 (RTAV)
- 多媒體重新導向
- 用戶端磁碟機重新導向
- 智慧卡重新導向
- 虛擬列印
- Microsoft Lync 重新導向
- 檔案重新導向和保留在 Dock 中功能
- 剪貼簿重新導向

使用者無法在協作工作階段中變更遠端桌面平台的解析度。

使用者在相同的用戶端機器上不能有多個協作工作階段。

設定適用於商務用 Skype 的 VMware 虛擬化套件

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

適用於商務用 Skype 的 VMware 虛擬化套件功能

適用於商務用 Skype 的 VMware 虛擬化套件提供下列功能：

- 使用 HTTPS Proxy 伺服器執行通話和會議功能
- 回應群組
- Microsoft Office 整合：從 Word、Outlook、SharePoint 等工具啟動商務用 Skype 通話
- 「經驗品質」可讓商務用 Skype 用戶端將通話評量回報給商務用 Skype 伺服器，以產生報告
- 以委派身分代表他人管理通話
- 主動識別發話者身分
- 從 X (住家、公司等) 撥號
- 從遠端桌面平台控制音量
- 撥打 E911
- 通話駐留和接聽
- 匿名加入外部會議

- 將通話重新導向到行動裝置
- 通話統計資料
- 智慧卡驗證
- 點對點音訊通話
- 點對點視訊通話
- 使用撥號鍵台的 PSTN 通話
- 傳送、轉接、靜音、保留及繼續通話
- HID 命令
- 透過中繼伺服器的 PSTN 通話
- 透過 Edge Server 的遠端連線和通話
- 等候音樂
- 自訂鈴聲
- 語音信箱整合
- USB 電話
- 已發佈的應用程式支援
- 音訊和視訊的前饋式錯誤修正 (FEC)
- 商務用 Skype 線上會議
- 立即開會會議
- 白板和螢幕畫面分享

適用於商務用 Skype 的 VMware 虛擬化套件的系統需求

適用於商務用 Skype 的 VMware 虛擬化套件支援下列組態。

表 2-7. 適用於商務用 Skype 的 VMware 虛擬化套件系統需求

系統	需求
Microsoft 伺服器	Lync Server 2013、商務用 Skype Server 2015、Office365、商務用 Skype Server 2019
Microsoft 用戶端	VMware 強烈建議您使用最新的商務用 Skype 用戶端更新。 ■ 商務用 Skype 2015 用戶端：15.0.4933.100 或更新版本 ■ 將商務用 Skype 2016 作為 Office 365 Plus 的一部分：16.0.7571.2072 或更新版本 ■ 將商務用 Skype 2016 作為 Office 2016 的一部分：16.0.4561.1000 或更新版本 **備註** 不支援商務用 Skype Basic 2015 或 2016 用戶端。

表 2-7. 適用於商務用 Skype 的 VMware 虛擬化套件系統需求 (續)

系統	需求
虛擬桌面平台作業系統	這些作業系統的最低需求為 2 個 vCPU。 ■ Windows 7 SP1 **備註** 安裝適用於 Horizon Agent 7.10 及更新版本的 .Net 4.0 或更新版本。 ■ Windows 8.1 ■ Windows 10 持續性和非持續性桌面平台 ■ Windows 2008 R2 SP1 桌面平台 ■ Windows 2012 R2 桌面平台 ■ Windows 2008 R2 SP1 RDSH 桌面平台 ■ Windows 2012 R2 RDSH 桌面平台 ■ Windows Server 2016 RDSH 桌面平台 ■ 已發佈的應用程式支援
用戶端機器作業系統	最低硬體需求為 2.4 GHz 雙核心 ■ Windows 7 SP1 ■ Windows 8.1 ■ Windows 10 ■ Windows Embedded Standard 7 ■ Windows 10 IoT ■ Windows Thin PC 適用於商務用 Skype 的 VMware 虛擬化套件與 Linux 版 Horizon Client 支援相同的 Linux 作業系統。 適用於商務用 Skype 的 VMware 虛擬化套件與 Mac 版 Horizon Client 支援相同的 Mac 作業系統。
部署	■ VDI (內部部署和雲端) ■ 持續性和非持續性桌面平台 ■ RDS 部署 (已發佈桌面平台和應用程式)
顯示通訊協定	VMware Blast 和 PCoIP
網路連接埠	原生商務用 Skype 用戶端所使用的相同連接埠。請參閱 https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/ports-and-protocols 中的用戶端連接埠。另請參閱 https://kb.vmware.com/s/article/52558。
麥克風和網路攝影機	能夠與商務用 Skype 搭配使用的相同裝置。請參閱 https://docs.microsoft.com/en-us/SkypeForBusiness/certification/devices-usb-devices 中列出的網路攝影機。
音訊與視訊轉碼器	原生商務用 Skype 所使用的相同音訊與視訊轉碼器。請參閱 https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/network-requirements。
相容的對等商務用 Skype 用戶端 (非 VDI)	■ 具有最新更新的商務用 Skype 2016 用戶端 ■ 具有最新更新的商務用 Skype 2015 用戶端 ■ 具有最新更新的 Lync 2013 用戶端 ■ Lync 2010 用戶端 (僅限語音通話)
Media Feature Pack	必須安裝在適用於 Windows 10 N 和 KN 版本的遠端桌面平台上。您可以從 https://www.microsoft.com/en-us/download/details.aspx?id=48231 安裝媒體功能。

安裝適用於商務用 Skype 的 VMware 虛擬化套件

若要使用商務用 Skype，您的用戶端機器上必須安裝適用於商務用 Skype 的 VMware 虛擬化套件。依預設會在 Windows 版 Horizon Client (4.6 及更新版本)、Linux 版 Horizon Client (4.6 及更新版本) 以及 Mac 版 Horizon Client (4.7 及更新版本) 安裝程式的執行過程中安裝「適用於商務用 Skype 的 VMware 虛擬化套件」軟體。如需 Horizon Client 的安裝資訊，請參閱 Horizon Client 版本的安裝和設定指南。

Horizon 管理員必須在 Horizon Agent 安裝期間於虛擬桌面平台上安裝「適用於商務用 Skype 的 VMware 虛擬化套件」。如需 Horizon Agent 的安裝資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件。

適用於商務用 Skype 的 VMware 虛擬化套件包含下列軟體模組：

- 安裝在虛擬桌面平台內的 Horizon Media Proxy
- 安裝在用戶端端點上的 Horizon Media Provider。

若要檢查虛擬機器上是否已安裝適用於商務用 Skype 的 VMware 虛擬化套件，請檢查這些登錄機碼：

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Lync\VdiMediaProvider – GUID(REG_SZ)`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Lync\VdiMediaProvider – GUID(REG_SZ)`

工作階段的配對模式

Lync.exe 會在啟動時載入「適用於商務用 Skype 的 VMware 虛擬化套件」外掛程式。外掛程式會檢查是否有有效的工作階段，並在登錄中寫入配對模式狀態。若要查詢配對模式，請在處理程序清單中確認 Lync.exe 正在執行，然後檢查 `HKEY_CURRENT_USER\Software\VMware, Inc.\VMWMMAPlugin – PairingMode(REG_SZ)`。

有效的配對模式包含：

- 最佳化：一個有效的工作階段
- 後援：無有效工作階段
- 最佳化 (版本不相符)
- 後援 (版本不相符)
- 正在連線
- 已中斷連線
- 未定義

當 Lync.exe 存在時，外掛程式會從登錄刪除配對模式值。

使用者不需要管理員權限即可檢查配對模式。登入遠端桌面平台上的多個使用者可以在 HKCU 登錄區中找到每位使用者的配對模式。

設定適用於商務用 Skype 的 VMware 虛擬化套件的群組原則設定

您可以設定群組原則設定來變更預設設定。請參閱適用於商務用 Skype 的 VMware 虛擬化套件的原則設定。

適用於商務用 Skype 的 VMware 虛擬化套件限制

適用於商務用 Skype 的 VMware 虛擬化套件具有下列限制：

- 不支援 Socks 和 HTTP Proxy 伺服器。
- 適用於商務用 Skype 的 VMware 虛擬化套件解決方案不支援與第三方多方會議裝置的互通性，例如 Pexip。
- 目前不支援圖庫檢視。
- 您無法錄製通話。
- 不支援媒體旁路。如需詳細資料，請參閱 https://kb.vmware.com/s/article/56977。
- 不支援雙躍點案例，例如與 Horizon Client 形成巢狀結構的 Horizon Agent。
- 商務用 Skype VDI 最佳化解決方案與 Lync 2010 用戶端之間沒有相容的相互操作性。
- 不支援在用戶端機器上使用 Lync 或商務用 Skype 時，同時在遠端桌面平台使用最佳化商務用 Skype。
- 將 Skype 2015 用戶端連線至 Lync 2013 伺服器時，不支援 Lync 2013 用戶端 UI。管理員可以在伺服器上設定 Skype 用戶端 UI：https://social.technet.microsoft.com/wiki/contents/articles/30282.switch-between-skype-for-business-and-lync-client-ui.aspx
- 在視訊預覽視窗中，如果您想要預覽未列出的攝影機，請在選取裝置後關閉對話方塊，然後再重新開啟以進行預覽。如果您想要攝影機動態更新，請使用商務用 Skype 2016 隨選即用安裝程式版本 16.0.11001.20097 或更新版本。
- 如果您在遠端桌面平台上安裝商務用 Skype 時連線至私人網路，則安裝程式會為該網路設定檔新增輸入和輸出防火牆規則。當您從網域網路登入遠端桌面平台之後使用商務用 Skype 時，您會看見防火牆例外狀況。若要修正此問題，請在所有網路設定檔的防火牆規則中手動新增商務用 Skype 用戶端的防火牆例外狀況。

收集記錄以進行商務用 Skype 的疑難排解

若要進行商務用 Skype 的疑難排解，請從 Windows 版 Horizon Agent 和 Horizon Client 收集記錄。

程序

1. 若要從 Horizon Agent 收集 Horizon 記錄 (包括 Media Proxy 記錄)，請登入安裝了 Horizon Agent 的虛擬機器。
2. 開啟命令提示字元並執行 `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat`。
3. 若要從 Horizon Client 收集 Horizon 記錄 (包括 Media Provider 記錄)，請登入安裝了 Horizon Client 的實體或虛擬機器。
4. 開啟命令提示字元並執行 `support.bat`。
   - 32 位元：`C:\Program Files\VMware\VMware Horizon View Client\DCT\support.bat`
   - 64 位元：`C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat`

包含壓縮記錄檔且名為 vdm-sdct 的資料夾會顯示在桌面平台上，且其中包含內有「商務用 Skype 的 VMware Horizon 虛擬化套件」之記錄的目錄：

- 用戶端裝置：%TEMP%\vmware-<username>\VMWMediaProvider
- 虛擬桌面平台：
  - %TEMP%\vmware-<username>\VMWMediaProviderProxy
  - %TEMP%\vmware-<username>\VMWMediaProviderProxyLocal
  - %TEMP%\vmware-<username>\MMAPlugin

預設記錄層級為 7，在此層級中，記錄層級大小和損毀傾印較小。您可以將記錄層級增加至 8，以獲得最大的記錄和完整的損毀傾印。所有設定皆為 DWORD：

- 用戶端：HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProvider/DebugLogging/LoggingPriority = 8
- 代理程式：HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxy/DebugLogging/LoggingPriority = 8
- 代理程式：HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxyLocal/DebugLogging/LoggingPriority = 8

設定 VMware Integrated Printing 重新導向

VMware Integrated Printing 功能可讓使用者列印到其 Windows、Mac 和 Linux 用戶端電腦上任何可用的印表機。

VMware Integrated Printing 支援用戶端印表機重新導向、依據位置列印，以及持續性列印設定。

用戶端印表機重新導向

用戶端印表機重新導向可讓使用者從遠端桌面平台列印至 Windows、Mac 或 Linux 用戶端上安裝的任何本機或網路印表機。對於從 Windows 用戶端重新導向至遠端桌面平台的印表機，VMware Integrated Printing 在遠端桌面平台上支援兩種類型的印表機驅動程式：

- 原生印表機驅動程式 (NPD)。您必須在遠端桌面平台上安裝與用戶端印表機驅動程式相同的印表機驅動程式。NPD 僅支援 v3 印表機。
- 通用印表機驅動程式 (UPD)。您無需在遠端桌面平台上安裝任何驅動程式。

依預設，如果在 Horizon Agent 上安裝原生驅動程式，則會使用 NPD。否則，將使用 UPD。您可以藉由設定群組原則來選取要在遠端桌面平台上使用的印表機驅動程式類型。

若要查看遠端桌面平台中使用的印表機驅動程式類型，請前往**控制台 > 硬體和音效 > 裝置和印表機**，在虛擬印表機上按一下滑鼠右鍵，然後從快顯功能表中選取**印表機內容**。在**一般**索引標籤上，如果**型號**為 VMware 通用 EMF 驅動程式，則會使用 UPD。否則，將使用 NPD。

依據位置列印

依據位置列印功能可以將實體位置鄰近用戶端系統的印表機對應至遠端桌面平台，讓使用者能夠從其遠端桌面平台列印至網路印表機。下列遠端桌面平台和應用程式支援依據位置列印功能：

- 在單一使用者機器上部署的桌面平台，包括 Windows 桌面平台和 Windows Server 機器
- 在 RDS 主機上部署的已發佈桌面平台和已發佈應用程式，其中 RDS 主機為虛擬機器或實體機器

若要使用依據位置列印，您必須在遠端桌面平台上安裝正確的印表機驅動程式，並在 `LBP.xml` 檔案中為每個依據位置印表機定義轉譯規則。這些轉譯規則會決定印表機是否對應至特定用戶端系統的遠端桌面平台。當使用者連線至遠端桌面平台時，Horizon 7 會將用戶端系統與轉譯規則進行比較。如果用戶端系統符合所有轉譯規則，則 Horizon 7 會在使用者工作階段期間將印表機對應至遠端桌面平台。

您可以根據已登入遠端桌面平台的使用者名稱、用戶端系統的 IP 位址、主機名稱以及 MAC 位址來定義轉譯規則。您可以為特定印表機指定一個轉譯規則，或是數個轉譯規則的組合。如果在 `LBP.xml` 中將任何依據位置印表機設定為預設值，則該印表機將成為遠端桌面平台上的預設印表機，其優先於用戶端系統上的預設印表機。

若要讓規則生效，請將 `LBP.xml` 儲存到遠端桌面平台上的 `%ProgramData%\VMware`，然後重新連線至遠端桌面平台或遠端應用程式。

您可以在 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` 中找到 `LBP.xml` 的範本。請參閱 Horizon 7 ADMX 範本檔。

您可以藉由設定群組原則來停用依據位置列印。

巢狀模式重新導向

在巢狀模式設定中，您可以將第一層和第二層上安裝的本機印表機重新導向至第三層上的遠端桌面平台或遠端應用程式。根據 GPO 設定，以及是否已安裝原生列印驅動程式，第三層上的重新導向印表機可使用 UPD 或 NPD。

靜態印表機名稱

重新導向的印表機會在工作階段之間保留其具有 vdi 尾碼的名稱，以便使用者在連線至其他工作階段時，無需手動重新對應印表機。只有在單一使用者機器上才支援靜態印表機名稱，在使用 VDI 模式的 Windows Server 上不支援此名稱。

持續性列印設定

在使用者登出桌面平台或從桌面平台中斷連線後，仍會保留已重新導向用戶端印表機 (包括原生印表機驅動程式和通用印表機驅動程式) 或依據位置印表機的印表機設定。例如，使用者可能會設定已重新導向用戶端印表機或依據位置印表機為使用黑白模式。在使用者登出並再次登入桌面平台後，先前的列印設定會持續保存。

您可以藉由設定群組原則來停用持續性列印設定。

通用印表機驅動程式列印設定

VMware Integrated Printing 可為從 Windows 用戶端機器重新導向的 UPD 印表機提供下列列印設定。

- **方向**：選取紙張的直向或橫向顯示。釘書釘和打孔裝訂選項取決於紙張的方向。
- **雙面列印**：為支援雙面模式的印表機選取雙面列印。
- **每張多頁**：如果您想要多個文件頁面列印到一個實體頁面上，請選取要列印到一個實體頁面上的頁數，然後選取頁面的配置。
- **紙張來源**：選取包含紙張大小類型 (例如 Letter 或 Legal) 的紙匣。
- **媒體**：選取列印的媒體類型。
- **色彩**：指定彩色印表機應列印彩色還是單色。
- **DPI**：指定印表機的解析度。
- **列印和預覽**：選取**直接列印**或**列印預覽**：
  - 使用**直接列印**時，您可以選取會在列印之前開啟用戶端印表機喜好設定的**利用開啟喜好設定對話方塊**，以便變更列印設定。
  - 使用**列印預覽**時，則無法使用**利用開啟喜好設定對話方塊**選項。
- **份數**：指定列印份數。
- **列印為影像**：將每個頁面列印為影像。
- **壓縮**：指定列印文件中的影像要如何壓縮。
- **裝訂**：為指定的印表機指定釘書釘和打孔選項。

原生印表機驅動程式裝訂選項

在將特定硬體連線到印表機時，這些重新導向的原生印表機支援裝訂選項：

表 2-8. 原生印表機驅動程式裝訂選項

印表機	裝訂選項	用戶端本機印表機上的需求
FX ApeosPort-IV C5575 PCL 6	釘書釘、小冊子	確認裝訂硬體裝置已與印表機連線。 在印表機內容中更新印表機資訊，加上雙向通訊。 在印表機喜好設定中啟用裝訂選項。
Ricoh MP C5003	釘書釘、打孔	根據裝置設定手動新增裝訂分頁器以啟用裝訂選項，即會在印表機喜好設定中提供該選項。

安裝 VMware Integrated Printing 重新導向

VMware Integrated Printing 是 Horizon Agent 安裝程式中的自訂安裝選項。依預設為未選取狀態。您必須選取 VMware Integrated Printing 進行安裝。若要在虛擬機器上安裝此功能，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件。若要在 RDS 主機上安裝此功能，請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件。這些文件發佈在 https://docs.vmware.com/tw/VMware-Horizon-7/index.html。若要在 Windows 用戶端上設定列印喜好設定，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件 (網址為 https://docs.vmware.com/tw/VMware-Horizon-Client-for-Windows/index.html) 中的〈設定 VMware Integrated Printing 重新導向功能的列印喜好設定〉。

設定 VMware Integrated Printing 重新導向群組原則設定

您可以使用 VMware View Agent 組態 ADMX 範本檔 (`printerRedirection.admx`) 中的群組原則設定來停用依據位置列印、停用列印設定持續性，以及選取已重新導向用戶端印表機的印表機驅動程式。請參閱 VMware 整合式列印原則設定。

設定 URL 內容重新導向

3

透過 URL 內容重新導向功能，您可以設定特定的 URL，使其在用戶端機器上或遠端桌面平台或已發佈應用程式中開啟。您可以將使用者在 Internet Explorer 網址列或應用程式中輸入的 URL 重新導向。

本章節討論下列主題：

瞭解 URL 內容重新導向

URL 內容重新導向功能支援從遠端桌面平台或已發佈應用程式到用戶端，以及從用戶端到遠端桌面平台或已發佈應用程式的重新導向。

從遠端桌面平台或已發佈應用程式到用戶端的重新導向稱為代理程式至用戶端重新導向。從用戶端至遠端桌面平台或已發佈應用程式的重新導向稱為用戶端至代理程式重新導向。

代理程式至用戶端重新導向	透過代理程式至用戶端重新導向，Horizon Agent 會將 URL 傳送至 Horizon Client，這會在用戶端機器上針對 URL 中的通訊協定開啟預設應用程式。
用戶端至代理程式重新導向	透過用戶端至代理程式重新導向，Horizon Client 會開啟您指定用來處理 URL 的遠端桌面平台或已發佈應用程式。如果 URL 重新導向至遠端桌面平台，則連結會在該桌面平台的通訊協定所適用的預設瀏覽器中開啟。如果

URL 重新導向至已發佈應用程式，則連結會以指定的已發佈應用程式來開啟。使用者必須有權存取桌面平台或應用程式集區。

您可以將某些 URL 從遠端桌面平台或已發佈應用程式重新導向至用戶端，並可將其他 URL 從用戶端重新導向至遠端桌面平台或已發佈應用程式。您可以重新導向任意數量的通訊協定，包括 HTTP、HTTPS、mailto 和 callto。使用 Chrome 瀏覽器的重新導向時不支援 callto 通訊協定。

URL 內容重新導向的需求

若要使用 URL 內容重新導向功能，您的用戶端機器、遠端桌面平台機器和 RDS 主機必須符合特定需求。

網頁瀏覽器

- Internet Explorer 9、10 和 11
- Chrome 60.0.3112.101 或更新版本 (官方組建)，64 位元或 32 位元

若要使用 Chrome 瀏覽器搭配 URL 內容重新導向，則必須安裝 VMware Horizon URL 內容重新導向 Helper 擴充功能並在 Chrome 中啟用。如需 Windows 安裝指示，請參閱為 Windows 上的 Chrome 安裝並啟用 URL 內容重新導向 Helper 擴充功能。如需 Mac 安裝指示，請參閱為 Mac 上的 Chrome 啟用 URL 內容重新導向 Helper。

Windows 用戶端

- Windows 版 Horizon Client 4.0 或更新版本。
- 若要使用 Chrome 瀏覽器搭配 URL 內容重新導向，則必須安裝 Horizon Client 4.7 或更新版本。
- 若要使用用戶端至代理程式重新導向，您必須在安裝 Windows 版 Horizon Client 期間啟用 URL 內容重新導向功能。

  備註 若要使用代理程式至用戶端重新導向，則不需要在 Windows 版 Horizon Client 中啟用 URL 內容重新導向功能。

Mac 用戶端

- Mac 版 Horizon Client 4.2 或更新版本。

  備註 在 Mac 版 Horizon Client 4.2 和 4.3 中，URL 內容重新導向是一項技術預覽功能，僅支援代理程式至用戶端重新導向。在 Mac 版 Horizon Client 4.4 和更新版本中，URL 內容重新導向受到正式支援，可同時支援代理程式至用戶端和用戶端至代理程式的重新導向。

- 若要使用 Chrome 瀏覽器搭配 URL 內容重新導向，則必須安裝 Horizon Client 4.7 或更新版本。

桌面平台虛擬機器和 RDS 主機

- 提供已發佈桌面平台和已發佈應用程式之遠端桌面平台虛擬機器與 RDS 主機中的 Horizon Agent 7.0 或更新版本。
- 若要使用 Chrome 瀏覽器搭配 URL 內容重新導向，則必須安裝 Horizon Agent 7.4 或更新版本。

- 您必須在安裝 Horizon Agent 期間啟用 URL 內容重新導向功能。

顯示通訊協定

- VMware Blast
- PCoIP

在 Cloud Pod 架構環境中使用 URL 內容重新導向

如果您擁有 Cloud Pod 架構環境，則除了本機 URL 內容重新導向設定以外，您還可以設定全域 URL 內容重新導向設定。

不同於僅顯示於本機網繭中的本機 URL 內容重新導向設定，全域 URL 內容重新導向設定會顯示在整個網繭聯盟中。透過全域 URL 內容重新導向設定，您可以將用戶端中的 URL 連結重新導向至全域資源，例如全域桌面平台權利和全域應用程式權利。

當使用者透過 Horizon Client 登入網繭聯盟中的連線伺服器執行個體時，連線伺服器執行個體會尋找所有指派給使用者的本機和全域 URL 內容重新導向設定。本機和全域設定會合併，且每當使用者按一下用戶端機器上的 URL 時，都會使用此合併的設定。

如需關於設定及管理 Cloud Pod 架構環境的完整資訊，請參閱《在 Horizon 7 中管理 Cloud Pod 架構》文件。

安裝具有 URL 內容重新導向功能的 Horizon Agent

若要使用從遠端桌面平台或已發佈應用程式到用戶端的 URL 內容重新導向 (代理程式至用戶端重新導向)，或是從用戶端至遠端桌面平台或已發佈應用程式的重新導向 (用戶端至代理程式重新導向)，您必須在安裝 Horizon Agent 時啟用 URL 內容重新導向功能。

在命令提示字元視窗中執行下列命令 (而不要按兩下安裝程式檔案)，以開始進行 Horizon Agent 安裝：

```
VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

依照提示完成安裝。

若要確認 URL 內容重新導向功能已安裝，請確定 `vmware-url-protocol-launch-helper.exe` 和 `vmware-url-filtering-plugin.dll` 檔案位於 `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection` 目錄中。如果您要在 Internet Explorer 中使用 URL 內容重新導向功能，也請確認 VMware Horizon View URL Filtering Plugin Internet Explorer 附加元件已啟用。

設定代理程式至用戶端重新導向

透過代理程式至用戶端重新導向，Horizon Agent 會將 URL 傳送至 Horizon Client，這會針對 URL 中的通訊協定開啟預設應用程式。

若要啟用代理程式至用戶端重新導向，請執行下列組態工作。

- 在 Horizon Agent 中啟用 URL 內容重新導向功能。請參閱安裝具有 URL 內容重新導向功能的 Horizon Agent。

- 將 URL 內容重新導向群組原則設定套用至您的遠端桌面平台和已發佈應用程式。請參閱將 URL 內容重新導向 ADMX 範本新增至 GPO。
- 設定群組原則設定，以指出 Horizon Agent 針對各種通訊協定進行 URL 重新導向的方式。請參閱 URL Content Redirection 群組原則設定。
- (選用) 若要在 Chrome 瀏覽器中使用 URL 內容重新導向，請安裝並啟用 VMware Horizon URL 內容重新導向 Helper 擴充功能。請參閱為 Windows 上的 Chrome 安裝並啟用 URL 內容重新導向 Helper 擴充功能。

將 URL 內容重新導向 ADMX 範本新增至 GPO

URL 內容重新導向 ADMX 範本檔 (名為 `urlRedirection.admx`) 包含可讓您控制 URL 連結要在用戶端上開啟 (代理程式至用戶端重新導向)，還是在遠端桌面平台或已發佈應用程式中開啟 (用戶端至代理程式重新導向) 的設定。

若要將 URL 內容重新導向群組原則設定套用至遠端桌面平台和已發佈應用程式，請將 ADMX 範本檔新增至您 Active Directory 伺服器上的 GPO。針對在遠端桌面平台或已發佈應用程式中點按之 URL 連結的相關規則，GPO 必須連結至包含您的虛擬桌面平台和 RDS 主機的 OU。

您也可以將群組原則設定套用至與包含 Windows 用戶端電腦的 OU 連結的 GPO，但一般常用來設定用戶端至代理程式重新導向的方法，是使用 `vdmutil` 命令列公用程式。由於 macOS 並不支援 GPO，因此如果您有 Mac 用戶端，則必須使用 `vmdutil`。

必要條件

- 在您安裝 Horizon Agent 時，確認 URL 內容重新導向功能包含在內。請參閱安裝具有 URL 內容重新導向功能的 Horizon Agent。
- 確認已為 URL Content Redirection 群組原則設定建立 Active Directory GPO。
- 確認 Active Directory 伺服器上有 MMC 和群組原則管理編輯器嵌入式管理單元可供使用。

程序

1 從 VMware 下載網站下載 Horizon 7 GPO 服務包 `.zip` 檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在「桌面平台及使用者運算」下，選取 VMware Horizon 7 下載，其中包含 GPO 服務包。

該檔案名為 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`，其中 *x.x.x* 為版本，而 *yyyyyyy* 為組建編號。為 Horizon 7 提供群組原則設定的所有 ADMX 檔案皆可從此檔案取得。

2 解壓縮 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` 檔案，並將 URL 內容重新導向 ADMX 檔案複製到您的 Active Directory 伺服器。

a 將 `urlRedirection.admx` 檔案複製到 `C:\Windows\PolicyDefinitions` 資料夾。

b 將 `urlRedirection.adml` 語言資源檔案複製到 `C:\Windows\PolicyDefinitions` 中的適當子資料夾。

例如，針對 EN 地區設定，將 `urlRedirection.adml` 檔案複製到 `C:\Windows\PolicyDefinitions\en-US` 資料夾。

3 在您的 Active Directory 伺服器上，開啟群組原則管理編輯器。

URL Content Redirection 群組原則設定會安裝在**電腦設定 > 原則 > 系統管理範本 > VMware Horizon URL 重新導向**中。

後續步驟

設定群組原則。請參閱 URL Content Redirection 群組原則設定。

URL Content Redirection 群組原則設定

URL 內容重新導向範本檔包含可讓您針對代理程式至用戶端和用戶端至代理程式的重新導向建立規則的群組原則設定。此範本檔包含「電腦組態」與「使用者組態」原則。所有設定皆位於群組原則管理編輯器的**VMware Horizon URL 重新導向**資料夾中。

下表說明 URL 內容重新導向範本檔中的群組原則設定。

表 3-1. URL Content Redirection 群組原則設定

設定	電腦	使用者	內容
`IE Policy: Prevent users from changing URL Redirection plugin loading behavior`	X		決定使用者是否可停用 URL 內容重新導向功能。 此設定依預設不會設定。
`IE Policy: Automatically enable URL Redirection plugin`	X		決定新安裝的 Internet Explorer 外掛程式是否會自動啟用。 此設定依預設不會設定。
`Url Redirection Enabled`	X		決定是否啟用 URL 內容重新導向功能。即使已在用戶端或代理程式中安裝 URL 內容重新導向功能，您仍可使用此設定來停用這項功能。 此設定依預設不會設定。

表 3-1. URL Content Redirection 群組原則設定 (續)

設定	電腦	使用者	內容
`Url Redirection Protocol 'http'`	X		針對所有使用 HTTP 通訊協定的 URL，指定應重新導向的 URL。此設定的選項如下： ■ **代理主機名稱** - 將 URL 重新導向至遠端桌面平台或應用程式時要使用之連線伺服器主機的 IP 位址或完整限定名稱。 ■ **遠端項目** - 可對指定於**代理程式規則**中的 URL 進行處理的遠端桌面平台或應用程式集區的顯示名稱。 ■ **用戶端規則** - 應重新導向至用戶端的 URL。例如，若您將**用戶端規則**設定為 **。*.mycompany.com**，所有包含文字 mycompany.com 的 URL 都會重新導向至 Windows 型用戶端，並在用戶端的預設瀏覽器中開啟。 ■ **代理程式規則** - 應重新導向至**遠端項目**中指定的遠端桌面平台或應用程式的 URL。例如，若您將**代理程式規則**設定為 **。*.mycompany.com**，所有包含 "mycompany.com" 的 URL 都會重新導向至遠端桌面平台或應用程式。 您可以在**用戶端規則**和**代理程式規則**中輸入規則運算式。如果啟用了 `Url Redirection IP Rules Enabled` 設定，您也可以輸入特定 IP 位址或 IP 位址範圍。如需完整的語法資訊，請參閱 URL 內容重新導向規則的語法。 在建立代理程式規則時，您也必須使用**代理主機名稱**選項指定連線伺服器主機的 IP 位址或完整網域名稱，以及使用**遠端項目**選項指定桌面平台或應用程式集區的顯示名稱。 最佳做法是為 HTTP 和 HTTPS 通訊協定設定相同的重新導向設定。如此一來，若使用者在 Internet Explorer 中輸入部分 URL (例如 mycompany.com)，則當該網站從 HTTP 自動重新導向至 HTTPS 時，URL 內容重新導向功能將會如預期般運作。在此範例中，若您為 HTTPS 設定規則，但並未針對 HTTP 設定相同的重新導向設定，則使用者輸入的部分 URL 不會進行重新導向。 此設定依預設為啟用。
`Url Redirection Protocol 'https'`	X		針對所有使用 HTTPS 通訊協定的 URL，指定應重新導向的 URL。 其選項和 `Url Redirection Protocol 'http'` 的相同。 此設定依預設不會設定。
`Url Redirection Protocol '[...]'`	X		對於 HTTP 和 HTTPS 以外的任何通訊協定 (例如電子郵件或 callto)，請使用此設定。 `Url Redirection Protocol 'http'` 和 `Url Redirection Protocol 'https'` 的選項相同。 如果您不需要設定其他通訊協定，您可以在將 URL 內容重新導向範本檔新增至 Active Directory 之前，先刪除或註解排除此項目。 此設定依預設不會設定。

表 3-1. URL Content Redirection 群組原則設定 (續)

設定	電腦	使用者	內容
`Install the Chrome extension that is required in the URL content redirection feature.`		X	此設定啟用時，將會以無訊息方式自動安裝 URL 內容重新導向功能所需的 Chrome 擴充功能。此安裝也包含授與必要權限。需要管理權限才能解除安裝。 此設定停用或未設定時，系統將不會安裝 URL 內容重新導向功能所需的 Chrome 擴充功能，且即便已設定重新導向，URL 內容重新導向仍無法在 Chrome 瀏覽器中正常運作，除非從 Chrome 線上應用程式商店手動安裝擴充功能。 此設定依預設不會設定。
`Url Redirection IP Rules Enabled`	X		如果啟用此設定，您可以在**用戶端規則**或**代理程式規則**中輸入特定 IP 位址或 IP 位址範圍。如需詳細資訊，請參閱 IP 位址和 IP 位址範圍篩選。 此設定依預設為停用。 **備註** 僅 Internet Explorer 和 IPv4 支援此功能。

針對用戶端至代理程式重新導向，如果您設定的通訊協定沒有預設處理常式，則在您設定此通訊協定的群組原則設定之後，您必須先啟動 Horizon Client 一次，指定此通訊協定的 URL 才會重新導向。

一般常用來設定用戶端至代理程式重新導向的方法是使用 `vdmutil` 命令列公用程式，而非群組原則設定。

URL 內容重新導向規則的語法

使用 URL 內容重新導向群組原則設定時，您必須指定要在用戶端上開啟哪些 URL (**用戶端規則**選項)，或是在遠端桌面平台或已發佈應用程式中開啟 (**代理程式規則**選項)。

URL

您可以在**用戶端規則**和**代理程式規則**中輸入 URL。您可以使用萬用字元 (*) 來指定符合多個 URL 的 URL 模式。要在規則項目中指定句點，您必須在句點前面加上逸出字元 (\)。例如，如果您指定 `".*\.net"`，則會重新導向 `xxxx.net`，而不會重新導向 `http://intranet`。

下表顯示包含 URL 的規則項目範例。

規則項目	說明
`.*`	指定要重新導向所有 URL。 若您針對代理程式規則 (**用戶端規則**選項) 使用此設定，則所有 URL 都會在指定的遠端桌面平台或已發佈應用程式中開啟。若您針對用戶端規則 (**用戶端規則**選項) 使用此設定，則所有 URL 都會重新導向至用戶端。
`.*\.acme\.com;.*\.example\.com`	指定所有包含文字 **.acme.com** 或 **.example.com** 的 URL 都會重新導向。請使用分號分隔多個項目。項目之間不得有空格。
`.*\.acme\.com/software`	指定所有包含文字 **.acme.com** 和子目錄 **/software** 的 URL 皆會重新導向。例如，系統會將 `http://www.acme.com/software` 重新導向。此外也會將 `http://www.acme.com/software/consumer` 重新導向。
[空格或保持空白]	指定不重新導向任何 URL。例如，讓**用戶端規則**選項保持空白，可指定所有 URL 皆不重新導向至用戶端。

規則運算式

您可以在**用戶端規則**和**代理程式規則**中輸入規則運算式。如需語法資訊，請參閱 URL 內容重新導向支援的規則運算式規則。

IP 位址和 IP 位址範圍篩選

如果您啟用 [已啟用 URL 重新導向 IP 規則] 群組原則設定，您可以在**用戶端規則**和**代理程式規則**中輸入特定的 IP 位址或 IP 位址範圍。

例如，如果您啟用 [已啟用 URL 重新導向 IP 規則] 並輸入 **".*\.mycompany\.com;22.22.22.22;10.10.1.2-10.10.12.20"**，則會重新導向下列 URL 和 IP 位址。

- 包含 .mycompany.com 的所有 URL
- IP 位址 22.22.22.22
- 在範圍 10.10.1.2 至 10.10.12.20 中的所有 IP 位址
- 解析為 IP 位址 22.22.22.22 的所有 URL
- 解析為 IP 位址範圍 10.10.1.2 至 10.10.12.20 的所有 URL

如果您同時輸入 URL 和 IP 位址或 IP 位址範圍，則 URL 規則具有較高的優先順序。如果 URL 相符，即會直接使用 URL 進行重新導向。如果 URL 不相符，則 Horizon 會執行 DNS 查詢，然後進行 IP 位址或 IP 位址範圍篩選。

僅 Internet Explorer 和 IPv4 支援此功能。此設定依預設為停用。

URL 內容重新導向支援的規則運算式規則

您可以在**用戶端規則**和**代理程式規則**中輸入規則運算式。規則運算式是說明字元模式的物件。規則運算式可對文字執行模式比對，以及搜尋和取代功能。

URL 內容重新導向支援下列規則運算式規則。

規則	詳細資料
括弧	[ ]、[^]、( )、(?:)、(?=)
\+metacharacter 或 metacharacter	'\w'、\'\W'、'\d'、'\D'、'\b'、'.'
數量詞	+、*、?、{x}、{x,y}、{x,}
替代符號	|

如需有關規則運算式的詳細資訊，請參閱 https://en.wikipedia.org/wiki/Regular_expression。

下表包含 URL 內容重新導向支援的規則運算式規則的範例。

規則項目	符合 URL 和 IP 位址的範例
。*\.net	www.hello.net、www.inter.net、train.word.net、test.train.net 和 train.chromeie.net.com.cn。
。*\.sth\.ctirial	example.sth.ctirial、www.google.sth.ctirial 和 www.google.com/test.sth.ctirial/editpage.action。
。*administra	www.administra.com、www.askadministra-tor.net 和 google.akmkda.eae/administra.cn。
。*a{4}custom\.com	world.banada.cn/aaaacustom.com、www.aaaacustom.com 和 exple.aaaacustom.com.net/nodepad.action。

規則項目	符合 URL 和 IP 位址的範例
。*a{2,3}custom\.com	world.banada.aacustom.com、www.aaacustom.com 和 exple.aacustom.com.net/nodepad.action。
。*train[abc]\.net	hello.traina.net、hello.trainb.net、example.trainc.net.com 和 www.testtraina.net.com/edit。
。*train[^abc]\.net	hello.traind.net、hello.traine.net、example.train2.net.com 和 www.testtrain3.net.com/edit。
。*a+c*tra\.net	www.actra.net.com。aactra.net.cn、atra.net.www.train 和 aaccctra.netword。
。*example(test)?\.cn	www.example.cn、www.exampletest.cn、example.cn/editpage 和 exampletest.cn/editpage。
sac(?=sprt)	helloworld.sacsprt.net、examplesacsprt.com/text 和 www.sacsprtexam.com。
sac(?!sprt)	helloworld.sacspra.net、examplesacbprt.com/text 和 www.sacexam.com。
10\.1\.1\.1[0-5]	10.1.1.10 到 10.1.1.15。
10\.1\.(1|2)\.1[0-5]	10.1.1.10 到 10.1.1.15 和 10.1.2.10 到 10.1.2.15。
10\.[2-4]\.19\.12	10.2.19.12、10.3.19.12 和 10.4.19.12。
10\.[^2-4]\.19\.12	10.6.19.12、10.1.19.12、10.5.19.12 和 10.7.19.12。
a(\w)cd(\d)345a\.com	www.abccd2345a.com.net 和 train.adc2cd1345a.com/edit.action。
abc(\W)cd(\D)345a\.com	google.abc+cda345a.com 和 test.train.net/abc&cda345a.com。
((25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])\.){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])	所有 IPv4 位址。
。*example(test)?\.cn;10\.1\.1\.1[0-5];a(\w)cd(\d)345a\.com	www.example.cn、example.cn/editpage,10.1.1.10 至 10.1.1.15、www.abccd2345a.com.net 和 train.adc2cd1345a.com/edit.action。

代理程式至用戶端重新導向群組原則範例

您可以使用代理程式至用戶端重新導向，以節省資源或作為新增的安全性層級。例如，若員工在遠端桌面平台或已發佈應用程式中觀看視訊，您可以將那些 URL 重新導向至用戶端機器，以避免在資料中心上增加額外負載。對於在公司網路外部工作的員工，基於安全性目的，您可能想要讓指向公司網路外的外部位置的所有 URL 在員工自己的用戶端機器上開啟。

例如，您可以設定規則，以便將未指向公司網路的任何 URL 重新導向至用戶端機器上開啟。在此範例中，您可以使用下列包含規則運算式的設定：

- 對於**代理程式規則**：`.*.mycompany.com`

  此規則會將任何包含文字 `mycompany.com` 的 URL 重新導向，使其在指定的遠端桌面平台或已發佈應用程式 (代理程式) 上開啟。

- 對於**用戶端規則**：`.*`

  此規則會將所有 URL 重新導向至用戶端，使其以預設的用戶端瀏覽器開啟。

URL 內容重新導向功能會使用下列程序來套用用戶端和代理程式規則：

1 當使用者按一下已發佈應用程式或遠端桌面平台中的連結時，系統會先檢查用戶端規則。

2 如果 URL 符合用戶端規則，則系統會接著檢查代理程式規則。

3 如果代理程式和用戶端規則之間發生衝突，連結會在本機上開啟。在此範例中，URL 會在代理程式機器上開啟。

4 如果不存在任何衝突，則 URL 會重新導向至用戶端。

   在此範例中，由於包含 **mycompany.com** 的 URL 是所有 URL 的子集，因此用戶端與代理程式規則發生衝突。由於發生此衝突，因此包含 **mycompany.com** 的 URL 會在本機上開啟。若您在位於遠端桌面平台時按一下 URL 中包含 **mycompany.com** 的連結，則 URL 會在該遠端桌面平台中開啟。若您從用戶端系統按一下 URL 中包含 **mycompany.com** 的連結，則 URL 會在用戶端上開啟。

設定用戶端至代理程式重新導向

透過用戶端至代理程式重新導向，Horizon Client 會開啟遠端桌面平台或已發佈應用程式，以處理使用者在用戶端上點按的 URL 連結。如果開啟了遠端桌面平台，則 URL 中的通訊協定所使用的預設應用程式會處理 URL。如果開啟了已發佈應用程式，則已發佈應用程式會處理 URL。

若要使用用戶端至代理程式重新導向，請執行下列組態工作。

- 在連線伺服器執行個體上使用 `vdmutil` 命令列公用程式建立 URL 內容重新導向設定，以指出 Horizon Client 針對各個通訊協定進行 URL 重新導向的方式。請參閱建立本機 URL 內容重新導向設定或建立全域 URL 內容重新導向設定。
- 在連線伺服器執行個體上使用 `vdmutil` 命令列公用程式，將 URL 內容重新導向設定指派給 Active Directory 使用者或群組。請參閱將 URL 內容重新導向設定指派給使用者或群組。
- 在 Horizon Agent 中啟用 URL 內容重新導向功能。請參閱安裝具有 URL 內容重新導向功能的 Horizon Agent。
- (僅限 Windows 用戶端) 在 Windows 版 Horizon Client 中啟用 URL 內容重新導向功能。請參閱安裝具有 URL 內容重新導向功能的 Windows 版 Horizon Client。
- (選用) 若要在 Chrome 瀏覽器中使用 URL 內容重新導向，請安裝並啟用 VMware Horizon URL 內容重新導向 Helper 擴充功能。針對 Windows 用戶端，請參閱為 Windows 上的 Chrome 安裝並啟用 URL 內容重新導向 Helper 擴充功能。針對 Mac 用戶端，請參閱為 Mac 上的 Chrome 啟用 URL 內容重新導向 Helper。
- 確認 URL 內容重新導向設定。請參閱測試 URL 內容重新導向設定。

重要 您可以使用群組原則設定來設定用戶端至代理程式重新導向規則，但使用 `vdmutil` 命令列公用程式是一般慣用的方法。如需使用群組原則設定的相關資訊，請參閱使用群組原則設定來設定用戶端至代理程式重新導向。對於 Mac 用戶端，您必須使用 `vdmutil` 設定用戶端至代理程式重新導向。由於 macOS 並不支援 GPO，因此如果您有 Mac 用戶端，就無法使用群組原則設定來設定用戶端至代理程式的組態。

在連線伺服器執行個體上使用 vdmutil 命令列公用程式

您可以在連線伺服器執行個體上使用 vdmutil 命令列介面，來建立、指派及管理用戶端至代理程式重新導向的 URL 內容重新導向設定。

備註 您必須使用 vdmutil 命令，設定 Mac 用戶端的用戶端至代理程式重新導向。由於 macOS 並不支援 GPO，因此如果您有 Mac 用戶端，將無法使用 GPO 來設定用戶端至代理程式的組態。

命令用法

vdmutil 命令的語法可控制它在 Windows 命令提示字元中的作業。

```
vdmutil command_option [additional_option argument] ...
```

可使用的其他選項視命令選項而定。

依預設，vdmutil 命令執行檔的路徑是 C:\Program Files\VMware\VMware View\Server\tools\bin。若要避免在命令列上輸入路徑，請將路徑新增至您的 PATH 環境變數中。

命令驗證

您必須以具有管理員角色的使用者身分執行 vdmutil 命令。

您可以使用 Horizon Administrator，將管理員角色指派給使用者。如需詳細資訊，請參閱《Horizon 7 管理》文件。

vdmutil 命令包括指定要用於驗證的使用者名稱、網域和密碼的選項。您必須使用這些驗證選項來搭配 --help 和 --verbose 之外的所有 vdmutil 命令選項。

表 3-2. vdmutil 命令驗證選項

選項	說明
--authAs	要對連線伺服器執行個體驗證的 Horizon 管理員使用者的使用者名稱。請勿使用 **domain\username** 或使用者主體名稱 (UPN) 格式。
--authDomain	在 --authAs 選項中指定的 Horizon 管理員使用者的完整網域名稱。
--authPassword	在 --authAs 選項中指定的 Horizon 管理員的密碼。輸入 **"*"** 而非密碼會使 vdmutil 命令提示輸入密碼，並且不會在命令列上的命令歷程記錄中保留敏感的密碼。

例如，下列 vdmutil 命令會以使用者 mydomain\johndoe 的身分登入。

```
vdmutil --listURLSetting --authAs johndoe --authDomain mydomain --authPassword secret
```

命令輸出

如果作業成功，vdmutil 命令將傳回 0；如果作業失敗，該命令將傳回失敗特定的非零代碼。vdmutil 命令會將錯誤訊息寫為標準錯誤。如果作業產生輸出，或使用 --verbose 選項啟用詳細記錄，vdmutil 命令會用美式英文將輸出寫為標準輸出。

URL 內容重新導向的選項

您可以使用下列 vdmutil 命令選項來建立、指派及管理 URL 內容重新導向設定。所有選項均以兩個破折號 (--) 開頭。

表 3-3. URL 內容重新導向的 vdmutil 命令選項

選項	說明
--addGroupURLSetting	將群組指派給特定的 URL 內容重新導向設定。
--addUserURLSetting	將使用者指派給特定的 URL 內容重新導向設定。
--createURLSetting	建立 URL 內容重新導向設定。
--deleteURLSetting	刪除 URL 內容重新導向設定。
--disableURLSetting	停用 URL 內容重新導向設定。
--enableURLSetting	啟用先前使用 --disableURLSetting 選項停用的 URL 內容重新導向設定。
--listURLSetting	列出連線伺服器執行個體上的所有 URL 內容重新導向設定。
--readURLSetting	顯示 URL 內容重新導向設定的相關資訊。
--removeGroupURLSetting	從 URL 內容重新導向設定中移除群組指派。
--removeUserURLSetting	從 URL 內容重新導向設定中移除使用者指派。
--updateURLSetting	更新現有的 URL 內容重新導向設定。

您可以輸入 **vdmutil --help**，以顯示所有 vdmutil 選項的語法資訊。若要顯示特定選項的詳細語法資訊，請輸入 **vdmutil --*option* --help**。

--agentURLPattern 選項的語法

當您使用 vdmutil 命令在連線伺服器執行個體上建立 URL 內容重新導向設定時，您可以在 --agentURLPattern 選項中輸入加上引號的字串，指定應在遠端桌面平台或已發佈的應用程式上開啟的一或多個 URL。

加上引號的字串包含規則運算式，且必須包含通訊協定前置詞。您可以使用萬用字元來指定符合多個 URL 的 URL 模式。

下表說明部分範例 URL 模式。

代理程式 URL 模式	說明
".*"	所有用戶端 URL 皆會重新導向至遠端桌面平台或已發佈應用程式。
"http://google.*"	所有包含文字 **google** 的用戶端 URL 皆會重新導向至遠端桌面平台或已發佈應用程式。
"http://acme.com/software"	所有包含文字 **acme.com** 和子目錄 **/software** 的用戶端 URL 皆會重新導向至遠端桌面平台或已發佈應用程式。例如，系統會將 http://www.acme.com/software 重新導向。此外也會將 http://www.acme.com/software/consumer 重新導向。

建立本機 URL 內容重新導向設定

您可以建立本機 URL 內容重新導向設定以重新導向特定的 URL，使其在遠端桌面平台或已發佈應用程式上開啟。本機 URL 內容重新導向設定只會顯示在本機網繭中。

您可以設定任意數量的通訊協定，包括 HTTP、HTTPS、mailto 和 callto。使用 Chrome 瀏覽器的重新導向時不支援 callto 通訊協定。

最佳做法是為 HTTP 和 HTTPS 通訊協定設定相同的重新導向設定。如此一來，若使用者在 Internet Explorer 中輸入部分 URL (例如 `mycompany.com`)，則當該網站從 HTTP 自動重新導向至 HTTPS 時，URL 內容重新導向功能將會如預期般運作。在此範例中，若您為 HTTPS 設定規則，但並未針對 HTTP 設定相同的重新導向設定，則使用者輸入的部分 URL 不會進行重新導向。

VMware 建議您不要為 URL 內容重新導向建立多個設定。

若要建立會顯示在整個網繭聯盟中的全域 URL 內容重新導向設定，請參閱建立全域 URL 內容重新導向設定。

必要條件

- 熟悉 `vdmutil` 命令列介面選項和需求，並確認您有足夠的權限可執行 `vdmutil` 命令。請參閱在連線伺服器執行個體上使用 vdmutil 命令列公用程式。
- 熟悉 URL 內容重新導向設定中 URL 的語法。請參閱--agentURLPattern 選項的語法。

程序

1 登入連線伺服器執行個體。

2 執行使用 `--createURLSetting` 選項的 `vdmutil` 命令，建立 URL 內容重新導向設定。

```
vdmutil --createURLSetting --urlSettingName url-filtering --urlRedirectionScope LOCAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop value]
[--agentURLPattern value]
```

選項	說明
--urlSettingName	URL 內容重新導向設定的唯一名稱。此名稱必須是 **`url-filtering`**。
--urlRedirectionScope	URL 內容重新導向設定的範圍。指定 LOCAL 會使設定僅顯示在本機網繭中。
--description	URL 內容重新導向設定的說明。說明可以包含 1 至 1024 個字元。
--urlScheme	套用 URL 內容重新導向設定的通訊協定，例如 http、https、mailto 或 callto。
--entitledApplication	顯示用來開啟指定 URL 的本機應用程式集區的名稱，例如 `iexplore-2012`。您也可以使用此選項來指定本機 RDS 桌面平台集區的顯示名稱。
--entitledDesktop	用來開啟指定 URL 的本機桌面平台集區的顯示名稱，例如 `Win10`。針對 RDS 桌面平台集區，請使用 `--entitledApplication` 選項。
--agentURLPattern	一個加上引號的字串，用以指定應在遠端桌面平台或已發佈應用程式上開啟的 URL。

3 (選擇性) 執行使用 `--updateURLSetting` 選項的 `vdmutil` 命令，將更多通訊協定、URL 和本機資源新增至您已建立的 URL 內容重新導向設定。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope LOCAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop value]
[--agentURLPattern value]
```

這些選項與使用 --createURLSetting 選項的 vdmutil 命令相同。

範例： 建立本機 URL 內容重新導向設定

下列範例會建立名為 url-filtering 的本機 URL 內容重新導向設定，將所有包含文字 http://google.*的用戶端 URL 重新導向至名為 iexplore2012 的應用程式集區。

```
VdmUtil --createURLSetting --urlSettingName url-filtering --urlScheme http
--entitledApplication iexplore2012 --agentURLPattern "http://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

下列範例會更新 url-filtering 設定，而將所有包含文字 https://google.*的用戶端 URL 重新導向至名為 iexplore2012 的應用程式集區。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme https
--entitledApplication iexplore2012 --agentURLPattern "https://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

下列範例會更新 url-filtering 設定，而將所有包含文字 mailto://.*.mycompany.com 的用戶端 URL 重新導向至名為 Outlook2008 的應用程式集區。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme mailto
--entitledApplication Outlook2008 --agentURLPattern "mailto://.*.mycompany.com"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

後續步驟

將 URL 內容重新導向設定指派給使用者或群組。請參閱將 URL 內容重新導向設定指派給使用者或群組。

建立全域 URL 內容重新導向設定

如果您擁有 Cloud Pod 架構環境，則可以建立全域 URL 內容重新導向設定以重新導向特定的 URL，使其在網繭聯盟中任何網繭內的遠端桌面平台或已發佈應用程式上開啟。

全域 URL 內容重新導向設定會顯示在整個網繭聯盟中。在建立全域 URL 內容重新導向設定時，您可以將 URL 重新導向至全域資源，例如全域桌面平台權利和全域應用程式權利。

您可以設定任意數量的通訊協定，包括 HTTP、HTTPS、mailto 和 callto。使用 Chrome 瀏覽器的重新導向時不支援 callto 通訊協定。

最佳做法是為 HTTP 和 HTTPS 通訊協定設定相同的重新導向設定。如此一來，若使用者在 Internet Explorer 中輸入部分 URL (例如 mycompany.com)，則當該網站從 HTTP 自動重新導向至 HTTPS 時，URL 內容重新導向功能將會如預期般運作。在此範例中，若您為 HTTPS 設定規則，但並未針對 HTTP 設定相同的重新導向設定，則使用者輸入的部分 URL 不會進行重新導向。

如需關於設定及管理 Cloud Pod 架構環境的完整資訊，請參閱《在 Horizon 7 中管理 Cloud Pod 架構》文件。

VMware 建議您不要為 URL 內容重新導向建立多個設定。

若要建立本機 URL 內容重新導向設定，請參閱建立本機 URL 內容重新導向設定。

必要條件

- 熟悉 vdmutil 命令列介面選項和需求，並確認您有足夠的權限可執行 vdmutil 命令。請參閱在連線伺服器執行個體上使用 vdmutil 命令列公用程式。
- 熟悉 URL 內容重新導向設定中 URL 的語法。請參閱--agentURLPattern 選項的語法。

程序

1 登入網繭聯盟中的任何連線伺服器執行個體。

2 執行使用 --createURLSetting 選項的 vdmutil 命令，建立 URL 內容重新導向設定。

```
vdmutil --createURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

選項	說明
--urlSettingName	URL 內容重新導向設定的唯一名稱。此名稱必須是 **url-filtering**。
--urlRedirectionScope	URL 內容重新導向設定的範圍。指定 GLOBAL 會使設定顯示在整個網繭聯盟中。
--description	URL 內容重新導向設定的說明。說明可以包含 1 至 1024 個字元。
--urlScheme	套用 URL 內容重新導向設定的通訊協定，例如 http、https、mailto 或 callto。
--entitledApplication	顯示用來開啟指定 URL 的全域應用程式權利的名稱。
--entitledDesktop	用來開啟指定 URL 的全域桌面平台權利的顯示名稱，例如 GE-1。
--agentURLPattern	一個加上引號的字串，用以指定應在遠端桌面平台或已發佈應用程式上開啟的 URL。

3 (選擇性) 執行使用 --updateURLSetting 選項的 vdmutil 命令，將更多通訊協定、URL 和全域資源新增至您已建立的 URL 內容重新導向設定。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

這些選項與使用 --createURLSetting 選項的 vdmutil 命令相同。

範例： 設定全域 URL 內容重新導向設定

下列範例會建立名為 url-filtering 的全域 URL 內容重新導向設定，將所有包含文字 http://google.*的 URL 重新導向至名為 GAE1 的全域應用程式權利。

```
vdmutil --createURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
--urlScheme http --entitledApplication GAE1 --agentURLPattern "http://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

下列範例會更新 url-filtering 設定，將所有包含文字 https://google.*的 URL 也重新導向至名為 GAE1 的全域應用程式權利。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
--urlScheme https --entitledApplication GAE1 --agentURLPattern "https://google.*" -authAs johndoe
--authDomain mydomain --authPassword secret
```

下列範例會更新 url-filtering 設定，將所有包含文字"mailto://.*.mycompany.com"的 URL 重新導向至名為 GA2 的全域應用程式權利。

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope GLOBAL
--urlScheme mailto --entitledApplication GAE2 --agentURLPattern "mailto://.*.mycompany.com"
--authAs johndoe --authDomain mydomain --authPassword secret
```

後續步驟

將 URL 內容重新導向設定指派給使用者或群組。請參閱將 URL 內容重新導向設定指派給使用者或群組。

將 URL 內容重新導向設定指派給使用者或群組

在建立 URL 內容重新導向設定後，您可以將其指派給 Active Directory 使用者或群組。

必要條件

熟悉 vdmutil 命令列介面選項和需求，並確認您有足夠的權限可執行 vdmutil 命令。請參閱在連線伺服器執行個體上使用 vdmutil 命令列公用程式。

程序

- 若要將 URL 內容重新導向設定指派給使用者，請在連線伺服器執行個體上執行使用 --addUserURLSetting 選項的 vdmutil 命令。

  ```
  vdmutil --addUserURLSetting --urlSettingName value --userName value
  ```

選項	說明
--urlSettingName	要指派的 URL 內容重新導向設定的名稱。此名稱必須是 **url-filtering**。
--userName	網域\使用者名稱格式的 Active Directory 使用者名稱。

- 若要將 URL 內容重新導向設定指派給群組，請執行使用 --addGroupURLSetting 選項的 vdmutil 命令。

  ```
  vdmutil --addGroupURLSetting --urlSettingName value --groupName value
  ```

選項	說明
--urlSettingName	要指派的 URL 內容重新導向設定的名稱。此名稱必須是 **url-filtering**。
--groupName	網域\群組格式的 Active Directory 群組名稱。

範例： 指派 URL 內容重新導向設定

下列範例會將名為 `url-filtering` 的 URL 內容重新導向設定指派給名為 `mydomain\janedoe` 的使用者。

```
vdmutil --addUserURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --userName mydomain\janedoe
```

下列範例會將名為 `url-filtering` 的 URL 內容重新導向設定指派給名為 `mydomain\usergroup` 的群組。

```
vdmutil --addGoupURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --groupName mydomain\usergroup
```

後續步驟

確認您的 URL 內容重新導向設定。請參閱測試 URL 內容重新導向設定。

安裝具有 URL 內容重新導向功能的 Windows 版 Horizon Client

若要使用從 Windows 用戶端至遠端桌面平台或已發佈應用程式的 URL 內容重新導向 (用戶端至代理程式重新導向)，您必須安裝具有 URL 內容重新導向功能的 Windows 版 Horizon Client。

若要啟用 URL 內容重新導向功能，您必須搭配使用 Windows 版 Horizon Client 安裝程式與命令列選項。在命令提示字元視窗中執行下列命令 (而不要按兩下安裝程式檔案)，以開始進行安裝：

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

若要確認 URL 內容重新導向功能已安裝，請確定 `vmware-url-protocol-launch-helper.exe` 和 `vmware-url-filtering-plugin.dll` 檔案位於 `%PROGRAMFILES%\VMware\VMware Horizon View Client` 目錄中。如果您要在 Internet Explorer 中使用 URL 內容重新導向功能，也請確認 VMware Horizon View URL Filtering Plugin Internet Explorer 附加元件已安裝。

備註 Mac 版 Horizon Client 4.4 依預設支援用戶端至代理程式重新導向。無需執行額外的安裝步驟。Mac 版 Horizon Client 4.2 和 4.3 不支援用戶端至代理程式重新導向。

測試 URL 內容重新導向設定

在建立並指派 URL 內容重新導向設定後，請執行特定步驟以確認設定可正常運作。

必要條件

熟悉 `vdmutil` 命令列介面選項和需求，並確認您有足夠的權限可執行 `vdmutil` 命令。請參閱在連線伺服器執行個體上使用 vdmutil 命令列公用程式。

程序

1 登入連線伺服器執行個體。

2 執行使用 --readURLSetting 選項的 vdmutil 命令。

例如：

```
vdmutil --readURLSetting --urlSettingName url-filtering --authAs johndoe
--authDomain mydomain --authPassword secret
```

此命令會顯示關於 URL 內容重新導向設定的詳細資訊。例如，url-filtering 設定的下列命令輸出顯示包含文字 google.* 的 HTTP 和 HTTPS URL 會從用戶端重新導向至名為 iexplore2012 的本機應用程式集區。

```
URL Redirection setting url-filtering
   Description                                    : null
   Enabled                                        : true
   Scope of URL Redirection Setting               : LOCAL
   URL Scheme And Local Resource handler pairs
      URL Scheme                                  : http
      Handler type                                : APPLICATION
      Handler Resource name                       : iexplore2012
      URL Scheme                                  : https
      Handler type                                : APPLICATION
      Handler Resource name                       : iexplore2012
   AgentPatterns
        https://google.*
        http://google.*
   ClientPatterns
      No client patterns configured
```

3 在 Windows 用戶端機器上開啟 Horizon Client，連線至連線伺服器執行個體，按一下與設定中設定的 URL 模式相符的 URL，然後確認這些 URL 如預期進行重新導向。

4 在相同的 Windows 用戶端機器上開啟登錄編輯程式 (regedit)，然後檢查路徑 \Computer \HKEY_CURRENT_USER\Software\Vmware.Inc.\VMware VDM\URLRedirection\ 中的登錄機碼。

對於每個指定於設定中的通訊協定，您都應該會看見一個機碼。您可以按一下通訊協定，以檢視與該通訊協定相關聯的規則。例如，agentRules 會顯示正在重新導向的 URL、brokerHostName 會顯示重新導向 URL 時所使用之連線伺服器執行個體的 IP 位址或完整主機名稱，而 remoteItem 則會顯示對重新導向的 URL 進行處理的桌面平台或應用程式集區的顯示名稱。

管理 URL 內容重新導向設定

您可以使用 vdmutil 命令管理您的 URL 內容重新導向設定。

您必須對所有命令指定 --authAs、--authDomain 和 --authPassword 選項。如需詳細資訊，請參閱在連線伺服器執行個體上使用 vdmutil 命令列公用程式。

顯示設定

執行使用 --listURLSetting 選項的 vdmutil 命令，可列出所有已設定的 URL 內容重新導向設定的名稱。

```
vdmutil --listURLSetting
```

執行使用 --readURLSetting 的 vdmutil 命令，可檢視關於特定 URL 內容重新導向設定的詳細資訊。

```
vdmutil --readURLSetting --urlSettingName value
```

刪除設定

執行使用 --deleteURLSetting 選項的 vdmutil 命令，可刪除 URL 內容重新導向設定。

```
vdmutil --deleteURLSetting --urlSettingName value
```

停用和啟用設定

執行使用 --disableURLSetting 選項的 vdmutil 命令，可停用 URL 內容重新導向設定。

```
vdmutil --disableURLSetting --urlSettingName value
```

執行使用 --enableURLSetting 選項的 vdmutil，可啟用已停用的 URL 內容重新導向設定。

```
vdmutil --enableURLSetting --urlSettingName value
```

從設定中移除使用者或群組

執行使用 --removeUserURLSetting 選項的 vdmutil 命令，可從 URL 內容重新導向設定中移除使用者。

```
vdmutil --removeUserURLSetting --urlSettingName value --userName value
```

執行使用 --removeGroupURLSetting 選項的 vdmutil 命令，可從 URL 內容重新導向設定中移除群組。

```
vdmutil --removeGroupURLSetting --urlSettingName value --userGroup value
```

指定使用者或群組名稱時，請使用網域\使用者名稱或網域\群組名稱格式。

使用群組原則設定來設定用戶端至代理程式重新導向

URL 內容重新導向 ADMX 範本檔 (urlRedirection.admx) 包含可用來建立規則，以將 URL 從用戶端重新導向至遠端桌面平台或已發佈應用程式 (用戶端至代理程式重新導向) 的群組原則設定。

重要 一般常用來設定用戶端至代理程式重新導向的方法，是使用 vdmutil 命令列介面。由於 macOS 並不支援群組原則，因此如果您有 Mac 用戶端，將無法使用群組原則來設定用戶端至代理程式的組態。

若要建立用戶端至代理程式重新導向的規則，您可以使用**遠端項目**選項指定桌面平台或已發佈應用程式集區的顯示名稱，並使用**代理程式規則**選項指定應重新導向至遠端桌面平台或已發佈應用程式的 URL。您也可以使用**代理主機名稱**選項，指定將 URL 重新導向至遠端桌面平台或已發佈應用程式時要使用之連線伺服器主機的 IP 位址或完整網域名稱。

例如，基於安全性目的，您可以讓所有指向公司網路的 HTTP URL 在遠端桌面平台或已發佈應用程式中開啟。在此案例中，您可以將**代理程式規則**選項設定為 **.*.mycompany.com**。

如需 URL 內容重新導向範本檔安裝指示、群組原則設定說明及**代理程式規則**選項語法，請參閱設定代理程式至用戶端重新導向。

URL 內容重新導向限制

URL 內容重新導向功能的行為可能有特定的非預期結果。

- 若 URL 根據地區設定開啟國家/地區特定頁面，則連結的來源會決定所開啟的地區設定頁面。例如，若遠端桌面平台 (代理程式來源) 位於日本的資料中心，且使用者的電腦位於美國，則當 URL 從代理程式重新導向至用戶端機器時，在美國用戶端上開啟的頁面會是日文頁面。
- 若使用者從網頁建立我的最愛，則會在重新導向之後建立我的最愛。例如，若使用者按一下用戶端機器上的連結，且 URL 重新導向至遠端桌面平台 (代理程式)，而使用者針對該頁面建立了我的最愛，則該項我的最愛會建立在代理程式上。下一次使用者在用戶端機器上開啟瀏覽器時，使用者可能會預期可在用戶端機器上找到我的最愛，但我的最愛卻是儲存在遠端桌面平台 (代理程式來源) 上。
- 例如，如果使用者在用戶端機器上按一下連結，而 URL 重新導向至遠端桌面平台，則使用者下載的檔案會出現在其瀏覽器用來開啟 URL 的機器上。若連結下載了檔案，或連結用於可讓使用者下載檔案的網頁，則檔案會下載至遠端桌面平台，而非用戶端機器。
- 如果您將 Horizon Agent 和 Horizon Client 安裝在相同的機器上，您將可在 Horizon Agent 或 Horizon Client 中啟用 URL 內容重新導向，但不可同時在這兩處啟用。在此機器上，您可以設定用戶端至代理程式重新導向或代理程式至用戶端重新導向，但不可兩者皆設定。

不支援的 URL 內容重新導向功能

URL 內容重新導向功能在特定情況下無法使用。

縮短 URL

縮短 URL (例如 `https://goo.gl/abc`) 可根據篩選規則進行重新導向，但篩選機制並不會檢查未縮短的原始 URL。

例如，如果您的規則所重新導向的 URL 包含 `acme.com`、原始 URL (例如 `http://www.acme.com/some-really-long-path`) 和原始 URL 的縮短 URL (例如 `https://goo.gl/xyz`)，則只會重新導向原始 URL，而不會重新導向縮短 URL。

您可以建立規則，將最常用來縮短 URL 之網站的 URL 封鎖或重新導向，以因應此限制。

內嵌 HTML 頁面

內嵌 HTML 頁面會略過 URL 重新導向，例如，當使用者移至不符合 URL 重新導向規則的 URL 時。如果頁面中的內嵌 HTML 頁面 (iFrame 或內嵌框架) 包含不符合重新導向規則的 URL，則 URL 重新導向規則不會發生作用。規則只會在頂層 URL 發生作用。

停用的 Internet Explorer 外掛程式

URL 內容重新導向不適用於 Internet Explorer 外掛程式停用的情況中，例如，當使用者在 Internet Explorer 中切換至 [InPrivate 瀏覽] 時。人們會使用隱私瀏覽，讓網頁和下載自網頁的檔案不會記錄在他們電腦上的瀏覽和下載歷程記錄中。之所以有此限制，是因為 URL 重新導向功能需要啟用特定的 Internet Explorer 外掛程式，但隱私瀏覽會停用這些外掛程式。

您可以使用 GPO 設定防止使用者停用外掛程式，以因應此限制。這些設定包括：「不允許使用者啟用或停用附加元件」以及「自動啟用新安裝的附加元件」。在群組原則管理編輯器中，這些設定位於**電腦設定 > 系統管理範本 > Windows 元件 > Internet Explorer** 下。

若要針對 Internet Explorer 因應此限制，請使用 GPO 設定來停用 InPrivate 模式。此設定稱為「關閉 InPrivate 瀏覽」。在群組原則管理編輯器中，這些設定位於**電腦設定 > 系統管理範本 > Windows 元件 > Internet Explorer > 隱私權**下。

這些因應措施是最佳做法，並且可防止隱私瀏覽以外的情況可能導致的重新導向相關問題。

Windows 10 通用應用程式是通訊協定的預設處理常式

若 Windows 10 通用應用程式為針對連結中所指定通訊協定的預設處理常式，則 URL 重新導向不會發生作用。通用應用程式建置在通用 Windows 平台上，因此可供下載至個人電腦、平板電腦和手機，其中包含了 Microsoft Edge 瀏覽器、郵件、地圖、相片、Grove Music 和其他應用程式。

如果點按了以這些應用程式之一為預設處理常式的連結，則 URL 不會重新導向。例如，若使用者按一下應用程式中的電子郵件連結，且預設電子郵件應用程式為「郵件」通用應用程式，則不會將連結中指定的 URL 重新導向。

您可以將不同的應用程式設為您要重新導向之 URL 的通訊協定所使用的預設處理常式，以因應此限制。例如，如果 Edge 是預設瀏覽器，請將 Internet Explorer 設為預設瀏覽器。

為 Windows 上的 Chrome 安裝並啟用 URL 內容重新導向 Helper 擴充功能

若要在 Windows 用戶端或 Windows 代理程式機器上使用 Chrome 瀏覽器搭配 URL 內容重新導向功能，您必須為 Chrome 安裝並啟用 VMware Horizon URL 內容重新導向 Helper 擴充功能。

您可以透過啟用 URL 內容重新導向群組原則設定，以安裝並啟用 VMware Horizon URL 內容重新導向 Helper 擴充功能。

此程序說明如何在 Active Directory 伺服器上，將 URL 內容重新導向群組原則設定套用至 GPO。針對 Windows 用戶端機器，GPO 必須連結至包含 Windows 用戶端電腦的 OU。針對遠端桌面平台和應用程式，GPO 必須連結至包含虛擬桌面平台和 RDS 主機的 OU。

若未使用群組原則來安裝並啟用 VMware Horizon URL 內容重新導向 Helper 擴充功能，則必須從 Chrome 線上應用程式商店手動安裝此擴充功能。

必要條件

- 針對 Windows 用戶端機器，請安裝 Horizon Client 4.7 或更新版本，並啟用 URL 內容重新導向功能。請參閱安裝具有 URL 內容重新導向功能的 Windows 版 Horizon Client。
- 針對 Windows 代理程式機器，請安裝 Horizon Agent 7.4 或更新版本，並啟用 URL 內容重新導向功能。請參閱安裝具有 URL 內容重新導向功能的 Horizon Agent。
- 安裝 Chrome 瀏覽器。如需支援的版本，請參閱 URL 內容重新導向的需求。
- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。

- 確認 Active Directory 伺服器上有 MMC 及群組原則物件編輯器嵌入式管理單元可供使用。
- 將 URL 內容重新導向 ADMX 範本檔新增至您的 Active Directory 伺服器。請參閱將 URL 內容重新導向 ADMX 範本新增至 GPO。

程序

1. 在您的 Active Directory 伺服器上開啟群組原則管理編輯器，並導覽至**使用者設定 > 原則 > 系統管理範本 > VMware Horizon URL 重新導向**資料夾。
2. 開啟**安裝 URL 內容重新導向功能中所需的 Chrome 擴充功能**設定，接著選取**已啟用**，然後按一下**確定**。
3. 在 Windows 機器上啟動 Chrome。

   VMware Horizon URL 內容重新導向 Helper 擴充功能會以無訊息方式安裝。
4. 若要確認 Chrome 擴充功能已安裝，請在 Chrome 瀏覽器中輸入 `chrome://extensions`。

   VMware Horizon URL 內容重新導向 Helper 會出現在 [擴充功能] 清單中，且系統會選取**已啟用**核取方塊。

後續步驟

第一次從用戶端上的 Chrome 瀏覽器重新導向 URL 時，系統會提示使用者在 Horizon Client 中開啟 URL。使用者必須按一下**開啟 URL: VMware Horizon Client 通訊協定**，否則 URL 重新導向將不會執行。如果使用者選取**記住我對 URL: VMware Horizon Client 通訊協定連結的選擇**核取方塊 (建議)，則不會再出現此提示。

為 Mac 上的 Chrome 啟用 URL 內容重新導向 Helper

若要在 Mac 用戶端上使用 Chrome 瀏覽器搭配 URL 內容重新導向功能，則必須為 Chrome 啟用 VMware Horizon URL 內容重新導向 Helper 擴充功能。

必要條件

- 在 Mac 用戶端上安裝 Chrome 瀏覽器。如需支援的版本，請參閱 URL 內容重新導向的需求。
- 在 Mac 上安裝 Horizon Client 4.7 或更新版本。如需相關資訊，請參閱《Mac 版 VMware Horizon Client 安裝和設定指南》文件。
- 在連線伺服器執行個體上設定 URL 內容重新導向設定。請參閱設定用戶端至代理程式重新導向。

程序

1. 在 Mac 上啟動 Horizon Client，並連線至已設定 URL 內容重新導向設定的連線伺服器執行個體。

   VMware Horizon URL 內容重新導向 Helper 擴充功能會自動安裝在 Mac 用戶端上的 Chrome 瀏覽器中。
2. 在 Mac 上重新啟動 Chrome 瀏覽器。

3 當系統提示您啟用 VMware Horizon URL 內容重新導向 Helper 擴充功能時，請按一下**啟用擴充功能**。

您必須啟用此擴充功能，才能從 Chrome 瀏覽器使用 URL 內容重新導向。

備註 如果您移除此擴充功能，仍可從 Chrome 線上應用程式商店手動進行安裝。

4 若要確認 Chrome 擴充功能已安裝，請在 Chrome 瀏覽器中輸入 **`chrome://extensions`**。

VMware Horizon URL 內容重新導向 Helper 會出現在 [擴充功能] 清單中，且系統會選取**已啟用**核取方塊。

後續步驟

第一次從 Mac 用戶端上的 Chrome 瀏覽器重新導向 URL 時，系統會提示使用者在 Horizon Client 中開啟 URL。使用者必須按一下**開啟 VMware Horizon Client**，否則 URL 重新導向將不會執行。如果使用者選取**記住我對 VMware Horizon Client 連結的選擇**核取方塊 (建議)，則不會再出現此提示。

將 USB 裝置與遠端桌面平台和應用程式搭配使用

4

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。如需支援之特定裝置類型的相關資訊，請參閱 USB 裝置類型的相關限制。

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。

重要 當您部署 USB 重新導向功能時，您可以採取步驟來保護組織不受可能影響 USB 裝置的安全漏洞侵犯。請參閱在安全的 Horizon 7 環境中部署 USB 裝置。

本章節討論下列主題：

- 在安全的 Horizon 7 環境中部署 USB 裝置
- 使用記錄檔進行疑難排解及判定 USB 裝置識別碼
- 使用原則來控制 USB 重新導向
- 對 USB 重新導向問題進行疑難排解

USB 裝置類型的相關限制

雖然 Horizon 7 並未明確阻止任何裝置搭配 USB 重新導向功能，但由於網路延遲和頻寬等因素，部分裝置比其他裝置運作得更順暢。依預設，部分裝置因自動篩選或封鎖而無法使用。

USB 3.0 裝置限制

從 Horizon 6 (6.0.1 版)，以及 Horizon Client 3.1 及更新版本開始，您可以將 USB 3.0 裝置插入用戶端機器上的 USB 3.0 連接埠。只有單一串流支援 USB 3.0 裝置。由於未實作多個串流支援，USB 裝置效能未提升。部分需要固定的高輸送量才能正常運作的 USB 3.0 裝置，可能因為網路延遲而無法在遠端工作階段中使用。

使用虛擬桌面平台的 USB 重新導向限制

下列類型的 USB 裝置可能不適合使用 USB 重新導向至在單一使用者機器上部署的遠端桌面平台。

- 網路攝影機對頻寬的要求 (通常耗用超過 60 Mbps 的頻寬) 使得其不受 USB 重新導向支援。對於網路攝影機，您可以使用即時音訊視訊功能。
- USB 音訊裝置的重新導向取決於網路的狀態，而且並不可靠。即使處於閒置狀態，一些裝置仍需要高資料流量。透過使用即時音訊視訊功能，音訊輸入和輸出裝置可順暢運作，且無需為這些裝置使用 USB 重新導向。
- 不支援 USB CD/DVD 燒錄。
- 視網路延遲和可靠性 (尤其是透過 WAN) 而定，部分 USB 裝置的效能可能會有較大差異。例如，單一 USB 儲存裝置讀取要求需要在用戶端與遠端桌面平台之間執行三個來回行程的時間。讀取完整檔案可能需要執行多個 USB 讀取作業，且延遲越大，所需來回行程越長。

  視格式而定，檔案結構可能非常大。大型的 USB 磁碟機需要幾分鐘的時間才會出現在桌面平台中。將 USB 裝置格式化為 NTFS 而非 FAT，有助於縮短初始連線時間。不穩定的網路連結會造成重試，並導致效能進一步降低。

  同樣地，USB CD/DVD 讀卡機和掃描器在延遲網路 (例如 WAN) 上無法正常運作。
- USB 掃描程式的重新導向取決於網路的狀態，並且掃描可能需要比平時更長的時間才能完成。

已發佈桌面平台和應用程式的 USB 重新導向限制

在 View Agent 6.2.x 及更新版本，或 Horizon Agent 7.0 及更新版本中，您可以重新導向本機連線的 USB 隨身碟和硬碟，以便在已發佈的桌面平台和應用程式中使用。從 Horizon Agent 7.0.2 開始，已發佈的桌面平台和應用程式也可支援更多常用的 USB 裝置，包括 TOPAZ 簽名板、Olympus 聽寫踏板和 Wacom 簽名板等。已發佈的桌面平台和應用程式不支援其他 USB 裝置類型，包括安全儲存磁碟機和 USB CD-ROM 光碟機。

USB 重新導向建議

針對某些類型的 USB 裝置，您可以使用 USB 重新導向的建議解決方案。

您可以不要使用 USB 重新導向，而改用下列可提升效能和使用者體驗的重新導向功能：

- 針對掃描器，使用掃描器重新導向。請參閱設定掃描器重新導向。
- 針對印表機，使用印表機重新導向。請參閱設定 VMware Integrated Printing 重新導向 。
- 針對智慧卡讀卡機，使用智慧卡重新導向。請參閱《Horizon 7 管理》文件。
- 針對序列埠裝置，使用序列埠重新導向。請參閱設定序列埠重新導向。
- 請使用用戶端磁碟機重新導向進行檔案共用，而不要對 USB 磁碟和大量儲存裝置使用 USB 重新導向。請參閱管理用戶端磁碟機重新導向的存取。

設定 USB 重新導向的概觀

若要設定部署，以便使用者連線卸除式裝置 (如 USB 快閃磁碟機、相機和耳機)，則必須在遠端桌面平台或 RDS 主機以及用戶端裝置上安裝特定的元件，且必須確認 Horizon Administrator 中已啟用 USB 裝置的全域設定。

此檢查清單包括在企業中設定 USB 重新導向的必要及選用工作。

USB 重新導向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，以取得特定類型之用戶端裝置的相關資訊。

重要 當您部署 USB 重新導向功能時，您可以採取步驟來保護組織不受可能影響 USB 裝置的安全漏洞侵犯。例如，您可以使用群組原則設定來停用某些遠端桌面平台和使用者的 USB 重新導向，或限制可重新導向的 USB 裝置類型。請參閱在安全的 Horizon 7 環境中部署 USB 裝置。

1 在遠端桌面平台來源或 RDS 主機上執行 Horizon Agent 安裝精靈時，請確定包含 USB 重新導向元件。

   預設會取消選取此元件。您必須選取此元件，才會加以安裝。

2 在用戶端系統上執行 VMware Horizon Client 安裝精靈時，請包含 USB 重新導向元件。

   預設會包含此元件。

3 請確認 Horizon Administrator 中已啟用從遠端桌面平台或已發佈應用程式存取 USB 裝置。

   在 Horizon Administrator 中，前往**原則 > 全域原則**，並確認 **USB 存取**設定為**允許**。

4 (選用) 設定 Horizon Agent 群組原則，以指定可重新導向的裝置類型。

請參閱使用原則來控制 USB 重新導向。

5 (選用) 在用戶端裝置上設定類似的設定。

您也可以設定 Horizon Client 連線到遠端桌面平台或應用程式或使用者插入 USB 裝置時，裝置是否自動連線。在用戶端裝置上設定 USB 設定的方式視裝置類型而定。例如，針對 Windows 用戶端，您可以設定群組原則。針對 Mac 用戶端，您可以使用命令列命令。如需更多資訊，請參閱安裝和設定文件以取得用戶端裝置的特定類型。

6 將使用者連線到遠端桌面平台或應用程式，並將其 USB 裝置插入本機用戶端系統。

如果遠端桌面平台或 RDS 主機上尚未安裝 USB 裝置的驅動程式，則客體作業系統會偵測 USB 裝置並搜尋合適的驅動程式，正如其在實體 Windows 電腦上所執行的一樣。

設定指紋掃描器重新導向

您可以將插入至 Windows 用戶端系統上的 USB 連接埠的生物識別裝置 (特別是指紋掃描器) 重新導向至虛擬桌面平台。

若要重新導向這些指紋掃描器，在遠端代理程式桌面平台上至少需要 200 Mbps 的網路頻寬。

支援的指紋掃描裝置如下：

表 4-1. 支援的指紋掃描器

裝置	用戶端作業系統	Windows 作業系統伺服器	通訊協定
U.are.U 5160 指紋辨識器	Windows 10 1809 64 位元 Windows 7 SP 1 Enterprise (32 位元、64 位元)	Windows 10 1809 64 位元 Windows 10 1903 64 位元 Windows 7 SP 1 Enterprise (32 位元、64 位元)	PCoIP、Blast
U.are.U 5300 指紋辨識器	Windows 10 1809 64 位元 Windows 7 SP 1 Enterprise (32 位元、64 位元)	Windows 10 1809 64 位元 Windows 10 1903 64 位元 Windows 7 SP 1 Enterprise (32 位元、64 位元)	PCoIP、Blast

設定讀卡機重新導向

您可以將插入 USB 連接埠的讀卡機透過 Windows 用戶端系統上的 PCoIP 虛擬通道重新導向至虛擬桌面平台。

支援的讀卡機如下：

表 4-2. 支援的讀卡機

裝置	用戶端作業系統	Windows 作業系統伺服器	通訊協定
Sony FeliCa RC-S320	Windows 10 1809 64 位元 Windows 7 SP 1 Enterprise (32 位元、64 位元)	Windows 10 1809 64 位元 Windows 10 1903 64 位元 Windows 7 SP 1 Enterprise (32 位元、64 位元)	PCoIP
Sony PaSoRi RC-S380	Windows 10 1809 64 位元 Windows 7 SP 1 Enterprise (32 位元、64 位元)	Windows 10 1809 64 位元 Windows 10 1903 64 位元 Windows 7 SP 1 Enterprise (32 位元、64 位元)	PCoIP

設定經由 PCoIP 虛擬通道的 USB

若要使用 UDP 連接埠 4172 設定經由 PCoIP 虛擬通道的 USB，請修改 Horizon Agent 中的登錄：

1 將登錄 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration \UsbVirtualChannelEnabled (REG_SZ) 設為 true。

2 將登錄 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware UsbRedirection \sideChannelType (REG_SZ) 設為 pcoip。

3 將 Horizon Agent 虛擬機器重新開機。

若要檢查組態是否生效：

1 使用 PCoIP 通訊協定連線至 Horizon Agent 桌面平台。

2 檢查位於「C:\Users\<username>\ AppData\Local\Temp\vmware-<username>\vmware-UsbRedirectionClient-xxxx.log」中的 Horizon Client 記錄。如果該組態已生效，您會在此檔案中看到「RPCManager::OnChannelDataObjectStateChanged()：正在要求虛擬端通道」。

網路流量和 USB 重新導向

用戶端系統和遠端桌面平台或應用程式之間的網路流量可以通過多個路由，視用戶端系統是否位於企業網路內部以及管理員選擇設定安全的方式而定。

USB 重新導向的運作不依賴顯示通訊協定，且 USB 流量通常使用 TCP 連接埠 32111。

如果用戶端系統位於公司網路內部，因而可在用戶端與遠端桌面平台或應用程式之間建立直接連線，則 USB 流量會使用 TCP 連接埠 32111。

如果用戶端系統位於公司網路外部，則用戶端可透過 DMZ 中的 Unified Access Gateway 應用裝置或安全伺服器連線。DMZ 中的 Unified Access Gateway 應用裝置和安全伺服器會與公司防火牆內的連線伺服器執行個體進行通訊，並防止連線伺服器執行個體連線至面向公眾的網際網路，而提供多一層的安全性。

Unified Access Gateway 應用裝置 (慣用方法) 不需要在防火牆上開啟其他連接埠供 USB 流量使用。安全伺服器則需要在防火牆上開啟 TCP 連接埠 32111，供 USB 流量使用。如需完整的安全伺服器連接埠需求，請參閱《Horizon 7 架構規劃》文件中的〈DMZ 型安全伺服器的防火牆規則〉。

您可以設定「透過工作階段增強功能 SDK 的 USB」功能，以避免開啟 TCP 連接埠 32111。請參閱啟用透過工作階段增強功能 SDK 的 USB 功能。

啟用透過工作階段增強功能 SDK 的 USB 功能

使用「透過工作階段增強功能 SDK 的 USB」功能，您無須開啟 TCP 連接埠 32111 即可傳輸 USB 流量。RDS 主機上的虛擬桌面平台和已發佈的桌面平台均支援此功能。

若要啟用「透過工作階段增強功能 SDK 的 USB」功能，請在遠端桌面平台上開啟 Windows 登錄編輯程式 (`regedit.exe`)、導覽至 `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration`，然後將 `UsbVirtualChannelEnabled` 機碼設為 `true`。

啟用此功能時，USB 流量可能會使用顯示通訊協定使用的 TCP 連線，或可能會使用專用的 TCP 連線。USB 流量使用的連線視您的組態而定。

例如，使用 VMware Blast 顯示通訊協定時，USB 流量可能會使用 VMware 虛擬通道 (VVC) 或 TCP 端通道。使用 PCoIP 顯示通訊協定時，USB 流量僅會使用 TCP 端通道。

依預設，TCP 端通道會使用 TCP 連接埠 9427。VVC 端通道會使用相同的連接埠作為 VMware Blast 顯示通訊協定。

如果將 USB 流量設定為使用 VVC，則在 Windows 代理程式上使用 PerfMon 所顯示的 USB 計數器為有效。

自動連線至 USB 裝置

在某些用戶端系統上，管理員、使用者或兩者都可以設定將 USB 裝置自動連線至遠端桌面平台。當使用者將 USB 裝置插入用戶端系統，或當用戶端連線至遠端桌面平台時，都可以進行自動連線。

在 Windows 用戶端上，從 Horizon Client 4.7 開始，USB 自動連線功能，包括 URI 查詢、命令列選項和群組原則設定，除了遠端桌面平台以外，也適用於已發佈的應用程式。

某些裝置 (例如智慧型手機和平板電腦) 需要自動連線，因為這些裝置在升級期間會因重新啟動而中斷連線。如果未將這些裝置設定為自動重新連線，則在升級期間，當裝置重新啟動後，它們會改為連線至本機用戶端系統。

管理員在用戶端上設定或使用者使用 Horizon Client 功能表項目設定的自動 USB 連線組態屬性，會套用至所有 USB 裝置，除非裝置已設定為從 USB 重新導向排除。例如，在某些用戶端版本中，依預設會將網路攝影機和麥克風排除在 USB 重新導向之外，因為這些裝置透過即時音訊視訊功能運作會更順暢。有時候，依預設可能不會將 USB 裝置從重新導向排除，而是需要管理員明確將裝置從重新導向排除。例如，下列類型的 USB 裝置不適合進行 USB 重新導向，因此不可自動連線至遠端桌面平台或應用程式：

- USB 乙太網路裝置。如果您重新導向 USB 乙太網路裝置，若此裝置是唯一的乙太網路裝置，則您的用戶端系統可能會失去網路連線。
- 觸控式螢幕裝置。如果您重新導向觸控式螢幕裝置，遠端桌面平台或應用程式會接收到觸控輸入，但不會接收到鍵盤輸入。

如果您將遠端桌面平台或應用程式設定為自動連線至 USB 裝置，您可以設定原則以排除特定裝置 (例如觸控式螢幕和網路裝置)。如需詳細資訊，請參閱設定 USB 裝置的篩選器原則設定。

在 Windows 用戶端上，除了使用自動連線已排除裝置以外之所有裝置的設定之外，您也可以在用戶端上編輯組態檔，將 Horizon Client 設定為僅將一或多個特定裝置 (例如智慧型手機和平板電腦) 重新連線。如需指示，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。

在安全的 Horizon 7 環境中部署 USB 裝置

USB 裝置容易受到稱為 BadUSB 的安全性威脅，其中，某些 USB 裝置上的韌體可能會遭到劫持並取代為惡意程式碼。例如，使裝置重新導向網路流量或模擬鍵盤並擷取按鍵輸入。您可以設定 USB 重新導向功能，以保護 Horizon 7 部署免遭此安全性弱點的影響。

透過停用 USB 重新導向，可以防止任何 USB 裝置重新導向至使用者的遠端桌面平台和應用程式。或者，可以停用特定 USB 裝置的重新導向功能，讓使用者僅能存取其遠端桌面平台和應用程式上的特定裝置。

根據組織中的安全性需求決定是否採取這些步驟。這些步驟不具有強制性。可以安裝 USB 重新導向功能，並針對 Horizon 7 部署中的所有 USB 裝置啟用該功能。請謹慎考慮，至少您的組織應嘗試限制暴露於此安全性弱點之下。

針對所有類型的裝置停用 USB 重新導向

部分高度安全的環境會要求防止使用者可能連接到用戶端裝置的所有 USB 裝置重新導向至遠端桌面平台和應用程式。您可以針對所有桌面平台集區、特定桌面平台集區或桌面平台集區中的特定使用者停用 USB 重新導向。

請根據情況使用以下任一策略：

- 在桌面平台映像或 RDS 主機上安裝 Horizon Agent 時，取消選取 **USB 重新導向**安裝選項。(依預設，會取消選取此選項)。此方法會防止存取所有從桌面平台映像或 RDS 主機部署的遠端桌面平台和應用程式上的 USB 裝置。
- 在 Horizon Administrator 中，編輯特定集區的 **USB 存取**原則，以拒絕或允許存取。透過此方法，您無需變更桌面平台映像，便可控制在特定桌面平台和應用程式集區中對 USB 裝置的存取。

  已發佈桌面平台和應用程式集區只能使用全域 **USB 存取**原則。無法針對個別已發佈桌面平台或應用程式集區設定此原則。
- 在 Horizon Administrator 中，於桌面平台或應用程式集區層級設定原則後，可以透過依序選取**使用者覆寫**設定和某個使用者來覆寫集區中特定使用者的原則。
- 請根據情況，在 Horizon Agent 端或用戶端上將 `Exclude All Devices` 原則設定為 **`true`**。
- 使用智慧原則建立原則，以停用 **USB 重新導向** Horizon 原則設定。透過此方法，您可以在符合特定條件時，停用特定遠端桌面平台上的 USB 重新導向。例如，您可以設定原則，在使用者從公司網路外部連線至遠端桌面平台時，停用 USB 重新導向。

如果將 `Exclude All Devices` 原則設定為 **`true`**，則 Horizon Client 會防止重新導向所有 USB 裝置。您可以使用其他原則設定，以允許重新導向特定裝置或裝置系列。如果將原則設定為 **`false`**，則除了由其他原則設定封鎖的裝置以外，Horizon Client 會允許重新導向所有 USB 裝置。您可以為 Horizon Agent 和 Horizon Client 設定此原則。下表顯示了您可以為 Horizon Agent 設定的 `Exclude All Devices` 原則如何與 Horizon Client 合併，以為用戶端電腦產生有效原則。依預設，允許重新導向所有 USB 裝置，封鎖的裝置除外。

表 4-3. 結合排除所有裝置原則的效果

排除 Horizon Agent 上的所有裝置原則	Horizon Client 上的排除所有裝置原則	結合的有效排除所有裝置原則
false 或未定義 (包含所有 USB 裝置)	**false** 或未定義 (包含所有 USB 裝置)	包含所有 USB 裝置
false (包含所有 USB 裝置)	**true** (排除所有 USB 裝置)	排除所有 USB 裝置
true (排除所有 USB 裝置)	任何或未定義	排除所有 USB 裝置

如果已將 `Disable Remote Configuration Download` 原則設為 **true**，則 Horizon Agent 上 `Exclude All Devices` 的值就不會傳送到 Horizon Client，但是 Horizon Agent 和 Horizon Client 會強制執行 `Exclude All Devices` 的本機值。

這些原則包含在 Horizon Agent 組態 ADMX 範本檔 (`vdm_agent.admx`) 中。

針對特定裝置停用 USB 重新導向

一些使用者可能需要重新導向特定的本機連線 USB 裝置，才能在遠端桌面平台或應用程式上執行工作。例如，醫師可能需要使用錄音機 USB 裝置來記錄患者的醫療資訊。在這些情況下，則無法停用對所有 USB 裝置的存取權限。您可以使用群組原則設定，針對特定裝置啟用或停用 USB 重新導向。

針對特定裝置啟用 USB 重新導向之前，請確保您信任已連線到企業中的用戶端機器的實體裝置。確保您可以信任供應鏈。如果可能，請追蹤 USB 裝置的保管鏈結。

此外，教導員工，以確保他們不會從未知來源連線裝置。如果可能，將環境中的裝置限制為僅接受已簽署的韌體更新、經過 FIPS 140-2 層級 3 認證以及不支援任何欄位可更新類型的韌體。這些類型的 USB 裝置來源難以找到，甚至可能找不到 (視裝置需求而定)。這些選項可能不切實際，但值得考慮。

每個 USB 裝置都有自己的廠商和產品識別碼，可供電腦進行識別。透過設定 Horizon Agent 組態群組原則設定，您可以針對未知裝置類型設定包含原則。透過此方法，可避免將未知裝置插入您環境所帶來的風險。

例如，您可以防止所有裝置 (除了已知裝置廠商和產品識別碼 `vid/pid=0123/abcd`) 重新導向至遠端桌面平台或應用程式：

```
ExcludeAllDevices   Enabled

IncludeVidPid       o:vid-0123_pid-abcd
```

備註 此範例組態會提供保護，但受到影響的裝置可能會報告任何 vid/pid，因此，仍可能會發生攻擊。

依預設，Horizon 7 會封鎖某些裝置系列，使其無法重新導向至遠端桌面平台或應用程式。例如，HID (人機介面裝置) 和鍵盤將被封鎖，無法顯示在客體中。一些已發佈的 BadUSB 程式碼將 USB 鍵盤裝置做為目標。

您可以防止特定的裝置系列重新導向至遠端桌面平台或應用程式。例如，可以封鎖所有視訊、音訊和大量儲存裝置：

```
ExcludeDeviceFamily   o:video;audio;storage
```

反之，可以建立一個白名單，阻止所有裝置重新導向，但允許使用特定的裝置系列。例如，可以封鎖儲存裝置以外的所有裝置：

```
ExcludeAllDevices     Enabled

IncludeDeviceFamily   o:storage
```

如果遠端使用者登入桌面平台或應用程式並對其產生影響，則可能會出現其他風險。您可以阻止 USB 存取來自公司防火牆外部的任何 Horizon 7 連線。USB 裝置可供內部使用，但無法對外使用。

請注意，如果您封鎖 TCP 連接埠 32111 以停用對 USB 裝置的外部存取，時區同步化將無法運作，因為連接埠 32111 也用於時區同步化。對於零用戶端，USB 流量將內嵌於 UDP 連接埠 4172 上的虛擬通道中。由於連接埠 4172 用於顯示通訊協定以及 USB 重新導向，因此，您無法封鎖連接埠 4172。如果需要，您可以在零用戶端上停用 USB 重新導向。如需詳細資料，請參閱零用戶端產品文宣或連絡零用戶端廠商。

設定原則以封鎖某些裝置系列或特定裝置，有助於降低受到 BadUSB 惡意程式碼之影響的風險。這些原則並不能降低所有風險，但有利於整體安全性策略。

使用記錄檔進行疑難排解及判定 USB 裝置識別碼

用戶端系統和遠端桌面平台作業系統或 RDS 主機上均會產生有用的 USB 記錄檔。使用這兩個位置上的記錄檔進行疑難排解。若要尋找特定裝置的產品識別碼，請使用用戶端記錄。

如果您嘗試設定 USB 裝置分割或篩選，或嘗試判斷為何 Horizon Client 功能表中未顯示特定裝置，請查詢用戶端記錄。用戶端記錄為 USB 仲裁程式及 Horizon View USB 裝置而產生。Windows 和 Linux 用戶端上的記錄依預設為啟用。在 Mac 用戶端上，依預設會停用記錄。若要在 Mac 用戶端上啟用記錄，請參閱《Mac 版 VMware Horizon Client 安裝和設定指南》文件。

當您設定分割和篩選 USB 裝置的原則時，部分設定值需要 USB 裝置的 VID (廠商識別碼) 及 PID (產品識別碼)。若要查詢 VID 和 PID，您可以在網際網路上搜尋產品名稱，並加上 `vid` 和 `pid`。或者，您也可以在 Horizon Client 執行時，將 USB 裝置插入本機系統後，查詢用戶端記錄檔。下表顯示了記錄檔的預設位置。

表 4-4. 記錄檔位置

用戶端或代理程式	記錄檔路徑
Windows 用戶端	`%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt` `C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log`
Horizon Agent	`%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt`
Mac 用戶端	`/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log` `/Library/Logs/VMware/vmware-usbarbitrator-xxxx.log`
Linux 用戶端	(預設位置) `/tmp/vmware-root/vmware-view-usbd-*.log`

如果裝置重新導向至遠端桌面平台或應用程式之後出現問題，請檢查用戶端及代理程式端記錄。

使用原則來控制 USB 重新導向

您可以為遠端桌面平台或應用程式 (Horizon Agent) 和 Horizon Client 設定 USB 原則。這些原則會指定用戶端裝置是否應該將複合 USB 裝置分割成重新導向所需的單獨元件。您可以將裝置分割成限制用戶端設為可供重新導向之用的 USB 裝置類型，以及讓 Horizon Agent 防止從用戶端電腦轉送某些 USB 裝置。

如果您已安裝舊版的 Horizon Agent 或 Horizon Client，則並非 USB 重新導向原則的所有功能皆可使用。此表格會顯示 Horizon 7 如何針對 Horizon Agent 和 Horizon Client 的不同組合來套用原則。

表 4-5. USB 原則設定的相容性

Horizon Agent 版本	Horizon Client 版本	USB 原則設定對 USB 重新導向的影響
5.1 或更新版本	5.1 或更新版本	USB 原則設定適用於 Horizon Agent 和 Horizon Client。您可以使用 Horizon Agent USB 原則設定來防止將 USB 裝置轉送至桌面平台。Horizon Agent 可以將裝置分割和篩選原則設定傳送至 Horizon Client。您可以使用 Horizon Client USB 原則設定來阻止從用戶端電腦將 USB 裝置重新導向到桌面平台。 **備註** 在 View Agent 6.1 或更新版本，或 Horizon Agent 7.0 及更新版本，和 Horizon Client 3.3 或更新版本中，這些 USB 重新導向原則設定適用於已發佈桌面平台和應用程式，也適用於在單一使用者機器上執行的遠端桌面平台。
5.1 或更新版本	5.0.x 或更舊版本	USB 原則設定僅適用於 Horizon Agent。您可以使用 Horizon Agent USB 原則設定來防止將 USB 裝置轉送至桌面平台。您無法使用 Horizon Client USB 原則設定來控制可以從用戶端電腦重新導向到桌面平台的裝置。Horizon Client 無法接收來自 Horizon Agent 的裝置分割和篩選原則設定。Horizon Client 針對 USB 重新導向所做的現有登錄設定會維持有效。
5.0.x 或更舊版本	5.1 或更新版本	USB 原則設定僅適用於 Horizon Client。您可以使用 Horizon Client USB 原則設定來阻止從用戶端電腦將 USB 裝置重新導向到桌面平台。您無法使用 Horizon Agent USB 原則設定來防止將 USB 裝置轉送至桌面平台。Horizon Agent 無法將裝置分割和篩選原則設定傳送至 Horizon Client。
5.0.x 或更舊版本	5.0.x 或更舊版本	USB 原則設定不適用。Horizon Client 針對 USB 重新導向所做的現有登錄設定會維持有效。

如果升級 Horizon Client，USB 重新導向的所有現有登錄設定 (例如 `HardwareIdFilters`) 會維持有效，直到您為 Horizon Client 定義 USB 原則為止。

在不支援用戶端 USB 原則的用戶端裝置上，您可以使用 Horizon Agent 的 USB 原則來控制允許從用戶端轉送到桌面平台或應用程式的 USB 裝置。

設定複合 USB 裝置的裝置分割原則設定

複合 USB 裝置由兩個或多個不同裝置的結合所組成，例如視訊輸入裝置和儲存裝置，或麥克風和滑鼠裝置。若您要允許一或多個元件可重新導向，則可以將複合裝置分割為其元件介面，將特定介面排除於重新導向之外及納入其他介面。

設定自動分割複合裝置的原則。若無法對特定裝置執行自動裝置分割，或自動分割無法產生應用程式所需結果，則可以手動分割複合裝置。

自動裝置分割

若啟用自動裝置分割，則 Horizon 7 將嘗試根據生效的篩選規則在複合裝置中分割功能或裝置。例如，聽寫麥克風可能會進行自動分割以便滑鼠裝置仍為用戶端的本機裝置，但是其餘裝置將轉送至遠端桌面平台。

下表顯示了 `Allow Auto Device Splitting` 設定的值如何決定 Horizon Client 是否嘗試自動分割複合 USB 裝置。依預設，會停用自動分割。

表 4-6. 結合停用自動分割原則的效果

允許 Horizon Agent 上的自動裝置分割原則	允許 Horizon Client 上的自動裝置分割原則	結合有效的允許自動裝置分割原則
`Allow – Default Client Setting`	**`false`** (停用自動分割)	停用自動分割
`Allow – Default Client Setting`	**`true`** (啟用自動分割)	啟用自動分割
`Allow – Default Client Setting`	未定義	啟用自動分割
`Allow – Override Client Setting`	任何或未定義	啟用自動分割
未定義	未定義	停用自動分割

備註 這些原則包含在 Horizon Agent 組態 ADMX 範本檔中。ADMX 範本檔名為 (`vdm_agent.admx`)。

依預設，Horizon 7 會停用自動分割，並將所有音訊輸出、鍵盤、滑鼠，或複合 USB 裝置的智慧卡元件排除於重新導向之外。

Horizon 7 會先套用裝置分割原則設定，然後才會套用任何篩選器原則設定。若啟用了自動分割，但是沒有將複合 USB 裝置明確排除於分割範圍之外 (透過指定複合 USB 裝置的廠商和產品識別碼)，Horizon 7 會檢查複合 USB 裝置的每個介面，根據篩選器原則設定，決定應包含或排除的介面。若您停用了自動裝置分割，但是未明確指定要分割的複合 USB 裝置的廠商和產品識別碼，Horizon 7 會將篩選器原則設定套用至整個裝置。

若您啟用自動分割，則可使用 `Exclude Vid/Pid Device From Split` (將 Vid/Pid 裝置排除於分割之外) 原則，指定要排除於分割範圍之外的複合 USB 裝置。

手動裝置分割

您可以使用 `Split Vid/Pid Device` (分割 Vid/Pid 裝置) 原則，指定要分割的複合 USB 裝置的供應商和產品識別碼。您也可以指定要排除於重新導向之外的複合 USB 裝置的元件介面。Horizon 7 不會將任何篩選器原則設定套用至您以這種方式排除的元件。

重要 若使用 `Split Vid/Pid Device` 原則，Horizon 7 將不會自動包含您未明確排除的元件。您必須指定篩選原則，例如 `Include Vid/Pid Device`，以納入那些元件。

表 4-7. 在 Horizon Agent 上，適用於裝置分割原則設定的分割修飾詞 顯示了修飾詞，指定如果有 Horizon Client 適用的對等裝置分割原則設定，Horizon Client 將如何處理 Horizon Agent 裝置分割原則設定。這些修飾詞適用於所有裝置分割原則設定。

表 4-7. 在 Horizon Agent 上，適用於裝置分割原則設定的分割修飾詞

修飾詞	說明
m (合併)	除了 Horizon Client 裝置分割原則設定，Horizon Client 還會套用 Horizon Agent 裝置分割原則設定。
o (覆寫)	Horizon Client 會使用 Horizon Agent 裝置分割原則設定，而不使用 Horizon Client 裝置分割原則設定。

表 4-8. 將分割修飾詞套用至裝置分割原則設定的範例 顯示了當您指定不同的分割修飾詞時，Horizon Client 會如何處理 `Exclude Device From Split by Vendor/Product ID` 的設定。

表 4-8. 將分割修飾詞套用至裝置分割原則設定的範例

在 Horizon Agent 上，依廠商/產品識別碼將裝置排除於分割之外	在 Horizon Client 上，依廠商/產品識別碼將裝置排除於分割之外	Horizon Client 使用的依廠商/產品識別碼將裝置排除於分割之外的有效原則設定
`m:vid-XXXX_pid-XXXX`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`
`o:vid-XXXX_pid-XXXX`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX`
`m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`
`o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`

Horizon Agent 不會將裝置分割原則設定套用至其連線端。

Horizon Client 會依照下列優先順序，評估裝置分割原則設定。

- `Exclude Vid/Pid Device From Split`
- `Split Vid/Pid Device`

將裝置排除於分割之外的裝置分割原則設定，其優先級高於任何裝置分割原則設定。若您定義了任何要排除於分割之外的介面或裝置，Horizon Client 會將相符的元件裝置排除於可重新導向的範圍之外。

設定原則以分割複合 USB 裝置的範例

為桌面平台設定分割原則，以在自動分割之後，將具有特定廠商和產品識別碼的裝置排除於重新導向之外，並將這些原則傳遞至用戶端電腦：

- 針對 Horizon Agent，將 `Allow Auto Device Splitting` 原則設為 `Allow – Override Client Setting`。
- 對於 Horizon Agent，將 `Exclude VidPid From Split` 原則設為 **o:vid-*xxx*_pid-*yyyy***，其中 *xxx* 和 *yyyy* 為適當的識別碼。

在桌面平台上允許自動裝置分割，並指定原則，用於在用戶端電腦上分割特定的裝置：

- 針對 Horizon Agent，將 `Allow Auto Device Splitting` 原則設為 `Allow – Override Client Setting`。
- 對於用戶端裝置，設定 `Include Vid/Pid Device` 篩選器原則以包含想要分割的特定裝置；例如，**vid-0781_pid-554c**。

- 對於用戶端裝置，例如將 `Split Vid/Pid Device` 原則設定為 **`vid-0781_pid-554c(exintf:00;exintf:01)`**，以分割指定的複合 USB 裝置，從而將介面 00 與介面 01 排除於重新導向之外。

設定 USB 裝置的篩選器原則設定

您為 Horizon Agent 和 Horizon Client 設定的篩選器原則設定，將決定可將哪些 USB 裝置從用戶端電腦重新導向至遠端桌面平台或應用程式。公司通常使用 USB 裝置篩選在遠端桌面平台上停用大量儲存裝置或封鎖轉送特定類型的裝置，例如，將用戶端裝置連線至遠端桌面平台的 USB 乙太網路介面卡。

連線至桌面平台或應用程式時，Horizon Client 會下載 Horizon Agent USB 原則設定，並結合使用 Horizon Client USB 原則設定，以決定您可從用戶端電腦重新導向哪些 USB 裝置。

Horizon 7 會先套用任何裝置分割原則設定，然後才會套用篩選器原則設定。如果您已分割複合 USB 裝置，Horizon 7 會根據篩選器原則設定檢查裝置的每個介面，以決定應排除或包含哪些裝置。如果您未分割複合 USB 裝置，Horizon 7 會將篩選器原則設定套用至整個裝置。

裝置分割原則包含在 Horizon Agent 組態 ADMX 範本檔 (`vdm_agent.admx`) 中。

代理程式強制 USB 設定的互動

下表列出修飾詞，指定在 Horizon Client 具有與代理程式可強制的設定對等的篩選器原則設定時，Horizon Client 將如何處理 Horizon Agent 篩選器原則設定。

表 4-9. 代理程式可強制設定的篩選器修飾詞

修飾詞	說明
`m` (合併)	除了 Horizon Client 篩選器原則設定，Horizon Client 還會套用 Horizon Agent 篩選器原則設定。在原則設定為 Boolean 或 true/false 的情況下，如果未設定用戶端原則，則會使用代理程式設定。如果已設定用戶端原則，則會忽略除 `Exclude All Devices` 設定之外的代理程式設定。如果已在代理程式端上設定 `Exclude All Devices` 原則，則該原則會覆寫用戶端設定。
`o` (覆寫)	Horizon Client 會使用 Horizon Agent 篩選器原則設定，而非 Horizon Client 篩選器原則設定。

例如，代理程式端上的以下原則會覆寫用戶端上的所有包括規則，並且僅裝置 VID-0911_PID-149a 會套用包括規則：

```
IncludeVidPid: o:VID-0911_PID-149a
```

也可以使用星號做為萬用字元；例如：**`o:vid-0911_pid-****`**

重要　如果將代理程式端設定為沒有 **`o`** 或 **`m`** 修飾詞，則組態規則會被視為無效並且將被忽略。

用戶端轉譯 USB 設定的互動

下表列出修飾詞，指定 Horizon Client 如何為用戶端轉譯的設定處理 Horizon Agent 篩選器原則設定。

表 4-10. 用戶端轉譯設定的篩選器修飾詞

修飾詞	說明
`Default` (在登錄設定中為 **d**)	如果 Horizon Client 篩選器原則設定不存在，Horizon Client 將會使用 Horizon Agent 篩選器原則設定。 如果 Horizon Client 篩選器原則設定存在，則 Horizon Client 會套用此原則設定，並忽略 Horizon Agent 篩選器原則設定。
`Override` (在登錄設定中為 **o**)	Horizon Client 會使用 Horizon Agent 篩選器原則設定，而非任何對等的 Horizon Client 篩選器原則設定。

Horizon Agent 不會在其連線端上為用戶端轉譯的設定套用篩選器原則設定。

下表顯示了您指定其他篩選器修飾詞時，Horizon Client 如何處理 `Allow Smart Cards` 設定的範例。

表 4-11. 將篩選器修飾詞套用至用戶端轉譯設定的範例

允許 Horizon Agent 上的智慧卡設定	允許 Horizon Client 上的智慧卡設定	有效允許由 Horizon Client 使用的智慧卡原則設定
`Disable – Default Client Setting` (在登錄設定中為 **d:false**)	**true** (允許)	**true** (允許)
`Disable – Override Client Setting` (在登錄設定中為 **o:false**)	**true** (允許)	**false** (停用)

如果您將 `Disable Remote Configuration Download` 原則設為 **true**，Horizon Client 將會忽略任何從 Horizon Agent 接收的篩選器原則設定。

即使您將 Horizon Client 設定為使用其他篩選器原則設定，或停用 Horizon Client 從 Horizon Agent 下載篩選器原則設定的功能，則 Horizon Agent 一律會在其連線端上，於代理程式可強制執行的設定中套用篩選器原則設定。Horizon Client 不會報告 Horizon Agent 正在封鎖轉送裝置。

設定的優先順序

Horizon Client 會根據優先順序評估篩選器原則設定。排除相符裝置重新導向的篩選器原則設定，優先於包含該裝置的同等篩選器原則設定。如果 Horizon Client 沒有遇到要排除裝置的篩選器原則設定，Horizon Client 就會允許裝置重新導向，除非已將 `Exclude All Devices` 原則設為 **true**。不過，如果已設定 Horizon Agent 上的篩選器原則設定以排除裝置，桌面平台或應用程式就會封鎖對其重新導向裝置的任何嘗試。

Horizon Client 會以下列優先順序評估篩選器原則設定，其中考量了 Horizon Client 設定、Horizon Agent 設定，以及您套用至 Horizon Agent 設定的修飾詞值。以下清單顯示了優先順序，項目 1 的優先順序最高。

1 `Exclude Path`

2 `Include Path`

3 `Exclude Vid/Pid Device`

4 `Include Vid/Pid Device`

5 `Exclude Device Family`

6 Include Device Family

7 Allow Audio Input Devices、Allow Audio Output Devices、Allow HIDBootable、Allow HID (Non Bootable and Not Mouse Keyboard)、Allow Keyboard and Mouse Devices、Allow Smart Cards 及 Allow Video Devices

8 已結合經評估為排除或包含所有 USB 裝置的有效 Exclude All Devices 原則

您可以僅為 Horizon Client 設定 Exclude Path 和 Include Path 篩選器原則設定。參考個別裝置系列的 Allow 篩選器原則設定有同等優先性。

如果您將原則設定設為根據廠商和產品識別碼值排除裝置，則 Horizon Client 會排除其廠商和產品識別碼值符合此原則設定的裝置，即使您已對該裝置所屬的系列設定 Allow 原則設定也一樣。

原則設定的優先順序可以解決原則設定之間的衝突。如果您設定 Allow Smart Cards，以允許重新導向智慧卡，則任何更高優先級的排除原則設定均會覆寫此原則。例如，您可能已設定 Exclude Vid/Pid Device 原則設定，以排除具有相符路徑或供應商與產品識別碼值的智慧卡裝置，或可能已設定 Exclude Device Family 原則設定，這樣也會全面排除 smart-card 裝置系列。

如果您已設定任何 Horizon Agent 篩選器原則設定，Horizon Agent 就會在遠端桌面平台或應用程式上依照下列優先順序 (項目 1 的優先順序最高) 評估並強制執行篩選器原則設定。

1 Exclude Vid/Pid Device

2 Include Vid/Pid Device

3 Exclude Device Family

4 Include Device Family

5 代理程式強制 Exclude All Devices 原則設為排除或包含所有 USB 裝置

Horizon Agent 會在其連線端上強制執行這一組限定的篩選器原則設定。

定義 Horizon Agent 的篩選器原則設定後，您就可以為非受管用戶端電腦建立篩選器原則。此功能也允許您封鎖裝置從用戶端電腦轉送，即使 Horizon Client 的篩選器原則設定允許重新導向也一樣。

例如，如果您將原則設定為讓 Horizon Client 允許裝置重新導向，但若 Horizon Agent 的原則已設定為排除該裝置，那麼 Horizon Agent 還是會封鎖裝置。

設定原則以篩選 USB 裝置的範例

這些範例中使用的廠商識別碼和產品識別碼只是範例。如需判定特定裝置之廠商識別碼和產品識別碼的相關資訊，請參閱使用記錄檔進行疑難排解及判定 USB 裝置識別碼。

- 在用戶端上，排除特定裝置，避免重新導向：

```
Exclude Vid/Pid Device:     Vid-0341_Pid-1a11
```

- 封鎖所有儲存裝置，避免重新導向至此桌面平台或應用程式集區。使用代理程式端設定：

```
Exclude Device Family:      o:storage
```

- 對於桌面平台集區中的所有使用者，封鎖音訊及視訊裝置，以確保這些裝置永遠可用於即時音訊視訊功能。使用代理程式端設定：

  ```
  Exclude Device Family:      o:video;audio
  ```

  請注意，其他策略會根據廠商和產品識別碼排除特定裝置。

- 在用戶端上，封鎖除特定裝置以外的所有裝置，避免重新導向：

  ```
  Exclude All Devices:        true
  Include Vid/Pid Device:     Vid-0123_Pid-abcd
  ```

- 排除某個特定公司製造的所有裝置，因為這些裝置會為使用者帶來問題。使用代理程式端設定：

  ```
  Exclude Vid/Pid Device:     o:Vid-0341_Pid-*
  ```

- 在用戶端上，包括兩個特定裝置，但排除所有其他裝置：

  ```
  Exclude All Devices:        true
  Include Vid/Pid Device:     Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
  ```

USB 裝置系列

您可以在為 Horizon Client 或是 View Agent 或 Horizon Agent 建立 USB 篩選規則時，指定 USB 裝置系列。

備註 某些裝置未顯示裝置系列。

表 4-12. USB 裝置系列

裝置系列名稱	說明
audio	任何音訊輸入或音訊輸出裝置。
audio-in	音訊輸入裝置，如麥克風。
audio-out	音訊輸出裝置，如喇叭與耳機。
bluetooth	以藍芽連線的裝置。
comm	通訊裝置，如數據機和有線網路卡。
hid	人機介面裝置，不包括鍵盤和指向裝置。
hid-bootable	啟動時可使用的人機介面裝置，不包括鍵盤和指標裝置。
imaging	影像裝置，如掃描器。
keyboard	鍵盤裝置。
mouse	指向裝置，如滑鼠。
other	未指定系列。
pda	個人數位助理。
physical	動力回饋裝置，如動力回饋搖桿。
printer	列印裝置。

表 4-12. USB 裝置系列 (續)

裝置系列名稱	說明
security	安全性裝置，如指紋辨識器。
smart-card	智慧卡裝置。
storage	大量儲存裝置，如隨身碟和外接式硬碟機。
unknown	未知系列。
vendor	具特定廠商功能的裝置。
video	視訊輸入裝置。
wireless	無線網路卡。
wusb	無線 USB 裝置。

Horizon Agent 組態 ADMX 範本中的 USB 設定

您可以為 Horizon Agent 和 Horizon Client 定義 USB 原則設定。連線時，Horizon Client 會從 Horizon Agent 下載 USB 原則設定，並將其與 Horizon Client USB 原則設定一起結合使用，以決定允許哪些裝置從用戶端電腦重新導向。

Horizon Agent 組態 ADMX 範本檔包含與 Horizon Agent 之驗證和環境元件有關的原則設定，包括 USB 重新導向。ADMX 範本檔名為 (vdm_agent.admx)。此設定適用於電腦層級。Horizon Agent 會優先從電腦層級的 GPO 讀取設定，然後再從 HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB 的登錄中讀取。

設定 USB 裝置分割的設定

下表說明 Horizon Agent 組態 ADMX 範本檔中用來分割複合 USB 裝置的每個原則設定。這些設定全都位於群組原則管理編輯器的 **VMware Horizon Agent 組態 > View USB 組態 > 僅供用戶端下載的設定**資料夾中。Horizon Agent 不會強制執行這些設定。Horizon Agent 會根據您指定合併 (m) 還是覆寫 (o) 修飾詞，將設定傳遞至 Horizon Client 進行解譯並強制執行。Horizon Client 會使用這些設定來決定是否將複合 USB 裝置分割成其元件裝置，以及是否將元件裝置排除在可供重新導向使用之外。如需 Horizon 如何套用分割複合 USB 裝置之原則的說明，請參閱設定複合 USB 裝置的裝置分割原則設定。

表 4-13. Horizon Agent 組態範本：裝置分割設定

設定	內容

`Allow Auto Device Splitting`
內容：
`AllowAutoDeviceSplitting`
	允許複合 USB 裝置的自動分割。
	該預設值未定義，其相當於 **`false`**。

`Exclude Vid/Pid Device from Split` 內容： `SplitExcludeVidPid`	排除依照廠商和產品識別碼指定的複合 USB 裝置，不進行分割。設定的格式為 {m|o}:vid-*xxx1*_pid-*yyy2*[;vid-*xxx2*_pid-*yyy2*]... 您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*****) 以取代個別數字。 例如：**o:vid-0781_pid-55**** 該預設值未定義。
`Split Vid/Pid Device` 內容： `SplitVidPid`	將依照廠商和產品識別碼指定的複合 USB 裝置元件視為個別裝置。設定的格式為 {m|o}:vid-*xxxx*_pid-*yyyy*(exintf:*zz*[;exintf:*ww*]) 或 {m|o}:vid-*xxxx*_pid-*yyyy*(exintf:*zz*[;exintf:*ww*]) 您可以使用 `exintf` 關鍵字，藉由指定他們的介面號碼來將元件自重新導向清單中排除。您必須以十六進位指定識別碼，及以十進位指定介面號碼，包括任何前置的 0。您可以在識別碼中使用萬用字元 (*****) 以取代個別數字。 例如：**o:vid-0781_pid-554c(exintf:01;exintf:02)** **備註** Horizon 7 不會自動包含您尚未明確排除的元件。您必須指定篩選原則，例如 `Include Vid/Pid Device`，以納入那些元件。 該預設值未定義。

Horizon Agent 強制執行的 USB 設定

下表說明在 Horizon Agent 組態 ADMX 範本檔中由每個代理程式強制執行的 USB 原則設定。這些設定全都位於群組原則管理編輯器的 **VMware Horizon Agent 組態 > View USB 組態**資料夾中。Horizon Agent 會使用這些設定來決定是否可以將某個 USB 裝置轉送至主機。Horizon Agent 也會根據您指定合併 (m) 還是覆寫 (o) 修飾詞，將設定傳遞至 Horizon Client 進行解譯並強制執行。Horizon Client 會使用這些設定來決定 USB 裝置是否可供重新導向使用。由於 Horizon Agent 一律會強制執行您所指定的代理程式強制執行原則設定，因此效果可能會抵銷您為 Horizon Client 設定的原則。如需 Horizon 7 如何套用 USB 裝置篩選原則的說明，請參閱設定 USB 裝置的篩選器原則設定。

表 4-14. Horizon Agent 組態範本：代理程式強制執行的設定

設定	內容
Exclude All Devices 內容： ExcludeAllDevices	將所有 USB 裝置排除在轉送之外。如果設為 **true**，您可以使用其他原則設定以允許轉送特定裝置或裝置系列。如果設為 **false**，您可以使用其他原則設定以防止轉送特定裝置或裝置系列。 如果設為 **true** 且傳遞至 Horizon Client，則此設定一律會覆寫 Horizon Client 上的設定。您無法搭配此設定使用合併 (m) 或複寫 (o) 修飾詞。 該預設值未定義，其相當於 **false**。
Exclude Device Family 內容： ExcludeFamily	將裝置系列排除在轉送之外。設定的格式為 {m|o}:*family_name_1*[;*family_name_2*]... 例如：**o:bluetooth;smart-card** 如果您已經啟用自動裝置分割，Horizon 7 會檢查複合 USB 裝置每個介面的裝置系列，以決定應該排除的介面。如果您已經停用自動裝置分割，Horizon 7 會檢查整個複合 USB 裝置的裝置系列。 該預設值未定義。
Exclude Vid/Pid Device 內容： ExcludeVidPid	將具有指定廠商和產品識別碼的裝置排除在轉送之外。設定的格式為 {m|o}:vid-*xxx1*_pid-*yyy2*[;vid-*xxx2*_pid-*yyy2*]... 您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 例如：**m:vid-0781_pid-****;vid-0561_pid-554c** 該預設值未定義。
Include Device Family 內容： IncludeFamily	包含可以轉送的裝置系列。設定的格式為 {m|o}:*family_name_1*[;*family_name_2*]... 例如：**m:storage** 該預設值未定義。
Include Vid/Pid Device 內容： IncludeVidPid	包含具有指定廠商和產品識別碼且可以轉送的裝置。設定的格式為 {m|o}:vid-*xxx1*_pid-*yyy2*[;vid-*xxx2*_pid-*yyy2*]... 您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 例如：**o:vid-0561_pid-554c** 該預設值未定義。

用戶端轉譯 USB 設定

下表說明在 Horizon Agent 組態 ADMX 範本檔中由用戶端解譯的每個原則設定。這些設定全都位於群組原則管理編輯器的 **VMware Horizon Agent 組態 > View USB 組態 > 僅供用戶端下載的設定**資料夾中。Horizon Agent 不會強制執行這些設定。Horizon Agent 會將這些設定傳遞至 Horizon Client 進行解譯並強制執行。Horizon Client 會使用這些設定來決定 USB 裝置是否可供重新導向使用。

表 4-15. Horizon Agent 組態範本：用戶端解譯的設定

設定	內容
Allow Audio Input Devices 內容： AllowAudioIn	允許轉送音訊輸入裝置。 該預設值未定義，其相當於 **true**。
Allow Audio Output Devices 內容： AllowAudioOut	允許轉送音訊輸出裝置。 該預設值未定義，其相當於 **false**。
Allow HID-Bootable 內容： AllowHIDBootable	允許轉送鍵盤和滑鼠以外，且可在開機時間使用的輸入裝置 (又稱為隱藏式可開機裝置)。 該預設值未定義，其相當於 **true**。

表 4-15. Horizon Agent 組態範本：用戶端解譯的設定 (續)

設定	內容
Allow Other Input Devices	允許轉送隱藏式可開機裝置或具備整合式指標裝置之鍵盤以外的輸入裝置。 該預設值未定義。
Allow Keyboard and Mouse Devices 內容： AllowKeyboardMouse	允許轉送具備整合式指標裝置 (例如滑鼠、軌跡球或觸控板) 的鍵盤。 該預設值未定義，其相當於 **false**。
Allow Smart Cards 內容： AllowSmartcard	允許轉送智慧卡裝置。 該預設值未定義，其相當於 **false**。
Allow Video Devices 內容： AllowVideo	允許轉送視訊裝置。 該預設值未定義，其相當於 **true**。

對 USB 重新導向問題進行疑難排解

Horizon Client 中的 USB 重新導向可能會發生各種問題。

問題

Horizon Client 中的 USB 重新導向無法將本機裝置提供給遠端桌面平台或應用程式使用，或是有些裝置無法在 Horizon Client 中重新導向。

原因

USB 重新導向可能基於下列原因而無法正確或如預期般運作。

- 裝置是複合 USB 裝置，並且預設會封鎖它包含的其中一個裝置。例如，預設會封鎖包含滑鼠的聽寫裝置，因為預設會封鎖滑鼠裝置。若要解決此問題，請參閱設定複合 USB 裝置的裝置分割原則設定。
- 部署已發佈桌面平台和應用程式的 Windows Server 2008 RDS 主機不支援 USB 重新導向。
- 裝置不適用於 USB 重新導向，或不支援使用已發佈桌面平台和應用程式。如需詳細資訊，請參閱 USB 裝置類型的相關限制。
- 不支援網路攝影機重新導向。
- USB 音訊裝置的重新導向取決於網路的狀態，而且並不可靠。即使處於閒置狀態，一些裝置仍需要高資料流量。
- 開機裝置不支援 USB 重新導向。若您在從 USB 裝置開機的 Windows 系統上執行 Horizon Client，且將此裝置重新導向至遠端桌面平台，則本機作業系統可能變得沒有反應或無法使用。請參閱 http://kb.vmware.com/kb/1021409。
- 依預設，Windows 版 Horizon Client 不允許您選取鍵盤、滑鼠、智慧卡和音訊輸出裝置來進行重新導向。請參閱 http://kb.vmware.com/kb/1011600。
- RDP 不支援主控台工作階段之 USB HID 的重新導向，也不支援智慧卡讀卡機的重新導向。請參閱 http://kb.vmware.com/kb/1011600。
- Windows Mobile 裝置中心可防止 RDP 工作階段之 USB 裝置重新導向。請參閱 http://kb.vmware.com/kb/1019205。

- 對於某些 USB HID，您必須對虛擬機器進行設定，以更新滑鼠指標位置。請參閱 http://kb.vmware.com/kb/1022076。
- 有些音訊裝置可能會要求對原則設定或登錄設定進行變更。請參閱 http://kb.vmware.com/kb/1023868。
- 網路延遲可能造成裝置互動緩慢，或導致設計為要與本機裝置互動的應用程式出現凍結的情形。容量非常大的 USB 磁碟機可能需要幾分鐘時間才會顯示在 Windows 檔案總管。
- 以 FAT32 檔案系統格式化的 USB Flash 卡載入速度遲緩。請參閱 http://kb.vmware.com/kb/1022836。
- 本機系統上的程序或服務在您連線至遠端桌面平台或應用程式之前已開啟裝置。
- 若您重新連接桌面平台或應用程式工作階段，即使桌面平台或應用程式顯示 USB 裝置是可用的，重新導向後的裝置仍會停止運作。
- USB 重新導向在 Horizon Administrator 中是停用的。
- 客體上遺失或停用的 USB 重新導向驅動程式。

解決方案

- 如果有的話，請使用 VMware Blast 或 PCoIP 而不是 RDP 做為通訊協定。
- 如果重新導向的裝置在暫時中斷連線後仍無法使用或停止運作，請移除裝置再重新插上，然後重試重新導向。
- 在 Horizon Administrator 中，移至**原則 > 全域原則**，確認 [View 原則] 下的 USB 存取是否設定為**允許**。
- 在客體的記錄中檢查 `ws_vhub` 類別的項目，並在用戶端的記錄中檢查 `vmware-view-usbd` 類別的項目。

  如果使用者不是管理員，或是 USB 重新導向驅動程式未安裝或無法運作，則會在記錄中寫入這些類別的項目。如需這些記錄檔的位置，請參閱使用記錄檔進行疑難排解及判定 USB 裝置識別碼。
- 在客體上開啟「裝置管理員」，展開「Universal Serial Bus controller」，如果 VMware View 虛擬 USB 主機控制器和 VMware View 虛擬 USB 集線器驅動程式已遺失，則重新安裝，如果已停用，則重新啟用。

為桌面平台和應用程式集區設定原則 5

您可以設定原則來控制桌面平台與應用程式集區、機器以及使用者的行為。您可以使用 Horizon Administrator 為用戶端工作階段設定原則。您可以使用 Active Directory 群組原則設定來控制 Horizon Agent、Windows 版 Horizon Client，以及影響單一使用者機器、RDS 主機、PCoIP 或 VMware Blast 之功能的行為。

本章節討論下列主題：

- Active Directory 群組原則範例

在 Horizon Administrator 中設定原則

您可以使用 Horizon Administrator 為用戶端工作階段設定原則。

您可以設定這些原則以影響特定使用者、特定桌面平台集區，或是所有用戶端工作階段使用者。會影響特定使用者和桌面平台集區的原則，稱為使用者層級原則和桌面平台集區層級原則。會影響所有工作階段和使用者的原則稱為廣域原則。

使用者層級原則會從等位的桌面平台集區層級原則設定繼承設定。同樣的，桌面平台集區層級原則會從等位的全域原則設定繼承設定。桌面平台集區層級原則設定優先於等位的全域原則設定。使用者層級原則設定優先於等位的全域和桌面平台集區層級原則設定。

層級較低的原則設定在限制方面，可能大於或小於層級較高的等位設定。例如，您可以將全域原則設定為**拒絕**，將等位的桌面平台集區層級原則設定為**允許**，反之亦然。

備註 僅全域原則適用於已發佈桌面平台和應用程式集區。您無法為已發佈桌面平台和應用程式集區設定使用者層級原則或集區層級原則。

設定全域原則設定

您也可設定全域原則控制所有用戶端工作階段使用者的行為。

必要條件

自行熟悉原則說明。請參閱 Horizon 7 原則。

程序

1 在 Horizon Administrator 中，選取**原則 > 全域原則**。

2 按一下 **View 原則**窗格中的**編輯原則**。

3 按一下**確定**儲存變更。

設定桌面平台集區的原則

您可以設定桌面平台層級原則影響特定桌面平台集區。桌面平台層級原則設定優先於等位的全域原則設定。

必要條件

自行熟悉原則說明。請參閱 Horizon 7 原則。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > 桌面平台集區**。

2 按兩下桌面平台集區的識別碼，然後按一下**原則**索引標籤。

原則索引標籤隨即顯示目前的原則設定。從等位的全域原則繼承設定時，**繼承**將出現在**桌面平台集區原則**欄中。

3 按一下 **View 原則**窗格中的**編輯原則**。

4 按一下**確定**儲存變更。

設定使用者原則

您可以設定使用者層級原則影響特定使用者。使用者層級原則設定始終優先於等位的全域及桌面平台集區層級原則設定。

必要條件

自行熟悉原則說明。請參閱 Horizon 7 原則。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > 桌面平台集區**。

2 按兩下桌面平台集區的識別碼，然後按一下**原則**索引標籤。

原則索引標籤隨即顯示目前的原則設定。從等位的全域原則繼承設定時，**繼承**將出現在**桌面平台集區原則**欄中。

3 按一下**使用者覆寫**，然後按一下**新增使用者**。

4 若要尋找使用者，請按一下**新增**，並輸入使用者的名稱或說明，然後按一下**尋找**。

5 從清單中選取一個或多個使用者，並按一下**確定**，然後按**下一步**。

「新增個別原則」對話方塊隨即出現。

6 設定 Horizon 原則並按一下**完成**，以儲存您的變更。

Horizon 7 原則

您可以將設定 Horizon 7 原則以影響所有用戶端工作階段，或是套用這些原則來影響特定桌面平台或使用者。

下表說明每個 Horizon 7 原則設定。

表 5-1. Horizon 原則

原則	說明
多媒體重新導向 (MMR)	決定是否啟用用戶端系統的 MMR。 MMR 是一種 Windows Media Foundation 篩選器，會將遠端桌面平台上特定轉碼器中的多媒體資料直接透過 TCP 通訊端轉送給用戶端系統。然後，當播放時，該資料會在用戶端系統上直接解碼。 預設值為**拒絕**。 如果用戶端系統的資源不足，無法處理本機多媒體解碼，請將設定保留為**拒絕**。 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。
USB 存取	決定遠端桌面平台是否可以使用連線至用戶端系統的 USB 裝置。 預設值為**允許**。基於安全理由，為避免使用外接裝置，請將設定變更為**拒絕**。
PCoIP 硬體加速	決定是否啟用 PCoIP 顯示通訊協定的硬體加速，並指定指派給 PCoIP 使用者工作階段的加速優先順序。 此設定只有在主控遠端桌面平台的實體電腦上有 PCoIP 硬體加速裝置時才有作用。 預設值為**允許**，優先順序為**中**。

使用 智慧原則

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

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

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

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

智慧原則的需求

若要使用智慧原則，您的 Horizon 7 環境必須符合特定需求。

- 您必須在想以智慧原則管理的遠端桌面平台上安裝 Horizon Agent 7.0 或更新版本以及 VMware Dynamic Environment Manager 9.0 或更新版本。
- 使用者必須使用 Horizon Client 4.0 或更新版本連線至您想以智慧原則管理的遠端桌面平台。

安裝 Dynamic Environment Manager

若要使用智慧原則來控制遠端桌面平台上的遠端桌面平台功能行為，您必須在遠端桌面平台上安裝 Dynamic Environment Manager 9.0 或更新版本。

您可以從 VMware 下載頁面下載 Dynamic Environment Manager 安裝程式。您必須在要以 Dynamic Environment Manager 管理的每個遠端桌面平台上安裝 VMware DEM FlexEngine。您可在想要從其管理 Dynamic Environment Manager 環境的桌面平台上安裝 Dynamic Environment Manager 管理主控台元件。

對於已發佈桌面平台集區，則必須在提供已發佈桌面平台工作階段的 RDS 主機上安裝 Dynamic Environment Manager。

如需 Dynamic Environment Manager 系統需求與完整安裝指示，請參閱《安裝和設定 VMware Dynamic Environment Manager》文件。

設定 Dynamic Environment Manager

您必須先設定 Dynamic Environment Manager，才能將其用來建立遠端桌面平台功能的智慧型原則。

若要設定 Dynamic Environment Manager，請遵照《VMware Dynamic Environment Manager 管理指南》中的組態指示來進行。以下組態步驟可補充該文件資訊的不足之處。

若要設定 Dynamic Environment Manager，請遵照《VMware Dynamic Environment Manager 管理指南》中的組態指示來進行。

- 在遠端桌面平台上設定 VMware DEM FlexEngine 用戶端元件時，請建立 FlexEngine 登入和登出指令碼。適用於多個工作階段。例如 RDSH 桌面平台和 RDSH 應用程式，或針對相同 RDSH 主機上相同使用者的多個 RDSH 應用程式工作階段，請在登入指令碼中使用 **–HorizonViewMultiSession–r** 參數。對於登出指令碼，請使用 **–HorizonViewMultiSession–s** 參數。

  備註 請勿使用登入指令碼啟動遠端桌面平台上的其他應用程式。額外的登入指令碼會讓遠端桌面平台登入作業延遲多達 10 分鐘。

- 在遠端桌面平台上啟用使用者群組原則設定**同步執行登入指令檔**。此設定位於**使用者設定\原則\系統管理範本\系統\指令碼**資料夾中。
- 在遠端桌面平台上啟用電腦群組原則設定**永遠在電腦啟動及登入時等待網路啟動**。此設定位於**電腦設定\系統管理範本\系統\登入**資料夾中。
- 若使用 Windows 8.1 遠端桌面平台，請停用電腦群組原則設定**設定登入指令碼延遲**。此設定位於**電腦設定\系統管理範本\系統\\群組原則**資料夾中。
- 若要確保系統會在使用者連線到桌面平台工作階段時重新整理 Horizon 智慧型原則設定，請使用 Dynamic Environment Manager 管理主控台來建立觸發的工作。將觸發設定為**重新連線工作階段**、將動作設定為 **User Environment 重新整理**，然後選取適用於重新整理的 **Horizon 智慧型原則**。

  備註 如果您在使用者已登入遠端桌面平台時建立觸發的工作，使用者必須先從桌面平台登出，觸發的工作才會生效。

Horizon 智慧型原則設定

您可建立 Horizon 智慧型原則，藉以控制 Dynamic Environment Manager 中遠端功能的行為。

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

您可以為 Dynamic Environment Manager 在使用者電腦開機時套用的電腦環境設定建立原則。這些 Horizon 智慧型原則會控制 Flash 多媒體重新導向、Integrated Printing 和 USB 重新導向的行為。電腦環境設定的 Horizon 智慧型原則會在電腦開機期間套用，且可在工作階段重新連線期間重新整理。請參閱《VMware Dynamic Environment Manager 管理指南》中的「設定電腦環境設定的 Horizon 智慧型原則」主題中的完整原則清單。

一般來說，為 Dynamic Environment Manager 中的遠端功能設定的 Horizon 智慧型原則設定，會覆寫對等的登錄機碼以及群組原則設定。

頻寬設定檔參考

透過智慧型原則，您將可使用 Bandwidth profile 原則設定，為遠端桌面平台上的 PCoIP 或 Blast 工作階段設定頻寬設定檔。

表 5-2. 頻寬設定檔

頻寬設定檔	最大工作階段 BW (Kbps)	最小工作階段 BW (Kbps)	啟用不失真 (BTL)	最大初始影像畫質	最小映像畫質	最大 FPS	最大音訊 BW (Kbps)	影像畫質效能
高速 LAN	900000	64	是	100	50	60	1600	50
LAN	900000	64	是	90	50	30	1600	50
專用 WAN	900000	64	否	80	40	30	500	50
寬頻 WAN	5000	64	否	70	40	20	500	50
低速 WAN	2000	64	否	70	30	15	200	25
極低速連線	1000	64	否	70	30	10	90	0

將條件新增至 Horizon 智慧型原則定義

在 Dynamic Environment Manager 中定義 Horizon 智慧型原則時，可新增必須符合才能讓原則生效的條件。例如，您可以新增只會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的條件。

您可以針對同一個遠端桌面平台功能新增多個條件。例如，您可以新增一個條件，以在使用者屬於 HR 群組的成員時啟用本機列印，並新增另一個條件，在遠端桌面平台位於 Win7 集區中時啟用本機列印。

如需在 Dynamic Environment Manager 管理主控台中新增和編輯條件的詳細資訊，請參閱《VMware Dynamic Environment Manager 管理指南》。

使用 Horizon Client 內容條件

使用者連線或重新連線至遠端桌面平台時，Horizon Client 將收集有關用戶端電腦的資訊，而且連線伺服器會將這些資訊傳送至遠端桌面平台。您可以將 Horizon Client 內容條件新增至 Horizon 原則定義中，依照遠端桌面平台所收到的資訊控制原則生效的時機。

備註 只有當使用者使用 PCoIP 顯示通訊協定或 VMware Blast 顯示通訊協定啟動遠端桌面平台時，Horizon Client 內容條件才會生效。若使用者使用 RDP 顯示通訊協定啟動遠端桌面平台，Horizon Client 原則條件將不會生效。

表 5-3. Horizon Client 內容條件的預先定義內容 說明當您使用 Horizon Client 內容條件時，可從**內容**下拉式功能表中選取的預先定義內容。各預先定義內容都對應一個 `ViewClient_` 登錄機碼。

表 5-3. Horizon Client 內容條件的預先定義內容

內容	對應的登錄機碼	說明
用戶端位置	`ViewClient_Broker_GatewayLocation`	指定使用者用戶端系統的位置。有效值如下： ■ Internal - 只有當使用者從公司網路內部連線至遠端桌面平台時，原則才會生效。 ■ External - 只有當使用者從公司網路外部連線至遠端桌面平台時，原則才會生效。 如需設定連線伺服器或安全伺服器主機之閘道位置的相關資訊，請參閱《Horizon 7 管理》文件。 如需設定 Access Point 應用裝置之閘道位置的相關資訊，請參閱《部署及設定 Unified Access Gateway》文件。
啟動標記	`ViewClient_Launch_Matched_Tags`	指定一或多個標記。使用逗號或分號分隔多個標記。只有在可讓遠端桌面平台或應用程式啟動的標記符合其中一個指定標記時，原則才會生效。 如需將標記指派給連線伺服器執行個體和桌面平台集區的相關資訊，請參閱您的《設定》文件。
集區名稱	`ViewClient_Launch_ID`	指定桌面平台或應用程式集區識別碼。只有當使用者在啟動遠端桌面平台或應用程式時所選取的桌面平台或應用程式集區的識別碼符合指定的桌面平台或應用程式集區識別碼時，原則才會生效。例如，若使用者選取 Win7 集區，且此內容設為 Win7，原則將會生效。 **備註** 如果在相同的 RDS 主機工作階段中啟動了多個應用程式集區，則值會是第一個從 Horizon Client 啟動之應用程式的識別碼。

內容下拉式功能表也是文字方塊，因此您可以在文字方塊中手動輸入任何 `ViewClient_` 登錄機碼。在輸入登錄機碼時，請勿包含 `ViewClient_` 這個前置詞。例如，若要指定 `ViewClient_Broker_URL`，請輸入 `Broker_URL`。

您可以使用遠端桌面平台上的 Windows 登錄編輯程式 (`regedit.exe`) 來檢視 `ViewClient_` 登錄機碼。Horizon Client 會將用戶端電腦資訊寫入部署在單一使用者機器上之遠端桌面平台上的系統登錄路徑 `HKEY_CURRENT_USER\Volatile Environment`。對於在 RDS 工作階段中部署的遠端桌面平台，Horizon Client 會將用戶端電腦資訊寫入系統登錄路徑 `HKEY_CURRENT_USER\Volatile Environment\`*x*，其中 *x* 是 RDS 主機上的工作階段識別碼。

使用其他條件

Dynamic Environment Manager 管理主控台提供許多條件。在建立遠端桌面平台功能的原則時，下列條件將會特別有用。

群組成員	您可以使用此條件，將原則設定為只在使用者屬於特定群組的成員時生效。
遠端顯示通訊協定	您可以使用此條件，將原則設定為只在使用者選取特殊顯示通訊協定時生效。條件設定包括 RDP、PCoIP 和 Blast。
IP 位址	您可以使用此條件，將原則設定為只在使用者從公司網路內部或外部連線時生效。使用條件設定可指定內部 IP 位址範圍或外部 IP 位址範圍。

備註 您也可以在 Horizon Client 內容條件中使用**用戶端位置**內容。

如需所有可用條件的說明，請參閱《VMware Dynamic Environment Manager 管理指南》文件。

在 Dynamic Environment Manager 中建立 Horizon 智慧型原則

您可以使用 Dynamic Environment Manager 管理主控台在 Dynamic Environment Manager 中建立 Horizon 智慧型原則。在定義 Horizon 智慧型原則時，可新增必須符合才能讓智慧型原則生效的條件。

必要條件

- 安裝和設定 Dynamic Environment Manager。請參閱安裝 Dynamic Environment Manager 與設定 Dynamic Environment Manager。
- 熟悉 Horizon 智慧型原則設定。請參閱 Horizon 智慧型原則設定。
- 熟悉可新增至 Horizon 智慧型原則定義的條件。請參閱將條件新增至 Horizon 智慧型原則定義。

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

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

如需使用 Dynamic Environment Manager 管理主控台的完整資訊，請參閱《VMware Dynamic Environment Manager 管理指南》文件。

程序

1 在 Dynamic Environment Manager 管理主控台中，選取**使用者環境**以建立使用者環境設定的原則，或選取**電腦環境**索引標籤以建立電腦環境設定的原則。

   現有 Horizon 智慧型原則定義 (若有) 會出現在 [Horizon 智慧型原則] 窗格中。

2 選取 **Horizon 智慧型原則**，然後按一下**建立**，以建立新的智慧型原則。

3 選取**設定**索引標籤，然後定義智慧型原則設定。

   a 在 [一般設定] 區段中，於**名稱**文字方塊中輸入智慧型原則的名稱。

   例如，若智慧型原則會影響用戶端磁碟機重新導向功能，可將智慧型原則命名為 CDR。

   b 在 [Horizon 智慧型原則設定] 區段中，選取要包括在智慧型原則中的遠端桌面平台功能和設定。

   您可以選取多個遠端桌面平台功能。

4 (選擇性) 若要在智慧型原則中新增條件，請選取**條件**索引標籤、按一下**新增**，然後選取條件。

   您可以在智慧型原則定義中新增多個條件。

5 按一下**儲存**以儲存智慧型原則。

Dynamic Environment Manager 會在每次使用者連線或重新連線到遠端桌面平台時處理 Horizon 智慧型原則。

Dynamic Environment Manager 會按照智慧型原則名稱的字母順序處理多個智慧型原則。Horizon 智慧型原則會按照字母順序出現在 [Horizon 智慧型原則] 窗格中。若智慧型原則互有衝突，則最後處理的智慧型原則會優先獲得採用。例如，若有一個名稱為 Sue 的智慧型原則會對名稱為 Sue 的使用者啟用 USB 重新導向，以及另一個名稱為 Pool 的智慧型原則會對名稱為 Win7 的桌面平台集區停用 USB 重新導向，則當 Sue 連線到 Win7 桌面平台集區的遠端桌面平台時，將會啟用 USB 重新導向功能。

使用 Active Directory 群組原則

您可以使用 Microsoft Windows 群組原則來最佳化及保護遠端桌面平台的安全、控制 Horizon 7 元件的行為，以及設定依據位置列印。

「群組原則」是 Microsoft Windows 作業系統的其中一個功能，可針對 Active Directory 環境中的電腦和遠端使用者，提供集中式管理與組態。

群組原則設定包含在稱為群組原則物件 (GPO) 的實體中。GPO 與 Active Directory 物件相關聯。您可以將 GPO 套用至全網域層級的 Horizon 7 元件，以控制 Horizon 7 環境的不同區域。套用之後，GPO 設定會儲存在指定元件的本機 Windows 登錄中。

您可以使用 Microsoft Windows 群組原則物件編輯器來管理群組原則設定。「群組原則物件編輯器」是一種 Microsoft Management Console (MMC) 嵌入式管理單元。MMC 是 Microsoft Group Policy Management Console (GPMC) 的一部分。如需安裝與使用 GPMC 的相關資訊，請參閱 Microsoft TechNet 網站。

為遠端桌面平台建立 OU

請針對遠端桌面平台在 Active Directory 中建立組織單位 (OU)。

若要避免群組原則設定套用至與您遠端桌面平台相同網域中的其他 Windows 伺服器或工作站，請為 Horizon 7 群組原則建立 GPO，並將其連結至包含遠端桌面平台的 OU。

請參閱 Microsoft TechNet 網站上的 Microsoft Active Directory 文件，以取得建立 OU 和 GPO 的相關資訊。

啟用遠端桌面平台的回送處理

依預設，使用者的原則設定來自 GPO 集，這些 GPO 套用至 Active Directory 中的使用者物件。不過，在 Horizon 7 環境中，GPO 會根據使用者所登入的電腦套用至使用者。

當您啟用回送處理時，一致的原則集會套用到所有登入特定電腦的使用者，無論他們在 Active Directory 中的位置為何。

如需啟用回送處理的相關資訊，請參閱 Microsoft Active Directory 文件。

備註 回送處理是在 Horizon 7 中處理 GPO 的唯一方法。您可能需要實作不同的方法。

使用 Horizon 7 群組原則管理範本檔

Horizon 7 提供數個元件專屬的群組原則管理 ADMX 範本檔。您可以將 ADMX 範本檔中的原則設定新增至 Active Directory 中新的或現有的 GPO，藉以最佳化及保護遠端桌面平台和應用程式的安全。

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

Horizon 7 ADMX 範本檔包含「電腦組態」與「使用者組態」群組原則。

- 「電腦組態」原則所設定的原則會套用至所有遠端桌面平台，不論誰連線到桌面平台都一樣。
- 「使用者組態」原則所設定的原則會套用至所有使用者，不論他們連線到哪個遠端桌面平台或應用程式都一樣。「使用者組態」原則會覆寫對等的「電腦組態」原則。

Microsoft Windows 會在桌面平台啟動及使用者登入時套用原則。

Horizon 7 ADMX 範本檔

Horizon 7 ADMX 範本檔提供可讓您控制及最佳化 Horizon 7 元件的群組原則設定。

ADMX 檔案可從 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 中取得，而您可以從 VMware 下載網站下載該 zip 檔案，網址為 https://my.vmware.com/web/vmware/downloads。在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含 ZIP 檔案。

表 5-4. Horizon ADMX 範本檔

範本名稱	範本檔	說明
VMware View Agent 組態	`vdm_agent.admx`	包含有關 Horizon Agent 之驗證與環境元件的原則設定。
VMware Horizon Client 組態	`vdm_client.admx`	包含與 Windows 版 Horizon Client 有關的原則設定。 從連線伺服器主機網域外部進行連線的用戶端，不會受到套用至 Horizon Client 的原則影響。 請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。

表 5-4. Horizon ADMX 範本檔 (續)

範本名稱	範本檔	說明
VMware Horizon URL 重新導向	urlRedirection.admx	包含與 URL 內容重新導向功能相關的原則設定。如果將此範本新增至遠端桌面平台集區或應用程式集區的 GPO，則在遠端桌面平台或應用程式內部點選的某些 URL 連結會重新導向至 Windows 用戶端，並在用戶端瀏覽器中開啟。 如果將此範本新增至用戶端 GPO，則當使用者在 Windows 用戶端系統中點選某些 URL 連結，該 URL 可在遠端桌面平台或應用程式中開啟。 請參閱第 3 章 設定 URL 內容重新導向和《Windows 版 VMware Horizon Client 安裝和設定指南》文件。
VMware View Server 組態	vdm_server.admx	包含與連線伺服器有關的原則設定。 請參閱《View 管理》文件。
VMware View 一般組態	vdm_common.admx	包含所有 Horizon 元件通用的原則設定。 請參閱《View 管理》文件。
PCoIP 工作階段變數	pcoip.admx	包含與 PCoIP 顯示通訊協定有關的原則設定。
PCoIP 用戶端工作階段變數	pcoip.client.admx	包含與 PCoIP 顯示通訊協定 (影響 Windows 版 Horizon Client) 有關的原則設定。 請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。
角色管理	ViewPM.admx	包含與 Horizon Persona Management 有關的原則設定。 請參閱《在 Horizon 7 中設定虛擬桌面平台》文件。
VMware 虛擬列印重新導向	printerRedirection.admx	包含用於停用依據位置列印、停用列印設定持續性，以及為已重新導向用戶端印表機選取印表機驅動程式的原則設定。
依據位置列印	LBP.xml	用於為每個依據位置印表機針對 VMware 虛擬列印定義轉譯規則的範本。
View RTAV 組態	vdm_agent_rtav.admx	包含有關與即時音訊視訊功能搭配使用的網路攝影機的原則設定。 請參閱即時音訊視訊群組原則設定 。
掃描器重新導向	vdm_agent_scanner.admx	包含與重新導向以在已發佈的桌面平台和應用程式中使用的掃描裝置有關的原則設定。 請參閱掃描器重新導向群組原則設定。
序列 COM	vdm_agent_serialport.admx	包含與重新導向以在虛擬桌面平台中使用的序列 (COM) 連接埠有關的原則設定。 請參閱序列埠重新導向群組原則設定。
VMware Horizon 印表機重新導向	vdm_agent_printing.admx	包含與篩選重新導向的印表機有關的原則設定。 請參閱篩選虛擬列印的印表機。
View Agent Direct-Connection	view_agent_direct_connection.admx	包含與 View Agent Direct-Connection 外掛程式相關的原則設定。請參閱《View Agent Direct-Connection 外掛程式管理》文件。

表 5-4. Horizon ADMX 範本檔 (續)

範本名稱	範本檔	說明
VMware Horizon 效能追蹤程式	`perf_tracker.admx`	包含與 VMware Horizon 效能追蹤程式功能相關的原則設定。 請參閱 VMware Horizon 效能追蹤程式原則設定。
VMware Horizon Client 用戶端磁碟機重新導向	`vdm_agent_cdr.admx`	包含與用戶端磁碟機重新導向功能相關的原則設定。 請參閱使用群組原則來設定磁碟機代號行為。

將 ADMX 範本檔新增至 Active Directory

您可以將 Horizon 7 ADMX 檔案中特定遠端桌面平台功能的原則設定新增至 Active Directory 中的群組原則物件 (GPO)。

必要條件

- 確認已在虛擬機器桌面平台和 RDS 主機上安裝要套用原則之遠端桌面平台功能的設定選項。如果未安裝遠端桌面平台功能，則群組原則設定沒有任何作用。如需安裝 Horizon Agent 的相關資訊，請參閱您的《設定》文件。
- 為要套用群組原則設定的遠端桌面平台功能建立 GPO，並將其連結至包含虛擬機器桌面平台或 RDS 主機的 OU。
- 確認要新增至 Active Directory 之 ADMX 範本檔的名稱。請參閱 Horizon 7 ADMX 範本檔。
- 確認可以在 Active Directory 伺服器上使用群組原則管理功能。

程序

1. 從 VMware 下載網站下載 Horizon 7 GPO 服務包 `.zip` 檔案，網址為 https://my.vmware.com/web/vmware/downloads。

   在「桌面平台及使用者運算」下，選取 VMware Horizon 7 下載，其中包含 GPO 服務包。

   該檔案名為 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`，其中 *x.x.x* 為版本，而 *yyyyyyy* 為組建編號。為 Horizon 7 提供群組原則設定的所有 ADMX 檔案皆可從此檔案取得。

2. 解壓縮 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` 檔案，並將 ADMX 檔案複製到您的 Active Directory 伺服器。

   a. 將 `.admx` 檔案和 `en-US` 資料夾複製到 Active Directory 伺服器上的 `%systemroot%\PolicyDefinitions` 資料夾。

   b. 將語言資源檔案 (`.adml`) 複製到 Active Directory 伺服器上 `%systemroot%\PolicyDefinitions\` 下的適當子資料夾中。

3. 在 Active Directory 伺服器上開啟群組原則管理編輯器，然後輸入範本檔在安裝後出現於編輯器中的路徑。

後續步驟

設定群組原則設定。

VMware View Agent 組態 ADMX 範本設定

VMware View Agent 組態 ADMX 範本檔 (vdm_agent.admx) 包含與 Horizon Agent 的驗證和環境元件有關的原則設定。

ADMX 檔案可從 VMware-Horizon-Extras-Bundle-*x.x.x-yyyyyyy*.zip 中取得，而您可以從 VMware 下載網站下載該 zip 檔案，網址為 https://my.vmware.com/web/vmware/downloads。在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含 ZIP 檔案。

下表說明 VMware View Agent 組態 ADMX 範本檔中的原則設定。範本包含「電腦組態」與「使用者組態」設定。「使用者組態」設定會覆寫對等的「電腦組態」設定。

代理程式組態設定

代理程式組態設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 代理程式組態**資料夾中。

表 5-5. 代理程式組態原則設定

設定	電腦	使用者	內容
AllowDirectRDP	X		決定 Horizon Client 裝置之外的用戶端是否可以使用 RDP 直接連線至遠端桌面平台。停用此設定時，代理程式僅允許受 Horizon 管理的連線通過 Horizon Client。 從 Mac 版 Horizon Client 連線至遠端桌面平台時，請勿停用 AllowDirectRDP 設定。如果停用此設定，則連線會失敗，並出現拒絕存取錯誤。 依預設，使用者登入遠端桌面工作階段時，您可以使用 RDP 連線至虛擬機器。RDP 連線會終止遠端桌面工作階段，且使用者未儲存的資料和設定可能會遺失。在關閉外部 RDP 連線前，使用者無法登入桌面平台。要避免發生此情況，停用 AllowDirectRDP 設定。 **重要** Windows 遠端桌面服務必須在每個桌面平台的客體作業系統上執行。您可以使用此設定，防止使用者建立 RDP 與其桌面平台的直接連線。 此設定依預設為啟用。
AllowSingleSignon	X		決定是否使用單一登入 (SSO) 將使用者連線至桌面平台和應用程式。若啟用此設定，當使用者登入伺服器時，只需要輸入一次認證。若停用此設定，當使用者進行遠端連線時，則必須重新驗證。 此設定依預設為啟用。
CommandsToRunOnConnect	X		指定首次連線某個工作階段時，要執行的命令或命令指令碼的清單。 如需詳細資訊，請參閱在 Horizon 桌面平台上執行命令。
CommandsToRunOnDisconnect	X		指定某個工作階段中斷連線時，要執行的命令或命令指令碼的清單。 如需詳細資訊，請參閱在 Horizon 桌面平台上執行命令。
CommandsToRunOnReconnect	X		指定某個工作階段中斷連線後重新連線時，要執行的命令或命令指令碼的清單。 如需詳細資訊，請參閱在 Horizon 桌面平台上執行命令。

表 5-5. 代理程式組態原則設定 (續)

設定	電腦	使用者	內容
ConnectionTicketTimeout	X		指定 Horizon 連線票證的有效時間長度 (以秒為單位)。 Horizon Client 裝置在連線至代理程式時，會使用連線票證以進行驗證和單一登入。基於安全理由，連線票證的有效時間長度是有限的。當使用者連線至遠端桌面平台時，在連線票證逾時期間內必須進行驗證，否則工作階段會逾時。如果未設定此設定，則預設的逾時期間為 900 秒。
CredentialFilterExceptions	X		指定不允許載入代理程式 CredentialFilter 的執行檔。檔案名稱不得包含路徑或尾碼。使用分號分隔多個檔案名稱。
Disable Time Zone Synchronization	X	X	決定遠端桌面平台的時區是否與連線之用戶端的時區同步。僅在 Horizon Client 組態原則的 Disable time zone forwarding 設定未設為停用時，才會套用啟用的設定。 此設定依預設為停用。
Disconnect Session Time Limit (VDI)	X		指定中斷連線的桌面平台工作階段將自動登出的時間量。 ■ **永不**：此機器上已中斷連線的工作階段將永遠不會登出。 ■ **立即**：已中斷連線的工作階段將立即登出。 您也可以在 Horizon Administrator 或 Horizon Console 的桌面平台集區設定**中斷連線後自動登出**中設定逾時。如果同時在這兩個位置設定了此設定，將會優先採用 GPO 值。 例如，無論在 Horizon Administrator 或 Horizon Console 中的設定為何，若在此處選取**永不**，皆會使此機器上已中斷連線的工作階段不會登出。
DPI Synchronization	X	X	調整遠端工作階段的全系統 DPI 設定。此設定啟用或未設定時，會將遠端工作階段的全系統 DPI 設定設為符合用戶端作業系統上對應的 DPI 設定。停用此設定時，遠端工作階段的全系統 DPI 設定絕不會變更。 如需支援的客體作業系統清單，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》說明文件中的〈使用 DPI 同步〉主題。 此設定依預設為啟用。
DPI Synchronization Per Connection	X	X	決定當使用者重新連線至遠端工作階段時，是否要調整顯示器 DPI 設定。 如果啟用，此設定會在使用者重新連線至遠端工作階段時，將顯示器 DPI 設定為符合用戶端系統上的 DPI 設定。也必須啟用 DPI Synchronization 設定。 如果停用或未設定，當使用者重新連線至遠端工作階段時，此設定不會變更顯示器 DPI 設定。 如需支援的客體作業系統清單，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》說明文件中的〈使用 DPI 同步〉主題。 此設定依預設為停用。

表 5-5. 代理程式組態原則設定 (續)

設定	電腦	使用者	內容
Enable Battery State Redirection	X		決定是否啟用電池狀態重新導向。Windows 和 Linux 用戶端系統均支援此功能。 此設定啟用時，Windows 或 Linux 用戶端系統電池的相關資訊會重新導向至 Windows 遠端桌面平台。在遠端桌面平台上，系統匣中的電池圖示會指出電池的充電百分比。如果電池電量低於或等於 10%，則會彈出一則訊息，指出電池電量不足。 此設定依預設為啟用。
Enable multi-media acceleration	X		決定是否在遠端桌面平台上啟用多媒體重新導向 (MMR)。 MMR 是一種 Windows Media Foundation 篩選器，會將遠端系統上特定轉碼器中的多媒體資料直接透過 TCP 通訊端轉送給用戶端。然後，當播放時，該資料會在用戶端上直接解碼。如果用戶端沒有足夠資源可處理本機多媒體解碼，您可以停用 MMR。 此設定依預設為啟用。
Enable Unauthenticated Access	X		啟用或停用未驗證存取功能。此設定啟用時，未驗證存取使用者不需要 AD 認證即可從 Horizon Client 存取已發佈的應用程式。此設定停用時，未驗證存取使用者必須要有 AD 認證，才可從 Horizon Client 存取已發佈的應用程式。 您必須將 RDS 主機重新開機，此設定才會生效。 此設定依預設為啟用。
Force MMR to use software overlay	X		MMR 會嘗試使用硬體重疊播放視訊以提升效能。使用多個顯示器時，硬體重疊只會存在於其中一個顯示器上，即主要顯示器或啟動 WMP 的顯示器。如果將 WMP 拖曳到其他顯示器，則視訊將會呈現為黑色矩形。使用此選項，可強制 MMR 使用可在所有顯示器上運作的軟體重疊。 此設定依預設為啟用。
Idle Time Until Disconnect (VDI)	X		指定桌面平台工作階段因使用者閒置而中斷連線的時間量。 如果此設定停用、未設定，或在設定了**永不**的情況下啟用，桌面平台工作階段將一律不會中斷連線。 如果桌面平台集區或機器已設定為在中斷連線後自動登出，則會接受該設定。
ShowDiskActivityIcon	X		本版本不支援此設定。
Single sign-on retry timeout	X		指定重試 Single Sign-On 之前的等待時間 (以毫秒為單位)。將此值設為 0，即會停用 Single Sign-On 重試。預設值為 5000 毫秒。 此設定依預設為啟用。
Toggle Display Settings Control	X		決定當用戶端工作階段使用 PCoIP 顯示通訊協定時，是否停用**顯示**控制台中的**設定**索引標籤。 此設定依預設為啟用。

備註 Horizon6 (6.1 版) 版本中已移除 Connect using DNS Name 設定。您可以設定 Horizon 7LDAP 屬性 **pae-PreferDNS**，指示連線伺服器在將桌面平台機器和 RDS 主機的位址傳送到用戶端和閘道時優先使用 DNS 名稱。請參閱《Horizon 7 安裝》文件中的〈當 Horizon 連線伺服器傳回位址資訊時優先使用 DNS 名稱〉。

代理程式安全性設定

代理程式安全性設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 代理程式安全性**資料夾中。

表 5-6. 代理程式安全性原則設定

設定	電腦	使用者	內容
Accept SSL encrypted framework channel		X	啟用採用 TLS 加密的架構通道。可用選項如下： ■ **停用** - 停用 TLS。 ■ **啟用** - 啟用 TLS。允許舊版用戶端在不使用 TLS 的情況下連線。 ■ **強制執行** - 啟用 TLS。拒絕舊版用戶端連線。 此設定依預設為啟用。

工作階段協作設定

工作階段協作設定位於群組原則管理編輯器中的 **VMware View Agent 組態 > 協作**資料夾中。請參閱工作階段協作原則設定。

角色管理設定

角色管理設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 角色管理**資料夾中。請參閱在 Horizon 7 中設定虛擬桌面平台文件。

掃描器重新導向設定

掃描器重新導向設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 掃描器重新導向**資料夾中。請參閱掃描器重新導向群組原則設定。

序列 COM 設定

序列 COM 設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 序列 COM** 資料夾中。請參閱序列埠重新導向群組原則設定。

智慧卡重新導向設定

智慧卡重新導向設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 智慧卡重新導向 > 本機讀卡機存取**資料夾中。

表 5-7. 智慧卡重新導向原則設定

設定	電腦	使用者	內容
Allow applications access to Local Smart Card readers	X		若啟用，應用程式能夠存取所有本機智慧卡讀卡機 (即使已安裝智慧卡重新導向功能)。啟用時，系統會監控桌面平台是否有本機讀卡機，若偵測到，則會關閉智慧卡重新導向以允許存取本機讀卡機。重新導向會維持關閉，直到使用者下次連線至工作階段。啟用本機存取時，應用程式將再也無法存取用戶端上的遠端讀卡機。 啟用遠端桌面服務角色時，此設定不適用於 RDP 或 RDS 主機。 此設定依預設為停用。
Local Reader Name	X		指定要監控之本機讀卡機的名稱，以便啟用本機存取。依預設，讀卡機必須已插入卡片才能啟用本機存取。您可以使用 Require an inserted Smart Card 設定來停用此需求。 此設定依預設為啟用。
Require an inserted Smart Card	X		若啟用，則僅在本機讀卡機已插入卡片時才會啟用本機讀卡機存取權。若停用，則只要偵測到本機讀卡機便會啟用本機存取。 此設定依預設為啟用。

True SSO 組態設定

True SSO 組態設定設定位於群組原則管理編輯器的 **VMware View Agent 組態 > True SSO 組態**資料夾中。請參閱《Horizon 7 管理》文件。

Unity Touch 和主控應用程式設定

Unity Touch 和主控應用程式的設定位於群組原則管理編輯器的 **VMware View Agent 組態 > Unity Touch 和主控應用程式**資料夾中。

表 5-8. Unity Touch 和主控應用程式原則設定

設定	電腦	使用者	內容
Send updates for empty or offscreen windows	X		指定用戶端是否會收到關於空視窗或幕後視窗的更新。此設定停用時，小於 2x2 像素或完全位於幕後的視窗，將不會有相關資訊傳送至用戶端。 此設定依預設為停用。
Enable UWP support on RDSH platforms	X		啟用時，通用 Windows 平台 (UWP) 應用程式可以在 Azure 上 Horizon Cloud Service 所主控的 Windows 10 虛擬桌面平台 (WVD) 主機上執行。停用時，應用程式狀態會在 Horizon Agent 中顯示為無法使用，且使用者將無法存取應用程式。重新啟動代理程式虛擬機器後，此設定才會生效。 此設定依預設為停用。
Enable Unity Touch	X		決定是否在遠端桌面平台上啟用 Unity Touch 功能。Unity Touch 支援在 Horizon Client 中傳遞已發佈的應用程式，並允許行動裝置使用者存取 Unity Touch 側邊列中的應用程式。 此設定依預設為啟用。
Enable system tray redirection for Hosted Apps	X		決定使用者執行已發佈應用程式時，是否啟用系統匣重新導向。 此設定依預設為啟用。

表 5-8. Unity Touch 和主控應用程式原則設定 (續)

設定	電腦	使用者	內容
Enable user profile customization for Hosted Apps	X	X	指定在使用已發佈應用程式時是否自訂使用者設定檔。此設定啟用時，系統會產生使用者設定檔、自訂 Windows 佈景主題，並登錄啟動應用程式。 此設定依預設為停用。
Only launch new instances of Hosted Apps if arguments are different	X		此原則會控制已發佈應用程式已啟動，但現有應用程式執行個體在已中斷連線的通訊協定工作階段內執行時的行為。停用時，現有的應用程式執行個體將會啟動。啟用時，僅在命令列參數相符的情況下，現有的應用程式執行個體才會啟動。 此設定依預設為停用。
Limit usage of Windows hooks	X		使用已發佈應用程式或 Unity Touch 時停用多數勾點。此設定適用於在設定作業系統層級勾點的情況下會有相容性問題的應用程式。例如，啟用此設定時，系統會停用 Windows 多數作用中的協助工具和執行中的勾點。 依預設會停用此設定，這表示會使用所有常用的勾點。
Unity Filter rule list	X		指定在使用已發佈的應用程式時用於 Unity 視窗的篩選規則。Horizon Agent 會使用這些規則來支援自訂應用程式。如需有關建立篩選規則的相關資訊，請參閱管理特殊 Unity 視窗。 此設定依預設不會設定。

Horizon Agent 直接連線組態設定

Horizon Agent 直接組態設定位於群組原則管理編輯器的 **VMware View Agent 組態 > View Agent Direct-Connection 組態**資料夾中。請參閱《View Agent Direct-Connection 外掛程式管理》文件。

即時音訊視訊組態設定

RTAV 組態設定位於群組原則管理編輯器的 **VMware View Agent 組態 > View RTAV 組態**資料夾中。請參閱即時音訊視訊群組原則設定 。

Horizon Agent 的 USB 組態設定

請參閱 Horizon Agent 組態 ADMX 範本中的 USB 設定。

VMware AppTap 組態

VMware AppTap 組態設定位於群組原則管理編輯器的 **VMware View Agent 組態 > VMware AppTap 組態**資料夾中。

表 5-9. VMware AppTap 組態設定

設定	電腦	使用者	內容
Processes to ignore when detecting empty application sessions	X		指定偵測空白應用程式工作階段時要略過的程序清單。您可以指定程序檔案名稱或完整路徑。值不區分大小寫。請勿在路徑中使用環境變數。允許 UNC 網路路徑，例如：\\vmware\temp\app.exe。 此設定依預設不會設定。

VMware 用戶端 IP 通透性設定

VMware 用戶端 IP 通透性設定位於群組原則管理編輯器的 **VMware View Agent 組態 > VMware 用戶端 IP 通透性**資料夾中。

表 5-10. VMware 用戶端 IP 通透性原則設定

設定	電腦	使用者	內容
Default auto detect proxy	X		預設 Internet Explorer 連線設定。開啟 [網際網路選項] > [區域網路 (LAN) 設定] 中的**自動偵測設定**。 依預設不會啟用此設定。
Default Proxy Server	X		Proxy 伺服器的預設 Internet Explorer 連線設定。指定要在 [網際網路選項] > [區域網路 (LAN) 設定] 中使用的 Proxy 伺服器。 依預設不會啟用此設定。
Enable	X		啟用 VMware 用戶端 IP 通透性。Internet Explorer 的遠端連線會使用用戶端的 IP 位址，而不使用遠端桌面平台機器的 IP 位址。此設定會在您下次登入時生效。 如果在 Horizon Agent 中選取 VMware 用戶端 IP 通透性自訂設定選項，依預設將會啟用此設定。
Set proxy for Java applet	X		設定 Java Applet 的 Proxy。可用選項如下： ■ **將用戶端 IP 通透性用於 Java Proxy** - 將遠端連線導向為使用用戶端的 IP 位址，而不使用遠端桌面平台機器的 IP 位址 (針對 Java Applet)。 ■ **將直接連線用於 Java Proxy** - 將直接連線用於 Java Applet，以略過瀏覽器設定。 ■ **使用 Java Proxy 的預設值** - 還原原始 Java Proxy 設定。 依預設不會啟用此設定。

Flash 重新導向設定

Flash 重新導向設定位於群組原則管理編輯器的 **VMware View Agent 組態 > VMware FlashMMR** 資料夾中。

表 5-11. FlashMMR 原則設定

設定	電腦	使用者	內容
Enable flash multi-media redirection	X		指定是否在代理程式上啟用 Flash 重新導向。
Minimum rect size to enable FlashMMR	X		指定啟用 Flash 重新導向的矩形大小下限。 預設寬度為 320 像素，而預設高度為 200 像素。

HTML5 多媒體重新導向設定

HTML5 多媒體重新導向設定位於群組原則管理編輯器的 **VMware View Agent 組態 > VMware HTML5 多媒體重新導向**資料夾中。請參閱 VMware HTML5 功能原則設定。

商務用 Skype 的 VMware 虛擬化套件設定

HTML5 多媒體重新導向設定位於群組原則管理編輯器的 **VMware View Agent 組態 > 適用於商務用 Skype 的 VMware 虛擬化套件**資料夾中。請參閱適用於商務用 Skype 的 VMware 虛擬化套件的原則設定。

傳送至遠端桌面平台的用戶端系統資訊

使用者連線或重新連線至遠端桌面平台時，Horizon Client 將收集有關用戶端系統的資訊，而且連線伺服器會將這些資訊傳送至遠端桌面平台。

Horizon Agent 會將用戶端電腦資訊寫入部署在單一使用者機器之遠端桌面平台上的系統登錄路徑 `HKCU\Volatile Environment`。對於在 RDS 工作階段中部署的遠端桌面平台，Horizon Agent 會將用戶端電腦資訊寫入系統登錄路徑 `HKCU\Volatile Environment\`*x*，其中 *x* 是 RDS 主機上的工作階段識別碼。

如果 Horizon Client 是在遠端桌面工作階段內執行，則會傳送實體用戶端資訊而非虛擬機器資訊至遠端桌面平台。例如，如果使用者從其用戶端系統連線至遠端桌面平台、在遠端桌面平台內啟動 Horizon Client 並連線至其他遠端桌面平台，則會傳送實體用戶端系統的 IP 位址至第二個遠端桌面平台。此功能稱為巢狀模式或雙躍點案例。Horizon Client 會傳送 `ViewClient_Nested_Passthrough` (其設為 1) 以及用戶端系統資訊來指出它正在傳送巢狀模式資訊。

備註 針對 Horizon Client 4.1，用戶端系統資訊會傳遞至初始通訊協定連線上的第二個躍點桌面平台。針對 Horizon Client 4.2 和更新版本，如果第一個躍點的通訊協定中斷連線並重新連線，則也會更新用戶端系統資訊。

您可以將命令新增至 Horizon Agent`CommandsToRunOnConnect`、`CommandsToRunOnReconnect` 和 `CommandsToRunOnDisconnect` 群組原則設定，以執行命令或命令指令碼，在使用者連線和重新連線至桌面平台時，從系統登錄讀取此資訊。如需詳細資訊，請參閱在 Horizon 桌面平台上執行命令。

表 5-12. 用戶端系統資訊 介紹了包含用戶端系統資訊的登錄機碼，並列出了支援登錄機碼的桌面平台和用戶端系統類型。如果**支援巢狀模式**欄出現 [是]，則表示會將實體用戶端資訊 (而非虛擬機器資訊) 傳送至第二個躍點桌面平台。

表 5-12. 用戶端系統資訊

登錄機碼	說明	支援巢狀模式	支援的桌面平台	支援的用戶端系統
`ViewClient_IP_Address`	用戶端系統的 IP 位址。	是	VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集
`ViewClient_MAC_Address`	用戶端系統的 MAC 位址。	是	VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android
`ViewClient_Machine_Name`	用戶端系統的機器名稱。	是	VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集
`ViewClient_Machine_Domain`	用戶端系統的網域。	是	VDI (單一使用者機器) RDS	Windows、Windows 市集

表 5-12. 用戶端系統資訊 (續)

登錄機碼	說明	支援巢狀模式	支援的桌面平台	支援的用戶端系統
ViewClient_LoggedOn_Username	登入用戶端系統所用的使用者名稱。		VDI (單一使用者機器) RDS	Windows、Linux、Mac
ViewClient_LoggedOn_Domainname	登入用戶端系統所用的網域名稱。		VDI (單一使用者機器) RDS	Windows、Windows 市集 對於 Linux 和 Mac 用戶端，請參閱 ViewClient_Machine_Domain。.ViewClient_LoggedOn_Domainname 並非由 Linux 或 Mac 用戶端提供，因為 Linux 及 Mac 帳戶並非繫結到 Windows 網域。
ViewClient_Type	用戶端系統的精簡型用戶端名稱或作業系統類型。	是	VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集
ViewClient_Broker_DNS_Name	View 連線伺服器執行個體的 DNS 名稱。		VDI (單一使用者機器) RDS	值是從 View 連線伺服器直接傳送的，並非由 Horizon Client 所收集。
ViewClient_Broker_URL	View 連線伺服器執行個體的 URL。		VDI (單一使用者機器) RDS	值是從 View 連線伺服器直接傳送的，並非由 Horizon Client 所收集。
ViewClient_Broker_Tunneled	View 連線伺服器的通道連線狀態，這可以是 true (已啟用) 或 false (已停用)。		VDI (單一使用者機器) RDS	值是從 View 連線伺服器直接傳送的，並非由 Horizon Client 所收集。
ViewClient_Broker_Tunnel_URL	View 連線伺服器通道連線的 URL (如果已啟用通道連線)。		VDI (單一使用者機器) RDS	值是從 View 連線伺服器直接傳送的，並非由 Horizon Client 所收集。
ViewClient_Broker_Remote_IP_Address	View 連線伺服器執行個體所看見的用戶端系統 IP 位址。		VDI (單一使用者機器) RDS	值是從 View 連線伺服器直接傳送的，並非由 Horizon Client 所收集。
ViewClient_TZID	Olson 時區識別碼。 若要停用時區同步，請啟用 Horizon AgentDisable Time Zone Synchronization 群組原則設定。		VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS

表 5-12. 用戶端系統資訊 (續)

登錄機碼	說明	支援巢狀模式	支援的桌面平台	支援的用戶端系統
ViewClient_Windows_Timezone	GMT 標準時間。 若要停用時區同步，請啟用 Horizon AgentDisable Time Zone Synchronization 群組原則設定。		VDI (單一使用者機器) RDS	Windows、Windows 市集
ViewClient_Broker_DomainName	用於通過 View 連線伺服器認證的網域名稱。		VDI (單一使用者機器) RDS	值是從 View 連線伺服器直接傳送的，並非由 Horizon Client 所收集。
ViewClient_Broker_UserName	用於通過 View 連線伺服器認證的使用者名稱。		VDI (單一使用者機器) RDS	值是從 View 連線伺服器直接傳送的，並非由 Horizon Client 所收集。
ViewClient_Client_ID	指定用作授權金鑰連結的 Unique Client HardwareId。		VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集
ViewClient_Displays.Number	指定用戶端上正在使用的監視器數。		VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集
ViewClient_Displays.Topology	指定用戶端上顯示器的排列、解析度和尺寸。		VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集
ViewClient_Keyboard.Type	指定用戶端上正在使用的鍵盤類型。例如：日文、韓文。		VDI (單一使用者機器) RDS	Windows
ViewClient_Launch_SessionType	指定工作階段類型。類型可以是桌面平台或應用程式。		VDI (單一使用者機器) RDS	值是從 View 連線伺服器直接傳送的，並非由 Horizon Client 所收集。
ViewClient_Mouse.Identifier	指定滑鼠類型。		VDI (單一使用者機器) RDS	Windows
ViewClient_Mouse.NumButtons	指定滑鼠支援的按鈕數。		VDI (單一使用者機器) RDS	Windows
ViewClient_Mouse.SampleRate	指定取樣 PS/2 滑鼠輸入的速率 (報告/秒)。		VDI (單一使用者機器) RDS	Windows
ViewClient_Protocol	指定所用的通訊協定。		VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集
ViewClient_Language	指定作業系統語言。		VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集

表 5-12. 用戶端系統資訊 (續)

登錄機碼	說明	支援巢狀模式	支援的桌面平台	支援的用戶端系統
ViewClient_Launch_Matched_Tags	指定一或多個標記。		VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集
ViewClient_Launch_ID	指定桌面平台或應用程式集區唯一識別碼。		VDI (單一使用者機器) RDS	Windows、Linux、Mac、Android、iOS、Windows 市集
ViewClient_Broker_Farm_ID	指定 RDS 主機上桌面平台或應用程式集區的伺服器陣列識別碼。		RDS	Windows、Linux、Mac、Android、iOS、Windows 市集

備註 表 5-12. 用戶端系統資訊中 ViewClient_LoggedOn_Username 和 ViewClient_LoggedOn_Domainname 的定義適用於 Windows 版 Horizon Client 2.2 或更新版本。

對於 Windows 版 Horizon Client 5.4 或舊版，ViewClient_LoggedOn_Username 傳送在 Horizon Client 中輸入的使用者名稱，ViewClient_LoggedOn_Domainname 傳送在 Horizon Client 中輸入的網域名稱。

Windows 版 Horizon Client 2.2 比 Windows 版 Horizon Client 5.4 更新。從 Horizon Client 2.2 開始，Windows 的發行編號與其他作業系統和裝置上的 Horizon Client 版本編號一致。

在 Horizon 桌面平台上執行命令

您可以在使用者連線、重新連線和中斷連線時，在 Horizon 桌面平台使用 Horizon Agent CommandsToRunOnConnect、CommandsToRunOnReconnect 和 CommandsToRunOnDisconnect 群組原則設定來執行命令和命令指令碼。

若要執行命令或命令指令碼，請將命令名稱或指令碼的檔案路徑新增至群組原則設定的命令清單。例如：

```
date
```

```
C:\Scripts\myscript.cmd
```

若要執行需要存取主控台的指令碼，請在 –C 或 –c 選項後加一個空格。例如：

```
–c C:\Scripts\Cli_clip.cmd
```

```
–C e:\procexp.exe
```

支援的檔案類型包括 .CMD、.BAT 和 .EXE。.VBS 檔案必須以 cscript.exe 或 wscript.exe 剖析才能執行。例如：

```
–C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

包含 –C 或 –c 選項在內的字串總長度不可超過 260 個字元。

工作階段協作原則設定

VMware View Agent 組態 ADMX 範本檔 (vdm_agent.admx) 包含與工作階段協作有關的原則設定。

這些設定位於群組原則管理編輯器的**電腦組態 > 系統管理範本 > VMware View Agent 組態 > 協作**資料夾中。

表 5-13. 工作階段協作原則設定

設定	說明
Allow control passing to collaborators	如果啟用，使用者可以在協作期間將輸入控制權傳送給其他協作者。如果停用，則不會在協作視窗中顯示切換開關。此設定依預設為啟用。
Allow inviting collaborators by e-mail	此選項啟用時，您可以使用已安裝的電子郵件應用程式來傳送協作邀請。停用時，即便已安裝電子郵件應用程式，您仍無法使用電子郵件邀請協作者。此設定依預設為啟用。
Allow inviting collaborators by IM	此選項啟用時，您可以使用已安裝的即時訊息 (IM) 應用程式來傳送協作邀請。停用時，即便已安裝 IM 應用程式，您仍無法使用 IM 邀請協作者。此設定依預設為啟用。
Separator used for multiple e-mail addresses in mailto: links	設定在 mailto: 連結中用於多個電子郵件地址的分隔符號，可讓不同的電子郵件用戶端之間有更好的相容性。未設定時，預設值會以不含空格的分號來區分電子郵件地址。 如果您的預設電子郵件用戶端不允許使用分號作為分隔符號，請嘗試使用其他組合，例如逗號加上一個空格，或分號加上一個空格。
Server URLs to include in invitation message	設定要納入協作邀請的伺服器 URL。如果保持未設定，系統將會使用預設的 URL，但在除了最簡單部署以外的所有部署中，這可能不正確。
Turn off collaboration	此選項啟用時，系統會完全關閉工作階段協作功能。停用或未設定時，您可以在伺服器陣列或桌面平台集區層級控制協作功能。此設定會在您將 Horizon Agent 機器重新開機後生效。
Maximum number of invited collaborators	指定您可以邀請加入工作階段的協作者數目上限。預設最大值為 5。限制為 10。

用戶端磁碟機重新導向原則設定

VMware Horizon 用戶端磁碟機重新導向 ADMX 範本檔 (vdm_agent_cdr.admx) 包含與用戶端磁碟機重新導向功能相關的原則設定。

用戶端磁碟機重新導向設定位於群組原則管理編輯器的 **VMware View Agent 組態 > VMware Horizon 用戶端磁碟機重新導向**資料夾中。

表 5-14. 用戶端磁碟機重新導向設定

設定	電腦	使用者	內容
Configure drive letter mapping mode	X		指定磁碟機代號對應模式。此設定啟用時，您可以選取下列其中一個模式： ■ **一對一對應**，這會將用戶端機器上的磁碟機代號對應至代理程式機器上的相同磁碟機代號。例如，用戶端機器上的磁碟機 X 會對應至代理程式機器上的磁碟機 X。 ■ **定義的對應**，這會根據在**定義磁碟機代號對應表**群組原則設定中定義的對應表，將用戶端機器上的磁碟機代號對應至代理程式機器上的特定磁碟機代號。 如果發生磁碟機代號衝突 (例如，如果要對應的磁碟機代號已在代理程式機器上使用)，則會依據從 Z 到 A 的順序使用第一個可用的磁碟機代號。如果沒有可用的磁碟機代號，則不會指派磁碟機代號。 只有在**顯示含有磁碟機代號的重新導向裝置**群組原則設定未停用時，此設定才有效。
Define drive letter mapping table	X		此設定啟用時，您可以按一下**顯示**，並定義磁碟機代號對應表。在**值名稱**欄中，輸入用戶端機器上的磁碟機代號。在對應的**值**欄中，輸入要在代理程式機器上使用的磁碟機代號。 只有在**設定磁碟機代號對應模式**群組原則設定中選取了**定義的對應**時，此設定才有效。
Display redirected device with drive letter	X		決定是否對使用用戶端磁碟機重新導向功能重新導向的磁碟機顯示磁碟機代號。 此設定依預設為啟用。
Timeout for drive letter initialization	X		針對以用戶端磁碟機重新導向功能來重新導向的磁碟機，指定等待 Windows 檔案總管初始化並顯示磁碟機代號的時間長度 (以毫秒為單位)。 停用或未設定此設定時，預設值為 5000 毫秒。

用來篩選用戶端裝置的原則設定

用戶端磁碟機重新導向的裝置篩選設定位於群組原則管理編輯器的 **VMware View Agent 組態 > VMware Horizon 用戶端磁碟機重新導向 > 裝置篩選**資料夾中。

裝置篩選功能僅適用於 Windows、Mac 和 Linux 版 Horizon Client5.1 及更新版本。當這些裝置篩選原則已設定時，將會為其他用戶端停用用戶端磁碟機重新導向，包括 Android、iOS、Chrome 和 Horizon Client5.0 版及更早版本。

表 5-15. 裝置篩選設定

設定	電腦	使用者	內容
Exclude Vid/Pid Device	X		排除具有指定廠商和產品識別碼的裝置，而不使用用戶端磁碟機重新導向功能加以重新導向。 您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。請使用分號分隔多個裝置。例如： `vid-0781_pid-554c;vid-0781_pid-****` 預設值為未定義 (不排除任何裝置)。 此設定會優先於**納入 Vid/Pid 裝置**設定。 **備註** 若要為所有裝置停用用戶端磁碟機重新導向，您可以指定 `vid-****_pid-****`。
Include Vid/Pid Device	X		指定具有指定的廠商和產品識別碼，而可使用用戶端磁碟機重新導向功能進行重新導向的裝置。 您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。請使用分號分隔多個裝置。例如： `vid-054C_pid-0099;vid-8888_pid-****` 預設值為未定義 (納入所有裝置)。

VMware HTML5 功能原則設定

VMware View Agent 組態 ADMX 範本檔 (`vdm_agent.admx`) 包含與 VMware HTML5 功能相關聯的原則設定。

一般 VMware HTML5 功能設定

一般 VMware HTML5 功能設定位於群組原則管理編輯器的**電腦設定 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能**資料夾中。

表 5-16. 一般 VMware HTML5 功能設定

設定	說明
Enable VMware HTML5 Features	啟用 VMware HTML5 功能。您必須啟用此設定，才能使用 VMware HTML5 多媒體重新導向、地理位置重新導向或瀏覽器重新導向功能。此設定會在您下次登入時生效。
Disable Automatically Detect Intranet	啟用此原則時，將會在下次登入期間停用 [包括所有未列在其他區域的近端內部網路網站] 和 [包含所有略過 Proxy 伺服器的網站] 內部網路設定。 停用此原則時，不會對 IE 近端內部網路區域進行變更。 **重要** 如果您啟用 Edge 瀏覽器的 HTML5 多媒體重新導向功能，或啟用地理位置重新導向功能，則必須啟用此設定。

VMware HTML5 多媒體重新導向功能設定

VMware HTML5 多媒體重新導向功能設定位於群組原則管理編輯器的**電腦設定 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能 > VMware HTML5 多媒體重新導向**資料夾中。

表 5-17. VMware HTML5 多媒體重新導向原則設定

設定	說明
`Enable VMware HTML5 Multimedia Redirection`	啟用 VMware HTML5 多媒體重新導向功能。此設定會在您下次登入時生效。
`Enable URL list for VMware HTML5 Multimedia Redirection`	指定哪些網站會使用 HTML5 多媒體重新導向功能。 在 [值名稱] 資料欄中，輸入可以將 HTML5 多媒體內容重新導向的網站 URL 清單。請在 URL 中加入 `http://` 或 `https://` 前置詞。您可以在 URL 中使用比對模式。 例如，若要重新導向 YouTube 上的所有視訊，請輸入 `https://www.youtube.com/*`。若要重新導向 Vimeo 上的所有視訊，請輸入 `https://www.vimeo.com/*`。 讓 [值] 欄保持空白。
`Enable Chrome Browser for VMware HTML5 Multimedia Redirection`	僅在 VMware HTML5 多媒體重新導向功能已啟用時，才會使用此原則。如果未設定此原則，則預設值與 [啟用 VMware HTML5 多媒體重新導向] 設定的值相同。
`Enable Edge Browser for VMware HTML5 Multimedia Redirection`	僅在 VMware HTML5 多媒體重新導向功能已啟用時，才會使用此原則。如果未設定此原則，則預設值與 [啟用 VMware HTML5 多媒體重新導向] 設定的值相同。

VMware 地理位置重新導向功能設定

VMware 地理位置重新導向功能設定位於群組原則管理編輯器的**電腦設定 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能 > VMware 地理位置重新導向**資料夾中。

表 5-18. VMware 地理位置重新導向設定

設定	說明
`Enable VMware Geolocation Redirection`	啟用地理位置重新導向功能。此設定會在您下次登入時生效。
`Enable URL list for VMware Geolocation Redirection`	指定哪些網站會使用地理位置重新導向功能。 在 [值名稱] 資料欄中，輸入可以將地理位置資訊重新導向的網站 URL 清單。請在 URL 中加入 `http://` 或 `https://` 前置詞。您可以在 URL 中使用比對模式。 例如，若要指定所有 YouTube 視訊，請輸入 `https://www.youtube.com/*`。若要指定所有 Vimeo 視訊，請輸入 `https://www.vimeo.com/*`。 讓 [值] 欄保持空白。
`Set the minimum distance for which to report location updates`	指定用戶端中的位置更新與上次向代理程式報告的更新 (必須向代理程式報告新位置) 之間的最小距離 (以公尺為單位)。 依預設，使用的最小距離為 75 公尺。

VMware Browser 重新導向功能設定

VMware Browser 重新導向功能設定位於群組原則管理編輯器的**電腦設定 > 系統管理範本 > VMware View Agent 組態 > VMware HTML5 功能 > VMware Browser 重新導向**資料夾中。

表 5-19. VMware Browser 重新導向設定

設定	說明
`Enable VMware Browser Redirection`	啟用瀏覽器重新導向功能。
`Enable URL list for VMware Browser Redirection`	指定瀏覽器重新導向功能的所有 URL。使用者可以透過在 Chrome 網址列或自訂網址列中輸入這些 URL 來造訪這些 URL。使用者也可以從清單中的其他 URL 開始導覽或從任何代理程式端轉譯的頁面來造訪這些 URL。 在 [值名稱] 欄中輸入 URL。請在 URL 中加入 `http://` 或 `https://` 前置詞。您可以在 URL 中使用比對模式。比對模式必須遵循 https://developer.chrome.com/extensions/match_patterns。 例如，若要指定所有 YouTube 內容，請輸入 `https://www.youtube.com/*`。 讓 [值] 欄保持空白。
`Enable Navigation URL list for VMware Browser Redirection`	指定允許使用者從**啟用 VMware Browser 重新導向的 URL 清單**白名單中指定的 URL 導覽的目的 URL，可以透過在自訂網址列中直接輸入 URL，或者從白名單中的 URL 開始導覽至該 URL。 使用者無法透過在 Chrome 網址列中輸入 URL 或從代理程式端呈現的頁面導覽至 URL 來直接造訪這些 URL。 在 [值名稱] 欄中輸入 URL 清單。請在 URL 中加入 `http://` 或 `https://` 前置詞。您可以在 URL 中使用比對模式。比對模式必須遵循 https://developer.chrome.com/extensions/match_patterns。 例如，若要指定所有 YouTube 內容，請輸入 `https://www.youtube.com/*`。 讓 [值] 欄保持空白。
`Enable automatic fallback after a whitelist violation`	啟用此設定後，如果使用者導覽至未在任何瀏覽器重新導向白名單中指定的 URL，無論是透過在自訂網址列中輸入 URL 或者透過從白名單中的任一 URL 開始導覽至 URL，則重新導向將針對該索引標籤停止，並改為在代理程式上擷取和顯示該 URL。 **備註** 如果使用者嘗試導覽至未在**啟用 VMware Browser 重新導向的 URL 清單**設定中指定的 URL，則無論是否啟用此設定，該索引標籤一律會回復為在代理程式上擷取和呈現該 URL。
`Show a page with error information before automatic fallback`	如果啟用此設定，則發生白名單違規時，系統會出現一個顯示倒數計時五秒的頁面。經過五秒後，該索引標籤將回復為在代理程式上擷取和呈現導致違規的 URL。如果停用此設定，則不會顯示五秒的警告頁面。 僅當同時啟用了**啟用白名單違規後的自動後援**設定時，此設定才會生效。

適用於商務用 Skype 的 VMware 虛擬化套件的原則設定

VMware View Agent 組態 ADMX 範本檔 (vdm_agent.admx) 包含與商務用 Skype 的 VMware 虛擬化套件相關的原則設定。

這些設定位於群組原則管理編輯器的**電腦組態 > 系統管理範本 > VMware View Agent 組態 > 商務用 Skype 的 VMware 虛擬化套件**資料夾中。

表 5-20. 商務用 Skype 的虛擬化套件的原則設定

設定	說明
Disable extended filter for acoustic echo cancellation in VMware Virtualization Pack for Skype for Business	原音回音消除的延伸篩選器依預設為啟用，可提供更理想的回音和反饋取消，且在 Horizon Client 系統的麥克風和喇叭距離十分接近時的案例中效果尤佳。如果您不想讓適用於商務用 Skype 的 VMware 虛擬化套件使用此篩選器，請啟用此原則。
EnableDetectProxySettings	當 Horizon Client 系統必須使用 Proxy 伺服器時，啟用此原則以降低延遲。啟用後，適用於商務用 Skype 的虛擬化套件會檢查 Horizon Client 系統上的 Proxy 設定，並將這些設定用於媒體流量。如果 Horizon Client 系統上沒有 Proxy 的設定，適用於商務用 Skype 的虛擬化套件將會使用直接連線。
Force Skype for Business in non-optimized mode	您可以強制商務用 Skype 針對 Horizon Client 連線在非最佳化模式中執行，方法是設定環境變數的名稱，名稱會在連線時顯示於安裝 Horizon Agent 所在的機器上。如果已設定變數名稱，則商務用 Skype 的虛擬化套件會還原為後援模式。 例如，如果已在遠端桌面平台代理程式機器上設定環境變數 ViewClient_F5_APM，則當 Horizon Client 機器使用 F5 負載平衡器從網路外部連線，且您想要強制使用非最佳化模式時，請將此值設為 ViewClient_F5_APM。依預設不會設定此原則。
Show Icon	顯示適用於商務用 Skype 之虛擬化套件的圖示。此原則依預設為啟用。如果已停用商務用 Skype 的虛擬化套件的「顯示圖示」原則，則圖示不會顯示。當該原則停用時，您無法檢視呼叫統計資料或訊息。
Show Messages	顯示適用於商務用 Skype 之虛擬化套件的訊息。此原則依預設為啟用。如果停用適用於商務用 Skype 之虛擬化套件的「顯示圖示」或「顯示訊息」原則，則系統不會顯示訊息。
Suppress minor version mismatch warning	如果適用於商務用 Skype 的虛擬化套件的次要 API 版本與 Horizon Client 系統和 Horizon 桌面平台上的不同，通知區域即會顯示警告。啟用此原則後，此警告即會隱藏。請注意，當次要 API 版本不相符時，商務用 Skype 呼叫將會最佳化，但是虛擬化套件可能不具有最新功能。

VMware Horizon 效能追蹤程式原則設定

Horizon 效能追蹤程式 ADMX 範本檔 (perf_tracker.admx) 包含與 VMware Horizon 效能追蹤程式功能相關的原則設定。

如需設定和使用 Horizon 效能追蹤程式功能的相關資訊，請參閱《Horizon 7 管理》文件。

表 5-21. Horizon 效能追蹤程式原則設定

設定	說明
Horizon 效能追蹤程式基本設定	啟用時，您可以設定 Horizon 效能追蹤程式收集資料的頻率 (以秒為單位)。
啟用 Horizon 效能追蹤程式在遠端桌面平台連線中自動啟動	啟用時，當使用者登入遠端桌面平台連線時，Horizon 效能追蹤程式即會自動啟動。若要清除此喜好設定 GPO 設定，請選取**停用**。
啟用 Horizon 效能追蹤程式在遠端應用程式連線中自動啟動	啟用時，當使用者登入遠端應用程式連線時，Horizon 效能追蹤程式即會自動啟動。若要清除此喜好設定 GPO 設定，請選取**停用**。

VMware 整合式列印原則設定

VMware View Agent 組態 ADMX 範本檔 (`printerRedirection.admx`) 包含與 VMware 整合式列印重新導向相關的原則設定。

這些設定位於群組原則管理編輯器的**電腦組態 > 系統管理範本 > VMware 整合式列印**資料夾中。

表 5-22. VMware 整合式列印原則設定

設定	說明
`Disable LBP`	指定是否啟用依據位置列印。啟用此設定時，將會停用依據位置列印。停用或未設定此設定時，則會啟用依據位置列印。
`Disable Printer Property Persistence`	指定是否啟用印表機內容持續性。啟用此設定時，印表機內容將不會在用戶端本機印表機和重新導向的印表機之間不具備持續性。停用或未設定此設定時，印表機內容將會在用戶端本機印表機和重新導向的印表機之間具備持續性。
`Print Preview Setting`	**停用列印選擇**會決定是否啟用列印目標。依預設為未設定狀態。如果勾選取，則使用者無法選擇列印目標。如果取消勾選或未設定，則使用者可以選擇列印目標。 ■ **直接列印**：列印 UI 中的預設列印選項是直接列印。 ■ **列印預覽**：列印 UI 中的預設列印選項是列印預覽。

表 5-22. VMware 整合式列印原則設定 (續)

設定	說明
Printer Driver Selection	指定用於重新導向用戶端印表機的印表機驅動程式：通用印表機驅動程式 (UPD) 或原生印表機驅動程式 (NPD)。啟用此設定時，可用的選項如下所示： ■ **一律使用 NPD**：將原生印表機驅動程式用於重新導向的印表機。 ■ **一律使用 UPD**：將通用印表機驅動程式用於重新導向的印表機。 ■ **先使用 NPD，然後使用 UPD**：先使用原生印表機驅動程式，如果該驅動程式不存在，則再使用通用印表機驅動程式。 ■ **先使用 UPD，然後使用 NPD**：先使用通用印表機驅動程式，如果該驅動程式不存在，則再使用原生印表機驅動程式。 停用或未設定此設定時，預設值為**先使用 NPD，然後使用 UPD**。

Specify a filter in redirecting client printers	如果啟用，請在**登錄值名稱：PrinterFilterString** 文字方塊中輸入篩選規則。此篩選規則是一個指定印表機不應重新導向 (黑名單) 的規則運算式。任何與篩選規則中的印表機不相符的印表機，都會重新導向。篩選規則依預設為空白，這表示所有用戶端印表機都會重新導向。
	■ 屬性：DriverName、VendorName 和 PrinterName
	■ 運算子：AND、OR 和 NOT
	■ 萬用字元：* 和 ?
	篩選規則範例：
	`(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e"`
	`PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF"`
	`PrinterName!=".*PDFCreator.*"`

PCoIP 原則設定

PCoIP ADMX 範本檔 (pcoip.admx) 包含與 PCoIP 顯示通訊協定相關的原則設定。您可以將設定設為管理員可以覆寫的預設值，或設為非可覆寫的值。

ADMX 檔案可從 VMware-Horizon-Extras-Bundle-*x.x.x-yyyyyyy*.zip 中取得，而您可以從 VMware 下載網站下載該 zip 檔案，網址為 https://my.vmware.com/web/vmware/downloads。在 [桌面平台及使用者運算] 下，選取 VMware Horizon 7 下載，其中包含 ZIP 檔案。

PCoIP 工作階段變數 ADMX 範本檔包含兩個子類別：

可覆寫的管理員預設值

指定 PCoIP 原則設定預設值。管理員可覆寫這些設定。這些設定會將登錄機碼寫至 HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults。所有這些設定位於群組原則管理編輯器的**電腦設定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 可覆寫的管理員預設值**資料夾中。

非可覆寫的管理員設定

包含與「可覆寫的管理員預設值」相同的設定，但管理員無法覆寫這些設定。這些設定會將登錄機碼寫至 HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin。所有這些設定位於群組原則管理編輯器的**使用者設**

定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 非可覆寫的管理員設定資料夾中。

範本包含「電腦設定」與「使用者設定」設定。

非原則登錄機碼

如果需套用本機電腦設定，且不能放置在 HKLM\Software\Policies\Teradici 下，則本機電腦設定可放置在 HKLM\Software\Teradici 中的登錄機碼中。相同的登錄機碼可放置在 HKLM\Software\Teradici 中，如同在 HKLM\Software\Policies\Teradici 中。如果這兩個位置有相同的登錄機碼，則 HKLM\Software\Policies\Teradici 中的設定會覆寫本機電腦值。

PCoIP 一般設定

PCoIP ADMX 範本檔包含可設定一般設定 (如 PCoIP 影像畫質、USB 裝置和網路連接埠) 的群組原則設定。

所有這些設定位於群組原則管理編輯器的**電腦設定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 可覆寫的管理員預設值**資料夾中。

所有這些設定也位於群組原則管理編輯器的**使用者設定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 非可覆寫的管理員設定**資料夾中。

表 5-23. PCoIP 一般原則設定

設定	說明
Configure PCoIP event log cleanup by size in MB	啟用依 PCoIP 事件記錄的大小 (MB) 進行清理的組態。 設定此原則後，此設定可控制記錄檔增長到多大時進行清理。如果 *m* 設定為非零值，系統會自動且無訊息刪除大於 *m* MB 的記錄檔。設定為 0 表示系統不會依據大小清理記錄檔。 如果停用或未設定此原則，預設會清理大小超過 100 MB 的事件記錄。 當工作階段啟動時，會執行一次記錄檔清理。如果變更此設定，此變更會在下一個工作階段生效。
Configure PCoIP event log cleanup by time in days	啟用依 PCoIP 事件記錄的時間 (天數) 進行清理的組態。 設定此原則後，此設定可控制記錄檔存留多少天後進行清理。如果 *n* 設定為非零值，系統會自動且無訊息刪除存留超過 *n* 天的記錄檔。設定為 0 表示系統不會依據時間清理記錄檔。 如果停用或未設定此原則，預設會清理存留時間超過 7 天的事件記錄。 當工作階段啟動時，會執行一次記錄檔清理。如果變更此設定，此變更會在下一個工作階段生效。
Configure PCoIP event log verbosity	設定 PCoIP 事件記錄詳細資訊。值的範圍為 0 (最不詳細) 至 3 (最詳細)。 啟用此設定時，您可以從 0 至 3 設定詳細資訊等級。未設定或停用此設定時，事件記錄詳細資訊等級會預設為 2。 在作用中的 PCoIP 工作階段期間修改此設定時，新設定會立即生效。

表 5-23. PCoIP 一般原則設定 (續)

設定	說明
Configure PCoIP image quality levels	控制 PCoIP 在網路壅塞期間轉譯映像的方式。**最低映像畫質**、**最高初始映像畫質**和**最大畫面播放速率**值會相互溝通，在網路頻寬受限的環境中提供良好的控制。 使用**最低映像畫質**值可在頻寬受限的情況下，平衡映像畫質與畫面播放速率。您可以指定一個介於 30 和 100 之間的值。預設值為 40。值越小，畫面播放速率越高，但可能會降低顯示的畫質。值越大，映像畫質越高，但可能會在網路頻寬受限時降低畫面播放速率。網路頻寬未受限時，PCoIP 會忽略此值並維持最高畫質。 使用**最高初始映像畫質**值可藉由限制已變更顯示器映像區域的初始畫質，減少 PCoIP 所需的網路頻寬尖峰。您可以指定一個介於 30 和 100 之間的值。預設值為 80。值越小，內容變更的映像畫質就越低，且尖峰頻寬的需求也會減少。值越大，內容變更的映像畫質就越高，且尖峰頻寬的需求也會增加。未變更的映像區域會忽略此值，並以漸進的方式建立起不失真 (完美) 的畫質。80 (含) 以下的值能夠使可用頻寬發揮最佳效用。 **最低映像畫質**值不得超過**最高初始映像畫質**值。 使用**最大畫面播放速率**值可藉由限制每秒的畫面更新數目，管理每位使用者使用的平均頻寬。您可以指定一個介於 1 到 120 之間的每秒畫面值。預設值為 30。值越大，可使用的頻寬就越多，但提供的抖動越少，因此可在變動的映像 (如視訊) 中提供更平滑的傳輸。值越小，可使用的頻寬越少，但會導致更多抖動。 這些映像畫質值僅適用於軟體主機，對於軟體用戶端沒有作用。 停用或未設定此設定時，會使用預設值。 在作用中的 PCoIP 工作階段期間修改此設定時，新設定會立即生效。
Configure frame rate vs image quality preference	從 0 (最高畫面播放速率) 到 100 (最高影像畫質) 設定畫面播放速率和影像畫質喜好設定。如果停用或未設定此原則，則會使用預設設定 50。 若值較高 (最大值為 100)，表示您偏好較高的影像畫質，即使畫面播放速率較差亦然。若值較低 (最小值為 0)，表示您偏好流暢的使用經驗，而可容忍較差的影像畫質。 此設定可與 Configure PCoIP image quality levels GPO 搭配使用，這會決定最大初始影像畫質層級和最小影像畫質層級。雖然 Frame rate and image quality preference 可調整每個畫面的影像畫質層級，但它不能超過 Configure PCoIP image quality levels GPO 所設定的最大/最小畫質層級臨界值。 如果在執行階段期間變更此原則，變更可能會立即生效。
Configure PCoIP session encryption algorithms	控制 PCoIP 端點在工作階段交涉期間公告的加密演算法。 勾選其中一個核取方塊就會停用相關的加密演算法。您必須至少啟用一種演算法。 此設定會同時套用至代理程式和用戶端。端點會交涉所使用的實際工作階段加密演算法。如果啟用 FIPS140-2 核准模式，就會一律覆寫**停用 AES-128-GCM 加密**值，如此便會啟用 AES-128-GCM 加密。 依優先順序，支援的加密演算法為 SALSA20/12-256、AES-GCM-128 和 AES-GCM-256。依預設，所有支援的加密演算法均可供此端點用於交涉。 如果兩個端點均設定為支援全部三種演算法，但連線並未使用安全閘道 (SG)，則會使用 SALSA20 演算法進行交涉。但是，如果連線使用 SG，則會自動停用 SALSA20，並使用 AES128 進行交涉。如果任一端點或 SG 停用了 SALSA20，且任一端點停用了 AES128，則會使用 AES256 進行交涉。

表 5-23. PCoIP 一般原則設定 (續)

設定	說明
Configure PCoIP USB allowed and unallowed device rules	針對使用執行 Teradici 韌體之零用戶端的 PCoIP 工作階段，指定授權和未授權的 USB 裝置。PCoIP 工作階段中使用的 USB 裝置必須出現在 USB 授權表中。出現在 USB 未授權表中的 USB 裝置無法在 PCoIP 工作階段中使用。 您最多可以定義 10 項 USB 授權規則以及 10 項 USB 未授權規則。請使用分隔號 (|) 字元分隔多項規則。 每一項規則都可以是廠商識別碼 (VID) 和產品識別碼 (PID) 的組合，或者規則可以說明某種 USB 裝置類別。類別規則可以允許或不允許整個裝置類別、單一子類別，或是子類別內的通訊協定。 VID/PID 規則組合的格式為 **1xxxxyyyy**，其中 **xxxx** 是十六進位格式的 VID，而 **yyyy** 是十六進位格式的 PID。例如，授權或封鎖 VID **0x1a2b** 且 PID **0x3c4d** 裝置的規則為 **11a2b3c4d**。 對於類別規則，請使用下列其中一種格式： **允許所有 USB 裝置** 格式：**23XXXXXX** 範例：**23XXXXXX** **允許包含特定類別識別碼的 USB 裝置** 格式：**22*class*XXXX** 範例：**22aaXXXX** **允許特定子類別** 格式：**21*class*-*subclass*XX** 範例：**21aabbXX** **允許特定通訊協定** 格式：**20*class*-*subclass*-*protocol*** 範例：**20aabbcc** 例如，允許 USB HID (滑鼠與鍵盤) 裝置 (類別識別碼 0x03) 和網路攝影機 (類別識別碼 0x0e) 的 USB 授權字串為 **2203XXXX|220eXXXX**。不允許 USB 大量儲存裝置 (類別識別碼 0x08) 的 USB 未授權字串為 **2208XXXX**。 空的 USB 授權字串表示沒有授權的 USB 裝置。空的 USB 未授權字串表示未禁用任何 USB 裝置。 此設定只會套用至 Horizon Agent，而且僅適用於遠端桌面平台的工作階段使用執行 Teradici 韌體的零用戶端時。裝置用途會在端點之間交涉。 依預設，允許所有裝置，且沒有不允許的裝置。

表 5-23. PCoIP 一般原則設定 (續)

設定	說明
Configure PCoIP virtual channels	指定可以及無法透過 PCoIP 工作階段操作的虛擬通道。此設定也會決定是否停用 PCoIP 主機上的剪貼簿處理。 PCoIP 工作階段中使用的虛擬通道必須出現在虛擬通道授權清單中。出現在未授權虛擬通道清單中的虛擬通道無法在 PCoIP 工作階段中使用。 您最多可以指定 15 個在 PCoIP 工作階段中使用的虛擬通道。 請使用分隔號 (|) 字元分隔多個通道名稱。例如，允許 mksvchan 和 vdp_rdpvcbridge 虛擬通道的虛擬通道授權字串為 **mksvchan|vdp_vdpvcbridge**。 如果通道名稱包含分隔號或反斜線 (\) 字元，請在前面插入反斜線字元。例如，通道名稱 awk|ward\channel 輸入為 **awk\\|ward\\\channel**。 授權的虛擬通道清單為空白時，表示不允許所有虛擬通道。未授權的虛擬通道清單為空白時，表示允許所有虛擬通道。 虛擬通道設定會同時套用至代理程式和用戶端。代理程式和用戶端上的虛擬通道都必須啟用，才能使用虛擬通道。 虛擬通道設定會另外提供一個核取方塊，讓您停用 PCoIP 主機上的遠端剪貼簿處理。此值僅適用於代理程式。 依預設，會啟用所有虛擬通道，包括剪貼簿處理。
Configure the PCoIP transport header	設定 PCoIP 傳輸標頭以及設定傳輸工作階段優先順序。 PCoIP 傳輸標頭為 32 位元標頭，會新增至所有 PCoIP UDP 封包 (但只有在雙方均啟用且支援傳輸標頭時)。PCoIP 傳輸標頭會允許網路裝置在處理網路壅塞時決定較佳的優先順序/QoS。傳輸標頭預設為啟用。 傳輸工作階段優先順序會決定 PCoIP 傳輸標頭報告的 PCoIP 工作階段優先順序。網路裝置會根據指定的傳輸工作階段優先順序，決定較佳的優先順序/QoS。 啟用 Configure the PCoIP transport header 設定時，可使用下列傳輸工作階段優先順序： ■ **高** ■ **中** (預設值) ■ **低** ■ **未定義** 傳輸工作階段優先順序值會由 PCoIP 代理程式和用戶端進行協議。如果 PCoIP 代理程式指定了傳輸工作階段優先順序值，則工作階段會使用代理程式所指定的工作階段優先順序。如果只有用戶端指定了傳輸工作階段優先順序，則工作階段會使用用戶端所指定的工作階段優先順序。如果代理程式和用戶端都沒有指定傳輸工作階段優先順序，或是指定了**未定義優先順序**，則工作階段會使用預設值，即**中**優先順序。

表 5-23. PCoIP 一般原則設定 (續)

設定	說明
Configure the TCP port to which the PCoIP host binds and listens	指定軟體 PCoIP 主機所繫結的 TCP 代理程式連接埠。 TCP 連接埠值會指定代理程式嘗試繫結的基礎 TCP 連接埠。TCP 連接埠範圍值會決定基礎連接埠無法使用時，要嘗試的其他連接埠數目。連接埠範圍必須介於 1 和 10 之間。 此範圍從基礎連接埠跨越至基礎連接埠和連接埠範圍的總和。例如，如果基礎連接埠為 4172 且連接埠範圍為 10，則範圍會從 4172 跨越至 4182。 請勿將重試連接埠範圍的大小設定為 0。將此值設定為 0 會導致使用者在使用 PCoIP 顯示通訊協定登入桌面平台時連線失敗。Horizon Client 會傳回錯誤訊息「此桌面平台的顯示通訊協定目前無法使用。請連絡您的系統管理員。」 此設定只會套用至 Horizon Agent。 在 View 4.5 及更新版本中，單一使用者機器上的預設基礎 TCP 連接埠為 4172。在 View 4.0.*x* 及更早版本中，預設基礎連接埠為 50002。依預設，連接埠範圍為 1。 在 RDS 主機上，預設基礎 TCP 連接埠為 4173。當 PCoIP 與 RDS 主機搭配使用時，每個使用者連線都會使用不同的 PCoIP 連接埠。遠端桌面服務所設定的預設連接埠範圍，足以容納預期的並行使用者連線數目上限。 **重要** 最佳做法是，請勿使用此原則設定來變更 RDS 主機的預設連接埠範圍，也不要變更 TCP 連接埠的預設值 4173。最重要的是，請勿將 TCP 連接埠值設定為 4172。將此值重設為 4172 會對 RDS 工作階段中的 PCoIP 效能造成不良影響。
Configure the UDP port to which the PCoIP host binds and listens	指定軟體 PCoIP 主機所繫結的 UDP 代理程式連接埠。 UDP 連接埠值會指定代理程式嘗試繫結的基礎 UDP 連接埠。UDP 連接埠範圍值會決定基礎連接埠無法使用時，要嘗試的其他連接埠數目。連接埠範圍必須介於 1 和 10 之間。 請勿將重試連接埠範圍的大小設定為 0。將此值設定為 0 會導致使用者在使用 PCoIP 顯示通訊協定登入桌面平台時連線失敗。Horizon Client 會傳回錯誤訊息「此桌面平台的顯示通訊協定目前無法使用。請連絡您的系統管理員。」 此範圍從基礎連接埠跨越至基礎連接埠和連接埠範圍的總和。例如，如果基礎連接埠為 4172 且連接埠範圍為 10，則範圍會從 4172 跨越至 4182。 此設定只會套用至 Horizon Agent。 在單一使用者機器上，View 4.5 及更新版本的預設基礎 UDP 連接埠為 4172，View 4.0.*x* 及更早版本的基礎 UDP 連接埠為 50002。依預設，連接埠範圍為 10。 在 RDS 主機上，預設基礎 UDP 連接埠為 4173。當 PCoIP 與 RDS 主機搭配使用時，每個使用者連線都會使用不同的 PCoIP 連接埠。遠端桌面服務所設定的預設連接埠範圍，足以容納預期的並行使用者連線數目上限。 **重要** 最佳做法是，請勿使用此原則設定來變更 RDS 主機的預設連接埠範圍，也不要變更 UDP 連接埠的預設值 4173。最重要的是，請勿將 UDP 連接埠值設定為 4172。將此值重設為 4172 會對 RDS 工作階段中的 PCoIP 效能造成不良影響。

表 5-23. PCoIP 一般原則設定 (續)

設定	說明
Enable access to a PCoIP session from a vSphere console	決定是否允許 vSphere Client 主控台顯示作用中 PCoIP 工作階段並且將輸入傳送至桌面平台。 依預設，透過 PCoIP 連接用戶端時，vSphere Client 主控台畫面會是空白的，而且主控台無法傳送輸入。預設設定可確保惡意使用者無法在 PCoIP 遠端工作階段作用中時，檢視使用者的桌面平台或提供輸入至主機本機。 此設定只會套用至 Horizon Agent。 停用或未設定此設定時，不允許主控台存取。啟用此設定時，主控台會顯示 PCoIP 工作階段而且允許主控台輸入。 啟用此設定時，主控台只能在 Windows 7 虛擬機器的硬體為 v8 時，才能顯示 Windows 7 系統上執行的 PCoIP 工作階段。硬體 v8 僅於 ESXi 5.0 及更新版本上提供。相反地，虛擬機器使用任何硬體版本時，都允許對 Windows 7 系統進行主控台輸入。
Enable/disable audio in the PCoIP session	決定是否在 PCoIP 工作階段中啟用音訊。兩個端點都必須啟用音訊。啟用此設定時，會允許 PCoIP 音訊。停用此設定時，會停用 PCoIP 音訊。未設定此設定時，預設為啟用音訊。
Enable/disable microphone noise and DC offset filter in PCoIP session	決定是否在 PCoIP 工作階段期間，啟用麥克風輸入的麥克風噪音和 DC 補償過濾。 此設定只會套用至 Horizon Agent 和 Teradici 音訊驅動程式。 未設定此設定時，Teradici 音訊驅動程式預設會使用麥克風噪音和 DC 補償過濾。
Turn on PCoIP user default input language synchronization	決定 PCoIP 工作階段中使用者的預設輸入語言是否與 PCoIP 用戶端端點的預設輸入語言同步。啟用此設定時，允許同步。停用或未設定此設定時，不允許同步。 此設定只會套用至 Horizon Agent。
Configure SSL Connections to satisfy Security Tools	指定建立 SSL 工作階段交涉連線的方式。 為了滿足連接埠掃描器，請啟用此 [設定 SSL 連線] 設定，並在 Horizon Agent 上完成下列工作： 1 在 Microsoft Management Console 中，針對本機電腦的電腦帳戶，將已正確命名並簽署的憑證儲存到「個人」存放區中，並將其標示為可匯出。 2 將簽署該憑證之憑證授權機構的憑證儲存到「受信任的根憑證」存放區中。 3 停用 VMware View 5.1 及更早版本的連線。 4 將 Horizon Agent 設定為僅從憑證存放區載入憑證。如果將「個人」存放區用於本機電腦，請將憑證存放區名稱保留為「MY」和「ROOT」(不含引號)，除非您在步驟 1 和 2 中使用不同的存放區位置。 產生的 PCoIP Server 將會滿足連接埠掃描器之類的安全工具。

表 5-23. PCoIP 一般原則設定 (續)

設定	說明
Configure SSL Protocols	設定 OpenSSL 通訊協定，以限制在建立加密 SSL 連線之前對特定通訊協定的使用。通訊協定清單由一或多個以冒號分隔的 openssl 通訊協定字串組成。請注意，所有加密字串皆不區分大小寫。 預設值為：「TLS1.1:TLS1.2」 這表示 TLS v1.1 和 TLS v1.2 皆會啟用 (停用 SSL v2.0、SSLv3.0 和 TLS v1.0)。 此設定會同時套用至 Horizon Agent 和 Horizon Client。 如果同時設定於兩端，系統將會遵循 OpenSSL 通訊協定交涉規則。
Configure SSL cipher list	設定 SSL 加密清單，以限制在建立加密 SSL 連線之前對於加密套件的使用。清單由一或多個以冒號分隔的加密套件字串組成。所有加密套件字串皆不區分大小寫。 預設值為 ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH。 如果已進行此設定，則會忽略**設定 SSL 連線以滿足安全工具**設定中的**強制執行用於 SSL 連線交涉的 AES-256 或更強的加密**核取方塊。 此設定必須同時套用至 PCoIP 伺服器和 PCoIP 用戶端。

PCoIP 剪貼簿和拖放設定

Horizon PCoIP ADMX 範本檔包含可針對複製並貼上和拖放作業進行剪貼簿設定的群組原則設定。

所有這些設定位於群組原則管理編輯器的**電腦設定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 可覆寫的管理員預設值**資料夾中。

所有這些設定也位於群組原則管理編輯器的**使用者設定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 非可覆寫的管理員設定**資料夾中。

表 5-24. PCoIP 剪貼簿原則設定

設定	說明
Configure clipboard audit	指定是否在代理程式機器上啟用剪貼簿稽核功能。啟用此設定時，可用的選項如下所示： ■ **雙向停用** - 不記錄剪貼簿資料的相關資訊。 ■ **僅啟用用戶端至伺服器** - 代理程式機器上的事件記錄中會記錄有關從用戶端機器複製到代理程式機器之剪貼簿資料的相關資訊。 ■ **雙向啟用** - 代理程式機器上的事件記錄中會記錄有關從用戶端機器複製到代理程式機器以及從代理程式機器複製到用戶端機器的剪貼簿資料的相關資訊。 ■ **僅啟用伺服器至用戶端** - 代理程式機器上的事件記錄中會記錄有關從代理程式機器複製到用戶端機器的剪貼簿資料的相關資訊。 當此設定停用或未設定時，預設值將是**雙向停用**。 您可以使用代理程式機器上的 Windows 事件檢視器來檢視事件記錄。記錄名稱為 VMware Horizon RX 稽核。若要從集中位置檢視事件記錄，您可以設定 VMware Log Insight 或 Windows Event Collector。 對於 Windows 用戶端，Horizon Client 4.9 及更新版本支援從代理程式機器至用戶端機器剪貼簿稽核。對於所有用戶端，Horizon Client 4.10 及更新版本支援從用戶端機器到代理程式機器剪貼簿稽核。 **備註** 只有 Windows 用戶端支援從代理程式機器至用戶端機器剪貼簿稽核。
Configure clipboard memory size on server	指定伺服器的剪貼簿記憶體大小值 (以選取的位元組或 KB 為單位)。若未設定，則記憶體大小將以 KB 為單位。 用戶端也有剪貼簿記憶體大小的值，一律以 KB 為單位。在工作階段設定之後，伺服器會將其剪貼簿記憶體大小值傳送至用戶端。有效的剪貼簿記憶體大小值是用戶端和伺服器的剪貼簿記憶體大小值中較小者。 此設定僅適用於安裝了 Horizon Client 4.1 或更新版本的 Windows、Linux 和 Mac 用戶端，以及安裝了 Horizon Client 4.7 或更新版本的 iOS 用戶端。在較舊的版本中，剪貼簿記憶體大小會設為 1 MB，且無法設定。 **備註** 取決於您的網路，如果剪貼簿記憶體大小太大，可能會影響效能。VMware 建議您不要將剪貼簿記憶體大小設定為超過 16 MB 的值。
Configure clipboard redirection	決定允許剪貼簿重新導向的方向。您可選取以下其中一個值： ■ **僅啟用用戶端至代理程式** ■ **兩個方向都停用** ■ **兩個方向都啟用** ■ **僅啟用代理程式至用戶端** 剪貼簿重新導向是當做虛擬通道實作。如果已停用虛擬通道，剪貼簿重新導向就無法運作。 此設定只會套用至 Horizon Agent。 停用或未設定此設定時，預設值為**僅啟用用戶端到代理程式**。
Configure drag and drop direction	指定允許拖放的方向。啟用時，可用的選項如下所示： ■ **兩個方向都停用** ■ **僅啟用用戶端至代理程式**。僅允許從用戶端系統拖放至代理程式。 ■ **僅啟用代理程式至用戶端**。僅允許從代理程式拖放至用戶端系統。 ■ **兩個方向都啟用** 停用或未設定此設定時，預設值為**僅啟用用戶端到代理程式**。 此設定僅會套用至代理程式。

表 5-24. PCoIP 剪貼簿原則設定 (續)

設定	說明
Configure drag and drop formats	決定每個資料格式所允許的拖放方向 (**雙向停用**、**僅啟用代理程式至用戶端**、**僅啟用用戶端至代理程式**或**雙向啟用**)。啟用此設定時，可用的選項如下所示： ■ **檔案格式的選項** ■ **文字格式的選項** ■ **RTF 文字格式的選項** ■ **影像格式的選項** ■ **HTML 格式的選項** ■ **檔案內容格式的選項** 此設定停用或未設定時，所有格式的預設值都是**雙向啟用**。 此設定僅會套用至代理程式。
Configure drag and drop size threshold	決定拖曳檔案和資料夾以外的通用資料類型的大小限制。 此設定啟用時，請從**選擇拖放大小的單位**下拉式功能表中選取拖曳資料大小的單位。您可以選取**位元組**、**KB** 或 **MB**。在**拖放大小臨界值**文字方塊中選取或輸入拖曳資料大小。每個單位的有效資料範圍如下： ■ **位元組**：1 到 1023 ■ **KB**：1 到 1023 ■ **MB**：1 到 16 (拖放的資料大小上限為 16 MB) 此設定停用或未設定時，會設定預設臨界值 1 MB。 此設定僅會套用至代理程式。
Filter text out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉文字資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Rich Text Format data out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉 RTF 格式資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter images out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉影像資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Microsoft Office text data out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉 Microsoft Office 文字格式資料 (BIFF12 格式)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉 Microsoft Office 圖表和 SmartArt 資料 (Art::GVML ClipFormat)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Microsoft Text Effects data out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉 Microsoft Office 文字效果資料 (HTML 格式)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter text out of the outgoing clipboard data	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉文字資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Rich Text Format data out of the outgoing clipboard data	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉 RTF 格式資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter images out of the outgoing clipboard data	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉影像資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。

表 5-24. PCoIP 剪貼簿原則設定 (續)

設定	說明
`Filter Microsoft Office text data out of the outgoing clipboard data`	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉 Microsoft Office 文字格式資料 (BIFF12 格式)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
`Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data`	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉 Microsoft Office 圖表和 SmartArt 資料 (Art::GVML ClipFormat)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
`Filter Microsoft Text Effects data out of the outgoing clipboard data`	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉 Microsoft Office 文字效果資料 (HTML 格式)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
`Whether block clipboard redirection to client side when client doesn't support audit`	指定是否對不支援剪貼簿稽核功能的用戶端封鎖剪貼簿重新導向。 啟用此設定時，您必須選取下列其中一個值。 ■ **封鎖** - 這會在代理程式機器支援剪貼簿稽核功能但用戶端機器不支援的情況下，封鎖代理程式至用戶端剪貼簿重新導向。 ■ **傳遞** - 這會在代理程式機器支援剪貼簿稽核功能但用戶端機器不支援的情況下，允許代理程式至用戶端剪貼簿重新導向。 當此設定停用或未設定時，預設值為**封鎖**。 您必須啟用 `Configure clipboard audit` 群組原則設定，此設定才會生效。

PCoIP 頻寬設定

Horizon PCoIP ADMX 範本檔包含可設定 PCoIP 頻寬特性的群組原則設定。

所有這些設定位於群組原則管理編輯器的**電腦設定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 可覆寫的管理員預設值**資料夾中。

所有這些設定也位於群組原則管理編輯器的**使用者設定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 非可覆寫的管理員設定**資料夾中。

表 5-25. Horizon PCoIP 工作階段頻寬變數

設定	說明
Configure the maximum PCoIP session bandwidth	指定 PCoIP 工作階段中的最大頻寬 (單位 KB/秒)。頻寬包括所有映像處理、音訊、虛擬通道、USB 和控制 PCoIP 流量。 將此值設定為端點所連線連結的總容量，並考量預期的並行 PCoIP 工作階段數目。例如，單一使用者的 VDI 組態 (即單一 PCoIP 工作階段) 是透過 4Mbit/s 網際網路連線來連線時，請將此值設為 4Mbit，或設定一個比此值低 10% 的值，留一些空間供其他網路流量使用。當您預期會有多個並行 PCoIP 工作階段共用一個包含多個 VDI 使用者或單一 RDS 組態的連結時，可能需要相應地調整此設定。但是，降低此值會限制每個作用中工作階段的最大頻寬。 設定此值可防止代理程式嘗試以高於連結容量的速率傳輸，這樣可能造成大量封包遺失並產生較差的使用者體驗。此值為對稱的。它會強制用戶端和代理程式使用用戶端和代理程式端上所設定的兩個值中的較低者。例如，將最大頻寬設定為 4Mbit/s 會強制代理程式以較低速率傳輸，即使該設定是在用戶端上設定的也一樣。 在端點上停用或未設定此設定時，端點就不會實施任何頻寬限制。設定此設定時，設定會當做端點的最大頻寬限制使用 (單位為每秒 kb)。 未設定此設定時的預設值為每秒 900000 KB。 此設定會套用至 Horizon Agent 和用戶端。如果兩個端點擁有不同的設定，則會使用較小的值。
Configure the PCoIP session bandwidth floor	指定 PCoIP 工作階段所保留頻寬的下限值 (單位為每秒 KB)。 此設定會設定端點的預期最小頻寬傳輸速率。當您使用此設定保留端點的頻寬時，使用者就不必等待可用的頻寬，如此就能改善工作階段的回應能力。 請確認不要過度訂閱所有端點的總保留頻寬。確定組態中所有連線的頻寬下限總和未超過網路能力。 預設值為 0，表示未保留最小頻寬。停用或未設定此設定時，不會保留最小頻寬。 此設定會套用至 Horizon Agent 和用戶端，但是只會影響設定此設定所在的端點。 在作用中的 PCoIP 工作階段期間修改此設定時，變更會立即生效。
Configure the PCoIP session MTU	針對 PCoIP 工作階段的 UDP 封包，指定傳輸單元最大值 (MTU) 大小。 MTU 大小包括 IP 和 UDP 封包標頭。TCP 會使用標準 MTU 探索機制設定 MTU，因此不會受此設定影響。 MTU 大小的最大值為 1500 個位元組。MTU 大小的最小值為 500 個位元組。預設值為 1300 個位元組。 通常您不需要變更 MTU 大小。如果您使用非一般的網路設定而造成 PCoIP 封包分段，請變更此值。 此設定會套用至 Horizon Agent 和用戶端。如果兩個端點擁有不同的 MTU 大小設定，則會使用最小的值。 如果停用或未設定此設定，用戶端會使用預設值與 Horizon Agent 交涉。

表 5-25. Horizon PCoIP 工作階段頻寬變數 (續)

設定	說明
`Configure the PCoIP session audio bandwidth limit`	指定 PCoIP 工作階段中的音訊 (聲音播放) 可使用的最大頻寬。 音訊處理會監控音訊所使用的頻寬。處理程序會選取在目前頻寬利用下，提供最佳音訊的音訊壓縮演算法。如果有設定頻寬限制，處理程序會變更壓縮演算法的選項來降低品質，直到達到頻寬限制為止。如果在指定的頻寬限制內無法提供最低品質的音訊，則會停用音訊。 若要允許未經壓縮的高品質立體聲音訊，請將此值設為高於每秒 1600 KB。值為每秒 450 KB 以上時，可提供立體聲的高品質壓縮音訊。介於每秒 50 KB 和 450 KB 之間的值時，會提供介於 FM 廣播和電話通話品質之間的音訊。低於每秒 50 KB 的值可能會導致沒有播放任何音訊。 此設定只會套用至 Horizon Agent。您必須在兩個端點上啟用音訊，此設定才會產生作用。 此外，此設定對於 USB 音訊沒有作用。 如果停用或未設定此設定，則會設定每秒 500 KB 的預設音訊頻寬限制來限制選取的音訊壓縮演算法。如果設定此設定，值的測量單位為每秒 kb，且預設音訊頻寬限制為每秒 500 kb。 此設定會套用至 View 4.6 和更新版本。此設定對於舊版 View 沒有作用。 在作用中的 PCoIP 工作階段期間修改此設定時，變更會立即生效。
`Turn off Build-to-Lossless feature`	指定要關閉還是開啟 PCoIP 通訊協定的不失真功能。此功能依預設已關閉。 如果已啟用或未設定此設定，將會關閉不失真功能，並且永遠無法以不失真狀態建立映像和其他桌面平台與應用程式內容。在頻寬受限的網路環境中，關閉不失真功能可節省頻寬。 如果停用此設定，將會開啟不失真功能。在需要以不失真狀態建立映像和其他桌面平台與應用程式內容的環境中，建議開啟不失真功能。 在作用中的 PCoIP 工作階段期間修改此設定時，變更會立即生效。 如需「PCoIP 不失真」功能的詳細資訊，請參閱 PCoIP 不失真功能。

PCoIP 鍵盤設定

View PCoIP ADMX 範本檔包含的群組原則設定可設定影響鍵盤使用的 PCoIP 設定。

所有這些設定位於群組原則管理編輯器的**電腦設定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 可覆寫的管理員預設值**資料夾中。

所有這些設定也位於群組原則管理編輯器的**使用者設定 > 原則 > 系統管理範本 > PCoIP 工作階段變數 > 非可覆寫的管理員設定**資料夾中。

表 5-26. 鍵盤的 Horizon PCoIP 工作階段變數

設定	說明
`Disable sending CAD when users press Ctrl+Alt+Del`	啟用此原則後，使用者必須按 Ctrl+Alt+Insert (而非 Ctrl+Alt+Del)，才能在 PCoIP 工作階段期間將 Secure Attention Sequence (SAS) 傳送至遠端桌面平台。 如果使用者在按 Ctrl+Alt+Del 來鎖定用戶端端點，並將 SAS 同時傳送到主機和客體時，感到疑惑，您可以啟用此設定。 此設定只會套用至 Horizon Agent，因此對用戶端沒有作用。 未設定或停用此原則時，使用者可以按 Ctrl+Alt+Del 或 Ctrl+Alt+Insert，將 SAS 傳送至遠端桌面平台。
`Use alternate key for sending Secure Attention Sequence`	指定替代鍵 (而非 Insert 鍵) 來傳送 Secure Attention Sequence (SAS)。 您可以使用此設定，在 PCoIP 工作階段期間，於自遠端桌面平台內部啟動的虛擬機器上，保留 Ctrl+Alt+Ins 鍵序列。 例如，使用者可以從 PCoIP 桌面平台內部啟動 vSphere Client，並在 vCenter Server 的虛擬機器上開啟主控台。如果在 vCenter Server 虛擬機器的客體作業系統內部使用 Ctrl+Alt+Ins 序列，就會將 Ctrl+Alt+Del SAS 傳送到虛擬機器。此設定可讓 Ctrl+Alt+*替代鍵* 序列將 Ctrl+Alt+Del SAS 傳送到 PCoIP 桌面平台。 啟用此設定時，您必須從下拉式功能表中選取一個替代鍵。啟用此設定時，必須指定此值。 停用或未設定此設定時，會將 Ctrl+Alt+Ins 鍵序列當做 SAS 使用。 此設定只會套用至 Horizon Agent，因此對用戶端沒有作用。

PCoIP 不失真功能

您可以將 PCoIP 顯示通訊協定設定為使用名為漸進式建立或不失真的編碼方法，此方法即使在網路條件受到限制的狀況下，也能提供最佳的整體使用者體驗。此功能依預設已關閉。

不失真功能會提供高度壓縮的初始映像，稱做失真映像，接著漸進式地將映像建立成完全無失真的狀態。無失真的狀態表示映像會以全真顯示。

在 LAN 上，PCoIP 一律使用無失真壓縮顯示文字。如果開啟不失真功能，而且如果每個工作階段的可用頻寬下降到 1 Mbs 以下，PCoIP 一開始會顯示失真的文字映像，然後快速地將映像建立為不失真狀態。此方法可讓桌面平台保持會回應，並在不斷變化的網路條件下顯示可能的最佳映像，以提供最佳的使用者經驗。

不失真功能有以下特色：

- 動態調整映像品質
- 當網路壅塞時降低映像品質
- 透過減少畫面更新的延遲性讓畫面繼續有回應
- 當網路不再壅塞時恢復最高的映像品質

您可以藉由停用 `Turn off Build-to-Lossless feature` 群組原則設定來開啟不失真功能。請參閱 PCoIP 頻寬設定。

VMware Blast 原則設定

VMware Blast ADMX 範本檔 (vdm_blast.admx) 包含 VMware Blast 顯示通訊協定的原則設定。在套用原則後，這些設定會儲存在登錄機碼 HKLM\Software\Policies\VMware, Inc.\VMware Blast\config 中。

這些設定適用於 HTML Access 和所有 Horizon Client 平台。

表 5-27. VMware Blast 原則設定

設定	說明
Audio playback	指定是否要啟用遠端桌面平台的音訊播放。此設定會啟用音訊播放。
Clipboard memory size on server	指定伺服器的剪貼簿記憶體大小值 (以選取的位元組或 KB 為單位)。若未設定，則記憶體大小將以 KB 為單位。 用戶端也有剪貼簿記憶體大小的值，一律以 KB 為單位。在工作階段設定之後，伺服器會將其剪貼簿記憶體大小值傳送至用戶端。有效的剪貼簿記憶體大小值是用戶端和伺服器的剪貼簿記憶體大小值中較小者。 對於 Windows 用戶端，Horizon Client 4.9 及更新版本支援從代理程式機器至用戶端機器剪貼簿稽核。對於所有用戶端，Horizon Client 4.10 及更新版本支援從用戶端機器到代理程式機器剪貼簿稽核。 **備註** 只有 Windows 用戶端支援從代理程式機器至用戶端機器剪貼簿稽核。
Configure clipboard audit	指定是否在代理程式機器上啟用剪貼簿稽核功能。啟用此設定時，可用的選項如下所示： ■ **雙向停用** - 不記錄剪貼簿資料的相關資訊。 ■ **僅啟用用戶端至伺服器** - 代理程式機器上的事件記錄中會記錄有關從用戶端機器複製到代理程式機器之剪貼簿資料的相關資訊。 ■ **雙向啟用** - 代理程式機器上的事件記錄中會記錄有關從用戶端機器複製到代理程式機器以及從代理程式機器複製到用戶端機器的剪貼簿資料的相關資訊。 ■ **僅啟用伺服器至用戶端** - 代理程式機器上的事件記錄中會記錄有關從代理程式機器複製到用戶端機器的剪貼簿資料的相關資訊。 當此設定停用或未設定時，預設值將是**雙向停用**。 **備註** 只有 Windows 用戶端支援從代理程式機器至用戶端機器剪貼簿稽核。所有其他用戶端僅支援從用戶端機器到代理程式機器剪貼簿稽核。 您可以使用代理程式機器上的 Windows 事件檢視器來檢視事件記錄。記錄名稱為 VMware Horizon RX 稽核。若要從集中位置檢視事件記錄，您可以設定 VMware Log Insight 或 Windows Event Collector。
Configure clipboard redirection	指定容許的剪貼簿重新導向行為。選項如下所示： ■ **兩個方向都啟用** ■ **兩個方向都停用** ■ **僅啟用用戶端至伺服器** ■ **僅啟用伺服器至用戶端** 預設值為**僅啟用用戶端至伺服器**。
Configure drag and drop direction	指定允許拖放的方向。啟用此設定時，可用的選項如下所示： ■ **兩個方向都停用** ■ **僅啟用用戶端至代理程式**。僅允許從用戶端系統拖放至代理程式。 ■ **僅啟用代理程式至用戶端**。僅允許從代理程式拖放至用戶端系統。 ■ **兩個方向都啟用** 停用或未設定此設定時，預設值為**僅啟用用戶端到代理程式**。 此設定僅會套用至代理程式。

表 5-27. VMware Blast 原則設定 (續)

設定	說明
Configure drag and drop formats	決定每個資料格式所允許的拖放方向 (**雙向停用**、**僅啟用代理程式至用戶端**、**僅啟用用戶端至代理程式**或**雙向啟用**)。啟用此設定時，可用的選項如下所示： ■ **檔案格式的選項** ■ **文字格式的選項** ■ **RTF 文字格式的選項** ■ **影像格式的選項** ■ **HTML 格式的選項** ■ **檔案內容格式的選項** 此設定停用或未設定時，所有格式的預設值都是**雙向啟用**。 此設定僅會套用至代理程式。
Configure drag and drop size threshold	決定拖曳檔案和資料夾以外的通用資料類型的大小限制。 此設定啟用時，請從**選擇拖放大小的單位**下拉式功能表中選取拖曳資料大小的單位。您可以選取**位元組**、**KB** 或 **MB**。在**拖放大小臨界值**文字方塊中選取或輸入拖曳資料大小。每個單位的有效資料範圍如下： ■ **位元組**：1 到 1023 ■ **KB**：1 到 1023 ■ **MB**：1 到 16 (拖放的資料大小上限為 16 MB) 此設定停用或未設定時，會設定預設臨界值 1 MB。 此設定僅會套用至代理程式。
Configure file transfer	指定遠端桌面平台與 HTML Access 用戶端之間的檔案傳輸容許行為。您可選取以下其中一個值： ■ **同時停用上傳和下載** ■ **同時啟用上傳和下載** ■ **僅啟用檔案上傳** (使用者僅可以從用戶端系統上傳檔案至遠端桌面平台。) ■ **僅啟用檔案下載** (使用者僅可以從遠端桌面平台下載檔案至用戶端系統。) 預設值為**僅啟用檔案上傳**。 此設定僅適用於 HTML Access 4.1 和更新版本。
Cookie Cleanup Interval	決定與非作用中工作階段相關聯之 Cookie 的刪除頻率 (以毫秒為單位)。預設值為 100 毫秒。

表 5-27. VMware Blast 原則設定 (續)

設定	說明
DSCP Marking	啟用或未設定時，此設定將允許在傳出 Blast 網路流量中建立區別服務代碼點 (DSCP) 值，此值是由各種個別設定針對每個網路躍點所指定。停用時，系統不會在 Blast 網路流量中建立 DSCP 值。 啟用時，您可針對下列網路連線設定範圍介於 0-63 的數值： ■ DSCP from Agent, TCP/IPv4 ■ DSCP from Agent, TCP/IPv6 ■ DSCP from Agent, UDP/IPv4 ■ DSCP from Agent, UDP/IPv6 ■ DSCP from BSG to Client, TCP/IPv4 ■ DSCP from BSG to Client, TCP/IPv6 ■ DSCP from BSG to Client, UDP/IPv4 ■ DSCP from BSG to Client, UDP/IPv6 ■ DSCP from BSG to Agent, TCP/IPv4 ■ DSCP from BSG to Agent, TCP/IPv6 ■ DSCP from BSG to Agent, UDP/IPv4 ■ DSCP from BSG to Agent, UDP/IPv6 ■ DSCP from Client, TCP/IPv4 ■ DSCP from Client, TCP/IPv6 ■ DSCP from Client, UDP/IPv4 ■ DSCP from Client, UDP/IPv6
Filter images out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉影像資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter images out of the outgoing clipboard data	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉影像資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉 Microsoft Office 圖表和 SmartArt 資料 (Art::GVML ClipFormat)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉 Microsoft Office 圖表和 SmartArt 資料 (Art::GVML ClipFormat)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Microsoft Office text data out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉 Microsoft Office 文字格式資料 (BIFF12 格式)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Microsoft Office text data out of the outgoing clipboard data	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉 Microsoft Office 文字格式資料 (BIFF12 格式)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。

表 5-27. VMware Blast 原則設定 (續)

設定	說明
Filter Microsoft Text Effects data out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉 Microsoft Office 文字效果資料 (HTML 格式)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Microsoft Text Effects data out of the outgoing clipboard data	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉 Microsoft Office 文字效果資料 (HTML 格式)。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Rich Text Format data out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉 RTF 格式資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter Rich Text Format data out of the outgoing clipboard data	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉 RTF 格式資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter text out of the incoming clipboard data	指定是否將來自用戶端至代理程式的剪貼簿資料篩選掉文字資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
Filter text out of the outgoing clipboard data	指定是否將傳送自代理程式至用戶端的剪貼簿資料篩選掉文字資料。啟用此設定並選取核取方塊時，會篩選掉資料。停用或未設定此設定時，則會允許資料。
H264	指定要使用 H.264 編碼還是 JPEG/PNG 編碼。預設值是使用 H.264 編碼。
H264 High Color Accuracy	在使用 H.264 編碼時以 YUV 4:4:4 色彩空間 (而非 4:2:0) 提高色彩準確度。 在使用極高解析度或多台監視器的情況下，此設定可能會導致效能下降。
H.264 Quality	針對設定為使用 H.264 編碼的遠端顯示指定影像畫質。您可以指定可決定控制影像無失真壓縮的最小和最大量化值。您可以指定最小量化值以獲得最佳影像畫質。您可以指定最大量化值以獲得最低影像畫質。您可以指定下列設定： ■ **H264maxQP** (可用值範圍：0-51，預設值：36) ■ **H264minQP** (可用值範圍：0-51，預設值：10) 如需最佳影像畫質，請將量化參數 (QP) 值設定為在可用值範圍的 +5 或 -5 之內。這些參數會判斷捨棄的資料量，因此較低的值會產生較高的影像畫質。
HEVC	啟用或未設定此設定時，系統會允許 HEVC 編碼以進行桌面平台的遠端處理。停用此設定時，系統會使用 H.264 或 JPEG/PNG 進行編碼。
HTTP Service	指定安全伺服器或 Access Point 應用裝置與桌面平台之間的安全通訊 (HTTPS) 所使用的連接埠。必須設定防火牆以開啟此連接埠。預設值為 22443。
Image Quality	指定遠端顯示的影像畫質。您可以指定兩個低畫質設定、兩個高畫質設定和一個中等畫質設定。低畫質設定用於經常變動的畫面區域，例如，在執行捲動時。高畫質設定用於較為靜態的畫面區域，可產生較佳影像畫質。您可以指定下列設定： ■ **低 JPEG 畫質** (可用值範圍：10 - 100，預設值：25) ■ **中 JPEG 畫質** (可用值範圍：10 - 100，預設值：35) ■ **高 JPEG 畫質** (可用值範圍：10 - 100，預設值：90)

表 5-27. VMware Blast 原則設定 (續)

設定	說明
Keyboard locale synchronization	指定是否要將用戶端的鍵盤地區設定清單和預設鍵盤地區設定同步至遠端桌面平台或應用程式。啟用此設定時，將會執行同步。此設定只會套用至 Horizon Agent。 **備註** 只有 Windows 版 Horizon Client 支援此功能。
Max Frame Rate	指定畫面更新的最大速率。使用此設定，可管理使用者所使用的平均頻寬。預設值為每秒 30 次更新。
Max Session Bandwidth	指定 VMware Blast 工作階段的最大頻寬 (單位為千位元/秒，即 kbps)。頻寬包括所有影像處理、音訊、虛擬通道、USB 和 VMware Blast 控制流量。預設值為 1 Gbps。
Max Session Bandwidth kbit/s Megapixel Slope	指定為 VMware Blast 工作階段保留的最大頻寬斜率 (單位為千位元/秒，即 kbps)。最小值為 100。最大值為 100000。預設值為 6200。
Min Session Bandwidth	指定為 VMware Blast 工作階段保留的最小頻寬 (單位為千位元/秒，即 kbps)。預設值為 256 kbps。
PNG	如果您啟用此設定或未進行此設定，則遠端工作階段可使用 PNG 編碼。如果您停用此設定，則 JPEG/PNG 模式中的編碼只會使用 JPEG 編碼。當 H.264 編碼器作用中時，此原則不適用。此設定依預設不會設定。
Screen Blanking	指定在桌面平台具有使用中的工作階段時，要讓桌面平台虛擬機器的主控台顯示使用者實際看到的桌面平台，還是顯示空白畫面。預設值是顯示空白畫面。
UDP Protocol	指定要使用 UDP 還是 TCP 通訊協定。預設值是使用 UDP 通訊協定。必須將登錄機碼所在的 Horizon Agent 機器重新開機才能完成此設定。此設定不適用於一律會使用 TCP 通訊協定的 HTML Access。
Whether block clipboard redirection to client side when client doesn't support audit	決定是否對不支援剪貼簿稽核功能的用戶端機器封鎖剪貼簿重新導向。 啟用此設定時，您必須選取下列其中一個值。 ■ **封鎖** - 這會在代理程式機器支援剪貼簿稽核功能但用戶端機器不支援的情況下，封鎖代理程式至用戶端剪貼簿重新導向。 ■ **傳遞** - 這會在代理程式機器支援剪貼簿稽核功能但用戶端機器不支援的情況下，允許代理程式至用戶端剪貼簿重新導向。 當此設定停用或未設定時，預設值為**封鎖**。 您必須啟用 Configure clipboard audit 群組原則設定，此設定才會生效。

套用 VMware Blast 原則設定

如果下列 VMware Blast 原則在用戶端工作階段期間有所變更，Horizon Client 會偵測到該變更，並立即套用新的設定。

- H264
- Audio Playback
- Max Session Bandwidth
- Min Session Bandwidth
- Max Frame Rate
- Image Quality

其餘所有的 VMware Blast 原則均適用 Microsoft GPO 更新規則。GPO 可以手動更新，或藉由重新啟動 Horizon Agent 機器來更新。如需詳細資訊，請參閱 Microsoft 說明文件。

啟用 VMware Blast 的無失真壓縮

您可以啟用 VMware Blast 顯示通訊協定，以使用名為漸進式建立或不失真的編碼方法。此功能會提供高度壓縮的初始映像，稱做失真映像，接著漸進式地將映像建立成完全無失真的狀態。無失真的狀態表示映像會以全真顯示。

若要啟用 VMware Blast 的無失真壓縮，請在代理程式機器上的 Windows 登錄中，將 `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` 資料夾中的 `EncoderBuildToPNG` 機碼設定為 `1`。預設值為 `0` (停用)，這表示轉碼器不會建立屬於無失真格式的 PNG。

`EncoderBuildToPNG` 機碼的組態變更會立即生效。

備註 啟用 VMware Blast 的無失真壓縮時，頻寬和 CPU 的使用量會因而增加。如果您需要無失真壓縮功能，VMware 建議您使用 PCoIP 顯示通訊協定，而不要使用 VMware Blast。如需設定 PCoIP 之無失真壓縮的相關資訊，請參閱 PCoIP 不失真功能。

使用遠端桌面平台服務群組原則

您可以使用遠端桌面平台服務群組原則，控制 RDS 主機和已發佈桌面平台與應用程式工作階段的組態和效能。Horizon 7 提供 ADMX 檔案，其中包含 Horizon 7 支援的 Microsoft RDS 群組原則。

最佳做法是設定 Horizon 7 ADMX 檔案中提供的群組原則，而非對應的 Microsoft 群組原則。Horizon 7 群組原則經認證可支援 Horizon 7 部署。

遠端桌面服務應用程式相容性設定

RDS 應用程式相容性群組原則設定控制 Windows 安裝程式相容性、遠端桌面平台 IP 虛擬化、網路介面卡選取，以及 RDS 主機 IP 位址的使用。

表 5-28. RDS 應用程式相容性群組原則設定

設定	說明
Turn off Windows Installer RDS Compatibility	此原則設定指定，對於完整安裝的應用程式是否以每個使用者為基礎執行 Windows 安裝程式 RDS 相容性。Windows 安裝程式允許一次執行 `msiexec` 程序的一個執行個體。依預設，Windows 安裝程式 RDS 相容性會開啟。 如果啟用此原則設定，Windows 安裝程式 RDS 相容性會關閉，並且一次僅能執行 `msiexec` 程序的一個執行個體。 如果停用或不設定此原則設定，則 Windows 安裝程式 RDS 相容性會開啟，且多個使用者應用程式安裝要求會佇列並且以收到的順序由 `msiexec` 程序處理。

Turn on Remote Desktop IP Virtualization	此原則設定指定遠端桌面平台 IP 虛擬化是否已開啟。
	依預設，遠端桌面平台 IP 虛擬化會關閉。
	如果啟用此原則設定，遠端桌面平台 IP 虛擬化會開啟。您可以選取會套用此設定的模式。如果使用「依程式」模式，您必須輸入程式清單以使用虛擬 IP 位址。列出每個程式，一行一個 (請勿在程式之間輸入任何空白行)。例如：
	`explorer.exe`
	`mstsc.exe`
	如果停用或不設定此原則設定，則遠端桌面平台 IP 虛擬化會關閉。

Select the network adapter to be used for Remote Desktop IP Virtualization	此原則設定指定與用於虛擬 IP 位址的網路介面卡對應的 IP 位址和網路遮罩。應該在無類別網域間路由選擇標記法中輸入 IP 位址和網路遮罩。例如： 192.0.2.96/24. 若啟用此原則設定，指定的 IP 位址和網路遮罩會用於選取虛擬 IP 位址所用的網路介面卡。 如果停用或不設定此原則設定，則遠端桌面平台 IP 虛擬化會關閉。必須設定網路介面卡，遠端桌面平台 IP 虛擬化才能正常運作。
Do not use Remote Desktop Session Host server IP address when virtual IP address is not available	此原則設定會指定在虛擬 IP 位址無法使用時，工作階段是否使用 RDS 主機的 IP 位址。 如果啟用此原則設定，則虛擬 IP 無法使用時，將不會使用 RDS 主機的 IP 位址。工作階段將不具備網路連線能力。 如果停用或未設定此原則設定，則虛擬 IP 無法使用時，將會使用 RDS 主機的 IP 位址。

遠端桌面服務連線設定

RDS 連線群組原則設定可讓使用者為 RDS 主機上的工作階段設定連線的原則。

Horizon 7 RDS 群組原則設定安裝於**電腦設定 > 原則 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 連線**資料夾中。

Horizon 7 RDS 群組原則設定也安裝於**使用者設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 連線**資料夾中。

表 5-29. RDS 連線群組原則設定

設定	說明
Automatic reconnection	指定是否要在遠端桌面連線用戶端的網路連結暫時中斷時，允許這些用戶端自動重新連線至 RDS 主機上的工作階段。依預設會以五秒為間隔嘗試重新連線，最多二十次。 如果啟用此原則設定，則所有執行遠端桌面連線之用戶端在網路連線中斷時，都會嘗試自動重新連線。 如果停用此原則設定，則會禁止用戶端的自動重新連線。 若未設定此原則設定，則不會在群組原則層級上指定自動重新連線。不過，使用者可使用遠端桌面連線中的**進階設定**索引標籤上的**如果連線中斷的話，重新連線**核取方塊，設定自動重新連線。
Allow users to connect remotely using Remote Desktop Services	此原則會設定使用遠端桌面服務對電腦的遠端存取。 如果您啟用此原則設定，使用者若是目標電腦上的「遠端桌面使用者」群組成員，將可使用遠端桌面服務從遠端連線至目標電腦。 如果停用此原則設定，使用者即無法使用遠端桌面服務從遠端連線至目標電腦。目標電腦將保留任何目前的連線，但將不接受任何新的傳入連線。 若未設定此原則設定，遠端桌面服務會使用目標電腦上的遠端桌面設定來決定是否允許遠端連線。此設定位於**系統內容**中的**遠端**索引標籤上。依預設不會允許遠端連線。 **備註** 您可以設定位於**電腦設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 安全性**資料夾中的「透過使用網路層級驗證以要求對遠端連線進行使用者驗證」原則設定，限制哪些用戶端能夠使用遠端桌面服務從遠端連線。您可以在 [遠端桌面工作階段主機設定] 工具中的**網路介面卡**索引標籤上設定 [連線數目上限] 選項，或設定位於**電腦設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 連線**資料夾中的「限制連線數目」原則設定，以限制可同時連線的使用者數目。
Deny logoff of an administrator logged in to the console session	此原則設定可決定嘗試從遠端連線至伺服器主控台的管理員，是否可將目前登入主控台的管理員登出。 當目前連線的管理員不想遭到其他管理員登出時，此原則將相當實用。如果連線的管理員遭到登出，先前未儲存的任何資料都將遺失。 如果啟用此原則設定，即不允許登出連線的管理員。 如果停用或未設定此原則設定，即允許登出連線的管理員。 **備註** 主控台工作階段也稱為「工作階段 0」。您可以在電腦欄位名稱的遠端桌面連線或命令列中使用 `/console` 參數，來取得主控台的存取權。

表 5-29. RDS 連線群組原則設定 (續)

設定	說明
Configure keep-alive connection interval	此原則設定可讓您輸入持續連線間隔，以確保 RDS 主機上的工作階段狀態與用戶端狀態是一致的。 用戶端失去與 RDS 主機的連線後，RDS 主機上的工作階段仍可保持使用中狀態，而不是變更為中斷連線狀態，即使用戶端實際上已中斷與 RDS 主機的連線亦然。如果用戶端再次登入相同的 RDS 主機，則系統可能會建立新的工作階段 (如果 RDS 主機設定成允許多個工作階段)，且原始工作階段仍可保持為使用中。 如果啟用此原則設定，則必須輸入持續連線間隔。持續連線間隔會決定伺服器檢查工作階段狀態的頻率 (以分鐘為單位)。您可以輸入的值範圍為 1 到 999,999。 如果停用或未設定此原則設定，則不會設定持續連線間隔，且伺服器將不會檢查工作階段狀態。
Limit number of connections	指定遠端桌面服務是否會限制伺服器的同時連線數目。 您可以使用此設定來限制伺服器上可處於使用中狀態的「遠端桌面服務」工作階段數目。超出此數目時，嘗試連線的其他使用者將會收到一則錯誤訊息，表示伺服器忙碌中請稍後再試一次。限制工作階段數目可提升效能，因為需要系統資源的工作階段較少。依預設，RDS 主機會允許無數目限制的「遠端桌面服務」工作階段，而系統管理的遠端桌面則會允許兩個「遠端桌面服務」工作階段。 若要使用此設定，請輸入要指定為伺服器連線數目的上限。若要指定無數目限制的連線，請輸入 999999。 如果啟用此原則設定，連線數目上限將會限制為與伺服器上執行的 Windows 版本和遠端桌面服務模式所指定的數目一致。 如果停用或未設定此原則設定，則不會在群組原則層級上強制限制連線數目。 **備註** 此設定的設計是用於 RDS 主機上，這些主機伺服器執行 Windows 作業系統，且安裝有「遠端桌面工作階段主機」角色服務。
Set rules for remote control of Remote Desktop Services user sessions	使用此原則設定，可指定「遠端桌面服務」工作階段中允許的遠端控制層級。 您可以使用此原則設定選取兩個遠端控制層級的其中之一：「檢視工作階段」或「完全控制」。「檢視工作階段」允許遠端控制使用者查看工作階段。「完全控制」允許管理員與工作階段互動。遠端控制可在使用者授與或未授與權限的情況下建立。 如果啟用此原則設定，管理員將可根據指定的規則，與使用者的「遠端桌面服務」工作階段進行遠端互動。若要設定這些規則，請在 [選項] 清單中選取所需的控制層級和權限。若要停用遠端控制，請選取「不允許遠端控制」。 如果停用或未設定此原則設定，遠端控制規則將取決於 [遠端桌面工作階段主機設定] 工具之**遠端控制**索引標籤上的設定。依預設，在使用者授與權限的情況下，遠端控制使用者具有工作階段的完全控制權。 **備註** 此原則設定會同時顯示在「電腦設定」和「使用者設定」中。如果同時設定了這兩個原則設定，則以「電腦設定」原則設定優先。

表 5-29. RDS 連線群組原則設定 (續)

設定	說明
Restrict Remote Desktop Services users to a single Remote Desktop Services session	使用此原則設定，可限制使用者僅能擁有一個「遠端桌面服務」工作階段。 如果啟用此原則設定，使用遠端桌面服務從遠端登入的使用者，將被限制在該伺服器上只能有單一工作階段 (使用中或中斷連線)。如果使用者退出工作階段，並使其成為中斷連線狀態，則在下次登入時，使用者將自動重新連線至該工作階段。 如果停用此原則設定，使用者將可使用遠端桌面服務建立不受限制的同時遠端連線。 若未設定此原則設定，則「遠端桌面工作階段主機設定」工具中的 [限制每個使用者只能有一個工作階段] 設定將決定是否限制使用者只能有一個遠端桌面服務工作階段。
Allow remote start of unlisted programs	使用此原則設定，可指定遠端使用者在啟動「遠端桌面服務」工作階段時，是否可啟動 RDS 主機上的任何程式，或僅能啟動 [RemoteApp 程式] 清單中列出的程式。 您可以使用 RemoteApp 管理員工具建立 RemoteApp 程式清單，以控制可從遠端啟動 RDS 主機上的哪些程式。依預設，使用者在啟動「遠端桌面服務」工作階段時只能啟動 [RemoteApp 程式] 清單中的程式。 如果啟用此原則設定，則遠端使用者在啟動「遠端桌面服務」工作階段時將可啟動 RDS 主機上的任何程式。例如，遠端使用者可在連線時使用「遠端桌面連線」用戶端指定程式的可執行檔路徑來啟動任何程式。 如果停用或未設定此原則設定，則遠端使用者在啟動「遠端桌面服務」工作階段時，將只能啟動 RemoteApp 管理員的 [RemoteApp 程式] 清單中列出的程式。
Turn off Fair Share CPU Scheduling	公平共用 CPU 排程會根據工作階段數量和每個工作階段中的處理器時間需求，在同一 RDS 主機上的所有遠端桌面服務工作階段之間動態分配處理器時間。 如果啟用此原則設定，則會關閉公平共用 CPU 排程。 如果停用或不設定此原則設定，則會開啟公平共用 CPU 排程。

RDS 裝置和資源重新導向設定

RDS 裝置及資源重新導向群組原則設定控制遠端桌面服務工作階段中用戶端電腦上的裝置存取和資源存取。

Horizon 7 RDS 群組原則設定安裝於**電腦設定 > 原則 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 裝置及資源重新導向**資料夾中。

Horizon 7 RDS 群組原則設定也安裝於**使用者設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 裝置及資源重新導向**資料夾中。

表 5-30. RDS 裝置及資源重新導向群組原則設定

設定	說明
Allow audio and video playback redirection	使用此原則設定，可指定使用者是否可在「遠端桌面服務」工作階段中重新導向遠端電腦的音訊和視訊輸出。 使用者可在遠端桌面連線 (RDC) 中的 [本機資源] 索引標籤上設定遠端音訊設定，以指定遠端電腦音訊輸出的播放位置。使用者可選擇在遠端電腦或本機電腦上播放遠端音訊。使用者也可選擇不播放音訊。使用遠端桌面通訊協定 (.rdp) 檔案中的 videoplayback 設定，可設定視訊播放。依預設會啟用視訊播放。 依預設，在連線至執行 Windows Server 2008 R2、Windows Server 2008 或 Windows Server 2003 的電腦時，將不允許音訊與視訊播放重新導向。連線至執行 Windows 7、Windows Vista 或 Windows XP Professional 的電腦時，依預設會允許音訊與視訊播放重新導向。 如果啟用此原則設定，將會允許音訊與視訊播放重新導向。 如果停用這個原則設定，就不允許重新導向音訊與視訊播放，即使已在 RDC 中指定音訊播放重新導向，或已在 .rdp 檔案中指定視訊播放。 如果未設定這個原則設定，則由遠端桌面工作階段主機設定工具中 [用戶端設定] 索引標籤上的 [音訊與視訊播放] 設定來決定是否允許重新導向音訊與視訊播放。
Allow audio recording redirection	使用此原則設定，可指定使用者是否可在「遠端桌面服務」工作階段中將音訊錄製到遠端電腦。 使用者可在遠端桌面連線 (RDC) 中的 [本機資源] 索引標籤上設定遠端音訊設定，以指定是否將音訊錄製到遠端電腦。使用者可使用本機電腦上的音訊輸入裝置 (例如內建麥克風) 來錄製音訊。 依預設，連線至執行 Windows Server 2008 R2 的電腦時，將不允許音訊錄製重新導向。連線至執行 Windows 7 的電腦時，依預設會允許音訊錄製重新導向。 如果啟用此原則設定，將會允許音訊錄製重新導向。 如果您停用這個原則設定，就不允許音訊錄製重新導向，即使已在 RDC 中指定音訊錄製重新導向。 如果未設定這個原則設定，則由遠端桌面工作階段主機設定工具中 [用戶端設定] 索引標籤上的 [錄製音訊] 設定來決定是否允許音訊錄製重新導向。
Limit audio playback quality	使用此原則設定，可限制「遠端桌面服務」工作階段的音訊播放品質。限制音訊播放的品質可以改善連線效能，特別是使用慢速連結時。 如果啟用這個原則設定，您必須選取下列其中一項：[高]、[中] 或 [動態]。如果選取 [高]，音訊會在最短延遲的狀況下，不經壓縮立即傳送。此選項需要大量頻寬。如果選取 [中]，音訊會在所用轉碼器決定的最短延遲內，經壓縮後傳送。如果選取 [動態]，則依遠端連線的頻寬決定壓縮等級後，將音訊壓縮後傳送。 使用這個原則設定在遠端電腦上所指定的音訊播放品質是遠端桌面服務工作階段可用的最高品質，而不論用戶端電腦上設定的音訊播放品質為何。例如，如果用戶端電腦上設定的音訊播放品質較高，遠端電腦上設定的音訊播放品質較低，將使用較低的音訊播放品質。 使用遠端桌面通訊協定 (.rdp) 檔案中的 audioqualitymode 設定，可在用戶端電腦上設定音訊播放品質。依預設，音訊播放品質會設為「動態」。

表 5-30. RDS 裝置及資源重新導向群組原則設定 (續)

設定	說明
Do not allow clipboard redirection	指定在「遠端桌面服務」工作階段期間是否要防止遠端電腦與用戶端電腦之間的剪貼簿內容共用 (剪貼簿重新導向)。 您可以使用此設定，防止使用者在遠端電腦與本機電腦之間相互重新導向剪貼簿資料。依預設，遠端桌面服務會允許剪貼簿重新導向。 如果啟用此設定，使用者將無法重新導向剪貼簿資料。 如果停用此設定，則遠端桌面服務一律會允許剪貼簿重新導向。 若未設定此設定，則不會在群組原則層級上指定剪貼簿重新導向。不過，管理員仍然可以使用 [遠端桌面工作階段主機設定] 工具來停用剪貼簿重新導向。
Do not allow COM port redirection	指定是否要在「遠端桌面服務」工作階段中，防止資料從遠端電腦重新導向至用戶端 COM 連接埠。 您可以使用此設定，防止使用者在登入「遠端桌面服務」工作階段期間，將資料重新導向至 COM 連接埠周邊設備或對應本機 COM 連接埠。依預設，遠端桌面服務會允許此 COM 連接埠重新導向。 如果啟用此設定，使用者即無法將伺服器資料重新導向至本機 COM 連接埠。 如果停用此設定，則遠端桌面服務一律會允許 COM 連接埠重新導向。 若未設定此設定，則不會在群組原則層級上指定 COM 連接埠重新導向。不過，管理員仍然可以使用 [遠端桌面工作階段主機設定] 工具來停用 COM 連接埠重新導向。
Do not allow drive redirection	指定是否要在「遠端桌面服務」工作階段中防止用戶端磁碟機的對應 (磁碟機重新導向)。 依預設，RD 工作階段主機伺服器會在連線時自動對應用戶端磁碟機。對應的磁碟機會以 <computername> 上的 <driveletter> 格式顯示在 Windows 檔案總管或電腦的工作階段資料夾樹狀目錄中。您可以使用此設定覆寫這項行為。 如果啟用此設定，即不允許在「遠端桌面服務」工作階段中用戶端磁碟機重新導向。 如果停用此設定，則一律會允許用戶端磁碟機重新導向。 若未設定此設定，則不會在群組原則層級上指定用戶端磁碟機重新導向。不過，管理員仍然可以使用 [遠端桌面工作階段主機設定] 工具來停用用戶端磁碟機重新導向。
Do not allow LTP Port redirection	指定是否要在「遠端桌面服務」工作階段期間防止資料重新導向至用戶端 LPT 連接埠。 您可以使用此設定，防止使用者對應本機 LPT 連接埠，以及將資料從遠端電腦重新導向至本機 LPT 連接埠周邊設備。依預設，遠端桌面服務會允許此 LPT 連接埠重新導向。 如果啟用此設定，「遠端桌面服務」工作階段中的使用者即無法將伺服器資料重新導向至本機 LPT 連接埠。 如果停用此設定，則一律會允許 LPT 連接埠重新導向。 若未設定此設定，則不會在群組原則層級上指定 LPT 連接埠重新導向。不過，管理員仍然可以使用 [遠端桌面工作階段主機設定] 工具來停用 LPT 連接埠重新導向。

表 5-30. RDS 裝置及資源重新導向群組原則設定 (續)

設定	說明
Do not allow supported Plug and Play device redirection	使用此原則設定，可在「遠端桌面服務」工作階段中控制將支援的隨插即用裝置 (例如 Windows 可攜式裝置) 重新導向至遠端電腦的行為。 依預設，遠端桌面服務會允許支援的隨插即用裝置進行重新導向。使用者可在遠端桌面連線的 [本機資源] 索引標籤上使用「更多」選項，選擇支援的隨插即用裝置以重新導向至遠端電腦。 如果啟用此原則設定，使用者即無法將其支援的隨插即用裝置重新導向至遠端電腦。 如果停用或未設定此原則設定，則使用者可將其支援的隨插即用裝置重新導向至遠端電腦。 **備註** 您也可以在 [遠端桌面工作階段主機設定] 工具的 [用戶端設定] 索引標籤上，不允許支援的隨插即用裝置進行重新導向。您可以使用 **電腦設定 > 系統管理範本 > 系統 > 裝置安裝 > 裝置安裝限制**資料夾中的原則設定，不允許特定類型的受支援隨插即用裝置進行重新導向。
Do not allow smart card device redirection	使用此原則設定，可控制「遠端桌面服務」工作階段中的智慧卡裝置重新導向。 如果啟用此原則設定，遠端桌面服務使用者將無法使用智慧卡登入「遠端桌面服務」工作階段。 如果停用或未設定此原則設定，則會允許智慧卡裝置重新導向。依預設，遠端桌面服務會在連線時自動重新導向智慧卡裝置。 **備註** 用戶端電腦至少必須執行 Microsoft Windows 2000 Server 或 Microsoft Windows XP Professional，而且目標伺服器必須加入網域。
Allow time zone redirection	此原則設定判斷用戶端電腦是否會將其時區設定重新導向至遠端桌面服務工作階段。 如果您啟用此原則設定，能夠進行時區重新導向的用戶端會將其時區資訊傳送至伺服器。然後，伺服器基礎時間會被用於計算目前的工作階段時間 (目前的工作階段時間 = 伺服器基礎時間 + 用戶端時區)。 如果您停用或不設定此原則設定，用戶端電腦不會重新導向其時區資訊，並且工作階段時區會與伺服器時區相同。

遠端桌面服務授權設定

RDS 授權群組原則設定控制尋找 RDS 授權伺服器的順序、是否顯示問題通知，以及針對 RDS 用戶端存取使用權 (CAL) 使用「每一使用者」授權還是「每一裝置」授權。

Horizon 7 RDS 群組原則設定安裝於**電腦設定 > 原則 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 授權**資料夾中。

表 5-31. RDS 授權群組原則設定

設定	說明
Use the specified Remote Desktop license servers	此原則設定可讓您指定 RDS 主機伺服器嘗試尋找遠端桌面授權伺服器的順序。 如果啟用此原則設定，RDS 主機伺服器會先嘗試尋找您指定的授權伺服器。若找不到指定的授權伺服器，則 RDS 主機伺服器會嘗試自動探索授權伺服器。 自動探索授權伺服器期間，Windows Server 型網域中的 RDS 主機伺服器會以下列順序嘗試連絡授權伺服器： 1 [遠端桌面工作階段主機設定] 工具中指定的授權伺服器。 2 Active Directory Domain Services 中發佈的授權伺服器。 3 RDS 主機所在網域中的網域控制站上安裝的授權伺服器。 如果停用或未設定此原則設定，則 RDS 主機會使用 [遠端桌面工作階段主機設定] 工具中指定的授權伺服器探索模式。
Hide notifications about RD Licensing problems that affect the RD Session Host server	此原則設定會決定在發生對 RDS 主機造成影響的 RD 授權問題時，是否在 RDS 主機上顯示通知。 依預設，當您以本機管理員身分登入後，若有影響 RDS 主機的 RD 授權問題，則會在 RDS 主機上顯示通知。若適用，還會另外顯示一則通知，指出至 RDS 主機的授權寬限期到期尚餘的天數。 如果啟用此原則設定，將不會在 RDS 主機上顯示這些通知。 如果停用或未設定此原則設定，則您以本機管理員身分登入後，將會在 RDS 主機上顯示這些通知。
Set the Remote Desktop licensing mode	此原則設定可讓您指定連線至此 RDS 主機時所需的遠端桌面服務用戶端存取使用權 (RDS CAL) 類型。 您可以使用此原則設定選取兩種授權模式的其中一種：「每一使用者」或「每一裝置」。 使用「每一使用者」授權模式時，連線至此 RDS 主機的每個使用者帳戶都必須具有「RDS 每個使用者的 CAL」。 使用「每一裝置」授權模式時，連線至此 RDS 主機的每個裝置都必須具有「RDS 每一裝置的 CAL」。 如果啟用此原則設定，則您指定的授權模式優先於安裝遠端桌面工作階段主機期間或遠端桌面工作階段主機組態工具中指定的授權模式。 如果停用或不設定此原則設定，則將使用安裝遠端桌面工作階段主機角色服務期間或遠端桌面工作階段主機組態工具中指定的授權模式。

遠端桌面服務印表機重新導向設定

RDS 印表機重新導向群組原則設定可讓使用者設定印表機重新導向的原則。

Horizon 7 RDS 群組原則設定安裝於**電腦設定 > 原則 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 印表機重新導向**資料夾中。

Horizon 7 RDS 群組原則設定也安裝於**使用者設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 印表機重新導向**資料夾中。

表 5-32. RDS 印表機重新導向群組原則設定

設定	說明
Do not set default client printer to be default printer in a session	使用此原則設定，可指定用戶端預設印表機是否會在 RDS 主機上的工作階段中自動設定為預設印表機。 依預設，遠端桌面服務會在 RDS 主機上的工作階段中，自動將用戶端預設印表機指定為預設印表機。您可以使用此原則設定覆寫這項行為。 如果啟用此原則設定，則預設印表機為遠端電腦上指定的印表機。 如果停用此原則設定，RDS 主機將會在連線時自動對應用戶端預設印表機，並將其設定為預設印表機。 若未設定此原則設定，則不會在群組原則層級上指定預設印表機。不過，管理員可使用 [遠端桌面工作階段主機設定] 工具來設定用戶端工作階段的預設印表機。
Do not allow client printer redirection	使用此原則設定，可指定是否要在「遠端桌面服務」工作階段中防止用戶端印表機對應。 您可以使用此原則設定，防止使用者將列印工作從遠端電腦重新導向至連接到本機 (用戶端) 電腦的印表機。依預設，遠端桌面服務會允許此用戶端印表機對應。 如果啟用此原則設定，使用者即無法在「遠端桌面服務」工作階段中，將列印工作從遠端電腦重新導向至本機用戶端印表機。 如果停用此原則設定，則使用者可透過用戶端印表機對應重新導向列印工作。 若未設定此原則設定，則不會在群組原則層級上指定用戶端印表機對應。不過，管理員可仍使用 [遠端桌面工作階段主機設定] 工具來停用用戶端印表機對應。
Use Remote Desktop Easy Print printer driver first	使用此原則設定，可指定是否要先使用「遠端桌面輕鬆列印」印表機驅動程式來安裝所有的用戶端印表機。 如果啟用或未設定此原則設定，RDS 主機將會先嘗試使用「遠端桌面輕鬆列印」印表機驅動程式來安裝所有的用戶端印表機。如果「遠端桌面輕鬆列印」印表機驅動程式因故無法使用，則會使用 RDS 主機上與用戶端印表機相符的印表機驅動程式。如果 RDS 主機上沒有與用戶端印表機相符的印表機驅動程式，用戶端印表機即無法用於遠端桌面工作階段。 如果停用此原則設定，則 RDS 主機會嘗試尋找適用的印表機驅動程式來安裝用戶端印表機。如果 RDS 主機上沒有與用戶端印表機相符的印表機驅動程式，RDS 主機會嘗試使用「遠端桌面輕鬆列印」驅動程式來安裝用戶端印表機。如果「遠端桌面輕鬆列印」印表機驅動程式因故無法使用，用戶端印表機即無法用於「遠端桌面服務」工作階段。 **備註** 如果啟用「不允許用戶端印表機重新導向」原則設定，則會忽略「優先使用遠端桌面輕鬆列印印表機驅動程式」原則設定。

表 5-32. RDS 印表機重新導向群組原則設定 (續)

設定	說明
Specify RD Session Host Server fallback printer driver behavior	使用此原則設定，可指定 RDS 主機後援印表機驅動程式的行為。 依預設會停用 RDS 主機後援印表機驅動程式。如果 RDS 主機上沒有與用戶端印表機相符的印表機驅動程式，則將沒有任何印表機可用於「遠端桌面服務」工作階段。 如果啟用此原則設定，則會啟用後援印表機驅動程式，而預設行為將是由 RDS 主機尋找適用的印表機驅動程式。如果找不到印表機驅動程式，即無法使用用戶端印表機。您可以選擇變更此預設行為。可用選項包括： ■ Do nothing if one is not found。如果沒有相符的印表機驅動程式，RDS 主機會嘗試尋找適用的驅動程式。如果找不到，即無法使用用戶端印表機。這是預設行為。 ■ Default to PCL if one is not found。如果找不到適用的印表機驅動程式，則預設為印表機控制語言 (PCL) 後援印表機驅動程式。 ■ Default to PS if one is not found。如果找不到適用的印表機驅動程式，則預設為 PostScript (PS) 後援印表機驅動程式。 ■ Show both PCL and PS if one is not found。如果找不到適用的驅動程式，則會同時顯示 PS 和 PCL 型後援印表機驅動程式。 如果停用此原則設定，則會停用 RDS 主機後援驅動程式，且 RDS 主機將不會嘗試使用後援印表機驅動程式。 若未設定此原則設定，依預設會關閉後援印表機驅動程式行為。 **備註** 如果啟用「不允許用戶端印表機重新導向」設定，則會忽略此原則設定，並停用後援印表機驅動程式。
Redirect only the default client printer	使用此原則設定，可指定預設用戶端印表機是否為「遠端桌面服務」工作階段中唯一重新導向的印表機。 如果啟用此原則設定，則只有預設用戶端印表機會在「遠端桌面服務」工作階段中重新導向。 如果停用或未設定此原則設定，則會在「遠端桌面服務」工作階段中重新導向所有的用戶端印表機。

RDS 設定檔設定

RDS 設定檔群組原則設定可控制遠端桌面服務工作階段的漫遊設定檔和主目錄設定。

表 5-33. RDS 設定檔群組原則設定

設定	說明
`Limit the size of the entire roaming user profile cache`	此原則設定可讓您限制本機磁碟機上整個漫遊使用者設定檔快取的大小。此原則設定僅適用於已安裝遠端桌面工作階段主機角色服務的電腦。 **備註** 如果要限制個別使用者設定檔的大小，請使用位於**使用者設定\原則\系統管理範本\系統\使用者設定檔**中的 `Limit profile size` 原則設定。 如果啟用此原則設定，您必須指定整個漫遊使用者設定檔快取的監控間隔 (分鐘) 和大小上限 (GB)。監控間隔會決定檢查整個漫遊使用者設定檔快取大小的頻率。當整個漫遊使用者設定檔快取的大小超過指定的大小上限時，就會刪除最舊的 (最久不曾使用的) 漫遊使用者設定檔，直到整個漫遊使用者設定檔快取的大小小於指定的大小上限為止。 如果停用或未設定此原則設定，則對於可在本機磁碟機上存放的整個漫遊使用者設定檔快取大小沒有限制。 注意：如果已啟用位於**電腦設定\原則\系統管理範本\系統\使用者設定檔**中的 `Prevent Roaming Profile changes from propagating to the server` 原則設定，就會忽略這個原則設定。
`Set Remote Desktop Services User Home Directory`	指定遠端桌面服務是否會使用指定的網路共用或是本機目錄路徑，做為遠端桌面服務工作階段使用者主目錄的根目錄。 若要使用此設定，請從 [位置] 下拉式清單選取主目錄 (網路或本機) 的位置。如果選擇將目錄放置在網路共用上，請以 `\\Computername\Sharename` 的格式輸入主目錄根路徑，然後選取網路共用的對應磁碟機代號。 如果選擇將主目錄保留在本機電腦上，請以 `Drive:\Path` 格式輸入不含環境變數或省略號的主目錄根路徑。請不要為使用者別名指定預留位置，因為遠端桌面服務會在登入時自動附加使用者別名。 **備註** 如果選擇指定本機路徑，就會略過 [磁碟機代號] 欄位。如果選擇指定本機路徑，但之後又在 [主目錄根路徑] 中輸入網路共用的名稱，則遠端桌面服務會將使用者的主目錄放在網路位置。 如果狀態設定為 [已啟用]，遠端桌面服務會在本機電腦或網路上的指定位置，建立使用者的主目錄。每個使用者的主目錄路徑就是指定的主目錄根路徑和使用者的別名。 如果狀態設定為 [已停用] 或 [未設定]，則使用者的主目錄是伺服器上指定的位置。

表 5-33. RDS 設定檔群組原則設定 (續)

設定	說明
`Use mandatory profiles on the RD Session Host server`	此原則設定可讓您指定遠端桌面服務是否會針對所有遠端連線到 RDS 主機的使用者使用強制設定檔。 如果啟用此原則設定，遠端桌面服務會使用 `Set path for Remote Desktop Services Roaming User Profile` 原則設定中指定的路徑，做為強制使用者設定檔的根資料夾。所有遠端連線到 RDS 主機的使用者都會使用相同的使用者設定檔。 如果停用或未設定此原則設定，則遠端連線到 RDS 主機的使用者不會使用強制使用者設定檔。 **備註** 若要讓此原則設定生效，您也必須啟用和設定 `Set path for Remote Desktop Services Roaming User Profile` 原則設定。
`Set path for Remote Desktop Services Roaming User Profile`	此原則設定可讓您指定遠端桌面服務針對漫遊使用者設定檔使用的網路路徑。 依預設，遠端桌面服務會將所有使用者設定檔儲存在本機的 RDS 主機。您可以使用此原則設定指定可以集中儲存使用者設定檔的網路共用，讓使用者可在設定成使用網路共用做為使用者設定檔的所有 RDS 主機上，存取所有工作階段的相同設定檔。 如果啟用此原則設定，遠端桌面服務會使用指定的路徑做為所有使用者設定檔的根目錄。設定檔包含在以每個使用者的帳戶名稱命名的子資料夾中。 若要設定此原則設定，請以 `\\Computername\Sharename` 的格式輸入網路共用的路徑。請不要為使用者帳戶名稱指定預留位置，因為當使用者登入並建立設定檔時，遠端桌面服務會自動新增使用者帳戶名稱。如果指定的網路共用不存在，遠端桌面服務會在 RDS 主機上顯示錯誤訊息，並將使用者設定檔儲存在 RDS 主機上的本機位置。 如果停用或未設定此原則設定，則使用者設定檔會儲存在本機的 RDS 主機。您可以在使用者帳戶的 [內容] 對話方塊的 [遠端桌面服務設定檔] 索引標籤上，設定使用者的設定檔路徑。 備註: 1 原則設定所啟用的漫遊使用者設定檔只適用於遠端桌面服務連線。使用者可能也已設定 Windows 漫遊使用者設定檔。但在遠端桌面服務工作階段中，遠端桌面服務漫遊使用者設定檔永遠具有優先權。 2 若要為從遠端連線至 RDS 主機的所有使用者設定強制的遠端桌面服務漫遊使用者設定檔，請使用此原則設定，以及位於**電腦設定\系統管理範本\Windows 元件\遠端桌面服務\RD 工作階段主機\設定檔**中的 `Use mandatory profiles on the RD Session Host server` 原則設定。在 `Set path for Remote Desktop Services Roaming User Profile` 原則設定中所設定的路徑應該包含強制設定檔。

RDS 連線伺服器設定

RDS 連線伺服器群組原則設定可讓使用者設定連線伺服器的原則。

Horizon 7 RDS 群組原則設定安裝於**電腦設定 > 原則 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > RD 連線代理人**資料夾中。

表 5-34. RDS 連線伺服器群組原則設定

設定	說明
Join RD Connection Broker	使用此原則設定，可指定 RDS 主機是否應加入至安裝在 RDS 主機上之連線伺服器中的伺服器陣列。RDS 主機上的連線伺服器會追蹤使用者工作階段，並可讓使用者重新連線至其在負載平衡 RDS 伺服器陣列中的現有工作階段。若要加入 RDS 主機上的連線伺服器，必須在 RDS 主機上安裝遠端桌面工作階段主機角色服務。 如果啟用此原則設定，RDS 主機將會加入至「設定 RD 連線代理人伺服器陣列名稱」設定中指定的伺服器陣列。伺服器陣列會存在於「設定 RD 連線代理人伺服器名稱」原則設定中指定的連線伺服器上。 如果停用此原則設定，則 RDS 主機不會加入至連線伺服器中的伺服器陣列，且不會執行使用者工作階段追蹤。此設定停用時，您無法使用遠端桌面工作階段主機設定工具或終端機服務 WMI 提供者將 RDS 主機加入至連線伺服器。 若未設定此原則設定，則不會在群組原則層級上指定設定。在此情況下，您可以使用遠端桌面工作階段主機設定工具或終端機服務 WMI 提供者來設定 RDS 主機，使其加入至 RDS 主機上的連線伺服器。 **備註** 1 啟用此設定時，您也必須啟用「設定 RD 連線代理人伺服器陣列名稱」和「設定 RD 連線代理人伺服器名稱」原則設定，或使用遠端桌面工作階段主機設定工具或終端機服務 WMI 提供者來設定這些設定。 2 就 Windows Server 2008 而言，至少需要 Windows Server 2008 Standard 才支援此原則設定。
Configure RD Connection Broker farm name	使用此原則設定，可指定要在 RDS 主機的連線伺服器中加入的伺服器陣列名稱。連線伺服器會使用伺服器陣列名稱來判斷哪些 RDS 主機位於相同的 RDS 伺服器陣列中。因此，對於相同負載平衡伺服器陣列中的所有 RDS 主機，您必須使用相同的伺服器陣列名稱。伺服器陣列名稱不需要對應於 Active Directory 網域服務中的名稱。 如果您指定新的伺服器陣列名稱，則 RDS 主機的連線伺服器中將會建立新的伺服器陣列。如果您指定現有伺服器陣列名稱，則 RDS 主機會加入至其連線伺服器中的那個伺服器陣列。 如果啟用此原則設定，您必須指定 RDS 主機之連線伺服器中的伺服器陣列名稱。 如果停用或未設定此原則設定，則群組原則不會指定伺服器陣列名稱。在此情況下，您可以使用遠端桌面工作階段主機設定工具或終端機服務 WMI 提供者來調整伺服器陣列名稱。 **備註** 就 Windows Server 2008 而言，至少需要 Windows Server 2008 Standard 才支援此原則設定。若要讓此設定生效，則必須同時啟用「加入 RD 連線代理人」和「設定 RD 連線代理人伺服器名稱」設定，並使用群組原則、遠端桌面工作階段主機設定工具或終端機服務 WMI 提供者進行設定。

表 5-34. RDS 連線伺服器群組原則設定 (續)

設定	說明
Use IP Address Redirection	使用此原則設定，可指定在用戶端裝置重新連線至負載平衡 RDS 伺服器陣列中的現有「遠端桌面服務」工作階段時，所使用的重新導向方法。此設定適用於設定為使用 RDS 主機上連線伺服器的 RDS 主機，不適用於遠端桌面平台上的連線伺服器。 如果啟用此原則設定，遠端桌面服務用戶端將會查詢 RDS 主機上的連線伺服器，並使用現有工作階段所在之 RDS 主機的 IP 位址重新導向至該工作階段。若要使用此重新導向方法，用戶端電腦必須能夠以 IP 位址直接連線至伺服器陣列中的 RDS 主機。 如果停用此原則設定，則系統不會將 RDS 主機的 IP 位址傳送至用戶端。此時，IP 位址會內嵌在權杖中。當用戶端重新連線至負載平衡器時，系統會使用路由權杖將用戶端重新導向至伺服器陣列中正確 RDS 主機上的現有工作階段。僅在您的網路負載平衡解決方案支援使用 RDS 主機連線伺服器路由權杖，且您不想讓用戶端以 IP 位址直接連線至負載平衡伺服器陣列中的 RDS 主機時，才需要停用此設定。 若未設定此原則設定，則會使用遠端桌面工作階段主機設定工具中的「使用 IP 位址重新導向」設定。依預設，會啟用遠端桌面工作階段主機設定工具中的這項設定。 **備註** 就 Windows Server 2008 而言，至少需要 Windows Server 2008 Standard 才支援此原則設定。

表 5-34. RDS 連線伺服器群組原則設定 (續)

設定	說明
Configure RD Connection Broker Server name	使用此原則設定，可指定 RDS 主機針對負載平衡 RDS 伺服器陣列進行使用者工作階段追蹤和重新導向的連線伺服器。指定的 RDS 主機必須執行連線伺服器服務。負載平衡伺服器陣列中的所有 RDS 主機應使用相同的連線伺服器。 如果啟用此原則設定，則必須使用連線伺服器的主機名稱、IP 位址或完整網域名稱，來指定 RDS 主機的連線伺服器。如果您為連線伺服器指定了無效的名稱或 IP 位址，則系統會在 RDS 主機上的事件檢視器中記錄錯誤訊息。 如果停用或未設定此原則設定，您可以使用遠端桌面工作階段主機設定工具或終端機服務 WMI 提供者，來調整 RDS 主機連線伺服器名稱或 IP 位址。 **備註** ■ 就 Windows Server 2008 而言，至少需要 Windows Server 2008 Standard 才支援此原則設定。 ■ 若要讓此設定生效，則必須啟用「加入 RD 連線代理人」原則設定，或使用遠端桌面工作階段主機設定工具或終端機服務 WMI 提供者，將 RDS 主機設定為加入 RDS 主機上的連線伺服器。 ■ 若要成為 RDS 伺服器陣列上已啟用連線伺服器之工作階段的作用中成員，伺服器陣列中每個 RDS 主機的電腦帳戶，皆必須是 RDS 主機之連線伺服器上「Session Directory Computers」本機群組的成員。
Use RD Connection Broker load balancing	使用此原則設定，可指定是否在 RDS 主機上的連線伺服器中使用負載平衡功能，以在 RDS 伺服器陣列中的伺服器之間平衡負載。 如果啟用此原則設定，RDS 主機上的連線伺服器會將目前沒有工作階段的使用者重新導向至伺服器陣列中具有最少工作階段的 RDS 主機。目前有工作階段之使用者的重新導向行為將不受影響。如果伺服器設定為使用 RDS 主機上的連線伺服器，則目前有工作階段的使用者會重新導向至其工作階段所在的 RDS 主機。 如果停用此原則設定，則目前沒有工作階段的使用者會登入他們所連線的第一個 RDS 主機。 若未設定此原則設定，您可以使用遠端桌面工作階段主機設定工具或終端機服務 WMI 提供者，將 RDS 主機設定為加入 RDS 主機的連線伺服器負載平衡。 **備註** 如果啟用此原則設定，您也必須啟用「加入 RD 連線代理人」、「設定 RD 連線代理人伺服器陣列名稱」和「設定 RD 連線代理人伺服器名稱」原則設定。

RDS 遠端工作階段環境設定

「RDS 遠端工作階段環境」群組原則設定控制「遠端桌面服務」工作階段中使用者介面的組態。

Horizon 7 RDS 群組原則設定安裝於**電腦設定 > 原則 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 遠端工作階段環境**資料夾中。

Horizon 7 RDS 群組原則設定也安裝於**使用者設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 遠端工作階段環境**資料夾中。

表 5-35. RDS 遠端工作階段環境群組原則設定

設定	說明
Limit maximum color depth	使用此原則設定，可指定遠端桌面服務連線的最大色彩解析度 (色彩深度)。 您可以使用此原則設定，為使用 RDP 的任何連線設定色彩深度的限制。限制色彩深度可改善連線的效能 (特別是透過慢速連結時)，並減少伺服器的負載。 如果啟用此原則設定，您指定的色彩深度將是透過 RDP 之使用者連線所允許的最大色彩深度。連線的實際色彩深度取決於用戶端電腦上支援的可用色彩。如果您選取「用戶端相容」，將會使用用戶端支援的最高色彩深度。 **備註** 只有 Windows XP Professional 和 Windows Server 2003 支援 24 位元的色彩深度。 如果停用或未設定此原則設定，則會由 [遠端桌面工作階段主機設定] 工具中 [用戶端設定] 索引標籤上的「限制最大色彩深度」設定來決定連線的色彩深度，除非使用者在連線時指定了較低的等級。
Enforce Removal of Remote Desktop Wallpaper	指定是否要對透過遠端桌面服務連線的遠端用戶端顯示桌面底色圖案。 您可以使用這個設定，在遠端桌面服務工作階段期間，強制移除底色圖案。依預設，Windows XP Professional 會根據用戶端的設定，對透過遠端桌面連線的遠端用戶端顯示底色圖案。如需詳細資訊，請檢視 [遠端桌面連線] 選項中的 [進階設定] 索引標籤。依預設，執行 Windows Server 2003 的伺服器不會對「遠端桌面服務」工作階段顯示底色圖案。 如果啟用此設定，底色圖案永遠不會顯示在「遠端桌面服務」工作階段中。 如果停用此設定，則底色圖案可能會顯示在「遠端桌面服務」工作階段中，視用戶端組態而定。 若未設定此設定，則會套用預設行為。
Configure RemoteFX	使用此原則設定，可在遠端桌面虛擬主機 (RD 虛擬主機) 和 RDS 主機上控制 RemoteFX 的可用性。 在 RD 虛擬主機伺服器上部署時，RemoteFX 會使用圖形處理單元 (GPU) 或硬體來轉譯伺服器上的內容，以提供豐富的使用者體驗。依預設，RD 虛擬主機的 RemoteFX 會使用伺服器端 GPU 或硬體，透過 LAN 連線和 RDP 7.1 提供豐富的使用者體驗。 部署於 RDS 主機時，RemoteFX 會使用硬體加速壓縮配置提供豐富的使用者體驗。 如果啟用此原則設定，將會使用 RemoteFX 透過 LAN 連線和 RDP 7.1 提供豐富的使用者體驗。 如果停用此原則設定，則會停用 RemoteFX。 若未設定此原則設定，則會使用預設行為。依預設會啟用 RD 虛擬主機的 RemoteFX，並停用 RDS 主機的 RemoteFX。

表 5-35. RDS 遠端工作階段環境群組原則設定 (續)

設定	說明
Limit maximum display resolution	使用此原則設定，可指定每個監視器可用來顯示「遠端桌面服務」工作階段的最大顯示器解析度。限制用來顯示遠端工作階段的解析度，可改善連線的效能 (特別是透過慢速連結時)，並減少伺服器的負載。 如果啟用此原則設定，則必須指定解析度寬度和高度。指定的解析度將是每個監視器可用來顯示「遠端桌面服務」工作階段的最大解析度。 如果停用或未設定此原則設定，則每個監視器可用來顯示「遠端桌面服務」工作階段的最大解析度，將由 [遠端桌面工作階段主機設定] 工具中 [顯示設定] 索引標籤所指定的值來決定。
Limit maximum number of monitors	使用此原則設定，可限制使用者能夠用來顯示「遠端桌面服務」工作階段的監視器數目。限制用來顯示「遠端桌面服務」工作階段的監視器數目，可改善連線的效能 (特別是透過慢速連結時)，並減少伺服器的負載。 如果啟用此原則設定，您將可指定能夠用來顯示「遠端桌面服務」工作階段的監視器數目。您可以指定 1 到 10 之間的數字。 如果停用或未設定此原則設定，則可用來顯示「遠端桌面服務」工作階段的監視器數目，將由 [遠端桌面工作階段主機設定] 工具中 [顯示設定] 索引標籤上的「每個工作階段的監視器數目上限」方塊所指定的值來決定。
Remove "Disconnect" option from Shut Down dialog	使用此原則設定，可從「遠端桌面服務」工作階段的 [關閉 Windows] 對話方塊中移除「中斷連線」選項。 您可以使用此原則設定，防止使用者透過這個常用的方法中斷其用戶端與 RDS 主機的連線。 如果啟用此原則設定，[關閉 Windows] 對話方塊的下拉式清單中就不會顯示「中斷連線」選項。 如果停用或未設定此原則設定，則不會從 [關閉 Windows] 對話方塊的清單中移除「中斷連線」。 **備註** 此原則設定只會影響 [關閉 Windows] 對話方塊。它不會防止使用者使用其他的方法中斷「遠端桌面服務」工作階段的連線。此原則設定也不會妨礙伺服器上已中斷連線的工作階段。您可以設定**電腦設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > RD 工作階段主機 > 工作階段時間限制**資料夾中的「設定已斷線工作階段的時間限制」原則設定，以控制已中斷連線工作階段在伺服器上維持使用中狀態的時間長度。
Optimize visual experience when using RemoteFX	使用此原則設定，可指定遠端使用者在使用 RemoteFX 的遠端桌面連線 (RDC) 連線中所將擁有的視覺效果。您可以使用此原則，在網路頻寬使用量與提供的圖形效果類型之間取得平衡。 視使用者需求之不同，您可以降低螢幕擷取速率，以降低網路頻寬使用量。您也可以藉由降低影像品質 (增加執行的影像壓縮量) 來降低網路頻寬使用量。 如果您的網路頻寬高於平均值，您可以選取螢幕擷取速率的最高設定及影像品質的最高設定，讓頻寬使用量最大化。 依預設，使用 RemoteFX 的「遠端桌面連線」工作階段會透過 LAN 狀況將平衡效果最佳化。如果您停用或未設定這個原則設定，使用 RemoteFX 的遠端桌面連線工作階段將與選取中等螢幕擷取速率及中等影像壓縮設定 (預設行為) 相同。

表 5-35. RDS 遠端工作階段環境群組原則設定 (續)

設定	說明
Set compression algorithm for RDP data	使用此原則設定，可指定所要使用的遠端桌面通訊協定 (RDP) 壓縮演算法。 依預設，伺服器會使用以伺服器硬體組態為基礎的 RDP 壓縮演算法。 如果啟用此原則設定，您可以指定所要使用的 RDP 壓縮演算法。如果您選取的演算法最佳化為使用較少的記憶體，此選項較不需要大量的記憶體，但會使用較多的網路頻寬。如果您選取的演算法最佳化為使用較少的網路頻寬，此選項會使用較少的網路頻寬，但較需要大量的記憶體。此外，還有第三個選項可平衡記憶體使用量和網路頻寬。 您也可以選擇不使用 RDP 壓縮演算法。選擇不使用 RDP 壓縮演算法會使用較多的網路頻寬，因此，只有在您使用的硬體裝置設計成將網路流量最佳化時，才建議使用此做法。即使您選擇不使用 RDP 壓縮演算法，仍有某些圖形資料會進行壓縮。 如果停用或未設定此原則設定，則會使用預設的 RDP 壓縮演算法。
Optimize visual experience for Remote Desktop Services sessions	使用此原則設定，可指定遠端使用者在「遠端桌面服務」工作階段中看到的視覺效果。之後，遠端電腦上的遠端工作階段會最佳化成支援此視覺效果。 依預設，「遠端桌面服務」工作階段會針對豐富的多媒體內容進行最佳化，例如使用 Silverlight 或 Windows Presentation Foundation 的應用程式。 如果啟用此原則設定，您必須選取要最佳化「遠端桌面服務」工作階段的視覺效果。您可以選取 [豐富的多媒體內容] 或 [文字]。 如果停用或未設定此原則設定，則「遠端桌面服務」工作階段會針對豐富的多媒體內容進行最佳化。

表 5-35. RDS 遠端工作階段環境群組原則設定 (續)

設定	說明
Start a program on connection	設定遠端桌面服務，使其在連線時自動執行指定的程式。 您可以使用此設定，指定要在使用者登入遠端電腦時自動執行的程式。 依預設，「遠端桌面服務」工作階段會提供完整 Windows 桌面的存取權，除非伺服器管理員或設定用戶端連線的使用者對此設定另有指定。啟用此設定，將會覆寫伺服器管理員或使用者所設定的「啟動程式」設定。畫面上不會顯示 [開始] 功能表和 Windows 桌面，而且當使用者結束程式時，工作階段會自動登出。 若要使用此設定，請在 [程式路徑和檔案名稱] 中，輸入在使用者登入時所要執行之可執行檔的完整路徑和檔案名稱。如有必要，請在 [工作目錄] 中輸入程式之啟動目錄的完整路徑。如果將 [工作目錄] 保留為空白，程式將會以其預設工作目錄執行。如果指定的程式路徑、檔案名稱或工作目錄不是有效目錄的名稱，則 RDS 主機連線將會失敗，並出現錯誤訊息。 如果狀態設為 [已啟用]，則「遠端桌面服務」工作階段將會自動執行指定的程式，並使用指定的工作目錄 (若未指定工作目錄，則為程式預設目錄) 作為程式的工作目錄。 如果狀態設為 [已停用] 或 [未設定]，則「遠端桌面服務」工作階段會以完整桌面啟動，除非伺服器管理員或使用者另有指定。如需詳細資訊，請查看**電腦設定 > 系統管理範本 > 系統 > 登入**資料夾中的「當使用者登入時執行這些程式」原則設定。 **備註** 此設定會同時顯示在「電腦設定」和「使用者設定」中。如果同時設定了這兩項設定，則「電腦設定」設定的優先權會高於「使用者設定」設定。
Always show desktop on connection	此原則設定可決定在用戶端連線至遠端電腦後，是否一律顯示桌面，或讓初始程式可以執行。使用此設定可要求在用戶端連線至遠端電腦後要顯示桌面，即使已在預設使用者設定檔、遠端桌面連線、遠端桌面服務用戶端中指定初始程式，或已透過群組原則來指定。 如果啟用此原則設定，用戶端連線至遠端電腦時，一律會顯示桌面。此原則設定會覆寫任何初始程式原則設定。 如果停用或未設定此原則設定，則可以指定在用戶端連線至遠端電腦後要在遠端電腦上執行的初始程式。若未指定初始程式，則在用戶端連線至遠端電腦後，遠端電腦上一律會顯示桌面。 **備註** 如果啟用此原則設定，則會忽略「連線時啟動程式」原則設定。

表 5-35. RDS 遠端工作階段環境群組原則設定 (續)

設定	說明
Allow desktop composition for remote desktop sessions	使用此原則設定，可指定是否允許遠端桌面工作階段的桌面轉譯緩衝處理。此原則設定不適用於 RemoteApp 工作階段。 桌面轉譯緩衝處理可為遠端桌面工作階段提供 Windows Aero 的使用者介面元素，例如半透明視窗。由於 Windows Aero 需要額外的系統和頻寬資源，因此允許遠端桌面的桌面轉譯緩衝處理可能會降低連線效能 (特別是透過慢速連結時)，並且增加遠端電腦上的負載。 如果您啟用此原則設定，將會允許遠端桌面工作階段的桌面轉譯緩衝處理。在用戶端電腦上，您可以在遠端桌面連線 (RDC) 的 [進階設定] 索引標籤上設定桌面轉譯緩衝處理，或使用遠端桌面通訊協定 (.rdp) 檔案中的「允許桌面轉譯緩衝處理」設定來進行設定。此外，用戶端電腦必須具有支援 Windows Aero 功能所需的硬體。 **備註** 遠端電腦上可能還需要有其他設定才能讓 Windows Aero 功能在遠端桌面工作階段使用。例如，遠端電腦上必須安裝桌面體驗功能，而且遠端電腦上的最大色彩深度必須設定為每一像素 32 位元。此外，遠端電腦上也必須啟用佈景主題服務。 如果停用或未設定此原則設定，即使已在 RDC 或 .rdp 檔案中啟用桌面轉譯緩衝處理，也不會允許遠端桌面的桌面轉譯緩衝處理。
Do not allow font smoothing	使用此原則設定，可指定是否允許遠端連線的字型平滑處理。 字型平滑處理可為遠端連線提供 ClearType 功能。ClearType 是一種顯示電腦字型的技術，可讓字型變得更清晰平順，尤其是在使用 LCD 監視器的時候。由於字型平滑處理需要額外的頻寬資源，因此不允許遠端連線的字型平滑處理將可提升連線效能，特別是透過慢速連結時。 依預設會允許遠端連線的字型平滑處理。您可以在遠端桌面連線 (RDC) 的 [進階設定] 索引標籤上設定字型平滑處理，或使用遠端桌面通訊協定 (.rdp) 檔案中的「允許字型平滑處理」設定來進行設定。 如果啟用此原則設定，即使已在 RDC 或 .rdp 檔案中啟用字型平滑處理，仍不會允許遠端連線的字型平滑處理。 如果停用或未設定此原則設定，則會允許遠端連線的字型平滑處理。
Remove Windows Security item from Start menu	指定是否從 [遠端桌面] 用戶端上的 [設定] 功能表中移除 [Windows 安全性] 項目。使用此設定可防止沒有經驗的使用者不小心登出遠端桌面服務。 如果將狀態設定為 [啟用]，則 [開始] 功能表上的 [設定] 將不再顯示 [Windows 安全性]。因此，使用者必須輸入安全性注意順序，例如 CTRL+ALT+END，才能在用戶端電腦上開啟 [Windows 安全性] 對話方塊。 如果將狀態設定為 [啟用] 或 [未設定]，則 [Windows 安全性] 將保留在 [設定] 功能表中。

遠端桌面服務安全性設定

RDS 安全群組原則設定控制是否允許本機管理員自訂權限。

Horizon 7 RDS 群組原則設定安裝於**電腦設定 > 原則 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 安全性**資料夾中。

表 5-36. RDS 安全群組原則設定

設定	說明
Server Authentication Certificate Template	使用此原則設定可指定憑證範本的名稱，以決定應自動選取哪個憑證來驗證 RDS 主機。 在 RDP 連線期間使用 SSL (TLS 1.0) 保護用戶端與 RDS 主機之間的通訊安全時，必須要有憑證才能驗證 RDS 主機。 如果啟用此原則設定，則必須指定憑證範本名稱。自動選取用來驗證 RDS 主機的憑證時，將只會考量使用指定憑證範本所建立的憑證。只有在未選取特定憑證時，才會執行自動憑證選取。 如果找不到以指定憑證範本建立的憑證，RDS 主機將會發出憑證註冊要求，且在此要求完成前將會使用目前的憑證。如果找到多個以指定憑證範本建立的憑證，則會選取最近即將到期、且符合目前 RDS 主機名稱的憑證。 如果停用或未設定此原則設定，依預設會使用自我簽署憑證來驗證 RDS 主機。您可以在 [遠端桌面工作階段主機設定] 工具的 [一般] 索引標籤上，選取要用來驗證 RDS 主機的特定憑證。 **備註** 如果您選取了特定憑證用來驗證 RDS 主機，則該憑證的優先順序將高於此原則設定。
Set client connection encryption level	指定在遠端桌面通訊協定 (RDP) 連線期間，是否要求使用特定加密層級來保護用戶端與 RDS 主機之間的通訊安全。 如果啟用此設定，則在遠端連線期間，用戶端與 RDS 主機之間的所有通訊都必須使用此設定中指定的加密方法。依預設，加密層級會設為 [高]。可用的加密方法如下： ■ High。[高] 設定會使用增強式 128 位元加密，加密從用戶端傳送至伺服器以及從伺服器傳送至用戶端的資料。在僅包含 128 位元用戶端 (例如執行遠端桌面連線的用戶端) 的環境中，請使用此加密層級。不支援此加密層級的用戶端無法連線至 RDS 主機伺服器。 ■ Client Compatible。[用戶端相容] 設定會以用戶端所支援的最大金鑰效力來加密在用戶端與伺服器之間傳送的資料。如果環境中包含不支援 128 位元加密的用戶端，請使用此加密層級。 ■ Low。[低] 設定只會使用 56 位元加密，對用戶端傳送至伺服器的資料進行加密。 如果停用或未設定此設定，則不會透過群組原則強制執行要對 RDS 主機之遠端連線使用的加密層級。但您可以使用 [遠端桌面工作階段主機設定] 工具，設定這些連線的必要加密層級。 **重要** FIPS 相容可透過**電腦設定 > Windows 設定 > 安全性設定 > 本機原則 > 安全性選項**資料夾中的「系統加密編譯: 使用 FIPS 相容演算法於加密，雜湊，以及簽章」原則設定來設定，或透過 [遠端桌面工作階段主機設定] 中的「FIPS 相容」設定來設定。[FIPS 相容] 設定會透過美國聯邦資訊處理標準 (FIPS) 140-1 加密演算法，使用 Microsoft 密碼編譯模組來加密及解密從用戶端傳送至伺服器和從伺服器傳送至用戶端的資料。當用戶端與 RDS 主機之間的通訊需要最高層級的加密時，請使用此加密層級。如果已透過群組原則「系統加密編譯: 使用 FIPS 相容演算法於加密，雜湊，以及簽章」啟用 FIPS 相容，該設定將會覆寫在此群組原則設定中或 [遠端桌面工作階段主機設定] 工具中指定的加密層級。

表 5-36. RDS 安全群組原則設定 (續)

設定	說明
Always prompt for password upon connection	指定遠端桌面服務在連線時是否一律會提示用戶端提供密碼。 您可以使用這個設定，對登入遠端桌面服務的使用者強制執行密碼提示，即使他們已經在遠端桌面連線用戶端中提供過密碼。 依預設，遠端桌面服務允許使用者在遠端桌面連線用戶端中輸入密碼即可自動登入。 如果啟用此設定，使用者將無法在遠端桌面連線用戶端中提供其密碼而自動登入遠端桌面服務。他們會看見提供登入密碼的提示。 如果停用此設定，則使用者一律可在遠端桌面連線用戶端中提供其密碼以自動登入遠端桌面服務。 若未設定此設定，則不會在群組原則層級上指定自動登入。但管理員仍然可以使用 [遠端桌面工作階段主機設定] 工具強制執行密碼提示。
Require secure RPC communication	指定 RDS 主機是否要求在所有用戶端使用安全 RPC 通訊，或允許不安全的通訊。 您可以使用此設定，藉由僅允許經過驗證和加密的要求，強化用戶端的 RPC 通訊安全性。 如果啟用此設定，遠端桌面服務會接受支援安全要求之 RPC 用戶端的要求，且不允許與未受信任的用戶端進行不安全的通訊。 如果停用此設定，則遠端桌面服務一律會要求所有 RPC 流量的安全性。不過，未回應要求的 RPC 用戶端仍可進行不安全的通訊。 若未設定此設定，則會允許不安全的通訊。 **備註** RPC 介面可用來管理及設定遠端桌面服務。
Require use of specific security layer for remote (RDP) connections	指定在遠端桌面通訊協定 (RDP) 連線期間，是否要求使用特定安全性階層來保護用戶端與 RDS 主機之間的通訊安全。 如果啟用此設定，則在遠端連線期間，用戶端與 RDS 主機之間的所有通訊都必須使用此設定中指定的安全性方法。可用的安全性方法如下： ■ Negotiate。交涉方法會強制執行用戶端支援的最安全方法。如果支援傳輸層安全性 (TLS) 1.0 版，則會用來驗證 RDS 主機。如果不支援 TLS，則會使用原生遠端桌面通訊協定 (RDP) 加密來保護通訊安全，但不會驗證 RDS 主機。 ■ RDP。RDP 方法會使用原生 RDP 加密來保護用戶端與 RDS 主機之間的通訊安全。如果選取此設定，則不會驗證 RDS 主機。 ■ SSL (TLS 1.0)。SSL 方法必須使用 TLS 1.0 來驗證 RDS 主機。如果不支援 TLS，則連線會失敗。 如果停用或未設定此設定，則不會透過群組原則強制執行要對 RDS 主機的遠端連線使用的安全性方法。但您可以使用 [遠端桌面工作階段主機設定] 工具，設定這些連線的必要安全性方法。

表 5-36. RDS 安全群組原則設定 (續)

設定	說明
Require user authentication for remote connections by using Network	使用此原則設定，可指定是否要使用「網路層級驗證」要求 RDS 主機的遠端連線進行使用者驗證。這個原則設定要求使用者驗證在遠端連線處理程序初期執行，以增強安全性。 如果啟用此原則設定，將只有支援網路層級驗證的用戶端電腦可連線至 RDS 主機。 若要判斷用戶端電腦是否支援網路層級驗證，請在用戶端電腦上啟動 [遠端桌面連線]，按一下 [遠端桌面連線] 對話方塊左上角的圖示，然後按一下 [關於]。在 [關於遠端桌面連線] 對話方塊中，尋找是否出現「支援網路層級驗證」。 如果停用或未設定此原則設定，則在允許遠端連線至 RDS 主機之前，無需使用網路層級驗證進行使用者驗證。 您可以使用 [遠端桌面工作階段主機設定] 工具，或是 [系統內容] 中的 [遠端] 索引標籤，指定必須使用網路層級驗證進行使用者驗證。 **重要** 停用或未設定這個原則設定將提供較低的安全性，因為使用者驗證將在遠端連線程序後期執行。
Do not allow local administrators to customize permissions	指定是否停用管理員在「遠端桌面工作階段主機設定」工具中自訂安全性權限的權限。 您可以使用這個設定，防止管理員在「遠端桌面工作階段主機設定」工具中的 [權限] 索引標籤上對使用者群組進行變更。依預設，管理員有權進行此類變更。 若狀態設定為 [已啟用]，則無法使用「遠端桌面工作階段主機設定」工具中的 [權限] 索引標籤來自訂每個連線的安全性說明元，也不能變更現有群組的預設安全性說明元。所有安全性說明元皆為「唯讀」。 若狀態設定為 [已停用] 或 [未設定]，則伺服器管理員具有在「遠端桌面工作階段主機設定」工具中的 [權限] 索引標籤上完整讀取/寫入使用者安全性說明元的權限。 **備註** 管理使用者存取的慣用方法，是將使用者新增至遠端桌面平台使用者群組。

RDS 工作階段時間限制

RDS 工作階段時間限制群組原則設定可讓使用者為 RDS 主機上的工作階段設定時間限制的原則。

Horizon 7 RDS 群組原則設定安裝於**電腦設定 > 原則 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 工作階段時間限制**資料夾中。

Horizon 7 RDS 群組原則設定也安裝於**使用者設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 工作階段時間限制**資料夾中。

表 5-37. RDS 工作階段時間限制群組原則設定

設定	說明
Set time limit for disconnected sessions	使用此原則設定，可為中斷連線的「遠端桌面服務」工作階段設定時間限制。 您可以使用此原則設定，指定中斷連線的工作階段在伺服器上保持為使用中狀態的時間長度上限。依預設，遠端桌面服務可讓使用者在無須登出及結束工作階段的情況下，中斷「遠端桌面服務」工作階段的連線。 當工作階段處於中斷連線狀態時，即使使用者目前已不在連線中的狀態，執行中的程式仍會保持使用中狀態。依預設，這些中斷連線的工作階段在伺服器上會無限期保留。 如果啟用此原則設定，經過指定的時間後會將已中斷連線的工作階段從伺服器中刪除。若要強制執行將中斷連線的工作階段無限期保留的預設行為，請選取「永不」。如果您有主控台工作階段，則不會套用中斷連線的工作階段時間限制。 如果停用或未設定此原則設定，則會無限期保留中斷連線的工作階段。您可以在 [遠端桌面工作階段主機設定] 工具的 [工作階段] 索引標籤上，為中斷連線的工作階段指定時間限制。 **備註** 此原則設定會同時顯示在「電腦設定」和「使用者設定」中。如果同時設定了這兩個原則設定，則以「電腦設定」原則設定優先。
Set time limit for active but idle Remote Desktop Services sessions	使用此原則設定，可指定使用中的「遠端桌面服務」工作階段在自動中斷連線之前可閒置 (沒有使用者輸入) 的時間長度上限。 如果啟用此原則設定，則必須在 [閒置工作階段限制] 下拉式清單中選取所需的時間限制。遠端桌面服務將在指定的時間長度經過後，自動將使用中但閒置的工作階段中斷連線。使用者會在工作階段中斷連線前兩分鐘收到警告訊息，讓他們可以按下按鍵或移動滑鼠，使工作階段保持使用中狀態。如果您有主控台工作階段，則不會套用閒置工作階段時間限制。 如果停用或未設定此原則設定，遠端桌面服務將會無限期地允許工作階段保持在使用中但閒置的狀態。您可以在 [遠端桌面工作階段主機設定] 工具的 [工作階段] 索引標籤上，為使用中但閒置的工作階段指定時間限制。 如果您要讓遠端桌面服務在達到時間限制時終止工作階段，而非中斷其連線，則可以設定**電腦設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 工作階段時間限制**資料夾中的「超過使用時間限制就終止工作階段」原則設定。 **備註** 此原則設定會同時顯示在「電腦設定」和「使用者設定」中。如果同時設定了這兩個原則設定，則以「電腦設定」原則設定優先。

表 5-37. RDS 工作階段時間限制群組原則設定 (續)

設定	說明
Set time limit for active Remote Desktop Services sessions	使用此原則設定，可指定「遠端桌面服務」工作階段在自動中斷連線之前可處於使用中狀態的時間長度上限。 如果啟用此原則設定，則必須在 [使用中工作階段限制] 下拉式清單中選取所需的時間限制。遠端桌面服務將在指定的時間長度經過後，自動將使用中的工作階段中斷連線。使用者會在遠端桌面服務工作階段中斷連線的前兩分鐘收到警告訊息，讓使用者能夠儲存開啟的檔案並關閉程式。如果您有主控台工作階段，則不會套用使用中的工作階段時間限制。 如果停用或未設定此原則設定，遠端桌面服務將會無限期允許工作階段保持在使用中狀態。您可以在 [遠端桌面工作階段主機設定] 工具的 [工作階段] 索引標籤上，為使用中的工作階段指定時間限制。 如果您要讓遠端桌面服務在達到時間限制時終止工作階段，而非中斷其連線，則可以設定**電腦設定 > 系統管理範本 > Windows 元件 > 遠端桌面服務 > 遠端桌面工作階段主機 > 工作階段時間限制**資料夾中的「超過使用時間限制就終止工作階段」原則設定。 **備註** 此原則設定會同時顯示在「電腦設定」和「使用者設定」中。如果同時設定了這兩個原則設定，則以「電腦設定」原則設定優先。

表 5-37. RDS 工作階段時間限制群組原則設定 (續)

設定	說明
Terminate session when time limits are reached	指定是否要終止逾時的「遠端桌面服務」工作階段，而非中斷其連線。 您可以使用此設定，指示遠端桌面服務在達到使用中或閒置工作階段的時間限制後終止工作階段 (即登出使用者，並從伺服器中刪除工作階段)。依預設，遠端桌面服務會將達到時間限制的工作階段中斷連線。 時間限制由伺服器管理員在本機設定，或在群組原則中設定。請參閱「設定使用中遠端桌面服務工作階段的時間限制」和「為使用中但閒置的遠端桌面服務工作階段設定時間限制」設定。 如果啟用此設定，遠端桌面服務將會終止任何達到逾時限制的工作階段。 如果停用此設定，即使伺服器管理員另行指定，遠端桌面服務一律會將逾時的工作階段中斷連線。 若未設定此設定，則遠端桌面服務會將逾時的工作階段中斷連線，除非本機設定中另行指定。 **備註** 此設定只適用於在 [遠端桌面工作階段主機設定] 工具或群組原則管理主控台中慎重設定的逾時限制，不適用於因連線或網路狀況而發生的逾時事件。此外，請注意這個設定同時出現在「電腦設定」和「使用者設定」中。如果同時設定了這兩項設定，將會以「電腦設定」設定優先。
Set time limit for logoff of RemoteApp sessions	使用此原則設定，可指定使用者的遠端應用程式工作階段在從 RDS 主機登出之前可處於中斷連線狀態的時間長度。 依預設，如果使用者關閉遠端應用程式，即會從 RDS 主機中斷工作階段的連線。 如果啟用此原則設定，當使用者關閉遠端應用程式時，在達到您所指定的時間限制之前，遠端應用程式工作階段仍將處於中斷連線狀態。在達到指定的時間限制時，遠端應用程式工作階段將會從 RDS 主機登出。如果使用者在達到時間限制之前啟動遠端應用程式，使用者將重新連線至 RDS 主機上已中斷連線的工作階段。 如果停用或未設定此原則設定，當使用者關閉遠端應用程式時，將會從 RDS 主機中斷工作階段的連線。 **備註** 此原則設定會同時顯示在「電腦設定」和「使用者設定」中。如果同時設定了這兩個原則設定，則以「電腦設定」原則設定優先。

RDS 暫存資料夾設定

RDS 連線群組原則設定可控制「遠端桌面平台服務」工作階段之暫存資料夾的建立與刪除。

表 5-38. RDS 暫存資料夾群組原則設定

設定	說明
`Do not delete temp folder upon exit`	指定「遠端桌面平台服務」在使用者登出時是否保留每個工作階段的暫存資料夾。 即便使用者已經從工作階段登出，您還是可以使用此設定，於遠端電腦上保留使用者工作階段特定的暫存資料夾。依預設，「遠端桌面平台服務」會在使用者登出時刪除使用者的暫存資料夾。 如果將狀態設定為「啟用」，則在使用者登出工作階段時，會保留使用者的每個工作階段暫存資料夾。 如果將狀態設定為「停用」，則即使管理員在「遠端桌面工作階段主機設定」工具中另有指定，使用者登出時也依然會刪除暫存資料夾。 如果將狀態設定為「未設定」，則除非伺服器管理員另有指定，否則「遠端桌面平台服務」會在登出時從遠端電腦中刪除暫存資料夾。 **備註** 此設定僅在伺服器上每個工作階段暫存資料夾處於使用中狀態時生效。即，如果啟用了「不要使用每一工作階段的暫存資料夾」設定，則此設定將不會生效。
`Do not use temporary folders per session`	此原則設定可讓您防止「遠端桌面平台服務」建立工作階段特定的暫存資料夾。 您可以在遠端電腦上使用此原則設定，以停用針對每個工作階段建立的不同暫存資料夾。依預設，「遠端桌面平台服務」會為使用者在遠端電腦上維持的每個作用中工作階段建立不同暫存資料夾。將在遠端電腦之使用者設定檔資料夾下的 Temp 資料夾中建立這些暫存資料夾，且會命名為 `sessionid`。 如果啟用此原則設定，則不會建立每個工作階段暫存資料夾。而是遠端電腦上所有工作階段的使用者暫存資料夾都儲存於遠端電腦上使用者設定檔資料夾下的通用暫存資料夾中。 如果停用此原則設定，則一律會建立每個工作階段暫存資料夾，即使在「遠端桌面工作階段主機設定」工具中另有指定亦然。 如果未設定此原則設定，則除非在「遠端桌面工作階段主機設定」工具中另有指定，否則便會建立每個工作階段暫存資料夾。

篩選虛擬列印的印表機

虛擬列印功能啟用時，使用者可以從遠端桌面平台和應用程式列印至其用戶端系統上任何可用的印表機。您可以使用**重新導向用戶端印表機時指定篩選器**代理程式群組原則設定，防止虛擬列印功能將特定用戶端印表機重新導向至遠端桌面平台和應用程式。

重新導向用戶端印表機時指定篩選器群組原則設定在 VMware Horizon 印表機重新導向 ADMX 範本檔 (`vdm_agent_printing.admx`) 中提供，而此檔案隨附於 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` 檔案中。如需安裝指示，請參閱將 ADMX 範本檔新增至 Active Directory。

當您啟用**重新導向用戶端印表機時指定篩選器**群組原則設定時，您必須在**登錄值名稱: PrinterFilterString** 文字方塊中輸入篩選規則。此篩選規則是一個指定印表機不應重新導向 (黑名單) 的規則運算式。任何與篩選規則中的印表機不相符的印表機，都會重新導向。篩選規則依預設為空白，這表示所有用戶端印表機都會重新導向。

下表列出可在篩選規則中使用的屬性、運算子和萬用字元。

表 5-39. 篩選規則支援的屬性、運算子和萬用字元

屬性	運算子	萬用字元
DriverName、VendorName 和 PrinterName	AND、OR 和 NOT	* 和 ?

以下提供數個篩選規則範例。

```
(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e"

PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF"

PrinterName!=".*PDFCreator.*"
```

當您在虛擬桌面平台或 RDS 主機上安裝 Horizon Agent 時，可以啟用虛擬列印功能。如需安裝指示，請參閱《在 Horizon 7 中設定虛擬桌面平台》和《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件。

設定依據位置列印

依據位置列印功能可以將實體位置鄰近用戶端系統的印表機對應至遠端桌面平台，讓使用者能夠從其遠端桌面平台列印至本機或網路印表機。

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。

依據位置列印功能適用於 Windows、Mac、Linux 和行動用戶端裝置。此功能也適用於瀏覽器型用戶端。

備註 如果您使用 HTML Access 連線至遠端桌面平台和已發佈的應用程式，則不支援使用 MAC 位址或用戶端名稱的依據位置列印原則。

下列遠端桌面平台和應用程式支援依據位置列印功能：

- 在單一使用者機器上部署的桌面平台，包括 Windows 桌面平台和 Windows Server 機器。
- 在 RDS 主機上部署的已發佈桌面平台和已發佈應用程式，其中 RDS 主機為虛擬機器或實體機器
- 從遠端桌面平台內的 Horizon Client 啟動的已發佈應用程式

若要使用依據位置列印功能，您必須在安裝 Horizon Agent 的同時一併安裝虛擬列印安裝選項，並在桌面平台上安裝正確的印表機驅動程式。

若要設定依據位置列印，請設定 Active Directory 群組原則設定 `AutoConnect Map Additional Printers for VMware View`，位於**電腦設定**下，**軟體設定**資料夾中的 Microsoft 群組原則物件編輯器中。

備註 `AutoConnect Map Additional Printers for VMware View` 是一種電腦專用原則。電腦專用原則適用於所有遠端桌面平台，無論誰連線至桌面平台都一樣。

`AutoConnect Map Additional Printers for VMware View` 會實作為名稱轉譯表。您可以使用表中的每一列來識別特定印表機，並為該印表機定義一組轉譯規則。轉譯規則會決定印表機是否對應至特定用戶端系統的遠端桌面平台。

使用者連線至遠端桌面平台時，Horizon 7 會將用戶端系統與表格中每個印表機相關聯的轉譯規則進行比較。如果用戶端系統符合為印表機設定的所有轉譯規則，或是印表機沒有相關聯的轉譯規則，則 Horizon 7 會在使用者工作階段期間，將印表機對應至遠端桌面平台。

您可以依據用戶端系統的 IP 位址、名稱和 MAC 位址，以及使用者的名稱和群組，來定義轉譯規則。您可以為特定印表機指定一個轉譯規則，或是數個轉譯規則的組合。

用來將印表機對應至遠端桌面平台的資訊會儲存在遠端桌面平台的登錄項目中，路徑為 `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect`。

適用於隨選列印的印表機設定

使用者登出桌面平台或與其中斷連線之後，隨選印表機的印表機設定會保留。例如，使用者可設定依據位置印表機使用黑白模式。使用者登出桌面平台並再次登入後，依據位置印表機會繼續使用黑白模式。

若要在已發佈的應用程式中跨工作階段儲存印表機設定，使用者必須從應用程式的列印對話方塊中選取依據位置的印表機、以滑鼠右鍵按一下選取的印表機，然後選取**列印喜好設定**。使用者選取印表機並按一下應用程式之列印對話方塊中的**喜好設定**按鈕時，印表機設定將不會儲存。

如果設定儲存在印表機驅動程式的私密空間，而非印表機驅動程式的 DEVMODE 延伸部分 (如 Microsoft 建議)，則適用於依據位置印表機的持續性設定不受支援。若要支援持續性設定，請部署印表機將設定儲存在印表機驅動程式的 DEVMODE 部分。

登錄依據位置列印群組原則 DLL 檔案

您必須先登錄 DLL 檔 `TPVMGPoACmap.dll`，才能設定依據位置列印的群組原則設定。

32 位元和 64 位元版本的 `TPVMGPoACmap.dll` 可從封裝的 `.zip` 檔案中取得，該檔案名為 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`，其中 *x.x.x* 為版本，*yyyyyyy* 為組建編號。您可以從 VMware 下載網站下載此檔案，網址為 http://www.vmware.com/go/downloadview。

程序

1. 將適當版本的 `TPVMGPoACmap.dll` 複製到您的 Active Directory 伺服器，或者您用來設定群組原則的網域電腦。
2. 使用 `regsvr32` 公用程式登錄 `TPVMGPoACmap.dll` 檔。

   例如：`regsvr32 "C:\TPVMGPoACmap.dll"`

後續步驟

為依據位置列印設定群組原則設定。

設定依據位置列印群組原則

若要設定依據位置列印，請設定 `AutoConnect Map Additional Printers for VMware View` 群組原則設定。群組原則設定為將印表機對應至 Horizon 桌面平台的名稱轉譯表。

必要條件

- 確認 Active Directory 伺服器上或您用來設定群組原則的網域電腦上，提供 Microsoft MMC 和群組原則物件編輯器嵌入式管理單元。
- 在 Active Directory 伺服器上或您用來設定群組原則的網域電腦上，登錄 DLL 檔案 `TPVMGPoACmap.dll`。請參閱登錄依據位置列印群組原則 DLL 檔案。
- 自行熟悉 `AutoConnect Map Additional Printers for VMware View` 群組原則設定的語法。請參閱依據位置列印群組原則設定語法。
- 為依據位置的群組原則設定建立 GPO，並將其連結至包含 Horizon 桌面平台的 OU。請參閱建立 Horizon 7 群組原則的 GPO 中關於如何為 Horizon 群組原則建立 GPO 的範例。
- 確認虛擬列印安裝選項已經隨同 Horizon Agent 一併安裝於桌面平台中。若要確認，請檢查桌面平台作業系統中是否安裝了 TP 自動連線服務與 TP VC 安全閘道服務。
- 由於列印工作會從 Horizon 桌面平台直接傳送至印表機，因此請確認桌面平台上已安裝必要的印表機驅動程式。

程序

1 在 Active Directory 伺服器上，編輯 GPO。

AD 版本	瀏覽路徑
Windows 2003	a 選取**開始 > 所有程式 > 系統管理工具 > Active Directory 使用者和電腦**。 b 以滑鼠右鍵按一下包含 Horizon 桌面平台的 OU，然後選取**屬性**。 c 在 **群組原則** 標籤上，按一下 **開啟** 以開啟群組原則管理外掛程式。 d 在右窗格中，以滑鼠右鍵按一下您為依據位置列印群組原則設定所建立的 GPO，然後選取**編輯**。
Windows 2008	a 選取**開始 > 系統管理工具 > 群組原則管理**。 b 展開您的網域，以滑鼠右鍵按一下您為依據位置列印群組原則設定所建立的 GPO，然後選取**編輯**。

群組原則物件編輯器視窗隨即出現。

2 展開**電腦設定**，開啟**軟體設定**資料夾，然後選取**為 VMware View 自動連線對應其他印表機**。

3 在「原則」窗格中，按兩下**設定自動連線對應其他印表機**。

此時會出現**為 VMware View 自動連線對應其他印表機**視窗。

4 選取**已啟用**以啟用群組原則設定。

此時轉譯表的標題和按鈕均會出現在群組原則視窗中。

重要 按一下**已停用**會刪除所有資料表項目。為了安全起見，請先儲存您的組態，以便日後匯入。

5 新增您要對應至 Horizon 桌面平台的印表機，然後定義其相關聯的轉譯規則。

6 按一下**確定**儲存變更。

依據位置列印群組原則設定語法

您可以使用 AutoConnect Map Additional Printers for VMware View 群組原則設定，將印表機對應至遠端桌面平台。

AutoConnect Map Additional Printers for VMware View 是一種名稱轉譯表，可識別印表機並定義相關的轉譯規則。表 5-40. 轉譯表欄與值中說明轉譯表的語法。

依據位置列印會將本機印表機對應至遠端桌面平台，但不支援對應透過使用 UNC 路徑設定的網路印表機。

表 5-40. 轉譯表欄與值

欄	說明
IP Range	指定用戶端系統 IP 位址範圍的轉譯規則。 若要指定特定範圍內的 IP 位址，請使用下列標記法： ***ip_address-ip_address*** 例如：**10.112.116.0-10.112.119.255** 若要指定特定子網路內的所有 IP 位址，請使用下列標記法： *ip_address/subnet_mask_bits* 例如：**10.112.4.0/22** 此標記法會指定從 10.112.4.1 到 10.112.7.254 的可使用 IPv4 位址。 輸入星號以符合任何 IP 位址。 **重要** 在 IPv6 混合模式環境中，針對一台印表機新增兩個 IP 位址範圍 (一個範圍用於 IPv4 位址，而另一個用於 IPv6 位址)，以確保無論 Horizon Client 使用哪種通訊協定進行連線，印表機皆會顯示在遠端工作階段中。
Client Name	指定電腦名稱的轉譯規則。 例如：**Mary's Computer** 輸入星號以符合任何電腦名稱。
Mac Address	指定 MAC 位址的轉譯規則。在 GPO 編輯器中，您必須使用與用戶端系統使用的相同格式。例如： ■ Windows 用戶端使用連字號：**01-23-45-67-89-ab** ■ Linux 用戶端使用冒號：**01:23:45:67:89:ab** 輸入星號以符合任何 MAC 位址。
User/Group	指定使用者或群組名稱的轉譯規則。 若要指定特定使用者或群組，請使用下列標記法： *\\domain\user_or_group* 例如：**\\mydomain\Mary** 完整網域名稱 (FQDN) 不是網域名稱的支援標記法。輸入星號以符合任何使用者或群組名稱。
Printer Name	印表機對應至遠端桌面平台時的名稱。 例如：**PRINTER-2-CLR** 對應的名稱不必符合用戶端系統上的印表機名稱。 該印表機必須是用戶端裝置的印表機。不支援對應 UNC 路徑中的網路印表機。

表 5-40. 轉譯表欄與值 (續)

欄	說明
Printer Driver	印表機使用的驅動程式名稱。 例如：**HP Color LaserJet 4700 PS** **重要** 因為印表機工作是直接從遠端桌面平台傳送至印表機，所以印表機驅動程式必須安裝在遠端桌面平台上。
IP Port/ThinPrint Port	對於網路印表機，印表機的 IP 位址字首為 **IP_**。 例如：**IP_10.114.24.1** 預設連接埠是 9100。您可以透過為 IP 位址附加連接埠號碼來指定一個非預設連接埠。 例如：**IP_10.114.24.1:9104**
Default	表示印表機是否為預設印表機。

使用顯示在欄標題上方的按鈕可新增、刪除與移動資料列，並儲存與匯入資料表項目。每個按鈕都有等同的鍵盤快速鍵。將滑鼠移動每個按鈕上方，便會顯示按鈕的說明及其等同的鍵盤快速鍵。例如，若要將資料列插入至資料表結尾，請按一下第一個資料表按鈕或按 Alt+A。按一下最後兩個按鈕可匯入與儲存資料表項目。

表 5-41. 依據位置列印群組原則設定範例會顯示一個有關兩個轉譯表資料列範例。

表 5-41. 依據位置列印群組原則設定範例

IP 範圍	用戶端名稱	Mac 位址	使用者/群組	印表機名稱	印表機驅動程式	IP 連接埠/ThinPrint 連接埠	預設值
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

在第一列指定的網路印表機將對應至任何用戶端系統的遠端桌面平台，因為星號出現在所有的轉譯規則欄中。只有在用戶端系統的 IP 位址範圍在 10.112.116.140 到 10.112.116.145 之間，在第二列指定的網路印表機才會對應至遠端桌面平台。

管理特殊 Unity 視窗

在使用已發佈的應用程式時，您可以使用 **Unity 篩選規則清單**代理程式群組原則設定來篩選 Unity 視窗，或將 Unity 視窗對應到特定類型。如果您遇到視窗顯示問題 (例如視窗有黑色背景，或下拉式視窗的大小不正確)，則此功能很實用。

Unity 篩選規則清單群組原則設定在 VMware View Agent 組態 ADMX 範本檔 (vdm_agent.admx) 中提供，而此檔案隨附於 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip 檔案中。如需安裝指示，請參閱將 ADMX 範本檔新增至 Active Directory。

啟用 **Unity 篩選規則清單**群組原則設定時，請按一下**顯示**，並在**值**文字方塊中輸入篩選規則。篩選規則由特性和動作組成。如果您指定對應動作，則也必須包含類型。下表列出可在篩選規則中使用的特性、動作和類型。

表 5-42. Unity 篩選規則的特性、動作和類型

特性	動作	類型
classname、company、product、major、minor、build、revision	block、map	normal、panel、dialog、tooltip、splash、toolbar、dock、desktop、widget、combobox、startscreen、sidepanel、taskbar、metrofullscreen、metrodocked

Windows 類別名稱通常是慣用的特性，例如 `classname=CustomClassName`。如果您必須將規則限制至特定產品，此處提供 `company`、`product`、`major`、`minor`、`build` 和 `revision` 特性。您可以在可執行檔的**內容**視窗中找到這些特性的值。這些特性的值必須是大小寫完全相符，包括任何特殊字元。如果您提供多個特性，則所有值皆必須相符，才能將規則套用至視窗。

若要指定動作，請輸入 `action=`*`value`*，例如 `action=block`。`block` 動作告知 Horizon Agent 不要在用戶端上顯示視窗。當用戶端上的視窗顯示過大或干擾正常的視窗焦點行為時，請使用 `block` 動作。

`map` 動作 (例如 `action=map`) 告知 Horizon Agent 將視窗視為某種經過硬式編碼的類型。若要指定類型，您必須在規則中包含 `type=`*`value`*，例如 `type=normal`。由於難以判斷視窗是否對應至錯誤類型，因此，只有在 VMware 支援指示您將視窗對應至某個類型時，您才需要這麼做。

篩選規則範例

下列篩選規則會封鎖所有類別名稱為 MyClassName 的視窗。

```
classname=MyClassName;action=block
```

下列篩選規則會封鎖來自名稱為 MyProduct 之產品的所有視窗。

```
product=MyProduct;action=block
```

下列篩選規則會將自訂類別對應至下拉式方塊類型。

```
classname=MyClassName;action=map;type=combobox
```

備註 與在 RDS 主機上 `%ProgramData%\VMware\RdeServer\Unity Filters` 目錄內檔案中指定的篩選規則相比，**Unity 篩選規則清單**群組原則設定具有較低優先順序。

Active Directory 群組原則範例

在 Horizon 7 中實作 Active Directory 群組原則的一種方法，是為提供遠端桌面工作階段的機器建立一個 OU，並將一或多個 GPO 連結至該 OU。您可以使用這些 GPO 將群組原則設定套用至您的 Horizon 7 機器。

如果原則設定套用至網域內的所有電腦，則您可以將 GPO 直接連結至網域。但是，最佳做法是，大多數部署應該將 GPO 連結至個別 OU，避免在網域中的所有電腦上進行原則處理。

您可以在 Active Directory 伺服器或網域中的任何電腦上設定原則。此範例顯示如何在 Active Directory 伺服器上直接設定原則。

備註 由於各個 Horizon 7 環境均不相同，因此您可能需要執行不同的步驟，才能滿足組織特定的需求。

建立 Horizon 7 機器的 OU

若要將群組原則套用至提供遠端桌面工作階段的機器，而不影響相同 Active Directory 網域中的其他 Windows 電腦，請專門針對您的 Horizon 7 機器建立一個 OU。您可以為整個 Horizon 7 部署建立一個 OU，或分別為虛擬桌面平台機器和 RDS 主機建立個別的 OU。

程序

1. 在 Active Directory 伺服器上，選取**開始 > 所有程式 > 系統管理工具 > Active Directory 使用者和電腦**。
2. 在包含 Horizon 7 機器的網域上按一下滑鼠右鍵，然後選取**新增 > 組織單位**。
3. 輸入 OU 的名稱，然後按一下**確定**。

   此時新 OU 會出現在左窗格中。
4. 將 Horizon 7 機器新增至新 OU。
   a. 按一下左窗格中的**電腦**。

      此時網域中的所有電腦物件都會出現在右窗格中。
   b. 在右面板中代表 Horizon 7 機器的電腦物件名稱上按一下滑鼠右鍵，然後選取**移動**。
   c. 選取 OU，然後按一下**確定**。

      當您選取 OU 時，Horizon 7 機器便會出現在右窗格中。

後續步驟

建立 Horizon 7 群組原則的 GPO。

建立 Horizon 7 群組原則的 GPO

建立 GPO 以包含 Horizon 7 元件的群組原則和依據位置列印，並將它們連結至 Horizon 7 機器的 OU。

必要條件

- 建立 Horizon 7 機器的 OU。
- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 和群組原則管理嵌入式管理單元可供使用。

程序

1. 在 Active Directory 伺服器上，開啟群組原則管理主控台。
2. 展開網域，在包含 Horizon 7 機器的 OU 上按一下滑鼠右鍵，並選取**在這個網域中建立 GPO 並連結到**。

3 輸入 GPO 名稱，然後按一下**確定**。

此時新 GPO 會出現在左窗格中的 OU 之下。

4 (選擇性) 將 GPO 套用至 OU 中的特定 Horizon 7 機器。

a 選取左窗格中的 GPO。

b 選取**安全性篩選 > 新增**。

c 輸入 Horizon 7 機器的電腦名稱，然後按一下**確定**。

此時 Horizon 7 機器會出現在 [安全性篩選] 窗格中。GPO 中的設定只會套用至這些機器。

後續步驟

將 Horizon ADMX 範本新增至 GPO。

將 Horizon 7 ADMX 範本檔新增至 GPO

若要將 Horizon 7 元件群組原則設定套用至您的桌面平台和應用程式，請將其 ADMX 範本檔新增至 GPO。

必要條件

- 為 Horizon 7 元件群組原則設定建立 GPO，並將其連結到包含 Horizon 7 機器的 OU。
- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 和群組原則管理嵌入式管理單元可供使用。

程序

1 從 VMware 下載網站下載 Horizon 7 GPO 服務包 `.zip` 檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在「桌面平台及使用者運算」下，選取 VMware Horizon 7 下載，其中包含 GPO 服務包。

該檔案名為 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`，其中 *x.x.x* 為版本，而 *yyyyyyy* 為組建編號。為 Horizon 7 提供群組原則設定的所有 ADMX 檔案皆可從此檔案取得。

2 解壓縮 `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` 檔案，並將 ADMX 檔案複製到您的 Active Directory 伺服器。

a 將 `.admx` 檔案和 `en-US` 資料夾複製到 Active Directory 伺服器上的 `%systemroot%\PolicyDefinitions` 資料夾。

b 將語言資源檔案 (`.adml`) 複製到 Active Directory 伺服器上 `%systemroot%\PolicyDefinitions\` 下的適當子資料夾中。

3 在 Active Directory 伺服器上開啟群組原則管理編輯器，然後輸入範本檔在安裝後出現於編輯器中的路徑。

後續步驟

設定群組原則設定，並啟用 Horizon 7 機器的回送處理。

啟用遠端桌面平台的回送處理

若要讓通常套用到電腦上的使用者組態設定，套用到所有登入該電腦的使用者上，請啟用回送處理。

必要條件

- 為 Horizon 7 元件群組原則設定建立 GPO，並將其連結到包含 Horizon 7 機器的 OU。
- 確認您可以用主控 Active Directory 伺服器之機器上的管理員網域使用者身分登入。
- 確認 Active Directory 伺服器上有 MMC 和群組原則管理嵌入式管理單元可供使用。

程序

1. 在 Active Directory 伺服器上，開啟群組原則管理主控台。
2. 展開網域，在為群組原則設定建立的 GPO 上按一下滑鼠右鍵，並選取**編輯**。
3. 在群組原則管理編輯器中，導覽至**電腦設定 > 原則 > 系統管理範本：原則定義 > 系統 > 群組原則**。
4. 在右窗格中，按兩下**使用者群組原則回送處理模式**。
5. 選取**已啟用**，再從**模式**下拉式功能表中選取回送處理模式。

選項	動作
合併	套用的使用者原則設定，是電腦與使用者 GPO 中所包含使用者原則設定的組合。當有衝突時，電腦 GPO 有優先性。
替換	使用者原則完全是從與電腦相關聯的 GPO 中定義。與使用者相關聯的任何 GPO 都會被忽略。

6. 按一下**確定**儲存變更。