Horizon 7 管理

2019 年 12 月
VMware Horizon 7 7.11

vmware®

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

如果您對於本文件有任何意見，歡迎寄至：

docfeedback@vmware.com

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

目錄

Horizon 7 管理

《Horizon 7 管理》說明如何設定和管理 VMware Horizon® 7，包括如何設定 Horizon 連線伺服器、建立管理員、設定使用者驗證、設定原則，以及在 Horizon Administrator 中管理 VMware ThinApp® 應用程式。此文件也說明如何維護 Horizon 7 元件和進行疑難排解。

主要對象

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

使用 Horizon Administrator 1

Horizon Administrator 是一個可用來設定 Horizon 連線伺服器及管理遠端桌面平台和應用程式的 Web 介面。

有關可以使用 Horizon Administrator、Cmdlet 及 `vdmadmin` 執行的作業的比較，請參閱《Horizon 7 整合》文件。

本章節討論下列主題：

- Horizon Administrator 和 Horizon 連線伺服器
- 登入 Horizon Administrator
- Horizon Administrator 介面的使用提示
- 對 Horizon Administrator 中的文字顯示進行疑難排解

Horizon Administrator 和 Horizon 連線伺服器

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

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

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

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

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

登入 Horizon Administrator

若要執行初始組態工作，您必須登入 Horizon Administrator。您可以使用安全 (TLS) 連線來存取 Horizon Administrator。

備註　Horizon Administrator 將於 2020 年初淘汰。您可以使用 Horizon Console 執行相同的管理工作。如需關於使用 Horizon Console 的詳細資訊，請參閱《VMware Horizon Console 管理》文件。

必要條件

- 確認 Horizon 連線伺服器已安裝在專用電腦上。
- 確認您使用 Horizon Administrator 支援的網頁瀏覽器。如需 Horizon Administrator 的需求，請參閱《Horizon 7 安裝》文件。

程序

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

`https://server/admin`

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

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

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

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

3 使用具有管理員角色的帳戶登入。

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

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

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

Horizon Administrator 介面的使用提示

您可以使用 Horizon Administrator 使用者介面功能來導覽 Horizon 頁面，並尋找、篩選和排序 Horizon 物件。

Horizon Administrator 包含多項常用的使用者介面功能。例如，每個頁面左側的導覽窗格，可將您引導至其他 Horizon Administrator 頁面。搜尋篩選器可以讓您選取與您要搜尋之物件相關的篩選準則。

下表針對幾項可協助您使用 Horizon Administrator 的其他功能加以說明。

表 1-1. Horizon Administrator 導覽和顯示功能

Horizon Administrator 功能	說明
在 Horizon Administrator 頁面中向後和向前瀏覽	按一下瀏覽器的**上一頁**按鈕，移至先前顯示的 Horizon Administrator 頁面。按一下**向前**按鈕以返回目前頁面。 若您在使用 Horizon Administrator 精靈或對話方塊時，按一下瀏覽器的**上一頁**按鈕，則會返回主要 Horizon Administrator 頁面。您在精靈或對話方塊中輸入的資訊將會遺失。 在 View 5.1 之前的版本中，您無法使用瀏覽器的**上一頁**和**下一頁**按鈕在 Horizon Administrator 內導覽。這些版本另外在 Horizon Administrator 視窗中提供**上一頁**和**下一頁**按鈕，供導覽之用。View 5.1 版移除了這些按鈕。
以書籤標示 Horizon Administrator 頁面	您可以在瀏覽器中以書籤標示 Horizon Administrator 頁面。
多欄排序	您可以使用多欄排序，以多種方式為 Horizon 物件排序。 按一下 Horizon Administrator 資料表頂端列的標題，可根據該標題按字母順序為 Horizon 物件排序。 例如，您可以在**資源 > 機器**頁面上按一下**桌面平台集區**，依包含桌面平台的集區為桌面平台排序。 標題旁會出現數字 **1**，指出這是主要的排序欄。您可以再次按一下標題以反轉排序順序，這會以向上或向下箭頭指示。 若要以次要項目為 Horizon 物件排序，請按住 Ctrl 並點選其他標題。 例如，在 [機器] 資料表中，您可以按一下**使用者**，依桌面平台的專屬使用者執行次要排序。第二標題旁會出現數字 **2**。在此範例中，桌面平台會依集區和每個集區中的使用者排序。 您可以繼續按 Ctrl 加標題，依重要性遞減順序為資料表中的所有欄排序。 按 Ctrl+Shift 同時按一下標題，可取消選取排序項目。 例如，您可能會想要顯示集區中，具有特殊狀態並儲存在特定資料存放區中的桌面平台。您可以選取**資源 > 機器**，按一下**資料存放區**標題，然後按住 Ctrl 並點選**狀態**標題。
自訂資料表欄	您可以隱藏選取的資料行並鎖定第一個資料行，以自訂 Horizon Administrator 資料表資料行的顯示方式。此功能可讓您控制大型資料表的顯示方式，例如包含許多資料行的**類別目錄 > 桌面平台集區**。 在任一欄標題上按一下滑鼠右鍵，以顯示可讓您採取下列動作的內容功能表： ■ 隱藏所選欄。 ■ 自訂欄。對話方塊顯示資料表中的所有欄。您可以選取欄以顯示或隱藏。 ■ 鎖定第一欄。此選項可以在水平捲動包含許多欄的資料表時，強制顯示左欄。例如，在**類別目錄 > 桌面平台集區**頁面上，當您水平捲動以查看其他桌面平台特性時，桌面平台識別碼會固定顯示在畫面上。

表 1-1. Horizon Administrator 導覽和顯示功能 (續)

Horizon Administrator 功能	說明
選取 Horizon 物件並顯示 Horizon 物件詳細資料	在列出 Horizon 物件的 Horizon Administrator 資料表中，您可以選取物件或顯示物件詳細資料。 ■ 若要選取物件，請在資料表中物件列的任何地方按一下。頁面上方用來管理物件的功能表和命令會變得可供使用。 ■ 若要顯示物件詳細資料，請按兩下物件列中的左側儲存格。物件詳細資料會以新頁面顯示。 例如，在**類別目錄 > 桌面平台集區**頁面上，按一下個別集區之資料列中的任一處，以啟用會影響集區的命令。 按兩下左側欄中的**識別碼**儲存格，以顯示包含集區詳細資料的新頁面。
展開對話方塊以檢視詳細資料	您可以展開 Horizon Administrator 對話方塊，以檢視資料表資料行中的詳細資料，例如桌面平台名稱和使用者名稱。 若要展開對話方塊，請將滑鼠置於對話方塊右下角的點上方，然後拖曳角落。
顯示 Horizon 物件的內容功能表	您可以對 Horizon Administrator 資料表中的 Horizon 物件按一下滑鼠右鍵，以顯示內容功能表。內容功能表可讓您存取作用於所選 Horizon 物件的命令。 例如，您可以在**類別目錄 > 桌面平台集區**頁面上，以滑鼠右鍵按一下桌面平台集區，以顯示**新增**、**編輯**、**刪除**、**停用 (或啟用) 佈建**等命令。

對 Horizon Administrator 中的文字顯示進行疑難排解

如果您的網頁瀏覽器執行於非 Windows 作業系統 (例如 Linux、UNIX 或 Mac OS 等)，Horizon Administrator 中的文字將無法正常顯示。

問題

Horizon Administrator 介面中的文字會變成亂碼。例如，文字中間會出現空格。

原因

Horizon Administrator 需要 Microsoft 特有的字型。

解決方案

在您的電腦上安裝 Microsoft 特有的字型。

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

設定 Horizon 連線伺服器 2

安裝和執行 Horizon 連線伺服器的初始組態後，即可將 vCenter Server 執行個體和 View Composer 服務新增至 Horizon 7 部署、設定角色以委派管理員責任，以及排程組態資料的備份時間。

本章節討論下列主題：

設定 vCenter Server 和 View Composer

若要使用虛擬機器做為遠端桌面平台，您必須將 View 設定為與 vCenter Server 通訊。若要建立和管理連結複製桌面平台集區，您必須在 Horizon Administrator 中進行 View Composer 設定。

您也可以進行 Horizon 7 的儲存設定。您可以允許 ESXi 主機回收連結複製虛擬機器上的磁碟空間。若要允許 ESXi 主機快取虛擬機器資料，您必須啟用 vCenter Server 的 View 儲存加速器。

建立 View Composer AD 作業的使用者帳戶

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

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

程序

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

2 將**建立電腦物件**、**刪除電腦物件**及**寫入全部內容**權限新增至建立連結複製電腦帳戶所在或是連結複製電腦帳戶移至其中的 Active Directory 容器中的帳戶。

下列清單顯示使用者帳戶需要的所有權限，包括預設指定的權限：

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

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

- 列出內容
- 讀取全部內容
- 讀取權限
- 重設密碼

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

後續步驟

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

將 vCenter Server 執行個體新增到 Horizon 7

在 Horizon 7 部署中，您必須設定 Horizon 7 以連線至 vCenter Server 執行個體。vCenter Server 會建立並管理 Horizon 7 在桌面平台集區中使用的虛擬機器。

如果需在連結模式群組中執行 vCenter Server 執行個體，您必須將每個 vCenter Server 執行個體分別新增至 Horizon 7。

Horizon 7 將使用安全通道 (SSL) 連線至 vCenter Server 執行個體。

必要條件

- 安裝連線伺服器產品授權金鑰。
- 讓 vCenter Server 使用者有權執行支援 Horizon 7 所需的 vCenter Server 作業。若要使用 View Composer，您必須將其他權限授予使用者。

  如需關於為 Horizon 7 設定 vCenter Server 使用者的詳細資料，請參閱《Horizon 7 安裝》文件。

- 確認在 vCenter Server 主機上安裝 TLS/SSL 伺服器憑證。在生產環境中，安裝受信任的憑證授權機構 (CA) 所簽署的有效憑證。

  在測試環境中，您可以使用與 vCenter Server 一併安裝的預設憑證，但是必須在將 vCenter Server 新增至 Horizon 7 時接受憑證指紋。

- 確認複寫的群組中所有連線伺服器執行個體皆信任 vCenter Server 主機上安裝之伺服器憑證所屬的根 CA 憑證。檢查根 CA 憑證是否出現在**受信任的根憑證授權單位 > 憑證**資料夾中；該資料夾位於連線伺服器主機的 Windows 本機電腦憑證存放區中。若未出現，請將根 CA 憑證匯入至 Windows 本機電腦憑證存放區。

  請參閱《Horizon 7 安裝》文件中的〈將根憑證和中繼憑證匯入至 Windows 憑證存放區〉。

- 確認 vCenter Server 執行個體包含 ESXi 主機。如果並未在 vCenter Server 執行個體中設定任何主機，則無法將執行個體新增至 Horizon 7。

- 如果您升級到 vSphere 5.5 或更新版本，請確認您用作 vCenter Server 使用者的網域管理員帳戶已明確獲得指派 vCenter Server 本機使用者登入 vCenter Server 的權限。

- 若您計劃以 FIPS 模式使用 Horizon 7，請確認您擁有 vCenter Server 6.0 或更新版本以及 ESXi 6.0 或更新版本的主機。

  如需詳細資訊，請參閱《Horizon 7 安裝》文件中的〈以 FIPS 模式安裝 Horizon 7〉。

- 請自行熟悉決定 vCenter Server 及 View Composer 作業數上限的設定。請參閱 vCenter Server 和 View Composer 的並行作業限制與設定並行電源作業率以支援遠端桌面平台登入風暴。

程序

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

2 在 **vCenter Server** 索引標籤上，按一下**新增**。

3 在 vCenter Server 設定**伺服器位址**文字方塊中，輸入 vCenter Server 執行個體的完整網域名稱 (FQDN)。

  FQDN 包含主機名稱及網域名稱。例如，在 FQDN ***myserverhost.companydomain.com*** 中，***myserverhost*** 是主機名稱，***companydomain.com*** 是網域。

  備註 如果使用 DNS 名稱或 URL 輸入伺服器，則 Horizon 7 將不執行 DNS 查詢來確認管理員先前是否使用此伺服器的 IP 位址，將此伺服器新增至 Horizon 7。如果使用 DNS 名稱及 IP 位址新增 vCenter Server，將發生衝突。

4 輸入 vCenter Server 使用者的名稱。

  例如：**domain\user** 或 **user@domain.com**

5 輸入 vCenter Server 使用者密碼。

6 (選擇性) 輸入此 vCenter Server 執行個體的描述。

7 輸入 TCP 連接埠號碼。

  預設連接埠為 443。

8 在「進階設定」下，設定 vCenter Server 及 View Composer 作業的並行作業限制。

9 按**下一步**將顯示「View Composer 設定」頁面。

後續步驟

設定 View Composer。

- 如果已使用簽署的 SSL 憑證設定 vCenter Server 執行個體，且連線伺服器信任根憑證，則「新增 vCenter Server」精靈將顯示「View Composer 設定」頁面。
- 如果已使用預設憑證設定 vCenter Server 執行個體，則必須先決定是否接受現有憑證的指紋。請參閱接受預設 TLS 憑證的指紋。

如果 Horizon 7 使用多個 vCenter Server 執行個體，則請重複執行此程序來新增其他 vCenter Server 執行個體。

設定 View Composer

若要使用 View Composer，您必須進行設定，允許 Horizon 7 連線至 VMware Horizon View Composer 服務。View Composer 可以安裝在本身的另一個主機上，或與 vCenter Server 相同的主機上。

每個 VMware Horizon View Composer 服務和 vCenter Server 執行個體之間必須有一對一對應。View Composer 服務僅能搭配一個 vCenter Server 執行個體運作。vCenter Server 執行個體僅能與一個 VMware Horizon View Composer 服務相關聯。

初始部署 Horizon 7 後，您可以將 VMware Horizon View Composer 服務移轉到新主機，以支援不斷成長或變更的 Horizon 7 部署。您可以在 Horizon Administrator 中編輯 View Composer 初始設定，但必須執行其他步驟才能確保移轉成功。請參閱將 View Composer 移轉至其他機器。

必要條件

- 確認您已在 Active Directory 中建立具有權限的使用者，該使用者能從包含連結複製的 Active Directory 網域中新增和移除虛擬機器。請參閱建立 View Composer AD 作業的使用者帳戶。
- 確認您已將 Horizon 7 設定為連線到 vCenter Server。若要這樣做，您必須完成「新增 vCenter Server」精靈的「vCenter Server 資訊」頁面。請參閱將 vCenter Server 執行個體新增到 Horizon 7。
- 確認此 VMware Horizon View Composer 服務尚未設定為連線到其他 vCenter Server 執行個體。

程序

1 在 Horizon Administrator 中，完成「新增 vCenter Server」精靈的「vCenter Server 資訊」頁面。

   a 選取 **View 組態 > 伺服器**。

   b 在 **vCenter Server** 索引標籤中，按一下**新增**，然後提供 vCenter Server 設定。

2 在「View Composer 設定」頁面上，如果不使用 View Composer，請選取**不使用 View Composer**。

   如果選取**不使用 View Composer**，其他 View Composer 設定就會變成非作用中。按**下一步**時，「新增 vCenter Server」精靈會顯示「儲存設定」頁面。不會顯示「View Composer 網域」頁面。

3 如果使用 View Composer，請選取 View Composer 主機的位置。

選項	說明
View Composer 安裝在與 vCenter Server 相同的主機上。	a 選取 **View Composer 與 vCenter Server 並行安裝**。 b 確定連接埠號碼與在 vCenter Server 上安裝 VMware Horizon View Composer 服務時所指定的連接埠相同。預設連接埠編號是 18443。
View Composer 安裝在本身的另一個主機上。	a 選取**獨立 View Composer Server**。 b 在「View Composer Server 位址」文字方塊中，輸入 View Composer 主機的完整網域名稱 (FQDN)。 c 輸入 View Composer 使用者的名稱。 例如：`domain.com\user` 或 `user@domain.com` d 輸入 View Composer 使用者的密碼。 e 確定連接埠號碼與安裝 VMware Horizon View Composer 服務時所指定的連接埠相同。預設連接埠編號是 18443。

4 按**下一步**以顯示「View Composer 網域」頁面。

後續步驟

設定 View Composer 網域。

- 如果已使用簽署的 TLS 憑證設定 View Composer 執行個體，且連線伺服器信任根憑證，「新增 vCenter Server」精靈便會顯示「View Composer 網域」頁面。
- 如果已使用預設憑證設定 View Composer 執行個體，則必須先決定是否接受現有憑證的指紋。請參閱接受預設 TLS 憑證的指紋。

設定 View Composer 網域

您必須設定 View Composer 部署連結複製桌面所在的 Active Directory 網域。您可以為 View Composer 設定多個網域。當您首次將 vCenter Server 和 View Composer 設定新增至 View 之後，您可以在 Horizon Administrator 中編輯 vCenter Server 執行個體，以新增更多 View Composer 網域。

必要條件

- Active Directory 管理員必須建立 AD 作業的 View Composer 使用者。此網域使用者必須擁有在包含連結複製的 Active Directory 網域中新增和移除虛擬機器的權限。如需此使用者所需權限的相關資訊，請參閱建立 View Composer AD 作業的使用者帳戶。
- 在 Horizon Administrator 中，確認您已完成「新增 vCenter Server」精靈中的「vCenter Server 資訊」和「View Composer 設定」頁面。

程序

1 在 [View Composer 網域] 頁面上，按一下**新增**以新增 AD 作業的 View Composer 使用者帳戶資訊。

2 輸入 Active Directory 網域的網域名稱。

例如：`domain.com`

3 輸入網域使用者名稱，包括 View Composer 使用者的網域名稱。

例如：**domain.com\admin**

4 輸入帳戶密碼。

5 按一下**確定**。

6 若要新增在您部署連結複製集區與所在其他 Active Directory 網域內具有權限的網域使用者帳戶，請重複前述步驟。

7 按一下**下一步**以顯示「儲存設定」頁面。

後續步驟

啟用虛擬機器磁碟空間回收，並為 Horizon 7 設定 View 儲存加速器。

允許 vSphere 回收連結複製虛擬機器中的磁碟空間

在 vSphere 5.1 和更新版本中，您可以啟用 Horizon 7 的磁碟空間回收功能。在 vSphere 5.1 中啟動後，Horizon 7 會以有效磁碟格式建立連結複製虛擬機器，讓 ESXi 主機能夠回收連結複製中未使用的磁碟空間，以減少連結複製所需的總儲存空間。

當使用者與連結複製桌面互動時，複製的作業系統磁碟會增加，最後會佔用到幾乎和完整複製桌面一樣的磁碟空間。磁碟空間回收可減少作業系統磁碟的大小，使您不必重新整理或重新撰寫連結複製。只要開啟虛擬機器電源，系統就會在使用者與遠端桌面平台互動的同時回收空間。

當部署無法利用登出後重新整理之類可節省儲存空間的策略時，磁碟空間回收功能就特別有用。例如，知識工作者在專用遠端桌面平台上安裝使用者應用程式後，若重新整理或重新撰寫遠端桌面平台，可能會遺失其個人應用程式。有了磁碟空間回收功能，Horizon 7 可以將連結複製一直維持在接近第一次佈建時初始的較少空間。

此功能具有兩個元件：空間效率高的磁碟格式和空間回收作業。

在 vSphere 5.1 或更新版本的環境中，若父虛擬機器是虛擬硬體版本 9 或更新版本，則不管是否啟用空間回收作業，Horizon 7 都會以空間效率高的作業系統磁碟來建立連結複製。

若要啟用空間回收作業，您必須使用 Horizon Administrator 來啟用 vCenter Server 的空間回收功能，並回收個別桌面平台集區的虛擬機器磁碟空間。在 vCenter Server 的空間回收設定中，您可以對所有受 vCenter Server 執行個體管理的桌面平台集區選擇停用此功能。停用 vCenter Server 的該功能會覆寫桌面平台集區層級的設定。

下列指導方針適用於空間回收功能：

- 僅在連結複製中空間高效的作業系統磁碟上運作。
- 不會影響 View Composer 持續性磁碟。
- 它僅適用於 vSphere 5.1 或更新版本，且僅限虛擬硬體版本 9 或更新版本的虛擬機器。
- 不會在完整複製桌面上運作。
- 會在含 SCSI 控制器的虛擬機器上運作。不支援 IDE 控制器。

集區中包含具有空間高效磁碟的虛擬機器時，不支援原生 NFS 快照技術 (VAAI)。

必要條件

- 確認您的 vCenter Server 與 ESXi 主機 (包括叢集中的所有 ESXi 主機) 均為包含 ESXi 5.1 下載修補程式 ESXi510-201212001 的 5.1 版或更新版本。

程序

1 在 Horizon Administrator 中，請先完成「新增 vCenter Server」精靈頁面，再完成「儲存設定」頁面。

   a 選取 **View 組態 > 伺服器**。

   b 在 **vCenter Server** 索引標籤上，按一下**新增**。

   c 完成「vCenter Server 資訊」、「View Composer 設定」，以及「View Composer 網域」頁面。

2 在「儲存設定」頁面上，確認已選取**啟用空間回收**。

   如果您是在執行 Horizon 7 5.2 或更新版本的全新安裝，則依預設將選取空間回收功能。如果您是在從 Horizon 7 5.1 或更早版本升級為 Horizon 7 5.2 或更新版本，則必須選取**啟用空間回收**。

後續步驟

在「儲存設定」頁面上，設定 View 儲存加速器。

若要在 Horizon 7 中完成磁碟空間回收的設定，請為桌面平台集區設定空間回收功能。

設定 vCenter Server 的 View 儲存加速器

在 vSphere 5.1 和更新版本中，您可以設定 ESXi 主機以快取虛擬機器磁碟資料。這項稱為 View 儲存加速器的功能使用 ESXi 主機的內容型讀取快取 (CBRC) 功能。當許多虛擬機器啟動或立即執行防毒掃描時會發生 I/O 風暴，而 View 儲存加速器可提升 I/O 風暴期間的 Horizon 7 效能。管理員或使用者頻繁載入應用程式或資料時，這項功能也相當實用。主機可以從快取讀取共同的資料區塊，而不是從儲存系統一再讀取整個作業系統或應用程式。

View 儲存加速器會透過減少開機風暴期間的 IOPS 數目，降低儲存陣列的需要，讓您使用較少的儲存 I/O 頻寬支援您的 Horizon 7 部署。

您可以在 Horizon Administrator 的 vCenter Server 精靈中選取「View 儲存加速器」設定，以啟用 ESXi 主機上的快取，如本程序所述。

請確定也已針對個別桌面平台集區設定 View 儲存加速器。若要在桌面平台集區上運作，必須針對 vCenter Server 及個別桌面平台集區啟用 View 儲存加速器。

桌面平台集區預設啟用 View 儲存加速器。此功能可在建立或編輯集區時停用或啟用。最佳方法是在初次建立桌面平台集區時啟用此功能。如果透過編輯現有集區啟用此功能，則必須確保新複本及其摘要磁碟會在佈建連結複製之前建立。可以透過將集區重新撰寫為新的快照或將集區重新平衡為新的資料存放區來建立新複本。僅當桌面平台集區中的虛擬機器關閉電源後，才能針對這些虛擬機器設定摘要檔案。

對於包含連結複製的桌面平台集區，以及包含完整虛擬機器的集區，您可以啟用 View 儲存加速器。

針對 View 儲存加速器啟用的集區不支援原生 NFS 快照技術 (VAAI)。

現在 View 儲存加速器適用於使用 Horizon 7 複本分層的組態，也就是複本會儲存於非連結複製所在的單獨資料存放區。雖然 View 儲存加速器與 Horizon 7 複本分層搭配使用的效能優點在實質上並不顯著，但是將複本儲存於單獨資料存放區，可能會實現某些與容量相關的優點。因此，這是已經過測試且受支援的組合。

重要 若您想使用此功能，而您使用多個共用部分 ESXi 主機的 Horizon 7 網繭，則您必須針對共用 ESXi 主機上的所有集區啟用 Horizon Storage Accelerator 功能。在多個網繭中擁有不一致的設定可能導致共用 ESXi 主機上的虛擬機器不穩定。

必要條件

- 確認 vCenter Server 及 ESXi 主機為 5.1 版或更新版本。

  在 ESXi 叢集中，確認所有主機皆為 5.1 版或更新版本。
- 確認已在 vCenter Server 中將**主機 > 組態 > 進階設定**權限指派給 vCenter Server 使用者。

  請參閱《Horizon 7 安裝》文件中說明 vCenter Server 使用者所需的 Horizon 7 及 View Composer 權限的主題。

程序

1 在 Horizon Administrator 中，請先完成「新增 vCenter Server」精靈頁面，再完成「儲存設定」頁面。

  a 選取 **View 組態 > 伺服器**。

  b 在 **vCenter Server** 索引標籤上，按一下**新增**。

  c 完成「vCenter Server 資訊」、「View Composer 設定」，以及「View Composer 網域」頁面。

2 在「儲存設定」頁面上，確認已選取**啟用 View 儲存加速器**核取方塊。

  此核取方塊預設為選取狀態。

3 指定預設的主機快取大小。

  預設快取大小會套用至此 vCenter Server 執行個體所管理的所有 ESXi 主機。

  預設值為 1,024MB。快取大小必須介於 100MB 和 2,048MB 之間。

4 若要針對個別 ESXi 主機指定不同的快取大小，請選取 ESXi 主機並按一下**編輯快取大小**。

  a 在「主機快取」對話方塊中，選取**覆寫預設的主機快取大小**。

  b 輸入**主機快取大小**值 (介於 100MB 和 2,048MB 之間) 並按一下**確定**。

5 在「儲存設定」頁面上，按**下一步**。

6 按一下**完成**以便將 vCenter Server、View Composer 及「儲存設定」新增至 Horizon 7。

後續步驟

設定用戶端工作階段和連線的設定。請參閱進行用戶端工作階段的設定。

若要完成 Horizon 7 中的 View 儲存加速器設定，請設定桌面平台集區的 View 儲存加速器。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈設定桌面平台集區的 View 儲存加速器〉。

vCenter Server 和 View Composer 的並行作業限制

當您將 vCenter Server 新增至 Horizon 7 或編輯 vCenter Server 設定時，您可以設定數個選項以設定 vCenter Server 和 View Composer 所執行的並行作業數目上限。

您要在「vCenter Server 資訊」頁面上的「進階設定」面板中設定這些選項。

表 2-1. vCenter Server 和 View Composer 的並行作業限制

設定	說明
vCenter 並行佈建作業上限	決定連線伺服器在此 vCenter Server 執行個體中佈建和刪除完整虛擬機器所能提出的並行要求數目上限。 預設值為 20。 此設定僅適用於完整虛擬機器。
並行電源作業數量上限	決定在此 vCenter Server 執行個體中，由連線伺服器管理的虛擬機器上可執行的並行電源作業 (啟動、關閉、暫止等) 數目上限。 預設值為 50。 如需計算此設定之值的指導方針，請參閱設定並行電源作業率以支援遠端桌面平台登入風暴。 此設定適用於完整虛擬機器和連結複製。
並行 View Composer 維護作業上限	決定可在此 View Composer 執行個體管理之連結複製上執行的並行 View Composer 重新整理、重新撰寫及重新平衡作業數目上限。 預設值為 12。 必須先登出具有使用中工作階段的遠端桌面平台，才能開始維護作業。如果維護作業一開始您就強制使用者登出，則遠端桌面平台上需要登出的並行作業數目上限為設定值的一半。例如，如果您將此設定設為 24 並強制使用者登出，則遠端桌面平台上需要登出的並行作業數目上限為 12。 此設定僅適用於連結複製。
並行 View Composer 佈建作業上限	決定可在此 View Composer 執行個體管理之連結複製上執行的並行建立與刪除作業數目上限。 預設值為 8。 此設定僅適用於連結複製。

設定並行電源作業率以支援遠端桌面平台登入風暴

並行電源作業上限設定會管理可發生在 vCenter Server 執行個體中的遠端桌面平台虛擬機器上的並行電源作業上限。依預設，此限制設定為 50。您可以在多名使用者同時登入桌面時，變更此值以支援尖峰電源開啟速率。

最佳做法是採用試驗階段，確定此設定的正確值為何。如需規劃指導方針，請參閱《Horizon 7 架構規劃》文件中的〈架構設計元素和規劃指導方針〉。

所需要的並行電源作業數量，是以桌面開啟電源的尖峰速率，以及桌面開啟電源、開機、可供連線所需要的時間量為基礎。一般來說，電源作業限制的建議值是桌面啟動時所需要的總時間，乘上尖峰電源開啟速率。

例如，桌面平均需要兩到三分鐘時間來啟動。因此，並行電源作業限制應該是尖峰電源開啟速率的 3 倍。預設值 50 預計每分鐘可支援 16 個桌面的尖峰電源開啟速率。

系統最久會等候 5 分鐘讓桌面平台啟動。如果啟動時間超出此一限制，可能會發生其他錯誤。為保守起見，您可以將並行電源作業限制設定為尖峰電源開啟速率的 5 倍。依照此一保守作法，預設值 50 每分鐘可支援 10 個桌面的尖峰電源開啟速率。

登入以及後續的桌面電源開啟作業，通常會以一般分佈方式在特定的時間範圍內發生。您可以假設電源開啟發生在時間範圍中間，以大致估計尖峰電源開啟速率，在此時間範圍中，約有 40% 的電源開啟作業發生在 1/6 的時間範圍中。例如，假設使用者在上午 8:00 和上午 9:00 之間登入，時間範圍為一小時，而 40% 的登入發生在上午 8:25 和上午 8:35 的 10 分鐘之間。如果有 2,000 名使用者，其中 20% 關閉桌面電源，則 400 個桌面電源開啟作業當中，有 40% 發生在這 10 分鐘之間。尖峰電源開啟速率為每分鐘 16 個桌面。

接受預設 TLS 憑證的指紋

當您將 vCenter Server 和 View Composer 執行個體新增至 Horizon 7 時，您必須確認用於 vCenter Server 和 View Composer 執行個體的 TLS 憑證是有效的，並受到連線伺服器的信任。如果與 vCenter Server 和 View Composer 一起安裝的預設憑證仍然在適當的位置，您必須決定是否接受這些憑證的指紋。

如果使用 CA 簽署的憑證設定 vCenter Server 或 View Composer 執行個體，且根憑證受到連線伺服器的信任，則您不需要接受憑證指紋。您不需要執行任何動作。

如果您將預設憑證取代為 CA 簽署的憑證，但連線伺服器不信任根憑證，則您必須決定是否接受憑證指紋。指紋是憑證的密碼編譯雜湊。指紋用來快速判斷所呈現的憑證是否與另一個憑證 (例如先前接受的憑證) 相同。

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

如需關於設定 TLS 憑證的詳細資料，請參閱《Horizon 7 安裝》文件中的〈設定 View Server 的 TLS 憑證〉。

您可以使用「新增 vCenter Server」精靈，先在 Horizon Administrator 中新增 vCenter Server 和 View Composer。如果憑證不受信任，而且您不接受指紋，您將無法新增 vCenter Server 和 View Composer。

新增這些伺服器之後，您可以在「編輯 vCenter Server」對話方塊中重新設定這些伺服器。

備註 當您從舊版升級，且 vCenter Server 或 View Composer 憑證不受信任時，或您將受信任的憑證取代成不受信任的憑證時，您也必須接受憑證指紋。

在 Horizon Administrator 儀表板上，vCenter Server 或 View Composer 圖示會變成紅色，而且會出現 [偵測到無效的憑證] 對話方塊。在 Horizon Administrator 中，按一下 **View 組態 > 伺服器**，然後編輯與 View Composer 服務相關聯的 vCenter Server 項目。然後，在 vCenter Server 設定中按一下**編輯**，並遵循提示來確認並接受自我簽署憑證。

同樣地，您可以在 Horizon Administrator 中設定由連線伺服器執行個體所使用的 SAML 驗證器。如果 SAML 伺服器憑證不受連線伺服器信任，則您必須決定是否接受憑證指紋。如果您不接受指紋，則無法在 Horizon 7 中設定 SAML 驗證器。設定 SAML 驗證器之後，您可以在 [編輯連線伺服器] 對話方塊中重新設定該驗證器。

程序

1 當 Horizon Administrator 顯示 [偵測到無效的憑證] 對話方塊時，按一下**檢視憑證**。

2 在「憑證資訊」視窗中檢查憑證指紋。

3 檢查針對 vCenter Server 或 View Composer 執行個體設定的憑證指紋。

   a 在 vCenter Server 或 View Composer 主機上，啟動 MMC 嵌入式管理單元，並開啟「Windows 憑證存放區」。

   b 導覽至 vCenter Server 或 View Composer 憑證。

   c 按一下「憑證詳細資料」索引標籤來顯示憑證指紋。

   同樣地，檢查 SAML 驗證器的憑證指紋。如果適當，請在 SAML 驗證器主機上採取上述步驟。

4 請確認「憑證資訊」視窗中的指紋符合 vCenter Server 或 View Composer 執行個體的指紋。

   同樣地，請確認 SAML 驗證器的指紋相符。

5 決定是否接受憑證指紋。

選項	說明
指紋相符。	按一下**接受**可使用預設憑證。
指紋不符。	按一下**拒絕**。 疑難排解不相符的憑證。例如，您可能已經為 vCenter Server 或 View Composer 提供不正確的 IP 位址。

從 Horizon 7 中移除 vCenter Server 執行個體

您可以移除 Horizon 7 與 vCenter Server 執行個體之間的連線。當您這麼做後，Horizon 7 便不再管理在該 vCenter Server 執行個體中建立的虛擬機器。

必要條件

刪除所有與 vCenter Server 執行個體相關的虛擬機器。如需關於刪除虛擬機器的詳細資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈刪除桌面平台集區〉。

程序

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

2 在 **vCenter Server** 索引標籤中，選取 vCenter Server 執行個體。

3 按一下**移除**。

   對話方塊會警告您 Horizon 7 將不再具有由此 vCenter Server 執行個體所管理之虛擬機器的存取權。

4 按一下**確定**。

Horizon 7 再也無法存取在 vCenter Server 執行個體中建立的虛擬機器。

從 Horizon 7 移除 View Composer

您可以將 Horizon 7 和與 vCenter Server 執行個體相關聯的 VMware Horizon View Composer 服務之間的連線移除。

在您停用 View Composer 的連線前，必須將 Horizon 7 中所有由 View Composer 建立的連結複製虛擬機器移除。如果仍存在任何相關聯的連結複製，則 Horizon 7 會阻止您移除 View Composer。在停用 View Composer 連線後，Horizon 7 便無法佈建或管理新的連結複製。

程序

1 移除由 View Composer 建立的連結複製桌面平台集區。

   a 在 Horizon Administrator 中，選取**類別目錄 > 桌面平台集區**。

   b 選取連結複製桌面平台集區，再按一下**刪除**。

   對話方塊警告，您將永久刪除 Horizon 7 中的連結複製桌面平台集區。如果連結複製虛擬機器設為具有持續性磁碟，則您可以中斷連結或刪除持續性磁碟。

   c 按一下**確定**。

   虛擬機器隨即自 vCenter Server 中刪除。此外，還會移除相關聯的 View Composer 資料庫項目及 View Composer 建立的複本。

   d 為每個由 View Composer 建立的連結複製桌面平台集區重複這些步驟。

2 選取 **View 組態 > 伺服器**。

3 在 **vCenter Server** 索引標籤中，選取與 View Composer 相關聯的 vCenter Server 執行個體。

4 按一下**編輯**。

5 在 [View Composer Server 設定] 下，按一下**編輯**，選取**不使用 View Composer**，並按一下**確定**。

您再也無法在此 vCenter Server 執行個體中建立連結複製桌面平台集區，但可以繼續在 vCenter Server 執行個體中建立與管理完整虛擬機器桌面平台集區。

後續步驟

如果您打算將 View Composer 安裝在另一個主機，並將 Horizon 7 重新設定為連線至新的 VMware Horizon View Composer 服務，則必須執行某些額外的步驟。請參閱移轉無連結複製虛擬機器的 View Composer。

有衝突的 vCenter Server 唯一識別碼

如果您的環境中已設定多個 vCenter Server 執行個體，則嘗試新增執行個體時可能會失敗，因為有衝突的唯一識別碼。

問題

您嘗試將 vCenter Server 執行個體新增至 Horizon 7，但是新 vCenter Server 執行個體的唯一識別碼與現有執行個體衝突。

原因

兩個 vCenter Server 執行個體無法使用相同的唯一識別碼。依預設，vCenter Server 的唯一識別碼隨機產生，但您可以編輯。

解決方案

1 在 vSphere Client 中，按一下**管理 > vCenter Server 設定 > 執行階段設定**。

2 輸入新的唯一識別碼，然後按一下**確定**。

如需有關編輯 vCenter Server 唯一識別碼值的詳細資料，請參閱 vSphere 文件。

備份 Horizon 連線伺服器

完成 Horizon 連線伺服器的初始組態後，應該排程 Horizon 7 及 View Composer 組態資料的定期備份。

如需備份和還原 Horizon 7 組態的相關資訊，請參閱備份和還原 Horizon 7 組態資料。

進行用戶端工作階段的設定

您進行的全域設定，會影響連線伺服器執行個體或複寫群組所管理的用戶端工作階段和連線。您可以設定工作階段逾時長度，顯示預先登入和警告訊息，以及設定安全相關的用戶端連線選項。

為用戶端工作階段和連線設定選項

您可以設定全域設定，以確定用戶端工作階段和連線的運作方式。

全域設定不限於單一連線伺服器執行個體。它們會影響所有由獨立的連線伺服器執行個體，或複寫的執行個體群組所管理的用戶端工作階段。

您也可以將連線伺服器執行個體設定為在 Horizon 用戶端和遠端桌面平台之間，使用直接、非通道連線。請參閱 設定安全通道和 PCoIP 安全閘道 以取得設定直接連線的相關資訊。

必要條件

自行熟悉全域設定。請參閱用戶端工作階段的全域設定與用戶端工作階段和連線的全域安全性設定。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 全域設定**。

2 選擇要設定一般設定還是安全設定。

選項	說明
一般全域設定	在 [一般] 窗格中按一下**編輯**。
全域安全設定	在「安全」窗格中，按一下**編輯**。

3 設定全域設定。

4 按一下**確定**。

後續步驟

您可以變更在安裝期間所提供的資料復原密碼。請參閱變更資料復原密碼。

變更資料復原密碼

您安裝連線伺服器 5.1 版或更新版本時，需要提供資料復原密碼。安裝完成後，您可以在 View Administrator 中變更此密碼。從備份復原 View LDAP 組態時，需要此密碼。

備份連線伺服器時，系統會將 View LDAP 組態匯出為加密的 LDIF 資料。若要還原加密的備份 Horizon 7 組態，您必須提供資料復原密碼。

密碼必須包含 1 至 128 個字元。請遵循組織的最佳做法，產生安全密碼。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 全域設定**。

2 在「安全性」窗格中，按一下**變更資料復原密碼**。

3 輸入兩次新密碼。

4 (選擇性) 輸入密碼提醒。

備註 排程將備份的 Horizon 7 組態資料時，也可變更資料復原密碼。請參閱排程 Horizon 7 組態備份。

後續步驟

當您使用 `vdmimport` 公用程式還原備份 Horizon 7 組態時，請提供新密碼。

用戶端工作階段的全域設定

一般全域設定可決定工作階段逾時長度、SSO 啟用與逾時限制、Horizon Administrator 中的狀態更新、是否顯示預先登入與警告訊息、Horizon Administrator 是否將 Windows Server 視為遠端桌面平台的受支援作業系統，以及其他設定。

對下表中任何設定所做的變更會立即生效。無需重新啟動 Horizon 7 連線伺服器或 Horizon Client。

表 2-2. 用戶端工作階段的一般全域設定

設定	說明
View Administrator 工作階段逾時	決定 Horizon Administrator 工作階段會持續閒置多久的時間，工作階段才會逾時。 **重要** 若將 Horizon Administrator 工作階段逾時分鐘設為很大的數字，會增加未經授權使用 Horizon Administrator 的風險。若您允許讓工作階段持續閒置很長的時間，請小心。 依預設，Horizon Administrator 工作階段逾時為 30 分鐘。您可以將工作階段逾時設為 1 到 4320 分鐘 (72 小時)。
強制中斷使用者連線	自使用者登入 Horizon 7 起經過指定的分鐘數後，將中斷與所有桌面平台及應用程式的連線。將會同時中斷所有桌面平台和應用程式的連線，無論使用者在何時開啟它們。 針對不支援應用程式遠端處理的用戶端，如果此設定的值為**永不**或大於 1200 分鐘，則會套用逾時值上限，即 1200 分鐘。 預設值為 **600 分鐘後**。

表 2-2. 用戶端工作階段的一般全域設定 (續)

設定	說明
Single sign-on (SSO)	如果 SSO 已啟用，則 Horizon 7 會快取使用者認證，以便使用者能夠不提供登入遠端 Windows 工作階段的認證即可啟動遠端桌面平台或應用程式。預設為**已啟用**。 如果您計劃使用 Horizon 7 或更新版本中引進的 True SSO 功能，則必須啟用 SSO。透過 True SSO，如果使用者採用 Active Directory 認證以外的其他驗證形式登入，True SSO 功能會在使用者登入 VMware Identity Manager 後，產生要使用的短期憑證 (而非快取的認證)。 **備註** 如果從 Horizon Client 啟動桌面平台，並且該桌面平台已根據安全性原則由使用者或 Windows 鎖定，則桌面平台正在執行 Horizon 7 Agent 6.0 或更新版本或 Horizon Agent 7.0 或更新版本時，Horizon 7 連線伺服器會捨棄使用者的 SSO 認證。使用者必須提供用於啟動新桌面平台或新應用程式的登入認證，或者重新連線至任何中斷連線的桌面平台或應用程式。若要再次啟用 SSO，使用者必須從 Horizon 7 連線伺服器中斷連線或結束 Horizon Client，然後重新連線至 Horizon 7 連線伺服器。但是，如果從 Workspace ONE 或 VMware Identity Manager 啟動桌面平台，並且該桌面平台已鎖定，則不會捨棄 SSO 認證。
支援應用程式的用戶端。 **如果使用者停止使用鍵盤與滑鼠，請中斷與應用程式的連線並捨棄 SSO 認證：**	在用戶端裝置上無鍵盤或滑鼠活動時保護應用程式工作階段。如果設定為 **...分鐘後**，則 Horizon 7 將在無使用者活動進行後的指定分鐘數後中斷與所有應用程式的連線，並捨棄 SSO 認證。不會中斷與桌面平台工作階段的連線。使用者必須再次登入才能與中斷連線的應用程式重新連線，或者啟動新的桌面平台或應用程式。 此設定也適用於 True SSO 功能。捨棄 SSO 認證後，會提示使用者輸入 Active Directory 認證。如果使用者未使用 AD 認證登入 VMware Identity Manager 且不知道該輸入什麼 AD 認證，則可登出 VMware Identity Manager 並再次登入以存取其遠端桌面平台和應用程式。 **重要** 使用者必須瞭解，應用程式和桌面平台開啟時，由於此逾時已中斷連線其應用程式，所以其桌面平台會保持連線狀態。使用者不得依賴此逾時來保護其桌面平台。 如果設定為**永不**，Horizon 7 將永不會因為使用者無活動而中斷應用程式連線或捨棄 SSO 認證。 預設值為**永不**。
其他用戶端。 **捨棄 SSO 認證:**	指定分鐘數後捨棄 SSO 認證。此設定適用於不支援應用程式遠端處理的用戶端。如果設定為 **...分鐘後**，使用者必須在其登入 Horizon 7 起的指定分鐘數後再次登入才能連線到桌面平台，無論用戶端裝置上發生任何使用者活動。 如果設為**永不**，則使用者關閉 Horizon Client 或者達到**強制中斷使用者連線**逾時 (以發生者為準) 之後，Horizon 7 才會儲存 SSO 認證。 預設值為 **15 分鐘後**。
啟用自動狀態更新	決定狀態更新是否每隔幾分鐘就顯示於 Horizon Administrator 左上角的全域狀態窗格。Horizon Administrator 的儀表板頁面也會每隔幾分鐘更新。 依預設，此設定未啟用。
顯示預先登入訊息	當 Horizon Client 使用者登入時會顯示免責聲明或其他訊息。 在 [全域設定] 對話方塊的文字方塊中，輸入您的資訊或指示。 若不要顯示訊息，請將此核取方塊保持為未選取。

表 2-2. 用戶端工作階段的一般全域設定 (續)

設定	說明
強制登出前顯示警告	當因排程或立即更新，例如桌面平台重新整理作業即將開始，而強制使用者登出時，顯示警告訊息。此設定也可決定在警告訊息顯示多久的時間後，便將使用者登出。 勾選取方塊即可顯示警告訊息。 輸入在顯示警告後與將使用者登出前等待的分鐘數。預設值為 5 分鐘。 輸入您的警告訊息。您可以使用預設訊息： `您的桌面已排程進行重要更新，將於 5 分鐘後關閉。請立即儲存任何未儲存的工作。`
啟用 Windows Server 桌面平台	決定您是否可以選取當做桌面平台使用的可用 Windows Server 2008 R2 和 Windows Server 2012 R2 機器。啟用此設定時，Horizon Administrator 會顯示所有可用的 Windows Server 機器，其中包括安裝 Horizon 7 Server 元件所在的機器。 **備註** Horizon Agent 軟體無法與其他任何 Horizon 7 server 軟體元件 (包括安全伺服器、Horizon 7 連線伺服器或 Horizon 7 Composer) 共存於相同的虛擬或實體機器上。
當 HTML Access 的索引標籤關閉時，清理認證	當使用者在 HTML Access 用戶端中關閉連線至遠端桌面平台或應用程式的索引標籤，或關閉連線至桌面平台和應用程式選擇頁面的索引標籤時，會從快取移除使用者的認證。 啟用此設定時，在下列 HTML Access 用戶端案例中，Horizon 7 也會從快取移除認證： ■ 使用者重新整理桌面平台和應用程式選擇頁面或遠端工作階段頁面。 ■ 伺服器出示自我簽署憑證、使用者啟動遠端桌面平台或應用程式，以及使用者在安全性警告出現時接受憑證。 ■ 使用者在包含遠端工作階段的索引標籤中執行 URI 命令。 停用此設定時，認證會留在快取中。此功能依預設為停用。 **備註** 此功能可在 Horizon 7 (7.0.2 版) 和更新版本中使用。
Mirage 伺服器組態	可讓您使用格式 **`mirage://`*`server-name`*`:`*`port`*** 或 **`mirages://`*`server-name`*`:`*`port`*** 來指定 Mirage 伺服器的 URL。其中 *server-name* 為完整網域名稱。若不指定連接埠號碼，則會使用預設連接埠號碼 8000。 **備註** 透過在桌面平台集區設定中指定 Mirage 伺服器，您可以覆寫此全域設定。 可以在 Horizon Administrator 中指定 Mirage 伺服器，也可以在安裝 Mirage 用戶端時指定 Mirage 伺服器。若要瞭解哪些版本的 Mirage 支援在 Horizon Administrator 中指定伺服器，請參閱 Mirage 說明文件，網址為 https://www.vmware.com/support/pubs/mirage_pubs.html。
在用戶端使用者介面中隱藏伺服器資訊	啟用此安全性設定，可在 Horizon Client 4.4 或更新版本中隱藏伺服器 URL 資訊。

表 2-2. 用戶端工作階段的一般全域設定 (續)

設定	說明
在用戶端使用者介面中隱藏網域清單	啟用此安全性設定，可在 Horizon Client 4.4 或更新版本中隱藏網域下拉式功能表。 當使用者登入啟用了**在用戶端使用者介面中隱藏網域清單**全域設定的連線伺服器執行個體時，Horizon Client 中的網域下拉式功能表會是隱藏的，使用者必須在 Horizon Client 的**使用者名稱**文字方塊中提供網域資訊。例如，使用者必須以格式 `domain\username` 或 `username@domain` 輸入其使用者名稱。 **重要** 如果您啟用**在用戶端使用者介面中隱藏網域清單**設定，並且為連線伺服器執行個體選取了雙因素驗證 (RSA SecureID 或 RADIUS)，則請不要強制執行 Windows 使用者名稱比對。強制執行 Windows 使用者名稱比對會防止使用者在使用者名稱文字方塊中輸入網域資訊，導致登入一律會失敗。如果有單一使用者網域，則此功能不適用 Horizon Client 5.0 版及更新版本。 **重要** 如需關於此設定的安全性和可用性含意的詳細資訊，請參閱《Horizon 7 安全性》文件。
傳送網域清單	選取此核取方塊，可允許連線伺服器在驗證使用者之前將網域名稱清單傳送至用戶端。 **重要** 如需關於此設定的安全性和可用性含意的詳細資訊，請參閱《Horizon 7 安全性》文件。

用戶端工作階段和連線的全域安全性設定

全域安全性設定可決定在發生中斷後是否重新驗證用戶端、是否啟用訊息安全性模式，以及 IPSec 是否用於安全伺服器連線。

所有與 Horizon 7 之間的 Horizon Client 連線和 Horizon Administrator 連線都需要 TLS。如果您的 Horizon 7 部署使用負載平衡器或其他面向用戶端的中繼伺服器，您可以將 TLS 卸載到這些負載平衡器或中繼伺服器，然後在個別連線伺服器執行個體與安全伺服器上設定非 TLS 連線。請參閱將 TLS 連線卸載至中繼伺服器。

表 2-3. 用戶端工作階段和連線的全域安全性設定

設定	說明
網路中斷後重新驗證安全通道連線	決定當 Horizon Client 使用安全通道連線至遠端桌面平台時，在網路中斷後是否必須重新驗證使用者認證。 當您選取此設定時，如果安全通道連線中斷，則 Horizon Client 需要使用者先重新驗證，才能重新連線。 此設定可加強安全性。例如，如果筆記型電腦遭竊，並移到不同網路上，使用者便無法在未輸入認證的情況下自動取得遠端桌面平台的存取權。 若未選取此設定，則用戶端會重新連線到遠端桌面平台，不需要使用者重新驗證。 此設定在未使用安全通道的情況下無效。
訊息安全模式	決定用於在元件之間傳送 JMS 訊息的安全性機制 ■ 將模式設定為**已啟用**後，會簽署與驗證 Horizon 7 元件之間傳遞的 JMS 訊息。 ■ 當將模式設定為**增強**時，安全性會透過相互驗證的 TLS 來提供。JMS 連線以及對 JMS 的存取控制主題。 如需詳細資料，請參閱 Horizon 7 元件的訊息安全模式。 對於全新安裝，預設將訊息安全模式設定為**增強**。如果從舊版升級，則會保留舊版中使用的設定。

表 2-3. 用戶端工作階段和連線的全域安全性設定 (續)

設定	說明
增強安全性狀態 (唯讀)	當**訊息安全模式**由**已啟用**變更為**增強**時顯示的唯讀欄位。因為變更是分階段進行，此欄位會顯示在不同階段時的進度： ■ **等待訊息匯流排重新啟動**是第一階段。在您手動重新啟動網繭中的所有連線伺服器執行個體或網繭中所有連線伺服器主機上的 VMware Horizon 訊息匯流排元件服務之前，會一直顯示此狀態。 ■ **正在擱置增強**是下一個狀態。重新啟動所有 Horizon 訊息匯流排元件服務之後，系統會開始針對所有桌面平台和安全伺服器將訊息安全模式變更為**增強**。 ■ **增強**是最後的狀態，表示所有元件目前正在使用**增強**訊息安全模式。 也可以使用 `vdmutil` 命令列公用程式來監控進度。請參閱使用 vdmutil 公用程式設定 JMS 訊息安全模式。
使用 IPSec 進行安全伺服器連線	決定安全伺服器與連線伺服器執行個體之間是否使用網際網路通訊協定安全性 (IPSec) 連線。 依預設，安全伺服器連線的安全連線 (使用 IPSec) 為啟用。

備註　如果您從舊版 Horizon 7 升級到 View 5.1 或更新版本，則**用戶端連線需要 SSL** 全域設定會在 Horizon Administrator 中顯示，但只有在您升級前此設定已在 Horizon 7 組態中停用時才會顯示。由於與 Horizon 7 之間的所有 Horizon Client 連線及 Horizon Administrator 連線都需要 TLS，因此此設定不會在 Horizon 7 5.1 或更新版本的全新安裝中顯示，且此設定如果已在先前的 Horizon 7 組態中啟用，則在升級後不會顯示。

升級後，如果您不啟用**用戶端連線需要 SSL** 設定，則從 Horizon 用戶端的 HTTPS 連線會失敗，除非這些連線會連線到已設為使用 HTTP 進行前進連線的中繼裝置。請參閱將 TLS 連線卸載至中繼伺服器。

Horizon 7 元件的訊息安全模式

您可以設定訊息安全模式，以指定 JMS 訊息在通過 Horizon 7 元件時所使用的安全機制。

下表顯示可設定訊息安全模式的選項。若要設定選項，請在 [全域設定] 對話方塊視窗的**訊息安全模式**清單中選取該選項。

表 2-4. 訊息安全模式選項

選項	說明
已停用	停用訊息安全模式。
混合	啟用訊息安全模式，但未強制實施。 您可以使用此模式偵測 Horizon 7 環境中早於 Horizon 7 3.0 的元件。連線伺服器產生的記錄檔包含這些元件的參考。這不是建議使用的設定。請僅在探索需要升級的元件時才使用此設定。

表 2-4. 訊息安全模式選項 (續)

選項	說明
已啟用	訊息安全模式會啟用，使用訊息簽署和加密的組合。如果簽章遺失或無效，或如果簽署簽章後修改了訊息，便會拒絕 JMS 訊息。 某些 JMS 訊息由於帶有如使用者認證的機密資訊，因此已加密。如果您使用**已啟用**設定，則也可以使用 IPSec 來加密連線伺服器執行個體之間，以及連線伺服器執行個體和安全伺服器之間的所有 JMS 訊息。 **備註** 不允許早於 3.0 版的 Horizon 7 元件與其他 Horizon 7 元件通訊。
增強	所有 JMS 連線均會使用 SSL。此外也會啟用 JMS 存取控制，讓桌面平台、安全伺服器和連線伺服器執行個體只能傳送和接收某些主題的 JMS 訊息。 早於 Horizon 6 (6.1 版) 的 Horizon 7 元件無法與連線伺服器 6.1 執行個體通訊。 **備註** 使用此模式需要在以 DMZ 為基礎的安全伺服器和其配對的連線伺服器執行個體之間開啟 TCP 連接埠 4002。

當您第一次將 Horizon 7 安裝在系統上時，訊息安全模式會設為**增強**。如果您從舊版升級 Horizon 7，訊息安全模式會保持不變更其現有設定。

重要 如果您打算將升級的 Horizon 7 環境從**已啟用**變更為**增強**，您必須先將所有連線伺服器執行個體、安全伺服器和 Horizon 7 桌面平台升級到 Horizon 6 (6.1 版) 或更新版本。在將設定變更為**增強**之後，新設定會分階段生效。

1 您必須在網繭中的所有連線伺服器主機上手動重新啟動 VMware Horizon View 訊息匯流排元件服務，或重新啟動連線伺服器執行個體。

2 在服務重新啟動之後，連線伺服器執行個體會在所有桌面平台和安全伺服器上重新設定訊息安全模式，將模式變更為**增強**。

3 若要在 Horizon Administrator 中監控進度，請前往 **View 組態 > 全域設定**。

   在**安全性**索引標籤上，當所有元件均已變更為 [增強] 模式時，**增強安全性狀態**項目將會顯示**增強**。

   此外，您可以使用 `vdmutil` 命令列公用程式來監控進度。請參閱使用 vdmutil 公用程式設定 JMS 訊息安全模式。

早於 Horizon 6 (6.1 版) 的 Horizon 7 元件無法與使用增強模式的連線伺服器 6.1 執行個體通訊。

如果您計劃將使用中 Horizon 7 環境從**已停用**變更為**已啟用**，或從**已啟用**變更為**已停用**，則進行最後變更前，請先短暫變更為**混合**模式。例如，如果目前模式為**已停用**，請先變更為**混合**模式一天，再變更為**已啟用**。在**混合**模式中，系統會將簽署附加至訊息但不驗證，這可讓訊息的變更在整個環境傳播。

使用 vdmutil 公用程式設定 JMS 訊息安全模式

您可以使用 `vdmutil` 命令列介面設定和管理在 Horizon 7 元件之間傳遞 JMS 訊息時所使用的安全機制。

公用程式的語法和位置

`vdmutil` 命令可以執行與舊版 Horizon 7 隨附的 `lmvutil` 命令相同的作業。此外，`vdmutil` 命令具有選項，可決定使用的訊息安全模式以及監控將所有 Horizon 7 元件變更為增強模式的進度。在 Windows 命令提示字元中使用 `vdmutil` 命令的下列格式。

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

可使用的其他選項視命令選項而定。此主題著重於訊息安全模式的選項。如需與 Cloud Pod 架構相關的其他選項，請參閱《在 Horizon 7 中管理 Cloud Pod 架構》文件。

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。

驗證

您必須以具有管理員角色的使用者身分執行命令。您可以使用 Horizon Administrator，將管理員角色指派給使用者。請參閱第 6 章 設定角色型委派管理。

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。

表 2-5. vdmutil 命令驗證選項

選項	說明
--authAs	Horizon 7 管理員使用者的名稱。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 7 管理員使用者的完整網域名稱。
--authPassword	在 --authAs 選項中指定的 Horizon 7 管理員使用者的密碼。輸入 **"*"** 而非密碼會使 vdmutil 命令提示輸入密碼，並且不會在命令列的命令歷程記錄中保留敏感的密碼。

您必須使用驗證選項搭配除 --help 和 --verbose 之外的所有 vdmutil 命令選項。

特定於 JMS 訊息安全模式的選項

下表僅列出與檢視、設定或監控 JMS 訊息安全模式相關的 vdmutil 命令列選項。如需可搭配特定選項使用的引數清單，請使用 --help 命令列選項。

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。

表 2-6. vdmutil 命令選項

選項	說明
--activatePendingConnectionServerCertificates	針對本機網繭中的連線伺服器執行個體啟用擱置安全憑證。
--countPendingMsgSecStatus	計算導致無法轉換為增強模式或從增強模式轉換的機器數目。
--createPendingConnectionServerCertificates	針對本機網繭中的連線伺服器執行個體建立新的擱置安全憑證。
--getMsgSecLevel	取得本機網繭的增強訊息安全狀態。此狀態與針對 Horizon 7 環境中的所有元件將 JMS 訊息安全模式從**已啟用**變更為**增強**的處理程序有關。
--getMsgSecMode	取得本機網繭的訊息安全模式。
--help	列出 vdmutil 命令選項。您也可以針對特定命令使用 --help，例如 --setMsgSecMode --help。
--listMsgBusSecStatus	列出本機網繭中所有連線伺服器的訊息匯流排安全狀態。
--listPendingMsgSecStatus	列出導致無法轉換為增強模式或從增強模式轉換的機器。預設限制為 25 個項目。

表 2-6. vdmutil 命令選項 (續)

選項	說明
--setMsgSecMode	設定本機網繭的訊息安全模式。
--verbose	啟用詳細記錄。您可以將此選項新增至任何其他選項，以取得詳細的命令輸出。vdmutil 命令會寫入到標準輸出。

設定安全通道和 PCoIP 安全閘道

啟用安全通道時，當使用者連線至遠端桌面平台時，Horizon Client 就會與 View 連線伺服器或安全伺服器主機建立第二個 HTTPS 連線。

啟用 PCoIP 安全閘道時，當使用者連線至具有 PCoIP 顯示通訊協定的遠端桌面平台時，Horizon Client 就會與連線伺服器或安全伺服器主機建立進一步的安全連線。

備註　透過 Horizon 6 (6.2 版) 及更新版本，您可以使用 Unified Access Gateway 應用裝置 (而非安全伺服器) 來對 Horizon 6 Server 和桌面平台進行安全的外部存取。如果使用 Unified Access Gateway 應用裝置，您必須停用連線伺服器執行個體上的安全閘道，並在 Unified Access Gateway 應用裝置上啟用這些閘道。如需詳細資訊，請參閱《部署及設定 Unified Access Gateway》。

未啟用安全通道或 PCoIP 安全閘道時，則會直接在用戶端系統和遠端桌面平台虛擬機器之間建立工作階段，而略過連線伺服器或安全伺服器主機。這種連線類型稱為直接連線。

重要　對外部用戶端提供安全連線的一般網路組態包括安全伺服器。若要使用 Horizon Administrator 來啟用或停用安全伺服器上的安全通道或 PCoIP 安全閘道，您必須編輯與安全伺服器配對的連線伺服器執行個體。

在外部用戶端直接連線至連線伺服器主機的網路組態中，您可以在 Horizon Administrator 中編輯該連線伺服器執行個體，以啟用或停用安全通道和 PCoIP 安全閘道。

必要條件

- 如果您打算啟用 PCoIP 安全閘道，請確認連線伺服器執行個體和配對的安全伺服器均為 Horizon 7 4.6 或更新版本。
- 如果連線伺服器執行個體上已啟用 PCoIP 安全閘道，則將安全伺服器與其配對時，請確認安全伺服器為 Horizon 7 4.6 或更新版本。

程序

1. 在 Horizon Administrator 中，選取 **View 組態 > 伺服器**。
2. 在**連線伺服器**索引標籤上，選取連線伺服器執行個體，然後按一下**編輯**。
3. 設定如何使用安全通道。

選項	說明
啟用安全通道	選取**使用安全通道連線到機器**。
停用安全通道	取消選取**使用安全通道連線到機器**。

預設為啟用安全通道。

4 設定如何使用 PCoIP 安全閘道。

選項	說明
啟用 PCoIP 安全閘道	選取**使用 PCoIP 安全閘道與機器進行 PCoIP 連線**
停用 PCoIP 安全閘道	取消選取**使用 PCoIP 安全閘道與機器進行 PCoIP 連線**

預設為停用 PCoIP 安全閘道。

5 按一下**確定**儲存變更。

設定 Blast 安全閘道

在 Horizon Administrator 中，可透過 HTML Access 或使用 VMware Blast 顯示通訊協定的用戶端連線，來設定使用 Blast 安全閘道安全存取遠端桌面平台和應用程式。

Blast 安全閘道包含 Blast Extreme Adaptive Transport (BEAT) 網路功能，它會根據網路情況 (例如不同的速度和封包遺失) 進行動態調整。

- Blast 安全閘道僅在 Unified Access Gateway 應用裝置上執行時，才支援 BEAT 網路功能。
- 連線至 Unified Access Gateway 應用裝置 3.3 版或更新版本時，可以在 TCP 連接埠 8443 和 UDP 連接埠 8443 (適用於 BEAT) 上並行處理使用 IPv4 的 Horizon Client 和使用 IPv6 的 Horizon Client。
- 使用一般網路狀況的 Horizon Client，則必須連線至連線伺服器 (已停用 BSG)、安全伺服器 (已停用 BSG)，或高於 2.8 版的 Unified Access Gateway 應用裝置。如果 Horizon Client 使用一般網路狀況來連線至連線伺服器 (已啟用 BSG)、安全伺服器 (已啟用 BSG)，或低於 2.8 版的 Unified Access Gateway 應用裝置，則用戶端會自動感應網路狀況，並回復為 TCP 網路功能。
- 使用網路狀況極差的 Horizon Client 必須連線至 2.9 版或更新版本的 Unified Access Gateway 應用裝置 (已啟用 UDP 通道伺服器)。如果 Horizon Client 使用極差的網路狀況來連線至連線伺服器 (已啟用 BSG)、安全伺服器 (已啟用 BSG)，或低於 2.8 版的 Unified Access Gateway 應用裝置，則用戶端會自動感應網路狀況，並回復為 TCP 網路功能。
- 如果 Horizon Client 使用極差的網路狀況連線至連線伺服器 (BSG 已停用)、安全伺服器 (BSG 已停用)，2.9 版或更新版本的 Unified Access Gateway 應用裝置 (未啟用 UDP 通道伺服器)，或 2.8 版的 Unified Access Gateway 應用裝置，則用戶端會自動感應網路狀況，並回復為一般網路狀況。

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

備註 您也可以使用 Unified Access Gateway 應用裝置 (而非安全伺服器) 從外部安全存取 Horizon 7 伺服器和桌面平台。如果使用 Unified Access Gateway 應用裝置，您必須停用連線伺服器執行個體上的安全閘道，並在 Unified Access Gateway 應用裝置上啟用這些閘道。如需詳細資訊，請參閱《部署及設定 Unified Access Gateway》。

當 Blast 安全閘道未啟用時，用戶端裝置和用戶端網頁瀏覽器會使用 VMware Blast Extreme 通訊協定直接連線到遠端桌面平台虛擬機器和應用程式，而略過 Blast 安全閘道。

重要 對外部使用者提供安全連線的一般網路組態包括安全伺服器。若要啟用或停用安全伺服器上的 Blast 安全閘道，您必須編輯與安全伺服器配對的連線伺服器執行個體。如果外部使用者直接連線至連線伺服器主機，那麼若要啟用或停用 Blast 安全閘道，則需編輯該連線伺服器執行個體。

必要條件

如果使用者使用 VMware Identity Manager 來選取遠端桌面平台，請確認 VMware Identity Manager 已安裝並設定為與連線伺服器搭配使用，且該連線伺服器已與 SAML 2.0 驗證伺服器配對。

程序

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

2 在**連線伺服器**索引標籤上，選取連線伺服器執行個體，然後按一下**編輯**。

3 設定如何使用 Blast 安全閘道。

選項	說明
啟用 Blast 安全閘道	選取**使用 Blast 安全閘道，以透過 Blast 連線至機器**
為 HTML Access 啟用 Blast 安全閘道	選取**僅將 Blast 安全閘道用於對機器的 HTML Access Blast 連線**
停用 Blast 安全閘道	選取**不使用 Blast 安全閘道**

Blast 安全閘道預設為啟用。

4 按一下**確定**儲存變更。

將 TLS 連線卸載至中繼伺服器

Horizon Client 必須使用 HTTPS 連線到 Horizon 7。如果您的 Horizon Client 連線至負載平衡器或其他將連線傳遞至連線伺服器執行個體或安全伺服器的中繼伺服器，則您可以將 TLS 卸載至中繼伺服器。

將 TLS 卸載伺服器的憑證匯入 Horizon 7 Server

如果您將 TLS 連線卸載至中繼伺服器，您必須將中繼伺服器的憑證匯入至連線至中繼伺服器的連線伺服器執行個體或安全伺服器。同一個 TLS 伺服器憑證必須位於正在卸載的中繼伺服器，以及連線至中繼伺服器的已卸載 Horizon 7 Server 上。

如果您要部署安全伺服器，則中繼伺服器以及連線至該伺服器的安全伺服器必須具有相同的 TLS 憑證。您不必在與安全伺服器配對的連線伺服器執行個體上安裝同一個 TLS 憑證，也請勿直接連線至中繼伺服器。

如果您不想部署安全伺服器，或您的網路環境混合了某些安全伺服器與某些面向外部的連線伺服器執行個體，則中繼伺服器及任何與其連線的連線伺服器執行個體必須具有相同的 TLS 憑證。

如果中繼伺服器的憑證未安裝在連線伺服器執行個體或安全伺服器上，用戶端便無法驗證與 Horizon 7 之間的連線。在此情況下，Horizon 7 Server 傳送的憑證指紋與 Horizon Client 所連線的中繼伺服器上的憑證不相符。

請勿將負載平衡與 TLS 卸載混淆。前者的需求適用於任何設定為提供 TLS 卸載的裝置，包括某些類型的負載平衡器。然而，單純的負載平衡不需要在裝置之間複製憑證。

如需將憑證匯入 Horizon 7 Server 的相關資訊，請參閱《Horizon 7 安裝》文件中的〈將簽署的伺服器憑證匯入 Windows 憑證存放區〉。

設定 Horizon 7 Server 外部 URL 以將用戶端指向 TLS 卸載伺服器

如果將 TLS 卸載至中繼伺服器，並且 Horizon Client 裝置使用安全通道與 Horizon 7 連線，您必須將安全通道外部 URL 設定為可供用戶端存取中繼伺服器的位址。

您可以在連線伺服器執行個體，或是與中繼伺服器連線的安全伺服器上，設定外部 URL 設定。

如果您部署安全伺服器，安全伺服器需要外部 URL，而與安全伺服器配對的連線伺服器執行個體則不需要。

如果您沒有部署安全伺服器，或者您擁有含部分安全伺服器和部分面向外部的連線伺服器執行個體的混合型網路環境，則連線至中繼伺服器的任何連線伺服器執行個體均需要外部 URL。

備註 您無法從 PCoIP 安全閘道 (PSG) 或 Blast 安全閘道卸載 TLS 連線。PCoIP 外部 URL 和 Blast 安全閘道外部 URL 必須允許用戶端連線至主控 PSG 和 Blast 安全閘道的電腦。除非您計劃需要中繼伺服器和 Horizon 7 伺服器之間的 TLS 連線，否則請勿重設 PCoIP 外部 URL 和 Blast 外部 URL 指向中繼伺服器。

如需設定外部 URL 的相關資訊，請參閱《Horizon 7 安裝》文件中的〈設定 PCoIP 安全閘道和通道連線的外部 URL〉。

允許來自中繼伺服器的 HTTP 連線

將 TLS 卸載至中繼伺服器時，您可以設定連線伺服器執行個體或安全伺服器，以允許從面向用戶端的中繼裝置進行 HTTP 連線。中繼裝置必須接受 HTTPS，才能進行 Horizon Client 連線。

若要允許 Horizon 7 Server 與中繼裝置之間的 HTTP 連線，您必須在每個允許 HTTP 連線的連線伺服器執行個體及安全伺服器上設定 `locked.properties` 檔案。

雖然允許 Horizon 7 Server 與中繼裝置之間的 HTTP 連線，但是您無法在 Horizon 7 中停用 TLS。Horizon 7 Server 將繼續接受 HTTPS 連線及 HTTP 連線。

備註 如果 Horizon Client 使用智慧卡驗證，用戶端必須向連線伺服器或安全伺服器直接進行 HTTPS 連線。智慧卡驗證不支援 TLS 卸載。

程序

1 在連線伺服器或安全伺服器主機上的 TLS/SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*install_directory*\VMware\VMware View\Server\SSLgateway\conf\locked.properties

2 若要設定 Horizon 7 Server 的通訊協定，請新增 `serverProtocol` 屬性，並將其設定為 `http`。

必須以小寫輸入值 `http`。

3 (選擇性) 新增屬性，設定 Horizon 7 Server 上非預設的 HTTP 接聽連接埠及網路介面。

- 若要變更為 80 以外的 HTTP 接聽連接埠，請將 `serverPortNonTLS` 設為設定中繼裝置連接的其他連接埠號碼。
- 如果 Horizon 7 Server 有多個網路介面，而且您想要伺服器僅接聽一個介面的 HTTP 連線，請將 `serverHostNonTLS` 設定為該網路介面的 IP 位址。

4 儲存 `locked.properties` 檔案。

5 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

範例： locked.properties 檔案

此檔案允許 Horizon 7 Server 的非 TLS HTTP 連線。Horizon 7 伺服器面向用戶端網路介面的 IP 位址為 10.20.30.40。伺服器會使用預設連接埠 80 來接聽 HTTP 連線。值 `http` 必須為小寫。

```
serverProtocol=http
serverHostNonTLS=10.20.30.40
```

設定 Horizon 連線伺服器或安全伺服器主機的閘道位置

依預設，Horizon 連線伺服器執行個體會將閘道位置設定為 `Internal`，而安全伺服器會將閘道位置設為 `External`。您可以藉由設定 `locked.properties` 檔案中的 `gatewayLocation` 內容來變更預設閘道位置。

閘道位置會決定遠端桌面平台中 `ViewClient_Broker_GatewayLocation` 登錄機碼的值。您可以將此值搭配智慧原則使用，建立只會在使用者從公司網路內部或外部連線到遠端桌面平台時生效的原則。如需更多資訊，請參閱《在 Horizon 7 中設定遠端桌面平台功能》文件中的〈使用智慧原則〉。

程序

1 在 Horizon 連線伺服器或安全伺服器主機上的 TLS/SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties

`locked.properties` 檔案中的屬性區分大小寫。

2 將下行內容新增到 `locked.properties` 檔案：

`gatewayLocation=`*value*

value 可為 `External` 或 `Internal`。`External` 代表閘道可供公司網路外部的使用者使用。`Internal` 代表閘道只可供公司網路內部的使用者使用。

例如：`gatewayLocation=External`

3 儲存 `locked.properties` 檔案。

4 重新啟動 VMware Horizon 連線伺服器服務或 VMware Horizon 安全伺服器服務，讓您的變更生效。

停用或啟用 Horizon 連線伺服器

您可以停用連線伺服器執行個體，以防止使用者登入其虛擬或已發佈的桌面平台和應用程式。停用執行個體之後，您可以再次將其啟用。

停用連線伺服器執行個體時，目前已登入桌面平台和應用程式的使用者不會受到影響。

您的 Horizon 7 部署會決定停用執行個體時使用者受影響的程度。

- 如果這是單一、獨立式連線伺服器執行個體，則使用者無法登入其桌面平台或應用程式。他們無法連線至連線伺服器。
- 如果這是複寫的連線伺服器執行個體，您的網路拓撲會決定是否將使用者路由至其他複寫的執行個體。如果使用者可以存取其他執行個體，他們就可以登入其桌面平台和應用程式。

程序

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

2 在**連線伺服器**索引標籤上，選取連線伺服器執行個體。

3 按一下**停用**。

您可以按一下**啟用**以再次啟用執行個體。

編輯外部 URL

您可以使用 Horizon Administrator 編輯連線伺服器執行個體與安全伺服器的外部 URL。

依預設，只有位於相同網路內的通道用戶端，才能與連線伺服器或安全伺服器主機連線。在您網路外執行的通道用戶端必須使用用戶端可解析的 URL，才能連線至連線伺服器或安全伺服器主機。

當使用者透過 PCoIP 顯示通訊協定連線至遠端桌面平台時，Horizon Client 會進一步連線至連線伺服器或安全伺服器主機上的 PCoIP 安全閘道。若要使用 PCoIP 安全閘道，用戶端系統必須具有 IP 位址存取權，該 IP 位址允許用戶端連絡連線伺服器或安全伺服器主機。您會在 PCoIP 外部 URL 中指定此 IP 位址。

第三個 URL 可讓使用者透過 Blast 安全閘道進行安全連線。

安全通道外部 URL、PCoIP 外部 URL 和 Blast 外部 URL 必須是用戶端系統用來連線此主機的位址。

備註 若安全伺服器尚未升級至連線伺服器 4.5 或更新版本，則您無法編輯該伺服器的外部 URL。

程序

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

選項	動作
View 連線伺服器執行個體	在**連線伺服器**索引標籤上選取連線伺服器執行個體，然後按一下**編輯**。
安全伺服器	在**安全伺服器**索引標籤上選取安全伺服器，然後按一下**編輯**。

2 在**外部 URL** 文字方塊中輸入安全通道外部 URL。

URL 必須包含通訊協定、用戶端可解析的主機名稱與連接埠號碼。

例如：https://view.example.com:443

備註 當無法解析主機名稱時，如果您具有連線伺服器執行個體或安全伺服器的存取權，則可以使用 IP 位址。然而，您連絡的主機將不符合為連線伺服器執行個體或安全伺服器設定的 SSL 憑證，造成存取遭封鎖或存取時不安全。

3 在 **PCoIP 外部 URL** 文字方塊中輸入 PCoIP 安全閘道外部 URL。

指定 PCoIP 外部 URL 作為 IP 位址，且連接埠號碼為 4172。請不要包含通訊協定名稱。

例如：`10.20.30.40:4172`

URL 必須包含 IP 位址與連接埠號碼，用戶端系統可用於連絡此安全伺服器或連線伺服器執行個體。

4 在 **Blast 外部 URL** 文字方塊中輸入 Blast 安全閘道外部 URL。

URL 必須包含 HTTPS 通訊協定、用戶端可解析的主機名稱，以及連接埠號碼。

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

依預設，URL 包含安全通道外部 URL 的 FQDN 和預設連接埠號碼 8443。URL 必須包含用戶端系統可用來連線此主機的 FQDN 和連接埠號碼。

5 確認此對話方塊中的所有位址皆允許用戶端系統連線此主機。

6 按一下**確定**儲存變更。

外部 URL 隨即更新。不需要重新啟動連線伺服器服務或安全伺服器服務，即可讓變更生效。

加入或退出客戶經驗計畫

當您安裝具有新組態的連線伺服器時，您可以選擇參與客戶經驗改進計劃。如果您在安裝後參與的心意改變了，您可以使用 Horizon Administrator 加入或退出計劃。

如果您參與計劃，VMware 便會收集您的匿名部署資料，以改進 VMware 對使用者需求的回應。不會收集任何可用於識別貴組織的資料。

若要檢閱所收集資料的欄位清單，包括要匿名的欄位，請參閱#unique_44。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 產品授權及使用**。

2 在客戶經驗計劃窗格中，按一下**編輯設定**。

3 透過選取或取消選取**將匿名資料傳送到 VMware** 核取方塊，可決定要參與或退出計劃。

4 (選擇性) 如果您參與，您可以選擇地理位置、業務類型，以及您組織中的員工數目。

5 按一下**確定**。

View LDAP 目錄

View LDAP 是所有 Horizon 7 組態資訊的資料存放庫。View LDAP 是內嵌的輕量型目錄存取通訊協定 (LDAP) 目錄，會隨連線伺服器安裝一併提供。

View LDAP 包含 Horizon 7 所使用的標準 LDAP 目錄元件。

- Horizon 7 架構定義
- 目錄資訊樹狀結構 (DIT) 定義
- 存取控制清單 (ACL)

View LDAP 包含代表 Horizon 7 物件的目錄項目。

- 遠端桌面平台項目，代表每一個可存取的桌面平台。每一個項目都包含 Active Directory 中經授權使用桌面平台的 Windows 使用者和群組的外部安全性主體 (FSP) 項目參照。
- 遠端桌面平台集區項目，代表一併管理的多個桌面平台
- 虛擬機器項目，代表每個遠端桌面平台的 vCenter Server 虛擬機器
- Horizon 7 元件項目，用於儲存組態設定

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

備註 安全伺服器執行個體不包含 View LDAP 目錄。

LDAP 複寫

當您安裝連線伺服器的複寫執行個體時，Horizon 7 會從現有的連線伺服器執行個體複製 View LDAP 組態資料。複寫群組中所有連線伺服器執行個體上的 View LDAP 組態資料會保持一致。在某個執行個體上進行變更時，更新的資訊會複製到其他執行個體。

如果複寫的執行個體失敗，群組中的其他執行個體會繼續運作。當失敗的執行個體恢復活動時，其組態會以中斷期間所做的變更進行更新。在 Horizon 7 及更新版本上，系統每 15 分鐘會執行一次複寫狀態檢查，以判斷每個執行個體是否可與複寫群組中的其他伺服器通訊，以及每個執行個體是否可從群組中的其他伺服器擷取 LDAP 更新。

您可使用 Horizon Administrator 中的儀表板來檢查複寫狀態。如果儀表板中有任何連線伺服器執行個體的圖示是紅色，請按一下圖示，查看複寫狀態。複寫可能會因為下列任何原因而無法正常運作：

- 防火牆可能封鎖了通訊
- VMware VDMDS 服務在連線伺服器執行個體上可能會停止。
- VMware VDMDS DSA 選項可能封鎖了複寫功能
- 發生網路問題

依預設，複寫檢查會每隔 15 分鐘發生一次。您可以在連線伺服器執行個體上使用 ADSI Edit 來變更間隔。若要設定分鐘數，請連線至 **DC=vdi,DC=vmware,DC=int** 並編輯 **CN=Common,OU=Global,OU=Properties** 物件上的 **pae-ReplicationStatusDataExpiryInMins** 屬性。

pae-ReplicationStatusDataExpiryInMins 屬性值應該介於 10 分鐘和 1440 分鐘 (一天) 之間。如果屬性值小於 10 分鐘，Horizon 7 會將它視為 10 分鐘。如果屬性值大於 1440，Horizon 7 會將它視為 1440 分鐘。

設定智慧卡驗證

3

若要加強安全性，您可以設定連線伺服器執行個體或安全伺服器，讓使用者和管理員可以使用智慧卡來驗證。

智慧卡是一塊內含電腦晶片的小塑料卡片。該晶片就像一部微型電腦，其中包含了安全的資料儲存區，包括私密金鑰和公開金鑰憑證。美國國防部使用的一種智慧卡稱為「通用存取卡」(CAC)。

利用智慧卡驗證，使用者或管理員就可以將智慧卡插入連接至用戶端電腦的智慧卡讀卡機，並輸入 PIN。智慧卡驗證提供雙因素驗證，一是驗證個人擁有的 (智慧卡)，一是驗證個人知道的 (PIN)。

如需實作智慧卡驗證的硬體和軟體需求的相關資訊，請參閱《Horizon 7 安裝》文件。Microsoft TechNet 網站上可取得針對 Windows 系統規劃和實作智慧卡驗證的詳細資訊。

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

本章節討論下列主題：

以智慧卡登入

當使用者或管理員將智慧卡插入智慧卡讀卡機時，如果用戶端作業系統為 Windows，智慧卡上的使用者憑證會複製到用戶端系統上的本機憑證存放區。本機憑證存放區中的憑證可供在用戶端電腦上執行的所有應用程式使用，包括 Horizon Client。

當使用者或管理員起始連線至設定為智慧卡驗證的連線伺服器執行個體或安全伺服器時，連線伺服器執行個體或安全伺服器會將受信任的憑證授權機構 (CA) 清單傳送至用戶端系統。用戶端系統會對照可用的使用者憑證檢查受信任的 CA 清單，選取適當的憑證，再提示使用者或管理員輸入智慧卡 PIN。如果有多個有效的使用者憑證，用戶端系統會提示使用者或管理員選取一個憑證。

用戶端系統會將使用者憑證傳送至連線伺服器執行個體或安全伺服器，它會檢查憑證的信任與有效期間，來驗證憑證。一般而言，使用者和管理員可成功驗證其使用者憑證是否已簽署且有效。如果已設定憑證撤銷檢查，已撤銷使用者憑證的使用者或管理員則無法進行驗證。

在部分環境中，一個使用者的智慧卡憑證可以對應至多個 Active Directory 網域使用者帳戶。一個使用者可能有多個具備管理員權限的帳戶，並且在智慧卡登入期間需要在 [使用者名稱提示] 欄位中指定要使用的帳戶。若要讓使用者名稱提示欄位出現在 Horizon Client 登入對話方塊中，管理員必須在 Horizon Administrator 中為連線伺服器執行個體啟用智慧卡使用者名稱提示功能。然後於智慧卡登入期間，智慧卡使用者即可以在 [使用者名稱提示] 欄位中輸入使用者名稱或 UPN。

如果您的環境使用 Unified Access Gateway 應用裝置進行外部安全存取，您必須將 Unified Access Gateway 應用裝置設定為支援智慧卡使用者名稱提示功能。智慧卡使用者名稱提示功能僅支援 Unified Access Gateway 2.7.2 版及更新版本。如需在 Unified Access Gateway 應用裝置中啟用智慧卡使用者名稱提示功能的相關資訊，請參閱《部署及設定 Unified Access Gateway》文件。

Horizon Client 不支援透過智慧卡驗證切換顯示通訊協定。在 Horizon Client 中透過智慧卡驗證後，若要變更顯示通訊協定，則使用者必須登出並再次登入。

在 Horizon Connection Server 上設定智慧卡驗證

若要設定智慧卡驗證，您必須取得根憑證，並將其新增至伺服器信任存放區檔案中，接著修改連線伺服器組態屬性，並進行智慧卡驗證設定。視您的特定環境而定，可能需要執行其他步驟。

程序

1 取得憑證授權機構憑證

針對您使用者和管理員提供的智慧卡上的所有受信任使用者憑證，您必須取得所有適用的 CA (憑證授權機構) 憑證。這些憑證包含根憑證，而且，如果使用者的智慧卡憑證是由中繼憑證授權機構發給的，則可以包含中繼憑證。

2 從 Windows 取得 CA 憑證

如果您具有 CA 簽署的使用者憑證或包含憑證的智慧卡，則當 Windows 信任根憑證時，可以從 Windows 匯出根憑證。若使用者憑證的發行者為中繼憑證授權單位，您可匯出該憑證。

3 將 CA 憑證新增至伺服器信任存放區檔案

您必須為所有信任的使用者和管理員將根憑證、中繼憑證或兩者新增至伺服器信任存放區檔案。連線伺服器執行個體和安全伺服器使用該資訊驗證智慧卡使用者和管理員。

4 修改 Horizon 連線伺服器組態屬性

若要啟用智慧卡驗證，您必須修改連線伺服器或安全伺服器主機的連線伺服器組態屬性。

5 在 Horizon Administrator 中進行智慧卡設定

您可以使用 Horizon Administrator 來指定設定，以容納不同的智慧卡驗證案例。

取得憑證授權機構憑證

針對您使用者和管理員提供的智慧卡上的所有受信任使用者憑證，您必須取得所有適用的 CA (憑證授權機構) 憑證。這些憑證包含根憑證，而且，如果使用者的智慧卡憑證是由中繼憑證授權機構發給的，則可以包含中繼憑證。

如果您沒有使用者和管理員所提供智慧卡上簽署憑證的 CA 根憑證或中繼憑證，您可以從 CA 簽署的使用者憑證或包含該憑證的智慧卡匯出憑證。請參閱 從 Windows 取得 CA 憑證。

程序

- 從以下其中一個來源取得 CA 憑證。
  - 執行 Microsoft 憑證服務的 Microsoft IIS 伺服器。請參閱 Microsoft TechNet 網站以取得在您組織中安裝 Microsoft IIS、發行憑證，及散佈憑證的相關資訊。
  - 信任 CA 的公用根憑證。這在已具備智慧卡基礎結構與標準化智慧卡散佈及驗證方法的環境中，是最常見的根憑證來源。

後續步驟

將根憑證、中繼憑證或兩者新增至伺服器信任存放區檔案。

從 Windows 取得 CA 憑證

如果您具有 CA 簽署的使用者憑證或包含憑證的智慧卡，則當 Windows 信任根憑證時，可以從 Windows 匯出根憑證。若使用者憑證的發行者為中繼憑證授權單位，您可匯出該憑證。

程序

1. 如果使用者憑證在智慧卡上，請將智慧卡插入讀卡機中，將使用者憑證新增至您的個人存放區。

   如果使用者憑證未出現在您的個人存放區中，請使用讀卡機軟體將使用者憑證匯出至檔案。在此程序的步驟 4 中使用此檔案。

2. 在 Internet Explorer 中，選取**工具 > 網際網路選項**。
3. 在**內容**索引標籤上，按一下**憑證**。
4. 在**個人**索引標籤上，選取您要使用的憑證，並按一下**檢視**。

   如果使用者憑證未出現在清單中，請按一下**匯入**手動從檔案匯入憑證。匯入憑證後，您便可以從清單中選取憑證。

5. 在**憑證路徑**索引標籤中，選取樹狀結構頂端的憑證，並按一下**檢視憑證**。

   如果已將使用者憑證簽署成為信任階層的一部分，則正在簽署的憑證可由另一個更高層級的憑證簽署。選取父憑證 (實際簽署使用者憑證的憑證) 作為您的根憑證。在某些情況下，發行者可能是中繼 CA。

6. 在**詳細資料**索引標籤上，按一下**複製到檔案**。

   憑證匯出精靈隨即出現。

7. 按**下一步 > 下一步**，並輸入您要匯出的檔案名稱與位置。
8. 按**下一步**將檔案儲存在指定的位置作為根憑證。

後續步驟

將 CA 憑證新增至伺服器信任存放區檔案。

將 CA 憑證新增至伺服器信任存放區檔案

您必須為所有信任的使用者和管理員將根憑證、中繼憑證或兩者新增至伺服器信任存放區檔案。連線伺服器執行個體和安全伺服器使用該資訊驗證智慧卡使用者和管理員。

必要條件

- 取得用於簽署憑證 (位於使用者或管理員出示的智慧卡上) 的根憑證或中繼憑證。請參閱取得憑證授權機構憑證與從 Windows 取得 CA 憑證。

  重要 如果使用者的智慧卡憑證是由中繼憑證授權機構發給的，則這些憑證可以包含中繼憑證。

- 確認 `keytool` 公用程式已新增至連線伺服器或安全伺服器主機上的系統路徑。如需詳細資訊，請參閱《Horizon 7 安裝》文件。

程序

1. 在連線伺服器或安全伺服器主機上，使用 `keytool` 公用程式將根憑證、中繼憑證或兩者匯入至伺服器信任存放區檔案。

   例如：

   `keytool -import -alias` *`alias`* `-file` *`root_certificate`* `-keystore` *`truststorefile.key`*

   在此命令中，*alias* 是信任存放區檔案中新項目區分大小寫的唯一名稱，*root_certificate* 是您取得或匯出的根憑證或中繼憑證，*truststorefile.key* 是將新增根憑證的目標信任存放區檔案的名稱。如果檔案不存在，將在當前目錄中建立該檔案。

   備註 `keytool` 公用程式會提示您建立信任存放區檔案的密碼。如果您日後需要將其他憑證新增至信任存放區檔案，將提示您提供此密碼。

2. 將信任存放區檔案複製到連線伺服器或安全伺服器主機上的 SSL 閘道組態資料夾。

   例如：*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\`*`truststorefile.key`*

後續步驟

修改連線伺服器組態屬性即可啟用智慧卡驗證。

修改 Horizon 連線伺服器組態屬性

若要啟用智慧卡驗證，您必須修改連線伺服器或安全伺服器主機的連線伺服器組態屬性。

必要條件

新增所有信任使用者憑證的 CA (憑證授權機構) 憑證至伺服器信任存放區檔案。這些憑證包含根憑證，而且，如果使用者的智慧卡憑證是由中繼憑證授權機構發給的，則可以包含中繼憑證。

程序

1 在連線伺服器或安全伺服器主機上的 TLS/SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties

2 將 `trustKeyfile`、`trustStoretype` 與 `useCertAuth` 屬性新增至 `locked.properties` 檔案。

a 將 `trustKeyfile` 設為您的信任存放區檔案名稱。

b 將 `trustStoretype` 設為 **`jks`**。

c 將 `useCertAuth` 設為 **`true`** 以啟用憑證驗證。

3 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

範例： locked.properties 檔案

顯示的檔案指定所有信任使用者的根憑證位於 `lonqa.key` 檔案中、將信任存放區類型設為 `jks`，並啟用憑證驗證。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
```

後續步驟

如果您為連線伺服器執行個體設定了智慧卡驗證，請在 Horizon Administrator 中設定智慧卡驗證設定。您不必為安全伺服器設定智慧卡驗證設定。在 Horizon 連線伺服器執行個體上設定的設定也適用於配對的安全伺服器。

在 Horizon Administrator 中進行智慧卡設定

您可以使用 Horizon Administrator 來指定設定，以容納不同的智慧卡驗證案例。

在連線伺服器執行個體上進行這些設定時，這些設定也會套用至配對的安全伺服器。

必要條件

- 在連線伺服器主機上修改連線伺服器組態屬性。
- 確認 Horizon 用戶端直接與連線伺服器或安全伺服器主機建立 HTTPS 連線。如果您將 TLS 卸載至中繼裝置，則不支援智慧卡驗證。

程序

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

2 在**連線伺服器**索引標籤上，選取連線伺服器執行個體並按一下**編輯**。

3 若要為遠端桌面平台和應用程式使用者設定智慧卡驗證，請執行這些步驟。

a 在**驗證**索引標籤上，從 [View 驗證] 區段中的**使用者的智慧卡驗證**下拉式功能表中選取組態選項。

選項	動作
不允許	連線伺服器執行個體上的智慧卡驗證已停用。
選用	使用者可以使用智慧卡驗證或密碼驗證連線至連線伺服器執行個體。如果智慧卡驗證失敗，使用者必須提供密碼。
必要	使用者連線至連線伺服器執行個體時，必須使用智慧卡驗證。 若必須進行智慧卡驗證，那麼使用者在連線至連線伺服器執行個體時選取了**以目前使用者身分登入**核取方塊，驗證便會失敗。這些使用者必須在登入連線伺服器時，以其智慧卡和 PIN 碼重新驗證。 **備註** 唯有 Windows 密碼驗證能夠換用智慧卡驗證。如果 SecurID 已啟用，使用者驗證時就必須同時使用 SecurID 和智慧卡驗證。

b 設定智慧卡移除原則。

若智慧卡驗證設定為**不允許**，就無法設定智慧卡移除原則。

選項	動作
使用者移除其智慧卡後就會中斷與 View 連線伺服器的連線。	選取**移除智慧卡時中斷使用者工作階段連線**核取方塊。
讓使用者在移除其智慧卡後保持與 View 連線伺服器的連線，並讓他們不需要重新驗證即可啟動新的桌面平台或應用程式工作階段。	取消選取**移除智慧卡時中斷使用者工作階段連線**核取方塊。

若是使用者在連線至連線伺服器執行個體時選取了**以目前使用者身分登入**核取方塊，則不適用於智慧卡移除原則，即使他們以智慧卡登入用戶端系統也一樣。

c 設定智慧卡使用者名稱提示功能。

若智慧卡驗證設定為**不允許**，就無法設定智慧卡使用者名稱提示功能。

選項	動作
讓使用者可使用單一智慧卡憑證來對多個使用者帳戶進行驗證。	選取**允許智慧卡使用者名稱提示**核取方塊。
讓使用者無法使用單一智慧卡憑證來對多個使用者帳戶進行驗證。	取消選取**允許智慧卡使用者名稱提示**核取方塊。

4 若要設定智慧卡驗證以使管理員登入 Horizon Administrator，請按一下**驗證**索引標籤，並從 [View 管理驗證] 區段中的**管理員的智慧卡驗證**下拉式功能表中選取組態選項。

選項	動作
不允許	連線伺服器執行個體上的智慧卡驗證已停用。
選用	管理員可以使用智慧卡驗證或密碼驗證登入 Horizon Administrator。如果智慧卡驗證失敗，管理員必須提供密碼。
必要	管理員在登入 Horizon Administrator 時，需要使用智慧卡驗證。

5 按一下**確定**。

6 重新啟動連線伺服器服務。

您必須重新啟動連線伺服器服務才能讓智慧卡設定的變更生效，有一個例外狀況。您可以將智慧卡驗證設定變更為**選用**或**必要**，而不必重新啟動連線伺服器服務。

目前登入的使用者和管理員不會受到智慧卡設定變更的影響。

後續步驟

若有必要，請準備 Active Directory 以便進行智慧卡驗證。請參閱為進行智慧卡驗證準備好 Active Directory。

確認您的智慧卡驗證組態。請參閱確認您的智慧卡驗證組態 。

在第三方解決方案上設定智慧卡驗證

負載平衡器和閘道之類的第三方解決方案可以透過傳遞包含智慧卡 X.590 憑證與加密 PIN 的 SAML 聲明，來執行智慧卡驗證。

本主題概述在憑證經由合作夥伴裝置驗證後，設定第三方解決方案以提供相關 X.590 憑證給連線伺服器的相關工作。由於此功能採用 SAML 驗證，因此其中一項工作就是在 Horizon Administrator 中建立 SAML 驗證器。

如需在 Unified Access Gateway 上設定智慧卡驗證的相關資訊，請參閱《部署及設定 Unified Access Gateway》。

程序

1 為第三方閘道或負載平衡器建立 SAML 驗證器。

請參閱在 Horizon Administrator 中設定 SAML 驗證器。

2 延長連線伺服器中繼資料的到期期限，使遠端工作階段不會在 24 小時後即終止。

請參閱在連線伺服器上變更服務提供者中繼資料的到期期限。

3 如有需要，請設定第三方裝置以使用來自連線伺服器的服務提供者中繼資料。

請參閱第三方裝置的產品說明文件。

4 在第三方裝置上設定智慧卡設定。

請參閱第三方裝置的產品說明文件。

為進行智慧卡驗證準備好 Active Directory

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

- 為智慧卡使用者新增 UPN

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

- 將根憑證新增至 Enterprise NTAuth Store

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

- 將根憑證新增至信任的根憑證授權單位

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

- 將中繼憑證新增至中繼憑證授權單位

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

為智慧卡使用者新增 UPN

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

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

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

必要條件

- 透過檢視憑證內容來取得包含在信任的 CA 的根憑證中的 SAN。
- 如果您的 Active Directory 伺服器上沒有出現 ADSI Edit 公用程式，請從 Microsoft 網站下載並安裝適當的 Windows 支援工具。

程序

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

2 在左窗格中，展開使用者所在的網域，然後按兩下 `CN=Users`。

3 在右窗格中，以滑鼠右鍵按一下使用者，然後按一下**內容**。

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

5 按一下**確定**來儲存屬性設定。

將根憑證新增至 Enterprise NTAuth Store

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

程序

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

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

CA 現在受到信任，可核發此類型的憑證。

將根憑證新增至信任的根憑證授權單位

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

程序

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

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

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

3 以滑鼠右鍵按一下**受信任的根憑證授權單位**，然後選取**匯入**。

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

5 關閉「群組原則」視窗。

網域中的所有系統現在在其受信任的根存放區中都有一份根憑證的複本。

後續步驟

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

將中繼憑證新增至中繼憑證授權單位

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

程序

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

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

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

3 以滑鼠右鍵按一下**中繼憑證授權單位**，然後選取**匯入**。

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

5 關閉「群組原則」視窗。

網域中的所有系統現在在其中繼憑證授權存放區中都有一份中繼憑證的複本。

確認您的智慧卡驗證組態

當您首次設定智慧卡驗證之後，或在智慧卡驗證無法正確運作時，應該要確認智慧卡驗證組態。

程序

- 確認每一個用戶端系統皆擁有智慧卡中介軟體、具備有效憑證的智慧卡，以及智慧卡讀卡機。對於使用者，確認他們擁有 Horizon Client。

  如需設定智慧卡軟體及硬體的相關資訊，請參閱您智慧卡廠商所提供的說明文件。

- 在每部用戶端系統上，選取**開始 > 設定 > 控制台 > 網際網路選項 > 內容 > 憑證 > 個人**，以確認憑證可供智慧卡驗證之用。

  當使用者或管理員將智慧卡插入智慧卡讀卡機時，Windows 會將憑證從智慧卡複製到使用者的電腦上。用戶端系統上的應用程式 (包括 Horizon Client) 可以使用這些憑證。

- 在連線伺服器或安全伺服器主機上的 `locked.properties` 檔案中，確認 `useCertAuth` 屬性設為 **`true`** 且拼寫正確。

  `locked.properties` 檔案位於 *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf` 中。`useCertAuth` 屬性常常拼錯成 `userCertAuth`。

- 如果您在連線伺服器執行個體上設定智慧卡驗證，請在 Horizon Administrator 中檢查智慧卡驗證設定。

  a 選取 **View 組態 > 伺服器**。

  b 在**連線伺服器**索引標籤上，選取連線伺服器執行個體並按一下**編輯**。

  c 如果您已為使用者設定智慧卡驗證，請在**驗證**索引標籤上，確認**使用者的智慧卡驗證**設為**選用**或**必要**。

  d 如果您已為管理員設定智慧卡驗證，請在**驗證**索引標籤上，確認**管理員的智慧卡驗證**設為**選用**或**必要**。

  您必須重新啟動連線伺服器服務，智慧卡設定的變更才會生效。

- 如果智慧卡使用者所在的網域不同於核發根憑證的來源網域，請確認使用者的 UPN 設為信任的 CA 的根憑證中所包含的 SAN。

  a 透過檢視憑證內容來找出包含在信任的 CA 的根憑證中的 SAN。

  b 在 Active Directory 伺服器上，選取**開始 > 系統管理工具 > Active Directory 使用者及電腦**。

  c 以滑鼠右鍵按一下**使用者**資料夾中的使用者，並選取**內容**。

  UPN 會顯示在**帳戶**索引標籤上的**使用者登入名稱**文字方塊中。

- 如果智慧卡使用者選取 PCoIP 顯示通訊協定或 VMware Blast 顯示通訊協定來連線至單一工作階段桌面平台，請確認稱為智慧卡重新導向的 View Agent 或 Horizon Agent 元件已安裝在單一使用者機器上。智慧卡功能可讓使用者透過智慧卡登入單一工作階段桌面平台。已安裝遠端桌面平台服務角色的 RDS 主機自動支援智慧卡功能，您不需要安裝該功能。

- 如需說明智慧卡驗證已啟用的訊息，請檢查連線伺服器或安全伺服器主機的 *`drive`*`:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 中的記錄檔。

使用智慧卡憑證撤銷檢查

藉由設定憑證撤銷檢查，您可以防止使用者憑證已遭撤銷的使用者使用智慧卡進行驗證。通常當使用者離開組織、遺失智慧卡，或調動部門時，就會撤銷憑證。

Horizon 7 使用「憑證撤銷清單」(CRL) 和「線上憑證狀態通訊協定」(OCSP) 來支援憑證撤銷檢查。CRL 是核發憑證的 CA 所發佈的撤銷憑證清單。OCSP 是用來取得 X.509 憑證的撤銷狀態的憑證驗證通訊協定。

您可以在連線伺服器執行個體或安全伺服器上設定憑證撤銷檢查。當連線伺服器執行個體已與安全伺服器配對時，可在安全伺服器上設定憑證撤銷檢查。必須可以從連線伺服器或安全伺服器主機存取 CA。

您可以在同一個連線伺服器執行個體或安全伺服器上設定 CRL 和 OCSP。當您設定兩種憑證撤銷檢查類型時，Horizon 7 會嘗試先使用 OCSP，如果 OCSP 失敗，再回復使用 CRL。但如果 CRL 失敗，Horizon 7 不會回復使用 OCSP。

- 透過 CRL 檢查登入

  當您設定 CRL 檢查時，Horizon 7 會建構與讀取 CRL，以判定使用者憑證的撤銷狀態。

- 登入並進行 OCSP 憑證撤銷檢查

  當您設定 OCSP 憑證撤銷檢查時，Horizon 7 會將要求傳送至 OCSP 回應者，來判定特定使用者憑證的撤銷狀態。Horizon 7 會使用 OCSP 簽署憑證來驗證它從 OCSP 回應者收到的回應是否正確。

- 設定 CRL 檢查

  設定 CRL 檢查時，Horizon 7 將讀取 CRL，決定智慧卡使用者憑證的撤銷狀態。

- 設定 OCSP 憑證撤銷檢查

  設定 CRL 憑證撤銷檢查時，Horizon 7 會將撤銷要求傳送至 OCSP 回應者，決定智慧卡使用者憑證的撤銷狀態。

- 智慧卡憑證撤銷檢查屬性

  您可以在 `locked.properties` 檔案中設定值，以啟用和設定智慧卡憑證撤銷檢查。

透過 CRL 檢查登入

當您設定 CRL 檢查時，Horizon 7 會建構與讀取 CRL，以判定使用者憑證的撤銷狀態。

如果憑證已撤銷，且智慧卡驗證為選擇性，則會出現**輸入您的使用者名稱與密碼**對話方塊，使用者必須提供密碼進行驗證。如果需要智慧卡驗證，則使用者會收到錯誤訊息，且不允許使用者進行驗證。如果 Horizon 7 無法讀取 CRL，則會發生相同的事件。

登入並進行 OCSP 憑證撤銷檢查

當您設定 OCSP 憑證撤銷檢查時，Horizon 7 會將要求傳送至 OCSP 回應者，來判定特定使用者憑證的撤銷狀態。Horizon 7 會使用 OCSP 簽署憑證來驗證它從 OCSP 回應者收到的回應是否正確。

如果使用者憑證已撤銷，且智慧卡驗證為選擇性，則會出現**輸入您的使用者名稱與密碼**對話方塊，使用者必須提供密碼進行驗證。如果需要智慧卡驗證，則使用者會收到錯誤訊息，且不允許使用者進行驗證。

如果 Horizon 7 未收到來自 OCSP 回應者的回應，或回應無效，則會退回 CRL 檢查。

設定 CRL 檢查

設定 CRL 檢查時，Horizon 7 將讀取 CRL，決定智慧卡使用者憑證的撤銷狀態。

必要條件

自行熟悉 CRL 檢查的 `locked.properties` 檔案屬性。請參閱智慧卡憑證撤銷檢查屬性。

程序

1 在連線伺服器或安全伺服器主機上的 TLS/SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties

2 將 `enableRevocationChecking` 及 `crlLocation` 屬性新增至 `locked.properties` 檔案。

a 將 `enableRevocationChecking` 設定為 **`true`** 即啟用智慧卡憑證撤銷檢查。

b 將 `crlLocation` 設定為 CRL 的位置。該值可以是 URL 或檔案路徑。

3 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

範例： locked.properties 檔案

這個顯示的檔案將啟用智慧卡驗證及智慧卡憑證撤銷檢查、設定 CRL 檢查，並指定 CRL 位置的 URL。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

設定 OCSP 憑證撤銷檢查

設定 CRL 憑證撤銷檢查時，Horizon 7 會將撤銷要求傳送至 OCSP 回應者，決定智慧卡使用者憑證的撤銷狀態。

必要條件

自行熟悉 OCSP 憑證撤銷檢查的 `locked.properties` 檔案屬性。請參閱智慧卡憑證撤銷檢查屬性。

程序

1 在連線伺服器或安全伺服器主機上的 TLS/SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

例如：*install_directory*\VMware\VMware View\Server\sslgateway\conf\locked.properties

2 將 `enableRevocationChecking`、`enableOCSP`、`ocspURL` 及 `ocspSigningCert` 屬性新增至 `locked.properties` 檔案。

a 將 `enableRevocationChecking` 設定為 **`true`** 即啟用智慧卡憑證撤銷檢查。

b 將 `enableOCSP` 設定為 **`true`** 即啟用 OCSP 憑證撤銷檢查。

c 將 `ocspURL` 設定為 OCSP 回應程式的 URL。

d 將 `ocspSigningCert` 設定為包含 OCSP 回應程式簽署憑證的檔案位置。

3 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

範例： locked.properties 檔案

這個顯示的檔案將啟用智慧卡驗證及智慧卡憑證撤銷檢查、設定 CRL 及 OCSP 憑證撤銷檢查、指定 OCSP 回應程式位置，並識別包含 OCSP 簽署憑證的檔案。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

智慧卡憑證撤銷檢查屬性

您可以在 `locked.properties` 檔案中設定值，以啟用和設定智慧卡憑證撤銷檢查。

表 3-1. 智慧卡憑證撤銷檢查的屬性 列出了憑證撤銷檢查的 `locked.properties` 檔案屬性。

表 3-1. 智慧卡憑證撤銷檢查的屬性

內容	說明
`enableRevocationChecking`	將此屬性設定為 **true** 以啟用憑證撤銷檢查。 當此屬性設定為 **false** 時，會停用憑證撤銷檢查，同時忽略其他所有的憑證撤銷檢查屬性。 預設值是 **false**。
`crlLocation`	指定 CRL 的位置，這可以是 URL 或檔案路徑。 若您不指定 URL，或指定的 URL 無效，Horizon 7 會在 `allowCertCRLs` 設定為 **true** 或是未指定時，對使用者憑證使用 CRL 清單。 如果 Horizon 7 無法存取 CRL，CRL 檢查則會失敗。
`allowCertCRLs`	當此屬性設定為 **true** 時，Horizon 7 會從使用者憑證擷取 CRL 清單。 預設值是 **true**。
`enableOCSP`	將此屬性設定為 **true** 可啟用 OCSP 憑證撤銷檢查。 預設值是 **false**。
`ocspURL`	指定 OCSP 回應程式的 URL。
`ocspResponderCert`	指定包含 OCSP 回應程式的簽署憑證的檔案。Horizon 7 會使用此憑證來驗證 OCSP 回應者的回應是否真實。
`ocspSendNonce`	當此屬性設定為 **true** 時，會臨時傳送 OCSP 要求以防止重複回應。 預設值是 **false**。
`ocspCRLFailover`	當此屬性設定為 **true** 時，Horizon 7 會在 OCSP 憑證撤銷檢查失敗時，使用 CRL 檢查。 預設值是 **true**。

設定其他使用者驗證類型

4

Horizon 7 會使用您現有的 Active Directory 基礎結構進行使用者和管理員驗證及管理。您也可以將 Horizon 7 與智慧卡以外的其他驗證形式整合，例如生物識別驗證或雙因素驗證解決方案 (例如 RSA SecurID 和 RADIUS)，以便驗證遠端桌面平台和應用程式使用者。

本章節討論下列主題：

使用雙因素驗證

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

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

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

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

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

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

- 使用雙因素驗證登入

  當使用者連線至 RSA SecurID 驗證或 RADIUS 驗證已啟用的連線伺服器執行個體時，會在 Horizon Client 中顯示一個特殊的登入對話方塊。

- 啟用 Horizon Administrator 中的雙因素驗證

  您可以修改 Horizon Administrator 中的連線伺服器設定，來啟用 RSA SecurID 驗證或 RADIUS 驗證的連線伺服器執行個體。

- 疑難排解 RSA SecurID 存取拒絕

  當 Horizon Client 與 RSA SecurID 驗證連線時，存取遭拒。

- 疑難排解 RADIUS 存取拒絕

  當 Horizon Client 與 RADIUS 雙因素驗證連線時，存取遭拒。

使用雙因素驗證登入

當使用者連線至 RSA SecurID 驗證或 RADIUS 驗證已啟用的連線伺服器執行個體時，會在 Horizon Client 中顯示一個特殊的登入對話方塊。

使用者可在特殊的登入對話方塊中輸入其 RSA SecurID 或 RADIUS 驗證使用者名稱與密碼。雙因素驗證密碼通常包含 PIN，後面跟隨著 Token 碼。

- 如果 RSA 驗證管理員需要使用者在輸入其 RSA SecurID 使用者名稱與密碼後輸入新的 RSA SecurID PIN，則會顯示 PIN 對話方塊。設定新的 PIN 後，系統會提示使用者等待下一個 Token 碼出現，再進行登入。如果 RSA 驗證管理員設為使用系統產生的 PIN，則會出現一個可確認 PIN 的對話方塊。
- 登入 Horizon 7 時，RADIUS 驗證方式與 RSA SecurID 非常相似。如果 RADIUS 伺服器會發出存取挑戰，則 Horizon Client 會顯示一個與 RSA SecurID 提示類似的對話方塊，以提示提供下一個 Token 碼。目前支援的 RADIUS 挑戰限制為提示文字輸入。任何從 RADIUS 伺服器傳出的挑戰文字都不會顯示。目前不支援較複雜的挑戰格式，例如複選與映像選擇。

  使用者在 Horizon Client 中輸入認證後，RADIUS 伺服器便可將 SMS 簡訊或電子郵件，或使用其他頻外機制的文字，連同代碼傳送到使用者手機。使用者可將此文字與代碼輸入到 Horizon Client，以完成驗證。
- 因為某些 RADIUS 供應商提供從 Active Directory 匯入使用者的功能，所以使用者會先看到要求提供 Active Directory 認證的提示，然後才會看到要求提供 RADIUS 驗證使用者名稱與密碼的提示。

啟用 Horizon Administrator 中的雙因素驗證

您可以修改 Horizon Administrator 中的連線伺服器設定，來啟用 RSA SecurID 驗證或 RADIUS 驗證的連線伺服器執行個體。

必要條件

在驗證管理員伺服器上安裝與設定雙因素驗證軟體，例如 RSA SecurID 軟體或 RADIUS 軟體。

- 對於 RSA SecurID 驗證，請從 RSA 驗證管理員匯出連線伺服器執行個體的 `sdconf.rec` 檔。請參閱 RSA 驗證管理員文件。

- 對於 RADIUS 驗證，請依照廠商的組態說明文件進行。請記下 RADIUS 伺服器的主機名稱或 IP 位址、用來接聽 RADIUS 驗證的連接埠號碼 (通常為 1812)、驗證類型 (PAP、CHAP、MS-CHAPv1 或 MS-CHAPv2) 及共用的密碼。您會在 Horizon Administrator 中輸入這些值。您可以輸入主要與次要 RADIUS 驗證器的這些值。

程序

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

2 在**連線伺服器**索引標籤上選取伺服器，並按一下**編輯**。

3 在**驗證**索引標籤上，進階驗證區段的**雙因素驗證**下拉式清單中，選取 **RSA SecureID** 或 **RADIUS**。

4 若要強制 RSA SecurID 或 RADIUS 使用者名稱符合 Active Directory 中的使用者名稱，請選取**強制執行 SecurID 及 Windows 使用者名稱比對**或**強制執行雙因素及 Windows 使用者名稱比對**。

   如果您選取此選項，則使用者必須使用相同的 RSA SecurID 或 RADIUS 使用者名稱進行 Active Directory 驗證。如果您未選取此選項，則名稱可以不同。

5 對於 RSA SecurID，請按一下**上傳檔案**，輸入 `sdconf.rec` 檔的位置，或按一下**瀏覽**搜尋檔案。

6 對於 RADIUS 驗證，請完成其餘的欄位：

   a 如果初始 RADIUS 驗證使用的 Windows 驗證會觸發 Token 碼的頻外傳輸，且此 Token 碼作為 RADIUS 挑戰的一部分，請選取**為 RADIUS 和 Windows 驗證使用相同的使用者名稱和密碼**。

      如果您選取此核取方塊，若 RADIUS 驗證使用 Windows 使用者名稱與密碼，則在 RADIUS 驗證後不會提示使用者提供 Windows 認證。使用者在 RADIUS 驗證後不必重新輸入 Windows 使用者名稱與密碼。

   b 從**驗證器**下拉式清單中，選取**建立新驗證器**並完成該頁面。

      - 將**帳戶處理連接埠**設為 **0**，但如果您要啟用 RADIUS 帳戶處理則不用如此設定。只有在您的 RADIUS 伺服器支援收集帳戶處理資料時，才將此連接埠設為非零的數字。如果 RADIUS 伺服器不支援帳戶處理訊息，且您將此連接埠設為非零的數字，則系統會傳送並忽略訊息，然後重試數次，造成驗證延遲。

        可使用帳戶處理資料，以便根據使用時間與資料向使用者收費。帳戶處理資料也可用於統計資料及一般網路監控。

      - 如果您指定領域首碼字串，則該字串傳送至 RADIUS 伺服器時會放置在使用者名稱的開頭。例如，如果在 Horizon Client 中輸入的使用者名稱為 **jdoe**，並指定領域首碼 **DOMAIN-A**，則會將使用者名稱 **DOMAIN-A\jdoe** 傳送至 RADIUS 伺服器。同樣的，如果您使用的領域尾碼 (也就是後置詞) 字串是 **@mycorp.com**，則會將使用者名稱 **jdoe@mycorp.com** 傳送至 RADIUS 伺服器。

7 按一下**確定**儲存變更。

   您不需要重新啟動連線伺服器服務。系統會自動散佈必要的組態檔，組態設定會立即生效。

當使用者開啟 Horizon Client 並驗證連線伺服器時，會提示使用者提供雙因素驗證。對於 RADIUS 驗證，登入對話方塊會顯示文字提示，其中包含您所指定的 Token 標籤。

變更 RADIUS 驗證設定會影響在組態變更後啟動的遠端桌面平台和應用程式工作階段。目前工作階段不受 RADIUS 驗證設定變更的影響。

後續步驟

如果您有複寫的連線伺服器執行個體群組，且您也要在這些執行個體上設定 RADIUS 驗證，則您可以重複使用現有的 RADIUS 驗證器組態。

疑難排解 RSA SecurID 存取拒絕

當 Horizon Client 與 RSA SecurID 驗證連線時，存取遭拒。

問題

Horizon Client 與 RSA SecurID 的連線顯示存取遭拒，而且 RSA 驗證管理員登入監視器顯示此錯誤：節點驗證失敗。

原因

RSA Agent 主機節點密碼需要重設。

解決方案

1. 在 Horizon Administrator 中，選取 **View 組態 > 伺服器**。
2. 在**連線伺服器**索引標籤上，選取連線伺服器並按一下**編輯**。
3. 在**驗證**索引標籤選取**清除節點密碼**。
4. 按一下**確定**以清除節點密碼。
5. 在執行 RSA 驗證管理員的電腦上，選取**開始 > 程式集 > RSA Security > RSA 驗證管理員主機模式**。
6. 選取**代理程式主機 > 編輯代理程式主機**。
7. 從清單中選取 **View 連線伺服器**，然後取消選取**所建立的節點密碼**核取方塊。

   每次在您編輯**所建立的節點密碼**時，此項目依預設均為選取狀態。
8. 按一下**確定**。

疑難排解 RADIUS 存取拒絕

當 Horizon Client 與 RADIUS 雙因素驗證連線時，存取遭拒。

問題

使用 RADIUS 雙因素驗證的 Horizon Client 連線顯示存取遭拒。

原因

RADIUS 沒有收到來自 RADIUS 伺服器的回覆，導致 Horizon 7 逾時。

解決方案

此一情形通常是由下列常見的組態錯誤造成：

- RADIUS 伺服器未設定為能接受連線伺服器執行個體作為 RADIUS 用戶端。每個使用 RADIUS 的連線伺服器執行個體都必須設定為 RADIUS 伺服器上的用戶端。請參閱 RADIUS 雙因素驗證產品文件。
- 連線伺服器執行個體和 RADIUS 伺服器的共用密碼值不相符。

使用 SAML 驗證

安全性聲明標記語言 (SAML) 是一種以 XML 為基礎的標準，用於說明以及交換不同安全網域之間的驗證與授權資訊。在被稱為 SAML 聲明的 XML 文件中，SAML 在身分識別提供者與服務提供者之間傳遞使用者相關資訊。

您可以使用 SAML 驗證來整合 Horizon 7 與 VMware Workspace ONE、VMware Identity Manager，或合格的第三方負載平衡器或閘道。為第三方裝置設定 SAML 時，請參閱廠商的說明文件，以取得設定 Horizon 7 以與其搭配使用的相關資訊。啟用 SSO 後，登入 VMware Identity Manager 或第三方裝置的使用者可以啟動遠端桌面平台與應用程式，而無需進行第二次登入程序。您也可以使用 SAML 驗證，在 VMware Access Point 或第三方裝置上實作智慧卡驗證。

若要委派驗證責任給 Workspace ONE、VMware Identity Manager 或第三方裝置，您必須在 Horizon 7 中建立 SAML 驗證器。SAML 驗證器包含 Horizon 7 和 Workspace ONE、VMware Identity Manager 或第三方裝置之間的信任和中繼資料交換。您可在 SAML 驗證器與連線伺服器執行個體之間建立關聯。

使用 SAML 驗證進行 VMware Identity Manager 整合

Horizon 7 與 VMware Identity Manager (舊稱 Workspace ONE) 之間的整合會使用 SAML 2.0 標準，建立單一登入 (SSO) 功能不可或缺的共同信任。啟用 SSO 後，使用 Active Directory 認證登入 VMware Identity Manager 或 Workspace ONE 的使用者可以啟動遠端桌面平台與應用程式，而無需第二次登入程序。

VMware Identity Manager 與 Horizon 7 整合後，每當使用者登入 VMware Identity Manager 並按一下桌面平台或應用程式圖示時，VMware Identity Manager 便會產生唯一的 SAML 構件。VMware Identity Manager 使用這個 SAML 構件來建立統一資源識別碼 (URI)。URI 包含桌面平台或應用程式集區所在的連線伺服器執行個體、所要啟動的桌面平台或應用程式，以及 SAML 構件的相關資訊。

VMware Identity Manager 會將 SAML 構件傳送至 Horizon Client，Horizon Client 繼而將此構件傳送至連線伺服器執行個體。連線伺服器執行個體會使用 SAML 構件從 VMware Identity Manager 擷取 SAML 判斷提示。

連線伺服器執行個體擷取 SAML 判斷提示後，將會驗證此判斷提示、解密使用者密碼，並使用解密的密碼啟動桌面平台或應用程式。

設定 VMware Identity Manager 與 Horizon 7 整合涉及使用 Horizon 7 資訊設定 VMware Identity Manager，以及將 Horizon 7 設定為委派責任以供 VMware Identity Manager 驗證。

若要委派責任給 VMware Identity Manager 以供驗證，則必須在 Horizon 7 中建立 SAML 驗證器。SAML 驗證器包含 Horizon 7 和 VMware Identity Manager 之間的信任和中繼資料交換。您可在 SAML 驗證器與連線伺服器執行個體之間建立關聯。

備註 如果您想要透過 VMware Identity Manager 提供對桌面平台與應用程式的存取，請確認您是以對 Horizon Administrator 中的根存取群組具有管理員角色的使用者身分，建立了桌面平台和應用程式集區。如果您為使用者提供的管理員角色所針對的是根存取群組之外的存取群組，則 VMware Identity Manager 將無法辨識您在 Horizon 7 中設定的 SAML 驗證器，而您也無法在 VMware Identity Manager 中設定集區。

在 Horizon Administrator 中設定 SAML 驗證器

若要從 VMware Identity Manager 啟動遠端桌面平台和應用程式，或透過第三方負載平衡器或閘道連線至遠端桌面平台和應用程式，您必須在 Horizon Administrator 中建立 SAML 驗證器。SAML 驗證器包含 Horizon 7 和用戶端所連線的裝置之間的信任和中繼資料交換。

您可在 SAML 驗證器與連線伺服器執行個體之間建立關聯。如果您的部署包含多個連線伺服器執行個體，則必須建立 SAML 驗證器與每個執行個體的關聯。

您一次可以讓一個靜態驗證器和多個動態驗證器上線。您可以設定 vIDM (動態) 和 Unified Access Gateway (靜態) 驗證器，並讓它們保持在作用中狀態。您可以透過其中一種驗證器進行連線。

您可以對連線伺服器設定多個 SAML 驗證器，且所有驗證器可同時處於作用中狀態。不過，在連線伺服器上設定的每個 SAML 驗證器必須有不同的實體識別碼。

儀表板中 SAML 驗證器的狀態一律會是綠色，因為它是靜態本質的預先定義中繼資料。紅色和綠色切換僅適用於動態驗證器。

如需為 VMware Unified Access Gateway 應用裝置設定 SAML 驗證器的相關資訊，請參閱《部署及設定 Unified Access Gateway》。

必要條件

- 確認 Workspace ONE、VMware Identity Manager 或第三方閘道或負載平衡器已完成安裝與設定。請參閱該產品的安裝文件。
- 確認用於 SAML 伺服器憑證之簽署 CA 的根憑證已安裝在連線伺服器主機上。VMware 建議您不要將 SAML 驗證器設定為使用自我簽署憑證。如需憑證驗證的相關資訊，請參閱《Horizon 7 安裝》文件。
- 記下 Workspace ONE 伺服器、VMware Identity Manager 伺服器或面向外部之負載平衡器的 FQDN 或 IP 位址。
- 若您使用 Workspace ONE 或 VMware Identity Manager，請記下連接器 Web 介面的 URL。
- 若您為 Unified Access Gateway 或需要您產生 SAML 中繼資料和建立靜態驗證器的第三方應用裝置建立驗證器，請對該裝置執行此程序即可產生 SAML 中繼資料，然後複製該中繼資料。

程序

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

2 在**連線伺服器**索引標籤上，選取要與 SAML 驗證器建立關聯的伺服器執行個體，然後按一下**編輯**。

3 在**驗證**索引標籤上的**將驗證委派給 VMware Horizon (SAML 2.0 驗證器)** 下拉式功能表中，選取設定以啟用或停用 SAML 驗證器。

選項	說明
已停用	停用 SAML 驗證。您只能從 Horizon Client 啟動遠端桌面平台和應用程式。
允許	SAML 驗證已啟用。您可從 Horizon Client 以及 VMware Identity Manager 或第三方裝置啟動遠端桌面平台和應用程式。
必要	SAML 驗證已啟用。您只能從 VMware Identity Manager 或第三方裝置啟動遠端桌面平台和應用程式。您無法從 Horizon Client 手動啟動桌面平台或應用程式。

您可以將部署中的每個連線伺服器執行個體設定為具有不同的 SAML 驗證設定，視您的需求而定。

4 按一下**管理 SAML 驗證器**後，按一下**新增**。

5 在 [新增 SAML 2.0 驗證器] 對話方塊中設定 SAML 驗證器。

選項	說明
類型	若為 Unified Access Gateway 或第三方裝置，請選取**靜態**。若為 VMware Identity Manager，請選取**動態**。對於動態驗證器，您可以指定中繼資料 URL 和管理 URL。對於靜態驗證器，則必須先在 Unified Access Gateway 或第三方裝置上產生中繼資料、加以複製，然後將其貼到 **SAML 中繼資料**文字方塊。
標籤	用於識別 SAML 驗證器的唯一名稱。
說明	SAML 驗證器的簡要說明。此值為選用。
中繼資料 URL	(適用於動態驗證器) 用來擷取在 SAML 身分識別提供者與連線伺服器執行個體之間交換 SAML 資訊所需之所有資訊的 URL。在 URL `https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml` 中，按一下 **<您的 Horizon Server 名稱>** 並將其更換為 VMware Identity Manager 伺服器或對外之負載平衡器 (第三方裝置) 的 FQDN 或 IP 位址。
管理 URL	(適用於動態驗證器) 用於存取 SAML 身分識別提供者的管理主控台的 URL。對於 VMware Identity Manager，此 URL 應指向 VMware Identity Manager Connector Web 介面。此值為選用。
SAML 中繼資料	(適用於靜態驗證器) 您所產生並從 Unified Access Gateway 或第三方裝置複製而來的中繼資料文字。
已為連線伺服器啟用	選取此核取方塊可啟用驗證器。您可以啟用多個驗證器。清單中只會顯示已啟用的驗證器。

6 按一下**確定**以儲存 SAML 驗證器組態。

如果已提供有效資訊，則必須接受自我簽署憑證 (不建議) 或針對 Horizon 7 和 VMware Identity Manager 或第三方裝置使用受信任的憑證。

[管理 SAML 驗證器] 對話方塊會顯示新建立的驗證器。

7 在 Horizon Administrator 儀表板上的 [系統健全狀況] 區段中，選取**其他元件 > SAML 2.0 驗證器**，選取已新增的 SAML 驗證器，並驗證詳細資料。

如果設定成功，則驗證器的健全狀況將顯示綠色。如果憑證不受信任，VMware Identity Manager 無法使用，或中繼資料 URL 無效，則驗證器的健全狀況將顯示紅色。如果憑證不受信任，您可以按一下**驗證**來驗證並接受此憑證。

後續步驟

延長連線伺服器中繼資料的到期期限，使遠端工作階段不會在 24 小時後即終止。請參閱在連線伺服器上變更服務提供者中繼資料的到期期限。

設定 VMware Identity Manager 的 Proxy 支援

Horizon 7 可為 VMware Identity Manager (vIDM) 伺服器提供 Proxy 支援。Proxy 詳細資料 (例如主機名稱和連接埠號碼) 可設定於 ADAM 資料庫中，且 HTTP 要求會透過 Proxy 進行路由傳送。

這項功能支援內部部署的 Horizon 7 部署能夠與雲端中主控的 vIDM 伺服器通訊的混合式部署。

必要條件

程序

1 在連線伺服器主機上啟動 ADSI Edit 公用程式。

2 展開物件路徑下的 ADAM ADSI 樹狀結構：`cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes`。

3 選取**動作 > 屬性**，並新增 **pae-SAMLProxyName** 和 **pae-SAMLProxyPort** 項目的值。

在連線伺服器上變更服務提供者中繼資料的到期期限

如果您未變更到期期限，連線伺服器會在 24 小時後停止接受來自 SAML 驗證器 (例如 Unified Access Gateway 應用裝置或第三方身分識別提供者) 的 SAML 判斷提示，屆時您將必須重新進行中繼資料交換。

請使用此程序，指定連線伺服器在經過多少天後會停止接受來自身分識別提供者的 SAML 判斷提示。目前的到期期限結束時將使用此數字。例如，如果目前的到期期限為 1 天，而您指定 90 天，則在經過 1 天後，連線伺服器就會產生到期期限為 90 天的中繼資料。

必要條件

有關如何在 Windows 作業系統版本使用 ADSI Edit 公用程式的資訊，請參閱 Microsoft TechNet 網站。

程序

1 在連線伺服器主機上啟動 ADSI Edit 公用程式。

2 在主控台樹狀結構中，選取**連線至**。

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

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

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

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

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

```
cs-samlencryptionkeyvaliditydays=number-of-days
cs-samlsigningkeyvaliditydays=number-of-days
```

在此範例中，*number-of-days* 是遠端連線伺服器停止接受 SAML 判斷提示前經過的天數。在這段時間過後，就必須重新進行交換 SAML 中繼資料的程序。

產生 SAML 中繼資料，讓連線伺服器做為服務提供者

為您要使用的身分識別提供者建立並啟用 SAML 驗證器後，您可能需要產生連線伺服器中繼資料。使用此中繼資料可在做為身分識別提供者的 Unified Access Gateway 應用裝置或第三方負載平衡器上建立服務提供者。

必要條件

確認您已為身分識別提供者 (Unified Access Gateway 或第三方負載平衡器或閘道) 建立 SAML 驗證器。在 Horizon Administrator 儀表板上的 [系統健全狀況] 區段中，您可以選取**其他元件 > SAML 2.0 驗證器**，選取已新增的 SAML 驗證器，並驗證詳細資料。

程序

1 開啟新的瀏覽器索引標籤並輸入 URL，以取得連線伺服器 SAML 中繼資料。

https://*connection-server.example.com*/SAML/metadata/sp.xml

在此範例中，*connection-server.example.com* 是連線伺服器主機的完整網域名稱。

此頁面會顯示來自連線伺服器的 SAML 中繼資料。

2 使用**另存新檔**命令，將網頁儲存為 XML 檔案。

例如，您可將頁面儲存至名為 `connection-server-metadata.xml` 的檔案。此檔案的內容開頭為下列文字：

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

後續步驟

在身分識別提供者上使用適當程序，複製連線伺服器 SAML 中繼資料。請參閱 Unified Access Gateway 或第三方負載平衡器或閘道的說明文件。

多個動態 SAML 驗證器的回應時間考量

如果您在連線伺服器執行個體上將 SAML 2.0 驗證設定為選用或必要，並且將多個動態 SAML 驗證器與連線伺服器執行個體產生關聯，如果有任何動態 SAML 驗證器變得無法連線，從其他動態 SAML 驗證器啟動遠端桌面平台的回應時間將會增加。

您可以使用 Horizon Administrator 停用無法連線的動態 SAML 驗證器，以縮短在其他動態 SAML 驗證器上啟動遠端桌面平台的回應時間。如需停用 SAML 驗證器的相關資訊，請參閱在 Horizon Administrator 中設定 SAML 驗證器。

在 Horizon Administrator 中設定 Workspace ONE 存取原則

Workspace ONE 或 VMware Identity Manager (vIDM) 管理員可設定存取原則，以限制對 Horizon 7 中已授權的桌面平台和應用程式的存取。若要強制執行在 vIDM 中建立的原則，您必須使 Horizon Client 進入 Workspace ONE 模式，而讓 Horizon Client 能夠推送使用者進入 Workspace ONE 用戶端以啟動權利。當您登入 Horizon Client 時，存取原則會指示您透過 Workspace ONE 登入，以存取已發佈的桌面平台和應用程式。

必要條件

- 為 Workspace ONE 中的應用程式設定存取原則。如需關於設定存取原則的詳細資訊，請參閱《VMware Identity Manager 管理指南》。
- 在 Horizon Administrator 中，授權使用者使用已發佈的桌面平台和應用程式。

程序

1. 在 Horizon Administrator 中，選取**組態 > 伺服器**。
2. 在**連線伺服器**索引標籤上，選取與 SAML 驗證器相關聯的伺服器執行個體，然後按一下**編輯**。
3. 在**驗證**索引標籤上，**將驗證委派給 VMware Horizon (SAML 2.0 驗證器)** 選項設為**必要**。

   [必要] 選項會啟用 SAML 驗證。使用者只能連線至已由 vIDM 或第三方身分識別提供者提供 SAML Token 的 Horizon Server。您無法從 Horizon Client 手動啟動桌面平台或應用程式。
4. 選取**啟用 Workspace ONE 模式**。
5. 在 **Workspace ONE 伺服器主機名稱**文字方塊中，輸入 Workspace ONE 主機名稱 FQDN 值。
6. (選擇性) 選取**封鎖來自不支援 Workspace ONE 模式的用戶端的連線**，限制支援 Workspace ONE 模式的 Horizon Client 存取應用程式。

   4.5 之前的 Horizon Client 不支援 Workspace ONE 模式功能。如果選取此選項，4.5 之前的 Horizon Client 將無法存取 Workspace ONE 中的應用程式。如果 Workspace ONE 版本早於 2.9.1 版，則不會為 Horizon 7 (7.2 版) 之後的版本啟用 Workspace ONE 模式功能。

設定生物識別驗證

您可以編輯 LDAP 資料庫中的 `pae-ClientConfig` 屬性，藉以設定生物識別驗證。

必要條件

有關如何在 Windows Server 中使用 ADSI Edit 公用程式的資訊，請參閱 Microsoft TechNet 網站。

程序

1 在連線伺服器主機上啟動 ADSI Edit 公用程式。

2 在「連線設定」對話方塊中，選取或連線至 **DC=vdi,DC=vmware,DC=int**。

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

例如：**`localhost:389`** 或 **`mycomputer.mydomain.com:389`**

4 在物件 **CN=Common, OU=Global, OU=Properties** 上，編輯 **pae-ClientConfig** 屬性並新增值 **BioMetricsTimeout=<integer>**。

以下為有效的 `BioMetricsTimeout` 值：

BioMetricsTimeout 值	說明
0	不支援生物識別驗證。這是預設值。
-1	支援生物識別驗證且無時間限制。
任何正整數	支援生物識別驗證且可使用指定的分鐘數。

新設定會立即生效。您不必重新啟動連線伺服器服務或用戶端裝置。

驗證使用者而不要求認證

5

使用者在登入用戶端裝置或 VMware Identity Manager 後，即可連線至已發佈的應用程式或桌面平台，而不會收到 Active Directory 認證提示。

管理員可以選擇根據使用者需求設定組態。

- 提供使用者對已發佈應用程式的未驗證存取。管理員可以進行設定，讓使用者不需使用 Active Directory (AD) 認證即可登入 Horizon Client。
- 對 Windows 用戶端使用「以目前使用者身分登入」。對於 Windows 用戶端，管理員可以進行設定，讓使用者在使用 AD 認證登入 Windows 用戶端後，不必提供其他認證即可登入 Horizon Server。
- 將認證儲存在行動用戶端和 Mac 用戶端中。對於行動和 Mac 用戶端，管理員則可以設定讓 Horizon Server 儲存認證。透過這項功能，使用者在對行動或 Mac 用戶端提供過一次 AD 認證後，就不用再記住用於 SSO (Single Sign-On) 的 AD 認證。
- 針對 VMware Identity Manager 設定 True SSO。對於 VMware Identity Manager，管理員可以設定 True SSO，讓使用 AD 認證以外的某些方法進行驗證的使用者，也可以登入已發佈的桌面平台或應用程式，而不會收到 AD 認證提示。

本章節討論下列主題：

提供已發佈應用程式的未驗證存取

管理員可以設定組態，讓未驗證使用者不需使用 AD 認證即可從 Horizon Client 存取其已發佈的應用程式。如果您的使用者需要存取具有本身安全性和使用者管理的順暢執行應用程式，請考慮設定未驗證存取。

當使用者啟動已針對未驗證存取設定的已發佈應用程式時，RDS 主機會視需求建立本機使用者工作階段，並將配置工作階段給使用者。

此功能需要 Horizon Client 4.4 版或更新版本。使用 HTML Access 用戶端時，此功能需要 4.5 版或更新版本。

設定未驗證使用者的工作流程

1 針對未驗證存取建立使用者。請參閱針對未驗證存取建立使用者。

2 對使用者啟用未驗證存取，並設定預設的未驗證使用者。請參閱啟用使用者未驗證存取。

3 授權未驗證使用者使用已發佈的應用程式。請參閱授權未驗證存取使用者使用已發佈的應用程式。

4 啟用來自 Horizon Client 的未驗證存取。請參閱來自 Horizon Client 的未驗證存取。

設定未驗證使用者的規則和指導方針

- 未驗證存取不支援雙因素驗證 (例如 RSA 和 RADIUS) 和智慧卡驗證。
- 智慧卡驗證和未驗證存取互斥。即使先前已啟用未驗證存取，在連線伺服器中將智慧卡驗證設為必要時仍會停用。
- 未驗證存取不支援 VMware Identity Manager 和 VMware App Volumes。
- PCoIP 和 VMware Blast 顯示通訊協定皆支援此功能。
- 未驗證存取功能不會驗證 RDS 主機的授權資訊。管理員必須設定和使用裝置授權。
- 未驗證存取功能不會保留任何使用者特定資料。使用者可以驗證應用程式的資料儲存需求。
- 您無法重新連線至未驗證應用程式工作階段。當使用者從用戶端中斷連線時，RDS 主機會自動登出本機使用者工作階段。
- 未驗證存取僅支援已發佈的應用程式。
- 從桌面平台集區發佈的應用程式不支援未驗證存取。
- 未驗證存取不支援安全伺服器或 Unified Access Gateway 應用裝置。
- 系統不會保留未驗證使用者的使用者喜好設定。
- 虛擬桌面平台不支援未驗證使用者。
- 如果已使用 CA 簽署的憑證設定連線伺服器，且已啟用未驗證存取但未設定預設的未驗證使用者，則 Horizon Administrator 會針對連線伺服器顯示紅色狀態。
- 如果安裝在 RDS 主機上的 Horizon Agent 已停用 `AllowSingleSignon` 群組原則設定，則未驗證存取功能將無法運作。管理員也可以控制是否要使用 `UnAuthenticatedAccessEnabled` Horizon Agent 群組原則設定來停用或啟用未驗證存取。`vdm_agent.admx` 範本檔中包含 Horizon Agent 群組原則設定。您必須將 RDS 主機重新開機，此原則才會生效。

針對未驗證存取建立使用者

管理員可以建立未驗證存取已發佈應用程式的使用者。在管理員針對未驗證存取設定使用者之後，使用者僅可以利用未驗證存取從 Horizon Client 登入至連線伺服器執行個體。

必要條件

- 確認您要設定未驗證存取的 Active Directory (AD) 使用者擁有有效的 UPN。您僅能將 AD 使用者設定為未驗證存取使用者。

備註　管理員僅可對每個 AD 帳戶建立一個使用者。管理員無法建立未驗證使用者群組。如果您建立未驗證存取使用者，並且該 AD 使用者具有現有用戶端工作階段，則必須重新啟動用戶端工作階段讓變更生效。

程序

1. 在 Horizon Administrator 中，選取**使用者與群組**。
2. 在**未驗證存取**索引標籤上，按一下**新增**。
3. 在**新增未驗證使用者**精靈中，選取一或多個搜尋準則，然後按一下**尋找**來根據您的搜尋準則尋找使用者。

   使用者必須擁有有效的 UPN。
4. 選取使用者，然後按**下一步**。

   若要新增多個使用者，可重複此步驟。
5. (選擇性) 輸入使用者別名。

   預設的使用者別名即為針對該 AD 帳戶所設定的使用者名稱。使用者可以利用該使用者別名，從 Horizon Client 登入至連線伺服器執行個體。
6. (選擇性) 檢閱使用者詳細資料並新增註解。
7. 按一下**完成**。

連線伺服器會建立未驗證存取使用者，並顯示使用者詳細資料，包括使用者別名、使用者名稱、名字和姓氏，來源網繭數量、應用程式權利和工作階段。您可以按一下來源網繭欄中的數量來顯示網繭資訊。

後續步驟

為連線伺服器中的使用者啟用未驗證存取。請參閱啟用使用者未驗證存取。

啟用使用者未驗證存取

針對未驗證存取建立使用者之後，您必須在連線伺服器中啟用未驗證存取，讓使用者連線及存取已發佈的應用程式。

程序

1. 在 Horizon Administrator 中，選取 **View 組態 > 伺服器**。
2. 按一下**連線伺服器**索引標籤。
3. 選取連線伺服器執行個體，然後按一下**編輯**。
4. 按一下**驗證**索引標籤。
5. 將**未驗證存取**變更為**已啟用**。

6 從**預設未驗證存取使用者**下拉式功能表，選取使用者做為預設使用者。

預設使用者必須出現在 Cloud Pod 架構 環境中的本機網繭上。如果您從不同的網繭選取預設使用者，則連線伺服器會在本機網繭上建立使用者，之後才讓使用者成為預設使用者。

7 (選擇性) 輸入使用者的預設工作階段逾時。

預設工作階段逾時為閒置後 10 分鐘。

8 按一下**確定**。

後續步驟

授權未驗證使用者使用已發佈的應用程式。請參閱授權未驗證存取使用者使用已發佈的應用程式。

授權未驗證存取使用者使用已發佈的應用程式

建立未驗證存取使用者之後，您必須授權使用者存取已發佈的應用程式。

必要條件

- 根據一組 RDS 主機建立伺服器陣列。請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件中的〈建立伺服器陣列〉。
- 針對執行於 RDS 主機之伺服器陣列上已發佈的應用程式建立應用程式集區。請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件中的〈建立應用程式集區〉。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > 應用程式集區**，然後按一下應用程式集區的名稱。

2 從**權利**下拉式功能表中選取**新增權利**。

3 按一下**新增**，選取一或多個搜尋準則，按一下**尋找**，然後選取**未驗證使用者**核取方塊，以便根據您的搜尋準則尋找未驗證存取使用者。

4 選取要授權使用集區中應用程式的使用者，然後按一下**確定**。

5 按一下**確定**儲存變更。

在權利程序完成之後，未驗證存取圖示會出現在未驗證存取使用者旁邊。

後續步驟

使用未驗證存取使用者來登入至 Horizon Client。請參閱來自 Horizon Client 的未驗證存取。

搜尋未驗證存取工作階段

使用 Horizon Administrator 來列出或搜尋未驗證存取使用者已連線的應用程式工作階段。未驗證存取使用者圖示會顯示在未驗證存取使用者已連線的那些工作階段旁邊。

程序

1 在 Horizon Administrator 中，選取**監視 > 工作階段**。

2 按一下**應用程式**以搜尋應用程式工作階段。

3 選取搜尋準則，然後開始搜尋。

搜尋結果包括使用者、工作階段的類型 (桌面平台或應用程式)、機器、集區或伺服器陣列、DNS 名稱、用戶端識別碼和安全閘道。搜尋結果也會顯示工作階段開始時間、持續時間、狀態和上一個工作階段。

刪除未驗證存取使用者

刪除未驗證存取使用者時，您也必須移除該使用者的應用程式集區權利。您無法刪除身為預設使用者的未驗證存取使用者。

備註 如果您刪除未驗證存取使用者，並且該 AD 使用者具有現有用戶端工作階段，則必須重新啟動用戶端工作階段讓變更生效。

程序

1 在 Horizon Administrator 中，選取**使用者與群組**。

2 在**未驗證存取**索引標籤上，按一下**刪除**。

3 按一下**確定**。

後續步驟

移除使用者的應用程式權利。請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件中的〈從桌面平台或應用程式集區移除權利〉。

來自 Horizon Client 的未驗證存取

使用未驗證存取登入至 Horizon Client 並啟動已發佈的應用程式。

為了確保更高的安全性，未驗證存取使用者擁有可讓您用來登入至 Horizon Client 的使用者別名。選取使用者別名時，您不需為使用者提供 AD 認證或 UPN。登入至 Horizon Client 之後，您可以按一下您已發佈的應用程式來啟動應用程式。如需關於安裝和設定 Horizon Client 的詳細資訊，請參閱 VMware Horizon Client 說明文件網頁上的 Horizon Client 說明文件。

必要條件

- 確認 Horizon 7 (7.1 版) 連線伺服器已進行「未驗證存取」的設定。
- 確認已在 Horizon Administrator 中建立「未驗證存取」使用者。如果預設的「未驗證存取」使用者是唯一的「未驗證存取」使用者，則 Horizon Client 會以預設使用者連線至連線伺服器執行個體。

程序

1 啟動 Horizon Client。

2 在 Horizon Client 中，選取**使用未驗證存取匿名登入**。

3 連線至連線伺服器執行個體。

4 從下拉式功能表選取使用者別名，然後按一下**登入**。

預設的使用者具有尾碼「default」。

5 按兩下已發佈的應用程式以啟動應用程式。

針對未驗證存取已發佈的應用程式設定登入減速

由於使用未驗證存取時使用者不會輸入認證，RDS 主機可能會因為已發佈的應用程式要求而無法負荷。登入減速可以減輕此情況。您可以調整減速的等級。您也可以封鎖不支援減速的用戶端。

必要條件

- 確認您已為使用者啟用未驗證存取。
- 確認您擁有 Horizon Client 4.9 版或更新版本。如果您使用 Horizon Client 4.8 版，當使用者使用未驗證存取匿名登入 Horizon 7 (7.6 版) 時，可能偶爾會失敗，而系統可能會要求重試登入。

程序

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

2 按一下**連線伺服器**索引標籤。

3 按一下**驗證**索引標籤。

4 從**登入減速等級**下拉式功能表中，為未驗證存取登入選取減速等級。

選項	說明
低	為未驗證存取登入設定低減速等級。若為 Microsoft Internet Explorer 和 Microsoft Edge 之類的網頁瀏覽器，建議設定低減速等級。
中	為未驗證存取登入設定中減速等級。此為依預設的設定。如果您使用 Horizon Client 4.8 版，請勿變更此設定。
高	為未驗證存取登入設定高減速等級。設定高減速等級可能會增加登入時間，且會影響使用者體驗。

5 (選擇性) 若要防止不支援登入減速的任何用戶端使用未驗證存取連線到 Horizon 7，請選取**封鎖不相容的用戶端**。

早於 Horizon Client 4.8 之前的版本不相容。

6 按一下**確定**。

後續步驟

使用未驗證存取登入至 Horizon Client 並啟動已發佈的應用程式。請參閱來自 Horizon Client 的未驗證存取。

為使用者設定混合登入

建立未驗證存取使用者之後，您可以為該使用者啟用混合登入。啟用混合登入可為未驗證的存取使用者提供網路資源的網域存取權，例如檔案共用或網路印表機，而不需輸入認證。

備註 對於已設定混合登入的指定未驗證存取使用者，混合登入功能會對所有登入的使用者使用相同的網域使用者。

備註 如果您從 RDS 主機利用使用者設定檔索引標籤將主目錄設定為網路路徑，則 Windows 上的管理使用者介面依預設會移除對主目錄資料夾的所有現有權限，並為管理員和具有完全控制的本機使用者新增權限。請使用管理員帳戶從權限清單中移除本機使用者，然後新增網域使用者，並讓該使用者擁有需要為其設定的權限。

必要條件

- 確認您在 RDS 主機上安裝 Horizon Agent 時選取了 [混合登入] 自訂選項。如需關於 RDS 主機之 Horizon Agent 自訂安裝選項的詳細資訊，請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件。
- 確認您已建立未驗證存取使用者。
- 確認未在網域中為使用者帳戶啟用 Kerberos DES 加密。混合登入功能不支援 Kerberos DES 加密。

程序

1. 在 Horizon Administrator 中，選取**使用者與群組**。
2. 在**未驗證存取**索引標籤上，按一下**新增**。
3. 在**新增未驗證使用者**精靈中，選取一或多個搜尋準則，然後按一下**尋找**來根據您的搜尋準則尋找未驗證存取使用者。

   使用者必須擁有有效的 UPN。
4. 選取一個未驗證存取使用者，然後按**下一步**。

   若要新增多個使用者，可重複此步驟。
5. (選擇性) 輸入使用者別名。

   預設的使用者別名即為針對該 AD 帳戶所設定的使用者名稱。使用者可以利用該使用者別名，從 Horizon Client 登入至連線伺服器執行個體。
6. (選擇性) 檢閱使用者詳細資料並新增註解。
7. 選取**啟用混合登入**。

   依預設會選取**啟用 True SSO** 選項。您必須已為 Horizon 7 環境啟用 True SSO。然後，啟用混合登入的未驗證存取使用者會使用 True SSO 從 Horizon Client 登入連線伺服器執行個體。

   備註 如果並未將連線伺服器網繭設定為使用 True SSO，則使用者可以透過未驗證存取來啟動授權的應用程式。不過，使用者並未擁有網路存取權限，因為網繭上未啟用 True SSO。

8 (選擇性) 若要讓使用者從 Horizon Client 登入連線伺服器執行個體，請選取**啟用密碼登入**，然後輸入使用者密碼。

如果您沒有為 Horizon 7 環境設定 True SSO，請使用此設定。

在 CPA 環境中，混合登入使用者功能僅在混合登入使用者已設定**啟用密碼登入**設定，且有權存取已發佈應用程式的連線伺服器網繭上正常運作。

例如，在包含網繭 A 和網繭 B 的 CPA 環境中，混合登入使用者設定了**啟用密碼登入**設定，且有權存取網繭 A 上的應用程式。該使用者可以從連線至網繭 A 或網繭 B 的用戶端檢視並啟動應用程式。不過，如果您稍後將網繭 B 上的另一個應用程式授權給相同的使用者，則該使用者將無法從連線至網繭 B 的用戶端檢視及啟動該應用程式。若要讓混合登入功能在網繭 B 上能夠正常運作，您必須建立另一個混合式登入使用者並進行**啟用密碼登入**設定，然後將應用程式授權給使用者。如需如何設定 CPA 環境的詳細資訊，請參閱《在 Horizon 7 中管理 Cloud Pod 架構》文件。

9 按一下**完成**。

後續步驟

授權使用者存取已發佈的應用程式。請參閱授權未驗證存取使用者使用已發佈的應用程式。

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

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

為了支援此功能，使用者認證會儲存在連線伺服器執行個體與用戶端系統上。

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

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

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

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

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

「以目前使用者身分登入」功能的限制與需求如下：

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

將認證儲存在行動裝置和 Mac Horizon Client 中

管理員可以設定連線伺服器，讓行動裝置和 Mac Horizon Client 記住使用者的使用者名稱、密碼和網域資訊。

對於適用於行動裝置的 Horizon Client，此功能會使**儲存密碼**核取方塊出現在登入對話方塊上。針對 Mac 版 Horizon Client，此功能會使**記住此密碼**核取方塊出現在登入對話方塊上。

如果使用者選擇儲存其認證，認證將在後續連線中新增至 Horizon Client 的登入欄位。

若要啟用此功能，您必須在 View LDAP 中設定一個值，以指出認證資訊要在用戶端中儲存多久。針對 Mac 版 Horizon Client，只有 4.1 版或更新版本支援此功能。

備註 在 Windows 系統的 Horizon Client 上，以目前使用者身分登入的功能不需要使用者多次提供認證。

設定儲存 Horizon Client 認證的逾時限制

您可以在 View LDAP 中設定一個值以設定逾時限制，指出 Horizon Client 認證資訊要在行動裝置和 Mac 用戶端系統上儲存多久。設定的逾時限制以分鐘為單位。變更連線伺服器執行個體上的 View LDAP 時，變更將傳播至所有複寫的連線伺服器執行個體。

必要條件

有關如何在 Windows 作業系統版本使用 ADSI Edit 公用程式的資訊，請參閱 Microsoft TechNet 網站。

程序

1 在連線伺服器主機上啟動 ADSI Edit 公用程式。

2 在「連線設定」對話方塊中，選取或連線至 **DC=vdi,DC=vmware,DC=int**。

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

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

4 在物件 **OU=Properties、OU=Global、CN=Common** 上，編輯 **pae-ClientCredentialCacheTimeout** 屬性值。

未設定 **pae-ClientCredentialCacheTimeout** 或將其設為 **0** 時，會停用此功能。若要啟用此功能，可設定保留認證資訊的分鐘數，或設定 **-1** 的值，表示無逾時。

在連線伺服器上，新的設定將立即生效。您不必重新啟動連線伺服器服務或用戶端電腦。

設定 True SSO

透過 True SSO (Single Sign-On) 功能，當使用者利用智慧卡或 RSA SecurID 或 RADIUS 驗證登入 VMware Identity Manager 後，或當第三方身分識別提供者使用 Unified Access Gateway 應用裝置時，使用者不需再輸入 Active Directory 認證，即可使用虛擬桌面平台或已發佈的桌面平台或應用程式。

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

連線至虛擬桌面平台或已發佈的應用程式時，使用者可以選取使用原生 Horizon Client 或 HTML Access。

這項功能具有下列的限制：

- 此功能不適用於使用 View Agent Direct-Connection 外掛程式提供的虛擬桌面。
- 只有 IPv4 環境才支援此功能。

以下清單列出為您的環境設定 True SSO 所必須執行的工作：

1 判定 True SSO 的架構

2 設定企業憑證授權機構

3 建立與 True SSO 搭配使用的憑證範本

4 安裝和設定註冊伺服器

5 匯出註冊服務用戶端憑證

6 設定 SAML 驗證來與 True SSO 搭配使用

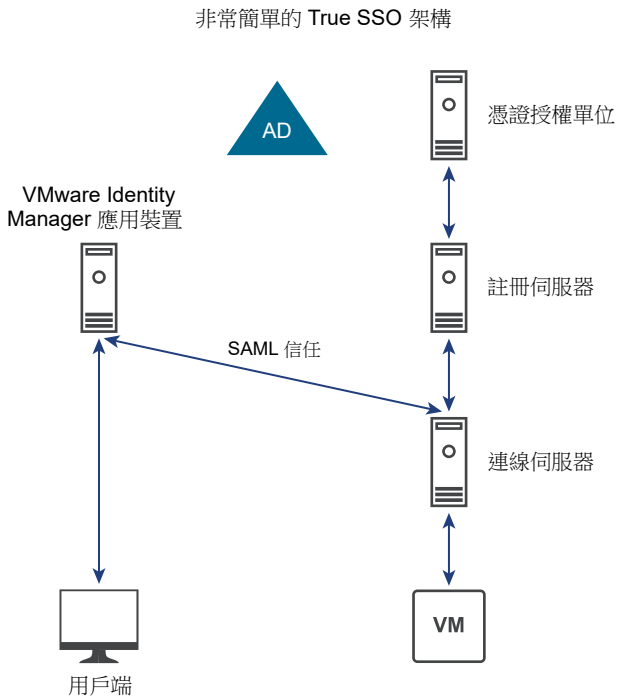
7 設定 Horizon 連線伺服器使用 True SSO

判定 True SSO 的架構

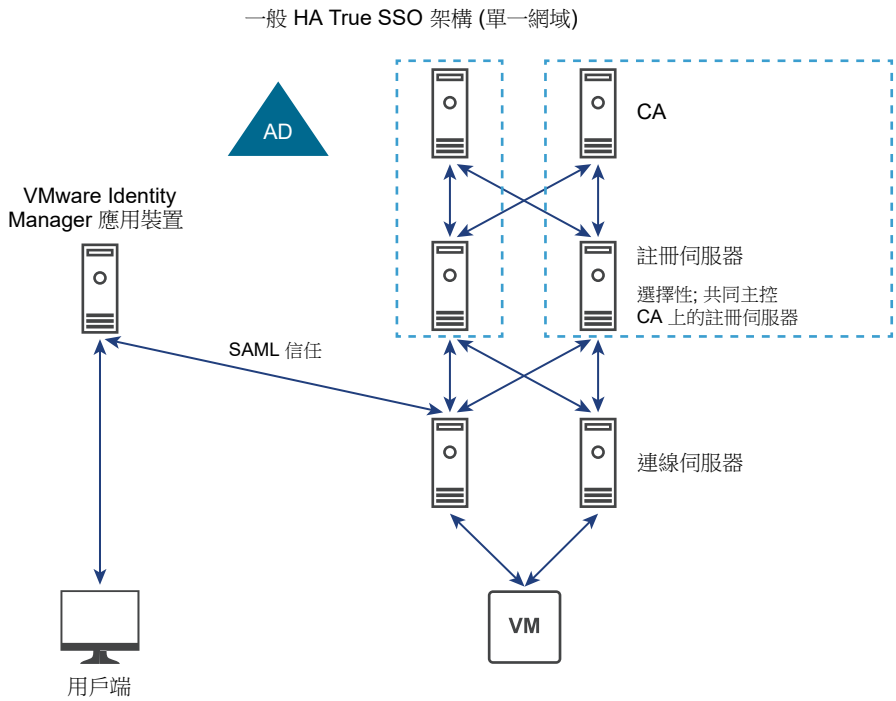
若要使用 True SSO，您必須具備或新增憑證授權單位，並建立註冊伺服器。這兩個伺服器會通訊以建立短期 Horizon 虛擬憑證，允許不使用密碼即可登入 Windows。您可在單一網域、具有多個網域的單一樹系，以及多個樹系、多個網域的設定中使用 True SSO。

VMware 建議部署兩個 CA 和兩個 ES 以使用 True SSO。下列範例說明不同架構中的 True SSO。

下圖說明簡單的 True SSO 架構。

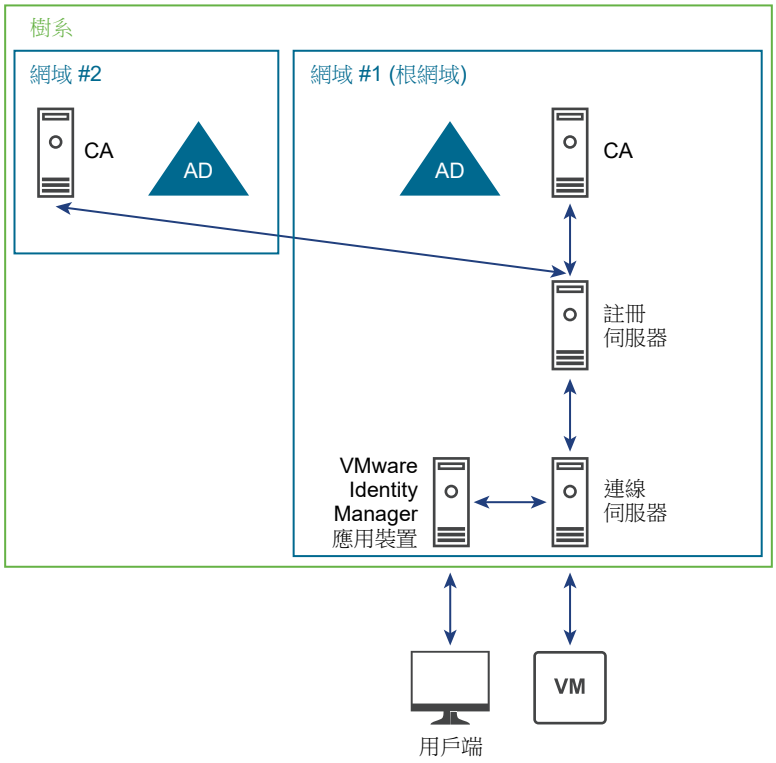


下圖說明單一網域架構中的 True SSO。



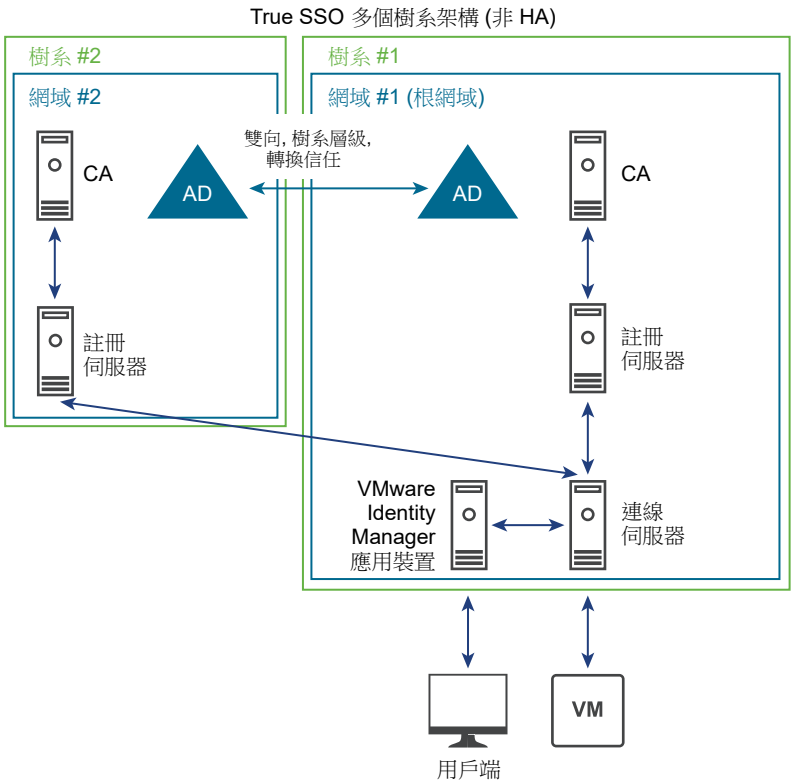
下圖說明具有多個網域的單一樹系架構中的 True SSO。

True SSO 具有多個網域的單一樹系架構 (非 HA)



下圖說明多個樹系架構中的 True SSO。

True SSO 多個樹系架構 (非 HA)



設定企業憑證授權機構

如果您尚未設定憑證授權機構，則必須新增 Active Directory 憑證服務 (AD CS) 角色至 Windows Server，並將該伺服器設定為企業 CA。

如果您已設定企業 CA，請確認您使用的是本程序中說明的設定。

您必須至少有一個企業 CA，而 VMware 建議具備兩個，以供容錯移轉和負載平衡之用。您要建立來用於 True SSO 的註冊伺服器會與企業 CA 通訊。如果您設定註冊伺服器為使用多個企業 CA，則註冊伺服器會在可用的 CA 間輪流使用。如果在主控企業 CA 的同一部機器上安裝註冊伺服器，您可設定註冊伺服器為優先使用本機 CA。建議使用此組態，以獲得最佳效能。

此程序中有一部分涉及啟用非持續性憑證處理。依預設，憑證處理包括在 CA 資料庫中儲存每個憑證要求與已核發憑證的記錄。持續的大量要求會提高 CA 資料庫的增長速度，若未加以監控，可能會耗用掉所有可用的磁碟空間。啟用非持續性憑證處理有助於降低 CA 資料庫的增長速度，以及進行資料庫管理工作的頻率。

必要條件

- 建立 Windows Server 2008 R2、Windows Server 2012 R2、Windows Server 2016 或是 Windows Server 2019 的虛擬機器。
- 確認虛擬機器屬於 Horizon 7 部署之 Active Directory 網域的一部分。
- 確認您使用的是 IPv4 環境。此功能目前在 IPv6 環境中不受支援。
- 確認系統具有靜態 IP 位址。

程序

1 以管理員身分登入虛擬機器作業系統，並啟動伺服器管理員。

2 選取用於新增角色的設定。

作業系統	選取項目
■ **Windows Server 2012 R2** ■ **Windows Server 2016** ■ **Windows Server 2019**	a 選取**新增角色及功能**。 b 在 [選取安裝類型] 頁面上，選取**角色型或功能型安裝**。 c 在 [選取目的地伺服器] 頁面上，選取伺服器。
Windows Server 2008 R2	a 選取導覽樹狀結構中的**角色**。 b 按一下**新增角色**以啟動**新增角色**精靈。

3 在 [選取伺服器角色] 頁面上，選取 **Active Directory 憑證服務**。

4 在新增角色及功能精靈中，按一下**新增功能**並保持選取**包括管理工具**核取方塊。

5 在 [選取功能] 頁面上，接受預設值。

6 在 [選取角色服務] 頁面上，選取**憑證授權機構**。

7 依照提示完成安裝。

8 安裝完成時，在 [安裝進度] 頁面上，按一下**設定目的地伺服器上的 Active Directory 憑證服務**連結，開啟 [AD CS 設定] 精靈。

9 在 [認證] 頁面上按**下一步**，依下表所述完成 [AD CS 設定] 精靈頁面。

選項	動作
角色服務	選取**憑證授權機構**，然後按**下一步** (而非**設定**)。
安裝類型	選取**企業 CA**。
CA 類型	選取**根 CA** 或**次級 CA**。有些企業偏好兩層 PKI 部署。如需詳細資訊，請參閱 http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx。
私密金鑰	選取**建立新的私密金鑰**。
CA 的密碼編譯	對於雜湊演算法，您可選取 **SHA1**、**SHA256**、**SHA384** 或 **SHA512**。對於金鑰長度，您可選取 **1024**、**2048**、**3072** 或 **4096**。 VMware 建議最低設定 SHA256 和 2048 金鑰。
CA 名稱	接受預設值或變更名稱。
有效期間	接受 5 年的預設值。
憑證資料庫	接受預設值。

10 在 [確認] 頁面上，按一下**設定**，當精靈報告組態成功時，關閉精靈。

11 開啟命令提示字元並輸入下列命令，以設定非持續性憑證處理的 CA：

```
certutil –setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

12 輸入下列命令，忽略 CA 上的離線 CRL (憑證撤銷清單) 錯誤：

```
certutil –setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

此旗標為必要，因為 True SSO 使用的根憑證會經常離線，因而撤銷檢查會失敗，但這是正常的。

13 輸入以下命令重新啟動服務：

```
sc stop certsvc
sc start certsvc
```

後續步驟

建立憑證範本。請參閱建立與 True SSO 搭配使用的憑證範本。

建立與 True SSO 搭配使用的憑證範本

您必須建立可用於發行短期憑證的憑證範本，且必須指定網域中的哪些電腦可要求這類憑證。

您可以建立多個憑證範本。每個網域只能設定一個範本，但您可以在多個網域之間共用範本。例如，如果您有具有三個網域的 Active Directory 樹系，而您想對三個網域全都使用 True SSO，則可選擇設定一個、兩個或三個範本。所有網域可以共用相同的範本，您也可以讓每個網域具有不同的範本。

必要條件

- 確認您有企業 CA 可用於建立本程序所述的範本。請參閱設定企業憑證授權機構。
- 確認您已備妥智慧卡驗證所需的 Active Directory。如需詳細資訊，請參閱《Horizon 7 安裝》文件。

- 建立註冊伺服器在網域和樹系中的安全群組，並將註冊伺服器的電腦帳戶加入該群組。

程序

1 若要設定 True SSO，在用於憑證授權機構的機器上，以管理員身分登入作業系統，然後前往**系統管理工具 > 憑證授權單位**。

a 展開左窗格中的樹狀結構，以滑鼠右鍵按一下**憑證範本**，然後選取**管理**。

b 以滑鼠右鍵按一下**智慧卡登入**範本，然後選取**複製**。

c 針對以下索引標籤進行以下變更：

索引標籤	動作
[相容性] 索引標籤	■ 針對**憑證授權機構**，選取 **Windows Server 2008 R2**。 ■ 針對**憑證收件者**，選取 **Windows 7/Windows Server 2008 R2**。
[一般] 索引標籤	■ 將範本顯示名稱變更為 **True SSO**。 ■ 將有效期間變更為一般工作日的時間長度；也就是說，使用者可能保持登入系統的時間長度。 為了讓使用者在登入時不會失去對網路資源的存取，有效期間必須比使用者網域中的 Kerberos TGT 更新時間還要長。 (票證的預設最長存留期為 10 小時。若要尋找預設網域原則，請至**電腦設定 > 原則 > Windows 設定 > 安全性設定 > 帳戶原則 > Kerberos 原則: 使用者票證最長存留期**。) ■ 將更新期間變更為有效期間的 50%-75%。
[處理要求] 索引標籤	■ 針對**目的**，選取**簽章和智慧卡登入**。 ■ 選取**針對智慧卡自動更新，...**
[密碼編譯] 索引標籤	■ 針對**提供者類別**，選取**金鑰儲存提供者**。 ■ 針對**演算法名稱**，選取 **RSA**。
[伺服器] 索引標籤	選取**不在 CA 資料庫中儲存憑證及要求**。 **重要** 請務必取消選取**不在簽發的憑證中包含撤銷資訊** (選取第一個方塊後就會選取此方塊，因此您必須取消選取 (清除) 此方塊)。
[發行需求] 索引標籤	■ 選取**授權簽章的數目**，然後在方塊中輸入 **1**。 ■ 針對**原則類型**，選取**應用程式原則**，然後將原則設為**憑證要求代理程式**。 ■ 針對**重新註冊必須要符合下列條件**，選取**現存憑證必須有效**。
[安全性] 索引標籤	針對為註冊伺服器電腦帳戶建立的安全群組 (如先決條件中所述)，請提供以下權限：讀取、註冊 1 按一下**新增**。 2 指定哪些電腦可註冊憑證。 3 針對這些電腦選取適用的核取方塊，給予電腦下列權限：讀取、註冊。

d 按一下 [新範本的內容] 對話方塊中的**確定**。

e 關閉 [憑證範本主控台] 視窗。

f 以滑鼠右鍵按一下**憑證範本**，然後選取**新增 > 要發出的憑證範本**。

備註 根據此範本核發憑證的所有憑證授權機構都需要執行此步驟。

g 在 [啟用憑證範本] 視窗中，選取剛建立的範本 (例如 **True SSO Template**)，然後按一下**確定**。

2 若要設定註冊代理程式電腦，在用於憑證授權機構的機器上，以管理員身分登入作業系統，然後前往**系統管理工具 > 憑證授權單位**。

a 展開左窗格中的樹狀結構，以滑鼠右鍵按一下**憑證範本**，然後選取**管理**。

b 找到並開啟註冊代理程式電腦範本，然後在**安全性**索引標籤上進行下列變更：

針對為註冊伺服器電腦帳戶建立的安全群組 (如先決條件中所述)，請提供以下權限：讀取、註冊

1 按一下**新增**。

2 指定哪些電腦可註冊憑證。

3 針對這些電腦選取適用的核取方塊，給予電腦下列權限：讀取、註冊。

c 以滑鼠右鍵按一下**憑證範本**，然後選取**新增 > 要發出的憑證範本**。

備註 根據此範本核發憑證的所有憑證授權機構都需要執行此步驟。

d 在 [啟用憑證範本] 視窗中，選取**註冊代理程式電腦**，然後按一下**確定**。

後續步驟

建立註冊服務。請參閱安裝和設定註冊伺服器。

安裝和設定註冊伺服器

您執行連線伺服器安裝程式並選取 Horizon 7 註冊伺服器選項來安裝註冊伺服器。註冊伺服器會代表您指定的使用者要求短期憑證。這些短期憑證是 True SSO 用於驗證的機制，可避免提示使用者輸入 Active Directory 認證。

您必須至少安裝並設定一部註冊伺服器，且註冊伺服器不能安裝在與 View 連線伺服器相同的主機上。VMware 建議您架設兩部註冊伺服器，以供容錯移轉和負載平衡之用。如果您擁有兩部註冊伺服器，依預設一部為優先伺服器，另一部則用於容錯移轉。不過，您可以變更此預設值，讓連線伺服器輪流傳送憑證要求給這兩部註冊伺服器。

如果在主控企業 CA 的同一部機器上安裝註冊伺服器，您可設定註冊伺服器為優先使用本機 CA。如需最佳效能，VMware 建議結合優先使用本機 CA 的組態以及負載平衡註冊伺服器的組態。如此一來，當憑證要求抵達時，連線伺服器會輪流使用註冊伺服器，而每部註冊伺服器會使用本機 CA 來服務要求。如需組態設定的相關資訊，請參閱 註冊伺服器組態設定 和 連線伺服器組態設定。

必要條件

- 建立至少具備 4 GB 記憶體的 Windows Server 2008 R2、Windows Server 2012 R2 或 Windows Server 2016 虛擬機器，或使用主控企業 CA 的虛擬機器。請勿使用做為網域控制站的機器。
- 確認虛擬機器上未安裝其他 View 元件，包括 View 連線伺服器、View Composer、安全伺服器、Horizon Client、View Agent 或 Horizon Agent。

- 確認虛擬機器屬於 Horizon 7 部署之 Active Directory 網域的一部分。
- 確認您使用的是 IPv4 環境。此功能目前在 IPv6 環境中不受支援。
- VMware 建議系統必須具備靜態 IP 位址。
- 確認您可以用具備管理員權限的網域使用者身分登入作業系統。您必須以管理員身分登入，才能執行安裝程式。

程序

1 在您計劃用於註冊伺服器的機器上，將憑證嵌入式管理單元新增到 MMC：

a 開啟 MMC 主控台並選取**檔案 > 新增/移除嵌入式管理單元**

b 在**可用的嵌入式管理單元**下方，選取**憑證**然後按一下**新增**。

c 在 [憑證嵌入式管理單元] 視窗中，選取**電腦帳戶**、按**下一步**，然後按一下**完成**。

d 在 [新增或移除嵌入式管理單元] 視窗中，按一下**確定**。

2 核發註冊代理程式憑證：

a 在憑證主控台上，展開主控台根樹狀結構，以滑鼠右鍵按一下**個人**資料夾，並選取**所有工作 > 要求新憑證**。

b 在憑證註冊精靈中，接受預設值，直到進入 [要求憑證] 頁面。

c 在 [要求憑證] 頁面上，選取**註冊代理程式 (電腦)** 核取方塊並按一下**註冊**。

d 接受其他精靈頁面上的預設值，並按一下最後一頁上的**完成**。

在 MMC 主控台中，如果展開**個人**資料夾並在左窗格中選取**憑證**，您會看到右窗格中列出新憑證。

3 安裝註冊伺服器：

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

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

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

b 按兩下安裝程式檔案以啟動精靈，並依照提示進行，直到進入 [安裝選項] 頁面。

c 在 [安裝選項] 頁面上，選取 **Horizon 7 註冊伺服器**並選擇註冊伺服器執行個體的驗證模式，然後按**下一步**。

選項	說明
Horizon 7	設定 Horizon 7 環境的驗證模式。
Horizon Cloud	設定 Horizon Cloud 環境的驗證模式。

d 依照提示完成安裝。

您必須在連接埠 32111 (TCP) 上啟用傳入連線，註冊伺服器才能運作。安裝程式預設會在安裝期間開啟連接埠。

後續步驟

- 如果在主控企業 CA 的同一部機器上安裝了註冊伺服器，請設定註冊伺服器為優先使用本機 CA。請參閱註冊伺服器組態設定。或者，如果您安裝並設定不只一部註冊伺服器，則可將連線伺服器設定為在註冊伺服器間啟用負載平衡。請參閱連線伺服器組態設定。
- 將連線伺服器與註冊伺服器配對。請參閱匯出註冊服務用戶端憑證。

匯出註冊服務用戶端憑證

若要完成配對，您可以使用 MMC 憑證嵌入式管理單元，匯出叢集中某個連線伺服器所自動產生的自我簽署註冊服務用戶端憑證。此憑證稱為用戶端憑證，因為連線伺服器是註冊伺服器提供之註冊服務的用戶端。

當 VMware Horizon 連線伺服器提示註冊伺服器為 Active Directory 使用者核發短期憑證時，註冊服務必須信任 VMware Horizon View 連線伺服器。因此，VMware Horizon 連線伺服器叢集或網繭必須與註冊伺服器配對。

安裝 Horizon 7 或更新版本的連線伺服器並啟動 VMware Horizon 連線伺服器服務時，註冊服務用戶端憑證就會自動建立。憑證會透過 View LDAP 散佈給稍後新增至叢集的其他 Horizon 7 連線伺服器。隨後會將憑證儲存至電腦上 Windows 憑證存放區的自訂容器 (`VMware Horizon View Certificates\Certificates`) 中。

必要條件

確認您有 Horizon 7 或更新版本的連線伺服器。如需安裝指示，請參閱 《Horizon 7 安裝》。如需升級指示，請參閱 《Horizon 7 升級》。

重要 客戶可以使用自己的憑證來進行配對，而非使用連線伺服器建立的自我產生憑證。若要執行此作業，請將偏好的憑證 (以及關聯的私密金鑰) 放入連線伺服器機器上 Windows 憑證存放區的自訂容器 (`VMware Horizon View Certificates\Certificates`) 中。接著必須將憑證的易記名稱設定為 **`vdm.ec.new`**，並重新啟動伺服器。叢集中的其他伺服器會從 LDAP 擷取此憑證。接著您可以執行此程序中的步驟。

程序

1. 在叢集的其中一部連線伺服器機器上，將憑證嵌入式管理單元新增到 MMC 中：
   a. 開啟 MMC 主控台並選取**檔案 > 新增/移除嵌入式管理單元**
   b. 在**可用的嵌入式管理單元**下方，選取**憑證**然後按一下**新增**。
   c. 在 [憑證嵌入式管理單元] 視窗中，選取**電腦帳戶**、按**下一步**，然後按一下**完成**。
   d. 在 [新增或移除嵌入式管理單元] 視窗中，按一下**確定**。
2. 在 MMC 主控台的左窗格中，展開 **VMware Horizon View 憑證**資料夾並選取**憑證**資料夾。
3. 在右窗格中，以滑鼠右鍵按一下具有易記名稱 **vdm.ec** 的憑證檔案，並選取**所有工作 > 匯出**。

4 在憑證匯出精靈中，接受預設值，包括保持選取**否，不要匯出私密金鑰**選項按鈕。

5 當系統提示您命名檔案時，請輸入檔案名稱，例如 **EnrollClient** (表示註冊服務用戶端憑證)，接著依照提示完成匯出憑證。

後續步驟

將憑證匯入註冊伺服器。請參閱在註冊伺服器上匯入註冊服務用戶端憑證。

在註冊伺服器上匯入註冊服務用戶端憑證

若要完成配對程序，請使用 MMC 憑證嵌入式管理單元，將註冊服務用戶端憑證匯入註冊伺服器。您必須在每部註冊伺服器上執行此程序。

必要條件

- 確認您有 Horizon 7 或更新版本的註冊伺服器。請參閱安裝和設定註冊伺服器。
- 確認您有正確的憑證以供匯入。您可以使用自己的憑證，也可以使用從叢集中某個連線伺服器所自動產生的自我簽署註冊服務用戶端憑證，如匯出註冊服務用戶端憑證所述。

  重要 若要使用自己的憑證進行配對，請將偏好的憑證 (以及關聯的私密金鑰) 放入連線伺服器機器上 Windows 憑證存放區的自訂容器 (`VMware Horizon View Certificates\Certificates`) 中。接著必須將憑證的易記名稱設定為 **vdm.ec.new**，並重新啟動伺服器。叢集中的其他伺服器會從 LDAP 擷取此憑證。接著您可以執行此程序中的步驟。

  如果您擁有自己的用戶端憑證，則必須複製到註冊伺服器的憑證是用來產生用戶端憑證的根憑證。

程序

1 將適當的憑證檔案複製到註冊伺服器機器。

  若要使用自動產生的憑證，請從連線伺服器複製註冊服務用戶端憑證。若要使用自己的憑證，請複製用來產生用戶端憑證的根憑證。

2 在註冊伺服器上，將憑證嵌入式管理單元新增到 MMC：

  a 開啟 MMC 主控台並選取**檔案 > 新增/移除嵌入式管理單元**

  b 在**可用的嵌入式管理單元**下方，選取**憑證**然後按一下**新增**。

  c 在 [憑證嵌入式管理單元] 視窗中，選取**電腦帳戶**、按**下一步**，然後按一下**完成**。

  d 在 [新增或移除嵌入式管理單元] 視窗中，按一下**確定**。

3 在 MMC 主控台的左窗格中，以滑鼠右鍵按一下 **VMware Horizon View 註冊伺服器信任根目錄**資料夾並選取**所有工作 > 匯入**。

4 在憑證匯入精靈中，依照提示瀏覽並開啟 **EnrollClient** 憑證檔案。

5 依照提示進行，並接受預設值以完成憑證的匯入作業。

6 以滑鼠右鍵按一下匯入的憑證，並增加易記名稱，例如 **vdm.ec** (代表註冊用戶端憑證)。

VMware 建議您使用可識別 Horizon 7 叢集的易記名稱，不過您也可以使用有助於輕鬆識別用戶端憑證的任何名稱。

後續步驟

設定用於委派驗證給 VMware Identity Manager 的 SAML 驗證器。請參閱設定 SAML 驗證來與 True SSO 搭配使用。

設定 SAML 驗證來與 True SSO 搭配使用

在 Horizon 7 推出 True SSO 功能後，使用者可以使用智慧卡、RADIUS 或 RSA SecurID 驗證登入 VMware Identity Manager 2.6 和更新版本，而且即使是第一次啟動遠端桌面平台或應用程式，也不會再收到提供 Active Directory 認證的提示。

在舊版中，SSO (Single Sign-On) 的運作方式是在使用者首次啟動遠端桌面平台或已發佈的應用程式，但先前未使用 Active Directory 認證通過驗證時，提示使用者提供 Active Directory 認證。然後系統會快取認證，讓使用者在後續啟動時不必再重新輸入認證。使用 True SSO 將會建立和使用短期憑證而非 AD 認證。

雖然用於設定 VMware Identity Manager 之 SAML 驗證的程序並未改變，但 True SSO 多了一個步驟。您必須設定 VMware Identity Manager，才能啟用 True SSO。

備註 如果您的部署包含多個連線伺服器執行個體，則必須建立 SAML 驗證器與每個執行個體的關聯。

必要條件

- 確認已將 Single Sign-On 啟用為全域設定。在 Horizon Administrator 中，選取**組態 > 全域設定**，並驗證已將 **Single Sign-On (SSO)** 設定為**已啟用**。
- 確認已安裝和設定 VMware Identity Manager。請參閱 VMware Identity Manager 說明文件，網址為 https://docs.vmware.com/tw/VMware-Identity-Manager/index.html。
- 確認用於 SAML 伺服器憑證之簽署 CA 的根憑證已安裝在連線伺服器主機上。VMware 建議您不要將 SAML 驗證器設定為使用自我簽署憑證。請參閱《Horizon 7 安裝》文件中〈設定 Horizon 7 Server 的 SSL 憑證〉一章中的〈將根憑證和中繼憑證匯入 Windows 憑證存放區〉。
- 記下 VMware Identity Manager 伺服器執行個體的 FQDN。

程序

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

2 在**連線伺服器**索引標籤上，選取要與 SAML 驗證器建立關聯的伺服器執行個體，然後按一下**編輯**。

3 在**驗證**索引標籤上，從**將驗證委派給 VMware Horizon (SAML 2.0 驗證器)** 下拉式功能表中選取**允許**或**必要**。

您可以依據需求，將部署中的每個連線伺服器執行個體設定為具有不同的 SAML 驗證設定。

4 按一下**管理 SAML 驗證器**後，按一下**新增**。

5 在 [新增 SAML 2.0 驗證器] 對話方塊中設定 SAML 驗證器。

選項	說明
標籤	您可以使用 VMware Identity Manager 伺服器執行個體的 FQDN。
說明	(選用) 您可以使用 VMware Identity Manager 伺服器執行個體的 FQDN。
中繼資料 URL	用於擷取在 SAML 身分識別提供者與 Horizon Connection Server 執行個體之間交換 SAML 資訊所需之全部資訊的 URL。在 URL `https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml` 中，按一下 **<您的 Horizon Server 名稱>** 並將其更換為 VMware Identity Manager 伺服器執行個體的 FQDN。
管理 URL	用於存取 SAML 身分識別提供者 (VMware Identity Manager 執行個體) 之管理主控台的 URL。此 URL 的格式是 **`https://<Identity-Manager-FQDN>:8443`**。

6 按一下**確定**以儲存 SAML 驗證器組態。

如果已提供有效資訊，則必須接受自我簽署憑證 (不建議) 或針對 Horizon 7 和 VMware Identity Manager 使用受信任的憑證。

SAML 2.0 驗證器下拉式功能表將顯示新建立的驗證器，該驗證器現已設定為選取的驗證器。

7 在 Horizon Administrator 儀表板上的 [系統健全狀況] 區段中，選取**其他元件 > SAML 2.0 驗證器**，選取已新增的 SAML 驗證器，並驗證詳細資料。

如果設定成功，則驗證器的健全狀況將顯示綠色。如果憑證不受信任、VMware Identity Manager 服務無法使用，或中繼資料 URL 無效，則驗證器的健全狀況將顯示紅色。如果憑證不受信任，您可以按一下**驗證**來驗證並接受此憑證。

8 登入 VMware Identity Manager 管理主控台，從**類別目錄 > 虛擬應用程式**頁面導覽至桌面平台集區，然後選取 **True SSO 已啟用**核取方塊。

後續步驟

- 延長連線伺服器中繼資料的到期期限，使遠端工作階段不會在 24 小時後即終止。請參閱在連線伺服器上變更服務提供者中繼資料的到期期限。
- 使用 `vdmutil` 命令列介面在連線伺服器上設定 True SSO。請參閱設定 Horizon 連線伺服器使用 True SSO。

如需 SAML 驗證運作方式的詳細資訊，請參閱 使用 SAML 驗證。

設定 Horizon 連線伺服器使用 True SSO

您可以使用 `vdmutil` 命令列介面來設定及啟用或停用 True SSO。

此程序只需在叢集的其中一個連線伺服器上執行。

重要 此程序只會使用要啟用 True SSO 所必須用到的命令。如需可用於管理 True SSO 組態之所有組態選項的清單及各個選項的說明，請參閱 用於設定 True SSO 的命令列參考。

必要條件

- 確認可以具有管理員角色的使用者身分執行命令。您可以使用 Horizon Administrator，將管理員角色指派給使用者。請參閱第 6 章 設定角色型委派管理。
- 確認您擁有下列伺服器的完整網域名稱 (FQDN)：
  - 連線伺服器
  - 註冊伺服器

    如需詳細資訊，請參閱安裝和設定註冊伺服器。
  - 企業憑證授權機構

    如需詳細資訊，請參閱設定企業憑證授權機構。
- 確認您有網域的 Netbios 名稱或 FQDN。
- 請確認您已建立憑證範本。請參閱建立與 True SSO 搭配使用的憑證範本。
- 確認您已建立 SAML 驗證器以將驗證委派給 VMware Identity Manager。請參閱設定 SAML 驗證來與 True SSO 搭配使用。

程序

1 在叢集的某個連線伺服器上，開啟命令提示字元，然後輸入命令來新增註冊伺服器。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --environment --add --enrollmentServer enroll-server-fqdn
```

註冊伺服器隨即新增到全域清單中。

2 輸入命令來列出該註冊伺服器的資訊。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn
```

命令的輸出會顯示樹系名稱、註冊伺服器的憑證是否有效、可使用之憑證範本的名稱和詳細資料，以及憑證授權機構的一般名稱。若要設定註冊伺服器可連線到的網域，可在註冊伺服器上使用 [Windows 登錄] 設定。預設是連線到所有信任的網域。

重要 您必須在下一個步驟中指定憑證授權機構的一般名稱。

3 輸入命令以建立用來保存組態資訊的 True SSO 連接器，並啟用連接器。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --create --connector --domain domain-fqdn --template TrueSSO-template-name --
primaryEnrollmentServer enroll-server-fqdn --certificateServer ca-common-name --mode enabled
```

在此命令中，*TrueSSO-template-name* 是上一個步驟的輸出中所顯示範本的名稱，而 *ca-common-name* 則是該輸出中所顯示之企業憑證授權機構的一般名稱。

指定網域的集區或叢集上已啟用 True SSO 連接器。若要在集區層級停用 True SSO，請執行 `vdmUtil --certsso --edit --connector <domain> --mode disabled`。若要停用個別虛擬機器的 True SSO，您可以使用 GPO (vdm_agent.adm)。

4 輸入命令來探索可使用的 SAML 驗證器。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --list --authenticator
```

當您使用 Horizon Administrator 設定 VMware Identity Manager 和連線伺服器之間的 SAML 驗證時，即會建立驗證器。

輸出中會顯示驗證器名稱並顯示是否已啟用 True SSO。

重要 您必須在下一個步驟中指定驗證器名稱。

5 輸入命令啟用驗證器，以使用 True SSO 模式。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --authenticator --edit --name authenticator-fqdn --truessoMode {ENABLED|ALWAYS}
```

針對 `--truessoMode`，若您只想在使用者已登入 VMware Identity Manager 但未提供密碼的情況下使用 True SSO，請使用 `ENABLED`。在此案例中，若已使用並快取密碼，系統將會使用該密碼。若在使用者已登入 VMware Identity Manager 且已提供密碼的情況下，您仍想使用 True SSO，請將 `--truessoMode` 設為 `ALWAYS`。

後續步驟

在 Horizon Administrator 中，確認 True SSO 組態的健全狀況狀態。如需詳細資訊，請參閱使用系統健全狀況儀表板來疑難排解與 True SSO 有關的問題。

若要設定進階選項，請在合適的系統上使用 Windows 進階設定。請參閱 True SSO 的進階組態設定。

用於設定 True SSO 的命令列參考

您可以使用 vdmutil 命令列介面來設定和管理 True SSO 功能。

公用程式的位置

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。

語法和驗證

在 Windows 命令提示字元中使用 `vdmutil` 命令的下列格式。

```
vdmutil authentication options --truesso additional options and arguments
```

可使用的其他選項視命令選項而定。本主題的重點是用於設定 True SSO (--truesso) 的選項。以下命令範例會列出已設定 True SSO 的連接器：

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --list --connector
```

vdmutil 命令包括指定要用於驗證的使用者名稱、網域和密碼的驗證選項。

表 5-1. vdmutil 命令驗證選項

選項	描述
--authAs	Horizon 7 管理員使用者的名稱。請勿使用 *domain\username* 或使用者主體名稱 (UPN) 格式。
--authDomain	--authAs 選項中指定之 Horizon 7 管理員使用者的完整網域名稱或網域的 Netbios 名稱。
--authPassword	在 Horizon 7 選項中指定的 --authAs 管理員使用者的密碼。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。

您必須使用驗證選項搭配除 --help 和 --verbose 之外的所有 vdmutil 命令選項。

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。

用於管理註冊伺服器的命令

您必須為每個網域新增一個註冊伺服器。您也可以新增第二個註冊伺服器，並於稍後指定該伺服器作為備用伺服器。

為了方便閱讀，下表中顯示的選項並非您需要輸入的完整命令。以下內容只包含特殊工作的專用選項。舉例來說，下表中有一列顯示 --environment --list --enrollmentServers 選項，但您實際要輸入的 vdmUtil 命令也包含用於驗證的選項以及用於指定您要設定 True SSO 的選項：

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --
truesso --environment --list --enrollmentServers
```

如需驗證選項的詳細資訊，請參閱 用於設定 True SSO 的命令列參考。

表 5-2. 用於管理註冊伺服器的 vdmutil truesso 命令選項

命令和選項	描述
--environment --add --enrollmentServer *enroll-server-fqdn*	將指定註冊伺服器新增至環境中，其中 *enroll-server-fqdn* 是註冊伺服器的 FQDN。若該註冊伺服器早已新增，執行此命令將不會有任何反應。
--environment --remove --enrollmentServer *enroll-server-fqdn*	從環境中移除指定註冊伺服器，其中 *enroll-server-fqdn* 是註冊伺服器的 FQDN。若該註冊伺服器早已移除，執行此命令將不會有任何反應。
--environment --list --enrollmentServers	列出環境中所有註冊伺服器的 FQDN。

表 5-2. 用於管理註冊伺服器的 vdmutil truesso 命令選項 (續)

命令和選項	描述
`--environment --list --enrollmentServer` *enroll-server-fqdn*	列出註冊伺服器所隸屬之網域和樹系信任的網域和樹系的 FQDN，以及註冊憑證的狀態 (可以是 VALID 或 INVALID)。VALID 代表註冊伺服器已安裝註冊代理程式憑證。狀態可能為 INVALID 的原因則有以下幾種： ■ 尚未安裝憑證。 ■ 憑證仍無效或已到期。 ■ 憑證並非由受信任的企業 CA 所發行。 ■ 私密金鑰無法使用。 ■ 憑證已損毀。 註冊伺服器的記錄檔可提供 INVALID 狀態的原因。
`--environment --list --enrollmentServer` *enroll-server-fqdn* `--domain` *domain-fqdn*	針對指定網域中的註冊伺服器，列出可用憑證授權單位的 CN (一般名稱)，並提供下列可用於 True SSO 之各憑證範本的相關資訊：名稱、最小金鑰長度和雜湊演算法。

用於管理連接器的命令

您可以為每個網域建立一個連接器。連接器會定義用於 True SSO 的參數。

為了方便閱讀，下表中顯示的選項並非您需要輸入的完整命令。以下內容只包含特殊工作的專用選項。舉例來說，下表中有一列顯示 `--list --connector` 選項，但您實際要輸入的 `vdmUtil` 命令也包含用於驗證的選項以及用於指定您要設定 True SSO 的選項：

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --
truesso --list --connector
```

如需驗證選項的詳細資訊，請參閱 用於設定 True SSO 的命令列參考。

表 5-3. 用於管理連接器的 vdmutil truesso 命令選項

選項	描述
`--create --connector --domain` *domain-fqdn* `--template` *template-name* `--primaryEnrollmentServer` *enroll-server1-fqdn* [`--secondaryEnrollmentServer`*enroll-server2-fqdn*] `--certificateServer`*CA-common-name*`--mode{enabled |disabled}`	為指定網域建立連接器，並設定連接器讓其使用以下設定： ■ *template-name* 是要使用之憑證範本的名稱。 ■ *enroll-server1-fqdn* 是要使用之主要註冊伺服器的 FQDN。 ■ *enroll-server2-fqdn* 是要使用之次要註冊伺服器的 FQDN。此設定為選用。 ■ *CA-common-name* 是要使用之憑證授權單位的一般名稱。這可以是以逗號分隔的 CA 清單。 若要確定特定註冊伺服器可以使用的憑證範本和憑證授權單位，您可以執行 `vdmutil` 命令並搭配 `--truesso --environment --list --enrollmentServer`*enroll-server-fqdn*`--domain` *domain-fqdn* 選項。
`--list --connector`	列出已建立連接器之網域的 FQDN。

表 5-3. 用於管理連接器的 vdmutil truesso 命令選項 (續)

選項	描述
`--list --connector --verbose`	列出具有連接器的所有網域，並針對每個連接器提供下列資訊： ■ 主要註冊伺服器 ■ 次要註冊伺服器 (若有) ■ 憑證範本的名稱 ■ 連接器已啟用還是停用 ■ 一個或多個 (若不只一個) 憑證授權單位伺服器的一般名稱
`--edit --connector` *domain-fqdn* [`--template`*template-name*] [`--mode{enabled |disabled`] [`--primaryEnrollmentServer`*enroll-server1-fqdn*] [`--secondaryEnrollmentServer`*enroll-server2-fqdn*] [`--certificateServer`*CA-common-name*]	針對為 *domain-fqdn* 所指定之網域所建立的連接器，可讓您變更下列任何一項設定： ■ *template-name* 是要使用之憑證範本的名稱。 ■ 模式可以是 `enabled` 或 `disabled`。 ■ *enroll-server1-fqdn* 是要使用之主要註冊伺服器的 FQDN。 ■ *enroll-server2-fqdn* 是要使用之次要註冊伺服器的 FQDN。此設定為選用。 ■ *CA-common-name* 是要使用之憑證授權單位的一般名稱。這可以是以逗號分隔的 CA 清單。
`--delete --connector` *domain-fqdn*	刪除已為 *domain-fqdn* 所指定之網域建立的連接器。

用於管理驗證器的命令

當您設定 VMware Identity ManagerHorizon 7 和連線伺服器之間的 SAML 驗證時，即會建立驗證器。驗證器唯一的管理工作就是啟用或停用 True SSO。

為了方便閱讀，下表中顯示的選項並非您需要輸入的完整命令。以下內容只包含特殊工作的專用選項。舉例來說，下表中有一列顯示 `--list --authenticator` 選項，但您實際要輸入的 `vdmUtil` 命令也包含用於驗證的選項以及用於指定您要設定 True SSO 的選項：

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --
truesso --list --authenticator
```

如需驗證選項的詳細資訊，請參閱 用於設定 True SSO 的命令列參考。

表 5-4. 用於管理驗證器的 vdmutil truesso 命令選項

命令和選項	說明
`--list --authenticator [--verbose]`	列出網域中找到之所有 SAML 驗證器的完整網域名稱 (FQDN)。針對每個驗證器，指定是否要啟用 True SSO。若您使用 `--verbose` 選項，則也會列出相關聯連線伺服器的 FQDN。
`--list --authenticator --name` *label*	針對指定驗證器，列出是否已啟用 True SSO，並列出相關聯連線伺服器的 FQDN。針對 *label*，請在您使用 `--authenticator` 選項但未使用 `--name` 選項時使用其中一個列出的名稱。
`--edit --authenticator --name` *label* `--truessoMode` *mode-value*	針對指定驗證器，將 True SSO 模式設為您指定的值，其中 *mode-value* 可以是下列其中一個值： ■ `ENABLED`。只有在使用者的 Active Directory 認證無法使用時，才會使用 True SSO。 ■ `ALWAYS`。即使 vIDM 具有使用者的 AD 認證，也一律會使用 True SSO。 ■ `DISABLED`。True SSO 已停用。 針對 *label*，請在您使用 `--authenticator` 選項但未使用 `--name` 選項時使用其中一個列出的名稱。

True SSO 的進階組態設定

您可以透過使用 Horizon Agent 機器上的 GPO 範本、註冊伺服器上的登錄設定，以及連線伺服器上的 LDAP 項目來管理 True SSO 進階設定。這些設定包括預設逾時、設定負載平衡、指定要併入的網域等等。

Horizon Agent 組態設定

您可使用代理程式作業系統上的 GPO 範本來關閉集區層級的 True SSO，或變更憑證設定的預設值，例如金鑰大小、計數以及重新連線嘗試次數的設定。

備註　下表顯示用於設定個別虛擬機器上代理程式的設定，但您也可以使用 Horizon Agent 組態範本檔。ADMX 範本檔名為 (`vdm_agent.admx`)。使用範本檔可讓這些原則設定套用於桌面平台或應用程式集區中的所有虛擬機器。如果設定原則，原則的優先順序將高於登錄設定。

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 5-5. 用於在 Horizon Agent 上設定 True SSO 的機碼

機碼	最小值與最大值	說明
`Disable True SSO`	N/A	將此機碼設定為 **`true`** 可停用代理程式上的功能。在群組原則中使用此設定可在集區層級停用 True SSO。預設值為 **`false`**。
`Certificate wait timeout`	10 - 120	指定憑證到達代理程式的逾時期間，以秒為單位。預設值為 **`40`**。
`Minimum key size`	1024 - 8192	金鑰的最小允許大小。預設值為 **`1024`**，表示依預設，如果金鑰大小小於 1024，則不能使用該金鑰。

表 5-5. 用於在 Horizon Agent 上設定 True SSO 的機碼 (續)

機碼	最小值與最大值	說明
`All key sizes`	N/A	可使用之金鑰大小的逗號分隔清單。最多可指定 5 個大小，例如：**`1024,2048,3072,4096`**。預設值為 **`2048`**。
`Number of keys to pre-create`	1 - 100	在提供遠端桌面平台和主控 Windows 應用程式的 RDS 伺服器上，預先建立的金鑰數目。預設值為 **`5`**。
`Minimum validity period required for a certificate`	N/A	重複使用某個憑證來重新連線使用者時所需的最短有效期間 (以分鐘為單位)。預設值為 **`5`**。

註冊伺服器組態設定

您可使用註冊伺服器作業系統上的 Windows 登錄設定，來設定要連線至哪些網域、各種逾時期間、輪詢期間、重試次數，以及是否偏好使用相同本機伺服器上安裝的憑證授權機構 (建議使用)。

若要變更進階組態設定，請開啟註冊伺服器機器上的 Windows 登錄編輯程式 (`regedit.exe`) 並瀏覽至下列登錄機碼：

```
HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service
```

表 5-6. 用於在註冊伺服器上設定 True SSO 的登錄機碼

登錄機碼	最小值與最大值	類型	說明
`ConnectToDomains`	N/A	REG_MULTI_SZ	註冊伺服器會自動嘗試連線的網域清單。對於這個多字串登錄類型，每個網域的 DNS 完整網域名稱 (FQDN) 會各以單獨一行列出。 預設是信任所有網域。
`ExcludeDomains`	N/A	REG_MULTI_SZ	註冊伺服器不會自動連線的網域清單。如果連線伺服器有提供含有任何網域的組態集，註冊伺服器會嘗試連線至該網域。對於這個多字串登錄類型，每個網域的 DNS FQDN 會各以單獨一行列出。 預設是不排除任何網域。
`ConnectToDomainsInForest`	N/A	REG_SZ	指定是否連線至並使用註冊伺服器所屬樹系中的所有網域。預設值是 TRUE。 使用下列其中一個值： ■ **`0`** 表示 false；不連線至所使用樹系的網域。 ■ **`!=0`** 表示 true。
`ConnectToTrustingDomains`	N/A	REG_SZ	指定是否連線至明確信任/傳入的網域。預設值是 TRUE。 使用下列其中一個值： ■ **`0`** 表示 false；不連線至明確信任/傳入的網域。 ■ **`!=0`** 表示 true。

表 5-6. 用於在註冊伺服器上設定 True SSO 的登錄機碼 (續)

登錄機碼	最小值與最大值	類型	說明
PreferLocalCa	N/A	REG_SZ	指定是否偏好本機安裝的 CA (若可用) 以提升效能。若設為 TRUE，註冊伺服器會傳送要求至本機 CA。如果連線至本機 CA 失敗，註冊伺服器會嘗試傳送憑證要求至替代 CA。預設值為 FALSE。 使用下列其中一個值： ■ **0** 表示 false。 ■ **!=0** 表示 true。
MaxSubmitRetryTime	9500-59000	DWORD	重試提交憑證簽署要求前等候的時間量，單位為毫秒。預設值為 **25000**。
SubmitLatencyWarningTime	500 - 5000	DWORD	介面標示為「降級」時，提交延遲警告時間 (單位為毫秒)。預設值為 **1500**。 註冊伺服器使用此設定來判定是否應將 CA 視為降級狀態。如果最後三個憑證要求完成的時間超過此設定指定的毫秒數，則會將此 CA 視為降級，並在 Horizon Administrator [健全狀況狀態] 儀表板中顯示此狀態。 CA 通常會在 20 毫秒內發出憑證，但如果 CA 已閒置數小時，則任何初始要求可能需要更長時間才能完成。此設定可讓管理員找出某個 CA 過慢，但無需將 CA 標示為緩慢。使用此設定可設定將 CA 標示為緩慢的臨界值。
WarnForLonglivedCert	N/A	REG_SZ	停用長時間執行之 True SSO 憑證 (範本) 的警告。預設值是 **True**。 如果憑證存留期設定為大於 14 天，註冊伺服器會在 Horizon Administrator [健全狀況狀態] 儀表板中顯示警告狀態，報告 True SSO 範本處於已降級或非最佳狀態。註冊伺服器會使用此設定來停用警告。 註冊伺服器必須重新啟動，此設定才會生效。

連線伺服器組態設定

您可以在連線伺服器上編輯 View LDAP 以設定用於產生憑證的逾時，以及是否要啟用註冊伺服器之間的負載平衡憑證要求 (建議)。

若要變更進階組態設定，您必須在連線伺服器主機上使用 ADSI Edit。您可以輸入辨別名稱 **DC=vdi, DC=vmware, DC=int** 做為連線點，並輸入電腦 **localhost:389** 的伺服器名稱和連接埠，來進行連線。在右窗格中展開 **OU=Properties**、選取 **OU=Global**，然後按兩下 **CN=Common**。

然後，您就可以編輯 **pae-NameValuePair** 屬性來新增下表所列的一個或多個值。在新增值時，您必須使用語法 *name=value*。

表 5-7. 連線伺服器的進階 True SSO 設定

登錄機碼	說明
`cs-view-certsso-enable-es-loadbalance=[true|false]`	指定是否要在兩台註冊伺服器之間啟用負載平衡 CSR 要求。預設值為 false。 例如，新增 `cs-view-certsso-enable-es-loadbalance=true` 以啟用負載平衡，以便在憑證要求抵達時，連線伺服器會使用替代註冊伺服器。若註冊伺服器和 CA 位於相同主機上，每個註冊伺服器皆可使用本機 CA 來服務要求。
`cs-view-certsso-certgen-timeout-sec=`*number*	在收到 CSR 後，等候產生憑證的時間量，以秒為單位。預設值為 **35**。

識別沒有 AD UPN 的 AD 使用者

您可以為連線伺服器設定 LDAP URL 篩選器，以識別沒有 AD UPN 的 AD 使用者。

您必須在連線伺服器主機上使用 ADAM ADSI Edit。您可以藉由輸入辨別名稱 **DC=vdi, DC=vmware, DC=int** 來進行連線。展開 **OU=Properties**，然後選取 **OU=Authenticator**。

接著，您可以編輯 **pae-LDAPURLList** 屬性以新增 LDAP URL 篩選器。

例如，您可以新增下列篩選器：

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(telephoneNumber=$NAMEID)
```

連線伺服器會使用下列預設 LDAP URL 篩選器：

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(&(objectCategory=user)
(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???(&(objectCategory=group)
(objectclass=group)(sAMAccountName=$NAMEID))
```

```
urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified=ldap:///???(&(objectCategory=user)
(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???(&(objectCategory=group)
(objectclass=group)(sAMAccountName=$NAMEID))
```

如果您設定 LDAP URL 篩選器，連線伺服器就會使用此 LDAP URL 篩選器，而不會使用預設 LDAP URL 篩選器來識別使用者。

您可以用於沒有 AD UPN 的 AD 使用者之 SAML 驗證的識別碼範例：

- `"cn"`
- `"mail"`
- `"description"`
- `"givenName"`
- `"sn"`
- `"canonicalName"`
- `"sAMAccountName"`
- `"member"`
- `"memberOf"`

- "distinguishedName"
- "telephoneNumber"
- "primaryGroupID"

使用 True SSO 和 Workspace ONE 解除鎖定桌面平台

使用者使用 True SSO 登入桌面平台後，可在重新驗證後，從 Workspace ONE 入口網站使用相同的登入認證將桌面平台解除鎖定。

必要條件

- 確認您擁有 Horizon 7 7.8 版或更新版本。
- 確認您擁有 Windows 版 Horizon Client 5.0 或更新版本。
- 確認您擁有 VMware Identity Manager 19.03 版或更新版本。

程序

1. 啟用 Workspace ONE，並將其設定為與連線伺服器搭配使用。

   請參閱 Workspace ONE 說明文件網頁上的 Workspace ONE 說明文件。

2. 設定 Horizon 連線伺服器以使用 True SSO。

   請參閱設定 Horizon 連線伺服器使用 True SSO。

3. 若要啟動虛擬或已發佈的桌面平台，請在 Workspace ONE 模式下連線至已設定 True SSO 的連線伺服器。請參閱 VMware Horizon Client 說明文件網頁上的 Horizon Client 說明文件。

4. 從 Workspace ONE 入口網站啟動虛擬或已發佈的桌面平台，讓使用者可透過 True SSO 使用單一登入。

5. 鎖定桌面平台。

6. 若要解除鎖定桌面平台，請選取 **VMware True SSO 使用者**，然後按一下**提交**。

後續步驟

您可以在安裝 Horizon Agent 的機器上設定登錄機碼以停用此功能，位置如下：

```
HKLM\Software\VMware, Inc.\VMware VDM\Agent\CertSSO[DisableCertSSOUnlock=true]
```

您也可以在 Windows 版 Horizon Client 上設定登錄機碼 `DisabledFeatures=TrueSSOUnlock` 以停用此功能，位置如下：

- 在 Windows 32 位元作業系統上：`[HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client]` 或 `[HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client]`。
- 在 Windows 64 位元作業系統上： `[HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client]` 或 `[HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client]`。

如果已設定此登錄機碼，當使用者解除鎖定桌面平台時，就不會顯示 **VMware True SSO 使用者**選項。

使用系統健全狀況儀表板來疑難排解與 True SSO 有關的問題

您可以使用 Horizon Administrator 中的系統健全狀況儀表板，以快速查看可能會影響 True SSO 功能的作業問題。

對於使用者而言，若在系統嘗試為使用者登入至遠端桌面平台或應用程式時 True SSO 停止運作，使用者會看見以下訊息：「使用者名稱或密碼不正確。」在按一下**確定**後，使用者就會看見登入畫面。使用者會在 Windows 登入畫面看到額外的動態磚，其標籤為 **VMware SSO 使用者**。若使用者擁有的 Active Directory 認證為具備權利的使用者所屬，使用者就能夠使用 AD 認證來登入。

系統健全狀況儀表板位於 Horizon Administrator 顯示畫面的左上部分，其中包含幾個與 True SSO 有關的項目。

備註　True SSO 功能每分鐘僅提供一次資訊給儀表板。按一下右上角的重新整理圖示，則可立即重新整理資訊。

- 您可以按一下以展開 **View 元件 > True SSO**，查看正在使用 True SSO 的網域清單。

  您可以按一下網域名稱，查看下列資訊：為該網域設定的註冊伺服器清單、企業憑證授權機構清單、正在使用的憑證範本名稱，以及狀態。若有任何問題，[狀態] 欄位會說明問題的內容。

  若要將 [True SSO 網域詳細資料] 對話方塊中顯示的任何組態設定予以變更，請使用 `vdmutil` 命令列介面來編輯 True SSO 連接器。如需詳細資訊，請參閱用於管理連接器的命令。
- 您可以按一下以展開**其他元件 > SAML 2.0 驗證器**，來查看用於將驗證委派給 VMware Identity Manager 執行個體所建立的 SAML 驗證器清單。您可以按一下驗證器名稱來檢查詳細資料和狀態。

備註　為能使用 True SSO，必須啟用 SSO 的全域設定。在 Horizon Administrator 中，選取**組態 > 全域設定**，並驗證已將 **Single Sign-On (SSO)** 設定為**已啟用**。

表 5-8. 連線伺服器到註冊伺服器連線狀態

狀態文字	說明
無法提取 True SSO 健全狀況資訊。	儀表板無法從連線伺服器執行個體擷取健全狀況資訊。
True SSO 組態服務無法連絡 <FQDN> 註冊伺服器。	在網繭中，系統已選擇其中一個連線伺服器執行個體以將組態資訊傳送給網繭使用的所有註冊伺服器。此連線伺服器執行個體將會每分鐘重新整理一次註冊伺服器組態。若組態工作無法更新註冊伺服器，就會顯示此訊息。如需其他資訊，請參閱註冊伺服器連線的表格。
無法連絡 <FQDN> 註冊伺服器以管理此連線伺服器上的工作階段。	目前的連線伺服器執行個體無法連線至註冊伺服器。系統僅會針對您的瀏覽器所指向的連線伺服器執行個體顯示此狀態。若網繭中有多個連線伺服器執行個體，您需要將瀏覽器變更為指向其他連線伺服器執行個體，才能檢查其狀態。如需其他資訊，請參閱註冊伺服器連線的表格。

表 5-9. 註冊伺服器連線

狀態文字	說明
此網域 <網域名稱> 不存在於 <FQDN> 註冊伺服器上。	已將 True SSO 連接器設定為使用此網域的此註冊伺服器，但尚未將註冊伺服器設定為連線至此網域。若此狀態維持超過一分鐘，您需要檢查目前負責將註冊組態重新整理之連線伺服器執行個體的狀態。
<FQDN> 註冊伺服器對網域 <網域名稱> 的連線仍在建立。	註冊伺服器還無法連線至此網域中的網域控制站。若此狀態維持超過一分鐘，您可能需要驗證從註冊伺服器到網域的名稱解析是否正確，且註冊伺服器和網域之間存在網路連線。

表 5-9. 註冊伺服器連線 (續)

狀態文字	說明
<FQDN> 註冊伺服器與網域 <網域名稱> 的連線正在停止或處於有問題的狀態。	註冊伺服器已連線至網域中的網域控制站，但無法從網域控制站讀取 PKI 資訊。若發生此情形，則表示實際的網域控制站可能有問題。若未正確設定 DNS，也可能發生此問題。請檢查註冊伺服器上的記錄檔，來查看註冊伺服器正嘗試使用哪個網域控制站，並驗證該網域控制站是否可完整運作。
<FQDN> 註冊伺服器尚未從網域控制站讀取註冊內容。	這是過渡狀態，只會在註冊伺服器啟動期間，或在將新網域新增至環境時才會顯示。此狀態持續的時間通常少於一分鐘。若此狀態持續超過一分鐘，則表示網路非常慢，或是發生問題造成網域控制站存取不易。
<FQDN> 註冊伺服器已讀取註冊內容至少一次，但有一段時間無法連線網域控制站。	只要註冊伺服器從網域控制站讀取到 PKI 組態，其便會每兩分鐘輪詢一次看看是否有變更。若已經有一小段時間無法連線到網域控制站 (DC)，就會設定此狀態。無法連絡 DC 通常可能表示註冊伺服器無法偵測到 PKI 組態中有任何變更。只要憑證伺服器仍可存取網域控制站，就仍可核發憑證。
<FQDN> 註冊伺服器已讀取註冊內容至少一次，但有一段時間無法連線網域控制站或存在其他問題。	若註冊伺服器已經很久無法連線到網域控制站，就會顯示此狀態。註冊伺服器接著會嘗試探索此網域的替代網域控制站。若憑證伺服器仍可存取網域控制站，就仍可核發憑證，但若此狀態維持超過一分鐘，則表示註冊伺服器已失去該網域所有網域控制站的存取權，且可能無法再核發憑證。

表 5-10. 註冊憑證狀態

狀態文字	說明
此網域的 <網域名稱> 樹系的有效註冊憑證未安裝在 <FQDN> 註冊伺服器上，或可能已到期	尚未安裝此網域的任何註冊憑證，或是憑證無效或已到期。註冊憑證必須由受樹系信任的企業 CA 核發，且此網域為該樹系的成員。驗證您已完成《Horizon 7 管理》文件中的步驟，其中說明了在註冊伺服器上安裝註冊憑證的方法。您也可以開啟 MMC、憑證管理嵌入式管理單元，來開啟本機電腦存放區。開啟個人憑證容器，並驗證是否已安裝憑證，以及憑證是否有效。您也可以開啟註冊伺服器記錄檔。註冊伺服器會記錄有關其找到之任何憑證的狀態的其他資訊。

表 5-11. 憑證範本狀態

狀態文字	說明
範本 <名稱> 不存在於 <FQDN> 註冊伺服器網域上。	檢查您指定的範本名稱是否正確。
此範本產生的憑證無法用來登入至 Windows。	此範本未啟用智慧卡的使用以及資料簽署。檢查您指定的範本名稱是否正確。請驗證您已完成建立與 True SSO 搭配使用的憑證範本中所述的步驟。
範本 <名稱> 已啟用智慧卡登入，但無法使用。	此範本已啟用智慧卡登入，但範本無法與 True SSO 搭配使用。檢查您指定的範本名稱是否正確，並驗證您已執行建立與 True SSO 搭配使用的憑證範本中所述的步驟。您也可以檢查註冊伺服器記錄檔，因為它會記錄範本中的哪項設定使得範本無法用於 True SSO。

表 5-12. 憑證伺服器組態狀態

狀態文字	說明
憑證伺服器 <CA 的 CN> 不存在於網域中。	驗證您指定的 CA 名稱是否正確。您必須指定一般名稱 (CN)。
憑證未在 NTAuth (企業) 存放區。	此 CA 並非企業 CA，或其 CA 憑證尚未新增至 NTAUTH 存放區。若此 CA 並非樹系成員，您必須手動將 CA 憑證新增至此樹系的 NTAUTH 存放區。

表 5-13. 憑證伺服器連線狀態

狀態文字	說明
<FQDN> 註冊伺服器未連線至憑證伺服器 <CA 的 CN>。	註冊伺服器未連線至憑證伺服器。若註冊伺服器才剛啟動，或是最近才將 CA 新增至 True SSO 連接器，則此狀態可能是過渡狀態。若狀態維持超過一分鐘，則表示註冊伺服器無法連線至 CA。確認名稱解析可正常運作，且您具備連線至 CA 的網路連線能力，且註冊伺服器的系統帳戶有存取 CA 的權限。
<FQDN> 註冊伺服器已連線至憑證伺服器 <CA 的 CN>，但憑證伺服器處於降級狀態	若 CA 在核發憑證時速度太慢，就會顯示此狀態。若 CA 維持此狀態，請檢查 CA 或 CA 所用之網域控制站的負載。 **備註** 若 CA 已標示為緩慢，該 CA 會維持此狀態，直到已順利完成至少一個憑證要求，且該憑證是在一般時間範圍內核發出去。
<FQDN> 註冊伺服器可以連線憑證伺服器 <CA 的 CN>，但服務無法使用。	若註冊伺服器與 CA 的連線處於作用中狀態，但 CA 無法核發憑證，就會發出此狀態。此狀態通常是過渡狀態。若 CA 沒有很快就變為可用，狀態就會變為已中斷連線。

設定角色型委派管理

6

Horizon 7 環境中的一個金鑰管理工作會用來決定誰可以使用 Horizon Administrator，以及這些使用者有權執行哪些工作。有了角色型委派管理，您便可以選擇性地將管理員角色指定給特定的 Active Directory 使用者和群組，讓他們擁有管理權限。

本章節討論下列主題：

瞭解角色和權限

在 Horizon Administrator 中執行工作的能力，是由包含管理員角色和權限的存取控制系統所管理。此系統和 vCenter Server 存取控制系統類似。

管理員角色是權限的集合。權限可授予執行特定動作的能力，例如將桌面平台集區的權限授予使用者。權限也能控制管理員可在 Horizon Administrator 看到哪些內容。例如，如果管理員沒有檢視和修改全域原則的權限，則在其登入 Horizon Administrator 時，即無法在導覽面板中看到**全域原則**設定。

管理員權限為全域權限或特定物件權限。全域權限可控制全系統作業，例如檢視與變更全域設定。物件特有的權限可控制特定類型物件的作業。

管理員角色通常結合執行高階管理工作所需要的所有個別權限。Horizon Administrator 所包含的預先定義角色，具有執行一般管理工作所需要的權限。您可以將這些預先定義的角色指派給管理員使用者和群組，或是將選取的權限組合起來，以建立自己的角色。您無法修改預先定義的角色。

若要建立管理員，請在 Active Directory 使用者和群組中選取使用者和群組，然後指派管理員角色。管理員會透過其角色指派取得權限。您不能將權限直接指派給管理員。具有多個角色指派的管理員，會取得這些角色所包含的所有權限。

使用存取群組來委派集區和伺服器陣列的管理

依預設，自動桌面平台集區、手動桌面平台集區以及伺服器陣列是在根存取群組中建立，根存取群組在 Horizon Administrator 中顯示為 / 或 Root(/)。已發佈桌面平台集區和應用程式集區繼承其伺服器陣列的存取群組。您可以在根存取群組下建立存取群組，將特定集區或伺服器陣列的管理工作委派給不同的管理員。

備註 您無法直接變更已發佈桌面平台集區或應用程式集區的存取群組。您必須變更已發佈桌面平台集區或應用程式集區所屬的伺服器陣列的存取群組。

虛擬或實體機器從其桌面平台集區繼承存取群組。附加的持續性磁碟會從其機器繼承存取群組。您最多可以有 100 個存取群組，包括根存取群組。

您可以藉由在該存取群組上將角色指派給管理員，來設定管理員對存取群組中資源的存取權。管理員僅能存取位於已指派角色的存取群組中的資源。管理員對存取群組所具備的角色會決定管理員對該存取群組中資源所擁有的存取層級。

因為角色是繼承自根存取群組，所以對根存取群組具備角色的管理員對於所有存取群組也就具備了該角色。具有根存取群組上管理員角色的管理員為超級管理員，因為他們具備系統中所有物件的完整存取權。

角色必須至少包含一個可套用於存取群組的物件特定權限。僅包含全域權限的角色無法套用到存取群組。

您可以使用 Horizon Administrator 建立存取群組，並將現有的桌面平台集區移至存取群組。當您建立自動桌面平台集區、手動集區或伺服器陣列時，您可以接受預設根存取群組或選取不同的存取群組。

備註 如果您想要透過 VMware Identity Manager 提供對桌面平台與應用程式的存取，請確認您是以對 Horizon Administrator 中的根存取群組具有管理員角色的使用者身分，建立了桌面平台和應用程式集區。如果您為使用者提供的管理員角色所針對的是根存取群組之外的存取群組，則 VMware Identity Manager 將無法辨識您在 Horizon 7 中設定的 SAML 驗證器，而您也無法在 VMware Identity Manager 中設定集區。

- 不同存取群組的不同管理員

  您可以在組態中建立不同的管理員來管理每個存取群組。
- 同一個存取群組的不同管理員

  您可以建立不同的管理員以管理同一個存取群組。

不同存取群組的不同管理員

您可以在組態中建立不同的管理員來管理每個存取群組。

例如，如果您公司的桌面平台集區位於某個存取群組，而軟體開發人員的桌面平台集區位於另一個存取群組，則可以建立不同的管理員來管理每個存取群組中的資源。

表 6-1. 不同存取群組的不同管理員顯示此類組態的範例。

表 6-1. 不同存取群組的不同管理員

管理員	角色	存取群組
view-domain.com\Admin1	詳細目錄管理員	/CorporateDesktops
view-domain.com\Admin2	詳細目錄管理員	/DeveloperDesktops

在此範例中，稱為 Admin1 的管理員在 CorporateDesktops 存取群組上具有「詳細目錄管理員」角色，而稱為 Admin2 的管理員在 DeveloperDesktops 存取群組上具有「詳細目錄管理員」角色。

同一個存取群組的不同管理員

您可以建立不同的管理員以管理同一個存取群組。

例如，如果您公司的桌面平台集區位於一個存取群組，您可以建立一個可以檢視和修改該集區的管理員，並建立另一個僅能檢視集區的管理員。

表 6-2. 同一個存取群組的不同管理員顯示此類組態的範例。

表 6-2. 同一個存取群組的不同管理員

管理員	角色	存取群組
view-domain.com\Admin1	詳細目錄管理員	/CorporateDesktops
view-domain.com\Admin2	詳細目錄管理員 (唯讀)	/CorporateDesktops

在此範例中，稱為 Admin1 的管理員在 CorporateDesktops 存取群組上具有「詳細目錄管理員」角色，而稱為 Admin2 的管理員在同一個存取群組上具有「詳細目錄管理員 (唯讀)」角色。

瞭解權限

Horizon Administrator 以權限來表示角色、管理員使用者或群組，以及存取群組的組合。角色定義可執行的動作，使用者或群組指出誰可以執行動作，而存取群組則包含做為動作之目標的物件。

Horizon Administrator 中的權限，會依照您選取的是管理員使用者或群組、存取群組或角色而有所不同。

下表顯示當您選取管理員使用者或群組時，Horizon Administrator 中的權限表示方式。管理員使用者稱為 Admin 1 並具有兩項權限。

表 6-3.「管理員和群組」索引標籤上，Admin 1 的權限

角色	存取群組
詳細目錄管理員	MarketingDesktops
管理員 (唯讀)	/

第一個權限顯示 Admin 1 在稱為 MarketingDesktops 的存取群組上，具有「詳細目錄管理員」角色。第二個權限顯示 Admin 1 在根存取群組上具有「管理員 (唯讀)」角色。

下表顯示當您選取 MarketingDesktops 存取群組時，相同的權限如何顯示在 Horizon Administrator。

表 6-4.「資料夾」索引標籤上，MarketingDesktops 的權限

Admin	角色	已繼承
view-domain.com\Admin1	詳細目錄管理員	
view-domain.com\Admin1	管理員 (唯讀)	是

第一項權限和 表 6-3.「管理員和群組」索引標籤上，Admin 1 的權限 中所示的第一項權限相同。第二項權限是從 表 6-3.「管理員和群組」索引標籤上，Admin 1 的權限 中所示的第二項權限繼承而來。由於存取群組會繼承根存取群組的權限，因此 Admin1 具有 `MarketingDesktops` 存取群組的「管理員 (唯讀)」角色。若權限是繼承而來的，「繼承」欄中會顯示「是」。

下表顯示當您選取「詳細目錄管理員」角色時，表 6-3.「管理員和群組」索引標籤上，Admin 1 的權限 中的第一項權限會如何顯示在 Horizon Administrator。

表 6-5.「角色」索引標籤上，詳細目錄管理員的權限

Administrator	存取群組
view-domain.com\Admin1	`/MarketingDesktops`

管理管理員

具備管理員角色的使用者可以使用 Horizon Administrator 新增與移除管理員使用者與群組。

管理員角色是 Horizon Administrator 中最強大的角色。一開始，會將管理員角色授與 Administrator 帳戶的成員。當您安裝連線伺服器時，您需要指定 Administrators 帳戶。Administrators 帳戶可以是連線伺服器電腦上的本機管理員群組 (BUILTIN\Administrators)，或是網域使用者或群組帳戶。

備註 依預設，網域管理員群組是本機管理員群組的成員。如果您已指定 Administrators 帳戶為本機管理員群組，且您不要網域管理員擁有詳細目錄物件與 Horizon 7 組態設定的完整存取權，您必須將網域管理員群組從本機管理員群組中移除。

- 建立管理員

  若要建立管理員，您可以在 Horizon Administrator 的 Active Directory 使用者和群組中選取使用者或群組，並指派管理員角色。

- 移除管理員

  您可以移除管理員使用者或群組。您無法移除系統中的最後一個超級管理員。超級管理員是具有根存取群組上管理員角色的管理員。

建立管理員

若要建立管理員，您可以在 Horizon Administrator 的 Active Directory 使用者和群組中選取使用者或群組，並指派管理員角色。

必要條件

- 請熟悉預先定義的管理員角色。請參閱預先定義的角色和權限。
- 請熟悉建立管理員使用者和群組的最佳做法。請參閱管理員使用者及群組的最佳做法。

- 若要將自訂角色指派給管理員，請建立自訂角色。請參閱新增自訂角色。
- 若要建立可以管理特定桌面平台集區的管理員，請建立存取群組並將桌面平台集區移至該存取群組。請參閱管理和檢閱存取群組。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 管理員**。

2 在**管理員和群組**索引標籤中，按一下**新增使用者或群組**。

3 按一下**新增**，並選取一個或多個搜尋準則，然後按一下**尋找**以根據搜尋準則篩選 Active Directory 使用者或群組。

4 選取您要當作管理員使用者或群組的 Active Directory 使用者或群組，按一下**確定**，然後按**下一步**。

您可以按 Ctrl 或 Shift 鍵，選取多個使用者和群組。

5 選取角色以指派給管理員使用者或群組。

[套用到存取群組] 欄表示角色是否套用到存取群組。只有包含物件特定權限的角色才會套用至存取群組。只包含全域權限的角色不會套用至存取群組。

選項	動作
您選取的角色會套用至存取群組	選取一或多個存取群組，然後按**下一步**。
您要將角色套用至所有存取群組	選取根存取群組，然後按**下一步**。

6 按一下**完成**即可建立管理員使用者或群組。

此時新的管理員使用者或群組就會出現在左窗格中，而您所選的角色和存取群組會出現在**管理員和群組**索引標籤的右窗格中。

移除管理員

您可以移除管理員使用者或群組。您無法移除系統中的最後一個超級管理員。超級管理員是具有根存取群組上管理員角色的管理員。

程序

1 在 View Administrator 中，選取 **View 組態 > 管理員**。

2 在**管理員和群組**索引標籤上，選取管理員使用者或群組，按一下**移除使用者或群組**，再按一下**確定**。

管理員使用者或群組不再出現在**管理員和群組**索引標籤上。

管理和檢閱權限

您可以使用 Horizon Administrator 為特定管理員使用者與群組、特定角色，以及特定存取群組新增、刪除和檢閱權限。

- 新增權限

  您可以新增包含特定管理員使用者或群組、特定角色或特定存取群組的權限。

- 刪除權限

  您可以刪除包含特定管理員使用者或群組、特定角色或特定存取群組的權限。

- 檢閱權限

  您可以檢閱包含特定管理員或群組、特定角色，或特定存取群組的權限。

新增權限

您可以新增包含特定管理員使用者或群組、特定角色或特定存取群組的權限。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 管理員**。

2 建立權限。

選項	動作
建立包含特定管理員使用者或群組的權限	a 在**管理員和群組**索引標籤上，選取管理員或群組，並按一下**新增權限**。 b 選取角色。 c 如果角色不套用於存取群組，請按一下**完成**。 d 如果角色套用於存取群組，請按**下一步**，選取一或多個存取群組，然後再按一下**完成**。角色必須至少包含一個可套用於存取群組的物件特定權限。
建立包含特定角色的權限	a 在**角色**索引標籤上，選取角色，並按一下**權限**，然後按一下**新增權限**。 b 按一下**新增**，選取一個或多個搜尋準則，然後按一下**尋找**來尋找符合搜尋準則的管理員使用者或群組。 c 選取要包含在權限中的管理員使用者或群組，並按一下**確定**。您可以按 Ctrl 或 Shift 鍵，選取多個使用者和群組。 d 如果角色不套用於存取群組，請按一下**完成**。 e 如果角色套用於存取群組，請按**下一步**，選取一或多個存取群組，然後再按一下**完成**。角色必須至少包含一個可套用於存取群組的物件特定權限。
建立包含特定存取群組的權限	a 在**存取群組**索引標籤上選取存取群組，並按一下**新增權限**。 b 按一下**新增**，選取一個或多個搜尋準則，然後按一下**尋找**來尋找符合搜尋準則的管理員使用者或群組。 c 選取要包含在權限中的管理員使用者或群組，並按一下**確定**。您可以按 Ctrl 或 Shift 鍵，選取多個使用者和群組。 d 按**下一步**，選取角色，然後按一下**完成**。角色必須至少包含一個可套用於存取群組的物件特定權限。

刪除權限

您可以刪除包含特定管理員使用者或群組、特定角色或特定存取群組的權限。

如果您移除管理員使用者或群組的最後權限，該管理員使用者或群組也會移除。因為至少一個管理員必須具有根存取群組上的管理員角色，您無法移除會造成管理員移除的權限。您無法刪除繼承的權限。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 管理員**。

2 選取要刪除的權限。

選項	動作
刪除會套用至特定管理員或群組的權限	在**管理員和群組**索引標籤上選取管理員或群組。
刪除會套用至特定角色的權限	在**角色**索引標籤上選取角色。
刪除會套用至特定存取群組的權限	在**存取群組**索引標籤上選取資料夾。

3 選取權限，然後按一下**刪除權限**。

檢閱權限

您可以檢閱包含特定管理員或群組、特定角色，或特定存取群組的權限。

程序

1 選取 **View 組態 > 管理員**。

2 檢閱權限。

選項	動作
檢閱包含特定管理員或群組的權限	在**管理員和群組**索引標籤上選取管理員或群組。
檢閱包含特定角色的權限	在**角色**索引標籤上選取角色並按一下**權限**。
檢閱包含特定存取群組的權限	在**存取群組**索引標籤上選取資料夾。

管理和檢閱存取群組

您可以使用 Horizon Administrator 來新增與刪除存取群組，以及檢閱特定存取群組中的桌面平台集區與機器。

- 新增存取群組

  您可以透過建立存取群組，將特定機器、桌面平台集區或伺服器陣列委派給不同管理員管理。依預設，桌面平台集區、應用程式集區和伺服器陣列均位於根存取群組。

- 將桌面平台集區或伺服器陣列移至不同的存取群組

  在建立存取群組後，您可以將自動桌面平台集區、手動集區或伺服器陣列移至新的存取群組。

- 移除存取群組

  如果存取群組中未包含任何物件，您可以將其移除。您不能移除根存取群組。

- 檢閱存取群組中的桌面平台集區、應用程式集區或伺服器陣列

  您可以在 Horizon Administrator 中，查看特定存取群組中的桌面平台集區、應用程式集區或伺服器陣列。

- 檢閱存取群組中的 vCenter 虛擬機器

  您可以在 Horizon Administrator 的特定存取群組中查看 vCenter 虛擬機器。vCenter 虛擬機器從其集區繼承存取群組。

新增存取群組

您可以透過建立存取群組，將特定機器、桌面平台集區或伺服器陣列委派給不同管理員管理。依預設，桌面平台集區、應用程式集區和伺服器陣列均位於根存取群組。

您最多可以有 100 個存取群組，包括根存取群組。

程序

1 在 Horizon Administrator 中，導覽至 [新增存取群組] 對話方塊。

選項	動作
從類別目錄	■ 選取**類別目錄 > 桌面平台集區**。 ■ 從頂部視窗窗格的**存取群組**下拉式功能表中，選取**新增存取群組**。
從資源	■ 選取**資源 > 伺服器陣列**。 ■ 從頂部視窗窗格的**存取群組**下拉式功能表中，選取**新增存取群組**。
從 View 組態	■ 選取 **View 組態 > 管理員**。 ■ 在**存取群組**索引標籤中，選取**新增存取群組**。

2 輸入存取群組的名稱和說明，然後按一下**確定**。

說明為選用。

後續步驟

將一或多個物件移至存取群組中。

將桌面平台集區或伺服器陣列移至不同的存取群組

在建立存取群組後，您可以將自動桌面平台集區、手動集區或伺服器陣列移至新的存取群組。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > 桌面平台集區**或**資源 > 伺服器陣列**。

2 選取集區或伺服器陣列。

3 從頂部視窗窗格的**存取群組**下拉式功能表中，選取**變更存取群組**。

4 選取存取群組，並按一下**確定**。

Horizon Administrator 便會將集區移至您所選的存取群組。

移除存取群組

如果存取群組中未包含任何物件，您可以將其移除。您不能移除根存取群組。

必要條件

如果該存取群組包含多個物件，請將這些物件移到另一個存取群組或根存取群組。請參閱 將桌面平台集區或伺服器陣列移至不同的存取群組。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 管理員**。

2 在**存取群組**索引標籤上，選取該存取群組，然後按一下**移除存取群組**。

3 按一下**確定**移除該存取群組。

檢閱存取群組中的桌面平台集區、應用程式集區或伺服器陣列

您可以在 Horizon Administrator 中，查看特定存取群組中的桌面平台集區、應用程式集區或伺服器陣列。

程序

1 在 Horizon Administrator 中，導覽至物件的主頁面。

物件	動作
桌面平台集區	選取**類別目錄 > 桌面平台集區**。
應用程式集區	選取**類別目錄 > 應用程式集區**。
伺服器陣列	選取**資源 > 伺服器陣列**。

依預設會顯示所有存取群組中的物件。

2 從主視窗窗格的**存取群組**下拉式功能表中選取存取群組。

隨即會顯示所選取存取群組中的物件。

檢閱存取群組中的 vCenter 虛擬機器

您可以在 Horizon Administrator 的特定存取群組中查看 vCenter 虛擬機器。vCenter 虛擬機器從其集區繼承存取群組。

程序

1 在 Horizon Administrator 中，選取**資源 > 機器**。

2 選取 **vCenter 虛擬機器**索引標籤。

依預設，將會顯示所有存取群組的 vCenter 虛擬機器。

3 從**存取群組**下拉式功能表中選取存取群組。

此時將會顯示您所選取的存取群組中的 vCenter 虛擬機器。

管理自訂角色

您可以使用 Horizon Administrator 新增、修改與刪除自訂角色。

- 新增自訂角色

  如果預先定義的管理員角色不符合您的需求，您可以結合特定權限，在 Horizon Administrator 中建立自己的角色。

- 修改自訂角色中的權限
  您可以修改自訂角色的權限。您無法修改預先定義的管理員角色。
- 移除自訂角色
  如果自訂角色未包含在權限中，您便可移除自訂角色。您無法移除預先定義的管理員角色。

新增自訂角色

如果預先定義的管理員角色不符合您的需求，您可以結合特定權限，在 Horizon Administrator 中建立自己的角色。

必要條件

自行熟悉可用於建立自訂角色的管理員權限。請參閱 預先定義的角色和權限。

備註 建立自訂管理員角色時，自訂管理員使用者沒有可用的全域權限。只有預先定義的管理員角色擁有全域權限，可啟用 Cloud Pod 架構環境中的全域權利管理。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 管理員**。

2 在**角色**索引標籤上，按一下**新增角色**。

3 輸入新角色的名稱及描述，並選取一個或多個權限，然後按一下**確定**。

新角色隨即出現在左窗格中。

修改自訂角色中的權限

您可以修改自訂角色的權限。您無法修改預先定義的管理員角色。

必要條件

自行熟悉可用於建立自訂角色的管理員權限。請參閱預先定義的角色和權限。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 管理員**。

2 在**角色**索引標籤上，選取角色。

3 按一下**權限**以顯示角色中的權限，並按一下**編輯**。

4 選取或取消選取權限。

5 按一下**確定**儲存變更。

移除自訂角色

如果自訂角色未包含在權限中，您便可移除自訂角色。您無法移除預先定義的管理員角色。

必要條件

如果角色包含在權限中，請刪除該權限。請參閱刪除權限。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 管理員**。

2 在**角色**索引標籤上，選取角色，並按一下**移除角色**。

預先定義的角色或包含在權限中的自訂角色沒有**移除角色**按鈕。

3 按一下**確定**以移除角色。

預先定義的角色和權限

Horizon Administrator 包含預先定義的角色，您可以將這些角色指派給您的管理員使用者與群組。您也可以藉由結合所選的權限，來建立您自己的管理員角色。

- 預先定義的管理員角色

  預先定義的管理員角色結合了執行一般管理工作所需的所有個別權限。您無法修改預先定義的角色。

- 全域權限

  全域權限可控制全系統作業，例如檢視與變更全域設定。僅包含全域權限的角色無法套用到存取群組。

- 物件特定的權限

  物件特有的權限可控制特定類型詳細目錄物件的作業。包含物件特定權限的角色可套用至存取群組。

- 內部權限

  部分預先定義的管理員角色包含內部權限。您在建立自訂角色時，無法選取內部權限。

預先定義的管理員角色

預先定義的管理員角色結合了執行一般管理工作所需的所有個別權限。您無法修改預先定義的角色。

備註 為使用者指派預先定義或自訂角色的組合，可讓使用者存取個別預先定義或自訂角色內無法進行的作業。

下表中說明預先定義的角色，並指出角色是否可套用到存取群組。

表 6-6. Horizon Administrator 中預先定義的角色

角色	使用者功能	套用到存取群組
管理員	執行所有的管理員作業，包括建立額外的管理員使用者與群組。在 Cloud Pod 架構環境中，擁有此角色的管理員可以設定並管理網繭聯盟，也可以管理遠端網繭工作階段。 具有根存取群組上管理員角色的管理員為超級使用者，因為他們具備系統中所有詳細目錄物件的完整存取權。管理員角色包含所有權限，因此您應將該角色指派給受限的一組使用者。一開始，連線伺服器主機上的本機管理員群組成員都會獲得根存取群組上的這個角色。 **重要** 管理員必須具備根存取群組上的管理員角色，才能執行以下工作： ■ 新增和刪除存取群組。 ■ 在 Horizon Administrator 中管理 ThinApp 應用程式與組態設定。 ■ 使用 `vdmadmin`、`vdmimport` 以及 `lmvutil` 命令。	是
管理員 (唯讀)	■ 檢視 (但無法修改) 全域設定與詳細目錄物件。 ■ 檢視 (但無法修改) ThinApp 應用程式和設定。 ■ 執行所有 PowerShell 命令與命令列公用程式，包括 `vdmexport`，但 `vdmadmin`、`vdmimport` 以及 `lmvutil` 除外。 在 Cloud Pod 架構環境中，具備此角色的管理員可以檢視全域資料層中的詳細目錄物件和設定。 管理員具備存取群組的這個角色時，僅能檢視該存取群組中的詳細目錄物件。	是
代理程式登錄管理員	登錄未受管理的機器，例如實體系統、獨立虛擬機器以及 RDS 主機。	否
全域組態及原則管理員	檢視和修改全域原則及組態設定，但管理員角色與權限以及 ThinApp 應用程式和設定除外。	否
全域組態及原則管理員 (唯讀)	檢視 (但無法修改) 全域原則與組態設定，但管理員角色與權限以及 ThinApp 應用程式和設定除外。	否
服務台管理員	執行桌面平台和應用程式動作，例如關閉、重設、重新啟動，以及執行遠端協助動作，例如結束使用者桌面平台或應用程式的處理程序。管理員必須在根存取群組上擁有權限才能存取 Horizon Help Desk Tool。 ■ Horizon Help Desk Tool 的唯讀存取權。 ■ 管理全域工作階段。 ■ 可登入 Horizon Administrator。 ■ 執行所有機器和工作階段相關命令。 ■ 管理遠端處理程序和應用程式。 ■ 遠端協助虛擬桌面平台或已發佈桌面平台。	否
服務台管理員 (唯讀)	檢視使用者和工作階段資訊，並深入檢視工作階段詳細資料。管理員必須在根存取群組上擁有權限才能存取 Horizon Help Desk Tool。 ■ Horizon Help Desk Tool 的唯讀存取權。 ■ 可登入 Horizon Administrator。	否

表 6-6. Horizon Administrator 中預先定義的角色 (續)

角色	使用者功能	套用到存取群組
詳細目錄管理員	■ 執行所有機器、工作階段以及與集區相關的作業。 ■ 管理持續性磁碟。 ■ 重新同步、重新整理與重新平衡連結複製集區，及變更預設集區映像。 管理員具備存取群組的這個角色時，僅能對該存取群組中的詳細目錄物件執行這些作業。	是
詳細目錄管理員 (唯讀)	檢視 (但無法修改) 詳細目錄物件。 管理員具備存取群組的這個角色時，僅能檢視該存取群組中的詳細目錄物件。	是
本機管理員	執行所有的本機管理員作業，建立額外的管理員使用者與群組作業除外。在 Cloud Pod 架構環境中，具備此角色的管理員無法在全域資料層中執行作業，也無法管理遠端網繭上的工作階段。 **備註** 具有本機管理員角色的管理員無法存取 Horizon Help Desk Tool。在非 CPA 環境中的管理員不具有「管理全域工作階段」權限，而這是在 Horizon Help Desk Tool 中執行工作的必要權限。	是
本機管理員 (唯讀)	與管理員 (唯讀) 角色一樣，但不包括檢視全域資料層中的詳細目錄物件與設定。具備此角色的管理員在本機網繭上僅擁有唯讀權限。 **備註** 具有本機管理員 (唯讀) 角色的管理員無法存取 Horizon Help Desk Tool。在非 CPA 環境中的管理員不具有「管理全域工作階段」權限，而這是在 Horizon Help Desk Tool 中執行工作的必要權限。	是

全域權限

全域權限可控制全系統作業，例如檢視與變更全域設定。僅包含全域權限的角色無法套用到存取群組。

下表說明全域權限，並列出包含每個權限的預先定義角色。

表 6-7. 全域權限

權限	使用者功能	預先定義的角色
主控台互動	登入並使用 Horizon Administrator。	管理員 管理員 (唯讀) 詳細目錄管理員 詳細目錄管理員 (唯讀) 全域組態及原則管理員 全域組態及原則管理員 (唯讀) 服務台管理員 服務台管理員 (唯讀) 本機管理員 本機管理員 (唯讀)
直接互動	執行所有的 PowerShell 命令與命令列公用程式，但 `vdmadmin` 與 `vdmimport` 除外。 管理員必須具備根存取群組的管理員角色，才能使用 `vdmadmin`、`vdmimport` 及 `lmvutil` 命令。	管理員 管理員 (唯讀)

表 6-7. 全域權限 (續)

權限	使用者功能	預先定義的角色
管理全域組態和原則	檢視和修改全域原則及組態設定，但管理員角色與權限除外。	管理員 全域組態及原則管理員
管理全域工作階段	管理 Cloud Pod 架構環境中的全域工作階段。	管理員
管理角色和權限	建立、修改和刪除管理員角色與權限。	管理員
註冊代理程式	將 Horizon Agent 安裝在未受管理的機器上，例如實體系統、獨立虛擬機器及 RDS 主機。 在 Horizon Agent 安裝期間，您必須提供管理員登入認證，才能向連線伺服器執行個體登錄未受管理的機器。	管理員 代理程式登錄管理員

物件特定的權限

物件特有的權限可控制特定類型詳細目錄物件的作業。包含物件特定權限的角色可套用至存取群組。

下表說明物件特定的權限。管理員與詳細目錄管理員是預先定義的角色，包含所有上述的權限。

表 6-8. 物件特定的權限

權限	使用者功能	物件
啟用伺服器陣列和桌面平台集區	啟用和停用桌面平台集區。	桌面平台集區, 伺服器陣列
賦予桌面平台和應用程式集區權利	新增和移除使用者權利。	桌面平台集區, 應用程式集區
管理 Composer 桌面平台集區映像	重新同步、重新整理與重新平衡連結複製集區，及變更預設集區映像。	桌面平台集區
管理機器	執行所有機器和工作階段相關作業。	機器
管理持續性磁碟	執行所有的 View Composer 持續性磁碟作業，包括連接、中斷連結與匯入持續性磁碟。	持續性磁碟
管理伺服器陣列及桌面平台和應用程式集區	新增、修改及刪除伺服器陣列。新增、修改、刪除及授權桌面平台和應用程式集區。新增及移除機器。	桌面平台集區, 應用程式集區, 伺服器陣列
管理工作階段	中斷連線並登出工作階段，並傳送訊息給使用者。	工作階段
管理重新啟動作業	重設虛擬機器或重新啟動虛擬桌面平台。	機器

內部權限

部分預先定義的管理員角色包含內部權限。您在建立自訂角色時，無法選取內部權限。

下表說明內部權限，並列出包含每個權限的預先定義角色。

表 6-9. 內部權限

權限	說明	預先定義的角色
完整 (唯讀)	授與所有設定的唯讀存取權。	管理員 (唯讀)
管理詳細目錄 (唯讀)	授與詳細目錄物件的唯讀存取權。	詳細目錄管理員 (唯讀)
管理全域組態和原則 (唯讀)	授與組態設定與全域原則的唯讀存取權，唯管理員與角色除外。	全域組態及原則管理員 (唯讀)

一般工作的必要權限

許多一般管理工作需要一組協調的權限。某些作業除了需要正在操作的物件存取權外，還需要根存取群組的權限。

管理集區的權限

管理員必須具備可在 Horizon Administrator 中管理集區的特定權限。

下表列出一般集區管理工作，並顯示執行每個工作所需的權限。

表 6-10. 集區管理工作與權限

工作	所需的權限
啟用或停用桌面平台集區	**啟用伺服器陣列和桌面平台集區**
將使用者權利賦予或取消賦予給集區	**賦予桌面平台和應用程式集區權利**
新增集區	**管理伺服器陣列及桌面平台和應用程式集區**
修改或刪除集區	**管理伺服器陣列及桌面平台和應用程式集區**
新增或移除集區的桌面平台	**管理伺服器陣列及桌面平台和應用程式集區**
重新整理、重新撰寫、重新平衡或變更預設的 View Composer 映像	**管理 Composer 桌面平台集區映像**
變更存取群組	來源與目標存取群組上的**管理伺服器陣列及桌面平台和應用程式集區**。

管理機器的權限

管理員必須具備可在 Horizon Administrator 中管理機器的特定權限。

下表列出一般機器管理工作，並顯示執行每個工作所需的權限。

表 6-11. 機器管理工作與權限

工作	所需的權限
移除虛擬機器	**管理機器**
重設虛擬機器	**管理重新啟動作業**
重新啟動虛擬桌面平台	**管理重新啟動作業**
指派或移除使用者擁有權	**管理機器**

表 6-11. 機器管理工作與權限 (續)

工作	所需的權限
進入或離開維護模式	**管理機器**
中斷連線或登出工作階段	**管理工作階段**

管理持續性磁碟的權限

管理員必須具備可在 Horizon Administrator 中管理持續性磁碟的特定權限。

下表列出一般持續性磁碟管理工作，並顯示執行每個工作所需的權限。您可在 Horizon Administrator 的「持續性磁碟」頁面中執行這些工作。

表 6-12. 持續性磁碟管理工作與權限

工作	所需的權限
中斷連結磁碟	磁碟上的**管理持續性磁碟**，以及集區上的**管理伺服器陣列及桌面平台和應用程式集區**。
附加磁碟	磁碟上的**管理持續性磁碟**，以及機器上的**管理伺服器陣列及桌面平台和應用程式集區**。
編輯磁碟	磁碟上的**管理持續性磁碟**，以及所選集區上的**管理伺服器陣列及桌面平台和應用程式集區**。
變更存取群組	來源與目標存取群組上的**管理持續性磁碟**。
重新建立桌面平台	磁碟上的**管理持續性磁碟**，以及最後一個集區上的**管理伺服器陣列及桌面平台和應用程式集區**。
從 vCenter 匯入	資料夾上的**管理持續性磁碟**，以及集區上的**管理集區**。
刪除磁碟	磁碟上的**管理持續性磁碟**。

管理使用者和管理員的權限

管理員必須具備可在 Horizon Administrator 中管理使用者與管理員的特定權限。

下表列出一般使用者工作和管理員管理工作，並顯示執行每個工作所需的權限。您需要在 Horizon Administrator 的「使用者與群組」頁面上管理使用者。您需要在 Horizon Administrator 的「全域管理員檢視」頁面上管理管理員。

表 6-13. 使用者與管理員管理工作和權限

工作	所需的權限
更新一般使用者資訊	**管理全域組態和原則**
將訊息傳送至使用者	機器上的**管理遠端工作階段**。
新增管理員使用者或群組	**管理角色和權限**
新增、修改或刪除管理員權限	**管理角色和權限**
新增、修改或刪除管理員角色	**管理角色和權限**

Horizon Help Desk Tool 工作的權限

Horizon Help Desk Tool 管理員必須具備可在 Horizon Administrator 中執行疑難排解工作的特定權限。

下表列出 Horizon Help Desk Tool 管理員可執行的一般工作，並顯示執行各項工作的權限。

表 6-14. Horizon Help Desk Tool 工作和權限

工作	所需的權限
Horizon Help Desk Tool 的唯讀存取權。	**管理服務台 (唯讀)**
管理全域工作階段。	**管理全域工作階段**
可登入 Horizon Administrator。	**主控台互動**
執行所有機器和工作階段相關命令。	**管理機器**
重設或重新啟動機器。	**管理重新啟動作業**
中斷連線並登出工作階段。	**管理工作階段**
管理遠端處理程序和應用程式。	**管理遠端處理程序和應用程式**
遠端協助虛擬桌面平台或已發佈桌面平台。	**遠端協助**
中斷連線、登出、重設以及重新啟動全域工作階段的作業。	**管理服務台 (唯讀)** 和**管理全域工作階段**
重設並重新啟動本機工作階段的作業。	**管理服務台 (唯讀)** 和**管理重新啟動作業**
遠端協助作業。	**管理服務台 (唯讀)** 和**遠端協助**
結束遠端處理程序和應用程式。	**管理服務台 (唯讀)** 和**管理遠端處理程序和應用程式**
在 Horizon Help Desk Tool 中執行所有工作。	**管理服務台 (唯讀)**、**管理全域工作階段**、**管理重新啟動作業**、**遠端協助**，以及**管理遠端處理程序和應用程式**
遠端協助作業以及結束遠端處理程序和應用程式。	**管理服務台 (唯讀)**、**遠端協助**，以及**管理遠端處理程序和應用程式**
中斷連線並登出本機工作階段的作業。	**管理服務台 (唯讀)** 和**管理工作階段**

一般管理工作和命令的權限

管理員必須具備某些權限，才能執行一般管理工作與命令列公用程式。

下表中顯示執行一般管理工作與命令列公用程式所需的權限。

表 6-15. 一般管理工作和命令的權限

工作	所需的權限
新增或刪除存取群組	必須具備根存取群組的本機管理員角色或管理員角色，才能刪除存取群組。 必須具備根存取群組的詳細目錄管理員或本機管理員或管理員角色。
在 Horizon Administrator 中管理 ThinApp 應用程式與設定	必須具備根存取群組的管理員角色。
將 Horizon Agent 安裝在未受管理的機器上，如實體系統、獨立虛擬機器或 RDS 主機	**註冊代理程式**
檢視或修改 Horizon Administrator 中的組態設定 (管理員除外)	**管理全域組態和原則**

表 6-15. 一般管理工作和命令的權限 (續)

工作	所需的權限
執行所有的 PowerShell 命令與命令列公用程式，但 `vdmadmin` 與 `vdmimport` 除外。	**直接互動** **備註** 從 Horizon 7(7.10 版) 開始，直接互動權限會自動新增至新角色，且不會顯示在 Horizon Console 的權限清單中。
使用 `vdmadmin` 與 `vdmimport` 命令	必須具備根存取群組的管理員角色。
使用 `vdmexport` 命令	必須具備管理員角色或根存取群組的管理員 (唯讀) 角色。
以唯讀方式存取 vCenter Server 組態。	**管理 vCenter 組態 (唯讀)**

管理員使用者及群組的最佳做法

若要增加 Horizon 7 環境的安全性和管理能力，您應該遵循最佳做法對管理員使用者和群組進行管理。

- 在 Active Directory 中建立新使用者群組，並將管理角色指派給這些群組。避免使用 Windows 內建群組或其他現有群組，因為其中可能包含不需要或不應擁有 Horizon 7 權限的使用者。
- 將擁有 Horizon 7 管理權限的使用者保持在最低數目。
- 因為管理員角色擁有全部權限，因此不應用於日常管理。
- 由於 Administrator 這個字相當常見，而且很容易聯想猜測，因此，建立管理員使用者和群組時，請避免使用 Administrator 作為名稱。
- 建立存取群組以區隔機密的桌面平台和伺服器陣列。將這些存取群組委派給限定人數的一組使用者管理。
- 分別建立可修改全域原則和 Horizon 7 組態設定的管理員。

在 Horizon Administrator 和 Active Directory 中設定原則

7

您可以使用 Horizon Administrator 為用戶端工作階段設定原則。您可以設定 Active Directory 群組原則設定，以控制 View 連線伺服器的行為、PCoIP 顯示通訊協定以及 Horizon 7 登入和效能警示。

您也可以設定 Active Directory 群組原則設定，以控制 Horizon Agent、Windows 版 Horizon Client、Horizon Persona Management 及特定功能的行為。如需這些原則設定的相關資訊，請參閱《在 Horizon 7 中設定遠端桌面平台功能》文件。

本章節討論下列主題：

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。

- 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。

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 7-1. 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 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 7-2. 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。 請參閱《在 Horizon 7 中設定遠端桌面平台功能》文件。
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。
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《在 Horizon 7 中設定遠端桌面平台功能》文件和《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。
VMware View 一般組態	`vdm_common.admx`	包含所有 Horizon 元件通用的原則設定。
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。 請參閱《在 Horizon 7 中設定遠端桌面平台功能》文件。

表 7-2. Horizon ADMX 範本檔 (續)

範本名稱	範本檔	說明
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《在 Horizon 7 中設定遠端桌面平台功能》文件。
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《在 Horizon 7 中設定遠端桌面平台功能》文件。
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《在 Horizon 7 中設定遠端桌面平台功能》文件。
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《在 Horizon 7 中設定遠端桌面平台功能》文件。
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。
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。 請參閱使用 VMware Horizon 效能追蹤程式。
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《在 Horizon 7 中設定遠端桌面平台功能》文件。

Horizon 連線伺服器組態 ADMX 範本設定

View Server 組態 ADMX (`vdm_server.admx`) 範本檔包含與所有 Horizon 連線伺服器相關的原則設定。

下表說明連線伺服器組態 ADMX 範本檔中的每個原則設定。此範本僅包含「電腦組態」設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View Server 組態**資料夾中。

表 7-3. Horizon Server 組態範本設定

設定	內容
Enumerate Forest Trust Child Domains	決定是否列舉伺服器所在網域所信任的每個網域。為了建立完整的信任鏈結，也要列舉每個信任的網域所信任的網域，在搜尋到所有信任的網域之前，程序才會以遞迴的方式繼續。此資訊會傳遞到連線伺服器，以確保用戶端在登入時可以使用所有信任的網域。 此內容依預設為啟用。停用時，只會列舉直接信任的網域，因此不會與遠端網域控制站建立連線。 **備註** 在網域關係複雜的環境 (例如，在其樹系中使用網域間具備信任的多個樹系結構的環境) 中，此程序可能需要幾分鐘才能完成。
Recursive Enumeration of Trusted Domains	決定是否列舉伺服器所在網域所信任的每個網域。若要建立完整的信任鏈結，也要列舉每個信任的網域所信任的網域，在搜尋到所有信任的網域之前，程序才會以遞迴的方式繼續。此資訊會傳遞到 View 連線伺服器，讓用戶端在登入時，可以使用所有信任的網域。 此設定依預設為啟用。停用此設定時，只會列舉直接信任的網域，因此不會與遠端網域控制站建立連線。 在網域關係複雜的環境 (例如，在其樹系中使用網域間具備信任的多個樹系結構的環境) 中，此程序可能需要幾分鐘才能完成。
Windows Password Authentication Mode	選取 Windows 密碼驗證模式。 ■ KerberosOnly。使用 Kerberos 進行驗證。 ■ KerberosWithFallbackToNTLM。使用 Kerberos 進行驗證，但失敗時則退回使用 NTLM。 ■ Legacy。使用 NTLM 進行驗證，但失敗時則退回使用 Kerberos。用於支援舊版 NT 網域控制站。 預設為 KerberosOnly。

Horizon 7 一般組態 ADMX 範本設定

Horizon 7 一般組態 ADMX (vdm_common.admx) 範本檔包含所有 Horizon 元件通用的原則設定。這些範本僅包含「電腦組態」設定。

記錄組態設定

下表說明 Horizon 一般組態 ADMX 範本檔中的記錄組態原則設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View 一般組態 > 記錄組態**資料夾中。

表 7-4. View 一般組態範本：記錄組態設定

設定	內容
Number of days to keep production logs	指定記錄檔保留在系統上的天數。若未設定值，會套用預設值且記錄檔會保留 7 天。
Maximum number of debug logs	指定要保留在系統上的偵錯記錄檔數目上限。當記錄檔到達其大小上限時，則不會新增其他項目而且會建立新的記錄檔。當先前的記錄檔數目到達此值時，則會刪除最舊的記錄檔。
Maximum debug log size in Megabytes	指定偵錯記錄可到達的大小上限 (MB)，記錄檔超過此上限後會關閉並建立新的記錄檔。

表 7-4. View 一般組態範本：記錄組態設定 (續)

設定	內容
Log Directory	指定記錄檔目錄的完整路徑。如果無法寫入該位置，則會使用預設位置。若是用戶端記錄檔，則會建立具有用戶端名稱的額外目錄。
Send logs to a Syslog server	允許將 View server 記錄傳送至 Syslog 伺服器，例如 VMware vCenter Log Insight。將從設定此 GPO 之 OU 或網域中的所有 View server 中傳送記錄。 透過在 GPO 中 (連結至包含桌面平台的 OU) 啟用此設定，您可以將 Horizon Agent 記錄傳送到 Syslog 伺服器。 若要傳送記錄資料至 Syslog 伺服器，請啟用此設定，並指定記錄層級和伺服器完整網域名稱 (FQDN) 或 IP 位址。若不想使用預設連接埠 514，則可以指定替代連接埠。指定時請以分隔號 (|) 分隔每個元素。使用下列語法： `Log Level|Server FQDN or IP [|Port number(514 default)]` 例如：`Debug|192.0.2.2` **重要** Syslog 資料會在未經軟體式加密的情況下傳送到網路上。由於 View Server 記錄可能包含敏感資料，因此請避免在不安全的網路上傳送 Syslog 資料。如果可能，請使用連結層安全性 (例如 IPsec) 來避免此資料可能會在網路上遭到監控的情況。

效能警示設定

表 7-5. View 一般組態範本：效能警示設定說明 Horizon 一般組態 ADMX 範本檔中的效能警示設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View 一般組態 > 效能警示**資料夾中。

表 7-5. View 一般組態範本：效能警示設定

設定	內容
CPU and Memory Sampling Interval in Seconds	指定 CPU 和記憶體輪詢間隔 CPU。取樣間隔低，會導致輸出到記錄的層級變高。
Overall CPU usage percentage to issue log info	指定記錄系統總體 CPU 使用率的臨界值。當有多個處理器可使用時，此百分比表示合併的使用率。
Overall memory usage percentage to issue log info	指定記錄總體已認可系統記憶體使用率的臨界值。已認可系統記憶體是指已由處理器配置，而且作業系統已在分頁檔中認可實體記憶體或分頁插槽的記憶體。
Process CPU usage percentage to issue log info	指定記錄任何個別程序之 CPU 使用率的臨界值。

表 7-5. View 一般組態範本：效能警示設定 (續)

設定	內容
Process memory usage percentage to issue log info	指定記錄任何個別程序之記憶體使用率的臨界值。
Process to check, comma separated name list allowing wild cards and exclusion	指定對應於要檢查之一或多個程序名稱的查詢清單 (以逗號分隔)。您可以在每個查詢中使用萬用字元來篩選清單。 ■ 星號 (*) 可符合零或更多字元。 ■ 問號 (?) 可符合單一字元。 ■ 驚嘆號 (!) 放在查詢開頭會排除該查詢所產生的任何結果。 例如，下列查詢會選取開頭為 **ws** 的所有程序，並排除結尾為 **sys** 的所有程序： **'! *sys,ws*'**

備註 效能警示設定僅適用於 Horizon 連線伺服器和 Horizon Agent 系統。不適用於 Horizon Client 系統。

安全性設定

表 7-6. View 一般組態範本：安全性設定說明 Horizon 一般組態 ADMX 範本檔中的安全性設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View 一般組態 > 安全性設定**資料夾中。

表 7-6. View 一般組態範本：安全性設定

設定	內容
Only use cached revocation URLS	憑證撤銷檢查只能存取快取 URL。 如果未設定，預設為 false。
Revocation URL check timeout milliseconds	所有撤銷 URL 線擷取的累積逾時 (以毫秒為單位)。 未設定或將值設為 0 代表使用 Microsoft 預設處理。
Type of certificate revocation check	選取要完成的憑證撤銷檢查類型： ■ None ■ EndCertificateOnly ■ WholeChain ■ WholeChain 預設為 WholeChainButRoot。

一般設定

表 7-7. View 一般組態範本：一般設定說明 Horizon 一般組態 ADMX 範本檔中的一般設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View 一般組態**資料夾中。

表 7-7. View 一般組態範本：一般設定

設定	內容
Disk threshold for log and events in Megabytes	指定記錄和事件的最小剩餘磁碟空間臨界值。若未指定值，則預設值為 200。當達到指定的值時，事件記錄會停止。
Enable extended logging	決定記錄檔中是否包含追蹤和偵錯事件。
Override the default View Windows event generation	支援下列值： ■ 0 = 僅針對 View 事件產生事件記錄項目 (記錄訊息不會產生事件記錄項目) ■ 1 = 在 4.5 (及更早版本) 相容模式中產生事件記錄項目。標準 View 事件不會產生事件記錄項目。系統僅根據記錄檔文字產生事件記錄項目。 ■ 2 = 在 4.5 (及更早版本) 相容模式中產生事件記錄項目，同時包含 View 事件。

維護 Horizon 7 元件

8

若要讓 Horizon 7 元件保持為可用與執行中，您可以執行各種維護工作。

本章節討論下列主題：

備份和還原 Horizon 7 組態資料

您可以排程或執行 Horizon Administrator 的自動備份，以備份 Horizon 7 和 View Composer 組態資料。您可以手動匯入所備份的 View LDAP 檔案及 View Composer 資料庫檔案，以還原 Horizon 7 組態。

您可以使用備份及還原功能，保留和移轉 Horizon 7 組態資料。

備份 Horizon 連線伺服器及 View Composer 資料

完成連線伺服器的初始組態後，應該排程 Horizon 7 及 View Composer 組態資料的定期備份。您可使用 Horizon Administrator 保留 Horizon 7 及 View Composer 資料。

Horizon 7 將連線伺服器組態資料儲存於 View LDAP 存放庫中。View Composer 將連結複製桌面平台的組態資料儲存於 View Composer 資料庫中。

備註 依預設，Horizon 7 會在每天上午 12 點自動備份連線伺服器和 View Composer 資料。

使用 Horizon Administrator 執行備份時，Horizon 7 將備份 View LDAP 組態資料及 View Composer 資料庫。這兩組備份檔案均儲存於同一個位置。View LDAP 資料是以加密的 LDAP 資料交換格式 (LDIF) 匯出。如需 View LDAP 的說明，請參閱 View LDAP 目錄。

有幾種方法可執行備份。

- 使用 Horizon 7 組態備份功能排程自動備份。
- 使用 Horizon Administrator 的**立即備份**功能，立即起始備份。
- 使用 `vdmexport` 公用程式，手動匯出 View LDAP 資料。連線伺服器的各個執行個體均提供此公用程式。

  `vdmexport` 公用程式可匯出 View LDAP 資料成為加密的 LDIF 資料、純文字，或移除了密碼和其他機密資料的純文字。

  備註 `vdmexport` 工具僅可備份 View LDAP 資料。此工具不會備份 View Composer 資料庫資訊。

  如需關於 `vdmexport` 的詳細資訊，請參閱從 Horizon 連線伺服器匯出組態資料。

下列準則適用於備份 Horizon 7 組態資料：

- Horizon 7 可匯出任何連線伺服器執行個體的組態資料。
- 如果複寫的群組中有多個連線伺服器執行個體，只需要匯出其中一個執行個體的資料即可。所有複寫的執行個體均包含相同的組態資料。
- 請勿依賴使用複寫的連線伺服器執行個體作為備份機制。Horizon 7 同步處理複寫的連線伺服器執行個體中所含的資料時，其中一個執行個體發生任何資料遺失均可能造成群組中所有成員的資料遺失。
- 如果連線伺服器將多個 vCenter Server 執行個體與多個 Composer 服務搭配使用，Horizon 7 將備份與 vCenter Server 執行個體相關聯的所有 View Composer 資料庫。

排程 Horizon 7 組態備份

您可以排程定期備份 Horizon 7 組態資料。Horizon 7 會備份 View LDAP 存放庫的內容，而連線伺服器執行個體會將其組態資料儲存在其中。

若您要立即備份組態，請選取連線伺服器執行個體，然後按一下**立即備份**。

必要條件

自行熟悉備份設定。請參閱 Horizon 7 組態備份設定。

程序

1. 在 Horizon Administrator 中，選取 **View 組態 > 伺服器**。
2. 在**連線伺服器**索引標籤上，選取要備份的連線伺服器執行個體，然後按一下**編輯**。
3. 在**備份**索引標籤上，指定 Horizon 7 組態備份設定，以設定備份頻率、備份數量上限，以及備份檔案的資料夾位置。

4 (選擇性) 變更資料復原密碼。

a 按一下**變更資料復原密碼**。

b 輸入兩次新密碼。

c (選擇性) 輸入密碼提醒。

d 按一下**確定**。

5 按一下**確定**。

Horizon 7 組態備份設定

Horizon 7 可以定期備份您的連線伺服器和 View Composer 組態資料。在 Horizon Administrator 中，您可以設定備份作業的頻率和其他方面的內容。

備註 依預設，Horizon 7 會在每天上午 12 點自動備份連線伺服器和 View Composer 資料。

表 8-1. Horizon 7 組態備份設定

設定	說明
自動備份頻率	每小時。備份會在每小時整點時進行。 每 6 小時。備份會在午夜、早上 6 點、中午和下午 6 點進行。 每 12 小時。備份會在午夜和中午進行。 每天。備份會在每天午夜時進行。 每 2 天。備份會在星期六、星期一、星期三和星期五的午夜進行。 每週。備份會在每週六的午夜進行。 每 2 週。備份會在每隔一週的星期六午夜進行。 永不。備份不會自動進行。
備份數目上限	可以儲存在連線伺服器執行個體上的備份檔案數目。此數字必須是大於 0 的整數。 達到數目上限時，Horizon 7 會刪除最舊的備份檔案。 此設定也會套用至使用**立即備份**時建立的備份檔案。
資料夾位置	連線伺服器執行所在電腦上備份檔案的預設位置：`C:\Programdata\VMWare\VDM\backups` 當您使用**立即備份**時，Horizon 7 也會將備份檔案儲存在這個位置。

從 Horizon 連線伺服器匯出組態資料

您可以透過匯出 View LDAP 存放庫的內容，來備份 Horizon 連線伺服器執行個體的組態資料。

您可以使用 `vdmexport` 命令，將 View LDAP 組態資料匯出至加密的 LDIF 檔。您也可以使用 `vdmexport -v` (逐字) 選項將資料匯出為純文字 LDIF 檔，或 `vdmexport -c` (已清理) 選項，將資料匯出為密碼與其他機密資料已移除的純文字。

您可以在任何連線伺服器執行個體上執行 `vdmexport` 命令。如果複寫的群組中有多個連線伺服器執行個體，只需要匯出其中一個執行個體的資料即可。所有複寫的執行個體均包含相同的組態資料。

備註 `vdmexport.exe` 命令只會備份 View LDAP 資料。此命令不會備份 View Composer 資料庫資訊。

必要條件

- 找到與連線伺服器一起安裝在預設路徑的 vdmexport.exe 命令可執行檔。

  C:\Program Files\VMware\VMware View\Server\tools\bin

- 以「管理員」或「管理員 (唯讀)」角色的使用者身分登入連線伺服器執行個體。

程序

1 選取**開始 > 命令提示字元**。

2 在命令提示字元中，輸入 vdmexport 命令並將輸出重新導向至一個檔案。例如：

```
vdmexport > Myexport.LDF
```

依預設，匯出的資料會加密。
您可以將輸出檔案名稱指定為 –f 選項的引數。例如：

```
vdmexport –f Myexport.LDF
```

您可以使用 –v 選項以純文字格式 (逐字) 匯出資料。例如：

```
vdmexport –f Myexport.LDF –v
```

您可以使用 –c 選項，以密碼與機密資料已移除 (已清理) 的純文字格式匯出資料。例如：

```
vdmexport –f Myexport.LDF –c
```

備註 請不要規劃使用已清理的備份資料還原 View LDAP 組態。已清理的組態資料中會遺失密碼與其他重大資訊。

如需關於 vdmexport 命令的詳細資訊，請參閱《Horizon 7 整合》文件。

後續步驟

您可以使用 vdmimport 命令還原或傳輸連線伺服器的組態資訊。

如需匯入 LDIF 檔案的詳細資料，請參閱還原 Horizon 連線伺服器與 View Composer 組態資料。

還原 Horizon 連線伺服器與 View Composer 組態資料

您可以手動還原由 Horizon 7 備份的連線伺服器 LDAP 組態檔與 View Composer 資料庫檔案。

您手動執行另外的公用程式來還原連線伺服器與 View Composer 組態資料。

在您還原組態資料前，請確認已備份 Horizon Administrator 中的組態資料。請參閱備份 Horizon 連線伺服器及 View Composer 資料。

您要使用 vdmimport 公用程式，將連線伺服器資料從 LDIF 備份檔案匯入到連線伺服器執行個體中的 View LDAP 存放庫。

您可以使用 SviConfig 公用程式將 View Composer 資料從 .svi 備份檔案匯入到 View Composer SQL 資料庫。

備註 在某些狀況中，您可能必須安裝目前版本的連線伺服器執行個體，並藉由匯入連線伺服器 LDAP 組態檔來還原現有的 Horizon 7 組態。您的業務持續性與災難復原 (BC/DR) 計劃可能需要此程序，做為使用現有 Horizon 7 組態設定第二個資料中心的方法，或用做其他目的。如需詳細資訊，請參閱《Horizon 7 安裝》文件。

將組態資料匯入 Horizon 連線伺服器

您可以透過匯入儲存在 LDIF 檔案中的資料備份複本，來還原連線伺服器執行個體的組態資料。

您使用 vdmimport 命令將資料從 LDIF 檔案匯入到連線伺服器執行個體的 View LDAP 存放庫中。

如果您使用 Horizon Administrator 或預設的 vdmexport 命令備份您的 View LDAP 組態，則匯出的 LDIF 檔案會加密。您必須先將 LDIF 檔案解密，才能匯入該檔案。

如果匯出的 LDIF 檔案是純文字格式，則不必將檔案解密。

備註 請不要匯入已清理格式的 LDIF 檔案，已清理格式是已移除密碼與其他機密資料的純文字。如果您匯入，則還原的 View LDAP 存放庫中會遺失重大的組態資訊。

如需備份 View LDAP 存放庫的相關資訊，請參閱 備份 Horizon 連線伺服器及 View Composer 資料。

必要條件

- 找到連同連線伺服器一起安裝在預設路徑的 vdmimport 命令可執行檔。

  ```
  C:\Program Files\VMware\VMware View\Server\tools\bin
  ```

- 以具有管理員角色的使用者身分登入連線伺服器執行個體。
- 確認您知道資料復原密碼。如果有設定密碼提醒，您可以執行不搭配密碼選項的 vdmimport 命令，來顯示提醒。

程序

1. 透過停止執行 View Composer 的伺服器上的 Windows 服務 VMware Horizon View Composer，來停止所有 View Composer 的執行個體。
2. 透過停止所有安全伺服器上的 Windows 服務 VMware Horizon 安全伺服器，來停止所有安全伺服器執行個體。
3. 解除安裝所有 Horizon 連線伺服器執行個體。

   解除安裝 VMware Horizon 連線伺服器與 AD LDS 執行個體 VMwareVDMDS。
4. 安裝一個連線伺服器執行個體。
5. 透過停止 Windows 服務 VMware Horizon 連線伺服器，來停止連線伺服器執行個體。
6. 按一下**開始 > 命令提示字元**。

7 將加密的 LDIF 檔案解密。

在命令提示字元輸入 `vdmimport` 命令。指定 `-d` 選項、搭配資料復原密碼的 `-p` 選項，以及搭配現有解密 LDIF 檔案的 `-f` 選項，後面加上所解密 LDIF 檔案的名稱。例如：

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

如果您忘記資料復原密碼，請輸入不含 `-p` 選項的命令。該公用程式會顯示密碼提醒，並提示您輸入密碼。

8 匯入解密的 LDIF 檔案來還原 View LDAP 組態。

指定 `-f` 選項並搭配解密的 LDIF 檔案。例如：

```
vdmimport -f MyDecryptedexport.LDF
```

9 解除安裝連線伺服器。

僅解除安裝套件 VMware Horizon 連線伺服器。

10 解除安裝連線伺服器。

11 登入 Horizon Administrator 並驗證組態是否正確。

12 啟動 View Composer 執行個體。

13 重新安裝複寫伺服器執行個體。

14 啟動安全伺服器執行個體。

如果存在安全伺服器組態不一致的風險，則應該將其解除安裝而非停止或在程序結束時重新安裝。

`vdmimport` 命令會使用 LDIF 檔案中的組態資料更新連線伺服器中的 View LDAP 存放庫。如需關於 `vdmimport` 命令的詳細資訊，請參閱《Horizon 7 安裝》文件。

備註 請確定還原中的組態與 vCenter Server 及 View Composer (如果正在使用) 已知的虛擬機器相符。如有必要，請從備份中還原 View Composer 組態。請參閱還原 View Composer 資料庫。還原 View Composer 組態之後，如果 vCenter Server 中的虛擬機器自 View Composer 組態備份後發生變更，則您可能需要手動解決不一致問題。

還原 View Composer 資料庫

您可以將 View Composer 組態的備份檔案匯入至儲存連結複製資訊的 View Composer 資料庫。

您可以使用 `SviConfig restoredata` 命令在系統失敗後還原 View Composer 資料庫資料，或使用此命令將 View Composer 組態還原至先前的狀態。

重要 只有具豐富經驗的 View Composer 管理員才能使用 `SviConfig` 公用程式。此公用程式用於解決與 View Composer 服務相關的問題。

必要條件

確認 View Composer 資料庫備份檔案位置。依預設，Horizon 7 會將備份檔案儲存在連線伺服器電腦的 C: 磁碟機中，路徑為 C:\Programdata\VMWare\VDM\backups。

View Composer 備份檔案使用的命名慣例包含日期戳記與 .svi 尾碼。

Backup-*YearMonthDayCount-vCenter Server Name_Domain Name*.svi

例如：Backup-20090304000010-foobar_test_org.svi

自行熟悉 SviConfig restoredata 參數：

- DsnName - 用於連線至資料庫的 DSN。DsnName 為強制參數，不能為空白字串。
- Username - 用於連線至資料庫的使用者名稱。如果未指定此參數，則使用 Windows 驗證。
- Password - 連線至資料庫的使用者密碼。如果未指定此參數，且未使用 Windows 驗證，則會提示您稍後輸入密碼。
- BackupFilePath - View Composer 備份檔案的路徑。

DsnName 與 BackupFilePath 為必要參數，不能為空白字串。Username 與 Password 為選用參數。

程序

1 將 View Composer 備份檔案從連線伺服器電腦，複製到可從安裝有 VMware Horizon View Composer 服務的電腦存取的位置。

2 在有安裝 View Composer 的電腦上，停止 VMware Horizon View Composer 服務。

3 開啟 Windows 命令提示字元，並導覽至 SviConfig 執行檔。

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

4 執行 SviConfig restoredata 命令。

```
sviconfig -operation=restoredata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -BackupFilePath=path_to_View_Composer_backup_file
```

例如：

```
sviconfig -operation=restoredata -dsnname=LinkedClone
-username=Admin -password=Pass
-backupfilepath="C:\Program Files (x86)\VMware\VMware View
Composer\Backup-20090304000010-foobar_test_org.SVI"
```

5 啟動 VMware Horizon View Composer 服務。

後續步驟

有關 SviConfig restoredata 命令的輸出結果代碼，請參閱 用於還原 View Composer 資料庫的結果代碼。

用於還原 View Composer 資料庫的結果代碼

當您還原 View Composer 資料庫時，SviConfig restoredata 命令會顯示結果代碼。

表 8-2. Restoredata 結果代碼

代碼	說明
0	作業已成功結束。
1	找不到提供的 DSN。
2	提供的資料庫管理員認證無效。
3	不支援資料庫的驅動程式。
4	發生非預期的問題，命令無法完成。
14	另一個應用程式正在使用 VMware Horizon View Composer 服務。先關閉服務，再執行命令。
15	還原程序期間發生問題。在畫面記錄輸出中提供詳細資料。

匯出 View Composer 資料庫中的資料

您可以將 View Composer 資料庫中的資料匯出至檔案。

重要　只有豐富經驗的 View Composer 管理員才能使用 SviConfig 公用程式。

必要條件

依預設，Horizon 7 會將備份檔案儲存在 C:View 連線伺服器電腦的磁碟機中，路徑為 C:\Programdata\VMWare\VDM\backups。

自行熟悉 SviConfig exportdata 參數：

- DsnName - 用於連線至資料庫的 DSN。如果未指定此參數，則會從伺服器組態檔中擷取 DSN 名稱、使用者名稱和密碼。
- Username - 用於連線至資料庫的使用者名稱。如果未指定此參數，則使用 Windows 驗證。
- Password - 連線至資料庫的使用者密碼。如果未指定此參數，且未使用 Windows 驗證，則會提示您稍後輸入密碼。
- OutputFilePath - 輸出檔案的路徑。

程序

1. 在有安裝 View Composer 的電腦上，停止 VMware Horizon View Composer 服務。
2. 開啟 Windows 命令提示字元，並導覽至 SviConfig 執行檔。

   該檔案與 View Composer 應用程式位於同一個位置。

   View-Composer-installation-directory\sviconfig.exe

3 執行 SviConfig exportdata 命令。

```
sviconfig –operation=exportdata
          –DsnName=target_database_source_name_(DSN)
          –Username=database_administrator_username
          –Password=database_administrator_password
          –OutputFilePath=path_to_View_Composer_output_file
```

例如：

```
sviconfig –operation=exportdata –dsnname=LinkedClone
–username=Admin –password=Pass
–outputfilepath="C:\Program Files\VMware\VMware View
Composer\Export–20090304000010–foobar_test_org.SVI"
```

後續步驟

有關 SviConfig exportdata 命令的輸出結果代碼，請參閱用於匯出 View Composer 資料庫的結果代碼。

用於匯出 View Composer 資料庫的結果代碼

當您匯出 View Composer 資料庫時，SviConfig exportdata 命令會顯示結束碼。

表 8-3. Exportdata ExitStatus 代碼

代碼	描述
0	匯出資料成功結束。
1	找不到提供的 DSN 名稱。
2	提供的認證無效。
3	提供的資料庫不支援該驅動程式。
4	發生非預期的問題。
18	無法連線到資料庫伺服器。
24	無法開啟輸出檔案。

監控 Horizon 7 元件

您可以使用 Horizon Administrator 儀表板快速調查 Horizon 7 部署中 Horizon 7 與 vSphere 元件的狀態。

Horizon Administrator 會顯示連線伺服器執行個體、事件資料庫、閘道、安全伺服器、View Composer 服務、資料存放區、vCenter Server 執行個體以及網域的相關監控資訊。

備註 Horizon 7 無法判斷 Kerberos 網域的相關狀態資訊。即使當網域已設定且在運作中，Horizon Administrator 也會將 Kerberos 網域狀態顯示為不明。

程序

1 在 Horizon Administrator 中，按一下**儀表板**。

2 在 [系統健全狀況] 窗格中，展開 **View 元件**、**vSphere 元件**或**其他元件**。

- 綠色向上箭頭表示元件沒有問題。
- 紅色向下箭頭表示元件無法使用或未運作。
- 黃色雙向箭頭表示元件為警告狀態。
- 問號表示元件狀態不明。

3 按一下元件名稱。

對話方塊隨即顯示名稱、版本、狀態與其他元件資訊。

後續步驟

使用 vCenter Server 監控任何 vSAN 叢集，以及 vSAN 資料存放區內包含的磁碟。如需在 vSphere 5.5 Update 1 中監控 vSAN 的詳細資訊，請參閱《vSphere 儲存區》文件和《vSphere 監控和效能》說明文件。如需 vSphere 6 或更新版本中關於監控 vSAN 的詳細資訊，請參閱《管理 VMware vSAN》文件。

監控機器狀態

您可以使用 Horizon Administrator 儀表板快速調查 Horizon 7 部署中的機器狀態。例如，您可以顯示所有中斷連線的機器，或在維護模式中的機器。

必要條件

自行熟悉虛擬機器狀態值。如需關於虛擬機器狀態的詳細資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈vCenter Server 虛擬機器的狀態〉。

程序

1 在 Horizon Administrator 中，按一下**儀表板**。

2 在「機器狀態」窗格中，展開狀態資料夾。

選項	說明
正在準備	列示當機器正在佈建、刪除或在維護模式中時的狀態。
問題機器	列示錯誤狀態。
準備好可供使用	列示當機器已備妥使用時的狀態。

3 找到機器狀態，並按一下旁邊的超連結數字。

機器頁面會顯示所有其狀態已選取的機器。

後續步驟

按一下機器名稱可查看機器的詳細資料，或按一下 Horizon Administrator 向後箭頭可回到儀表板頁面。

瞭解 Horizon 7 服務

連線伺服器執行個體和安全伺服器作業取決於系統上執行的數個服務。這些系統雖然會自動啟動和停止，但您有時可能會認為有必要手動調整這些服務的作業。

您可以使用 Microsoft Windows 服務工具來停止或啟動 Horizon 7 服務。若您停止連線伺服器主機或安全伺服器上的 Horizon 7 服務，使用者必須等到您重新啟動服務，才能連線至他們的遠端桌面平台或應用程式。您也必須在服務停止執行，或是由服務所控制的 Horizon 7 功能沒有回應時，重新啟動服務。

停止和啟動 Horizon 7 服務

連線伺服器執行個體和安全伺服器作業取決於系統上執行的數個服務。當您疑難排解 Horizon 7 作業問題時，有時可能會發現需要手動停止和啟動這些服務。

當您停止 Horizon 7 服務時，使用者無法連線至他們的遠端桌面平台和應用程式。您應在排定的系統維護期間執行此動作，或是警告使用者，其桌面平台和應用程式將暫時無法使用。

備註 僅停止連線伺服器主機上的 VMware Horizon View 連線伺服器服務，或是安全伺服器上的 VMware Horizon View 安全伺服器服務。請勿停止其他任何元件服務。

必要條件

請參閱連線伺服器主機上的服務和安全伺服器上的服務中的說明，以自行熟悉在連線伺服器主機和安全伺服器上執行的服務。

程序

1. 在命令提示字元處輸入 **services.msc** 以啟動 Windows 服務工具。
2. 在連線伺服器主機上選取 VMware Horizon View 連線伺服器服務，或是在安全伺服器上選取 VMware Horizon View 安全伺服器服務，然後視情況按一下**停止**、**重新啟動**，或**啟動**。
3. 確認所列服務的狀態如預期變更。

連線伺服器主機上的服務

Horizon 7 的作業取決於在連線伺服器主機上執行的數個服務。

表 8-4. Horizon 連線伺服器主機服務

服務名稱	啟動類型	說明
VMware Horizon View Blast 安全閘道	自動	提供安全的 HTML Access 和 Blast Extreme 服務。如果用戶端是透過 Blast 安全閘道連線至連線伺服器，則此服務必須在執行狀態下。
VMware Horizon View 連線伺服器	自動	提供連線 Broker 服務。此服務必須永遠處於執行狀態。當您啟動或停止這項服務時，該服務也會啟動或停止 Framework、訊息匯流排、安全閘道和 Web 服務。此服務不會啟動或停止 VMwareVDMDS 服務或 VMware Horizon View 指令碼主機服務。
VMware Horizon View Framework 元件	手動	提供事件記錄、安全和 COM+ 架構服務。此服務必須永遠處於執行狀態。
VMware Horizon View 訊息匯流排元件	手動	在 Horizon 7 元件之間提供通訊服務。此服務必須永遠處於執行狀態。

表 8-4. Horizon 連線伺服器主機服務 (續)

服務名稱	啟動類型	說明
VMware Horizon View PCoIP 安全閘道	手動	提供 PCoIP 安全閘道服務。如果用戶端是透過 PCoIP 安全閘道連線至連線伺服器，則此服務必須在執行狀態下。
VMware Horizon View 指令碼主機	已停用	針對在您刪除虛擬機器時執行的第三方指令碼提供支援。此服務依預設為停用。若您要執行指令碼，則須啟用此服務。
VMware Horizon View 安全閘道元件	手動	提供一般閘道服務。此服務必須永遠處於執行狀態。
VMware Horizon View Web 元件	手動	提供 Web 服務。此服務必須永遠處於執行狀態。
VMwareVDMDS	自動	提供 LDAP 目錄服務。此服務必須永遠處於執行狀態。在 Horizon 7 升級期間，此服務可確保現有資料能正確移轉。

安全伺服器上的服務

Horizon 7 的作業取決於在安全伺服器上執行的數個服務。

表 8-5. 安全伺服器服務

服務名稱	啟動類型	說明
VMware Horizon View Blast 安全閘道	自動	提供安全的 HTML Access 和 Blast Extreme 服務。如果用戶端是透過 Blast 安全閘道連線至此安全伺服器，則此服務必須處於執行狀態。
VMware Horizon View 安全伺服器	自動	提供安全伺服器服務。此服務必須永遠處於執行狀態。當您啟動或停止這項服務時，該服務也會啟動或停止 Framework 和安全閘道服務。
VMware Horizon View Framework 元件	手動	提供事件記錄、安全和 COM+ 架構服務。此服務必須永遠處於執行狀態。
VMware Horizon View PCoIP 安全閘道	手動	提供 PCoIP 安全閘道服務。如果用戶端是透過 PCoIP 安全閘道連線至此安全伺服器，則此服務必須處於執行狀態。
VMware Horizon View 安全閘道元件	手動	提供一般閘道服務。此服務必須永遠處於執行狀態。

變更產品授權金鑰

如果系統上目前的授權到期，或者您要存取目前未授權的 Horizon 7 功能，則可以使用 Horizon Administrator 來變更產品授權金鑰。根據 VMware Horizon Cloud Service 上的 Horizon 7 部署，您可以取得 Horizon 7 的永久授權或訂閱授權。您可以使用 Horizon Administrator 為網繭將授權模式從訂閱授權變更為永久授權，反之亦然。

您可以在 Horizon 7 執行時將授權新增至 Horizon 7。您不必重新啟動系統，而且桌面平台和應用程式的存取不會中斷。

必要條件

- 為了讓 Horizon 7 以及 View Composer 和已發佈的應用程式等附加功能成功運作，請取得有效的產品授權金鑰。
- 若要使用訂閱授權，請確認已為訂閱授權啟用 Horizon 7。請參閱《Horizon 7 安裝》文件。**授權**面板會顯示關於 Horizon 7 網繭的訂閱授權的資訊。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 產品授權及使用**。

目前授權金鑰的前五個和後五個字元會顯示在**授權**面板中。

2 若要編輯授權金鑰，請按一下**編輯授權**，輸入授權序號並按一下**確定**。

授權面板將顯示更新的授權資訊。

3 (選擇性) 若要為 Horizon 7 網繭從訂閱授權變更為永久授權，請按一下**使用永久授權**，並按一下**確定**。

授權面板將顯示更新的授權資訊。

4 若要為 Horizon 7 網繭從永久授權變更為訂閱授權，請按一下**使用訂閱授權**，並按一下**確定**。然後 VMware Horizon Cloud Service 管理員可以為 Horizon 7 網繭啟用訂閱授權。

授權面板將顯示更新的授權資訊。

5 確認授權到期日。

6 根據產品授權賦予您使用權限的 VMware Horizon 7 版本，確認已啟用或停用桌面平台、應用程式遠端處理和 View Composer 授權。

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

7 確認授權使用量模型符合產品授權中使用的模型。

根據您產品授權的版本和使用量合約而定，會以具名使用者或並行使用者的數目來計算使用量。

監控產品授權使用量

在 Horizon 7 Administrator 中，您可以監控在同時間連線至 Horizon 的作用中使用者。**產品授權及使用**頁面會顯示目前及歷史最高的使用量數目。您可以使用這些數目來追蹤產品授權使用率。您也可以重設歷史使用率資料，並重新以目前資料開始進行記錄。

Horizon 提供兩個授權使用量模型，一個用於具名使用者，另一個用於並行使用者。無論您的產品授權版本或使用量模型合約為何，Horizon 都會計算您環境中的具名使用者和並行使用者數目。

對於具名使用者，Horizon 會計算已存取 Horizon 環境的唯一使用者數目。如果某個具名使用者執行多個單一使用者桌面平台、已發佈的桌面平台和已發佈的應用程式，該使用者只會計算一次。

對於具名使用者，**產品授權及使用**頁面上的**目前**資料行會顯示首次設定 Horizon 部署以來或上次重設**具名使用者計數**以後的使用者數目。**最高**資料行不適用於具名使用者。

對於並行使用者，Horizon 會計算每個工作階段的單一使用者桌面平台連線數目。如果並行使用者執行多個單一使用者桌面平台，則每個連線的桌面平台工作階段會分開計算。

對於並行使用者，系統會計算每個使用者的已發佈桌面平台和應用程式連線數目。如果某個並行使用者執行多個已發佈的桌面平台工作階段和應用程式，即使不同的已發佈桌面平台或應用程式主控於不同的 RDS 主機上，使用者仍僅會計算一次。如果某個並行使用者執行單一使用者桌面平台和其他已發佈的桌面平台和應用程式，則使用者僅會計算一次。

對於並行使用者，**產品授權及使用**頁面上的**最高**資料行會顯示首次設定 Horizon 部署以來或上次重設**最高計數**以後，並行桌面平台工作階段和已發佈的桌面平台及應用程式使用者的最高數目。

您可以監控協作工作階段的數目以及連線至工作階段的工作階段協作者數目。

- 作用中 - 協作工作階段：工作階段擁有者已邀請一或多個使用者加入工作階段的工作階段數目。範例：John 邀請了兩人加入其工作階段，而 Mary 邀請了一人加入其工作階段。無論是否有任何受邀者加入工作階段，此資料列的值皆為 2。
- 作用中 - 協作者總數：已連線至協作工作階段的使用者總數，包括工作階段擁有者和任何協作者。範例：John 邀請了兩人，但只有一人加入工作階段。Mary 邀請了一人，但該受邀者並未加入工作階段。此資料列的值為 3：John 的協作工作階段中有一個主要受邀者和一個次要受邀者，而 Mary 的協作工作階段有一個主要受邀者和零個次要受邀者。由於工作階段擁有者會納入計算，因此協作者總數保證永遠大於或等於協作工作階段總數。

重設產品授權使用量資料

在 Horizon Administrator 中，您可以重設歷史產品使用量資料，並重新以目前資料開始進行記錄。

具備**管理全域組態和原則**權限的管理員可以選取**重設最高計數**和**重設具名使用者計數**設定。若要限制對這些設定的存取，請只將此權限授予指定的管理員。

必要條件

自行熟悉產品授權使用量。請參閱監控產品授權使用量。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > 產品授權及使用**。

2 (選擇性) 在**使用量**窗格中，選取**重設最高計數**。

  並行連線的歷史最高數目會重設為目前的數目。

3 (選擇性) 在**使用量**窗格中，選取**重設具名使用者計數**。

從 Active Directory 更新一般使用者資訊

您可以利用儲存在 Active Directory 中的目前使用者資訊來更新 Horizon 7。此功能會更新 Horizon 7 使用者的姓名、電話、電子郵件、使用者名稱和預設的 Windows 網域。此外也會更新信任的外部網域。

若您修改 Active Directory 中受信任的外部網域清單，尤其是網域間經過變更之信任關係會影響 Horizon 7 中的使用者權限時，請使用此功能。

此功能會掃描 Active Directory 中的最新使用者資訊，並重新整理 Horizon 7 組態。

更新一般使用者資訊也會將具名使用者的數目重設為 0。此數目會出現在 Horizon Administrator 的**產品授權及使用**頁面上。請參閱重設產品授權使用量資料。

您也可以使用 `vdmadmin` 命令來更新使用者和網域資訊。請參閱使用 -F 選項更新外部安全性主體。

必要條件

確認您能夠以具有**管理全域組態和原則**權限的管理員身分登入 Horizon Administrator。

程序

1 在 Horizon Administrator 中，按一下**使用者與群組**。

2 選擇要更新所有使用者還是個別使用者的資訊。

選項	動作
所有使用者	按一下**更新一般使用者資訊**。 更新所有使用者和群組會花很長的時間。
個別使用者	a 按一下您要更新的使用者名稱。 b 按一下**更新一般使用者資訊**。

將 View Composer 移轉至其他機器

在某些狀況下，您可能需要將 VMware Horizon View Composer 服務移轉至新的 Windows Server 虛擬或實體機器。例如，您可以將 View Composer 與 vCenter Server 移轉至新的 ESXi 主機或叢集，以展開 Horizon 7 部署。此外，不必將 View Composer 與 vCenter Server 安裝在同一部 Windows Server 機器上。

您可將 View Composer 自 vCenter Server 機器移轉至獨立機器，或自獨立機器移轉至 vCenter Server 機器。

- View Composer 移轉指導方針

  移轉 VMware Horizon View Composer 服務所需的步驟，視您是否要保留現有的連結複製虛擬機器而定。

- 移轉具有現有資料庫的 View Composer

  當您將 View Composer 移轉至另一部實體或虛擬機器後，如果您想要保留目前的連結複製虛擬機器，則新的 VMware Horizon View Composer 服務必須繼續使用現有的 View Composer 資料庫。

- 移轉無連結複製虛擬機器的 View Composer

  如果目前的 VMware Horizon View Composer 服務無法管理任何連結複製虛擬機器，您可以將 View Composer 移轉至新的實體或虛擬機器，而無需將 RSA 金鑰移轉至新機器。移轉後的 VMware Horizon View Composer 服務可連線至原始 View Composer 資料庫，或者您可以為 View Composer 準備新的資料庫。

- 針對移轉 Migrating RSA 金鑰準備 Microsoft .NET Framework

  若要使用現有的 View Composer 資料庫，您必須在機器之間移轉 RSA 金鑰容器。您可以使用 Microsoft .NET Framework 隨附的 ASP.NET IIS 登錄工具，來移轉 RSA 金鑰容器。

- 將 RSA 金鑰容器移轉至新的 View Composer 服務

  若要使用現有的 View Composer 資料庫，您必須將 RSA 金鑰容器從現有 VMware Horizon View Composer 服務所在的來源實體或虛擬機器，移轉至您要安裝新 VMware Horizon View Composer 服務的機器上。

View Composer 移轉指導方針

移轉 VMware Horizon View Composer 服務所需的步驟，視您是否要保留現有的連結複製虛擬機器而定。

若要在部署中保留連結複製虛擬機器，則您安裝在新的虛擬或實體機器上的 VMware Horizon View Composer 服務必須繼續使用現有的 View Composer 資料庫。View Composer 資料庫包含建立、佈建、維護及刪除連結複製所需的資料。

移轉 VMware Horizon View Composer 服務時，您也可以將 View Composer 資料庫移轉至新機器。

無論您是否移轉 View Composer 資料庫，該資料庫都必須設定在與 VMware Horizon View Composer 服務安裝所在新機器相同的網域或信任網域中的可用機器上。

View Composer 會建立 RSA 金鑰組，以加密與解密儲存在 View Composer 資料庫中的驗證資訊。若要讓此資料來源與新的 VMware Horizon View Composer 服務相容，您必須移轉由原始 VMware Horizon View Composer 服務建立的 RSA 金鑰容器。您必須將 RSA 金鑰容器匯入到您安裝新服務的機器。

如果目前的 VMware Horizon View Composer 服務無法管理任何連結複製虛擬機器，您可以移轉該服務，而無需使用現有的 View Composer 資料庫。您不必移轉 RSA 金鑰，無論您是否使用現有的資料庫。

備註 VMware Horizon View Composer 服務的每個執行個體必須有自己的 View Composer 資料庫。多個 VMware Horizon View Composer 服務無法共用一個 View Composer 資料庫。

移轉具有現有資料庫的 View Composer

當您將 View Composer 移轉至另一部實體或虛擬機器後，如果您想要保留目前的連結複製虛擬機器，則新的 VMware Horizon View Composer 服務必須繼續使用現有的 View Composer 資料庫。

當您以下列任何方向移轉 View Composer 時，請依照此程序中的步驟：

- 從 vCenter Server 機器到獨立機器
- 從獨立機器到 vCenter Server 機器
- 從一台獨立機器到另一台獨立機器
- 從一台 vCenter Server 機器到另一台 vCenter Server 機器

移轉 VMware Horizon View Composer 服務時，您也可以將 View Composer 資料庫移轉至新位置。例如，如果目前資料庫位於您正在移轉的 vCenter Server 機器，您必須也移轉 View Composer 資料庫。

當您將 VMware Horizon View Composer 服務安裝在新機器上時，您必須將該服務設定為連線至 View Composer 資料庫。

必要條件

- 自行熟悉 View Composer 移轉需求。請參閱 View Composer 移轉指導方針。

- 請自行熟悉將 RSA 金鑰容器移轉至新 VMware Horizon View Composer 服務的步驟。請參閱針對移轉 Migrating RSA 金鑰準備 Microsoft .NET Framework 與將 RSA 金鑰容器移轉至新的 View Composer 服務。
- 在《Horizon 7 安裝》文件中自行熟悉如何安裝 VMware Horizon View Composer 服務。
- 自行熟悉《Horizon 7 安裝》文件中的設定 View Composer 的 TLS 憑證。
- 自行熟悉如何在 Horizon Administrator 中設定 View Composer。請參閱設定 View Composer 與設定 View Composer 網域。
- 最佳做法是確認您用於移轉 View Composer 的來源和目的地機器相同且共用相同的管理員認證。將 View Composer 從獨立機器移轉至已安裝 View Composer 的 vCenter Server 機器時，如果在兩個機器上使用的認證不同，則設定 View Composer 可能會失敗。

程序

1 在與 VMware Horizon View Composer 服務相關聯的 vCenter Server 執行個體中停用虛擬機器佈建。

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

   b 在 **vCenter Server** 索引標籤上，選取 vCenter Server 執行個體，並按一下**停用佈建**。

2 (選擇性) 將 View Composer 資料庫移轉至新位置。

   如果您需要採取此步驟，請詢問資料庫管理員相關的移轉指示。

3 解除安裝目前機器上的 VMware Horizon View Composer 服務。

4 將 RSA 金鑰容器移轉至新機器。

5 將 VMware Horizon View Composer 服務安裝在新機器上。

   安裝期間，請指定原始 VMware Horizon View Composer 服務所使用資料庫的 DSN。此外也指定先前為該資料庫所提供 ODBC 資料來源的網域管理員名稱與密碼。

   如果您已移轉資料庫，則 DSN 與資料來源資訊必須指向資料庫的新位置。無論您是否已移轉資料庫，新的 VMware Horizon View Composer 服務都必須有權存取有關連結複製的原始資料庫資訊。

6 設定新機器上 View Composer 的 SSL 伺服器憑證。

   您可以複製原始機器上為 View Composer 安裝的憑證，或安裝新的憑證。

7 在 Horizon Administrator 中，設定新的 View Composer 設定。

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

   b 在 **vCenter Server** 索引標籤上，選取與此 View Composer 服務相關聯的 vCenter Server 執行個體，然後按一下**編輯**。

   c 在 View Composer Server [設定] 窗格中，按一下**編輯**並提供新的 View Composer 設定。

      如果您要將 View Composer 連同 vCenter Server 一起安裝在新機器上，請選取 **View Composer 與 vCenter Server 並行安裝**。

      如果您要將 View Composer 安裝在獨立機器上，請選取**獨立式 View Composer Server**，並提供 View Composer 機器的 FQDN，以及 View Composer 使用者的使用者名稱和密碼。

d 在網域窗格中，按一下**驗證伺服器資訊**，並視需要新增或編輯 View Composer 網域。

e 按一下**確定**。

移轉無連結複製虛擬機器的 View Composer

如果目前的 VMware Horizon View Composer 服務無法管理任何連結複製虛擬機器，您可以將 View Composer 移轉至新的實體或虛擬機器，而無需將 RSA 金鑰移轉至新機器。移轉後的 VMware Horizon View Composer 服務可連線至原始 View Composer 資料庫，或者您可以為 View Composer 準備新的資料庫。

必要條件

- 在《Horizon 7 安裝》文件中自行熟悉如何安裝 VMware Horizon View Composer 服務。
- 在《Horizon 7 安裝》文件中自行熟悉如何設定 View Composer 的 TLS 憑證。
- 請熟悉將 View Composer 從 Horizon Administrator 移除的步驟。請參閱從 Horizon 7 移除 View Composer。

  請先確認 View Composer 不再管理任何的連結複製桌面，再移除 View Composer。如果有任何連結複製殘留，您必須將它刪除。
- 自行熟悉如何在 Horizon Administrator 中設定 View Composer。請參閱設定 View Composer 與設定 View Composer 網域。

程序

1 在 Horizon Administrator 中，從 Horizon Administrator 移除 View Composer。

  a 選取 **View 組態 > 伺服器**。

  b 在 **vCenter Server** 索引標籤上，選取與 View Composer 服務相關聯的 vCenter Server 執行個體，然後按一下**編輯**。

  c 在 View Composer Server 設定窗格中，按一下**編輯**。

  d 選取**不使用 View Composer**，然後按一下**確定**。

2 解除安裝目前機器上的 VMware Horizon View Composer 服務。

3 將 VMware Horizon View Composer 服務安裝在新機器上。

  安裝期間，將 View Composer 設定為連線至原始或新 View Composer 資料庫的 DSN。

4 設定新機器上 View Composer 的 TLS 伺服器憑證。

  您可以複製原始機器上為 View Composer 安裝的憑證，或安裝新的憑證。

5 在 Horizon Administrator 中，設定新的 View Composer 設定。

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

  b 在 **vCenter Server** 索引標籤上，選取與此 View Composer 服務相關聯的 vCenter Server 執行個體，然後按一下**編輯**。

  c 在 [View Composer Server 設定]窗格中，按一下**編輯**。

d 提供新的 View Composer 設定。

如果您要將 View Composer 連同 vCenter Server 一起安裝在新機器上，請選取 **View Composer 與 vCenter Server 並行安裝**。

如果您要將 View Composer 安裝在獨立機器上，請選取**獨立式 View Composer Server**，並提供 View Composer 機器的 FQDN，以及 View Composer 使用者的使用者名稱和密碼。

e 在網域窗格中，按一下**驗證伺服器資訊**，並視需要新增或編輯 View Composer 網域。

f 按一下**確定**。

針對移轉 Migrating RSA 金鑰準備 Microsoft .NET Framework

若要使用現有的 View Composer 資料庫，您必須在機器之間移轉 RSA 金鑰容器。您可以使用 Microsoft .NET Framework 隨附的 ASP.NET IIS 登錄工具，來移轉 RSA 金鑰容器。

必要條件

下載 .NET Framework 並瞭解 ASP.NET IIS 登錄工具。請前往 http://www.microsoft.com/net。

程序

1 將 .NET Framework 安裝在已安裝與現有資料庫相關聯之 VMware Horizon View Composer 服務的實體或虛擬機器上。

2 將 .NET Framework 安裝在您要安裝新 VMware Horizon View Composer 服務的目的地機器上。

後續步驟

將 RSA 金鑰容器移轉至目的地機器。請參閱 將 RSA 金鑰容器移轉至新的 View Composer 服務。

將 RSA 金鑰容器移轉至新的 View Composer 服務

若要使用現有的 View Composer 資料庫，您必須將 RSA 金鑰容器從現有 VMware Horizon View Composer 服務所在的來源實體或虛擬機器，移轉至您要安裝新 VMware Horizon View Composer 服務的機器上。

您必須先執行此程序，再安裝新的 VMware Horizon View Composer 服務。

必要條件

確認來源與目的地機器上已安裝 Microsoft .NET Framework 與 ASP.NET IIS 登錄工具。請參閱針對移轉 Migrating RSA 金鑰準備 Microsoft .NET Framework。

程序

1 在現有 VMware Horizon View Composer 服務所在的來源機器上，開啟命令提示字元，並導覽至 `%windir%\Microsoft.NET\Framework\v2.0`*xxxxx* 目錄。

2 輸入 aspnet_regiis 命令，將 RSA 金鑰組儲存在本機檔案中。

aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri

ASP.NET IIS 登錄工具會將 RSA 公開-私密金鑰組從 SviKeyContainer 容器匯出至 keys.xml 檔案，並將該檔案儲存在本機。

3 將 keys.xml 檔案複製到您要安裝新 VMware Horizon View Composer 服務的目的地機器。

4 在目的地機器上，開啟命令提示字元，並導覽至 %windir%\Microsoft.NET\Framework\v2.0*xxxxx* 目錄。

5 輸入 aspnet_regiis 命令以移轉 RSA 金鑰組資料。

aspnet_regiis -pi "SviKeyContainer" "*path*\keys.xml" -exp

其中 *path* 是所匯出檔案的路徑。

-exp 選項會建立可匯出的金鑰組。如果未來需要移轉，則可從此機器匯出金鑰，並匯入到另一部機器。如果您先前已將金鑰移轉到此機器，但當時未使用 -exp 選項，您可以使用 -exp 選項再次匯入金鑰，讓您可以在未來匯出金鑰。

登錄工具可將金鑰組資料匯入至本機金鑰容器。

後續步驟

將新的 VMware Horizon View Composer 服務安裝在目的地機器上。提供 DSN 與 ODBC 資料來源資訊，該資訊允許 View Composer 連線至原始 VMware Horizon View Composer 服務所使用的相同資料庫資訊。如需安裝指示，請參閱《Horizon 7 安裝》文件中的〈安裝 View Composer〉。

完成這些步驟，將 View Composer 移轉至新機器並使用同一個資料庫。請參閱移轉具有現有資料庫的 View Composer。

更新連線伺服器執行個體、安全伺服器或 View Composer 上的憑證

當您收到更新過的伺服器 TLS 憑證或中繼憑證時，請將憑證匯入至每個連線伺服器、安全伺服器或 View Composer 主機上的 Windows 本機電腦憑證存放區。

伺服器憑證通常在 12 個月後到期。根憑證和中繼憑證則在 5 或 10 年後到期。

如需匯入伺服器憑證和中繼憑證的詳細資訊，請參閱《Horizon 7 安裝》文件中的＜將 Horizon 連線伺服器、安全伺服器或 View Composer 設定為使用新的 TLS 憑證＞。

必要條件

- 在目前的有效憑證到期前，從 CA 取得更新過的伺服器和中繼憑證。
- 確認憑證嵌入式管理單元已新增至 Windows Server (連線伺服器執行個體、安全伺服器或 VMware Horizon View Composer 服務已安裝在其中) 的 MMC 中。

程序

1 將已簽署的 TLS 伺服器憑證匯入至 Windows Server 主機上的 Windows 本機電腦憑證存放區。

   a 在憑證嵌入式管理單元中，將伺服器憑證匯入至**憑證 (本機電腦) > 個人 > 憑證**資料夾。

   b 選取**將這個金鑰設成可匯出**。

   c 按**下一步**，然後再按一下**完成**。

2 在連線伺服器或安全伺服器方面，請刪除核發給 Horizon 7 Server 之舊憑證的憑證易記名稱 **vdm**。

   a 在舊憑證上按右鍵，然後按一下**屬性**

   b 在「一般」索引標籤上，刪除「易記」名稱文字 **vdm**。

3 在連線伺服器或安全伺服器方面，請將憑證易記名稱 **vdm**，新增至用以取代先前憑證的新憑證。

   a 在新憑證上按右鍵，然後按一下**屬性**

   b 在「一般」索引標籤上，在「易記」名稱欄位中，輸入 **vdm**。

   c 按一下**套用**，然後再按一下**確定**。

4 如果是核發給 View Composer 的伺服器憑證，請執行 `SviConfig ReplaceCertificate` 公用程式，將新憑證繫結至 View Composer 使用的連接埠。

   此公用程式會以新的憑證繫結，取代舊的憑證繫結。

   a 停止 VMware Horizon View Composer 服務。

   b 開啟 Windows 命令提示字元，並導覽至 `SviConfig` 執行檔。

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

   c 輸入 `SviConfig ReplaceCertificate` 命令。例如：

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

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

   d 若要選取憑證，請輸入憑證編號，然後按 Enter 鍵。

5 如果核發給連線伺服器、安全伺服器或 View Composer 主機的是中繼憑證，請將中繼憑證的最新更新匯入至 Windows 憑證存放區中的**憑證 (本機電腦) > 中繼憑證授權機構 > 憑證**資料夾。

6 重新啟動 VMware Horizon View 連線伺服器服務、VMware Horizon View 安全伺服器服務或 VMware Horizon View Composer 服務，讓您的變更生效。

加入客戶經驗改進計劃

您可以設定 Horizon 7 以加入 VMware 客戶經驗改進計劃 (CEIP)。

如需 VMware 透過 CEIP 所收集資料類型以及 VMware 如何使用該資料的相關資訊，請參閱 http://www.vmware.com/trustvmware/ceip.html 的信任與保證中心。

若要在 Horizon Client 中設定資料共用，請參閱適當的 Horizon Client 安裝和設定指南。例如，針對 Windows 用戶端，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。若要在 HTML Access 中設定資料共用，請參閱《VMware Horizon HTML Access 安裝和設定指南》文件。

程序

1. 在 Horizon Administrator 中，選取 **View 組態 > 產品授權及使用**。
2. 在**客戶經驗計畫**面板中，按一下**編輯設定**。
3. 若要加入 CEIP，請選取**加入 VMware 客戶經驗改進計劃**。

   若未選取此選項，則無法加入 CEIP。
4. 按一下**確定**。

在 Horizon Administrator 中管理 ThinApp 應用程式

9

您可以使用 Horizon Administrator 散佈與管理 VMware ThinApp 隨附的應用程式。在 Horizon Administrator 中管理 ThinApp 應用程式所需作業包括擷取與儲存應用程式套件、新增 ThinApp 應用程式至 Horizon Administrator，以及將 ThinApp 應用程式指派給機器與桌面平台集區。

您必須具備授權，才能使用 Horizon Administrator 中的 ThinApp 管理功能。

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

本章節討論下列主題：

ThinApp 應用程式的 Horizon 7 需求

擷取並儲存將散佈到 Horizon Administrator 中遠端桌面平台的 ThinApp 應用程式時，您必須符合特定需求。

- 您必須將應用程式封裝為 Microsoft Installation (MSI) 套件。
- 您必須使用 ThinApp 4.6 版或更新版本建立或重新封裝 MSI 套件。
- 您必須將 MSI 套件儲存在連線伺服器主機和遠端桌面平台可存取的 Active Directory 網域中的 Windows 網路共用上。檔案伺服器必須根據電腦帳戶，支援驗證與檔案權限。
- 您必須在裝載 MSI 套件的網路共用上設定檔案和共用權限，才能將讀取權限提供給內建的 Active Directory 群組網域電腦。如果您打算將 ThinApp 應用程式散發到網域控制站，您也必須將讀取權限提供給內建的 Active Directory 群組網域控制站。

- 若要允許使用者存取串流的 ThinApp 應用程式套件，必須為使用者將主控 ThinApp 套件之網路共用的 NTFS 權限設定為讀取與執行。
- 請確定脫離的命名空間不會防止網域成員電腦存取裝載 MSI 套件的網路共用。當 Active Directory 網域名稱不同於該網域中的機器所使用的 DNS 命名空間時，就會發生脫離的命名空間。如需詳細資訊，請參閱 VMware 知識庫 (KB) 文章 1023309。
- 若要在遠端桌面平台上執行串流的 ThinApp 應用程式，使用者必須能夠存取裝載 MSI 套件的網路共用。

擷取和儲存應用程式套件

ThinApp 會將應用程式從基礎作業系統及其程式庫和架構中分離，並且將應用程式綁定到稱為應用程式套件的單一可執行檔，以進行應用程式虛擬化。

若要管理 Horizon Administrator 中的 ThinApp 應用程式，您必須使用 ThinApp **安裝程式擷取**精靈擷取應用程式，並將應用程式封裝為 MSI 格式，然後將 MSI 套件儲存於應用程式存放庫。

應用程式存放庫是 Windows 網路共用。您可使用 Horizon Administrator 登錄網路共用成為應用程式存放庫。您可以註冊多個應用程式存放庫。

備註 如果您有多個應用程式存放庫，可使用第三方解決方案管理負載平衡及可用性。Horizon 7 不包含負載平衡或可用性解決方案。

如需 ThinApp 功能及如何使用 ThinApp **安裝程式擷取**精靈的完整資訊，請參閱 VMware ThinApp 簡介及 ThinApp 使用者指南。

程序

1 封裝應用程式

使用 ThinApp **安裝程式擷取**精靈可擷取並封裝您的應用程式。

2 建立 Windows 網路共用

您必須建立 Windows 網路共用以裝載散佈給 Horizon Administrator 中遠端桌面平台和集區的 MSI 套件。

3 註冊應用程式存放庫

您必須將主控 MSI 套件的 Windows 網路共用登錄成為 Horizon Administrator 中的應用程式存放庫。

4 將 ThinApp 應用程式新增至 Horizon Administrator

您可以掃描應用程式存放庫，並選取 ThinApp 應用程式，以將 ThinApp 應用程式新增至 Horizon Administrator。將 ThinApp 應用程式新增至 Horizon Administrator 後，即可指派至機器和桌面平台集區。

5 建立 ThinApp 範本

您可以在 Horizon Administrator 中建立範本以指定 ThinApp 應用程式的群組。您可以使用範本將應用程式分組，可依功能、廠商或任何其他在組織中合理的邏輯分組方法。

封裝應用程式

使用 ThinApp **安裝程式擷取**精靈可擷取並封裝您的應用程式。

必要條件

- 從 http://www.vmware.com/products/thinapp 下載 ThinApp 軟體，並安裝在一部乾淨的電腦上。View 支援 ThinApp 4.6 及更新版本。
- 自行熟悉《ThinApp 使用者指南》中的 ThinApp 軟體需求與應用程式封裝指示。

程序

1. 啟動 ThinApp **安裝程式擷取**精靈，並依照精靈的提示進行。
2. 當 ThinApp **安裝程式擷取**精靈提示您提供專案位置時，請選取**建立 MSI 套件**。
3. 如果您打算將應用程式串流至遠端桌面平台，請將 `package.ini` 檔案中的 MSIStreaming 屬性設為 1。

```
MSIStreaming=1
```

ThinApp **安裝程式擷取**精靈便會將應用程式、執行該應用程式所需的所有元件及應用程式本身封裝至 MSI 套件中。

後續步驟

建立 Windows 網路共用以儲存 MSI 套件。

建立 Windows 網路共用

您必須建立 Windows 網路共用以裝載散佈給 Horizon Administrator 中遠端桌面平台和集區的 MSI 套件。

必要條件

- 使用 ThinApp **安裝程式擷取**精靈以封裝應用程式。
- 確認網路共用符合 Horizon 7 儲存 ThinApp 應用程式的需求。如需詳細資訊，請參閱 ThinApp 應用程式的 Horizon 7 需求。

程序

1. 在電腦上的 Active Directory 網域中建立共用資料夾，使其可供連線伺服器主機和遠端桌面平台存取。
2. 在共用資料夾上設定檔案和共用權限，以將讀取存取權提供給內建 Active Directory 群組的網域電腦。
3. 如果您打算將 ThinApp 應用程式指派給網域控制站，則請將讀取存取權提供給內建 Active Directory 群組的網域控制站。
4. 如果您打算使用串流 ThinApp 應用程式套件，請為使用者將主控 ThinApp 套件之網路共用的 NTFS 權限設為讀取與執行。
5. 將 MSI 套件複製到共用資料夾。

後續步驟

在 Horizon Administrator 中，將 Windows 網路共用登錄為應用程式存放庫。

註冊應用程式存放庫

您必須將主控 MSI 套件的 Windows 網路共用登錄成為 Horizon Administrator 中的應用程式存放庫。

您可以註冊多個應用程式存放庫。

必要條件

建立 Windows 網路共用。

程序

1 在 Horizon Administrator 中，選取 **View 組態 > ThinApp 組態**，然後按一下**新增存放庫**。

2 在**顯示名稱**文字方塊中輸入應用程式存放區的顯示名稱。

3 在**共用路徑**文字方塊中，輸入託管應用程式套件的 Windows 網路共用的路徑。

網路共用路徑的格式必須是 *\\ServerComputerName\ShareName*，其中 *ServerComputerName* 是伺服器電腦的 DNS 名稱。不要指定 IP 位址。

例如：`\\server.domain.com\MSIPackages`

4 按一下**儲存**向 Horizon Administrator 登錄應用程式存放庫。

將 ThinApp 應用程式新增至 Horizon Administrator

您可以掃描應用程式存放庫，並選取 ThinApp 應用程式，以將 ThinApp 應用程式新增至 Horizon Administrator。將 ThinApp 應用程式新增至 Horizon Administrator 後，即可指派至機器和桌面平台集區。

必要條件

透過 Horizon Administrator 登錄應用程式存放庫。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**。

2 按一下**摘要**索引標籤中的**掃描新 ThinApp**。

3 選取要掃描的應用程式存放庫及資料夾，並按**下一步**。

如果應用程式存放庫包含子資料夾，即可展開根資料夾，並選取子資料夾。

4 選取要新增至 Horizon Administrator 的 ThinApp 應用程式。

您可以透過 Ctrl+按一下或 Shift+按一下，選取多個 ThinApp 應用程式。

5 按一下**掃描**，開始掃描選取的 MSI 封裝。

如果要停止掃描，可按一下**停止掃描**。

Horizon Administrator 將報告各個掃描作業的狀態，以及新增至 Horizon Administrator 的 ThinApp 應用程式數目。如果選取 Horizon Administrator 中已存在的應用程式，則不會再次新增。

6 按一下**完成**。

新的 ThinApp 應用程式隨即出現在**摘要**索引標籤上。

後續步驟

(選用) 建立 ThinApp 範本。

建立 ThinApp 範本

您可以在 Horizon Administrator 中建立範本以指定 ThinApp 應用程式的群組。您可以使用範本將應用程式分組，可依功能、廠商或任何其他在組織中合理的邏輯分組方法。

有了 ThinApp 範本，您就可以簡化多個應用程式的散佈程序。將 ThinApp 範本指派給機器或桌面平台集區時，Horizon Administrator 會安裝目前範本中的所有應用程式。

建立 ThinApp 範本為選用。

備註 如果在將範本指派給機器或桌面平台集區之後，將應用程式新增至 ThinApp 範本的話，Horizon Administrator 就不會將新的應用程式自動指派給機器或桌面平台集區。如果是先前指派給機器或桌面平台集區的 ThinApp 範本，而您移除其中的應用程式，應用程式仍會維持指派給機器或桌面平台集區。

必要條件

將所選的 ThinApp 應用程式新增至 Horizon Administrator。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**，然後按一下**新增範本**。

2 輸入範本名稱，然後按一下**新增**。

此時所有可用的 ThinApp 應用程式都會出現在資料表中。

3 若要尋找特定 ThinApp 應用程式，請在**尋找**文字方塊中輸入應用程式的名稱，然後按一下**尋找**。

4 選取您要包含在範本中的 ThinApp 應用程式，然後按一下**新增**。

您可以按住 Ctrl 再按一下或按住 Shift 再按一下以選取多個應用程式。

5 按一下**確定**以儲存範本。

將 ThinApp 應用程式指派給機器和桌面平台集區

若要在遠端桌面平台安裝 ThinApp 應用程式，可使用 Horizon Administrator 將 ThinApp 應用程式指派給機器或桌面平台集區。

將 ThinApp 應用程式指派給機器時，Horizon Administrator 將在幾分鐘後開始在虛擬機器上安裝應用程式。將 ThinApp 應用程式指派給桌面平台集區時，Horizon Administrator 將在使用者第一次登入集區中的遠端桌面平台時開始安裝應用程式。

串流	Horizon Administrator 可在遠端桌面平台上安裝 ThinApp 應用程式的捷徑。此捷徑指向存放庫所在的網路共用上的 ThinApp 應用程式。使用者必須有權存取網路共用，才能執行串流的 ThinApp 應用程式。
完整	Horizon Administrator 可在本機檔案系統安裝完整 ThinApp 應用程式。

安裝 ThinApp 應用程式所需的時間取決於應用程式的大小。

重要 您可以將 ThinApp 應用程式指派給虛擬機器型桌面平台和自動化桌面平台集區或包含 vCenter Server 虛擬機器的手動集區。您無法將 ThinApp 應用程式指派給已發佈的桌面平台或傳統電腦。

- 指定 ThinApp 應用程式的最佳做法

  將 ThinApp 應用程式指派至機器和桌面平台集區時，遵循最佳做法。
- 將 ThinApp 應用程式指派至多台機器

  您可以將特定 ThinApp 指派至一或多台機器。
- 將多個 ThinApp 應用程式指派至機器

  您可以將一或多個 ThinApp 應用程式指派至特定機器。
- 將 ThinApp 應用程式指派給多個桌面平台集區

  您可以將特定 ThinApp 應用程式指派給一或多個桌面平台集區。
- 將多個 ThinApp 應用程式指派至桌面平台集區

  您可以將一或多個 ThinApp 應用程式指派至特定的桌面平台集區。
- 將 ThinApp 範本指派給機器或桌面平台集區

  您可以將 ThinApp 範本指派給機器或桌面平台集區，來精簡多個 ThinApp 應用程式的散佈程序。
- 檢閱 ThinApp 應用程式指派

  您可以檢閱特定 ThinApp 應用程式目前被指派到的所有機器和桌面平台集區。您也可以檢閱指派給特定機器或桌面平台集區的所有 ThinApp 應用程式。
- 顯示 MSI 套件資訊

  將 ThinApp 應用程式新增至 Horizon Administrator 後，即可顯示有關其 MSI 套件的資訊。

指定 ThinApp 應用程式的最佳做法

將 ThinApp 應用程式指派至機器和桌面平台集區時，遵循最佳做法。

- 若要在特定遠端桌面平台上安裝 ThinApp 應用程式，請將應用程式指派至主控該桌面平台的虛擬機器。如果對於機器使用一般命名慣例，可以使用機器指派將應用程式快速散佈到使用該命名慣例的所有機器。

- 若要在桌面平台集區中的所有機器上安裝 ThinApp 應用程式，請將該應用程式指派至桌面平台集區。如果您按照部門或使用者類型組織桌面平台集區，可使用桌面平台集區指派將應用程式快速散佈到特定部門或使用者。例如，如果您有會計部門使用者的桌面平台集區，可將應用程式指派至會計集區，藉以將相同的應用程式散佈到會計部門中所有的使用者。
- 若要簡化多個 ThinApp 應用程式的散佈，請將應用程式加入 ThinApp 範本中。將 ThinApp 範本指派至機器或桌面平台集區時，Horizon Administrator 將安裝目前範本中所有的應用程式。
- 如果範本包含已指派至機器或桌面平台集區的 ThinApp 應用程式，請勿將 ThinApp 範本指派至該機器或桌面平台集區。另外，請勿以不同的安裝類型，將 ThinApp 範本多次指派至相同的機器或桌面平台集區。Horizon Administrator 將在這些情況下傳回 ThinApp 指派錯誤。

將 ThinApp 應用程式指派至多台機器

您可以將特定 ThinApp 指派至一或多台機器。

必要條件

掃描應用程式存放庫，並且將選取的 ThinApp 應用程式新增至 Horizon Administrator。請參閱將 ThinApp 應用程式新增至 Horizon Administrator。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**，並選取 ThinApp 應用程式。

2 從**新增指派**下拉式功能表中選取**指派機器**。

尚未指派 ThinApp 應用程式的機器將出現在資料表中。

選項	動作
尋找特定機器	在**尋找**文字方塊中輸入機器的名稱，並按一下**尋找**。
尋找所有依循相同命名慣例的機器	在**尋找**文字方塊中輸入部分機器名稱，並按一下**尋找**。

3 選取要指派 ThinApp 應用程式的機器，並按一下**新增**。

您可以按住 Ctrl 再按一下或按住 Shift 再按一下以選取多台機器。

4 選取安裝類型，並按一下**確定**。

選項	動作
串流	在機器上安裝應用程式的捷徑。此捷徑指向存放庫所在的網路共用上的應用程式。使用者必須有權存取網路共用，才能執行應用程式。
完整	在機器的本機檔案系統上安裝完整應用程式。

某些 ThinApp 應用程式不支援兩種安裝類型。建立應用程式套件的方式將決定可用的安裝類型。

Horizon Administrator 將在幾分鐘後開始安裝 ThinApp 應用程式。安裝完成後，應用程式即可供由虛擬機器主控之桌面平台的所有使用者使用。

將多個 ThinApp 應用程式指派至機器

您可以將一或多個 ThinApp 應用程式指派至特定機器。

必要條件

掃描應用程式存放庫，並且將選取的 ThinApp 應用程式新增至 Horizon Administrator。請參閱將 ThinApp 應用程式新增至 Horizon Administrator。

程序

1 在 Horizon Administrator 中，選取**資源 > 機器**，然後連按兩下 [機器] 欄中的機器名稱。

2 在**摘要**索引標籤中，按一下 ThinApp 窗格中的**新增指派**。

尚未指派至機器的 ThinApp 應用程式隨即出現在資料表中。

3 若要尋找特定應用程式，可在**尋找**文字方塊中輸入應用程式的名稱，並按一下**尋找**。

4 選取要指派至機器的 ThinApp 應用程式，並按一下**新增**。

若要新增多個應用程式，可重複此步驟。

5 選取安裝類型，並按一下**確定**。

選項	動作
串流	在機器上安裝應用程式的捷徑。此捷徑指向存放庫所在的網路共用上的應用程式。使用者必須有權存取網路共用，才能執行應用程式。
完整	在機器的本機檔案系統上安裝完整應用程式。

某些 ThinApp 應用程式不支援兩種安裝類型。建立應用程式套件的方式將決定可用的安裝類型。

Horizon Administrator 將在幾分鐘後開始安裝 ThinApp 應用程式。安裝完成後，應用程式即可供由虛擬機器主控之桌面平台的所有使用者使用。

將 ThinApp 應用程式指派給多個桌面平台集區

您可以將特定 ThinApp 應用程式指派給一或多個桌面平台集區。

如果將 ThinApp 應用程式指派至連結複製集區，並且稍後重新整理、重新撰寫或重新平衡該集區，Horizon Administrator 將為您重新安裝該應用程式。您不必手動重新安裝應用程式。

必要條件

掃描應用程式存放庫，並且將選取的 ThinApp 應用程式新增至 Horizon Administrator。請參閱將 ThinApp 應用程式新增至 Horizon Administrator。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**，並選取 ThinApp 應用程式。

2 從**新增指派**下拉式功能表中選取**指派桌面平台集區**。

尚未指派 ThinApp 應用程式的桌面平台集區將出現在資料表中。

選項	動作
尋找特定桌面平台集區	在**尋找**文字方塊中輸入桌面平台集區的名稱，並按一下**尋找**。
尋找所有依循相同命名慣例的桌面平台集區	在**尋找**文字方塊中輸入部分桌面平台集區名稱，並按一下**尋找**。

3 選取要指派 ThinApp 應用程式的桌面平台集區，並按一下**新增**。

您可以按住 Ctrl 再按一下或按住 Shift 再按一下，選取多個桌面平台集區。

4 選取安裝類型，並按一下**確定**。

選項	動作
串流	在機器上安裝應用程式的捷徑。此捷徑指向存放庫所在的網路共用上的應用程式。使用者必須有權存取網路共用，才能執行應用程式。
完整	在機器的本機檔案系統上安裝完整應用程式。

某些 ThinApp 應用程式不支援兩種安裝類型。建立應用程式套件的方式將決定可用的安裝類型。

使用者第一次登入集區中的桌面平台時，Horizon Administrator 將開始安裝 ThinApp 應用程式。安裝完成後，應用程式即可供桌面平台集區的所有使用者使用。

將多個 ThinApp 應用程式指派至桌面平台集區

您可以將一或多個 ThinApp 應用程式指派至特定的桌面平台集區。

如果將 ThinApp 應用程式指派至連結複製集區，並且稍後重新整理、重新撰寫或重新平衡該集區，Horizon Administrator 將為您重新安裝該應用程式。您不必手動重新安裝應用程式。

必要條件

掃描應用程式存放庫，並且將選取的 ThinApp 應用程式新增至 Horizon Administrator。請參閱將 ThinApp 應用程式新增至 Horizon Administrator。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > 桌面平台集區**，然後連按兩下集區識別碼。

2 在**詳細目錄**索引標籤上，按一下 **ThinApp**，然後按一下**新增指派**。

尚未指派至集區的 ThinApp 應用程式隨即出現在資料表中。

3 若要尋找特定應用程式，可在**尋找**文字方塊中輸入 ThinApp 應用程式的名稱，並按一下**尋找**。

4 選取要指派至集區的 ThinApp 應用程式，並按一下**新增**。

若要選取多個應用程式，可重複此步驟。

5 選取安裝類型，並按一下**確定**。

選項	動作
串流	在機器上安裝應用程式的捷徑。此捷徑指向存放庫所在的網路共用上的應用程式。使用者必須有權存取網路共用，才能執行應用程式。
完整	在機器的本機檔案系統上安裝完整應用程式。

某些 ThinApp 應用程式不支援兩種安裝類型。建立應用程式套件的方式將決定可用的安裝類型。

使用者第一次登入集區中的桌面平台時，Horizon Administrator 將開始安裝 ThinApp 應用程式。安裝完成後，應用程式即可供桌面平台集區的所有使用者使用。

將 ThinApp 範本指派給機器或桌面平台集區

您可以將 ThinApp 範本指派給機器或桌面平台集區，來精簡多個 ThinApp 應用程式的散佈程序。

將 ThinApp 範本指派給機器或桌面平台集區時，Horizon Administrator 將安裝目前在範本中已有的 ThinApp 應用程式。

必要條件

建立 ThinApp 範本。請參閱建立 ThinApp 範本。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**。

2 選取 ThinApp 範本。

3 從**新增指派**下拉式功能表中選取**指派機器**或**指派桌面平台集區**。

所有機器或桌面平台集區都會出現在資料表中。

選項	動作
尋找特定機器或桌面平台集區	在**尋找**文字方塊中輸入機器或桌面平台集區的名稱，並按一下**尋找**。
尋找所有依循相同命名慣例的機器或桌面平台集區	在**尋找**文字方塊中輸入部分機器或桌面平台集區名稱，並按一下**尋找**。

4 選取要指派 ThinApp 範本的機器或桌面平台集區，並按一下**新增**。

若要選取多個機器或桌面平台集區，可重複此步驟。

5 選取安裝類型，並按一下**確定**。

選項	動作
串流	在機器上安裝應用程式的捷徑。此捷徑指向存放庫所在的網路共用上的應用程式。使用者必須有權存取網路共用，才能執行應用程式。
完整	在機器的本機檔案系統上安裝完整應用程式。

某些 ThinApp 應用程式不支援兩種安裝類型。建立應用程式套件的方式將決定可用的安裝類型。

將 ThinApp 範本指派給機器時，Horizon Administrator 將在幾分鐘後開始安裝範本中的應用程式。將 ThinApp 範本指派給桌面平台集區時，Horizon Administrator 將在使用者第一次登入桌面平台集區中的遠端桌面平台時開始安裝範本中的應用程式。安裝完成後，應用程式即可供機器或桌面平台集區的所有使用者使用。

如果 ThinApp 範本包含已指派給機器或桌面平台集區的應用程式，則 Horizon Administrator 將傳回應用程式指派錯誤。

檢閱 ThinApp 應用程式指派

您可以檢閱特定 ThinApp 應用程式目前被指派到的所有機器和桌面平台集區。您也可以檢閱指派給特定機器或桌面平台集區的所有 ThinApp 應用程式。

必要條件

自行熟悉 ThinApp 應用程式安裝狀態值中的 ThinApp 安裝狀態值。

程序

- 選取您要檢閱的 ThinApp 應用程式指派。

選項	動作
檢閱特定 ThinApp 應用程式被指派到的所有機器和桌面平台集區	選取**類別目錄 > ThinApp**，再按兩下 ThinApp 應用程式的名稱。 **指派**索引標籤顯示應用程式目前被指派到的機器和桌面平台集區，包括安裝類型。 **機器**索引標籤顯示目前與應用程式相關聯的機器，包括安裝狀態資訊。 **備註** 當您將 ThinApp 應用程式指派給集區時，集區中的機器只會在應用程式安裝後，才顯示在**機器**索引標籤上。
檢閱指派給特定機器的所有 ThinApp 應用程式	選取**資源 > 機器**，然後在 [機器] 欄中按兩下機器名稱。 **摘要**索引標籤上的 ThinApp 窗格會顯示目前指派給機器的每個應用程式，包括安裝狀態。
檢閱指派給特定桌面平台集區的所有 ThinApp 應用程式	選取**類別目錄 > 桌面平台集區**，按兩下集區識別碼，選取**詳細目錄**索引標籤，然後按一下 **ThinApp**。 [ThinApp 指派] 窗格會顯示目前指派給桌面平台集區的每個應用程式。

ThinApp 應用程式安裝狀態值

在您將 ThinApp 應用程式指派給機器或集區之後，Horizon Administrator 會指出安裝狀態。

下表說明每個狀態值。

表 9-1. ThinApp 應用程式安裝狀態

狀態	說明
已指派	ThinApp 應用程式已指派給機器。
安裝錯誤	當 Horizon Administrator 試圖安裝 ThinApp 應用程式時發生錯誤。
解除安裝錯誤	當 Horizon Administrator 試圖解除安裝 ThinApp 應用程式時發生錯誤。
已安裝	ThinApp 應用程式已經安裝。

表 9-1. ThinApp 應用程式安裝狀態 (續)

狀態	說明
正在擱置安裝	Horizon Administrator 正試圖安裝 ThinApp 應用程式。 您不能取消指派具有此狀態的應用程式。 **備註** 桌面平台集區中的機器不會出現此值。
正在擱置解除安裝	Horizon Administrator 正試圖解除安裝 ThinApp 應用程式。

顯示 MSI 套件資訊

將 ThinApp 應用程式新增至 Horizon Administrator 後，即可顯示有關其 MSI 套件的資訊。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**。

摘要索引標籤會列出目前可用的應用程式，並顯示完整和串流指派的數目。

2 按兩下 ThinApp 欄中的應用程式名稱。

3 選取**摘要**索引標籤以查看有關 MSI 套件的一般資訊。

4 按一下**套件資訊**以查看有關 MSI 套件的詳細資訊。

在 Horizon Administrator 中維護 ThinApp 應用程式

在 Horizon Administrator 中維護 ThinApp 應用程式所需的工作包括移除 ThinApp 應用程式指派、移除 ThinApp 應用程式與應用程式存放庫，及修改與刪除 ThinApp 範本。

備註 若要升級 ThinApp 應用程式，您必須取消指定並移除舊版的應用程式，然後新增並指定新版的應用程式。

- 將 ThinApp 應用程式指派從多個機器中移除

  您可以將對特定 ThinApp 應用程式指派從一或多個機器中移除。
- 將多個 ThinApp 應用程式指派從機器中移除

  您可以將一或多個 ThinApp 應用程式指派從特定機器中移除。
- 從多個桌面平台集區中移除 ThinApp 應用程式指派

  您可以從一或多個桌面平台集區中移除對特定 ThinApp 應用程式指派。
- 從桌面平台集區中移除多個 ThinApp 應用程式指派

  可以從特定桌面平台集區中移除一或多個 ThinApp 應用程式指派
- 將 ThinApp 應用程式從 Horizon Administrator 中移除

  當您將 ThinApp 應用程式從 Horizon Administrator 移除後，您便再也無法將應用程式指派給機器與桌面平台集區。

- 修改或刪除 ThinApp 範本

  您可以從 ThinApp 範本中新增與移除應用程式。您也可以刪除 ThinApp 範本。

- 移除應用程式存放庫

  您可以將應用程式存放庫從 Horizon Administrator 中移除。

將 ThinApp 應用程式指派從多個機器中移除

您可以將對特定 ThinApp 應用程式指派從一或多個機器中移除。

必要條件

通知機器主控的遠端桌面平台使用者您打算移除應用程式。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**，然後按兩下 ThinApp 應用程式的名稱。

2 在**指派**索引標籤上，選取機器並按一下**移除指派**。

  您可以按住 Ctrl 再按一下或按住 Shift 再按一下以選取多台機器。

Horizon Administrator 會在幾分鐘後解除安裝 ThinApp 應用程式。

重要　如果當 Horizon Administrator 嘗試解除安裝應用程式時，使用者正在使用 ThinApp 應用程式，則解除安裝會失敗，應用程式狀態會變更為 [解除安裝錯誤]。發生此錯誤時，您必須先手動解除安裝機器中的 ThinApp 應用程式檔案，再按一下 Horizon Administrator 中的**移除桌面平台的應用程式狀態**。

將多個 ThinApp 應用程式指派從機器中移除

您可以將一或多個 ThinApp 應用程式指派從特定機器中移除。

必要條件

通知機器主控的遠端桌面平台使用者您打算移除應用程式。

程序

1 在 Horizon Administrator 中，選取**資源 > 機器**，然後連按兩下 [機器] 欄中的機器名稱。

2 在**摘要**索引標籤中，選取 ThinApp 應用程式，按一下 ThinApp 窗格中的**移除指派**。

  重複此步驟移除其他的應用程式指派。

Horizon Administrator 會在幾分鐘後解除安裝 ThinApp 應用程式。

重要　如果當 Horizon Administrator 嘗試解除安裝應用程式時，使用者正在使用 ThinApp 應用程式，則解除安裝會失敗，應用程式狀態會變更為 [解除安裝錯誤]。發生此錯誤時，您必須先手動解除安裝機器中的 ThinApp 應用程式檔案，再按一下 Horizon Administrator 中的**移除桌面平台的應用程式狀態**。

從多個桌面平台集區中移除 ThinApp 應用程式指派

您可以從一或多個桌面平台集區中移除對特定 ThinApp 應用程式指派。

必要條件

通知集區中遠端桌面平台的使用者您打算移除應用程式。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**，然後按兩下 ThinApp 應用程式的名稱。

2 在**指派**索引標籤上，選取桌面平台集區並按一下**移除指派**。

您可以按住 Ctrl 再按一下或按住 Shift 再按一下，選取多個桌面平台集區。

使用者第一次登入集區中的遠端桌面平台時，Horizon Administrator 會解除安裝 ThinApp 應用程式。

從桌面平台集區中移除多個 ThinApp 應用程式指派

可以從特定桌面平台集區中移除一或多個 ThinApp 應用程式指派

必要條件

通知集區中遠端桌面平台的使用者您打算移除應用程式。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > 桌面平台集區**，然後連按兩下集區識別碼。

2 在**詳細目錄**索引標籤上，按一下 **ThinApp**，選取 ThinApp 應用程式，並按一下**移除指派**。

重複此步驟移除多個應用程式。

使用者第一次登入集區中的遠端桌面平台時，Horizon Administrator 會解除安裝 ThinApp 應用程式。

將 ThinApp 應用程式從 Horizon Administrator 中移除

當您將 ThinApp 應用程式從 Horizon Administrator 移除後，您便再也無法將應用程式指派給機器與桌面平台集區。

如果您的組織決定使用其他版本的應用程式取代 ThinApp 應用程式，您可能需要將該應用程式移除。

備註 如果 ThinApp 應用程式已指派給機器或桌面平台集區，或是在 [正在擱置解除安裝] 狀態，則您無法移除 ThinApp 應用程式。

必要條件

如果 ThinApp 應用程式目前已指派給機器或桌面平台集區，請將該指派從機器或桌面平台集區移除。

程序

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**，並選取 ThinApp 應用程式。

2 按一下**移除 ThinApp**。

3 按一下**確定**。

修改或刪除 ThinApp 範本

您可以從 ThinApp 範本中新增與移除應用程式。您也可以刪除 ThinApp 範本。

如果在將範本指派給機器或桌面平台集區之後，將應用程式新增至 ThinApp 範本的話，Horizon Administrator 就不會將新的應用程式自動指派給機器或桌面平台集區。如果是先前指派給機器或桌面平台集區的 ThinApp 範本，而您移除其中的應用程式，應用程式仍會維持指派給機器或桌面平台集區。

程序

- 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**，並選取 ThinApp 範本。

選項	動作
從範本新增或移除 ThinApp 應用程式	按一下**編輯範本**。
刪除範本	按一下**移除範本**。

移除應用程式存放庫

您可以將應用程式存放庫從 Horizon Administrator 中移除。

如果您不再需要應用程式存放庫中包含的 MSI 套件，或者您必須將 MSI 套件移至不同的網路共用，則您必須移除應用程式存放庫。您在 Horizon Administrator 中無法編輯應用程式存放庫的共用路徑。

程序

1. 在 Horizon Administrator 中，選取 **View 組態 > ThinApp 組態**，再選取應用程式存放庫。
2. 按一下**移除存放庫**。

在 Horizon Administrator 中監視與疑難排解 ThinApp 應用程式

Horizon Administrator 會將與 ThinApp 應用程式管理相關的事件記錄到「事件與報告」資料庫。您可以在 Horizon Administrator 的**事件**頁面上檢視這些事件。

當發生下列狀況時，事件會出現在**事件**頁面上。

- ThinApp 應用程式已指派，或應用程式指派已移除。
- ThinApp 應用程式在機器上已安裝或解除安裝
- ThinApp 應用程式無法安裝或解除安裝
- 已從 Horizon Administrator 登錄、修改或移除 ThinApp 應用程式存放庫。
- ThinApp 應用程式已新增至 Horizon Administrator

對於常見的 ThinApp 應用程式管理問題都提供疑難排解提示。

無法註冊應用程式存放庫

您無法在 Horizon Administrator 中登錄應用程式存放庫。

問題

您嘗試在 Horizon Administrator 中登錄應用程式存放庫時，出現錯誤訊息。

原因

連線伺服器主機無法存取主控應用程式存放庫的網路共用。您在**共用路徑**文字方塊中輸入的網路共用路徑可能不正確，主控應用程式存放庫的網路共用位於連線伺服器主機無法存取的網域，或者未正確設定網路共用權限。

解決方案

- 如果網路共用路徑不正確，請輸入正確的網路共用路徑。不支援包含 IP 位址的網路共用路徑。
- 如果網路共用並非位於可存取的網域，請將應用程式套件複製到可從連線伺服器主機存取的網域中的網路共用。
- 確認共用資料夾的檔案及共用權限授予內建 Active Directory 群組網域電腦的讀取權。如果您計劃將 ThinApp 指派給網域控制站，請確認檔案及共用權限也授予內建 Active Directory 群組網域控制站的讀取權。設定或變更權限後，需要長達 20 分鐘的時間才可存取網路共用。

無法將 ThinApp 應用程式新增至 Horizon Administrator

Horizon Administrator 無法將 ThinApp 應用程式新增至 Horizon Administrator。

問題

按一下 Horizon Administrator 中的**掃描新 ThinApp** 時，沒有任何 MSI 套件可用。

原因

應用程式套件並非 MSI 格式，或者連線伺服器主機無法存取網路共用中的目錄。

解決方案

- 確認應用程式存放庫中的應用程式套件為 MSI 格式。
- 確認網路共用符合 ThinApp 應用程式的 Horizon 7 需求。如需詳細資訊，請參閱 ThinApp 應用程式的 Horizon 7 需求。
- 確認對網路共用中的目錄具備適當的權限。如需詳細資訊，請參閱無法註冊應用程式存放庫。

掃描應用程式存放庫時，連線伺服器偵錯記錄檔中將出現訊息。連線伺服器記錄檔位於連線伺服器主機的 *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs 目錄中。

無法指定 ThinApp 範本

您無法將 ThinApp 範本指派給機器或桌面平台集區。

問題

您嘗試將 ThinApp 範本指派給機器或桌面平台集區時，Horizon Administrator 將傳回指派錯誤。

原因

ThinApp 範本包含已指派給機器或桌面平台集區的應用程式，或者先前已將 ThinApp 範本指派給不同安裝類型的機器或桌面平台集區。

解決方案

如果範本包含已指派給機器或桌面平台集區的 ThinApp 應用程式，請建立不包含應用程式的新範本，或編輯現有範本，並移除應用程式。將新範本或修改的範本指派給機器或桌面平台集區。

若要變更 ThinApp 應用程式的安裝類型，您必須移除機器或桌面平台集區的現有應用程式指派。解除安裝 ThinApp 應用程式後，即可將其指派給不同安裝類型的機器或桌面平台集區。

ThinApp 應用程式尚未安裝

Horizon Administrator 無法安裝 ThinApp 應用程式。

問題

ThinApp 應用程式安裝狀態顯示「正在擱置安裝」或「安裝錯誤」。

原因

造成此問題的常見原因包括：

- 機器的磁碟空間不足，無法安裝 ThinApp 應用程式。
- 連線伺服器主機和機器之間，或是連線伺服器主機和應用程式存放庫之間失去網路連線。
- 無法在網路共用中存取 ThinApp 應用程式。
- 之前已經安裝過 ThinApp 應用程式，或是機器已有目錄或檔案。

您可以參閱 Horizon Agent 和連線伺服器記錄檔，以取得問題成因的詳細資訊。

Horizon Agent 記錄檔位於機器的 *drive*:\ProgramData\VMware\VDM\logs 中。

連線伺服器記錄檔位於連線伺服器主機的 *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs 目錄中。

解決方案

1 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**。

2 按一下 ThinApp 應用程式的名稱。

3 在**機器**索引標籤上，選取機器並按一下**重試安裝**，以重新安裝 ThinApp 應用程式。

ThinApp 應用程式尚未解除安裝

Horizon Administrator 無法解除安裝 ThinApp 應用程式。

問題

ThinApp 應用程式安裝狀態顯示「解除安裝錯誤」。

原因

造成此錯誤的常見原因包括：

- 當 Horizon Administrator 嘗試解除安裝 ThinApp 應用程式時，應用程式正忙碌中。
- 失去連線伺服器主機和機器之間的網路連線。

您可以參閱 Horizon Agent 和連線伺服器記錄檔，以取得問題成因的詳細資訊。

Horizon Agent 記錄檔位於機器的 *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs (Windows XP 系統) 和 *drive*:\ProgramData\VMware\VDM\logs (Windows 7 系統) 中。

連線伺服器記錄檔位於連線伺服器主機的 *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs 目錄中。

解決方案

1. 在 Horizon Administrator 中，選取**類別目錄 > ThinApp**。
2. 按一下 ThinApp 應用程式的名稱。
3. 按一下**機器**索引標籤，選取機器，然後按一下**重試解除安裝**，以重試解除安裝作業。
4. 如果解除安裝作業仍然失敗，請手動移除機器上的 ThinApp 應用程式，然後按一下**移除桌面平台的應用程式狀態**。

   此命令會清除 Horizon Administrator 中的 ThinApp 應用程式指派。它不會移除機器上的任何檔案或設定。

   重要 只在手動移除機器的 ThinApp 應用程式之後，才使用此命令。

MSI 套件無效

Horizon Administrator 回報應用程式存放庫中的 MSI 套件無效。

問題

Horizon Administrator 回報 MSI 套件在掃描作業期間無效。

原因

此問題的一般原因如下：

- MSI 檔案損毀。
- MSI 檔案不是使用 ThinApp 建立的。
- MSI 檔案是使用不支援的 ThinApp 版本建立或重新封裝的。您必須使用 ThinApp 4.6 或更新版本。

解決方案

請參閱 ThinApp 使用者指南以取得疑難排解 MSI 套件問題的資訊。

ThinApp 組態範例

ThinApp 組態範例帶您逐步瞭解一般的 ThinApp 組態過程，從擷取和封裝應用程式開始，到檢查安裝狀態為止。

必要條件

請參閱下列主題，以取得在此範例中執行各項步驟的完整資訊。

- 擷取和儲存應用程式套件
- 將 ThinApp 應用程式指派給機器和桌面平台集區

程序

程序

1 從 http://www.vmware.com/products/thinapp 下載 ThinApp 軟體，並安裝在一部乾淨的電腦上。

Horizon 7 支援 ThinApp 4.6 及更新版本。

2 使用 ThinApp **安裝程式擷取**精靈，以 MSI 格式擷取和封裝您的應用程式。

3 在 Active Directory 網域 (連線伺服器主機和遠端桌面平台均可存取) 中的電腦上建立共用資料夾，對共用資料夾設定檔案和共用權限，將「讀取」權限授予內建的 Active Directory 群組網域電腦。

若您打算將 ThinApp 應用程式指派給網域控制站，請同時將「讀取」權限授予內建的 Active Directory 群組網域控制站。

4 將 MSI 套件複製到共用資料夾。

5 在 Horizon Administrator 中將共用資料夾登錄為應用程式存放庫。

6 在 Horizon Administrator 中，於應用程式存放庫中掃描 MSI 套件，並將選取的 ThinApp 應用程式新增至 Horizon Administrator。

7 決定是否將 ThinApp 應用程式指派給機器或桌面平台集區。

如果對於機器使用一般命名慣例，可以使用機器指派將應用程式快速散佈到使用該命名慣例的所有機器。如果您按照部門或使用者類型組織桌面平台集區，可使用桌面平台集區指派將應用程式快速散佈到特定部門或使用者。

8 在 Horizon Administrator 中，選取要指派給機器或桌面平台集區的 ThinApp 應用程式，並指定安裝方法。

選項	動作
串流	在機器上安裝應用程式的捷徑。此捷徑指向存放庫所在的網路共用上的應用程式。使用者必須有權存取網路共用，才能執行應用程式。
完整	在機器的本機檔案系統上安裝完整應用程式。

9 在 Horizon Administrator 中，檢查 ThinApp 應用程式的安裝狀態。

設定 Kiosk 模式下的用戶端

10

您可以設定可從 Horizon 7 取得桌面平台存取權的自動用戶端。

Kiosk 模式下的用戶端為精簡型用戶端或鎖定電腦，可執行 Horizon Client 以連線至連線伺服器執行個體，並啟動工作階段。使用者通常不需要登入即可存取用戶端裝置，雖然已發佈的桌面平台可能會要求其為某些應用程式提供驗證資訊。範例應用程式包括醫療資料輸入工作站、航空公司登機站、客戶自助服務點，以及可供大眾存取的資訊終端機。

您應確保桌面平台應用程式針對安全交易實施驗證機制、實體網路能防止竄改和窺探，以及和網路連線的所有裝置均受信任。

Kiosk 模式下的用戶端支援用於遠端存取的標準功能，例如將 USB 裝置自動重新導向至遠端工作階段，以及依據位置列印。

Horizon 7 使用 Horizon 7 4.5 及更新版本中的彈性驗證功能，驗證 Kiosk 模式下的用戶端裝置，而非使用者。您可以設定連線伺服器執行個體，對符合以下條件的用戶端進行驗證：以 MAC 位址，或開頭是「custom-」字元或您在 ADAM 定義之替代首碼字串的使用者名稱，來自我識別的用戶端。若您將用戶端設定為具有自動產生的密碼，則無需指定密碼，即可在裝置上執行 Horizon Client。若您設定明確的密碼，則必須將此密碼指定至 Horizon Client。由於您通常會從指令碼執行 Horizon Client，而且密碼會以純文字形式顯示，您應該防範未獲授權的使用者讀取指令碼。

只有經您啟用、可對 Kiosk 模式下的用戶端進行驗證的連線伺服器執行個體，才能從符合以下條件的帳戶接受連線：開頭是「cm-」字元且後跟 MAC 位址，或開頭是「custom-」或您所定義的替代字串的帳戶。Horizon 7 4.5 及更新版本的 Horizon Client 不允許手動輸入這些形式的使用者名稱。

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

本章節討論下列主題：

將用戶端設定為 Kiosk 模式

若要設定 Active Directory 及 Horizon 7 以支援處於 Kiosk 模式的用戶端，必須依序執行幾項工作。

必要條件

確認您有執行組態工作所需的權限。

- Active Directory 中用來變更網域使用者和群組帳戶的 **Domain Admins** 或 **Account Operators** 憑證。
- **管理員**、**詳細目錄管理員**，或使用 Horizon Administrator 授權使用者或群組存取遠端桌面平台的同等角色。
- **管理員**或執行 `vdmadmin` 命令的同等角色。

程序

1 針對 Kiosk 模式中的用戶端備妥 Active Directory 與 Horizon 7

您必須設定 Active Directory 接受您建立用來驗證用戶端裝置的帳戶。只要您建立一個群組，您也必須將該群組授權給用戶端存取的桌面平台集區。您也可以備妥用戶端使用的桌面平台集區。

2 為 Kiosk 模式下的用戶端設定預設值

您可以使用 `vdmadmin` 命令，在 Active Directory 中為 kiosk 模式下的用戶端，設定組織單位、密碼到期和群組成員資格的預設值。

3 顯示用戶端裝置的 MAC 位址

如果您要建立以其 MAC 位址為基礎的用戶端帳戶，可以使用 Horizon Client 來搜索用戶端裝置的 MAC 位址。

4 在 Kiosk 模式下新增用戶端的帳戶

您可以使用 `vdmadmin` 命令，將用戶端的帳戶新增至連線伺服器群組的組態。新增用戶端後，啟用用戶端驗證的連線伺服器執行個體即可與該用戶端搭配使用。您也可以更新用戶端的組態，或從系統移除用戶端的帳戶。

5 以 Kiosk 模式啟用用戶端驗證

您可以使用 `vdmadmin` 命令，對嘗試透過連線伺服器執行個體連線至其遠端桌面平台的用戶端啟用驗證。

6 驗證 Kiosk 模式下的用戶端組態

您可以使用 `vdmadmin` 命令來顯示處於 Kiosk 模式的用戶端相關資訊，以及設定為驗證這類用戶端之連線伺服器執行個體的相關資訊。

7 在 Kiosk 模式下從用戶端連線至遠端桌面平台

您可以從命令列執行用戶端，或使用指令碼將用戶端連線至遠端工作階段。

針對 Kiosk 模式中的用戶端備妥 Active Directory 與 Horizon 7

您必須設定 Active Directory 接受您建立用來驗證用戶端裝置的帳戶。只要您建立一個群組，您也必須將該群組授權給用戶端存取的桌面平台集區。您也可以備妥用戶端使用的桌面平台集區。

最佳做法是，建立另外的組織單位與群組，以減少您管理 Kiosk 模式用戶端的工作。您可以為不屬於任何群組的用戶端新增個別帳戶，但如果您設定的用戶端數量較多，這會產生很大的額外管理負荷。

程序

1 在 Active Directory 中，建立另外的組織單位與群組以搭配 Kiosk 模式的用戶端使用。

您必須為該群組指定 Windows 2000 之前的名稱。您使用此名稱來識別 `vdmadmin` 命令群組。

2 為客體虛擬機器建立映像或範本。

您可使用由 vCenter Server 管理的虛擬機器做為自動集區的範本、做為連結複製集區的父系，或做為手動桌面平台集區的虛擬機器。您也可以在客體作業系統上安裝與設定應用程式。

3 設定客體作業系統，讓用戶端保持自動時不會被鎖定。

Horizon 7 會為在 Kiosk 模式中連線的用戶端隱藏登入前訊息。如果您需要事件去解除鎖定畫面並顯示訊息，您可以在客體作業系統上設定適當的應用程式。

4 在 Horizon Administrator 中，建立用戶端將使用的桌面平台集區，並將群組授權給此集區。

例如，您可以選擇建立浮動指派、連結複製桌面平台集區成為最適合您用戶端應用程式需求的桌面平台集區。您也可以將一或多個 ThinApp 應用程式與桌面平台集區建立關聯。

重要 請勿將用戶端或群組授權給多個桌面平台集區。如果您這麼做，Horizon 7 會從獲得用戶端授權的集區隨機指派遠端桌面平台，並產生警告事件。

5 如果您要為用戶端啟用依據位置列印，請設定以下 Active Directory 群組原則設定：`AutoConnect Location-based Printing for VMware View`，此設定位於電腦設定下 `Software Settings` 資料夾中的 Microsoft 群組原則物件編輯器內。

6 設定其他您必須最佳化的原則，並保護用戶端的遠端桌面平台。

例如，您可能要覆寫當本機 USB 裝置啟動或插入時連線至遠端桌面平台的原則。依預設，Windows 版 Horizon Client 會為 Kiosk 模式中的用戶端啟用這些原則。

範例： 針對 Kiosk 模式中的用戶端備妥 Active Directory

公司內部網路的網域為 MYORG，其組織單位的辨別名稱為 OU=myorg-ou,DC=myorg,DC=com。在 Active Directory 中，您可以建立辨別名稱為 OU=kiosk-ou,DC=myorg,DC=com 的組織單位 kiosk-ou，並建立群組 kc-grp 以搭配 Kiosk 模式中的用戶端使用。

後續步驟

設定用戶端的預設值。

為 Kiosk 模式下的用戶端設定預設值

您可以使用 `vdmadmin` 命令，在 Active Directory 中為 kiosk 模式下的用戶端，設定組織單位、密碼到期和群組成員資格的預設值。

在用戶端將用來連線至其已發佈桌面平台的連線伺服器執行個體所在的群組中，您必須對其中一個連線伺服器執行個體執行 `vdmadmin` 命令。

設定密碼到期日和 Active Directory 群組成員資格的預設值後，這些設定都會由群組中的所有連線伺服器執行個體共用。

程序

- 為用戶端設定預設值。

```
vdmadmin
-Q
-clientauth
-setdefaults [-b authentication_arguments] [-ouDN] [ -expirepassword | -noexpirepassword ]
[-groupgroup_name | -nogroup]
```

選項	說明
-expirepassword	指定用戶端帳戶的密碼到期時間，與連線伺服器群組相同。如果未定義群組的到期時間，則密碼不會到期。
-group *group_name*	對要新增用戶端帳戶的預設群組指定名稱。必須指定群組的名稱作為 Active Directory 的 Windows 2000 以前版本群組名稱。
-noexpirepassword	指定用戶端帳戶密碼不會過期。
-nogroup	清除預設群組的設定。
-ou *DN*	指定預設組織單位 (用戶端帳戶即新增至其中) 的辨別名稱。 例如：OU=kiosk-ou,DC=myorg,DC=com **備註** 您不能使用此命令來變更組織單位的組態。

此命令會為連線伺服器群組中的用戶端更新預設值。

範例： 為 Kiosk 模式下的用戶端設定預設值

設定組織單位、密碼到期日及用戶端群組成員資格的預設值。

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

後續步驟

為使用 MAC 位址來進行驗證的用戶端裝置找出其 MAC 位址。

顯示用戶端裝置的 MAC 位址

如果您要建立以其 MAC 位址為基礎的用戶端帳戶，可以使用 Horizon Client 來搜索用戶端裝置的 MAC 位址。

必要條件

在用戶端的主控台上登入。

程序

- 若要顯示 MAC 位址，請輸入適用於您平台的命令。

選項	動作
Windows	輸入 **C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo** 用戶端會使用您為其設定的預設連線伺服器執行個體。如果您未設定預設值，用戶端會提示您設定該值。 該命令會顯示 IP 位址、MAC 位址及用戶端裝置的機器名稱。
Linux	輸入 **vmware-view --printEnvironmentInfo -s *connection_server*** 您必須指定連線伺服器執行個體的 IP 位址或 FQDN，用戶端會用它來連線至桌面平台。 該命令會顯示 IP 位址、MAC 位址、機器名稱、網域、名稱、任何登入使用者的名稱和網域，以及用戶端裝置的時區。

後續步驟

新增用戶端帳戶。

在 Kiosk 模式下新增用戶端的帳戶

您可以使用 vdmadmin 命令，將用戶端的帳戶新增至連線伺服器群組的組態。新增用戶端後，啟用用戶端驗證的連線伺服器執行個體即可與該用戶端搭配使用。您也可以更新用戶端的組態，或從系統移除用戶端的帳戶。

在用戶端將用來連線至其已發佈桌面平台的連線伺服器執行個體所在的群組中，您必須對其中一個連線伺服器執行個體執行 vdmadmin 命令。

在 Kiosk 模式下新增用戶端時，Horizon 7 將在 Active Directory 中建立用戶端的使用者帳戶。如果指定用戶端的名稱，此名稱的開頭必須是已辨識的首碼字串，例如 "custom-"，或者是在 ADAM 中定義的備用首碼字串，而且長度不可超過 20 個字元。如果您不指定用戶端的名稱，Horizon 7 將從您為用戶端裝置所指定的 MAC 位址產生名稱。例如，如果 MAC 位址為 00:10:db:ee:76:80，則對應的帳戶名稱為 cm-00_10_db_ee_76_80。您僅能將這些帳戶用於您啟用以驗證用戶端的連線伺服器執行個體。

重要 請勿將一個指定的名稱用於多個用戶端裝置。未來版本可能不支援此組態。

程序

- 使用 -domain 及 -clientid 選項執行 vdmadmin 命令，指定用戶端的網域，以及用戶端的名稱或 MAC 位址。

```
vdmadmin
-Q
```

```
            -clientauth
            -add [-bauthentication_arguments] -domaindomain_name-clientidclient_id [-password
"password" | -genpassword] [-ouDN] [-expirepassword | -noexpirepassword] [-groupgroup_name | -nogroup]
[-description "description_text"]
```

選項	說明
-clientid *client_id*	指定用戶端的名稱或 MAC 位址。
-description "*description_text*"	為 Active Directory 中的用戶端裝置建立帳戶的說明。
-domain *domain_name*	指定用戶端的網域。
-expirepassword	指定用戶端帳戶上密碼的到期時間與連線伺服器群組相同。如果未定義群組的到期時間，則密碼不會到期。
-genpassword	產生用戶端帳戶的密碼。如果您未指定 -password 或 -genpassword，這將是預設行為。 產生的密碼有 16 個字元，至少包含一個大寫字母、一個小寫字母、一個符號及一個數字，並且可包含重複的字元。如果需要強度更高的密碼，可使用 -password 選項指定密碼。
-group *group_name*	指定新增用戶端帳戶的群組名稱。必須指定群組的名稱作為 Active Directory 的 Windows 2000 以前版本群組名稱。如果您先前已設定預設群組，用戶端帳戶將新增至此群組。
-noexpirepassword	指定用戶端帳戶的密碼不到期。
-nogroup	指定用戶端帳戶不新增至預設群組。
-ou *DN*	指定新增用戶端帳戶的組織單位辨別名稱。 例如：OU=kiosk-ou,DC=myorg,DC=com
-password "*password*"	指定用戶端帳戶的明確密碼。

此命令將為指定網域及群組 (如果有) 中的用戶端建立 Active Directory 中的使用者帳戶。

範例： 新增用戶端的帳戶

使用 group kc-grp 的預設設定，將以用戶端 MAC 位址指定的用戶端帳戶新增至 MYORG 網域。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

使用自動產生的密碼，將以用戶端 MAC 位址指定的用戶端帳戶新增至 MYORG 網域。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword
```

新增具名用戶端的帳戶，並指定用於用戶端的密碼。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou
"OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

使用自動產生的密碼，新增具名用戶端的帳戶。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Kiosk11 -genpassword -ou "OU=kiosk-
ou,DC=myorg,DC=com" -description "Kiosk 11"
```

後續步驟

啟用用戶端驗證。

以 Kiosk 模式啟用用戶端驗證

您可以使用 vdmadmin 命令，對嘗試透過連線伺服器執行個體連線至其遠端桌面平台的用戶端啟用驗證。

在用戶端將用來連線至其遠端桌面平台的連線伺服器執行個體所在的群組中，您必須對其中一個連線伺服器執行個體執行 vdmadmin 命令。

雖然您啟用個別連線伺服器執行個體的驗證，但群組中所有連線伺服器執行個體會共用用戶端驗證的所有其他設定。您只需要為用戶端新增帳戶一次。在連線伺服器群組中，任何已啟用的連線伺服器執行個體都可以驗證用戶端。

如果計劃在 RDS 主機上搭配使用 Kiosk 模式和工作階段型桌面平台，您還必須將使用者帳戶新增至遠端桌面平台使用者群組。

程序

1 啟用連線伺服器執行個體上的用戶端驗證。

```
vdmadmin
-Q
-enable [-bauthentication_arguments] -sconnection_server [-requirepassword]
```

選項	說明
-requirepassword	指定您需要用戶端提供密碼。 **重要** 如果您指定此選項，則連線伺服器執行個體無法驗證已自動產生密碼的用戶端。如果您變更連線伺服器執行個體的組態以指定此選項，則這類用戶端無法驗證自己，它們會失敗且出現以下錯誤訊息：使用者名稱不明或密碼不正確。
-s *connection_server*	指定要啟用用戶端驗證的連線伺服器執行個體的 NetBIOS 名稱。

此命令讓指定的連線伺服器執行個體能夠驗證用戶端。

2 如果已發佈的桌面平台是由 Microsoft RDS 主機提供的，請登入 RDS 主機並將使用者帳戶新增至遠端桌面平台使用者群組。

例如，在 Horizon 7 Server 上，將使用者帳戶 custom-11 授權給 RDS 主機上的工作階段型桌面平台。您必須登入 RDS 主機，透過前往**控制台 > 系統及安全性 > 系統 > 遠端設定 > 選取使用者 > 新增**，將使用者 custom-11 新增至遠端桌面平台使用者群組。

範例： 以 Kiosk 模式啟用用戶端驗證

啟用連線伺服器執行個體 csvr-2 的用戶端驗證。具有自動產生密碼的用戶端不須提供密碼即可自行驗證。

```
vdmadmin -Q -enable -s csvr-2
```

啟用連線伺服器執行個體 csvr-3 的用戶端驗證，需要用戶端對 Horizon Client 指定其密碼。具有自動產生密碼的用戶端無法自行驗證。

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

後續步驟

驗證連線伺服器執行個體與用戶端的組態。

驗證 Kiosk 模式下的用戶端組態

您可以使用 vdmadmin 命令來顯示處於 Kiosk 模式的用戶端相關資訊，以及設定為驗證這類用戶端之連線伺服器執行個體的相關資訊。

在用戶端將用來連線至其遠端桌面平台的連線伺服器執行個體所在的群組中，您必須對其中一個連線伺服器執行個體執行 vdmadmin 命令。

程序

- 顯示處於 Kiosk 模式之用戶端及用戶端驗證的相關資訊。

  ```
  vdmadmin
  –Q
  –clientauth
  –list [–b authentication_arguments] [–xml]
  ```

  此命令會顯示處於 Kiosk 模式之用戶端的相關資訊，以及已啟用用戶端驗證之連線伺服器執行個體的相關資訊。

範例： 顯示處於 Kiosk 模式之用戶端的相關資訊

以文字格式顯示用戶端的相關資訊。用戶端 cm-00_0c_29_0d_a3_e6 具有自動產生的密碼，且不需要使用者或應用程式指令碼對 Horizon Client 指定此密碼。用戶端 cm-00_22_19_12_6d_cf 擁有明確指定的密碼，且需要使用者提供。連線伺服器執行個體 CONSVR2 接受來自具有自動產生密碼之用戶端的驗證要求。CONSVR1 不接受 Kiosk 模式下用戶端的驗證要求。

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID               : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID           : cm–00_0c_29_0d_a3_e6
Domain             : myorg.com
Password Generated: true

GUID               : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID           : cm–00_22_19_12_6d_cf
Domain             : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                    : CONSVR1
```

```
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

後續步驟

確認用戶端可以連線至其遠端桌面平台。

在 Kiosk 模式下從用戶端連線至遠端桌面平台

您可以從命令列執行用戶端，或使用指令碼將用戶端連線至遠端工作階段。

您通常都是使用命令指令碼在已部署的用戶端裝置上執行 Horizon Client。

備註 在 Windows 或 Mac 用戶端上，依預設，當遠端桌面工作階段啟動時，如果其他應用程式或服務正在使用用戶端上的 USB 裝置，則不會自動轉送這些裝置。在所有用戶端上，預設不會轉送人機介面裝置 (HID) 和智慧卡讀卡機。

程序

- 若要連線至遠端工作階段，請輸入適用於您平台的命令。

選項	說明	
Windows	輸入 `C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL connection_server] [-userName user_name] [-password password]`	
	`-password`*password*	指定用戶端帳戶的密碼。如果您已定義帳戶的密碼，則必須指定此密碼。
	`-serverURL`*connection_server*	指定連線伺服器執行個體的 IP 位址或 FQDN，Horizon Client 會使用該執行個體來連線至其遠端桌面平台。如果您不指定用戶端將用來連線至遠端桌面平台的連線伺服器執行個體的 IP 位址或 FQDN，則該用戶端就會使用您為其設定的預設連線伺服器執行個體。
	`-userName`*user_name*	指定用戶端帳戶的名稱。如果您不想讓用戶端使用 MAC 位址，而是使用以識別的首碼字串為開頭 (例如 "custom-") 的帳戶名稱來自行驗證，則必須指定此名稱。
Linux	輸入 `vmware-view --unattended -s connection_server [--once] [-u user_name] [-p password]`	
	`--once`	指定您不想讓 Horizon Client 在發生錯誤時重新嘗試連線。 **重要** 您通常應指定此選項，並使用結束碼來處理錯誤。否則，可能會難以遠端結束 `vmware-view` 程序。
	`-p`*password*	指定用戶端帳戶的密碼。如果您已定義帳戶的密碼，則必須指定此密碼。
	`-s`*connection_server*	指定連線伺服器執行個體的 IP 位址或 FQDN，用戶端會使用該執行個體連線至其桌面平台。
	`-u`*user_name*	指定用戶端帳戶的名稱。如果您不想讓用戶端使用 MAC 位址，而是使用以識別的首碼字串為開頭 (例如 "custom-") 的帳戶名稱來自行驗證，則必須指定此名稱。

如果伺服器驗證 Kiosk 用戶端，且遠端桌面平台可用，則命令就會啟動遠端工作階段。

範例： 在 Kiosk 模式下於用戶端上執行 Horizon Client

在帳戶名稱採用本身 MAC 位址並具有自動產生的密碼的 Windows 用戶端上，執行 Horizon Client。

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -serverURL
consvr2.myorg.com
```

使用指派的名稱和密碼在 Linux 用戶端上執行 Horizon Client。

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

疑難排解 Horizon 7

11

您可以使用多種程序來診斷和修正使用 Horizon 7 時可能會遇到的問題。您可以使用 Horizon Help Desk Tool 進行疑難排解、使用其他疑難排解程序調查及更正問題，或從「VMware 技術支援」獲得協助。

如需關於疑難排解桌面平台和桌面平台集區的相關資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件。

本章節討論下列主題：

使用 Horizon Help Desk Tool

Horizon Help Desk Tool 是一個可用來取得 Horizon 7 使用者工作階段狀態及執行疑難排解和維護作業的 Web 應用程式。

在 Horizon Help Desk Tool 中，您可以查閱使用者工作階段，以排解問題及執行桌面平台維護作業，例如重新啟動或重設桌面平台。

若要設定 Horizon Help Desk Tool，您必須符合下列需求：

- Horizon 7 的 Horizon Enterprise 版授權或 Horizon Apps Advanced 版授權。若要確認您擁有正確的授權，請參閱確認 Horizon Help Desk Tool 授權。
- 用來儲存 Horizon 7 元件相關資訊的事件資料庫。如需關於設定事件資料庫的詳細資訊，請參閱《Horizon 7 安裝》文件。
- 用來登入 Horizon Help Desk Tool 的服務台管理員角色或服務台管理員 (唯讀) 角色。如需這些角色的詳細資訊，請參閱設定 Horizon Help Desk Tool 的角色型存取
- 在每個連線伺服器執行個體上啟用計時分析工具以檢視登入區段。

  請使用下列 vdmadmin 命令，在每個連線伺服器執行個體上啟用計時分析工具：

  ```
  vdmadmin -I -timingProfiler -enable
  ```

  請使用下列 vdmadmin 命令，在使用管理連接埠的連線伺服器執行個體上啟用計時分析工具：

  ```
  vdmadmin -I -timingProfiler -enable -server {ip/server}
  ```

確認 Horizon Help Desk Tool 授權

如果您並未擁有有效的產品授權金鑰，則無法登入 Horizon Help Desk Tool。您可以在 Horizon Administrator 中確認產品授權金鑰，並套用有效授權。

必要條件

- 取得 Horizon Enterprise 版授權或 Horizon Apps Advanced 版授權的有效產品授權金鑰。

程序

1. 在 Horizon Administrator 中，選取 **View 組態 > 產品授權及使用**。

   目前授權金鑰的前五個和後五個字元會顯示在**授權**面板中。

2. 確認**服務台授權**欄位中的授權狀態。

選項	說明
已停用	產品授權金鑰無效。您無法登入 Horizon Help Desk Tool。
已啟用	產品授權金鑰有效。您可以登入 Horizon Help Desk Tool。

3. (選擇性) 如果產品授權金鑰無效，請按一下**編輯授權**並輸入有效的授權序號，然後按一下**確定**並重新整理 Horizon Administrator URL。

   產品授權視窗將顯示更新的授權資訊。

後續步驟

登入 Horizon Help Desk Tool。

設定 Horizon Help Desk Tool 的角色型存取

您可以將預先定義的管理員角色指派給 Horizon Help Desk Tool 管理員，以將疑難排解工作委派給不同的管理員使用者。您也可以建立自訂角色，並根據預先定義的管理員角色新增權限。

您可以將下列預先定義的管理員角色指派給 Horizon Help Desk Tool 管理員：

- 服務台管理員
- 服務台管理員 (唯讀)

如果您為 Horizon Help Desk Tool 管理員建立自訂角色，則必須指派 [管理服務台 (唯讀)] 權限，以及根據 [服務台管理員] 角色或 [服務台管理員 (唯讀)] 角色指派任何其他權限。

必要條件

自行熟悉可用於建立自訂角色的管理員權限。請參閱 預先定義的角色和權限。

程序

1. 在 Horizon Administrator 中，選取 **View 組態 > 管理員**，然後按一下**角色**索引標籤。
2. 在**角色**索引標籤上按一下**新增角色**，接著選取 [服務台管理員] 角色或 [服務台管理員 (唯讀)] 角色，然後按一下**確定**。
   a. (選擇性) 若要新增自訂角色，請在**角色**索引標籤上按一下**新增角色**並選取 [管理服務台 (唯讀)] 權限，接著再根據 [服務台管理員] 角色或 [服務台管理員 (唯讀)] 角色選取任何權限，然後按一下**確定**。

登入 Horizon Help Desk Tool

Horizon Help Desk Tool 已整合至 Horizon Console。從 Horizon 7 (7.5 版) 開始，您無法再使用 Horizon Help Desk Tool URL 來登入 Horizon Help Desk Tool。

程序

1. 若要從 Horizon Administrator 登入 Horizon Help Desk Tool，請按一下右上方面板上的 **Horizon Console**。這是對 Horizon Console Web 介面的單一登入。
2. 在 Horizon Console 中，於 [使用者搜尋] 欄位中輸入使用者名稱。

   Horizon Console 會在搜尋結果中顯示使用者的清單。搜尋可以傳回最多 100 個相符的結果。
3. 選取使用者名稱。

   使用者資訊會顯示在使用者卡片中。

後續步驟

若要針對問題進行疑難排解，請在使用者卡片中按一下相關索引標籤。

在 Horizon Help Desk Tool 中對使用者進行疑難排解

在 Horizon Help Desk Tool 中，您可以檢視使用者卡片中的基本使用者資訊。您可以按一下使用者卡片中的索引標籤，以取得關於特定元件的詳細資料。

使用者詳細資料有時會顯示在資料表中。您可以依資料表資料行排序這些使用者詳細資料。

- 若要依遞增順序排序資料行，請按一下資料行。
- 若要依遞減順序排序資料行，請按兩下資料行。
- 若不要排序資料行，請按三下資料行。

基本使用者資訊

顯示基本使用者資訊，例如使用者的使用者名稱、電話號碼和電子郵件地址，以及使用者的連線或中斷連線狀態。如果使用者具有桌面平台或應用程式工作階段，則使用者會處於連線狀態。如果使用者沒有桌面平台或應用程式工作階段，則使用者會處於中斷連線狀態。

您可以按一下電話號碼以開啟商務用 Skype 工作階段，並打電話給使用者而與其協作進行疑難排解。

您也可以按一下電子郵件，以傳送訊息給使用者。

工作階段

工作階段索引標籤會顯示使用者連線的桌面平台或應用程式工作階段的相關資訊。

您可以使用**篩選器**文字方塊篩選桌面平台或應用程式工作階段。

備註　**工作階段**索引標籤不會顯示使用 Microsoft RDP 顯示通訊協定之工作階段的工作階段資訊，或是從 vSphere Client 或 ESXi 存取虛擬機器之工作階段的資訊。

工作階段索引標籤會包含下列資訊：

表 11-1. 工作階段索引標籤

選項	說明
狀態	顯示桌面平台或應用程式工作階段之狀態的相關資訊。 ■ 如果工作階段已連線，則呈現為綠色。 ■ 如果工作階段是本機工作階段，或工作階段執行於本機網繭中，則顯示 L。 ■ 如果工作階段執行於網繭聯盟中的不同網繭，則顯示 G。
電腦名稱	桌面平台或應用程式工作階段的名稱。按一下名稱可開啟卡片中的工作階段資訊。 您可以按一下工作階段卡片中的索引標籤來檢視其他資訊： ■ **詳細資料**索引標籤會顯示使用者資訊，例如虛擬機器資訊、CPU 或記憶體使用量。請參閱 Horizon Help Desk Tool 的工作階段詳細資料。 ■ **處理程序**索引標籤會顯示關於 CPU 和記憶體相關處理程序的資訊。請參閱 Horizon Help Desk Tool 的工作階段處理程序。 ■ **應用程式**索引標籤會顯示關於正在執行之應用程式的詳細資料。請參閱 Horizon Help Desk Tool 的應用程式狀態。
通訊協定	桌面平台或應用程式工作階段的顯示通訊協定。
類型	顯示桌面平台是已發佈的桌面平台、虛擬機器桌面平台還是應用程式。

表 11-1. 工作階段索引標籤 (續)

選項	說明
連線時間	工作階段與連線伺服器連線的時間。
工作階段持續時間	工作階段持續與連線伺服器連線的時間長度。

桌面平台權利

桌面平台權利索引標籤會顯示使用者有權使用的已發佈桌面平台或虛擬桌面平台的相關資訊。

表 11-2. 桌面平台權利

選項	說明
狀態	顯示桌面平台工作階段之狀態的相關資訊。 ■ 如果工作階段已連線，則呈現為綠色。
桌面平台集區名稱	工作階段的桌面平台集區名稱。
桌面平台類型	顯示桌面平台是已發佈的桌面平台還是虛擬機器桌面平台。 **備註** 如果工作階段執行於網繭聯盟中的不同網繭，則不會顯示任何資訊。
類型	顯示桌面平台權利類型的相關資訊。 ■ 若為本機權利，則顯示「本機」。 ■ 若為全域權利，則顯示「全域」。
vCenter	顯示 vCenter Server 中的虛擬機器名稱。 **備註** 如果工作階段執行於網繭聯盟中的不同網繭，則不會顯示任何資訊。
預設通訊協定	桌面平台或應用程式工作階段的預設顯示通訊協定。

應用程式權利

應用程式權利索引標籤會顯示使用者有權使用的已發佈應用程式的相關資訊。

表 11-3. 應用程式權利

選項	說明
狀態	顯示應用程式工作階段之狀態的相關資訊。 ■ 如果工作階段已連線，則呈現為綠色。
應用程式	顯示應用程式集區中已發佈的應用程式名稱。
伺服器陣列	工作階段連線的 RDS 主機所在之伺服器陣列的名稱。 **備註** 就全域應用程式權利而言，此資料行會顯示全域應用程式權利中的伺服器陣列數目。
類型	顯示應用程式權利類型的相關資訊。 ■ 若為本機權利，則顯示「本機」。 ■ 若為全域權利，則顯示「全域」。
發佈者	已發佈應用程式的軟體製造商名稱。

活動

活動索引標籤會顯示關於使用者活動的事件記錄資訊。您可以根據時間範圍篩選活動，例如過去 12 個小時或過去 30 天，或是依管理員名稱來篩選。按一下**僅限服務台事件**，即可僅根據 Horizon Help Desk Tool 活動進行篩選。按一下重新整理圖示以重新整理事件記錄。按一下匯出圖示以將事件記錄匯出為檔案。

備註　對於 CPA 環境中的使用者並不會顯示事件記錄資訊。

表 11-4. 活動

選項	說明
時間	選取時間範圍。預設值為過去 12 個小時。 ■ **過去 12 個小時** ■ **過去 24 個小時** ■ **過去 7 天** ■ **過去 30 天** ■ **全部**
管理員	管理員使用者的名稱。
訊息	針對使用者或管理員顯示其所執行活動的專屬訊息。
資源名稱	顯示活動執行所在桌面平台集區或虛擬機器名稱的相關資訊。

Horizon Help Desk Tool 的工作階段詳細資料

當您在**工作階段**索引標籤上的**電腦名稱**選項中按一下使用者名稱時，**詳細資料**索引標籤上會出現工作階段使用者詳細資料。您可以檢視 Horizon Client、虛擬或已發佈的桌面平台，以及 CPU 和記憶體的詳細資料。

Horizon Client

根據 Horizon Client 的類型顯示資訊，並且包含諸如使用者名稱、Horizon Client 的版本、用戶端機器的 IP 位址，以及用戶端機器的作業系統等詳細資料。

備註　如果您已升級 Horizon Agent，則必須也將 Horizon Client 升級至最新版本。否則將不會顯示 Horizon Client 的版本。如需關於升級 Horizon Client 的詳細資訊，請參閱《Horizon 7 升級》文件。

虛擬機器

顯示虛擬桌面平台或已發佈桌面平台的相關資訊。

表 11-5. 虛擬機器詳細資料

選項	說明
電腦名稱	桌面平台或應用程式工作階段的名稱。
代理程式版本	Horizon Agent 版本。
工作階段狀態	桌面平台或應用程式工作階段的狀態。
狀態持續時間	工作階段保持於相同狀態的時間。
登入時間	登入工作階段之使用者的登入時間。

表 11-5. 虛擬機器詳細資料 (續)

選項	說明
登入持續時間	登入工作階段的使用者持續登入的時間。
工作階段持續時間	工作階段持續與連線伺服器連線的時間。
連線伺服器	工作階段連線的連線伺服器。
Unifted Access Gateway 名稱	Unified Access Gateway 應用裝置的名稱。連線到工作階段後，此資訊可能需要 30 秒到 60 秒才會顯示。
Unified Access Gateway IP	Unified Access Gateway 應用裝置的 IP 位址。連線到工作階段後，此資訊可能需要 30 秒到 60 秒才會顯示。
集區	桌面平台或應用程式集區的名稱。
伺服器陣列	已發佈的桌面平台或應用程式工作階段之 RDS 主機的伺服器陣列。
vCenter	vCenter Server 的 IP 位址。

顯示 Blast 度量

顯示使用 VMware Blast 顯示通訊協定之虛擬或已發佈桌面平台工作階段的效能詳細資料。若要檢視這些效能詳細資料，請按一下**顯示 Blast 度量**。

表 11-6. Blast 顯示通訊協定詳細資料

選項	說明
Blast 工作階段計數器	■ **預估頻寬 (上行)**。上行訊號的預估頻寬。 ■ **封包遺失 (上行)**。上行訊號的封包遺失百分比。
Blast 影像處理計數器	■ **已傳輸的位元組**。已為 Blast 工作階段傳輸之影像處理資料的位元組總數。 ■ **已接收的位元組**。已為 Blast 工作階段接收之影像處理資料的位元組總數。
Blast 音訊計數器	■ **已傳輸的位元組**。已為 Blast 工作階段傳輸之音訊資料的位元組總數。 ■ **已接收的位元組**。已為 Blast 工作階段接收之音訊資料的位元組總數。
Blast CDR 計數器	■ **已傳輸的位元組**。已為 Blast 工作階段傳輸之用戶端磁碟機重新導向資料的位元組總數。 ■ **已接收的位元組**。已為 Blast 工作階段接收之用戶端磁碟機重新導向資料的位元組總數。

CPU、記憶體和延遲

顯示虛擬或已發佈桌面平台或應用程式的 CPU 和記憶體使用量圖，以及 PCoIP 或 Blast 顯示通訊協定的延遲。

表 11-7. CPU、記憶體和延遲的詳細資料

選項	說明
工作階段 CPU	目前工作階段的 CPU 使用率。
主機 CPU	指派工作階段之虛擬機器的 CPU 使用率。
工作階段記憶體	目前工作階段的記憶體使用量。
主機記憶體	指派工作階段之虛擬機器的記憶體使用量。
工作階段延遲	顯示 PCoIP 或 Blast 顯示通訊協定的延遲圖。 針對 Blast 顯示通訊協定，延遲時間即為來回行程時間 (以毫秒為單位)。追蹤此延遲時間的效能計數器為 **VMware Blast 工作階段計數器 > RTT**。 針對 PCoIP 顯示通訊協定，延遲時間即為來回延遲時間 (以毫秒為單位)。追蹤此延遲時間的效能計數器為 **PCoIP 工作階段網路統計資料 > 來回延遲**。

工作階段登入區段

顯示登入持續時間以及在登入期間建立的使用量區段。

表 11-8. 工作階段登入區段

選項	說明
登入持續時間	從使用者按一下桌面平台或應用程式集區時開始，計算到 Windows 檔案總管啟動時為止的時間長度。
工作階段登入時間	使用者登入工作階段的時間長度。
登入區段	顯示在登入期間建立的區段。 ■ **代理**。連線伺服器處理工作階段連線或重新連線的總時間。此時間從使用者按一下桌面平台集區時起算，計算到通道連線設定完成時為止。其中包括使用者驗證、機器選取，以及為了設定通道連線而執行的機器準備等連線伺服器工作所耗費的時間。 ■ **GPO 載入**。執行 Windows 群組原則處理的總時間。若未設定全域原則，則顯示 0。 ■ **設定檔載入**。執行 Windows 使用者設定檔處理的總時間。 ■ **互動式**。Horizon Agent 處理工作階段連線或重新連線作業的總時間。此時間從 PCoIP 或 Blast Extreme 使用通道連線時起算，計算到 Windows 檔案總管啟動時為止。 ■ **驗證**。連線伺服器驗證工作階段的總時間。 ■ **虛擬機器啟動**。啟動虛擬機器所花費的總時間。這段時間包括作業系統開機、繼續執行暫停的機器，以及 Horizon Agent 指出本身已準備好進行連線所花費的時間。

使用登入區段中的資訊進行疑難排解時，請遵循下列準則：

- 如果工作階段是新的虛擬桌面平台工作階段，則會顯示所有登入區段。若未設定全域原則，則 **GPO 載入**登入區段時間會是 0。
- 如果虛擬桌面平台工作階段是從中斷連線的工作階段重新連線的工作階段，則會顯示**登入持續時間**、**互動式**和**代理**登入區段。

- 如果工作階段是已發佈的桌面平台工作階段，則會顯示**登入持續時間**、**GPO 載入**或**設定檔載入**登入區段。針對新的工作階段應會顯示 **GPO 載入**和**設定檔載入**登入區段。如果新的工作階段未顯示這些登入區段，您必須重新啟動 RDS 主機。

Horizon Help Desk Tool 的工作階段處理程序

當您在**工作階段**索引標籤上的**電腦名稱**選項中按一下使用者名稱時，**處理程序**索引標籤上會顯示工作階段處理程序。

處理程序

針對每個工作階段，您可以檢視 CPU 和記憶體相關處理程序的其他詳細資料。例如，如果您發現某個工作階段的 CPU 和記憶體使用量異常偏高，則可以在**處理程序**索引標籤上檢視處理程序的詳細資料。

表 11-9. 工作階段處理程序詳細資料

選項	說明
處理程序名稱	工作階段處理程序的名稱。例如 chrome.exe。
CPU	處理程序的 CPU 使用率 (以百分比為單位)。
記憶體	處理程序的記憶體使用量 (以 KB 為單位)。
磁碟	記憶體磁碟 IOPS。系統會使用下列公式進行計算： (目前時間的 I/O 位元組總數) - (目前時間前一秒的 I/O 位元組總數)。 如果「工作管理員」顯示正值，則此計算顯示的值可能是每秒 0 KB。
使用者名稱	擁有處理程序之使用者的使用者名稱。
主機 CPU	指派工作階段之虛擬機器的 CPU 使用率。
主機記憶體	指派工作階段之虛擬機器的記憶體使用量。
處理程序	虛擬機器中的處理程序計數
重新整理	重新整理圖示會重新整理處理程序的清單。
結束處理程序	結束正在執行的處理程序。 **備註** 您必須具有服務台管理員角色才能結束處理程序。 若要結束處理程序，請選取處理程序，然後按一下**結束處理程序**按鈕。

Horizon Help Desk Tool 的應用程式狀態

當您在**工作階段**索引標籤上的**電腦名稱**選項中按一下使用者名稱時，您可以在**應用程式**索引標籤上檢視應用程式的狀態和詳細資料。

應用程式

您可以檢視每個應用程式目前的狀態和其他詳細資料。

表 11-10. 應用程式詳細資料

選項	說明
應用程式	應用程式的名稱。
說明	應用程式的說明。
狀態	應用程式的狀態。顯示應用程式是否正在執行中。
主機 CPU	指派工作階段之虛擬機器的 CPU 使用率。
主機記憶體	指派工作階段之虛擬機器的記憶體使用量。
應用程式	正在執行中的應用程式清單。
重新整理	重新整理圖示會重新整理應用程式的清單。

在 Horizon Help Desk Tool 中對桌面平台或應用程式工作階段進行疑難排解

在 Horizon Help Desk Tool 中，您可以根據使用者的連線狀態對桌面平台或應用程式工作階段進行疑難排解。

必要條件

- 啟動 Horizon Help Desk Tool。

程序

1 在使用者卡片上，按一下**工作階段**索引標籤。

效能卡隨即出現，顯示 CPU 和記憶體使用量，並且包含 Horizon Client 和虛擬或已發佈桌面平台的相關資訊。

2 選擇疑難排解選項。

選項	動作
傳送訊息	將訊息傳送給已發佈的桌面平台或虛擬桌面平台上的使用者。您可以選擇訊息的嚴重性，以包含「警告」、「資訊」或「錯誤」。 按一下**傳送訊息**，並輸入嚴重性類型和訊息詳細資料，然後按一下**提交**。
遠端協助	您可以為已連線的桌面平台或應用程式工作階段產生遠端協助票證。管理員可使用遠端協助票證來掌控使用者的桌面平台並對問題進行疑難排解。 按一下**遠端協助**，並下載服務台票證檔案。開啟票證，並等候遠端桌面平台上的使用者接受票證。您只能在 Windows 桌面平台上開啟票證。使用者接受票證之後，您可以與使用者交談，並要求控制使用者的桌面平台。 **備註** 服務台遠端協助功能以「Microsoft 遠端協助」為基礎。您必須安裝「Microsoft 遠端協助」，並在已發佈的桌面平台上啟用遠端協助功能。如果「Microsoft 遠端協助」有連線或升級方面的問題，服務台遠端協助功能可能無法啟動。如需詳細資訊，請參閱 Microsoft 網站上的《Microsoft 遠端協助》說明文件。

選項	動作
重新啟動	在虛擬桌面平台上啟動「Windows 重新啟動」程序。此功能不適用於已發佈的桌面平台或應用程式工作階段。 按一下**重新啟動 VDI**。
中斷連線	中斷桌面平台或應用程式工作階段的連線。 按一下**更多 > 中斷連線**。
登出	啟動已發佈的桌面平台或虛擬桌面平台的登出程序，或啟動應用程式工作階段的登出程序。 按一下**更多 > 登出**。
重設	啟動虛擬機器的重設作業。此功能不適用於已發佈的桌面平台或應用程式工作階段。 按一下**更多 > 重設虛擬機器**。 **備註** 使用者可能會遺失未儲存的工作。

使用 VMware 登入監視器

VMware 登入監視器可監控 Windows 使用者登入，以及報告效能度量，目的在於協助管理員、支援人員和開發人員疑難排解緩慢的登入效能。

度量包括登入時間、登入指令碼時間、CPU/記憶體使用量，以及網路連線速度。登入監視器也可以從其他 VMware 產品接收度量以提供登入程序的更多資訊。

支援的平台

登入監視器支援與 Horizon Agent 相同的 Windows 平台。

重要功能

登入監視器提供下列功能：

- 安裝為 Horizon Agent 的一部分。若要啟動服務，請參閱 KB 57051。
- 與 Horizon Help Desk Tool 計時分析工具整合。系統會彙總與登入相關的度量，並傳送至 Horizon Agent 事件資料庫。
- 可讓客戶將記錄上傳至檔案伺服器以便於存取。
- 與其他 VMware 產品整合，例如 Horizon Persona Management、App Volumes、UEM，以及將登入相關事件傳送至登入監視器的 Horizon Agent。登入監視器會在事件發生時記錄事件，以顯示登入流程中的事件及其持續多久。
- 監控相同機器上的並行登入。

記錄

登入監視器會寫入服務狀態訊息和使用者工作階段的記錄檔。依預設，所有記錄檔皆會寫入至 `C:\ProgramData\VMware\VMware Logon Monitor\Logs`。

- 主要記錄檔：主要的記錄檔 `vmlm.txt` 包含在監控登入之前和之後所傳入 vmlm 服務和工作階段事件的所有狀態訊息。檢查此記錄檔以判斷登入監視器是否正確執行。
- 工作階段記錄檔：工作階段記錄檔包含與使用者登入工作階段相關的所有事件。事件會在登入開始時在此記錄檔中啟動，且僅適用於單一使用者工作階段。記錄檔結尾處會寫入摘要，以提供最重要度量的概觀。檢查此記錄檔可疑難排解緩慢的登入。登入完成時，不會有進一步的事件寫入至工作階段記錄檔。

登入監視器度量

登入監視器會計算登入、群組原則、使用者設定檔，以及效能的相關度量。這些度量可提供系統管理員關於登入期間使用者系統的詳細檢視，以協助判斷效能瓶頸的根本原因。

表 11-11. 登入監視器度量

度量	參數	說明
登入時間	■ 啟動 ■ End ■ 時間總計	度量包括客體上登入開始的時間、登入完成的時間，以及載入設定檔和桌面平台顯示的時間，以及在客體上處理登入所耗費的時間總計。排除在客體外所耗費的任何時間。
工作階段開始到登入開始時間	時間總計	從 Windows 建立使用者工作階段直到登入開始之間的時間。
設定檔同步時間	時間總計	Windows 於登入期間耗費在協調使用者設定檔的時間。
殼層載入	■ 啟動 ■ End ■ 時間總計	Windows 會提供使用者殼層載入的開始時間。結束時間為總管視窗建立的時間。
登入到登錄區載入時間	時間總計	此度量提供從登入開始到載入使用者登錄區的時間總計。
Windows 資料夾重新導向	■ 啟動 ■ End ■ 時間總計	與 Windows 資料夾重新導向開始且完整套用時間，以及啟用 Windows 資料夾重新導向時間總計相關的度量。第一次套用資料夾重新導向，或如果正在將新檔案上傳到重新導向共用，則這個時間可能會很高。
群組原則時間	■ 使用者群組原則套用時間 ■ 電腦群組原則套用時間	與將群組原則套用至客體相關的度量，包括套用使用者群組原則和電腦群組原則所耗費的時間。
設定檔度量	■ 設定檔類型：本機、漫遊、暫存 ■ 設定檔大小：檔案數目、資料夾總數、MB 總計	與使用者設定檔相關的度量，指出使用者設定檔類型及其是否儲存在本機電腦、中央設定檔存放區上或在登出後刪除。 設定檔大小包含檔案數目、資料夾總數和使用者設定檔大小總計 (以 MB 為單位) 的度量。

表 11-11. 登入監視器度量 (續)

度量	參數	說明
設定檔大小分佈	■ 介於 0 到 1 MB 之間的檔案數目 ■ 介於 1 MB 到 10 MB 之間的檔案數目 ■ 介於 10 MB 到 100 MB 之間的檔案數目 ■ 介於 100 MB 到 1 GB 之間的檔案數目 ■ 介於 1 GB 到 10 GB 之間的檔案數目	使用者設定檔中各種大小範圍的檔案數目計數。
登入期間啟動的處理程序	■ 名稱 ■ 處理程序識別碼 ■ 父處理程序識別碼 ■ 工作階段識別碼	系統會針對每個處理程序從工作階段開始直到登入完成記錄這些值。
群組原則登入指令碼時間	時間總計	與執行群組原則登入指令碼報告執行群組原則登入指令碼所花費時間總計相關的度量。
群組原則 PowerShell 指令檔時間	時間總計	與執行群組原則 PowerShell 指令檔相關的度量，指出執行群組原則 PowerShell 指令檔所耗費的時間。
記憶體使用量	■ 可用的位元組：最小、最大、平均 ■ 已認可位元組：最小、最大、平均 ■ 分頁集區：最小、最大、平均	登入期間與記憶體使用量相關的 WMI 度量。取樣會在登入完成之前持續進行。預設為停用狀態。
CPU 使用率	■ 閒置 CPU：最小、最大、平均 ■ 使用者 CPU：最小、最大、平均 ■ 核心 CPU：最小、最大、平均	登入期間與 CPU 使用率相關的 WMI 度量。取樣會在登入完成之前持續進行。預設為停用狀態。
登入指令碼是否已同步?		報告群組原則登入指令碼會與登入同步執行或非同步執行。
網路連線狀態	■ 已捨棄 ■ 已還原	報告網路連線是否運作中或是中斷連線。
群組原則軟體安裝	■ 非同步：True/False ■ 錯誤碼 ■ 時間總計	與群組原則軟體安裝相關的度量，指出安裝與登入同步或非同步、安裝成功或失敗，以及使用群組原則安裝軟體所耗費的時間總計。
設定檔磁碟區的磁碟使用量	■ 使用者可用的磁碟空間 ■ 可用磁碟空間 ■ 磁碟空間總計	與存放使用者設定檔之磁碟區上磁碟使用量相關的度量。
網域控制站探索	■ 錯誤碼 ■ 時間總計	網域控制站相關度量。錯誤碼指出網域控制站是否出現故障。
估計的網路頻寬	頻寬	從事件識別碼 5327 所收集的值。
網路連線詳細資料	■ 頻寬 ■ 慢速連結臨界值 ■ 偵測到的慢速連結：True/False	從事件識別碼 5314 所收集的值。

表 11-11. 登入監視器度量 (續)

度量	參數	說明
影響登入時間的設定	■ 電腦\系統管理範本\登入\永遠在電腦啟動與登入時等待網路啟動 ■ 電腦\系統管理範本\登入\當使用者登入時執行這些程式 ■ 電腦\系統管理範本\使用者設定檔\等待漫遊使用者設定檔 ■ 電腦\系統管理範本\使用者設定檔\如果使用者有漫遊設定檔或遠端主目錄，設定網路的最大等待時間 ■ 電腦\系統管理範本\群組原則\設定登入指令碼延遲 ■ 使用者\系統管理範本\系統\登入\當使用者登入時執行這些程式 ■ 使用者\系統管理範本\系統\使用者設定檔\指定網路目錄僅在登入/登出時同步	
來自 Horizon Agent、角色管理、App Volumes 的度量		與登入監視器進行互動的 VMware 產品會在登入監視器記錄檔中報告自訂度量。這些度量可協助判斷這些產品是否可能對登入時間造成負面影響。

登入監視器組態設定

您可以使用 Windows 登錄值來設定登入監視器設定。

登錄設定

若要變更組態設定，請導覽至登錄機碼 `HKLM\Software\VMware, Inc.\VMware Logon Monitor`。

表 11-12. 登入監視器組態值

登錄機碼	類型	說明
RemoteLogPath	REG_SZ	上傳記錄檔的遠端共用路徑。當記錄檔複製到遠端記錄檔共用時會位於 RemoteLogPath 登錄機碼指定的資料夾。範例：`\\server\share\%username%。%userdomain%`。登入監視器會視需要建立資料夾。預設為停用狀態。 ■ 遠端記錄檔資料夾的 UNC 路徑 ■ (選用) 如果未設定則記錄檔不會上傳。 ■ 支援選用的本機環境變數。
Flags	REG_DWORD	此值為影響登入監視器行為的位元遮罩。 ■ 設定或移除以啟用或停用 CPU 和記憶體度量的值為 0x4。預設為停用狀態。 ■ 設定或移除以啟用處理事件和登入指令碼度量的值為 0x8。預設為停用狀態。 ■ 設定以啟用或停用與 Horizon 7 整合的值為 0x2。依預設為啟用。 ■ 設定以停用損毀傾印的值為 0x1。傾印會寫入至 `C:\ProgramData\VMware\VMware Logon Monitor\Data`。預設為停用狀態。 ■ 若要根據每位使用者在遠端路徑中建立資料夾，則需要設定的值為 0x10。預設為停用狀態。

表 11-12. 登入監視器組態值 (續)

登錄機碼	類型	說明
LogMaxSizeMB	REG_DWORD	主要記錄檔的大小上限 (以 MB 為單位)。預設為 100 MB。
LogKeepDays	REG_DWORD	輪流利用主要記錄檔之前保留的天數上限。預設值為 7 天。

計時分析工具設定

登入監視器會與 Horizon Help Desk 計時分析工具整合。計時分析工具依預設為關閉。

- 若要啟用登入監視器以使用計時分析工具將事件寫入至事件資料庫，請執行 `vdmadmin -I -timingProfiler -enable`。
- 若要停用登入監視器以使用計時分析工具，請執行 `vdmadmin -I -timingProfiler -disable`。

使用 VMware Horizon 效能追蹤程式

VMware Horizon 效能追蹤程式是一種公用程式，它會在遠端桌面平台中執行，並監控顯示通訊協定與系統資源使用量的效能。您也可以建立應用程式集區，並以已發佈的應用程式形式執行 Horizon 效能追蹤程式。

設定 VMware Horizon 效能追蹤程式

您可以在遠端桌面平台中執行 Horizon 效能追蹤程式。您也可以已發佈的應用程式形式執行 Horizon 效能追蹤程式。

Horizon 效能追蹤程式功能

Horizon 效能追蹤程式會顯示下列功能的重要資料：

表 11-13. Horizon 效能追蹤程式功能

效能監控	詳細資料
通訊協定的特定資料	■ 編碼器名稱：用於顯示通訊協定的編碼器名稱 ■ 使用的頻寬：顯示通訊協定 (PCoIP 或 Blast) 取樣期間內傳入和傳出頻寬的平均整體頻寬 ■ 每秒畫面播放速率：一秒取樣期間內編碼的影像處理畫面數目 ■ 音訊開啟：音訊功能是否開啟 ■ 音訊已啟動：音訊功能是否已啟動 ■ CPU 使用率: ■ 編碼器 CPU：目前使用者工作階段中顯示通訊協定編碼器的 CPU 使用率 ■ 系統 CPU：系統的 CPU 使用率總計
傳輸類型	■ 用戶端至遠端工作階段：用於從用戶端到遠端對等的 UDP 或 TCP 通訊協定傳輸套件 ■ 遠端工作階段至用戶端：用於從遠端對等到用戶端的 UDP 或 TCP 通訊協定傳輸套件 ■ Horizon Connection Server：用來連線至連線伺服器執行個體的 UDP 或 TCP 通訊協定傳輸套件
系統健全狀況狀態	■ 估計頻寬：Horizon Client 和 Horizon Agent 之間的整體估計可用頻寬 ■ 來回行程：Horizon Agent 和 Horizon Client 之間的來回行程延遲時間 (以毫秒為單位)
工作階段內容	■ 伺服器詳細資料，例如 DNS 名稱、網域名稱、是否使用通道、URL、遠端 IP 位址 ■ 用戶端機器詳細資料，例如顯示器號碼、IP 位址、鍵盤和滑鼠配置、語言、時區
即時通訊協定開關	

備註　Horizon 效能追蹤程式僅在 Horizon Agent 於虛擬桌面平台工作階段上執行時才會收集和顯示資料。

Horizon 效能追蹤程式的系統需求

Horizon 效能追蹤程式支援下列組態。

表 11-14. Horizon 效能追蹤程式系統需求

系統	需求
虛擬桌面平台作業系統	所有支援 Horizon Agent 的作業系統，Linux 代理程式除外。
用戶端機器作業系統	支援所有 Horizon Client 版本，但不支援已發佈應用程式形式的 Linux 版 Horizon Client 和 Windows 10 UWP 版 Horizon Client。
顯示通訊協定	VMware Blast 和 PCoIP
.NET Framework	Horizon 效能追蹤程式需要 .NET Framework 4.0 版或更新版本。

安裝 Horizon 效能追蹤程式

Horizon 效能追蹤程式是 Horizon Agent 安裝程式中的自訂安裝選項。您必須選取該選項，因為依預設不會選取。Horizon 效能追蹤程式同時適用於 IPv4 和 IPv6。

您可以在虛擬桌面平台或 RDS 主機上安裝 Horizon 效能追蹤程式。如果您在 RDS 主機上安裝，可以將其發佈為已發佈的應用程式，並從 Horizon Client 執行已發佈的應用程式。請參閱《在 Horizon 7 中設定已發佈的桌面平台和應用程式》文件。

安裝會在桌面平台建立捷徑。

設定 Horizon 效能追蹤程式群組原則設定

您可以設定群組原則設定來變更預設設定。請參閱設定 Horizon 效能追蹤程式群組原則設定。。

設定 Horizon 效能追蹤程式群組原則設定。

若要設定 Horizon 效能追蹤程式，請在代理程式機器上安裝 Horizon 效能追蹤程式 ADMX 範本檔 (`perf_tracker.admx`)，然後使用本機群組原則編輯器來進行原則設定。

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。

程序

1 從 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 檔案解壓縮出 `perf_tracker.admx` 檔案，並將檔案複製至代理程式機器上的 `%systemroot%\PolicyDefinitions` 資料夾中。

2 從 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` 檔案解壓縮出 `perf_tracker.adml` 檔案，並將檔案複製至代理程式機器上 `%systemroot%\PolicyDefinitions\` 資料夾的 language 子資料夾中。

   例如，將 `perf_tracker.adml` 檔案的 `en_us` 版本複製到 `%systemroot%\PolicyDefinitions\en_us` 子資料夾中。

3 啟動本機群組原則編輯器 (`gpedit.msc`)，然後導覽至**電腦組態 > 系統管理範本 > VMware Horizon 效能追蹤程式**。

4 編輯群組原則設定。

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，當使用者登入至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，當使用者登入至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**。

5 若要讓您的變更生效，請在代理程式機器上重新啟動 Horizon 效能追蹤程式。

執行 Horizon 效能追蹤程式

您可以使用 Horizon Client 在遠端桌面平台內執行 Horizon 效能追蹤程式，或將其執行為已發佈的應用程式。

如果您使用的 Horizon Client 平台支援多個工作階段，則可以從不同伺服器陣列執行多個 Horizon 效能追蹤程式已發佈的應用程式。在支援多個工作階段的 Windows 和 Mac 用戶端上，[概觀] 視窗中的機器名稱會識別已發佈應用程式的來源伺服器陣列。在 Android 和 iOS 用戶端和 HTML Access 上，一次僅支援一個開啟的工作階段。如果您從另一個伺服器陣列開啟第二個工作階段，則第一個工作階段會關閉。

必要條件

- 安裝和設定 Horizon 效能追蹤程式。請參閱設定 VMware Horizon 效能追蹤程式。
- 設定 Horizon 效能追蹤程式群組原則設定。請參閱設定 Horizon 效能追蹤程式群組原則設定。。

程序

- 若要在遠端桌面平台中執行 Horizon 效能追蹤程式，請使用 Horizon Client 或 HTML Access 來連線至伺服器，並啟動遠端桌面平台。

  如果當遠端桌面平台開啟時 Horizon 效能追蹤程式不會自動啟動，您可以按兩下 Windows 桌面平台上的 **VMware Horizon 效能追蹤程式**捷徑，或以啟動任何 Windows 應用程式的相同方式來啟動 Horizon 效能追蹤程式。

  若要選取選項以顯示 [概觀] 視窗或浮動列並結束應用程式，請在遠端桌面平台系統匣中的 VMware Horizon 效能追蹤程式圖示上按一下滑鼠右鍵。

- 若要以已發佈的應用程式形式來執行 Horizon 效能追蹤程式，請使用 Horizon Client 或 HTML Access 連線至伺服器，並啟動 Horizon 效能追蹤程式已發佈的應用程式。

  您使用 Horizon 效能追蹤程式已發佈應用程式的方式，取決於您使用的用戶端類型。您無法使用 Linux 版 Horizon Client 或 Windows 10 UWP 版 Horizon Client 將 Horizon 效能追蹤程式執行為已發佈的應用程式。

  - 使用 Windows 版 Horizon Client 時，Windows 用戶端系統上的系統匣中會顯示 VMware Horizon 效能追蹤程式圖示。您可以按兩下此圖示在 Windows 用戶端上開啟 Horizon 效能追蹤程式。您可以用滑鼠右鍵按一下此圖示，選取選項以顯示 [概觀] 視窗或浮動列並結束應用程式。
  - 使用 Mac 版 Horizon Client 時，Mac 用戶端系統的功能表列中會顯示 VMware Horizon 效能追蹤程式圖示。您可以按兩下此圖示在 Mac 用戶端上開啟 Horizon 效能追蹤程式。您也可以用滑鼠右鍵按一下此圖示，選取選項以顯示 [概觀] 視窗或浮動列並結束應用程式。
  - 使用 Android 版 Horizon Client 或 iOS 版 Horizon Client 時，Horizon Client 中的 Unity Touch 側邊列會顯示 VMware Horizon 效能追蹤程式圖示。您可以輕觸並按住此圖示，選取選項以顯示 [概觀] 視窗和浮動列並結束應用程式。
  - 使用 HTML Access 時，HTML Access 側邊列中會顯示 VMware Horizon 效能追蹤程式圖示。您可以用滑鼠右鍵按一下此圖示，然後選取選項以顯示 [概觀] 視窗或浮動列並結束應用程式。

後續步驟

如需 Horizon 效能追蹤程式顯示資料的相關資訊，請參閱設定 VMware Horizon 效能追蹤程式。

監控系統健全狀況

您可以使用 Horizon Administrator 中的系統健全狀況儀表板，快速查看可能會影響 Horizon 7 的作業或使用者對遠端桌面平台存取權的問題。

Horizon Administrator 顯示畫面左上角的系統健全狀況儀表板會提供一些連結，供您用來檢視 Horizon 7 作業的相關報告：

工作階段	提供 [工作階段] 畫面連結，此畫面可顯示遠端桌面平台和應用程式工作階段狀態的相關資訊。
問題 vCenter 虛擬機器	提供 [機器] 畫面連結，此畫面可顯示 Horizon 7 標記為有問題的 vCenter 虛擬機器、RDS 主機以及其他機器的相關資訊。
問題 RDS 主機	提供 [機器] 畫面上 **RDS 主機**索引標籤的連結，此畫面可顯示 Horizon 7 標記為有問題的 RDS 主機的相關資訊。
事件	提供 [事件] 畫面連結，其中已篩選出錯誤事件與警告事件。
系統健全狀況	提供 [儀表板] 畫面的連結，此畫面會顯示 Horizon 7 元件、已登錄 Unified Access Gateway 詳細資料 (3.4 版或更新版本)、vSphere 元件、網域、桌面平台、資料存放區使用量的狀態摘要。

系統健全儀表板會對照每個項目顯示帶有數字的連結。此值表示連結的報告所提供相關詳細資料的項目數目。

在 Horizon 7 中監控事件

事件資料庫會儲存連線伺服器主機或群組、Horizon Agent 與 Horizon Administrator 中發生事件的相關資訊，並在儀表板上顯示事件數目。您可以在「事件」畫面中詳細檢查事件。

備註 事件會在有限的期間內列於 Horizon Administrator 介面中。目前只有在歷史資料庫資料表中才有事件。您可以使用 Microsoft SQL Server 或 Oracle 資料庫報告工具檢查資料庫資料表中的事件。如需詳細資訊，請參閱《Horizon 7 整合》文件。

備註 事件資料庫無法使用時，Horizon 7 會保存在這段無法使用的期間內所發生事件的稽核線索，且在事件資料庫變得再次可用時將其儲存至資料庫。您必須重新啟動事件資料庫和連線伺服器，才能在 Horizon Administrator 介面中檢視這些事件。

除了監控 Horizon Administrator 中的事件，您還可以產生 `Syslog` 格式的 Horizon 7 事件，讓分析軟體能夠存取事件資料。請參閱《Horizon 7 安裝》文件中的使用 -l 選項以 Syslog 格式產生 Horizon 7 事件記錄訊息與〈設定 Syslog 伺服器的事件記錄〉。

必要條件

依照《Horizon 7 安裝》文件中的說明建立及設定事件資料庫。

程序

1 在 Horizon Administrator 中，選取**監視 > 事件**。

2 (選擇性) 在 [事件] 視窗中，您可以選取事件的時間範圍、將篩選器套用到事件，並依照一或多個資料欄排序列示的事件。

Horizon 7 事件訊息

Horizon 7 會在系統狀態變更或遭遇問題時報告事件。您可以使用事件訊息中的資訊採取適當的動作。

下表顯示 Horizon 7 報告的事件類型。

表 11-15. Horizon 7 報告的事件類型

事件類型	說明
稽核失敗或稽核成功	報告管理員或使用者對 Horizon 7 的作業或組態所做的變更失敗或成功。
錯誤	報告 Horizon 7 執行失敗的作業。
資訊	報告 Horizon 7 內的一般作業。
警告	報告作業或組態設定中發生的小問題，這些小問題可能會在經過一段時間後導致更嚴重的問題。

如果您看到與「稽核失敗」、「錯誤」或「警告」事件相關的訊息，可能需要採取某些動作。若是「稽核成功」或「資訊」事件，則不需採取任何動作。

收集 Horizon 7 的診斷資訊

您可以收集診斷資訊，以協助 VMware 技術支援診斷並解決 Horizon 7 的相關問題。

您可以收集各種 Horizon 7 元件的診斷資訊。收集這些資訊的方式取決於 Horizon 7 元件。

- 建立 Horizon Agent 的資料收集工具服務包

  若要協助 VMware 技術支援疑難排解 Horizon Agent 的問題，您可能需要使用 `vdmadmin` 命令，來建立資料收集工具 (DCT) 服務包。您也可以手動取得 DCT 服務包，不需使用 `vdmadmin`。

- 儲存 Windows 版 Horizon Client 的診斷資訊

  若您在使用 Windows 版 Horizon Client 時遇到問題，而且無法以一般網路疑難排解技巧加以解決，您可以儲存記錄檔複本和組態的相關資訊。

- 使用支援指令碼收集 View Composer 的診斷資訊

  您可以使用 View Composer 支援指令碼收集組態資料，並產生 View Composer 的記錄檔。這些資訊有助於 VMware 客戶支援診斷由於 View Composer 造成的任何問題。

- 收集 Horizon 連線伺服器的診斷資訊

  您可以使用支援工具設定記錄層級，並產生 Horizon 連線伺服器的記錄檔。

- 從主控台收集 Horizon Agent、Horizon Client 或 Horizon 連線伺服器的診斷資訊

  如果您可直接存取主控台，即可使用支援指令碼，針對連線伺服器、Horizon Client 或執行 Horizon Agent 的遠端桌面平台產生記錄檔。這些資訊有助於 VMware 技術支援診斷由於這些元件造成的任何問題。

建立 Horizon Agent 的資料收集工具服務包

若要協助 VMware 技術支援疑難排解 Horizon Agent 的問題，您可能需要使用 vdmadmin 命令，來建立資料收集工具 (DCT) 服務包。您也可以手動取得 DCT 服務包，不需使用 vdmadmin。

為了方便使用，您可以在連線伺服器執行個體上使用 vdmadmin 命令，從遠端桌面平台要求 DCT 服務包。服務包會傳回至連線伺服器。

或者您可以登入特定遠端桌面平台，並執行 support 命令，在該桌面平台上建立 DCT 服務包。如果已開啟使用者帳戶控制 (UAC)，您就必須以這種方式取得 DCT 服務包。

程序

1 以具有所需權限的使用者身分登入。

選項	動作
在 View 連線伺服器上使用 vdmadmin	以具有**管理員**角色的使用者身分，登入標準或複本執行個體連線伺服器。
在遠端桌面平台上	以具有系統管理員權限的使用者身分，登入遠端桌面平台。

2 開啟命令提示字元，並執行命令，以產生 DCT 服務包。

選項	動作
在 View 連線伺服器上使用 vdmadmin	若要指定輸出服務包檔案、桌面平台集區及機器的名稱，請搭配 -outfile、-d 及 -m 選項使用 vdmadmin 命令。 `vdmadmin -A [-b authentication_arguments] -getDCT -outfile local_file -d desktop -m machine`
在遠端桌面平台上	將目錄變更為 c:\Program Files\VMware\VMware View\Agent\DCT 並執行下列命令： `support`

命令會將服務包寫入指定的輸出檔案。

範例： 使用 vdmadmin 來建立 Horizon Agent 的服務包檔案

針對桌面平台集區 dtpool2 中的機器 machine1 建立 DCT 服務包，並將其寫入 zip 檔案 C:\myfile.zip 中。

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

後續步驟

如果您擁有現有支援要求，則可以藉由附加 DCT 服務包檔案來更新。

儲存 Windows 版 Horizon Client 的診斷資訊

若您在使用 Windows 版 Horizon Client 時遇到問題，而且無法以一般網路疑難排解技巧加以解決，您可以儲存記錄檔複本和組態的相關資訊。

您在儲存診斷資訊並與 VMware 技術支援聯絡之前，可以先嘗試解決 Windows 版 Horizon Client 的連線問題。如需詳細資訊，請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈Horizon Client 和 Horizon 連線伺服器之間的連線問題〉。

如需關於為其他 Horizon Client 平台收集支援資料的相關資訊，請參閱該平台的《安裝和設定指南》。以 Mac 版 Horizon Client 為例，請參閱《Mac 版 VMware Horizon Client 安裝和設定指南》。

程序

1 在 Horizon Client 中按一下**支援資訊**，或是在遠端桌面平台功能表，選取**選項 > 支援資訊**。

2 在**支援資訊**視窗中按一下**收集支援資料**，並在出現提示時按一下**是**。

命令視窗會顯示資訊收集進度。此程序可能需要幾分鐘時間。

3 在命令視窗中，藉由輸入您要據以測試 Horizon Client 組態之 Horizon 連線伺服器執行個體的 URL 來回應提示，如有需要，亦可選擇產生 Horizon 7 程序的診斷傾印。

此資訊會寫入用戶端機器之桌面平台資料夾中的 zip 檔案。

4 在 VMware 網站的「支援」頁面提出支援要求，並附加輸出的 zip 檔案。

使用支援指令碼收集 View Composer 的診斷資訊

您可以使用 View Composer 支援指令碼收集組態資料，並產生 View Composer 的記錄檔。這些資訊有助於 VMware 客戶支援診斷由於 View Composer 造成的任何問題。

必要條件

登入安裝了 View Composer 的電腦。

由於您必須使用 Windows Script Host 公用程式 (`cscript`) 執行支援指令碼，因此請自行熟悉使用 `cscript`。請參閱 http://technet.microsoft.com/library/bb490887.aspx。

程序

1 開啟命令提示字元視窗，並切換至 `C:\Program Files\VMware\VMware View Composer` 目錄。

如果並非將軟體安裝於預設目錄，請更改為適當的磁碟機代號及路徑。

2 輸入命令以執行 `svi-support` 指令碼。

```
cscript ".\svi-support.wsf" /zip
```

您可以使用 `/?` 選項，顯示可用於指令碼的其他命令選項的資訊。

指令碼完成時，將通知您輸出檔案的名稱及位置。

3 在 VMware 網站的「支援」頁面提出支援要求，並附加輸出檔案。

收集 Horizon 連線伺服器的診斷資訊

您可以使用支援工具設定記錄層級，並產生 Horizon 連線伺服器的記錄檔。

支援工具將收集連線伺服器的記錄資料。這些資訊有助於 VMware 技術支援診斷由於連線伺服器所造成的任何問題。支援工具並非用來收集 Horizon Client 或 Horizon Agent 的診斷資訊。您必須改用支援指令碼。請參閱從主控台收集 Horizon Agent、Horizon Client 或 Horizon 連線伺服器的診斷資訊。

必要條件

以具有**管理員**角色的使用者身分，登入連線伺服器的標準或複本執行個體。

程序

1 選取**開始 > 所有程式 > VMware > 設定 View 連線伺服器記錄層級**。

2 在**選擇**文字方塊中，輸入設定記錄層級的數值，並且按 Enter。

選項	說明
0	將記錄層級重設為預設值。
1	選取記錄的一般層級。
2	選取記錄的偵錯層級 (預設)。
3	選取完整記錄。

系統將以您選取的詳細資料層級，開始記錄資訊。

3 收集連線伺服器行為的充足資訊後，選取**開始 > 所有程式 > VMware > 產生 View 連線伺服器記錄服務包**。

支援工具會將記錄檔寫入連線伺服器執行個體的桌面平台上名為 `vdm-sdct` 的資料夾中。

4 在 VMware 網站的「支援」頁面提出支援要求，並附加輸出檔案。

從主控台收集 Horizon Agent、Horizon Client 或 Horizon 連線伺服器的診斷資訊

如果您可直接存取主控台，即可使用支援指令碼，針對連線伺服器、Horizon Client 或執行 Horizon Agent 的遠端桌面平台產生記錄檔。這些資訊有助於 VMware 技術支援診斷由於這些元件造成的任何問題。

必要條件

登入要收集資訊的系統。您必須以具有管理員權限的使用者身分登入。

- 對於 Horizon Agent，登入已安裝 Horizon Agent 的虛擬機器。
- 對於 Horizon Client，登入已安裝 Horizon Client 的系統。
- 對於連線伺服器，登入連線伺服器主機。

程序

1 開啟命令提示字元視窗，並針對要收集診斷資訊的 Horizon 7 元件變更為適當的目錄。

選項	說明
Horizon Agent	切換至 `C:\Program Files\VMware View\Agent\DCT` 目錄。
Horizon Client	切換至 `C:\Program Files\VMware View\Client\DCT` 目錄。
View 連線伺服器	切換至 `C:\Program Files\VMware View\Server\DCT` 目錄。

如果並非將軟體安裝於預設目錄，請更改為適當的磁碟機代號及路徑。

2 輸入命令以執行支援指令碼。

```
.\support.bat [loglevels]
```

如果要啟用進階記錄，請指定 `loglevels` 選項，並且在提示時輸入記錄層級的數值。

選項	說明
0	將記錄層級重設為預設值。
1	選取記錄的一般層級。
2	選取記錄的偵錯層級 (預設)。
3	選取完整記錄。
4	選取 PCoIP 的資訊記錄 (僅限 Horizon Agent 及 Horizon Client)。
5	選取 PCoIP 的偵錯記錄 (僅限 Horizon Agent 及 Horizon Client)。
6	選取虛擬通道的資訊記錄 (僅限 Horizon Agent 及 Horizon Client)。
7	選取虛擬通道的偵錯記錄 (僅限 Horizon Agent 及 Horizon Client)。
8	選取虛擬通道的追蹤記錄 (僅限 Horizon Agent 及 Horizon Client)。

指令碼會將壓縮的記錄檔寫入桌面平台的資料夾 `vdm-sdct`。

3 在 `C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support` 目錄中，您可找到 View Composer 客體代理程式記錄。

4 在 VMware 網站的「支援」頁面提出支援要求，並附加輸出檔案。

Horizon 連線伺服器與 Skyline Collector 應用裝置進行整合

您可以設定 Horizon 連線伺服器，使其與 Skyline Collector 應用裝置整合，供 VMware 技術支援用來診斷和解決 Horizon 7 的問題。Skyline Collector 應用裝置會針對為記錄收集所設定的 Horizon 7 管理員使用者提取連線伺服器記錄。

程序

1 在 Horizon Administrator 中，建立名為「記錄收集器管理員」、且具有「收集作業記錄」權限的自訂角色。請參閱新增自訂角色。

2 新增自訂角色的說明。

3 新增管理員使用者，並且為該使用者選擇「詳細目錄管理員 (唯讀)」權限和「記錄收集器管理員」角色。

Skyline Collector 應用裝置可為這個管理員使用者提取連線伺服器記錄，用以診斷和解決 Horizon 7 的問題。

更新支援要求

您可以在支援網站上更新現有的支援要求。

在您提出支援要求之後，可能會收到由 VMware 技術支援寄來的電子郵件要求，請您提供 `support` 或 `svi-support` 指令碼的輸出檔。在您執行指令碼時，指令碼會告訴您輸出檔的名稱和位置。請回覆電子郵件訊息，並在回覆中附加輸出檔。

如果輸出檔太大，無法以附件包含在郵件中 (10MB 或以上)，請連絡 VMware 技術支援，告訴他們您的支援要求編號，同時索取 FTP 上傳指示。或者您也可以在支援網站上，將檔案附加至現有的支援要求。

程序

1 造訪 VMware 網站的「支援」頁面並登入。

2 按一下**支援要求記錄**，然後找出適用的支援要求編號。

3 更新支援要求，同時附加您藉由執行 `support` 或 `svi-support` 指令碼而取得的輸出。

對安全伺服器與 Horizon 連線伺服器配對失敗進行疑難排解

如果安全伺服器無法與連線伺服器執行個體順利配對，安全伺服器可能無法運作。

問題

如果安全伺服器無法與連線伺服器配對，安全伺服器可能會發生下列問題：

- 當您再度嘗試安裝安全伺服器時，安全伺服器無法連線至連線伺服器。
- Horizon Client 無法與 Horizon 7 連線。將會出現下列錯誤訊息：`View` 連線伺服器驗證失敗。沒有閘道可用來提供與桌面平台的安全連線。請連絡您的網路管理員。
- 在 Horizon Administrator 儀表板上，安全伺服器會顯示為關閉。

原因

若您在開始安裝安全伺服器之後，於輸入安全伺服器配對密碼後取消安裝，或以其他方式中止安裝，則會發生這個問題。

解決方案

若您想要在 Horizon 7 環境中保留安全伺服器，請採取下列步驟：

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

2 在**安全伺服器**索引標籤上，選取一個安全伺服器，接著從**更多命令**下拉式功能表中選取**準備升級或重新安裝**，然後按一下**確定**。

3 在**連線伺服器**索引標籤上，選取要與安全伺服器配對的連線伺服器執行個體，接著從**更多命令**下拉式功能表中選取**指定安全伺服器配對密碼**，輸入密碼，然後按一下**確定**。

4 再次安裝安全伺服器。

若您想要從 Horizon 7 環境移除安全伺服器項目，請執行 `vdmadmin -S` 命令。

例如：**`vdmadmin -S -r -s`** ***`security_server_name`***

對 Horizon 7 Server 憑證撤銷檢查進行疑難排解

如果無法對伺服器的 TLS 憑證執行憑證撤銷檢查，則用於安全的 Horizon Client 連線的安全伺服器或連線伺服器執行個體會在 View Administrator 中顯示為紅色。

問題

Horizon Administrator 儀表板上的安全伺服器或連線伺服器圖示是紅色的。Horizon 7 Server 的狀態會顯示下列訊息：無法檢查伺服器的憑證。

原因

如果您的組織使用 Proxy 伺服器來進行網際網路存取，或是連線伺服器執行個體因防火牆或其他控制項，而無法與提供撤銷檢查的伺服器連線，則憑證撤銷檢查可能會失敗。

連線伺服器執行個體會對本身的憑證，以及與其配對之安全伺服器的憑證，執行憑證撤銷檢查。依預設，VMware Horizon View 連線伺服器服務會以 `LocalSystem` 帳戶啟動。當它在 `LocalSystem` 底下執行時，連線伺服器執行個體無法使用在 Internet Explorer 設定的 Proxy 設定來存取 CRL DP URL 或 OCSP 回應者，以確定憑證的撤銷狀態。

您可以使用 Microsoft `Netshell` 命令，將 Proxy 設定匯入至連線伺服器執行個體，如此一來，伺服器即可存取網際網路上的憑證撤銷檢查站台。

解決方案

1 在連線伺服器電腦上，使用**以系統管理員身分執行**設定開啟命令列視窗。

例如，按一下**開始**，輸入 **`cmd`**，以滑鼠右鍵按一下 `cmd.exe` 圖示，然後選取**以系統管理員身分執行**。

2 輸入 **`netsh`**，並按 Enter 鍵。

3 輸入 **`winhttp`**，並按 Enter 鍵。

4 輸入 **`show proxy`**，並按 Enter 鍵。

`Netshell` 顯示 Proxy 已設定為 DIRECT (直接) 連線。透過這項設定，若組織使用 Proxy，連線伺服器電腦即無法連線至網際網路。

5 設定 Proxy 設定。

例如，在 `netsh winhttp>` 提示，輸入 **`import proxy source=ie`**。

Proxy 設定會匯入至連線伺服器電腦。

6 您可以輸入 **`show proxy`** 以確認 Proxy 設定。

7 重新啟動 VMware Horizon View 連線伺服器服務。

8 在 Horizon Administrator 儀表板上，確認安全伺服器或連線伺服器圖示是否是綠色。

智慧卡憑證撤銷檢查疑難排解

已連接智慧卡的連線伺服器執行個體或安全伺服器，無法對伺服器的 TLS 憑證執行憑證撤銷檢查，除非您已設定智慧卡憑證撤銷檢查。

問題

如果您的組織使用 Proxy 伺服器來進行網際網路存取，或是連線伺服器執行個體或安全伺服器因防火牆或其他控制項，而無法與提供撤銷檢查的伺服器連線，則憑證撤銷檢查可能會失敗。

重要 請確定 CRL 檔案為最新。

原因

Horizon 7 使用「憑證撤銷清單」(CRL) 和「線上憑證狀態通訊協定」(OCSP) 來支援憑證撤銷檢查。CRL 是核發憑證的 CA (憑證授權機構) 所發佈的撤銷憑證清單。OCSP 是用來取得 X.509 憑證的撤銷狀態的憑證驗證通訊協定。必須可以從連線伺服器或安全伺服器主機存取 CA。只有在設定智慧卡憑證撤銷檢查時，才會發生此問題。請參閱使用智慧卡憑證撤銷檢查。

解決方案

1 建立您自己專屬 (手動) 程序，從您使用的 CA 網站下載最新的 CRL 到 Horizon 7 Server 上的路徑。

2 在連線伺服器或安全伺服器主機上的 TLS/SSL 閘道組態資料夾中，建立或編輯 `locked.properties` 檔案。

   例如：*`install_directory`*`\VMware\VMware View\Server\SSLgateway\conf\locked.properties`

3 將 `locked.properties` 檔案中的 `enableRevocationChecking` 和 `crlLocation` 內容新增至儲存 CRL 的本機路徑。

4 重新啟動連線伺服器服務或安全伺服器服務，讓您的變更生效。

進一步疑難排解資訊

您可以在 VMware 知識庫文章中找到進一步的疑難排程資訊。

VMware 知識庫 (KB) 會持續更新，以提供 VMware 產品的疑難排解新資訊。

如需疑難排解 Horizon 7 的詳細資訊，請參閱 VMware 知識庫網站上的知識庫文章：

http://kb.vmware.com/selfservice/microsites/microsite.do

使用 vdmadmin 命令

12

您可以使用 vdmadmin 命令列介面，在連線伺服器執行個體上執行各種管理工作。

您可以使用 vdmadmin 執行無法從使用者介面中執行的管理工作，或執行必須從指令碼自動執行的管理工作。

- vdmadmin 命令用法

  vdmadmin 命令的語法會控制其作業。

- 使用 -A 選項設定 Horizon Agent 中的記錄

  您可以將 vdmadmin 命令與 -A 選項搭配使用，以設定依 Horizon Agent 的記錄。

- 使用 -A 選項覆寫 IP 位址

  您可以將 vdmadmin 命令與 -A 選項搭配使用，以覆寫 Horizon Agent 報告的 IP 位址。

- 使用 -F 選項更新外部安全性主體

  您可以使用 vdmadmin 命令搭配 -F 選項，更新在 Active Directory 內獲授權使用桌面的 Windows 使用者的外部安全性主體 (FSP)。

- 使用 -H 選項列示並顯示健全狀況監視器

  您可以將 vdmadmin 命令搭配 -H 使用，以列出現有的健全狀況監視器、監控 Horizon 7 元件的執行個體，並顯示特定健全狀況監視器或監視器執行個體的詳細資料。

- 使用 -I 選項列示與顯示 Horizon 7 作業報告

  您可以將 vdmadmin 命令與 -I 選項搭配使用，以列示 Horizon 7 作業的可用報告，並顯示執行其中一個報告的結果。

- 使用 -I 選項以 Syslog 格式產生 Horizon 7 事件記錄訊息

  您可以將 vdmadmin 命令與 -I 選項搭配使用，將 Horizon 7 事件訊息以 Syslog 格式記錄在事件記錄檔中。許多第三方分析產品需要 Syslog 純文字檔案資料作為分析作業的輸入。

- 使用 -L 選項指派專用機器

  您可以將 vdmadmin 命令與 -L 選項搭配使用，以將專用集區中的機器指派給使用者。

- 使用 -M 選項顯示機器的相關資訊

  您可以將 vdmadmin 命令與 -M 選項搭配使用，以顯示虛擬機器或實體電腦的組態相關資訊。

- 使用 -M 選項回收虛擬機器上的磁碟空間

  您可以將 vdmadmin 命令與 -M 選項搭配使用，以標記要回收磁碟空間的連結複製虛擬機器。Horizon 7 會將 ESXi 主機導向至連結複製作業系統磁碟上的回收磁碟空間，無須等待作業系統磁碟上的未使用空間到達在 Horizon Administrator 中指定的臨界值下限。

- 使用 -N 選項設定網域篩選條件

  您可以將 vdmadmin 命令與 -N 選項搭配使用，以控制 Horizon 7 開放給使用者的網域。

- 設定網域篩選條件

  您可以設定網域篩選條件以限制連線伺服器執行個體或安全伺服器開放給使用者的網域。

- 使用 -O 與 -P 選項顯示未獲權使用者的機器與原則

  您可以將 vdmadmin 命令與 -O 和 -P 選項搭配使用，以顯示指派給不再有權使用系統之使用者的虛擬機器與原則。

- 使用 -Q 選項設定 Kiosk 模式中的用戶端

  您可以將 vdmadmin 命令與 -Q 選項搭配使用，以設定預設值並在 Kiosk 模式中建立用戶端的帳戶，以便啟用這些用戶端的驗證，和顯示其組態的相關資訊。

- 使用 -R 選項顯示機器的第一個使用者

  您可以將 vdmadmin 命令與 -R 選項搭配使用，找出受管理虛擬機器的初始指派。例如，當遺失 LDAP 資料時，您可能需要此資訊，以便將虛擬機器重新指派給使用者。

- 使用 -S 選項移除連線伺服器執行個體或安全伺服器項目

  您可以將 vdmadmin 命令與 -S 選項搭配使用，以移除 Horizon 7 組態中的連線伺服器執行個體或安全伺服器的項目。

- 使用 -T 選項為管理員提供次要認證

  您可以使用 vdmadmin 命令搭配 -T 選項，提供 Active Directory 次要認證給管理員使用者。

- 使用 -U 選項顯示使用者的相關資訊

  您可以將 vdmadmin 命令與 -U 選項搭配使用，以顯示使用者的詳細資訊。

- 使用 -V 選項解除鎖定或鎖定虛擬機器

  您可以將 vdmadmin 命令與 -V 選項搭配使用，以解除鎖定或鎖定資料中心的虛擬機器。

- 使用 -X 選項偵測和解決 LDAP 項目和結構描述衝突

  您可以將 vdmadmin 命令與 -X 選項搭配使用，以偵測和解決群組中已複寫連線伺服器執行個體上的 LDAP 項目衝突和 LDAP 結構描述衝突。您也可以使用此選項來偵測和解決 Cloud Pod 架構環境中的 LDAP 結構描述衝突。

vdmadmin 命令用法

vdmadmin 命令的語法會控制其作業。

在 Windows 命令提示字元中使用 vdmadmin 命令的下列格式。

```
vdmadmin command_option [additional_option argument] ...
```

可使用的其他選項視命令選項而定。

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

- vdmadmin 命令驗證

  您必須以**管理員**角色的使用者身分，執行 vdmadmin 命令，才能成功執行指定的動作。

- vdmadmin 命令輸出格式

  有些 vdmadmin 命令選項可讓您指定輸出資訊的格式。

- vdmadmin 命令選項

  您可以使用 vdmadmin 命令的命令選項來指定希望執行的作業。

vdmadmin 命令驗證

您必須以**管理員**角色的使用者身分，執行 vdmadmin 命令，才能成功執行指定的動作。

您可以使用 Horizon Administrator，將**管理員**角色指派給使用者。請參閱第 6 章 設定角色型委派管理。

如果您以權限不足的使用者身分登入，而且您知道已獲指定**管理員**角色之使用者的密碼，則可以以該使用者身分，使用 -b 選項執行命令。當指定的使用者位於指定的網域內時，您可以指定 -b 選項以執行 vdmadmin 命令。下列 -b 選項的使用格式是相同的。

```
-b
username
domain [password | *]
```

```
-b
username@domain [password | *]
```

```
-b
domain\username [password | *]
```

如果指定星號 (*) 而非指定密碼，系統會提示您輸入密碼，而且 vdmadmin 命令不會在命令列的命令歷程記錄中保留敏感的密碼。

您可以使用 -b 選項搭配所有命令選項，但 -R 和 -T 選項除外。

vdmadmin 命令輸出格式

有些 vdmadmin 命令選項可讓您指定輸出資訊的格式。

下表說明某些 vdmadmin 命令選項針對格式化輸出文字所提供的選項。

表 12-1. 選取輸出格式的選項

選項	說明
-csv	將輸出格式化為以逗號分隔的值。
-n	使用 ASCII (UTF-8) 字元顯示輸出。此為以逗號分隔的值和純文字輸出的預設字元集。
-w	使用 Unicode (UTF-16) 字元顯示輸出。此為 XML 輸出的預設字元集。
-xml	將輸出格式化為 XML。

vdmadmin 命令選項

您可以使用 vdmadmin 命令的命令選項來指定希望執行的作業。

下表說明您可以搭配 vdmadmin 命令使用的命令選項，以控制並檢查 Horizon 7 的作業。

表 12-2. Vdmadmin 命令選項

選項	說明
-A	管理 Horizon Agent 記錄在其記錄檔中的資訊。請參閱使用 -A 選項設定 Horizon Agent 中的記錄。 覆寫由 Horizon Agent 報告的 IP 位址。請參閱 使用 -A 選項覆寫 IP 位址
-C	設定連線伺服器群組的名稱。請參閱#unique_271。
-F	針對所有使用者或指定的使用者，更新 Active Directory 中的外部安全性原則 (FSP)。請參閱使用 -F 選項更新外部安全性主體。
-H	顯示 Horizon 7 服務的健全狀況資訊。請參閱使用 -H 選項列示並顯示健全狀況監視器。
-I	產生有關 Horizon 7 作業的報告。請參閱使用 -I 選項列示與顯示 Horizon 7 作業報告。
-L	將專用桌面平台指派給使用者或移除指派。請參閱使用 -L 選項指派專用機器。
-M	顯示有關虛擬機器或實體電腦的資訊。請參閱使用 -M 選項顯示機器的相關資訊。
-N	設定連線伺服器執行個體或群組可讓 Horizon Client 使用的網域。請參閱使用 -N 選項設定網域篩選條件。
-O	顯示指派給已無權使用某些桌面平台之使用者的那些遠端桌面平台。請參閱使用 -O 與 -P 選項顯示未獲權使用者的機器與原則。
-P	顯示與未獲權使用者的遠端桌面平台相關聯的使用者原則。請參閱使用 -O 與 -P 選項顯示未獲權使用者的機器與原則。
-Q	在 Kiosk 模式下，設定用戶端裝置之 Active Directory 帳戶及 Horizon 7 組態中的帳戶。請參閱使用 -Q 選項設定 Kiosk 模式中的用戶端。
-R	報告第一位存取遠端桌面平台的使用者。請參閱使用 -R 選項顯示機器的第一個使用者。
-S	從 Horizon 7 的組態中移除連線伺服器執行個體的組態項目。請參閱使用 -S 選項移除連線伺服器執行個體或安全伺服器項目。
-T	提供 Active Directory 次要認證給管理員使用者。請參閱使用 -T 選項為管理員提供次要認證。
-U	顯示使用者的相關資訊，包括其遠端桌面平台權利和 ThinApp 指派，以及管理員角色。請參閱使用 -U 選項顯示使用者的相關資訊。

表 12-2. Vdmadmin 命令選項 (續)

選項	說明
–V	解除鎖定或鎖定虛擬機器。請參閱使用 -V 選項解除鎖定或鎖定虛擬機器。
–X	偵測並解決在複寫的連線伺服器執行個體上的重複 LDAP 項目。請參閱使用 -X 選項偵測和解決 LDAP 項目和結構描述衝突。

使用 -A 選項設定 Horizon Agent 中的記錄

您可以將 vdmadmin 命令與 –A 選項搭配使用，以設定依 Horizon Agent 的記錄。

語法

```
vdmadmin
–A [–b authentication_arguments] –getDCT–outfile local_file–d desktop –m machine
```

```
vdmadmin
–A [–b authentication_arguments] –getlogfile logfile–outfile local_file–d desktop–mmachine
```

```
vdmadmin
–A [–b authentication_arguments] –getloglevel [–xml] –d desktop [–m machine]
```

```
vdmadmin
–A [–b authentication_arguments] –getstatus [–xml] –d desktop [–m machine]
```

```
vdmadmin
–A [–b authentication_arguments] –getversion [–xml] –d desktop [–mmachine]
```

```
vdmadmin
–A [–b authentication_arguments] –list [–xml] [–w | –n] –d desktop–m machine
```

```
vdmadmin
–A [–b authentication_arguments] –setloglevel level –ddesktop [–mmachine]
```

用法提示

若要協助 VMware 技術支援疑難排解 Horizon Agent 的問題，您可以建立資料收集工具 (DCT) 服務包。您也可以變更記錄層級、顯示 Horizon Agent 的版本和狀態，以及將個別記錄檔儲存至您的本機磁碟。

選項

下表顯示您可以指定用來在 Horizon Agent 中設定記錄的選項。

表 12-3. 在 Horizon Agent 中設定記錄的選項

選項	說明
`-d` *desktop*	指定桌面平台集區。
`-getDCT`	建立資料收集工具 (DCT) 服務包並將其儲存至本機檔案。
`-getlogfile` *logfile*	指定記錄檔名稱以儲存其複本。
`-getloglevel`	顯示 Horizon Agent 目前的記錄層級。
`-getstatus`	顯示 Horizon Agent 的狀態。
`-getversion`	顯示 Horizon Agent 的版本。
`-list`	列出 Horizon Agent 的記錄檔。
`-m` *machine*	指定桌面集區內的機器。
`-outfile` *local_file*	對要在其中儲存 DCT 服務包或記錄檔複本的本機檔案指定其名稱。
`-setloglevel` *level*	設定 Horizon Agent 的記錄層級。 **debug** 記錄錯誤、警告及除錯事件。 **normal** 記錄錯誤和警告事件。 **trace** 記錄錯誤、警告、資訊及除錯事件。

範例

針對桌面平台集區 dtpool2 中的機器 machine1 顯示 Horizon Agent 的記錄層級。

```
vdmadmin -A -d dtpool2 -m machine1 -getloglevel
```

針對桌面平台集區 dtpool2 中的機器 machine1 將 Horizon Agent 的記錄層級設定為除錯。

```
vdmadmin -A -d dtpool2 -m machine1 -setloglevel debug
```

針對桌面平台集區 dtpool2 中的機器 machine1 顯示 Horizon Agent 記錄檔的清單。

```
vdmadmin -A -d dtpool2 -m machine1 -list
```

針對桌面平台集區 dtpool2 中的機器 machine1，將 Horizon Agent 記錄檔 `log-2009-01-02.txt` 的複本另存為 `C:\mycopiedlog.txt`。

```
vdmadmin -A -d dtpool2 -m machine1 -getlogfile log-2009-01-02.txt -outfile C:\mycopiedlog.txt
```

針對桌面平台集區 dtpool2 中的機器 machine1 顯示 Horizon Agent 的版本。

```
vdmadmin -A -d dtpool2 -m machine1 -getversion
```

針對桌面平台集區 dtpool2 中的機器 machine1 顯示 Horizon Agent 的狀態。

```
vdmadmin -A -d dtpool2 -m machine1 -getstatus
```

針對桌面平台集區 dtpool2 中的機器 machine1 建立 DCT 服務包，並將其寫入 zip 檔案 C:\myfile.zip 中。

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

使用 -A 選項覆寫 IP 位址

您可以將 vdmadmin 命令與 -A 選項搭配使用，以覆寫 Horizon Agent 報告的 IP 位址。

語法

```
vdmadmin
-A [-bauthentication_arguments] -override-iip_or_dns-ddesktop-mmachine
```

```
vdmadmin
-A [-bauthentication_arguments] -override-list-ddesktop-mmachine
```

```
vdmadmin
-A [-bauthentication_arguments] -override-r-ddesktop [-mmachine]
```

用法提示

Horizon Agent 會向連線伺服器執行個體回報在其執行所在的機器上發現的 IP 位址。在連線伺服器執行個體不會信任 Horizon Agent 所回報值的安全組態中，您可以覆寫由 Horizon Agent 提供的值，並指定受管理機器應使用的 IP 位址。如果 Horizon Agent 回報的機器位址不符合定義的位址，則您無法使用 Horizon Client 存取該機器。

選項

下表顯示您可以指定用來覆寫 IP 位址的選項。

表 12-4. 可覆寫 IP 位址的選項

選項	說明
-d *desktop*	指定桌面平台集區。
-i *ip_or_dns*	指定 IP 位址或在 DNS 中可解析的網域名稱。
-m *machine*	指定桌面平台集區中機器的名稱。
-override	指定可覆寫 IP 位址的作業。
-r	移除覆寫後的 IP 位址。

範例

覆寫桌面平台集區 dtpool2 中機器 machine2 的 IP 位址。

```
vdmadmin –A –override –i 10.20.54.165 –d dtpool2 –m machine2
```

顯示為桌面平台集區 dtpool2 中機器 machine2 定義的 IP 位址。

```
vdmadmin –A –override –list –d dtpool2 –m machine2
```

移除為桌面平台集區 dtpool2 中機器 machine2 定義的 IP 位址。

```
vdmadmin –A –override –r –d dtpool2 –m machine2
```

移除為桌面平台集區 dtpool3 中桌面平台定義的 IP 位址。

```
vdmadmin –A –override –r –d dtpool3
```

使用 -F 選項更新外部安全性主體

您可以使用 vdmadmin 命令搭配 –F 選項，更新在 Active Directory 內獲授權使用桌面的 Windows 使用者的外部安全性主體 (FSP)。

語法

```
vdmadmin
–F [–bauthentication_arguments] [–udomain\user]
```

使用附註

如果您信任本機網域之外的網域，可以允許外部網域中的安全性主體存取本機網域資源。Active Directory 使用 FSP 代表信任的外部網域中的安全性主體。如果修改信任的外部網域清單，您可能希望更新使用者的 FSP。

選項

–u 選項會指定您要更新其 FSP 的使用者的名稱和網域。如果未指定此選項，則此命令會更新 Active Directory 中所有使用者的 FSP。

範例

更新 EXTERNAL 網域中使用者 Jim 的 FSP。

```
vdmadmin –F –u EXTERNAL\Jim
```

更新 Active Directory 中所有使用者的 FSP。

```
vdmadmin –F
```

使用 -H 選項列示並顯示健全狀況監視器

您可以將 vdmadmin 命令搭配 -H 使用，以列出現有的健全狀況監視器、監控 Horizon 7 元件的執行個體，並顯示特定健全狀況監視器或監視器執行個體的詳細資料。

語法

```
vdmadmin
-H [-b authentication_arguments] -list-xml [-w | -n]
```

```
vdmadmin
-H [-b authentication_arguments] -list-monitorid monitor_id -xml [-w | -n]
```

```
vdmadmin
-H [-b authentication_arguments] -monitoridmonitor_id -instanceid instance_id -xml [-w | -n]
```

用法提示

下表會顯示 Horizon 7 用來監控其元件健全狀況的健全狀況監視器。

表 12-5. 健全狀況監視器

監視器	說明
CBMonitor	監控連線伺服器執行個體健全狀況。
DBMonitor	監控事件資料庫的健全狀況。
DomainMonitor	監控連線伺服器主機其本機網域與所有信任網域的健全狀況。
SGMonitor	監控安全閘道服務與安全伺服器的健全狀況。
VCMonitor	監控 vCenter server 健全狀況。

如果某個元件有多個執行個體，Horizon 7 會建立另外的監視器執行個體來監視該元件的每個執行個體。

此命令會以 XML 格式輸出健全狀況監視器與監視器執行個體的所有相關資訊。

選項

下表會顯示您可指定以列示與顯示健全狀況監視器的選項。

表 12-6. 可列示與顯示健全狀況監視器的選項

選項	說明
-instanceid *instance_id*	指定健全狀況監視器執行個體
-list	如果未指定健全狀況監視器識別碼，則顯示現有的健全狀況監視器。

表 12-6. 可列示與顯示健全狀況監視器的選項 (續)

選項	說明
-list -monitorid *monitor_id*	顯示所指定健全狀況監視器識別碼的監視器執行個體。
-monitorid *monitor_id*	指定健全狀況監視器識別碼。

範例

以使用 Unicode 字元的 XML 格式列示所有現有的健全狀況監視器。

```
vdmadmin -H -list -xml
```

以使用 ASCII 字元的 XML 格式列示 vCenter 監視器 (VCMonitor) 的所有執行個體。

```
vdmadmin -H -list -monitorid VCMonitor -xml -n
```

顯示所指定的 vCenter 監視器執行個體的健全狀況。

```
vdmadmin -H -monitorid VCMonitor -instanceid 4aec2c99-4879-96b2-de408064d035 -xml
```

使用 -I 選項列示與顯示 Horizon 7 作業報告

您可以將 vdmadmin 命令與 -I 選項搭配使用，以列示 Horizon 7 作業的可用報告，並顯示執行其中一個報告的結果。

語法

```
vdmadmin
-I [-b authentication_arguments] -list [-xml] [-w | -n]
```

```
vdmadmin
-I [-b authentication_arguments] -report report -view view [-startdate yyyy-MM-dd-HH:mm:ss]
[-enddate yyyy-MM-dd-HH:mm:ss] [-w | -n] -xml | -csv
```

用法提示

您可以使用此命令顯示可用的報告與視圖，並顯示 Horizon 7 為所指定報告與視圖記錄的資訊。

您也可以將 vdmadmin 命令與 -I 選項搭配使用，以產生 syslog 格式的 Horizon 7 記錄訊息。請參閱使用 -I 選項以 Syslog 格式產生 Horizon 7 事件記錄訊息。

選項

下表顯示您可指定以列示與顯示報告及視圖的選項。

表 12-7. 可列示與顯示報告及視圖的選項

選項	說明
–enddate *yyyy-MM-dd-HH:mm:ss*	指定所要顯示的資訊日期上限。
–list	列示可用的報告與視圖。
–report *report*	指定報告。
–startdate *yyyy-MM-dd-HH:mm:ss*	指定所要顯示的資訊日期下限。
–view *view*	指定檢視。

範例

使用 Unicode 字元以 XML 格式列示可用的報告與視圖。

```
vdmadmin –I –list –xml –w
```

顯示自 2010 年 8 月 1 日起發生的使用者事件清單，並顯示成使用 ASCII 字元的以逗號分隔值。

```
vdmadmin –I –report events –view user_events –startdate 2010–08–01–00:00:00 –csv –n
```

使用 -I 選項以 Syslog 格式產生 Horizon 7 事件記錄訊息

您可以將 vdmadmin 命令與 –I 選項搭配使用，將 Horizon 7 事件訊息以 Syslog 格式記錄在事件記錄檔中。許多第三方分析產品需要 Syslog 純文字檔案資料作為分析作業的輸入。

語法

```
vdmadmin
–I
–eventSyslog
–disable
```

```
vdmadmin
–I
–eventSyslog
–enable
–localOnly
```

```
vdmadmin
–I
–eventSyslog
–enable
–path
```

```
        路徑
```

```
        vdmadmin
        -I
        -eventSyslog
        -enable
        -path
        path
        -user
        DomainName\username
        -password
        password
```

用法提示

您可以使用此命令以 Syslog 格式產生 Horizon 7 事件記錄檔訊息。在 Syslog 檔中，Horizon 7 事件記錄檔訊息採用索引鍵-值配對格式，讓記錄的資料可供分析軟體存取。

您也可以將 vdmadmin 命令與 -I 選項搭配使用，以列出可用報表與檢視清單，並顯示指定報告的內容。請參閱使用 -I 選項列示與顯示 Horizon 7 作業報告。

選項

您可以停用或啟用 eventSyslog 選項。您可以將 Syslog 輸出僅導向到本機系統，或導向到另一個位置。Horizon 7 5.2 或更新版本支援 Syslog 伺服器的直接 UDP 連線。請參閱《Horizon 7 安裝》文件中的〈設定 Syslog 伺服器的事件記錄〉。

表 12-8. 可使用 Syslog 格式產生 Horizon 7 事件記錄檔訊息的選項

選項	說明
-disable	停用 Syslog 記錄。
-e|-enable	啟用 Syslog 記錄。
-eventSyslog	指定以 Syslog 格式產生 Horizon 7 事件。
-localOnly	Syslog 輸出僅儲存在本機系統上。當您使用 -localOnly 選項時，Syslog 輸出的預設目的地是 %PROGRAMDATA%\VMware\VDM\events\。
-password *password*	為授權存取 Syslog 輸出其指定目的地路徑存取權的使用者指定密碼。
-path	決定 Syslog 輸出的目的地 UNC 路徑。
-u|-user *DomainName\username*	指定可存取 Syslog 輸出其目的地路徑的網域與使用者名稱。

範例

停用以 Syslog 格式產生 Horizon 7 事件。

```
vdmadmin -I -eventSyslog -disable
```

將 Horizon 7 事件的 Syslog 輸出僅導向至本機系統。

```
vdmadmin -I -eventSyslog -enable -localOnly
```

將 Horizon 7 事件的 Syslog 輸出僅導向至指定的路徑。

```
vdmadmin -I -eventSyslog -enable -path path
```

將 Horizon 7 事件的 Syslog 輸出導向至需要授權網域使用者存取權的指定路徑。

```
vdmadmin -I -eventSyslog -enable -path \\logserver\share\ViewEvents -user mydomain\myuser
 -password mypassword
```

使用 -L 選項指派專用機器

您可以將 vdmadmin 命令與 -L 選項搭配使用，以將專用集區中的機器指派給使用者。

語法

```
vdmadmin
-L [-bauthentication_arguments] -ddesktop-m machine-udomain\user
```

```
vdmadmin
-L [-bauthentication_arguments] -ddesktop [-mmachine | -udomain\user] -r
```

用法提示

Horizon 7 會在使用者第一次連線至專用桌面平台集區時將機器指派給使用者。在某些情況下，您可能想要將機器預先指派給使用者。例如，您可能想要在初始連線前備妥系統環境。在使用者連線至 Horizon 7 從專用集區所指派的遠端桌面平台後，主控該桌面平台的虛擬機器會在虛擬機器有效期間持續指派給該使用者。您可以將使用者指派至專用集區中的單一機器。

您可以將機器指派給任何授權使用者。復原連線伺服器執行個體上遺失的 View LDAP 資料時，或者要變更特定機器的擁有權時，您可能會想要這麼做。

在使用者連線至 Horizon 7 從專用集區所指派的遠端桌面平台後，該遠端桌面平台會在主控該桌面平台的虛擬機器有效期間持續指派給該使用者。如果使用者已離開組織、不再需要存取桌面平台或將使用不同桌面平台集區中的桌面平台，您可能想要移除對該使用者的機器指派。您也可以移除對存取桌面平台集區的所有使用者所進行的指派。

備註 `vdmadmin -L` 命令不會指派 View Composer 持續性磁碟的擁有權。若要將具有持續性磁碟的連結複製桌面平台指派給使用者，請使用 Horizon Administrator 中的**指派使用者**功能表選項。

如果使用 `vdmadmin -L` 將具有持續性磁碟的連結複製桌面平台指派給使用者，在某些情況下可能發生非預期的結果。例如，如果將持續性磁碟中斷連結，並使用該磁碟重新建立桌面平台，則重新建立的桌面平台將不會指派給原始桌面平台的擁有者。

選項

下表顯示的選項，可讓您指定以將桌面平台指派給使用者，或移除指派。

表 12-9. 用於指派專用桌面平台的選項

選項	說明
`-d` *desktop*	指定桌面平台集區的名稱。
`-m` *machine*	指定主控遠端桌面平台之虛擬機器的名稱。
`-r`	移除對指定使用者的指派，或對指定機器所有的指派。
`-u` *domain\user*	指定使用者的登入名稱和網域。

範例

將桌面平台集區 dtpool1 中的機器 machine2 指派給 CORP 網域中的使用者 Jo。

```
vdmadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

對於 CORP 網域中的使用者 Jo，將集區 dtpool1 中的桌面平台指派移除。

```
vdmadmin -L -d dtpool1 -u Corp\Jo -r
```

將桌面平台集區 dtpool3 中的機器 machine1 所有的使用者指派移除。

```
vdmadmin -L -d dtpool3 -m machine1 -r
```

使用 -M 選項顯示機器的相關資訊

您可以將 `vdmadmin` 命令與 `-M` 選項搭配使用，以顯示虛擬機器或實體電腦的組態相關資訊。

語法

```
vdmadmin
```

```
        -M [-b authentication_arguments] [-m machine | [-u domain\user][-d desktop]] [-xml | -csv] [-w
| -n]
```

用法提示

該命令會顯示遠端桌面平台之基礎虛擬機器或實體電腦的相關資訊。

- 顯示機器名稱。
- 桌面平台集區的名稱。
- 機器狀態。

  機器狀態可以是下列其中一個值：UNDEFINED、PRE_PROVISIONED、CLONING、CLONINGERROR、CUSTOMIZING、READY、DELETING、MAINTENANCE、ERROR、LOGOUT。

  該命令不會顯示在 Horizon Administrator 中顯示的所有動態機器狀態，例如已連線或已中斷連線。
- 指派使用者的 SID。
- 指派使用者的帳戶名稱。
- 指派使用者的網域名稱。
- 虛擬機器的詳細目錄路徑 (如適用)。
- 建立機器的日期。
- 機器的範本路徑 (如適用)。
- vCenter Server 的 URL (如適用)。

選項

下表顯示您可以用來指定要顯示詳細資料之機器的選項。

表 12-10. 顯示機器相關資訊的選項

選項	說明
-d *desktop*	指定桌面平台集區的名稱。
-m *machine*	指定虛擬機器的名稱。
-u *domain\user*	指定使用者的登入名稱和網域。

範例

針對已指派給 CORP 網域中使用者 Jo 的集區 dtpool2，顯示其中遠端桌面平台之基礎機器的相關資訊，並使用 ASCII 字元將輸出格式化為 XML。

```
vdmadmin -M -u CORP\Jo -d dtpool2 -xml -n
```

顯示機器 machine3 的相關資訊，並將輸出格式化為逗號分隔值。

```
vdmadmin -M -m machine3 -csv
```

使用 -M 選項回收虛擬機器上的磁碟空間

您可以將 vdmadmin 命令與 -M 選項搭配使用，以標記要回收磁碟空間的連結複製虛擬機器。Horizon 7 會將 ESXi 主機導向至連結複製作業系統磁碟上的回收磁碟空間，無須等待作業系統磁碟上的未使用空間到達在 Horizon Administrator 中指定的臨界值下限。

語法

```
vdmadmin
-M [-b authentication_arguments] -d desktop-m machine-markForSpaceReclamation
```

使用附註

基於示範或疑難排解的目的，您可以使用此選項在特定的虛擬機器上起始磁碟空間回收。

如果您在停止期間生效時執行此命令，則空間回收不會發生。

必須先符合以下先決條件，您才能將 vdmadmin 命令與 -M 選項搭配使用，來回收磁碟空間：

- 確認 Horizon 7 目前使用的是 vCenter Server 與 ESXi 5.1 版或更新版本。
- 確認 vSphere 5.1 或更新版隨附的 VMware Tools 已安裝在虛擬機器上。
- 確認虛擬機器的虛擬硬體版本為 9 或更新版本。
- 在 Horizon Administrator 中，確認已為 vCenter Server 選取了**啟用空間回收**選項。請參閱允許 vSphere 回收連結複製虛擬機器中的磁碟空間。
- 在 Horizon Administrator 中，確認已為桌面平台集區選取了**回收虛擬機器磁碟空間**選項。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈回收 View Composer 連結複製上的磁碟空間〉。
- 先確認虛擬機器的電源為開啟，再起始空間回收作業。
- 確認停止期間未生效。請參閱《在 Horizon 7 中設定虛擬桌面平台》文件中的〈設定 View Composer 連結複製的儲存加速器和空間回收停機時間〉。

選項

表 12-11. 可在虛擬機器上回收磁碟空間的選項

選項	說明
-d *desktop*	指定桌面平台集區的名稱。
-m *machine*	指定虛擬機器的名稱。
-MarkForSpaceReclamation	標記虛擬機器以進行磁碟空間回收。

範例

標記桌面平台集區 pool1 中的虛擬機器 machine3 進行磁碟空間回收。

```
vdmadmin -M -d pool1 -m machine3 -markForSpaceReclamation
```

使用 -N 選項設定網域篩選條件

您可以將 vdmadmin 命令與 -N 選項搭配使用，以控制 Horizon 7 開放給使用者的網域。

語法

```
vdmadmin
-N [-b authentication_arguments] -domains {-exclude | -include | -search} -domaindomain-add [-s connsvr]
```

```
vdmadmin
-N [-b authentication_arguments] -domains-list [-w | -n] [-xml]
```

```
vdmadmin
-N [-bauthentication_arguments] -domains-list-active [-w | -n] [-xml]
```

```
vdmadmin
-N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -remove [-s connsvr]
```

```
vdmadmin
-N [-b authentication_arguments] -domains {-exclude | -include | -search} -removeall [-s connsvr]
```

用法提示

指定其中一個 -exclude、-include 或 -search 選項以將作業分別套用至排除清單、包含清單或搜尋排除清單。

如果您將網域新增至搜尋排除清單，該網域便會從自動網域搜尋中排除。

如果您將網域新增至包含清單，該網域便會包含在搜尋結果中。

如果您將網域新增至排除清單，該網域便會從搜尋結果中排除。

選項

下表顯示您可以指定用來設定網域篩選條件的選項。

表 12-12. 設定網域篩選條件的選項

選項	說明
-add	將網域新增至清單。
-domain *domain*	指定要篩選的網域。 您必須依其 NetBIOS 名稱指定網域，而非依 DNS 名稱。
-domains	指定網域篩選條件作業。

表 12-12. 設定網域篩選條件的選項 (續)

選項	說明
–exclude	指定排除清單上的作業。
–include	指定包含清單上的作業。
–list	顯示每個連線伺服器執行個體上和連線伺服器群組中已在搜尋排除清單、排除清單及包含清單中設定的網域。
–list –active	顯示您在其上執行命令的連線伺服器執行個體的可用網域。
–remove	移除清單中的網域。
–removeall	移除清單中的所有網域。
–s *connsvr*	指定將作業套用至連線伺服器執行個體上的網域篩選條件。您可以依其名稱或 IP 位址指定連線伺服器執行個體。 如果不指定此作業，則您對搜尋組態所做的任何變更都會套用至群組中的所有連線伺服器執行個體。
–search	指定搜尋排除清單上的作業。

範例

將網域 FARDOM 新增至連線伺服器執行個體 csvr1 的搜尋排除清單。

```
vdmadmin –N –domains –search –domain FARDOM –add –s csvr1
```

將網域 NEARDOM 新增至連線伺服器群組的排除清單。

```
vdmadmin –N –domains –exclude –domain NEARDOM –add
```

顯示群組中和針對群組的連線伺服器執行個體上的網域搜尋組態。

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR–1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR–2
   Include:
   Exclude:
   Search :
```

Horizon 7 會將群組中每個連線伺服器主機上的網域搜尋限制為排除網域 FARDOM 和 DEPTX。CONSVR-1 之排除清單旁的字元 (*) 表示，Horizon 7 會排除 CONSVR-1 上網域搜尋結果中的 YOURDOM 網域。

使用 ASCII 字元以 XML 顯示網域篩選條件。

```
vdmadmin –N –domains –list –xml –n
```

顯示本機連線伺服器執行個體上可用於 Horizon 7 的網域。

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS:fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

使用 ASCII 字元以 XML 顯示可用網域。

```
vdmadmin –N –domains –list –active –xml –n
```

從排除清單中移除連線伺服器群組的網域 NEARDOM。

```
vdmadmin –N –domains –exclude –domain NEARDOM –remove
```

從包含清單中移除連線伺服器執行個體 csvr1 的所有網域。

```
vdmadmin –N –domains –include –removeall –s csvr1
```

設定網域篩選條件

您可以設定網域篩選條件以限制連線伺服器執行個體或安全伺服器開放給使用者的網域。

Horizon 7 將判定哪些網域可透過周遊的信任關係進行存取，並先以連線伺服器執行個體或安全伺服器所在的網域開始。若是一組連線良好的小型網域，Horizon 7 可以快速判定完整的網域清單，但此項作業所需的時間會隨著網域數量的增加或網域間連線的減少而增加。Horizon 7 還可能包含搜尋結果中您不想在使用者登入遠端桌面平台時提供給他們的網域。

如果您已將控制遞迴網域列舉的 Windows 登錄機碼之值 (`HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum`) 設定為 false，就會停用遞迴網域搜尋，而連線伺服器執行個體便只會使用主要網域。若要使用網域篩選功能，請刪除登錄機碼或將其值設定為 true，然後重新啟動系統。您必須在已設定此機碼的每個連線伺服器執行個體上進行此項作業。

下表顯示您可以指定來設定網域篩選的網域清單類型。

表 12-13. 網域清單類型

網域清單類型	說明
搜尋排除清單	指定 Horizon 7 可以在自動搜尋期間周遊的網域。該搜尋會忽略搜尋排除清單中所包含的網域，且不會嘗試尋找已排除網域所信任的網域。您無法排除該搜尋中的主要網域。
排除清單	指定 Horizon 7 從網域搜尋結果中排除的網域。您無法排除主要網域。
包含清單	指定 Horizon 7 不從網域搜尋結果中排除的網域。除了主要網域外，所有其他的網域都會移除。

自動網域搜尋擷取的網域清單中，會排除您在搜尋排除清單中指定的那些網域及它們所信任的網域。Horizon 7 會以此順序選取第一個非空白的排除清單或包含清單。

1 為連線伺服器執行個體設定的排除清單。

2 為連線伺服器群組設定的排除清單。

3 為連線伺服器執行個體設定的包含清單。

4 為連線伺服器群組設定的包含清單。

Horizon 7 只會將其所選的第一個清單套用至搜尋結果。

如果您指定要包含的網域，但它的網域控制站目前無法存取，Horizon 7 就不會在作用中網域清單中包含該網域。

您無法排除連線伺服器執行個體或安全伺服器所屬的主要網域。

篩選以包含網域範例

您可以使用包含清單來指定 Horizon 7 不會自網域搜尋結果中排除的網域。除了主要網域，會移除所有其他網域。

連線伺服器執行個體已加入主要 MYDOM 網域，且與 YOURDOM 網域有信任關係。YOURDOM 網域與 DEPTX 網域間有信任關係。

顯示連線伺服器執行個體的目前使用中網域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

DEPTY 與 DEPTZ 網域會出現在清單中，因為它們是 DEPTX 網域的信任網域。

指定連線伺服器執行個體除了主要 MYDOM 網域之外，應只讓 YOURDOM 與 DEPTX 網域可用。

```
vdmadmin -N -domains -include -domain YOURDOM -add
vdmadmin -N -domains -include -domain DEPTX -add
```

顯示在包含 YOURDOM 與 DEPTX 網域後的目前使用中網域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM
Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
```

Horizon 7 會將包含清單套用至網域搜尋結果。如果網域階層非常複雜，或某些網域的網路連線不佳，則網域搜尋會很慢。在這類情況下，請改用搜尋排除項目。

篩選以排除網域範例

您可以使用排除清單來指定 Horizon 7 會從網域搜尋結果中排除的網域。

一個包含兩個連線伺服器執行個體 (CONSVR-1 與 CONSVR-2) 的群組，會加入主要 MYDOM 網域，並與 YOURDOM 網域有信任關係。YOURDOM 網域和 DEPTX 及 FARDOM 網域間有信任關係。

FARDOM 網域位於遠端地理位置，並透過緩慢、高延遲的連結，經由網路連線至該網域。FARDOM 網域中的使用者不一定要能存取 MYDOM 網域中的連線伺服器群組。

顯示連線伺服器群組成員的目前使用中網域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

DEPTY 與 DEPTZ 網域是 DEPTX 網域的信任網域。

若要改善 Horizon Client 連線效能，請從連線伺服器群組的搜尋中排除 FARDOM 網域。

```
vdmadmin -N -domains -search -domain FARDOM -add
```

此命令會顯示從搜尋中排除 FARDOM 網域後的目前使用中網域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

延伸搜尋排除清單，將 DEPTX 網域及其所有的信任網域從群組中所有連線伺服器執行個體的網域搜尋中排除。此外也排除 YOURDOM 網域，讓其在 CONSVR-1 上不可用。

```
vdmadmin -N -domains -search -domain DEPTX -add
vdmadmin -N -domains -exclude -domain YOURDOM -add -s CONSVR-1
```

顯示新的網域搜尋組態。

```
C:\ vdmadmin -N -domains -list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR-1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR-2
   Include:
   Exclude:
   Search :
```

Horizon 7 會將群組中每個連線伺服器主機上的網域搜尋限制為排除網域 FARDOM 和 DEPTX。CONSVR-1 之排除清單旁的字元 (*) 表示，Horizon 7 會排除 CONSVR-1 上網域搜尋結果中的 YOURDOM 網域。

在 CONSVR-1 上顯示目前使用中網域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
```

```
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

在 CONSVR-2 上顯示目前使用中網域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-2)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
```

使用 -O 與 -P 選項顯示未獲權使用者的機器與原則

您可以將 vdmadmin 命令與 -O 和 -P 選項搭配使用，以顯示指派給不再有權使用系統之使用者的虛擬機器與原則。

語法

```
vdmadmin
-O [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

```
vdmadmin
-P [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

用法提示

如果您撤銷使用者使用持續性虛擬機器或實體系統的權利，則相關聯的遠端桌面平台指派並不會自動撤銷。如果您已暫止使用者的帳戶，或使用者休假中，則可能可接受此狀況。當您重新啟用權利後，使用者可繼續使用與先前相同的虛擬機器。如果使用者已離開組織，則其他使用者便無法存取虛擬機器，且該虛擬機器會視為孤立。您可能也想要檢查指派給未獲權使用者的任何原則。

選項

下表顯示的選項，可讓您指定以顯示未獲權使用者的虛擬機器與原則。

表 12-14. 用於顯示未獲權使用者的機器與原則的選項

選項	說明
-ld	依機器安排輸出項目順序。
-lu	依使用者安排輸出項目順序。

表 12-14. 用於顯示未獲權使用者的機器與原則的選項 (續)

選項	說明
-noxslt	指定預設樣式表不應套用至 XML 輸出。
-xsltpath *path*	指定用於轉換 XML 輸出的樣式表路徑。

表 12-15. XSL 樣式表 顯示您可套用到 XML 輸出以轉換為 HTML 的樣式表。樣式表位於目錄 C:\Program Files\VMware\VMware View\server\etc 中。

表 12-15. XSL 樣式表

樣式表檔案名稱	說明
unentitled-machines.xsl	轉換包含未獲權虛擬機器清單的報告，依使用者或系統分組，且目前已指派給使用者。這是預設的樣式表。
unentitled-policies.xsl	轉換包含虛擬機器清單的報告，這些虛擬機器具有已套用到未獲權使用者的使用者層級原則。

範例

顯示指派給未獲權使用者的虛擬機器，以文字格式依虛擬機器分組。

```
vdmadmin -O -ld
```

顯示指派給未獲權使用者的虛擬機器，以使用 ASCII 字元的 XML 格式依使用者分組。

```
vdmadmin -O -lu -xml -n
```

套用您自己的樣式表 C:\tmp\unentitled-users.xsl，並將輸出重新導向至檔案 uu-output.html。

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xsl" > uu-output.html
```

顯示與未獲權使用者的虛擬機器相關聯的使用者原則，並以使用 Unicode 字元的 XML 格式依桌面平台分組。

```
vdmadmin -P -ld -xml -w
```

套用您自己的樣式表 C:\tmp\unentitled-policies.xsl，並將輸出重新導向至檔案 up-output.html。

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xsl" > up-output.html
```

使用 -Q 選項設定 Kiosk 模式中的用戶端

您可以將 vdmadmin 命令與 -Q 選項搭配使用，以設定預設值並在 Kiosk 模式中建立用戶端的帳戶，以便啟用這些用戶端的驗證，和顯示其組態的相關資訊。

語法

```
vdmadmin
-Q
-clientauth
-add [-b authentication_arguments] -domain domain_name-clientid client_id [-password "password"
| -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-groupgroup_name | -nogroup] [-description
"description_text"]
```

```
vdmadmin
-Q
-disable [-b authentication_arguments] -s connection_server
```

```
vdmadmin
-Q
-enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

```
vdmadmin
-Q
-clientauth
-getdefaults [-b authentication_arguments] [-xml]
```

```
vdmadmin
-Q
-clientauth
-list [-b authentication_arguments] [-xml]
```

```
vdmadmin
-Q
-clientauth
-remove [-b authentication_arguments] -domain domain_name-clientid client_id
```

```
vdmadmin
-Q
-clientauth
-removeall [-b authentication_arguments] [-force]
```

```
vdmadmin
-Q
-clientauth
```

```
        -setdefaults [-b authentication_arguments] [-ou DN] [ -expirepassword | -noexpirepassword ] [-group
group_name | -nogroup]
```

```
        vdmadmin
        -Q
        -clientauth
        -update [-b authentication_arguments] -domain domain_name-clientid client_id [-password
"password" | -genpassword] [-description "description_text"]
```

用法提示

在用戶端用來連線至其遠端桌面平台的連線伺服器執行個體所在的群組中，您必須對其中一個連線伺服器執行個體執行 vdmadmin 命令。

設定密碼到期日和 Active Directory 群組成員資格的預設值後，這些設定都會由群組中的所有連線伺服器執行個體共用。

在 Kiosk 模式下新增用戶端時，Horizon 7 將在 Active Directory 中建立用戶端的使用者帳戶。如果您為用戶端指定名稱，此名稱必須以 "custom-" 字元開頭，或以能在 ADAM 中定義的其中一個替代字串開頭，長度不能超過 20 個字元。一個指定的名稱只能用於一個用戶端裝置。

您可以在連線伺服器執行個體上將替代首碼定義為 ADAM 中 cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int 之下 pae-ClientAuthPrefix 多值屬性中的「custom-」。請避免將這些首碼用於一般使用者帳戶。

如果您不指定用戶端的名稱，Horizon 7 將從您為用戶端裝置所指定的 MAC 位址產生名稱。例如，如果 MAC 位址為 00:10:db:ee:76:80，則對應的帳戶名稱為 cm 00_10_db_ee_76_80。您僅能將這些帳戶用於您啟用以驗證用戶端的連線伺服器執行個體。

某些精簡型用戶端僅允許以 "custom-" 或 "cm-" 開頭的帳戶名稱用於 Kiosk 模式。

自動產生的密碼長度為 16 個字元，至少包含一個大寫字母、一個小寫字母、一個符號及一個數字，而且可以包含重複的字元。如果您需要強度更高的密碼，必須使用 -password 選項來指定密碼。

如果使用 -group 選項來指定群組或先前已設定了預設群組，則 Horizon 7 會將用戶端的帳戶新增至此群組。您可以指定 -nogroup 選項以防止帳戶新增至任何群組。

如果啟用連線伺服器執行個體來驗證 Kiosk 模式下的用戶端，可以選擇性地將該用戶端指定為必須提供密碼。如果停用驗證，則用戶端便無法連線至其遠端桌面平台。

雖然您啟用或停用個別連線伺服器執行個體的驗證，但群組中所有連線伺服器執行個體會共用用戶端驗證的所有其他設定。您只需要新增用戶端一次，就能讓群組中的所有連線伺服器執行個體從用戶端接受要求。

如果在啟用驗證時指定了 -requirepassword 選項，則連線伺服器執行個體就無法驗證已自動產生密碼的用戶端。如果您變更連線伺服器執行個體的組態以指定此選項，則這類用戶端無法驗證自己，它們會失敗且出現以下錯誤訊息：未知的使用者名稱或不正確的密碼。

選項

下表顯示您可以指定用來在 Kiosk 模式中設定用戶端的選項。

表 12-16. 在 Kiosk 模式中設定用戶端的選項

選項	說明
`-add`	在 Kiosk 模式中新增用戶端的帳戶。
`-clientauth`	在 Kiosk 模式中指定用戶端設定驗證的作業。
`-clientid` *client_id*	指定用戶端的名稱或 MAC 位址。
`-description` "*description_text*"	為 Active Directory 中的用戶端裝置建立帳戶的說明。
`-disable`	在指定的連線伺服器執行個體上停用 Kiosk 模式下的用戶端驗證。
`-domain` *domain_name*	指定用戶端裝置帳戶的網域。
`-enable`	在指定的連線伺服器執行個體上啟用 Kiosk 模式下的用戶端驗證。
`-expirepassword`	指定用戶端帳戶上密碼的到期時間與連線伺服器群組相同。如果未定義群組的到期時間，則密碼不會到期。
`-force`	停用在 Kiosk 模式中移除用戶端帳戶時出現的確認提示。
`-genpassword`	產生用戶端帳戶的密碼。如果您未指定 `-password` 或 `-genpassword`，這將是預設行為。
`-getdefaults`	取得用於新增用戶端帳戶的預設值。
`-group` *group_name*	對要新增用戶端帳戶的預設群組指定名稱。必須指定群組的名稱作為 Active Directory 的 Windows 2000 以前版本群組名稱。
`-list`	顯示用戶端在 Kiosk 模式中的相關資訊，以及當您在其上以 Kiosk 模式啟用用戶端驗證時連線伺服器執行個體的相關資訊。
`-noexpirepassword`	指定帳戶的密碼不會到期。
`-nogroup`	新增用戶端的帳戶時，請指定此用戶端帳戶不會新增至預設群組。 設定用戶端的預設值時，請清除預設群組的設定。
`-ou` *DN*	對要新增用戶端帳戶的組織單位指定辨別名稱。 例如：OU=kiosk-ou,DC=myorg,DC=com **備註** 您無法使用 `-setdefaults` 選項來變更組織單位的組態。
`-password` "*password*"	指定用戶端帳戶的明確密碼。
`-remove`	在 Kiosk 模式中移除用戶端的帳戶。
`-removeall`	在 Kiosk 模式中移除所有用戶端的帳戶。
`-requirepassword`	指定 Kiosk 模式中的用戶端必須提供密碼。Horizon 7 將不會接受已產生的密碼來進行新的連線。
`-s` *connection_server*	對要在其上以 Kiosk 模式啟用或停用用戶端驗證的連線伺服器執行個體指定 NetBIOS 名稱。
`-setdefaults`	設定用於新增用戶端帳戶的預設值。
`-update`	在 Kiosk 模式中更新用戶端的帳戶。

範例

設定組織單位、密碼到期日及用戶端群組成員資格的預設值。

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

以純文字格式取得用戶端的目前預設值。

```
vdmadmin -Q -clientauth -getdefaults
```

以 XML 格式取得用戶端的目前預設值。

```
vdmadmin -Q -clientauth -getdefaults -xml
```

將由其 MAC 位址指定的用戶端帳戶新增至 MYORG 網域，並使用群組 kc-grp 的預設設定。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

將由其 MAC 位址指定的用戶端帳戶新增至 MYORG 網域，並使用自動產生的密碼。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword -ou "OU=kiosk-
ou,DC=myorg,DC=com" -group kc-grp
```

新增具名用戶端的帳戶，並指定用於用戶端的密碼。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou
"OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

更新用戶端帳戶，指定新的密碼和說明文字。

```
vdmadmin -Q -clientauth -update -domain MYORG -clientid custom-Terminal21 -password "Secret1!" -
description "Foyer Entry Workstation"
```

從 MYORG 網域移除由其 MAC 位址指定的 Kiosk 用戶端帳戶。

```
vdmadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```

移除所有用戶端帳戶而不出現確認移除的提示。

```
vdmadmin -Q -clientauth -removeall -force
```

啟用連線伺服器執行個體 csvr-2 的用戶端驗證。具有自動產生密碼的用戶端不須提供密碼即可自行驗證。

```
vdmadmin -Q -enable -s csvr-2
```

啟用連線伺服器執行個體 csvr-3 的用戶端驗證，需要用戶端對 Horizon Client 指定其密碼。具有自動產生密碼的用戶端無法自行驗證。

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

停用連線伺服器執行個體 csvr-1 的用戶端驗證。

```
vdmadmin –Q –disable –s csvr–1
```

以文字格式顯示用戶端的相關資訊。用戶端 cm-00_0c_29_0d_a3_e6 具有自動產生的密碼，且不需要使用者或應用程式指令碼對 Horizon Client 指定此密碼。用戶端 cm-00_22_19_12_6d_cf 具有明確指定的密碼，而且需要使用者提供此密碼。連線伺服器執行個體 CONSVR2 接受來自具有自動產生密碼之用戶端的驗證要求。CONSVR1 不接受 Kiosk 模式下用戶端的驗證要求。

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID               : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID           : cm–00_0c_29_0d_a3_e6
Domain             : myorg.com
Password Generated: true

GUID               : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID           : cm–00_22_19_12_6d_cf
Domain             : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                    : CONSVR1
Client Authentication Enabled : false
Password Required              : false

Common Name                    : CONSVR2
Client Authentication Enabled : true
Password Required              : false
```

使用 -R 選項顯示機器的第一個使用者

您可以將 vdmadmin 命令與 –R 選項搭配使用，找出受管理虛擬機器的初始指派。例如，當遺失 LDAP 資料時，您可能需要此資訊，以便將虛擬機器重新指派給使用者。

備註 具有 –R 選項的 vdmadmin 命令僅在 View Agent 5.1 以前的虛擬機器上有作用。在執行 View Agent 5.1 和更新版本及 Horizon Agent 7.0 和更新版本的虛擬機器上，此選項沒有作用。若要找到虛擬機器的第一個使用者，請使用事件資料庫判定哪些使用者曾登入機器。

語法

```
vdmadmin
–R
–i
network_address
```

使用附註

您無法以具權限的使用者身分使用 -b 選項執行此命令。您必須以 **Administrator** 角色的使用者身分登入。

選項

-i 選項可指定虛擬機器的 IP 位址。

範例

顯示存取 IP 位址為 10.20.34.120 的虛擬機器的第一個使用者。

```
vdmadmin -R -i 10.20.34.120
```

使用 -S 選項移除連線伺服器執行個體或安全伺服器項目

您可以將 vdmadmin 命令與 -S 選項搭配使用，以移除 Horizon 7 組態中的連線伺服器執行個體或安全伺服器的項目。

語法

```
vdmadmin
-S [-b authentication_arguments] -r-s server
```

用法提示

為確保高可用性，Horizon 7 允許您在連線伺服器群組中設定一或多個複寫連線伺服器執行個體。如果您停用群組中的連線伺服器執行個體，伺服器項目會在 Horizon 7 組態內存留下來。

您也可以將 vdmadmin 命令與 -S 選項搭配使用，以移除您 Horizon 7 環境中的安全伺服器。如果您打算升級或重新安裝安全伺服器，但不將它永久移除，您不必使用此選項。

若要永久移除，請執行這些工作：

1 執行連線伺服器安裝程式，將連線伺服器執行個體或安全伺服器從 Windows Server 電腦中解除安裝。

2 執行 [新增或移除程式] 工具，將 Adam Instance VMwareVDMDS 程式從 Windows Server 電腦中移除。

3 在另一個連線伺服器執行個體中，使用 vdmadmin 命令將已解除安裝的連線伺服器執行個體或安全伺服器項目從組態中移除。

如果您要在已移除的系統上重新安裝 Horizon 7，但不複寫原始群組的 Horizon 7 組態，請先重新啟動原始群組中所有的連線伺服器主機，再執行重新安裝。這會防止重新安裝的連線伺服器執行個體接收來自其原始群組的組態更新。

選項

-s 選項可指定待移除的連線伺服器執行個體或安全伺服器的 NetBIOS 名稱。

範例

移除連線伺服器執行個體 connsvr3 的項目。

```
vdmadmin –S –r –s connsvr3
```

使用 -T 選項為管理員提供次要認證

您可以使用 vdmadmin 命令搭配 –T 選項，提供 Active Directory 次要認證給管理員使用者。

語法

```
          vdmadmin
          –T [–b authentication_arguments] –domainauth
 {–add | –update | –remove | –removeall | –list} –ownerdomain\user–userdomain\user [–passworpassword]
```

用法提示

如果您的使用者和群組位在與連線伺服器網域具有單向信任關係的網域中，您必須為 Horizon Administrator 中的管理員使用者提供次要認證。管理員必須擁有次要認證，才能存取單向受信任網域。單向受信任網域可以是外部網域或位於可轉移樹系信任中的網域。

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

使用 vdmadmin 命令，您可依每位使用者為基礎來設定次要認證。您不能設定全域指定的次要認證。

至於樹系信任，通常僅可為樹系根網域設定次要認證。接著，連線伺服器就能列舉樹系信任中的子網域。

只有當位在單向受信任網域中的使用者首次登入時，才能執行 Active Directory 帳戶鎖定、停用和登入時數檢查。

單向受信任網域不支援使用者的 PowerShell 管理和智慧卡驗證。不支援單向受信任網域中使用者的 SAML 驗證。

次要認證帳戶需要下列權限。依預設，標準使用者帳戶應該具備這些權限。

- 列出內容
- 讀取全部內容
- 讀取權限
- 讀取 tokenGroupsGlobalAndUniversal (由 [讀取全部內容] 隱含表示)

限制

- 不支援單向受信任網域中使用者的 PowerShell 管理和智慧卡驗證。
- 不支援單向受信任網域中使用者的 SAML 驗證。

選項

表 12-17. 提供次要認證的選項

選項	說明
-add	新增擁有者帳戶的次要認證。 會執行 Windows 登入以確認指定的認證是否有效。並在 View LDAP 中為使用者建立外部安全性主體 (FSP)。
-update	更新擁有者帳戶的次要認證。 會執行 Windows 登入以確認更新的認證是否有效。
-list	顯示擁有者帳戶的安全性認證。不會顯示密碼。
-remove	移除擁有者帳戶的安全性認證。
-removeall	移除擁有者帳戶的所有安全性認證。

範例

新增所指定擁有者帳戶的次要認證。會執行 Windows 登入以確認指定的認證是否有效。

```
vdmadmin -T -domainauth -add -owner domain\user -user domain\user -password password
```

更新所指定擁有者帳戶的次要認證。會執行 Windows 登入以確認更新的認證是否有效。

```
vdmadmin -T -domainauth -update -owner domain\user -user domain\user -password password
```

移除所指定擁有者帳戶的次要認證。

```
vdmadmin -T -domainauth -remove -owner domain\user -user domain\user
```

移除所指定擁有者帳戶的所有次要認證。

```
vdmadmin -T -domainauth -removeall -owner domain\user
```

顯示所指定擁有者帳戶的所有次要認證。不會顯示密碼。

```
vdmadmin -T -domainauth -list -owner domain\user
```

使用 -U 選項顯示使用者的相關資訊

您可以將 vdmadmin 命令與 -U 選項搭配使用，以顯示使用者的詳細資訊。

語法

```
vdmadmin
-U [-b authentication_arguments] -u domain\user [-w | -n] [-xml]
```

使用附註

此命令可顯示從 Active Directory 與 Horizon 7 所取得的使用者相關資訊。

- Active Directory 中使用者帳戶的詳細資料。
- Active Directory 群組的成員資格。
- 機器權利，包括機器識別碼、顯示名稱、說明、資料夾，以及機器是否已停用。
- ThinApp 指派。
- 管理員角色，包括使用者的管理權限及使用者具有這些權限的資料夾。

選項

-u 選項可指定使用者的名稱與網域。

範例

以使用 ASCII 字元的 XML 格式，顯示 CORP 網域中使用者 Jo 的相關資訊。

```
vdmadmin -U -u CORP\Jo -n -xml
```

使用 -V 選項解除鎖定或鎖定虛擬機器

您可以將 vdmadmin 命令與 -V 選項搭配使用，以解除鎖定或鎖定資料中心的虛擬機器。

語法

```
vdmadmin
-V [-bauthentication_arguments] -e-ddesktop-mmachine [-m machine] ...
```

```
vdmadmin
-V [-bauthentication_arguments] -e-vcdnvCenter_dn-vmpath inventory_path
```

```
vdmadmin
-V [-b authentication_arguments] -p-d desktop -m machine [-mmachine] ...
```

```
vdmadmin
-V [-b authentication_arguments] -p-vcdnvCenter_dn-vmpath inventory_path
```

用法提示

您只能在遇到問題，使得遠端桌面平台出現不正確狀態時，才能使用 vdmadmin 命令來解除鎖定或鎖定虛擬機器。請勿使用此命令來管理正常運作的遠端桌面平台。

如果遠端桌面平台已鎖定且其虛擬機器項目已不存在於 ADAM 中，則使用 `-vmpath` 和 `-vcdn` 選項，指定虛擬機器和 vCenter Server 的詳細目錄路徑。您可以使用 vCenter Client 在 `Home/Inventory/VMs and Templates` 下找出遠端桌面平台之虛擬機器的詳細目錄路徑。您可以使用 ADAM ADSI Edit 在 `OU=Properties` 標題下找出 vCenter Server 的辨別名稱。

選項

下表顯示您可指定以解除鎖定或鎖定虛擬機器的選項。

表 12-18. 可用來解除鎖定或鎖定虛擬機器的選項

選項	說明
`-d` *desktop*	指定桌面平台集區。
`-e`	解除鎖定虛擬機器。
`-m` *machine*	指定虛擬機器的名稱。
`-p`	鎖定虛擬機器。
`-vcdn` *vCenter_dn*	指定 vCenter Server 的辨別名稱。
`-vmpath` *inventory_path*	指定虛擬機器的詳細目錄路徑。

範例

解除鎖定桌面平台集區 dtpool3 中的虛擬機器 machine1 和 machine2。

```
vdmadmin -V -e -d dtpool3 -m machine1 -m machine2
```

鎖定桌面平台集區 dtpool3 中的虛擬機器 machine3。

```
vdmadmin -V -p -d dtpool3 -m machine3
```

使用 -X 選項偵測和解決 LDAP 項目和結構描述衝突

您可以將 `vdmadmin` 命令與 `-X` 選項搭配使用，以偵測和解決群組中已複寫連線伺服器執行個體上的 LDAP 項目衝突和 LDAP 結構描述衝突。您也可以使用此選項來偵測和解決 Cloud Pod 架構環境中的 LDAP 結構描述衝突。

語法

```
        vdmadmin
        -X [-bauthentication_arguments] -collisions [-resolve]
vdmadmin-X [-bauthentication_arguments] -schemacollisions [-resolve] [-global]
```

使用附註

兩個以上的連線伺服器執行個體上有重複的 LDAP 項目時，可能會在 Horizon 7 中造成 LDAP 資料完整性的問題。在 LDAP 複寫未運作時升級，即可能發生此狀況。雖然 Horizon 7 會定期檢查此錯誤狀況，但您也可以在群組內的其中一個連線伺服器執行個體上執行 vdmadmin 命令，以手動偵測和解決 LDAP 項目衝突。

在 LDAP 複寫未運作時升級，也可能會發生 LDAP 結構描述衝突。由於 Horizon 7 不會檢查此錯誤狀況，因此您必須執行 vdmadmin 命令，以手動方式偵測和解決 LDAP 結構描述衝突。

選項

下表顯示可指定用來偵測和解決 LDAP 項目衝突的選項。

表 12-19. 偵測和解決 LDAP 項目衝突的選項

選項	說明
-collisions	指定在連線伺服器群組中偵測 LDAP 項目衝突的作業。
-resolve	解決 LDAP 執行個體中的所有 LDAP 衝突。若未指定此選項，則命令僅會列出它所發現的問題。

下表顯示可指定用來偵測和解決 LDAP 結構描述衝突的選項。

表 12-20. 偵測和解決 LDAP 結構描述衝突的選項

選項	說明
-schemacollisions	指定在連線伺服器群組或 Cloud Pod 架構環境中偵測 LDAP 結構描述衝突的作業。
-resolve	解決 LDAP 執行個體中的所有 LDAP 結構描述衝突。若未指定此選項，則命令僅會列出它所發現的問題。
-global	對 Cloud Pod 架構環境中的全域 LDAP 執行個體套用檢查和修正。若未指定此選項，則會對本機 LDAP 執行個體執行檢查。

範例

偵測連線伺服器群組中的 LDAP 項目衝突。

```
vdmadmin -X -collisions
```

偵測和解決本機 LDAP 執行個體中的 LDAP 項目衝突。

```
vdmadmin -X -collisions -resolve
```

偵測和解決全域 LDAP 執行個體中的 LDAP 結構描述衝突。

```
vdmadmin -X -schemacollisions -resolve -global
```