Horizon Console 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

Copyright © 2018-2019 VMware, Inc. 保留所有權利。 版權與商標資訊。

目錄

VMware Horizon Console 管理

1

《VMware Horizon Console 管理》說明如何在 Horizon Console 中設定和管理 VMware Horizon® 7、建立管理員、設定使用者驗證、設定原則，以及執行管理工作。此文件也說明如何維護 Horizon 7 元件和進行疑難排解。

如需如何使用 Horizon Console 來設定和管理 Cloud Pod 架構環境的相關資訊，請參閱《在 Horizon 7 中管理 Cloud Pod 架構》文件。

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 VMware Horizon Console 2

VMwareHorizon Console 是最新版本的 Web 介面，您可以透過它來建立和管理虛擬桌面平台和已發佈桌面平台和應用程式。Horizon Console 也整合用於管理工作區的 VMware Horizon Just-in-Time Management Platform (JMP) 整合式工作流程功能。

在您安裝並設定 Horizon 連線伺服器之後，Horizon Console 才可供使用。

如需關於 JMP 整合式工作流程功能的詳細資訊，請參閱第 10 章 開始使用 JMP Integrated Workflow。

本章節討論下列主題：

支援的 Horizon 7 功能

Horizon Console 以 HTML5 技術為基礎，且可讓您管理完整的 Horizon 7 部署。Horizon Console 會取代 Flash 型 Horizon Administrator。

如需支援使用 Horizon Administrator 之 Horizon 7 功能的相關資訊，請參閱《Horizon 7 管理》文件。

支援下列功能：

- 伺服器
  - Horizon 連線伺服器組態
  - 事件資料庫
- 權利
  - 使用者和群組權利
  - 桌面平台權利
  - 應用程式權利
  - 全域權利

    - 全域原則
- 驗證
    - 遠端存取驗證
    - 已發佈應用程式的未驗證存取
    - 智慧卡驗證
    - 角色型委派管理
- 虛擬桌面平台
    - 完整虛擬機器的自動化專用指派集區
    - 自動化、即時複製專用指派和浮動指派集區
    - 自動連結複製桌面平台集區
    - 完整虛擬機器的自動化浮動指派集區
    - 手動桌面平台集區
    - 持續性磁碟
- 已發佈桌面平台
    - 手動伺服器陣列
    - 自動化即時複製伺服器陣列
    - 自動連結複製伺服器陣列
    - RDS 桌面平台集區
- 已發佈的應用程式
    - 手動應用程式集區
    - 來自現有應用程式的應用程式集區
- 虛擬機器
    - vCenter Server 中可供使用的虛擬機器
    - vCenter Server 中無法使用的已登錄的機器
- Cloud Pod 架構

不支援下列功能：

- ThinApp 應用程式
- 安全伺服器
- Mirage 伺服器

使用 Horizon Console 的優點

使用 Horizon Console 的優點包括簡易的桌面平台和應用程式部署程序、即時桌面平台傳遞，以及可消除安全性風險的更安全 Web 介面。

更新了 Horizon Console Web 介面以納入方便使用的工作流程，以便用於部署和疑難排解桌面平台和應用程式。

Horizon Console 也包含 JMP Integrated Workflow 功能，它將即時複製、VMware App Volumes 和 VMware Dynamic Environment Manager 技術併入整合式工作流程，以提供可快速部署和調整的隨選桌面平台。如需詳細資訊，請參閱關於 JMP Integrated Workflow。

Horizon Console 具有以 HTML5 為基礎的 Web 介面，此介面更為安全且經過更新，可消除許多安全性風險和弱點。

安裝和設定 Horizon Console

在使用 Horizon 連線伺服器安裝程式來安裝和設定連線伺服器之後，您可以透過 Horizon Administrator Web 介面取得 Horizon ConsoleURL。使用 JMPServer 安裝程式來安裝和設定 JMP Server 之後，JMP Integrated Workflow 才會在 Horizon Console 中提供使用。

如需安裝連線伺服器的詳細資訊，請參閱《Horizon 7 安裝》文件。

如需安裝和設定 JMPServer 的詳細資訊，請參閱《VMware Horizon JMP Server 安裝和設定指南》文件。

登入 Horizon Console

若要執行桌面平台或應用程式集區部署工作、疑難排解工作或管理 JMP 工作流程，您必須登入 Horizon Console。您可以使用安全 (TLS) 連線來存取 Horizon Console。

必要條件

- 確認 Horizon 連線伺服器已安裝在專用電腦上。
- 必須為使用者指派任何預先定義的角色或預先定義角色的組合，才能登入 Horizon Console。當使用者獲指派一個自訂角色或預先定義與自訂角色的組合時，您無法登入 Horizon Console。如需關於設定角色型存取的詳細資訊，請參閱設定角色型委派管理。
- 確認您使用 Horizon Console 支援的網頁瀏覽器。如需受支援網頁瀏覽器的詳細資訊，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，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 Console 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 若要一律使用 Horizon Console 登入頁面，請按一下**一律使用此選項**。

備註 如果您按一下**一律使用此選項**然後按一下**啟動**，則下次在網頁瀏覽器中開啟索引標籤並輸入 **https://server/admin** 時，您將一律會看到 Horizon Console 登入頁面。若要再次存取**歡迎使用 VMware Horizon 7** 頁面，請移至 **https://server/admin/#home**。

3 按一下 Horizon Console 下方的**啟動**，以開啟 Horizon Console 登入頁面。

4 使用有認證可存取 Administrators 帳戶的使用者身分登入。

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。

後續步驟

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 Console 標頭中和網頁瀏覽器索引標籤中檢視該名稱。

在 Horizon Console 中設定 Horizon 連線伺服器

3

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 Horizon 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：

在 Horizon Console 中設定 vCenter Server 和 Horizon Composer

若要使用虛擬機器做為遠端桌面平台，您必須將 Horizon 7 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 Console 中進行 Horizon Composer 的設定。

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，您必須為 vCenter Server 啟用 Horizon Storage Accelerator。

建立 Horizon Composer AD 作業的使用者帳戶

如果使用 Horizon Composer，您必須在 Active Directory 中建立允許 Horizon Composer 在 Active Directory 中執行特定作業的使用者帳戶。Horizon 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，請建立另一個使用者帳戶來搭配 Horizon 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，Horizon 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 Horizon Composer 網域，以及設定並部署連結複製桌面平台集區時，請在 Horizon Console 中指定帳戶。

在 Horizon Console 中安裝產品授權金鑰

您必須先輸入產品授權金鑰，才能使用連線伺服器。

備註　如果您有 Horizon 7 訂閱授權，則不需要產品授權金鑰。如需訂閱授權的詳細資訊，請參閱《Horizon 7 安裝》文件中的〈啟用 Horizon 7 以進行訂閱授權〉。

初次登入時，Horizon Console 會顯示「授權及使用」頁面。

您不需要在安裝複寫的連線伺服器執行個體或安全伺服器時設定授權金鑰。複寫執行個體和安全伺服器會使用儲存在 View LDAP 組態中的一般授權金鑰。

備註　連線伺服器需要有效的授權金鑰。產品授權金鑰是 25 個字元的金鑰。

程序

1 在 Horizon Console 中，選取**設定 > 產品授權及使用**。

2 在**授權設定**面板中，按一下**編輯授權**。

3 輸入授權序號，並按一下**確定**。

4 確認授權到期日。

5 根據產品授權賦予您使用權限的 VMware Horizon 7 版本，確認已啟用或停用桌面平台、應用程式遠端處理和 View Composer 授權。

並非所有版本均提供 VMware Horizon 7 的全部特色與功能。如需比較各版本的功能集，請參閱 http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf。

在 Horizon Console 中將 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 (TLS) 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 Horizon 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 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 Horizon Composer 作業上限的設定。

程序

1 在 Horizon Console 中，導覽至**設定 > 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 (選擇性) 如果已在 VMware Cloud on AWS 上部署 vCenter Server，請選取 **VMware Cloud on AWS**。

如需將 Horizon 7 與 VMware Cloud on AWS 整合的詳細資訊，請參閱《Horizon 7 整合》文件。

9 在 [進階設定] 下，設定 vCenter Server 及 Horizon Composer 作業的並行作業限制。

10 按**下一步**，然後遵循提示來完成精靈。

後續步驟

進行 Horizon Composer 的設定。

- 如果已使用簽署的 TLS 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 [Horizon 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。

進行 Horizon Composer 的設定

若要使用 Horizon Composer，您必須進行設定，允許 Horizon 7 連線至 Horizon Composer 服務。Horizon 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 Horizon Composer 服務和 vCenter Server 執行個體之間必須有一對一對應。Horizon 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 Horizon Composer 服務相關聯。

在初始 Horizon 7 部署後，您可以將 Horizon Composer 服務移轉到新的主機，以支援擴充或變更中的 Horizon 7 部署。您可以在 Horizon Console 中編輯 Horizon Composer 初始設定，但必須執行其他步驟才能確保移轉成功。

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 Horizon 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。請參閱在 Horizon Console 中將 vCenter Server 執行個體新增到 Horizon 7。
- 確認此 Horizon Composer 服務尚未設定為連線至其他 vCenter Server 執行個體。

程序

1 在 Horizon Console 中，導覽至**設定 > 伺服器**。

2 在 **vCenter Server** 索引標籤上，按一下**新增**，並完成 **vCenter Server 設定**頁面上的 vCenter Server 資訊，然後按**下一步**。

3 在 **Horizon Composer 設定**頁面上，如果不使用 Horizon Composer，請選取**不使用 Horizon Composer**。

如果選取**不使用 Horizon Composer**，其他 Horizon 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。

4 如果您使用 Horizon Composer，請選取 Horizon Composer 主機的位置。

選項	說明
Horizon Composer 安裝在與 vCenter Server 相同的主機上。	a 選取 **Horizon Composer 與 vCenter Server 並行安裝**。 b 確認連接埠編號與當初在 vCenter Server 上安裝 Horizon Composer 服務時所指定的連接埠相同。預設連接埠編號是 18443。
Horizon Composer 安裝在本身的另一個主機上。	a 選取**獨立 Horizon Composer 伺服器**。 b 在 Horizon Composer 伺服器位址文字方塊中，輸入 Horizon Composer 主機的完整網域名稱 (FQDN)。 c 輸入 Horizon Composer 使用者的名稱。 例如：**`domain.com\user`** 或 **`user@domain.com`** d 輸入 Horizon Composer 使用者的密碼。 e 確認連接埠編號與當初安裝 Horizon Composer 服務時所指定的連接埠相同。預設連接埠編號是 18443。

5 按**下一步**以顯示 **Horizon Composer 網域**頁面。

後續步驟

設定 Horizon Composer 網域。

- 如果已使用簽署的 TLS 憑證設定 Horizon 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 [Horizon Composer 網域] 頁面。
- 如果已使用預設憑證設定 Horizon Composer 執行個體，則必須先決定是否接受現有憑證的指紋。

設定 Horizon Composer 網域

您必須設定 Horizon Composer 部署連結複製桌面所在的 Active Directory 網域。您可以為 Horizon Composer 設定多個網域。當您首次將 vCenter Server 和 Horizon Composer 設定新增至 Horizon 7 之後，您可以在 Horizon Console 中編輯 vCenter Server 執行個體，以新增更多 Horizon Composer 網域。

必要條件

- Active Directory 管理員必須建立 AD 作業的 Horizon 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 Horizon Composer AD 作業的使用者帳戶。
- 在 Horizon Console 中，確認您已完成**新增 vCenter Server** 精靈中的 **vCenter Server 設定**和 **Horizon Composer 設定**頁面。

程序

1. 在 Horizon Console 中，導覽至**設定 > 伺服器**。
2. 在 **vCenter Server** 索引標籤上，按一下**新增**，並完成 **vCenter Server 設定**頁面上的 vCenter Server 資訊，然後按**下一步**。
3. 在 **Horizon Composer 設定**頁面上，如果您使用 Horizon Composer，請選取 Horizon Composer 主機的位置，然後按**下一步**。

   如需 Horizon Composer 的詳細資訊，請參閱進行 Horizon Composer 的設定。
4. 在 **Horizon Composer 網域**頁面上，按一下**新增**以新增 AD 作業的 Horizon Composer 使用者帳戶資訊。
5. 輸入 Active Directory 網域的網域名稱。

   例如：**domain.com**
6. 輸入網域使用者名稱，包括 Horizon Composer 使用者的網域名稱。

   例如：**domain.com\admin**
7. 輸入帳戶密碼。
8. 按一下**確定**。
9. 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。
10. 按**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 Horizon Storage Accelerator。

在 Horizon Console 中新增即時複製網域管理員

您必須先將即時複製網域管理員新增至 Horizon 7，才能建立即時複製桌面平台集區。

必要條件

- 驗證即時複製網域管理員擁有所需的 Active Directory 網域權限。如需詳細資訊，請參閱《Horizon 7 安裝》文件中的〈建立即時複製作業的使用者帳戶〉。

程序

1. 在 Horizon Console 中，選取**設定 > 即時複製網域帳戶**。
2. 按一下**新增**。
3. 選取即時複製網域管理員的網域。
4. 輸入使用者名稱和密碼。

後續步驟

在 Horizon Console 中，您可以新增或移除即時複製網域管理員，或將即時複製管理員清單匯出至 Microsoft Excel。導覽至**設定 > 即時複製網域帳戶**，然後選取即時複製網域管理員。按一下**編輯**來編輯管理員的網域和登入資訊。按一下**移除**來移除管理員。按一下匯出圖示來將即時複製管理員清單匯出為 Microsoft Excel 檔案。

允許 vSphere 回收連結複製虛擬機器中的磁碟空間

在 vSphere 5.1 版或更新版本中，您可以啟用 Horizon 7 的磁碟空間回收功能。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 版或更新版本中，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 Console 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 Horizon Composer 持續性磁碟。
- 它僅適用於 vSphere 5.1 版或更新版本，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 Console 中，導覽至**設定 > 伺服器**。
2. 在 **vCenter Server** 索引標籤上，按一下**新增**，然後完成**儲存設定**頁面之前的**新增 vCenter Server** 精靈頁面。
3. 在**儲存設定**頁面上，選取**回收虛擬機器磁碟空間**。

   如果是執行 Horizon 7 的全新安裝，則依預設為選取此選項。如果是升級到 Horizon 7 的更新版本，則必須選取**回收虛擬機器磁碟空間**。

後續步驟

在**儲存設定**頁面上，設定 Horizon Storage Accelerator。

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。

為 vCenter Server 設定 Horizon Storage Accelerator

在 vSphere 中，您可以設定 ESXi 主機以快取虛擬機器磁碟資料。這項稱為 Horizon Storage Accelerator 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 Horizon Storage Accelerator 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。

Horizon Storage Accelerator 會透過減少開機風暴期間的 IOPS 數目，降低儲存陣列的需求，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 Console 的**新增 vCenter Server** 精靈中選取 Horizon Storage Accelerator 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 Horizon Storage Accelerator。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 Horizon Storage Accelerator。

依預設會針對桌面平台集區啟用 Horizon Storage Accelerator。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 Horizon Storage Accelerator。

針對 Horizon Storage Accelerator 啟用的集區不支援原生 NFS 快照技術 (VAAI)。

現在 Horizon Storage Accelerator 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 Horizon Storage Accelerator 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 Horizon Composer 權限的主題。

程序

1. 在 Horizon Console 中，導覽至**設定 > 伺服器**。
2. 在 **vCenter Server** 索引標籤上，按一下**新增**，然後完成**儲存設定**頁面之前的**新增 vCenter Server** 精靈頁面。
3. 在**儲存設定**頁面上，選取**啟用 Horizon 儲存加速器**。

   預設為選取此選項。
4. 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。

5 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**。

6 在「儲存設定」頁面上，按**下一步**。

7 檢閱**即將完成**頁面上的設定之後，按一下**提交**。

後續步驟

設定用戶端工作階段和連線的設定。請參閱《Horizon 7 管理》文件中的〈進行用戶端工作階段的設定〉。

若要完成 Horizon 7 中的 Horizon Storage Accelerator 設定，請為桌面平台集區設定 Horizon Storage Accelerator。請參閱《在 Horizon Console 中設定虛擬桌面平台》文件中的〈設定桌面平台集區的 Horizon 儲存加速器〉。

vCenter Server 和 Horizon 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 Horizon Composer 所執行的並行作業數目上限。

您可以在**新增 vCenter Server** 精靈的 **vCenter Server 設定**頁面上的 [進階設定] 面板中設定這些選項。

表 3-1. vCenter Server 和 Horizon 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 Horizon Composer 維護作業上限	決定可在此 Horizon Composer 執行個體管理之連結複製上執行的並行 Horizon 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。

表 3-1. vCenter Server 和 Horizon Composer 的並行作業限制 (續)

設定	說明
並行 Horizon Composer 佈建作業上限	決定可在此 Horizon 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。
並行即時複製引擎作業上限	決定可在此 vCenter Server 執行個體管理之即時複製上執行的並行建立與刪除作業數目上限。 此設定僅適用於即時複製。

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 Horizon Composer 執行個體新增至 Horizon 7 時，您必須確認用於 vCenter Server 和 Horizon 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 Horizon 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 Horizon 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 Horizon 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 Horizon 7 Server 的 TLS 憑證〉。

您可以使用**新增 vCenter Server** 精靈，先在 Horizon Console 中新增 vCenter Server 和 Horizon 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 vCenter Server。

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 Horizon 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。

程序

1 當 Horizon Console 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 Horizon Composer 執行個體設定的憑證指紋。

   a 在 vCenter Server 或 Horizon 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 Horizon 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 Horizon 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 Horizon 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 Console 中，導覽至**設定 > 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**。

對話方塊訊息會警告您 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 Horizon Composer

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

在停用與 Horizon Composer 的連線之前，您必須從 Horizon 7 移除由 Horizon Composer 建立的所有連結複製虛擬機器。如果仍存在任何相關聯的連結複製，則 Horizon 7 會阻止您移除 Horizon Composer。在停用 Horizon 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 Horizon Composer 建立的連結複製桌面平台集區。

a 在 Horizon Console 中，選取**詳細目錄 > 桌面平台**。

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，也會移除相關聯的 Horizon Composer 資料庫項目，以及由 Horizon Composer 建立的複本。

d 對由 Horizon Composer 建立的每個連結複製桌面平台集區重複這些步驟。

2 導覽至**設定 > 伺服器**。

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

4 按一下**編輯**。

5 在 **Horizon Composer** 索引標籤上的 [Horizon Composer 伺服器設定] 下，選取**不使用 Horizon Composer**，然後按一下**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 Horizon Composer 安裝在另一個主機，並將 Horizon 7 重新設定為連線至新的 Horizon Composer 服務，則必須執行某些額外的步驟。如需有關如何在沒有連結複製虛擬機器的情況下移轉 Horizon Composer 的詳細資訊，請參閱《Horizon 7 管理》文件。

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。

在 Horizon Console 中備份 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 Horizon 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 Horizon 連線伺服器及 Horizon Composer 資料。

在 Horizon Console 中設定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。

Horizon Console 中的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 Console 中的狀態更新、是否顯示預先登入與警告訊息、Horizon Console 是否將 Windows Server 視為遠端桌面平台的支援作業系統，以及其他設定。

在 Horizon Console 中，您可以透過導覽至**設定 > 全域設定 > 一般設定**來設定全域設定。

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 3-2. 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 Console 工作階段要持續閒置多久的時間，工作階段才會逾時。 **重要** 若將 Horizon Console 工作階段逾時設為很大的分鐘數，會增加未經授權使用者 Horizon Console 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 Console 工作階段逾時為 30 分鐘。您可以將工作階段逾時設為 10 到 4320 分鐘 (72 小時)。 在工作階段逾時之前，會顯示一則附有 60 秒倒數計時的警告訊息。如果在倒數計時結束之前按一下工作階段，工作階段就會繼續。經過 60 秒後將會顯示一則錯誤訊息，通知您工作階段已逾時，您必須重新登入。
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**。
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。
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 Console 左上角的全域狀態窗格中。Horizon Console 的儀表板頁面也會每隔幾分鐘更新一次。 依預設，此設定未啟用。
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**。

表 3-2. 用戶端工作階段的一般全域設定 (續)

設定	說明
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**。
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。
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 Console 會顯示所有可用的 Windows Server 機器，其中包括 Horizon 7 Server 元件安裝所在的機器。 **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) 及更新版本中使用。
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 Client4.4 或更新版本中隱藏伺服器 URL 資訊。

表 3-2. 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 Client4.4 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 Client5.0 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。

Horizon Console 中用戶端工作階段和連線的全域安全性設定

全域安全性設定會決定在中斷連線、啟用訊息安全模式，以及安全性狀態增強之後是否要重新驗證用戶端。

在 Horizon Console 中，您可以透過導覽至**設定 > 全域設定 > 安全性設定**來設定全域安全性設定。

所有與 Horizon 7 之間的 Horizon Client 連線和 Horizon Console 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。

表 3-3. 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。 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。
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。

Horizon Console 中用戶端工作階段的全域用戶端限制設定

全域用戶端限制設定可將虛擬桌面平台、已發佈的桌面平台和已發佈的應用程式限制為啟動至特定的用戶端和版本。

在 Horizon Console 中，您可以透過導覽至**設定 > 全域設定 > 用戶端限制設定**，並輸入 Horizon Client 的版本以設定全域用戶端限制設定。

Horizon Client 必須為 4.5.0 或更新版本，但 Chrome 版 Horizon Client (必須為 4.8.0 版或更新版本) 除外。如果設定了此功能，則舊版 Horizon Client 將無法連線至遠端桌面平台和已發佈的應用程式。

備註　用戶端限制設定僅防止使用者啟動遠端桌面平台和已發佈的應用程式。此功能不會防止使用者登入 Horizon 7。

表 3-4. 用戶端工作階段的全域用戶端限制設定

設定	說明
Windows 版 Horizon Client	輸入 4.5.0 版或更新版本的 Horizon Client 版本號碼。
Linux 版 Horizon Client	輸入 4.5.0 版或更新版本的 Horizon Client 版本號碼。
Mac 版 Horizon Client	輸入 4.5.0 版或更新版本的 Horizon Client 版本號碼。
iOS 版 Horizon Client	輸入 4.5.0 版或更新版本的 Horizon Client 版本號碼。

表 3-4. 用戶端工作階段的全域用戶端限制設定 (續)

設定	說明
Android 版 Horizon Client	輸入 4.5.0 版或更新版本的 Horizon Client 版本號碼。
UWP 版 Horizon Client	輸入 4.5.0 版或更新版本的 Horizon Client 版本號碼。
Chrome 版 Horizon Client	輸入 4.8.0 版或更新版本的 Horizon Client 版本號碼。
Horizon Client 表示 HTML Access	輸入 4.5.0 版或更新版本的 Horizon Client 版本號碼。
封鎖其他用戶端	當您選取此選項時，除了已加入白名單之 Horizon Client 以外的所有其他用戶端都將遭到封鎖，而無法啟動任何桌面平台或已發佈的應用程式。 不過，如果您想要讓使用者使用其他用戶端類型來啟動桌面平台和已發佈的應用程式，則必須將用戶端類型新增至 `pae-AdditionalClientTypes` LDAP 屬性，以略過該用戶端類型的封鎖設定。 您可以使用 ADSI Edit 公用程式來編輯連線伺服器上的 LDAP 屬性。 在 ADSI Edit 公用程式中，`pae-AdditionalClientTypes` LDAP 屬性可在 `CN=Common`、`OU=Global`、`OU=Properties`、`DC=vdi`、`DC=vmware` 與 `DC=int` 下取得。
訊息	如果使用者嘗試從未加入白名單之用戶端類型或版本啟動桌面平台或已發佈的應用程式，請輸入要顯示的訊息。

在 Horizon Console 中停用或啟用 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 Console 中，選取**設定 > 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 Horizon 連線伺服器執行個體的外部 URL

您可以使用 Horizon Console 來編輯連線伺服器執行個體的外部 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。

程序

1 在 Horizon Console 中，選取**設定 > 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 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://horizon.example.com:443

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

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

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 必須包含用戶端系統可以用來聯繫這個連線伺服器執行個體的 IP 位址和連接埠號碼。

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

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

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

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

6 確認此對話方塊中的所有位址皆允許用戶端系統連線此主機。

7 按一下**確定**儲存變更。

外部 URL 隨即更新。您不必重新啟動連線伺服器，變更就會生效。

在 Horizon Console 中登錄閘道

Horizon Client 會透過您在 Horizon Console 中登錄的閘道或 Unified Access Gateway 應用裝置連線。

您可以在 Horizon Console 中登錄或解除登錄閘道。若要解除登錄閘道，請選取閘道或 Unified Access Gateway 應用裝置，然後按一下**解除登錄**。

程序

1 在 Horizon Console 中，選取**設定 > 伺服器**。

2 在**閘道**索引標籤上，按一下**登錄**。

3 輸入閘道或 Unified Access Gateway 應用裝置的 FQDN。

4 按一下**確定**。

設定智慧卡驗證

4

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 Console 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的連線伺服器組態屬性。

5 在 Horizon Console 中設定智慧卡設定

您可以使用 Horizon Console 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。

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。

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來讓您的變更生效。

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 Console 中設定智慧卡驗證設定。

在 Horizon Console 中設定智慧卡設定

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

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 Console 中，選取**設定 > 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 [Horizon 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 若要為登入 Horizon Console 的管理員設定智慧卡驗證，請從 **Horizon Administrator 驗證**區段中的**管理員的智慧卡驗證**下拉式功能表選取組態選項。

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 Console。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 Console 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。請參閱在 Horizon Console 中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 Console 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 Unified Access Gateway 說明文件。

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 Console 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。

在 Horizon Console 中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 Console 中檢查智慧卡驗證設定。

  a 選取**設定 > 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 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 4-1. 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 4-1. 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

5

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。

- 在 Horizon Console 中啟用雙因素驗證

  您可以修改 Horizon Console 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 SecureID 拒絕存取

  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。

在 Horizon Console 中啟用雙因素驗證

您可以修改 Horizon Console 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。您可以在 Horizon Console 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 Console 中，導覽至**設定 > 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 在**驗證**索引標籤上，**進階驗證**區段的**雙因素驗證**下拉式功能表中，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**下拉式功能表，選取**建立新驗證器**並完成該頁面。

      - 若要讓自訂使用者名稱和密碼標籤顯示在使用者的 RADIUS 驗證對話方塊中，請在**使用者名稱標籤**和**密碼標籤**欄位中輸入自訂標籤。
      - 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 SecureID 拒絕存取

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 Console 中，導覽至**設定 > 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. 在**驗證**索引標籤上，從**進階驗證**區段的**雙因素驗證**下拉式功能表中，選取 **RSA SecureID**。
4. 選取**清除節點密碼**，然後按一下**確定**。
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 Console 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 Console 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 Console 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 Unified Access Gateway 說明文件。

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 應用裝置或需要您產生 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 Console 中，導覽至**設定 > 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
類型	若為 Unified Access Gateway 應用裝置或第三方裝置，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 應用裝置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	(對於靜態驗證器) 您所產生並從 Unified Access Gateway 應用裝置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。

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。

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 Console 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 Console 中設定 SAML 驗證器。

在 Horizon Console 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 Console 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 Console 中，導覽至**設定 > 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。

驗證使用者和群組

6

登入 Horizon Console 之後，您可以設定使用者和群組的驗證來控制對應用程式與桌面平台的存取。

您可以設定遠端存取，以限制使用者和群組從網路外部存取桌面平台。您可以設定組態，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。

本章節討論下列主題：

限制網路外部的遠端桌面平台存取

您可以對來自外部網路具備權利的特定使用者和群組允許存取，同時對其他具備權利的使用者和群組限制存取。所有具備權利的使用者將可從內部網路內存取桌面平台和應用程式。如果您選擇不要對來自外部網路的特定使用者限制存取，則所有具備權利的使用者將可從外部網路存取。

基於安全理由，管理員可能需要限制網路外部的使用者和群組，使其無法存取網路內的遠端桌面平台和應用程式。當受限制的使用者從外部網路存取系統時，會出現訊息，說明使用者未獲授權，無法使用出現的系統。使用者必須位於內部網路內，才能取得對桌面平台和應用程式集區權利的存取權。

設定遠端存取

您可以允許使用者和群組從網路外部存取連線伺服器執行個體，同時限制其他使用者和群組的存取。

必要條件

- 必須在網路外部部署 Unified Access Gateway 應用裝置、安全伺服器或負載平衡器，作為使用者有權使用之連線伺服器執行個體的閘道。如需關於部署 Unified Access Gateway 應用裝置的詳細資訊，請參閱《部署及設定 Unified Access Gateway》文件。
- 取得遠端存取的使用者必須獲授權使用桌面平台或應用程式集區。

程序

1 在 Horizon Console 中，選取**使用者與群組**。

2 按一下**遠端存取**索引標籤。

3 按一下**新增**並選取一或多個搜尋條件，然後按一下**尋找**，根據搜尋條件尋找使用者或群組。

備註 未驗證存取使用者不會顯示在搜尋結果中。

4 若要為使用者或群組或具有未驗證存取的使用者提供遠端存取，請選取使用者或群組，然後按一下**確定**。

5 若要從遠端存取移除使用者或群組，請選取使用者或群組，按一下**刪除**，然後按一下**確定**。

設定未驗證存取

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。

備註 桌面平台集區中發佈的應用程式不支援未驗證存取。

此功能需要設定 Horizon 7 7.1 版環境和 Horizon Client 4.4 版。

如需設定使用者以使用未驗證存取的規則和指導方針的相關資訊，請參閱《Horizon 7 管理》文件。

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

- 管理員僅可對每個 Active Directory 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。
- 如果您選取擁有桌面平台權利的使用者，並讓使用者成為未驗證存取使用者，使用者將無法存取獲授權的桌面平台。

程序

1 在 Horizon Console 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。

4 選取使用者，然後按**下一步**。

5 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**提交**。

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、網域、應用程式權利和工作階段。

後續步驟

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應用程式。請參閱《Horizon 7 管理》文件中的〈啟用使用者未驗證存取〉。

在 Horizon Console 中為使用者啟用未驗證存取

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 Console 中，選取**設定 > 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。如需關於建立伺服器陣列的詳細資訊，請參閱《在 Horizon Console 中設定已發佈的桌面平台和應用程式》文件。
- 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。如需與建立已發佈的應用程式有關的詳細資訊，請參閱《在 Horizon Console 中設定已發佈的桌面平台和應用程式》。

程序

1. 在 Horizon Console 中，選取**使用者與群組**。
2. 在**權利**索引標籤中，從**權利**下拉式功能表選取**新增應用程式權利**。
3. 按一下**新增**，選取一或多個搜尋準則，接著選取**未驗證使用者**核取方塊，然後按一下**尋找**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. 選取集區中的應用程式，然後按一下**提交**。

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。

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。如果您刪除預設使用者，Horizon Console 會顯示內部錯誤訊息，以及成功移除使用者訊息。但是，系統不會從 Horizon Console 刪除預設使用者。

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 Console 中，選取**使用者與群組**。
2. 在**未驗證存取**索引標籤上，選取使用者，然後按一下**刪除**。
3. 按一下**確定**。

後續步驟

移除使用者的應用程式權利。

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。

在 Horizon Console 中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 Console 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。請參閱針對未驗證存取建立使用者。
- 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 Console 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。

在 Horizon Console 中設定角色型委派管理

7

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 Console，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 Console 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 Console 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 Console 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 Console 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。如果角色包含物件特定權限，您可能需要將該角色套用到某個存取群組。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。

在 Horizon Console 中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 Console 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 Console 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。

- 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 7-1. 不同存取群組的不同管理員顯示此類組態的範例。

表 7-1. 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 7-2. 同一個存取群組的不同管理員顯示此類組態的範例。

表 7-2. 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 Console 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 Console 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 Console 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 7-3. [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 Console。

表 7-4. [資料夾] 索引標籤上，MarketingDesktops 的權限

Admin	角色	已繼承
horizon-domain.com\Admin1	詳細目錄管理員	
horizon-domain.com\Admin1	管理員 (唯讀)	是

第一項權限和 表 7-3. [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 7-3. [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 7-3. [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 Console。

表 7-5. 角色權限索引標籤上詳細目錄管理員的權限

Administrator	存取群組
horizon-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 Console 新增與移除管理員使用者與群組。

管理員角色是 Horizon Console 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。

- 在 Horizon Console 中建立管理員

  若要建立管理員，您可以在 Horizon Console 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。

- 在 Horizon Console 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。

在 Horizon Console 中建立管理員

若要建立管理員，您可以在 Horizon Console 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。請參閱在 Horizon Console 中新增自訂角色。
- 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 Console 中，導覽至**設定 > 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。

在 Horizon Console 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 Horizon Console 中，導覽至**設定 > 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 Console 來新增、刪除和檢閱特定管理員使用者和群組、角色和存取群組的權限。

- 在 Horizon Console 中新增權限

  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。

- 在 Horizon Console 中刪除權限

  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。

- 在 Horizon Console 中檢閱權限

  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。

在 Horizon Console 中新增權限

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 Console 中，導覽至**設定 > 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**角色權限**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。

在 Horizon Console 中刪除權限

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 Console 中，導覽至**設定 > 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**移除權限**。

在 Horizon Console 中檢閱權限

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 在 Horizon Console 中，導覽至**設定 > 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**角色權限**索引標籤上選取角色，然後按一下**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 Console 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。

- 在 Horizon Console 中新增存取群組

  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。

- 在 Horizon Console 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。

- 在 Horizon Console 中移除存取群組

  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。

- 在存取群組中檢閱物件

  您可以在 Horizon Console 中檢視特定存取群組中的桌面平台集區、應用程式集區、伺服器陣列或持續性磁碟。

- 檢閱存取群組中的 vCenter 虛擬機器

  您可以在 Horizon Console 中的特定存取群組中檢視 vCenter 虛擬機器。vCenter 虛擬機器從其集區繼承存取群組。

在 Horizon Console 中新增存取群組

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 Console 中，導覽至 [存取群組] 對話方塊。

選項	動作
從桌面平台	■ 選取**詳細目錄 > 桌面平台**。 ■ 從**存取群組**下拉式功能表中，選取**新增存取群組**。
從伺服器陣列	■ 選取**詳細目錄 > 伺服器陣列**。 ■ 從**存取群組**下拉式功能表中，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。

在 Horizon Console 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 Console 中，選取**詳細目錄 > 桌面平台**或**詳細目錄 > 伺服器陣列**。

2 選取集區或伺服器陣列。

3 從**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 Console 會將集區或伺服器陣列移至您所選取的存取群組。

在 Horizon Console 中移除存取群組

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。請參閱在 Horizon Console 中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 Console 中，導覽至**設定 > 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。

在存取群組中檢閱物件

您可以在 Horizon Console 中檢視特定存取群組中的桌面平台集區、應用程式集區、伺服器陣列或持續性磁碟。

程序

1 在 Horizon Console 中，導覽至物件的主頁面。

物件	動作
桌面平台集區	選取**詳細目錄 > 桌面平台**。
應用程式集區	選取**詳細目錄 > 應用程式**。
伺服器陣列	選取**詳細目錄 > 伺服器陣列**。
持續性磁碟	選取**詳細目錄 > 持續性磁碟**。

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 Console 中的特定存取群組中檢視 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 Console 中，導覽至**詳細目錄 > 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 Console 新增、修改與刪除自訂角色。

- 在 Horizon Console 中新增自訂角色

  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 Console 中建立自己的角色。

- 在 Horizon Console 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。

- 在 Horizon Console 中移除自訂角色

  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。

在 Horizon Console 中新增自訂角色

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 Console 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 Console 中，導覽至**設定 > 管理員**。

2 在**角色權限**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。

在 Horizon Console 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 Console 中，導覽至**設定 > 管理員**。

2 在**角色權限**索引標籤上，選取角色。

3 檢視角色中的權限，然後按一下**編輯**。

4 選取或取消選取權限。

5 按一下**確定**儲存變更。

在 Horizon Console 中移除自訂角色

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。請參閱在 Horizon Console 中刪除權限。

程序

1 在 Horizon Console 中，導覽至**設定 > 管理員**。

2 在**角色權限**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 Console 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 7-6. Horizon Console 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，具備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 Console 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。 ■ 可以登入 Horizon Console。 ■ 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。 ■ 可以登入 Horizon Console。	否

表 7-6. Horizon Console 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。 ■ 管理自動伺服器陣列。 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。 具備此角色的管理員無法建立手動伺服器陣列或未受管理的手動集區，也無法對此伺服器陣列或未受管理的手動集區新增或移除 RDS 主機。	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 7-7. 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 Console。 **備註** 從 Horizon 7(7.10 版) 開始，**主控台互動**權限會自動新增至新角色，且不會出現在 Horizon Console 的全域權限清單中。	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。 **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，且不會出現在 Horizon Console 的全域權限清單中。	管理員 管理員 (唯讀)
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
管理 vCenter 組態 (唯讀)	以唯讀方式存取 vCenter Server 組態。	管理員 管理員 (唯讀) 詳細目錄管理員 詳細目錄管理員 (唯讀) 本機管理員 本機管理員 (唯讀)

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 7-8. 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
在自動桌面平台和伺服器陣列上管理維護作業	重新撰寫、重新整理、重新平衡、排程推送映像、排程維護並變更桌面平台集區和伺服器陣列的預設映像。	桌面平台集區, 伺服器陣列
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 Horizon 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 7-9. 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 Console 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 7-10. 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**

表 7-10. 集區管理工作與權限 (續)

工作	所需的權限
新增集區。	**管理伺服器陣列及桌面平台和應用程式集區** **備註** 不適用於新增未受管理的桌面平台集區。管理員也必須具備全域組態及原則管理員 (唯讀) 角色，才能執行此工作。
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** **備註** 不適用於刪除未受管理的桌面平台集區。管理員也必須具備全域組態及原則管理員 (唯讀) 角色，才能執行此工作。
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** **備註** 不適用於新增或移除桌面平台集區中未受管理的虛擬桌面平台。管理員也必須具備全域組態及原則管理員 (唯讀) 角色，才能執行此工作。
重新整理、重新撰寫、重新平衡或變更預設的 Horizon Console 映像。	**管理 Composer 桌面平台集區映像**和**管理 vCenter 組態 (唯讀)**。
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 Console 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 7-11. 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**或**管理伺服器陣列及桌面平台和應用程式集區** **備註** 不適用於從桌面平台集區或伺服器陣列移除未受管理桌面平台或 RDS 主機。管理員也必須具備全域組態及原則管理員 (唯讀) 角色，才能執行此工作。
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**
進入或結束維護模式。	**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 Console 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 Console 的 [持續性磁碟] 頁面中執行這些工作。

表 7-12. 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。	■ 如果磁碟為次要磁碟，則需要**管理持續性磁碟**權限。 ■ 如果磁碟是主要磁碟，則必須要有**管理持續性磁碟**和**管理機器**權限。 ■ 若要中斷連結不同資料存放區上的任何磁碟，管理員也必須具備**管理 vCenter 組態 (唯讀)** 權限。
連結磁碟。	磁碟上的**管理持續性磁碟**，以及機器上的**管理機器**。
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**，以及最後一個桌面平台集區上的**管理伺服器陣列及桌面平台和應用程式集區**或**管理機器**。
從 vCenter 匯入。	磁碟上的**管理持續性磁碟**和**管理 vCenter 組態 (唯讀)**。
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 Console 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 Console 的**使用者與群組**頁面上管理使用者。您需要在 Horizon Console 的**全域管理員檢視**頁面上管理管理員。

表 7-13. 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 Console 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 7-14. 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**
可以登入 Horizon Console。	**主控台互動** **備註** 從 Horizon 7(7.10 版) 開始，**主控台互動**權限會自動新增至新角色，且不會出現在 Horizon Console 的全域權限清單中。

表 7-14. Horizon Help Desk Tool 工作和權限 (續)

工作	所需的權限
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 7-15. 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**
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 Console 中設定原則

8

您可以使用 Horizon Console 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。

本章節討論下列主題：

設定全域原則

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。

程序

1 在 Horizon Console 中，選取**設定 > 全域原則**。

全域原則窗格顯示會影響所有用戶端工作階段、桌面平台集區或使用者的設定。

表 8-1. 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**。

2 按一下**編輯原則**以變更設定。

3 按一下**確定**儲存變更。

維護 Horizon 7 元件

9

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 Console 的自動備份，以備份 Horizon 7 和 Horizon Composer 組態資料。您可以手動匯入所備份的 View LDAP 檔案及 Horizon 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 Horizon Composer 資料

完成連線伺服器的初始組態後，應該排程 Horizon 7 及 Horizon Composer 組態資料的定期備份。您可以透過使用 Horizon Console 來保留您的 Horizon 7 和 Horizon Composer 資料。

Horizon 7 將連線伺服器組態資料儲存於 View LDAP 存放庫中。Horizon Composer 會將連結複製桌面平台的組態資料儲存在 Horizon Composer 資料庫中。

使用 Horizon Console 執行備份時，Horizon 7 將備份 View LDAP 組態資料及 Horizon 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 的指示，請參閱《Horizon 7 管理》文件中的〈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 Console 中的**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 Horizon Console 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 Horizon 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 Horizon 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 Console 中，選取**設定 > 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**立即備份**。
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 Horizon Composer 組態資料。在 Horizon Console 中，您可以設定備份作業的頻率和其他方面的內容。

表 9-1. 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。
備份時間	排程備份的時間。
備份時間位移	排定備份的時間位移。
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 Horizon 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 Horizon Composer 組態資料。

還原 Horizon 連線伺服器與 Horizon 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 Horizon 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 Horizon Composer 組態資料。

在您還原組態資料前，請確認已備份 Horizon Console 中的組態資料。請參閱備份 Horizon 連線伺服器及 Horizon 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 Horizon Composer 資料從 .svi 備份檔案匯入到 Horizon 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 Console 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 Horizon 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. 停止執行 Horizon Composer 所在伺服器上的 VMware Horizon Composer Windows 服務，來停止 Horizon Composer 的所有執行個體。
2. 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。
3. 安裝一個連線伺服器執行個體。
4. 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。
5. 按一下**開始 > 命令提示字元**。
6. 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：

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。

7 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：

8 解除安裝連線伺服器。

僅解除安裝套件 VMware Horizon 連線伺服器。

9 重新安裝連線伺服器。

10 登入 Horizon Console 並驗證組態是否正確。

11 啟動 Horizon Composer 執行個體。

12 重新安裝複寫伺服器執行個體。

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 Horizon 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 Horizon Composer 組態。請參閱還原 Horizon Composer 資料庫。還原 Horizon Composer 組態之後，如果 vCenter Server 中的虛擬機器自 Horizon 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 Horizon Composer 資料庫

您可以將 Horizon Composer 組態的備份檔案匯入至儲存連結複製資訊的 Horizon Composer 資料庫。

您可以使用 SviConfig restoredata 命令在系統失敗後還原 Horizon Composer 資料庫資料，或使用此命令將 Horizon Composer 組態還原至先前的狀態。

重要 只有具豐富經驗的 Horizon Composer 管理員才能使用 SviConfig 公用程式。此公用程式用於解決與 Horizon Composer 服務相關的問題。

必要條件

確認 Horizon 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。

Horizon 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 - Horizon 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 Horizon Composer 備份檔案從連線伺服器電腦，複製到可從安裝有 VMware Horizon Composer 服務的電腦存取的位置。

2 在已安裝 Horizon Composer 的電腦上，停止 VMware Horizon 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 Horizon 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 Composer 服務。

後續步驟

有關 SviConfig restoredata 命令的輸出結果代碼，請參閱 還原 Horizon Console 資料庫的結果代碼。

還原 Horizon Console 資料庫的結果代碼

當您還原 Horizon Console 資料庫時，SviConfig restoredata 命令會顯示結果代碼。

表 9-2. 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。

表 9-2. Restoredata 結果代碼 (續)

代碼	說明
14	其他應用程式正在使用 VMware Horizon Console 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 Horizon Composer 資料庫中的資料

您可以將 Horizon Composer 資料庫中的資料匯出至檔案。

重要　只有豐富經驗的 Horizon 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連線伺服器電腦的 C: 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. 在已安裝 Horizon Composer 的電腦上，停止 VMware Horizon 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 Horizon Composer 應用程式位於同一個位置。

   Horizon-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_Horizon_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，請參閱匯出 Horizon Composer 資料庫的結果代碼。

匯出 Horizon Composer 資料庫的結果代碼

當您匯出 Horizon Composer 資料庫時，`SviConfig exportdata` 命令會顯示結束碼。

表 9-3. Exportdata ExitStatus 代碼

代碼	說明
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 Console 儀表板快速調查 Horizon 7 部署中的 Horizon 7 與 vSphere 元件的狀態。

Horizon Console 會顯示連線伺服器執行個體、事件資料庫、閘道、Horizon 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。即使網域已設定且在運作中，Horizon Console 也會將 Kerberos 網域狀態顯示為不明。

程序

1. 在 Horizon Console 中，導覽至**監視 > 儀表板**。
2. 在**系統健全狀況**窗格中，按一下**檢視**。

   [詳細資料] 窗格會顯示與每個問題相關的名稱、版本和其他資訊。

   - 綠色勾號表示元件沒有問題。
   - 紅色驚嘆號表示元件無法使用或未運作。
   - 黃色驚嘆號表示元件處於警告狀態。
   - 問號表示元件狀態不明。

3 進行選擇以檢視有關問題的詳細資訊。

選項	敘述
元件	顯示服務元件的相關資訊。 按一下**連線伺服器**、**閘道伺服器**、**事件資料庫**、**View Composer Server** 或 **True SSO** 索引標籤，以檢視服務元件的相關資訊並執行疑難排解工作。 選取元件以執行下列工作： ■ 檢視狀態、名稱、版本和其他詳細資料。 ■ 如果您選取連線伺服器，請按一下**檢視服務狀態**索引標籤，以檢視閘道服務的相關資訊。 ■ 如果您選取連線伺服器，請按一下**檢視工作階段詳細資料**索引標籤，以檢視連線伺服器工作階段的相關資訊。
RDS 伺服器陣列	顯示伺服器陣列的相關資訊。按一下伺服器陣列識別碼，以檢視關於伺服器陣列的詳細資訊，包括屬於該伺服器陣列的 RDS 主機。
vSphere	顯示與 vSphere 相關的元件資訊。 按一下**資料存放區**、**ESX 主機**和 **vCenter Server** 索引標籤，以檢視每個元件的相關資訊。
其他元件	按一下**網域**、**SAML 2.0** 和**授權服務**索引標籤，以檢視更多關於每個元件的資訊。本節也適用於 Horizon Composer。 **備註** 如果 SAML 2.0 驗證器因憑證不受信任而出現警告，您可以按一下憑證連結以接受和驗證憑證。
遠端網繭	顯示遠端 Horizon 7 網繭的相關資訊。 **備註** 僅在 Cloud Pod 架構功能啟用時才會顯示此區段。

4 在**工作階段**窗格中，您可以檢視可顯示虛擬桌面平台、已發佈的桌面平台和已發佈的應用程式的作用中、已中斷連線或閒置工作階段數的長條圖。

5 在**工作階段**窗格中，按一下**檢視**以檢視工作階段。

[工作階段] 頁面會顯示工作階段的相關資訊。

6 在**工作負載**窗格中，按一下**檢視**以檢視資料存放區。

您可以選取資料存放區以檢視其他詳細資料，例如資料存放區目前的使用方式。如果資料存放區的可用空間低於臨界值，Horizon Console 會顯示警告。如果有與選取的資料存放區相關的桌面平台集區，您可以在選取資料存放區時檢視桌面平台集區的資訊。**其他資料存放區**欄會顯示跨多個資料存放區的桌面平台集區或伺服器陣列的相關資訊。

監控 Horizon 連線伺服器負載狀態

您可以在 Horizon Console 儀表板中監控連線伺服器的負載。對於每個連線伺服器，您可以檢視耗用的 CPU 與記憶體百分比、顯示通訊協定工作階段的數目、連線伺服器連線工作階段，或可連線至連線伺服器的工作階段數目上限的臨界值。您也可以檢視 RDS 主機已連線的工作階段數目。

程序

1 在 Horizon Console 中，導覽至**監視 > 儀表板**。

2 在**系統健全狀況**窗格中，按一下**檢視**。

在**元件**窗格中的**連線伺服器**索引標籤上，**工作階段**欄會顯示每個連線伺服器的連線伺服器工作階段百分比。**CPU 耗用量**欄會顯示每個連線伺服器所耗用的 CPU 百分比。**記憶體耗用量**欄會顯示每個連線伺服器所耗用的記憶體百分比。

備註 如果連線伺服器未以 HTTP(s) 安全通道、PCoIP 安全閘道和 Blast 安全閘道連線設定安全閘道連線，則 Horizon Console 不會顯示連線伺服器工作階段的百分比，並且會列出連線伺服器工作階段的數目。

3 選取連線伺服器，然後按一下**檢視工作階段詳細資料**，以檢視連線伺服器工作階段、連線伺服器工作階段的數目上限，以及顯示通訊協定工作階段。

備註 如果連線伺服器未設定使用 HTTP(s) 安全通道、PCoIP 安全閘道和 Blast 安全閘道連線的安全閘道連線，則 Horizon Console 不會顯示最大工作階段臨界值，因為並沒有可連線至連線伺服器的工作階段數目臨界值。

4 若要檢視 RDS 主機上的工作階段數目，請在**元件**窗格中按一下 **RDS 伺服器陣列**，然後按一下伺服器陣列識別碼。

[工作階段] 欄會顯示 RDS 主機上的工作階段數目。

監控 Horizon 連線伺服器上的服務

您可以在 Horizon Console 儀表板中監控在連線伺服器上執行的閘道服務元件。閘道服務元件包含以 HTTP(s) 安全通道、PCoIP 閘道和 Blast 安全閘道連線設定的安全閘道連線。

程序

1 在 Horizon Console 中，導覽至**監視 > 儀表板**。

2 在**系統健全狀況**窗格中，按一下**檢視**。

3 選取連線伺服器，然後選取**檢視服務狀態**。

閘道服務狀態對話方塊會顯示閘道服務元件的狀態和使用中的閘道服務元件。

備註 未啟用的服務元件會呈現灰色。

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 9-4. 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。
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。

表 9-4. Horizon 連線伺服器主機服務 (續)

服務名稱	啟動類型	說明
VMware Horizon View 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 9-5. 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。

在 Horizon Console 中變更產品授權金鑰或授權模式

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 Console 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 Console 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 Horizon 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 Console 中，選取**設定 > 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**。

授權設定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**。

授權設定面板將顯示更新的授權資訊。

4 (選擇性) 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。

授權設定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 Horizon 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。

監控授權使用量

在 Horizon Console 中，您可以監控在同時間連線至 Horizon 7 的作用中使用者。**使用設定**面板會顯示目前和最高的歷史使用數字。您可以使用這些數目來追蹤產品授權使用量。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 7 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 7 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 7 會計算已存取 Horizon 7 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，**使用設定**面板上的**目前**資料行會顯示首次設定 Horizon 7 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 7 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，**使用設定**面板上的**最高**資料行會顯示首次設定 Horizon 7 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。

重設授權使用量資料

在 Horizon Console 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。請參閱監控授權使用量。

程序

1. 在 Horizon Console 中，選取**設定 > 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**。

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 Console 中，選取**設定 > 產品授權及使用**。
2. 選取**客戶經驗計畫**索引標籤，然後按一下**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 (選擇性) 選取您的地理位置、垂直業務或組織中的員工數。

5 按一下**確定**。

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 Console 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。請參閱在 Horizon Console 中新增自訂角色。

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)」角色和「記錄收集器管理員」自訂角色。

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。

開始使用 JMP Integrated Workflow

10

自行熟悉高階 JMP Integrated Workflow 概念並完成開始使用 JMP Integrated Workflow 功能所需的工作。

本章節討論下列主題：

- 關於 JMP Integrated Workflow
- 開始使用 JMP 整合工作流程

關於 JMP Integrated Workflow

使用 VMware HorizonJMP (Just-in-Time Management Platform) 整合式工作流程功能，您可以使用單一主控台來定義和管理使用者或使用者群組的桌面平台工作區。

桌面平台工作區是透過定義包含了 VMware Horizon 桌面平台集區、VMware App Volumes AppStack 和 VMware Dynamic Environment Manager 設定相關資訊的 JMP 指派來建立。提交 JMP 指派之後，JMP 自動化引擎會與 Horizon 7、App Volumes 和 Dynamic Environment Manager 系統通訊，以賦予使用者桌面平台的存取權。

您可以使用 Horizon Console 中的**指派 (JMP)** 索引標籤來管理現有的 JMP 指派。您也可以使用各自的 JMP 元件主控台來修改每個元件指派。例如，對 JMP 指派中所定義桌面平台集區的變更也可以透過 Horizon Console 選取**詳細目錄 > 桌面平台**來修改。

在 Horizon Console 中開啟 JMP 指派時，系統會對 JMP 指派每個元件的目前狀態進行驗證，以確保其為預期的狀態。發現差異時，受影響的區域會在主控台中反白顯示，而您可以接受目前的狀態，或修改指派來達到所需的狀態，並重新授權使用者。

在您安裝和設定 VMware HorizonJMP Server 後，即可於 Horizon Console 中使用 JMP Integrated Workflow 功能。如需詳細資訊，請參閱開始使用 JMP 整合工作流程和《VMware Horizon JMP Server 安裝和設定指南》。

備註 JMP Integrated Workflow 功能不支援 AWS 上的 VMware Cloud®，因為 App Volumes 不支援 VMware Cloud

開始使用 JMP 整合工作流程

若要開始使用 JMP Integrated Workflow 功能，您必須安裝和設定 JMP Server，並進行 JMP 設定。

必要條件

針對您計劃要安裝的所有技術元件檢閱必要條件和系統需求。

程序

1 如果必要，請在 Active Directory 中設定所需的管理員使用者和群組。

請參閱《Horizon 7 安裝》文件中的〈準備 Active Directory〉。進行 JMP 設定時，需要 Active Directory 資訊。

2 設定 Microsoft SQL Server，並確保您計劃在 JMP Server 安裝程序期間使用的登入認證已建立。如需詳細資訊，請參閱《VMware Horizon JMP Server 安裝和設定指南》文件中的〈JMP Server 的資料庫需求〉。

3 安裝並設定 VMware Horizon 7 (7.5 版) 或更新版本。

請參閱《Horizon 7 安裝》文件。

4 (選用) 安裝和設定可提供即時應用程式交付功能的 VMware App Volumes 2.14 或更新版本。

如需詳細資料，請參閱《VMware App Volumes 安裝指南》文件。

5 (選用) 若要提供內容原則管理，請安裝並設定 VMware Dynamic Environment Manager 9.2.1 或更新版本。

請參閱《安裝和設定 VMware Dynamic Environment Manager》文件。

6 取得 JMP Server 與您組織網路內其他伺服器安全地通訊所必須使用之 CA 簽署的 SSL 憑證。

7 安裝 JMP Server 並設定 SSL 憑證，讓 JMP Server 與 JMP Integrated Workflow 功能所需的其他伺服器進行通訊。

如需詳細資訊，請參閱《VMware Horizon JMP Server 安裝和設定指南》。

8 第一次進行 JMP 設定。如需詳細資料，請參閱第一次進行 JMP 設定。

後續步驟

成功完成前述的工作後，您現在可以建立 JMP 指派。如需相關資訊，請參閱建立 JMP 指派。

管理 JMP 設定

11

安裝 JMP Server 之後，您必須使用必要的認證進行 JMP 設定之後，才能建立任何 JMP 指派並可以開始使用 JMP Integrated Workflow 功能。您可以編輯初始 JMP 設定，並且在適用時新增設定資訊。

本章節討論下列主題：

第一次進行 JMP 設定

在可以建立任何 JMP 指派之前，您必須使用 Horizon Console 進行 JMP 設定。您必須提供用來為使用者或使用者群組指派桌面平台工作區的 Active Directory 網域認證。您可以選擇性地包含認證資訊，以在建立 JMP 指派時使用 App Volumes AppStack 和 Dynamic Environment Manager 組態共用。

必要條件

- 確認已成功安裝 VMware HorizonJMP Server，並且您擁有其 URL。如需詳細資訊，請參閱《VMware Horizon JMP Server 安裝和設定指南》。
- 取得您計劃搭配 JMP Server 使用之 Horizon 7 (7.5 版) 或更新版本的管理員帳戶認證。
- 取得必須與 JMP Server 搭配使用的 Active Directory 認證。
- 如果您要指派應用程式至 JMP 指派，請確定您擁有要使用之 VMware App Volumes Manager 執行個體的 URL 和管理員帳戶認證。如果負載平衡器管理您計劃使用的 App Volumes Manager 執行個體，請取得負載平衡器的 URL 並在設定 App Volumes Manager 資訊時使用。
- 如果您選擇使用 VMware Dynamic Environment Manager 組態共用，請取得其 UNC 路徑，以及存取它所需的管理員帳戶認證。

程序

1. 在 Horizon Console 中，按一下 **JMP 組態**。
2. 輸入 JMP Server 資訊。
   a. 在 **JMP Server** 索引標籤中，按一下**新增 JMP Server**。
   b. 以格式 `https://jmp.yourcompany.com` 輸入 JMP Server URL。
   c. 按一下**儲存**。

JMP Server URL 即會進行驗證。如果您收到 `JMP Server 無法連線`訊息，請確認您已輸入正確的 URL、已正確設定 JMP Server，且 JMP Server 可連線。

3 輸入您計劃搭配 JMP Server 使用之 Horizon 7 連線伺服器 (7.5 版) 或更新版本的帳戶資訊。

a 按一下 **Horizon 7** 索引標籤。

b 如果沒有自動填入，請輸入**連線伺服器 URL** 的值。此 URL 與 Horizon Console 所連線 Horizon 7 連線伺服器的 URL 相同。

c 輸入 Horizon 7 服務帳戶使用者名稱和密碼。

d 在**服務帳戶網域**文字方塊中，輸入有效名稱以便與您要建立的 JMP 指派搭配使用，然後按 **Enter**。

e 按一下**儲存**。

4 輸入您要搭配 JMP 指派使用的 Active Directory 資訊。

a 按一下 **Active Directory** 索引標籤。

b 按一下**新增**。

c 在 **NETBIOS 名稱**文字方塊中，從可用的 NetBIOS 網域名稱清單中選取。

[DNS 網域名稱] 和 [內容] 文字方塊會更新為預設值。

d 確認 **DNS 網域名稱**文字方塊中新增的預設值是要使用的正確值。選擇性地輸入另一個 Active Directory 的完整網域名稱。例如，`mycompany.com`。

e 在**通訊協定**區段中，選取您 Active Directory 所使用的通訊協定。

f 在**繫結使用者名稱**和**繫結密碼**文字方塊中，輸入繫結辨別名稱 (DN) 使用者帳戶的認證。例如，`administrator`。

g 如果您想要使用與預設值不同的值，請修改**內容**文字方塊中的值。

該值會用作 Active Directory 資料搜尋的根目錄。

h (選用) 按一下**進階屬性**，並修改預設的連接埠號碼值。

預設的 [連接埠] 值會根據您先前選取的通訊協定而定。您可以修改 [連接埠] 值，或將文字方塊保留空白。

i 在**網域控制站**文字方塊中，選擇性地輸入要用於處理 Active Directory 流量的一或多個主機名稱或 IP 位址。

例如，`adserver.mycompany.com, 10.111.XXX.XXX`。如果您將文字方塊保留空白，則會使用 **DNS 網域名稱**文字方塊中的值。

j 按一下**儲存**。

5 如果您計劃在建立 JMP 指派時使用 App Volumes AppStack，請設定您計劃使用的 App Volumes Manager。

a 按一下 **App Volumes** 索引標籤。

b 按一下**新增**。

c 在**名稱**文字方塊中，輸入要指派給 App Volumes 執行個體的名稱。如果將文字方塊保留空白，則會使用您在 **App Volumes 伺服器 URL** 文字方塊中輸入的值。

d 輸入您想要 JMP Server 網繭與其建立關聯之 App Volumes Manager 的有效 URL。

重要 如果您計劃使用的 App Volumes Manager 是由負載平衡器管理，請輸入該負載平衡器的 URL。

e 輸入您的 JMP Server 可以用來存取 App Volumes Manager 的 App Volumes Manager 或負載平衡器管理員帳戶認證。

f 輸入要用於 JMP 指派的 App Volumes Manager 服務帳戶網域名稱。

g (選用) 如果您要登錄多個 App Volumes Manager，請使用切換按鈕來指出您要新增的 App Volumes Manager 是否為建立 JMP 指派時要使用的預設伺服器。您可以變更建立 JMP 指派時您想要使用的執行個體。

h 按一下**儲存**。

6 如果您計劃在建立 JMP 指派時使用 Dynamic Environment Manager 組態共用，請將該資訊新增至 JMP 設定。

a 按一下 **UEM** 索引標籤。

b 按一下**新增**。

c 以 `\\fileserver-name\UEM-configuration-share-pathname` 格式在**檔案共用 UNC 路徑**文字方塊中輸入值。例如，`\\FileServer\UEMConfig`。

重要 請勿在您輸入的檔案共用 UNC 路徑中包含 `General`。

d 輸入要用於連線至 Dynamic Environment Manager 組態共用的 Dynamic Environment Manager 管理員帳戶認證。

e 從 **Active Directory** 的清單中，選取要與 Dynamic Environment Manager 組態共用搭配使用的網域名稱。

備註 Active Directory 僅能與一個 Dynamic Environment Manager 組態共用建立關聯。

f 按一下**儲存**。

後續步驟

成功設定初始 JMP 設定之後，您現在可以建立 JMP 指派。如需詳細資訊，請參閱建立 JMP 指派。

管理 JMP 設定

您可以使用 Horizon Console 來修改、新增或刪除 JMP 設定的資訊。

- 備妥修改特定 JMP 設定所需的資訊。
- 若要修改 JMP 設定，請確定您擁有適當的管理權限。

編輯 JMP Server 設定

您可以使用 Horizon Console 對現有 JMP Server 設定進行變更。

必要條件

- 備妥修改特定 JMP Server 設定所需的資訊。
- 確保您有適當的管理權限可登入 Horizon Console 並修改 JMP Server 設定

程序

1 在 Horizon Console 中，選取 **JMP 組態**。

2 在 [JMP 設定] 窗格中，按一下 **JMP Server** 索引標籤。

3 按一下**編輯**。

4 輸入新的 **JMP Server URL**。

5 按一下**儲存**。

隨即會驗證新 JMP Server URL，如果無效，則會出現錯誤訊息。

編輯 Horizon 7 認證

使用 Horizon Console 來變更現有的 Horizon 7 連線伺服器認證。

程序

1 在 Horizon Console 中，按一下 **JMP 組態**。

2 按一下 **Horizon 7** 索引標籤。

3 按一下**編輯認證**。

4 如有必要，請在**服務帳戶使用者名稱**中輸入新的使用者名稱。

5 如有必要，請在**服務帳戶密碼**中輸入新密碼。

6 如有必要，請變更**服務帳戶網域**中的值。

7 按一下**儲存**。

編輯 Horizon 連線伺服器 URL

如果您想要將現有的 JMP 指派與不同的 Horizon Connection Server 建立關聯，則必須修改已向與那些 JMP 指派相關聯之 JMP Server 設定登錄的 Horizon Connection Server URL。

Horizon Console 中沒有使用者介面可讓您修改 Horizon Connection Server 資訊。您必須使用 SQL Server Management Studio 來修改 JMP 設定中的現有 Horizon Connection Server 主機 URL。

必要條件

- 確保您有適當的系統管理員權限可登入 SQL Server Management Studio 工作階段，且能存取為 JMP Server 建立的 SQL Server 資料庫。

- 備份 SQL Server 資料庫後再繼續進行資料庫修改。

程序

1. 如果目前已登入 Horizon Console 工作階段，請登出。
2. 以 sysadmin (SA) 身分或使用具有 SA 權限的使用者帳戶登入 SQL Server Management Studio 工作階段。
3. 確認您計劃使用的取代 Horizon Connection Server 主機 URL 尚未向另一個 JMP Server 執行個體登錄。

   例如，如果取代 Horizon Connection Server 主機的 URL 為 `new-horizon-host.com`，請使用下列 SQL 陳述式來確認該 URL 尚未登錄。

   ```
   SELECT * from  xms_services
   WHERE xms_services.host = "new-horizon-host.com"
   ```

4. 如果先前的 SQL 陳述式未傳回任何結果，請繼續進行下一個步驟。否則，請使用下列陳述式來刪除現有 Horizon Connection Server 主機的資訊。

   ```
   DELETE from xms_services
   WHERE xms_services.host = "new-horizon-host.com"
   ```

5. 使用下列陳述式更新現有的 JMP Server 設定，其中 `new-horizon-server-host.com` 為取代 Horizon Connection Server 主機的 URL，而 `old-horizon-host.com` 為目前已登錄 Horizon Connection Server 主機的 URL。

   ```
   UPDATE xms_service_endpoints
   SET host = 'new-horizon-host.com', is_available = 1
   WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
       AND host = 'old-horizon-host.com')
   AND host = 'old-horizon-host.com'

   UPDATE xms_services
   SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
   WHERE service_type = 'horizon'
   AND host = 'old-horizon-host.com'
   ```

6. 使用新的 Horizon Connection Server URL 登入 Horizon Console，並確認新 Horizon Connection Server 主機現在與先前與舊 Horizon Connection Server 主機相關聯的現有 JMP 指派相關聯。

新增 Active Directory 網域

在設定初始的 Active Directory 網域之後，如果您需要新增另一個，請使用 Horizon Console。

程序

1. 在 Horizon Console 中，按一下 **JMP 組態**。
2. 按一下 **Active Directory** 索引標籤，然後按一下**新增**。

3 在 **NETBIOS 名稱**文字方塊中，從可用的 NetBIOS 網域名稱清單中選取。

[DNS 網域名稱] 和 [內容] 文字方塊會更新為預設值。

4 在 **DNS 網域名稱**文字欄位中，確認更新 NETBIOS 名稱之後新增的預設值。選擇性地輸入另一個 Active Directory 的完整網域名稱。例如，`mycompany.com`。

5 在**通訊協定**區段中，選取您 Active Directory 所使用的通訊協定。

6 在**繫結使用者名稱**和**繫結密碼**文字欄位中，輸入繫結辨別名稱 (DN) 使用者帳戶 (例如管理員) 的認證。

7 如果您想要使用與預設值不同的值，請修改**內容**文字欄位中的值。

8 (選用) 按一下**進階屬性**，並修改預設的連接埠號碼值。

預設的 [連接埠] 值會根據您先前選取的通訊協定而定。您可以修改 [連接埠] 值，或將文字欄位保留空白。

9 在**網域控制站**文字欄位中，選擇性地輸入要用於處理 Active Directory 流量的一或多個主機名稱或 IP 位址。

10 按一下**儲存**。

Active Directory 資料表中會出現已新增 Active Directory 網域的相關資訊。

編輯 Active Directory 網域資訊

如果在您最初進行 JMP 設定之後某些資訊已變更，請使用 Horizon Console 來修改 Active Directory 網域設定資訊。

程序

1 在 Horizon Console 中，按一下 **JMP 組態**。

2 按一下 **Active Directory** 索引標籤。

3 在 Active Directory 網域的資料表中選取一個資料列，然後按一下**編輯**。

4 修改必須更新的 Active Directory 資訊。

5 按一下**儲存**。

刪除 Active Directory 網域資訊

如果您必須刪除現有的 Active Directory (AD) 網域設定資訊，請使用 Horizon Console。

只有在某個 Active Directory 網域未由任何現有 JMP 指派使用時，您才可以從 JMP 設定中刪除該已登錄網域的相關資訊。

程序

1 在 Horizon Console 中，按一下 **JMP 組態**。

2 按一下 **Active Directory** 索引標籤。

3 選取您想要從 JMP 設定刪除之 Active Directory 網域的資料表資料列。

4 在顯示的刪除確認對話方塊中閱讀訊息，並按一下**刪除**以確認您要刪除此 Active Directory 網域資訊。

如果沒有使用 Active Directory 網域的任何 JMP 指派，則會將它移除。

如果任何 JMP 指派正在使用 Active Directory 網域，則會出現警告對話方塊。警告訊息包含正在使用 Active Directory 網域之 JMP 指派的清單。僅在從 JMP 指派中移除網域或刪除使用該網域的那些 JMP 指派後，您才可以刪除網域資訊。

新增 App Volumes 資訊

使用 Horizon Console 來針對任何其他 App Volumes Manager 新增資訊，以便建立 JMP 指派時可以使用。

程序

1 在 Horizon Console 中，按一下 **JMP 組態**。

2 按一下 **App Volumes** 索引標籤，然後按一下**新增**。

新增 App Volumes 執行個體對話方塊隨即顯示。

3 在**名稱**文字方塊中，輸入要指派給 App Volumes 執行個體的唯一名稱。如果將文字方塊保留空白，則會使用您在 **App Volumes 伺服器 URL** 文字方塊中輸入的值。

4 在 **App Volumes 伺服器 URL** 文字方塊中，輸入您想要與 JMP Server 建立關聯之 App Volumes Manager 的有效 URL。如果您要新增的 App Volumes Manager 是由負載平衡器管理，請輸入該負載平衡器的 URL。

> 備註 如果您已新增的 App Volumes Manager 已連線至不同的 SQL 資料庫，您所新增 App Volumes Manager 的相關資訊會顯示在 App Volumes 索引標籤中。如果 App Volumes Manager 已連線至相同的 SQL 資料庫，則在 App Volumes 索引標籤上，僅會顯示先前已登錄 App Volumes Manager 的相關資訊。

5 輸入您 JMP Server 可以用來存取 App Volumes Manager 的 App Volumes 管理員使用者名稱和密碼。

6 輸入用於 JMP 指派的 App Volumes 服務帳戶網域名稱。

7 若要讓您目前新增的 App Volumes Manager 成為建立 JMP 指派時所使用的預設 App Volumes Manager 伺服器，請按一下切換按鈕。您可以變更建立 JMP 指派時所要使用的伺服器。

切換按鈕會變更為藍色的**是**標籤。

8 按一下**儲存**。

編輯 App Volumes 執行個體資訊

如果您必須修改目前由 JMP 指派所使用 App Volumes 執行個體的現有相關資訊，請使用 Horizon Console 來修改資訊。

程序

1 在 Horizon Console 中，按一下 **JMP 組態**。

2 按一下 **App Volumes** 索引標籤，然後選取您想要修改之 App Volumes 執行個體的資料表資料列。

3 按一下**編輯**。

新增 App Volumes 執行個體對話方塊隨即顯示。

4 修改必須更新的 App Volumes 執行個體資訊。

5 按一下**儲存**。

刪除 App Volumes 執行個體資訊

如果您必須刪除關於 App Volumes 執行個體的現有設定資訊，請使用 Horizon Console。

僅在某個執行個體未由任何 JMP 指派使用時，您才可以從 JMP 設定中刪除該已登錄 App Volumes 執行個體的相關資訊。

程序

1 在 Horizon Console 中，按一下 **JMP 組態**。

2 按一下 **App Volumes** 索引標籤。

3 選取您想要從 JMP 設定刪除之 App Volumes 執行個體資訊的資料列。

4 按一下**刪除**以確認您要刪除此 App Volumes 執行個體資訊。

如果沒有使用 App Volumes 執行個體的任何 JMP 指派，則會將它移除。

如果任何 JMP 指派正在使用 App Volumes 執行個體，則會出現警告對話方塊。警告訊息包含正在使用 App Volumes 執行個體之 JMP 指派的清單。僅在從 JMP 指派中移除網域或刪除使用網域的那些 JMP 指派後，您才可以刪除 App Volumes 執行個體資訊。

新增 Dynamic Environment Manager 組態共用資訊

如果設定初始的 Dynamic Environment Manager 組態共用之後，您必須新增另一個，請使用 Horizon Console。

每個 AD 網域您僅能新增一個 Dynamic Environment Manager 組態共用。因此，您所要新增組態共用的 IP 或 DNS 位址，不能與您 JMP Server 設定中已包含的組態共用相同。

程序

1 在 Horizon Console 中，按一下 **JMP 組態**。

2 按一下 **UEM** 索引標籤，然後按一下**新增**。

新增 UEM 檔案共用對話方塊隨即顯示。

3 以 `\\server-name\UEM-configuration-share-pathname` 格式在**檔案共用 UNC 路徑**文字方塊中輸入值。

例如，如果組態共用位置為 `\\<IP-address>\uemshare\config\general\FlexRepository\..`，您需要在**檔案共用 UNC 路徑**文字方塊中輸入的路徑為 **`\\<IP-address>\uemshare\config`**。

4 輸入連線至 Dynamic Environment Manager 組態檔案共用時必須使用的 Dynamic Environment Manager 使用者名稱和密碼。

5 從 **Active Directory** 清單中，選取要與 Dynamic Environment Manager 組態檔案共用搭配使用的網域名稱。

> 備註 Active Directory 僅能與一個 Dynamic Environment Manager 組態檔案共用建立關聯。

6 按一下**儲存**。

Dynamic Environment Manager 組態檔案共用的相關資訊隨即新增至 JMP 設定，並且一個新資料列會新增至 **UEM** 索引標籤中的表格。

編輯 Dynamic Environment Manager 組態檔案共用資訊

如果您必須修改已由 JMP 指派所使用有關 Dynamic Environment Manager 組態檔案共用的現有資訊，請使用 Horizon Console。

程序

1 在 Horizon Console 中，按一下 **JMP 組態**。

2 按一下 **UEM** 索引標籤，然後從現有資訊的資料表中，選取您想要修改之 Dynamic Environment Manager 組態檔案共用的資料列。

3 按一下**編輯**。

編輯 UEM 檔案共用對話方塊隨即出現。

4 修改必須更新的 Dynamic Environment Manager 組態檔案共用資訊。

5 按一下**儲存**。

刪除 Dynamic Environment Manager 組態共用資訊

如果您必須刪除關於 Dynamic Environment Manager 組態共用的現有設定資訊，請使用 Horizon Console。

僅在某個組態共用未由任何 JMP 指派使用時，您才可以從 JMP 設定中刪除該已登錄 Dynamic Environment Manager 組態共用的相關資訊。

程序

1 在 Horizon Console 中，按一下 **JMP 組態**。

2 按一下 **UEM** 索引標籤。

3 選取您想要從 JMP 設定刪除之 Dynamic Environment Manager 組態共用資訊的資料列。

4 按一下**刪除**以確認您要刪除此 Dynamic Environment Manager 組態共用資訊。

如果沒有使用 Dynamic Environment Manager 組態共用的任何 JMP 指派，則會將它移除。

如果任何 JMP 指派正在使用 Dynamic Environment Manager 組態共用，則會出現警告對話方塊。警告訊息包含正在使用 Dynamic Environment Manager 組態共用之 JMP 指派的清單。僅在從 JMP 指派中移除網域或刪除使用網域的那些 JMP 指派後，您才可以刪除 Dynamic Environment Manager 組態共用資訊。

管理 JMP 指派

12

安裝 JMP Server 並進行 JMP 設定後，您可以開始使用 JMP Integrated Workflow 功能來建立、修改、複製或刪除 JMP 指派。

您必須先安裝 JMP Server，並進行 JMP 設定之後才能開始建立 JMP 指派。如需詳細資訊，請參閱《VMware Horizon JMP Server 安裝和設定指南》和第一次進行 JMP 設定。

在建立、編輯、複製或刪除 JMP 指派之前，請確保已滿足下列必要條件。

- 確認向 JMP 設定登錄的 Horizon 7 執行個體已啟動且正在執行。
- 確保使用 JMP 設定至少登錄一個 Active Directory 網域。
- 確認您向 JMP 設定登錄的 App Volumes 執行個體已啟動且正在執行。
- 確認在 JMP 設定中定義的 Dynamic Environment Manager 組態共用已啟動且正在執行。

備註 不支援全域權利。

當您嘗試建立、編輯、複製或刪除 JMP 指派時，您可能會收到訊息，指出嘗試的動作並未成功完成。例如，嘗試連線至其中一個基礎 JMP 技術元件時可能會遇到一些問題，且指派驗證無法成功完成。在 [JMP 指派] 摘要畫面上，您可以透過選取以下選項之一來嘗試修正問題。

- 按一下**編輯**以手動更正問題。
- 按一下**修復**可讓 JMP Server 嘗試修正在目前的 JMP 指派上發現的問題。
- 按一下**強制刪除** 以完全移除 JMP 指派。

本章節討論下列主題：

建立 JMP 指派

您可以使用 Horizon Console 建立 JMP 指派，並使用該指派來為使用者或使用者群組建立桌面平台工作區。

您可以選取 Horizon 桌面平台集區、App Volumes AppStack 和 User Environment Manager 設定來定義 JMP 指派。

必要條件

確保已符合第 12 章 管理 JMP 指派中列出的必要條件。

程序

1 在 Horizon Console 中，按一下**指派 (JMP)**。

2 按一下**新增**。

3 在 [新增指派] 精靈的**使用者**索引標籤中，於 Active Directory 下拉式清單旁輸入一些字元，然後選取要在新 JMP 指派中包含的使用者或使用者群組。

您的選取項目會在 [選取的使用者/群組] 區段中新增。

4 按**下一步**。

5 在**桌面平台**索引標籤中，選取您要包含在 JMP 指派的桌面平台集區，然後按**下一步**。

6 在**應用程式**索引標籤中，按一下您想要包含在 JMP 指派中應用程式名稱旁的核取方塊。完成選擇之後，按**下一步**。

7 在**使用者環境**索引標籤中，決定是否要以任何可用的使用者環境設定來設定 JMP 指派。

- 將**停用 UEM 設定?** 設為**否**時，按一下**略過**表示 User Environment Manager 指派檔案不會儲存在 User Environment Manager 組態共用中。系統會使用您目前所建立的 JMP 指派，將所有 User Environment Manager 設定套用到為使用者建立的虛擬桌面平台工作區。
- 將**停用 UEM 設定?** 設定為**否**時，請選取要套用至所要建立 JMP 指派的使用者環境設定。按**下一步**會以選取的使用者環境設定來建立 User Environment Manager 指派檔案。系統會使用您目前所建立的 JMP 指派，將選取的設定套用到為使用者建立的虛擬桌面平台工作區。
- 將**停用 UEM 設定?** 設定為**是**時，系統會從檢視中移除可用使用者環境設定的清單。當您按**下一步**時，系統會將空白指派檔案寫入 User Environment Manager 組態共用。停用 User Environment Manager 設定可確保系統不會使用您目前所建立的 JMP 指派，將使用者環境設定套用到為使用者建立的虛擬桌面平台工作區。

8 在**定義**索引標籤中，接受 JMP 指派的預設名稱，或將名稱取代為其他名稱，並選擇性地新增說明。

9 在 **AppStack 連結**下拉式清單中，選取將 AppStack 連結至 JMP 指派的時機，然後按**下一步**。

10 在**摘要**索引標籤中，檢閱新指派的詳細資料。如果可接受，請按一下**提交**。如果需要進行變更，按**上一步**可進行調整。

新的 JMP 指派會排入佇列以儲存至 JMP 資料庫，且會新增至 [JMP 指派] 窗格中指派的清單。在 JMP 指派成功新增至 JMP 資料庫後，狀態會從「擱置中」狀態變更。JMP 指派將成為可從 JMP 指派清單選取，以便您可以編輯、複製或將其刪除。

您也可以使用下列資訊來確認針對新 JMP 指派建立的指派或權利。

- 若要確認針對 JMP 指派所建立 Horizon 桌面平台集區的相關資訊，請使用 Horizon Console。選取**詳細目錄 > 桌面平台**，並找出由 JMP Server 建立的桌面平台集區。
- 若要檢視 JMP Server 針對新 JMP 指派所建立的 AppStack 資訊，請使用 App Volumes Manager 主控台。選取**磁碟區 > Appstack**，並找出由 JMP Server 建立的 Appstack。
- 若要確認您針對 JMP 指派進行的使用者環境設定，請使用 Dynamic Environment Manager 管理主控台，然後按一下**使用者環境**索引標籤。在左側窗格中，選取 JMP 指派使用的使用者環境設定，然後從產生的對話方塊中按一下**指派**索引標籤，以檢視該使用者環境設定的 JMP 指派資訊。

編輯 JMP 指派

由於用來定義指派的元件變更，您可能需要修改現有的 JMP 指派。您可以使用 Horizon Console 來對 JMP 指派進行必要的變更。

必要條件

- 確保已符合第 12 章 管理 JMP 指派中列出的必要條件。
- 您計劃編輯的 JMP 指派不能處於「擱置中」狀態。

程序

1. 在 Horizon Console 中，按一下**指派 (JMP)**。
2. 透過按一下核取方塊或按一下清單中的 JMP 指派名稱來選取您要編輯的 JMP 指派。
3. 按一下**編輯**。
4. 在 [編輯指派] 精靈中，修改目前的設定。

   如果您要在編輯程序期間的任何時間點停止，請按一下**取消**。

   a 如果您要移除任何目前選取的使用者或群組，請按一下刪除圖示 (**X**)。

   b 按**下一步**。

   c 在**桌面平台**索引標籤中，選取您要包含在 JMP 指派的桌面平台集區。按**下一步**。

   d 在**應用程式**索引標籤中，選取要新增至 JMP 指派的可用應用程式，或取消選取先前選取的應用程式。按**下一步**。

e 在**使用者環境**索引標籤中，決定是否要以任何可用的使用者環境設定來設定 JMP 指派。

- 將**停用 UEM 設定?**設為**否**時，按一下**略過**表示 User Environment Manager 指派檔案不會儲存在 User Environment Manager 組態共用中。系統會使用您目前所編輯的 JMP 指派，將所有 User Environment Manager 設定套用到為使用者建立的虛擬桌面平台工作區。
- 將**停用 UEM 設定?**設定為**否**時，請選取要套用至所要建立 JMP 指派的使用者環境設定。按**下一步**會以選取的使用者環境設定來建立 User Environment Manager 指派檔案。系統會使用您目前所編輯的 JMP 指派，將選取的設定套用到為使用者建立的虛擬桌面平台工作區。
- 將**停用 UEM 設定?**設定為**是**時，系統會從檢視中移除可用使用者環境設定的清單。當您按**下一步**時，系統會將空白指派檔案寫入 User Environment Manager 組態共用。停用 User Environment Manager 設定可確保系統不會使用您目前所編輯的 JMP 指派，將使用者環境設定套用到為使用者建立的虛擬桌面平台工作區。

f 在**定義**索引標籤中，如果適用，請修改**名稱**、**說明**中目前的值，或將 AppStack 連結至 JMP 指派的時機。

g 按**下一步**。

h 檢閱您所做變更的摘要，然後按一下**提交**以儲存修改。

如果成功，則會儲存變更。如果發生任何問題，則會提供其他資訊，並顯示您可以採取的任何可能動作。

複製 JMP 指派

您可以透過複製與您要建立之 JMP 指派類似的現有指派，更快速地建立 JMP 指派。

必要條件

- 確保已符合第 12 章 管理 JMP 指派中列出的必要條件。
- 您計劃複製的 JMP 指派不能處於「擱置中」或「錯誤」狀態。

程序

1 從 Horizon Console 中，選取**指派 (JMP)**。

2 選取您想要複製的 JMP 指派，然後按一下**複製**。

3 在新增指派精靈中，視需要修改複製的 JMP 指派。

a 選取新使用者或群組，或移除任何目前所選的使用者或群組。按**下一步**。

b 在 [桌面平台] 窗格中，選取新的桌面平台集區或移除已包含在已複製 JMP 指派中的任何桌面平台集區。按**下一步**。

c 選取要包含在新 JMP 指派中的其他應用程式，並取消選取目前選取的應用程式。按**下一步**。

d 在 [使用者環境] 窗格中，選取您要套用至新 JMP 指派的 User Environment Manager 設定。按**下一步**。

e 在定義名稱中，視需要取代建立的預設名稱。新增說明，並指定您想要將 AppStack 附加至新 JMP 指派的時機。

f 按**下一步**，然後檢閱新 JMP 指派的詳細資料摘要。

g 如果資訊令人滿意，請按一下**提交**。否則，請按**上一步**以進行任何修正。

新的 JMP 指派即會進行驗證，這可能需要一些時間。成功驗證後，新建立的 JMP 指派便會新增至 [JMP 指派] 窗格上的清單。當您指向其名稱時，在將它成功儲存至 JMP 資料庫為止，您會看到它的狀態為擱置中。JMP 指派不再處於擱置中狀態之後，您可以在指派上採取任何其他動作。

刪除 JMP 指派

使用 Horizon Console 來刪除 JMP 指派。

刪除 JMP 指派時，系統會刪除與 JMP 指派相關聯的 Horizon 集區權利、AppStack 指派和 UEM 權利。不過，如果 JMP 指派所使用的 Horizon 集區權利或 AppStack 指派於 JMP 指派建立之前便已存在，則不會將它們刪除。刪除 JMP 指派之後，即不會將其套用至使用者或桌面平台。

必要條件

- 確認已符合第 12 章 管理 JMP 指派中列出的必要條件。
- 您計劃刪除的 JMP 指派不能處於「擱置」狀態。

程序

1 在 Horizon Console 中，按一下**指派 (JMP)**。

2 在 [JMP 指派] 窗格中，選取一或多個 JMP 指派，然後按一下**刪除**。

3 在確認對話方塊中，按一下**刪除**以確認您要永久刪除指派。

如果成功，即會從 JMP 資料庫中移除 Horizon 集區權利，並從 [JMP 指派] 窗格的清單中移除。

如果刪除作業的一部分失敗，則不會刪除 JMP 指派。按一下狀態指示器，即可提供刪除作業失敗原因的詳細資訊。

在 Horizon Console 中設定事件報告

13

您可以建立一個事件資料庫，用於記錄 Horizon 7 事件的相關資訊。此外，如果您使用 Syslog 伺服器，則可以設定連線伺服器將事件傳送至 Syslog 伺服器，或建立以 Syslog 格式寫入之事件的一般檔案。

本章節討論下列主題：

在 Horizon Console 中新增 Horizon 7 事件的資料庫和資料庫使用者

您可以透過將事件資料庫新增到現有的資料庫伺服器來建立該事件資料庫。接著，您可以使用報告軟體來分析資料庫中的事件。

在專用伺服器上部署事件資料庫的資料庫伺服器，以便事件記錄活動不會影響佈建和對 Horizon 7 部署非常重要的其他活動。

備註 您不需要建立此資料庫的 ODBC 資料來源。

必要條件

- 確認您在連線伺服器執行個體可存取的系統上，具有支援的 Microsoft SQL Server 或 Oracle 資料庫伺服器。

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

- 請確認您擁有在資料庫伺服器上建立資料庫和使用者所需的資料庫權限。

- 如果您不熟悉在 Microsoft SQL Server 資料庫伺服器上建立資料庫的程序，請參閱《Horizon 7 安裝》文件中的「將 View Composer 資料庫新增至 SQL Server」。
- 如果您不熟悉在 Oracle 資料庫伺服器上建立資料庫的程序，請參閱《Horizon 7 安裝》文件中的「將 View Composer 資料庫新增至 Oracle 12c 或 11g」。

程序

1 將資料庫新增至伺服器，並為其提供描述性名稱，例如 HorizonEvents。

對於 Oracle 12c 或 Oracle 11g 資料庫，也請提供 Oracle 系統識別碼 (SID)，當您在 Horizon Console 中設定事件資料庫時將會用到此識別碼。

2 為此資料庫新增有權建立資料表、視圖、Oracle 觸發程序與序列，且有權讀取或寫入這些物件的使用者。

若是 Microsoft SQL Server 資料庫，請不要使用「整合式 Windows 驗證」安全性模型驗證方法。確認您使用 SQL Server 驗證方法進行驗證。

系統會建立資料庫，但在 Horizon Console 中設定資料庫之前，並不會安裝結構描述。

後續步驟

請依照在 Horizon Console 中設定事件資料庫中的指示進行。

準備用於 Horizon Console 中事件報告的 SQL Server 資料庫

您必須先設定正確的 TCP/IP 內容，並確認伺服器使用 SQL Server 驗證，才能使用 Horizon Console 在 Microsoft SQL Server 上設定事件資料庫。

必要條件

- 建立用於事件報告的 SQL Server 資料庫。請參閱在 Horizon Console 中新增 Horizon 7 事件的資料庫和資料庫使用者。
- 確認您擁有設定資料庫的必要資料庫權限。
- 確認資料庫伺服器使用 SQL Server 驗證方法進行驗證。請勿使用 Windows 驗證。

程序

1 開啟「SQL Server 組態管理員」，並展開 **SQL Server *YYYY* 網路組態**。

2 選取 ***server_name* 的通訊協定**。

3 在通訊協定清單中，以滑鼠右鍵按一下 **TCP/IP** 並選取**內容**。

4 將**已啟用**內容設為**是**。

5 確認已指定連接埠，必要時請指定一個連接埠。

如需靜態和動態連接埠及如何指定連接埠的相關資訊，請參閱 SQL Server 組態管理員的線上說明。

6 確認此連接埠未遭到防火牆封鎖。

後續步驟

使用 Horizon Console 將資料庫連線至連線伺服器。請依照在 Horizon Console 中設定事件資料庫中的指示進行。

在 Horizon Console 中設定事件資料庫

事件資料庫會將 Horizon 7 事件的相關資訊以記錄的形式儲存在資料庫中 (而非記錄檔中)。

在安裝連線伺服器執行個體之後，您會設定事件資料庫。您只需要在連線伺服器群組中設定一個主機。系統會自動設定群組中的其餘主機。

備註 儘管事件流量受限於 Horizon 7 環境的相關健全狀況資訊，但連線伺服器執行個體與外部資料庫之間的資料庫連線安全性是管理員的責任。如果希望採取額外的預防措施，您可以透過 IPSec 或其他方式保護此通道的安全，也可以將資料庫部署在連線伺服器電腦本機上。

您可以使用 Microsoft SQL Server 或 Oracle 資料庫報告工具檢查資料庫資料表中的事件。如需詳細資訊，請參閱《Horizon 7 整合》文件。

您也可以使用 `Syslog` 格式產生 Horizon 7 事件，讓協力廠商分析軟體可以存取事件資料。您可以將 `vdmadmin` 命令與 `-I` 選項搭配使用，將 Horizon 7 事件訊息以 `Syslog` 格式記錄在事件記錄檔中。請參閱《Horizon 7 管理》文件中的〈使用 -I 選項以 Syslog 格式產生 Horizon 7 事件記錄訊息〉。

必要條件

您需要下列資訊才能設定事件資料庫：

- 資料庫伺服器的 DNS 名稱或 IP 位址。
- 資料庫伺服器類型：Microsoft SQL Server 或 Oracle。
- 用來存取資料庫伺服器的連接埠號碼。Oracle 的預設值為 1521，SQL Server 的預設值為 1433。對於 SQL Server，如果資料庫伺服器是具名執行個體，或者您使用的是 SQL Server Express，則可能必須決定連接埠號碼。請參閱有關連線至 SQL Server 具名執行個體的 Microsoft 知識庫文章，網址為：http://support.microsoft.com/kb/265808。
- 您在資料庫伺服器上建立之事件資料庫的名稱。請參閱在 Horizon Console 中新增 Horizon 7 事件的資料庫和資料庫使用者。

  針對 Oracle 12c 或 11g 資料庫，當您在 Horizon Console 中設定事件資料庫時，必須使用 Oracle 系統識別碼 (SID) 作為資料庫名稱。
- 您為此資料庫建立之使用者的使用者名稱和密碼。請參閱在 Horizon Console 中新增 Horizon 7 事件的資料庫和資料庫使用者。

  為此使用者使用 SQL Server 驗證。不要使用整合式 Windows 驗證的安全性模型驗證方法。

- 事件資料庫中資料表的前置詞，例如 VE_。前置詞可讓資料庫在 Horizon 7 安裝期間共用。

  備註 您必須輸入對您使用之資料庫軟體有效的字元。當您完成對話方塊時，系統不會檢查前置詞的語法。如果您輸入的字元對您所使用的資料庫軟體而言無效，當連線伺服器嘗試連線至資料庫伺服器時，將會發生錯誤。如果資料庫名稱無效，記錄檔會指出所有錯誤，包括此錯誤及從資料庫伺服器傳回的其他所有錯誤。

程序

1. 在 Horizon Console 中，選取**設定 > 事件組態**。
2. 在**事件資料庫**區段中，按一下**編輯**，在提供的欄位中輸入資訊，再按一下**確定**。

   若要清除事件資料庫資訊，請按一下**清除**。
3. (選擇性) 在「事件設定」視窗中，按一下**編輯**，變更顯示事件的時間長度，以及將事件分類為新事件的天數，然後按一下**確定**。

   關於事件時間長度的這些設定會在 Horizon Console 介面中列出。目前只有在歷史資料庫資料表中才有事件。
4. 選取**監視 > 事件**以確認與事件資料庫的連線成功。

   如果連線不成功，則會出現錯誤訊息。如果您使用的是 SQL Express，或者使用的是 SQL Server 的具名執行個體，則可能必須決定正確的連接埠號碼 (如先決條件所述)。

在 Horizon Console 中設定事件記錄至檔案或 Syslog 伺服器

您可以使用 Syslog 格式產生 Horizon 7 事件，讓分析軟體可以存取事件資料。

您只需要在連線伺服器群組中設定一個主機。系統會自動設定群組中的其餘主機。

如果您啟用事件的檔案式記錄，事件會累積在本機記錄檔中。如果您指定檔案共用，這些記錄檔會移至該共用。

- 刪除最舊的檔案之前，事件記錄 (包括已關閉的記錄檔) 之本機目錄的大小上限為 300MB。Syslog 輸出的預設目的地為 `%PROGRAMDATA%\VMware\VDM\events\`。
- 如果您沒有 Syslog 伺服器或事件資料庫，或者您目前的 Syslog 伺服器不符需求，請使用 UNC 路徑來儲存長期事件記錄的記錄檔。

或者，您可以使用 `vdmadmin` 命令，以 Syslog 格式設定事件的檔案式記錄。請參閱《Horizon 7 管理》文件中，關於使用 `vdmadmin` 命令的 `-I` 選項以 Syslog 格式產生 Horizon 7 事件記錄訊息的主題。

重要 傳送 Syslog 伺服器時，Syslog 資料會以沒有軟體式加密的方式傳送到網路上，而且可能包含機密資料，例如使用者名稱。VMware 建議使用連結層安全性 (例如 IPSEC) 以避免此資料可能在網路上遭到監視。

必要條件

您需要使用下列資訊設定連線伺服器，才能以 Syslog 格式記錄事件和/或將事件傳送至 Syslog 伺服器：

- 如果您打算使用 Syslog 伺服器在 UDP 連接埠上接聽 Horizon 7 事件，您必須具有 Syslog 伺服器的 DNS 名稱或 IP 位址以及 UDP 連接埠號碼。預設 UDP 連接埠號碼為 514。
- 如果您打算以一般檔案格式收集記錄，則必須擁有檔案共用及儲存記錄檔所在資料夾的 UNC 路徑，而且還必須擁有使用者名稱、網域名稱，以及具備寫入檔案共用之權限的帳戶密碼。

程序

1 在 Horizon Console 中，選取**設定 > 事件組態**。

2 (選擇性) 在 **Syslog** 區域中，若要設定連線伺服器以將事件傳送到 Syslog 伺服器，請按一下**傳送到 syslog 伺服器**下方的**新增**，並提供伺服器名稱或 IP 位址以及 UDP 連接埠號碼。

3 (選擇性) 在**事件到檔案系統**區域中，選擇是否要啟用事件記錄訊息的產生，並在記錄檔中以 Syslog 格式儲存。

選項	說明
永遠	永遠產生並在記錄檔中以 Syslog 格式儲存事件記錄訊息。
發生錯誤時記錄到檔案 (預設)	寫入事件到事件資料庫或 Syslog 伺服器發生問題時，將稽核事件記錄到記錄檔。此選項依預設為啟用。
永不	永不產生並在記錄檔中以 Syslog 格式儲存事件記錄訊息。

除非您指定檔案共用的 UNC 路徑，否則記錄檔會保留在本機上。

4 (選擇性) 若要將 Horizon 7 事件記錄訊息儲存在檔案共用上，請按一下**複製到位置**下方的**新增**，並提供要用來儲存記錄檔之檔案共用和資料夾的 UNC 路徑，以及有權寫入檔案共用之帳戶的使用者名稱、網域名稱和密碼。

以下為 UNC 路徑範例：

```
\\syslog-server\folder\file
```

在 Horizon 7 中監視事件

事件資料庫會儲存連線伺服器主機或群組、Horizon Agent 與 Horizon Console 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**頁面中詳細檢查事件。

備註　事件會在有限的期間內列於 Horizon Console 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 Console 介面中檢視這些事件。

除了監控 Horizon Console 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》文件中的在 Horizon Console 中設定事件記錄至檔案或 Syslog 伺服器和〈使用 -l 選項以 Syslog 格式產生 Horizon 7 事件記錄訊息〉。

如果是為多個連線伺服器設定事件資料庫，Horizon Console 會在**事件**頁面上顯示所有連線伺服器的事件。Horizon Console 會根據您所執行的工作篩選事件，並在**桌面平台集區**或**應用程式集區**頁面之類的相關頁面上顯示這些事件。

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 Console 中，選取**監視 > 事件**。

2 (選擇性) 在**事件**頁面上，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。

後續步驟

在 Horizon Console 中，導覽至桌面平台或應用程式集區、虛擬機器、持續性磁碟或是使用者或群組，然後按一下**事件**索引標籤以檢視特定事件。

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 13-1. 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。

在 Horizon Console 中使用 Horizon Help Desk Tool

14

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《Horizon 7 管理》文件。
- 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 管理》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《Horizon 7 管理》文件。
- 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}
  ```

本章節討論下列主題：

在 Horizon Console 中 啟動 Horizon Help Desk Tool

Horizon Help Desk Tool 已整合至 Horizon Console。您可以搜尋要在 Horizon Help Desk Tool 中疑難排解問題的使用者。

程序

1 您可以在 [使用者搜尋] 文字方塊中搜尋使用者名稱，或直接導覽至 Horizon Help Desk Tool 工具。

- 在 Horizon Console 中，於 [使用者搜尋] 文字方塊中輸入使用者名稱。
- 選取**監視器 > 服務台**，然後在 [使用者搜尋] 文字方塊中輸入使用者名稱。

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。

2 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。

您也可以按一下電子郵件位址，以傳送訊息給使用者。

您也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。

備註　商務用 Skype 資訊不會對 Linux 桌面平台使用者顯示。

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 14-1. 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。
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。 ■ **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。 ■ **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。 **備註** 針對 Linux 桌面平台工作階段，您無法存取**應用程式**索引標籤。
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桌面平台、虛擬機器桌面平台還是應用程式。
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

桌面平台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 14-2. 桌面平台

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。針對 Linux 桌面平台工作階段將 Linux 顯示為桌面平台集區。
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。

表 14-2. 桌面平台 (續)

選項	說明
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」。
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

應用程式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。

備註 針對 Linux 桌面平台工作階段，您無法存取**應用程式**索引標籤。

表 14-3. 應用程式

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** 如果有全域應用程式，此資料行會顯示全域應用程式權利中的伺服器陣列數目。
Type	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」。
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 Cloud Pod 架構環境中的使用者並不會顯示事件記錄資訊。

表 14-4. 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詳細資料。您可以檢視 Horizon Client、虛擬或已發佈桌面平台，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 14-5. 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。
作業系統版本	作業系統版本。
連線伺服器	工作階段連線的連線伺服器。
集區	桌面平台或應用程式集區的名稱。針對 Linux 桌面平台集區顯示 Linux。
vCenter	vCenter Server 的 IP 位址。
工作階段狀態	桌面平台或應用程式工作階段的狀態。工作階段狀態可以是閒置、作用中或已中斷連線。如果使用者處於非作用中達到一分鐘，則工作階段狀態會變為閒置。狀態圖示顯示為綠色框線代表閒置、綠色實心代表作用中，而灰色代表已中斷連線。 **備註** Linux 桌面平台工作階段不會顯示閒置狀態。

表 14-5. 虛擬機器詳細資料 (續)

選項	說明
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。
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。
登入持續時間	登入工作階段的使用者持續登入的時間。
閘道/Proxy 名稱	安全伺服器、Unified Access Gateway 應用裝置或負載平衡器的名稱。連線至工作階段後，此資訊可能需要 30 秒到 60 秒才會顯示。
閘道/Proxy IP	安全伺服器、Unified Access Gateway 應用裝置或負載平衡器的 IP 位址。連線至工作階段後，此資訊可能需要 30 秒到 60 秒才會顯示。
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。

使用者經驗度量

顯示使用 PCoIP 或 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**更多**。若要重新整理這些詳細資料，請按一下重新整理圖示。

表 14-6. PCoIP 顯示通訊協定詳細資料

選項	說明
TX 頻寬	PCoIP 工作階段中的傳輸頻寬 (單位為每秒 kb)。
畫面播放速率	PCoIP 工作階段中的畫面播放速率 (每秒畫面數)。
封包遺失	PCoIP 工作階段中封包遺失的百分比。
Skype 狀態	PCoIP 工作階段中商務用 Skype 的狀態。 ■ 最佳化 ■ 後援 ■ 最佳化 (版本不相符) ■ 後援 (版本不相符) ■ 正在連線 ■ 已中斷連線 ■ 未定義 此選項會對 Linux 桌面平台工作階段顯示為不適用。

表 14-7. Blast 顯示通訊協定詳細資料

選項	說明
畫面播放速率	Blast 工作階段中的畫面播放速率 (每秒畫面數)。
Skype 狀態	Blast 工作階段中商務用 Skype 的狀態。 ■ 最佳化 ■ 後援 ■ 最佳化 (版本不相符) ■ 後援 (版本不相符) ■ 正在連線 ■ 已中斷連線 ■ 未定義 此選項會對 Linux 桌面平台工作階段顯示為不適用。
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 和記憶體使用量以及網路和磁碟效能

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 顯示通訊協定的網路或磁碟效能。

備註　在桌面平台上 Horizon Agent 啟動或重新啟動之後，效能圖可能不會立即顯示時間表。時間表會在幾分鐘後顯示。

表 14-8. CPU 使用率

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。

表 14-9. 記憶體使用量

選項	說明
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。

表 14-10. 網路效能

選項	說明
延遲	顯示 PCoIP 或 Blast 工作階段的延遲圖。 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**。

表 14-11. 磁碟效能

選項	說明
讀取	每秒讀取輸入/輸出 (I/O) 作業的數目。
寫入	每秒寫入 I/O 作業的數目。
磁碟延遲	顯示磁碟延遲的圖表。磁碟延遲即為從 Windows 效能計數器所擷取每秒輸入/輸出作業 (IOPS) 資料的時間 (以毫秒為單位)。
平均讀取	每秒隨機讀取 I/O 作業的平均數目。
平均寫入	每秒隨機寫入 I/O 作業的平均數目。
平均延遲	從 Windows 效能計數器擷取之 IOPS 資料的平均延遲時間 (以毫秒為單位)。

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 14-12. 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。 ■ **通訊協定連線**。PCoIP 或 Blast 通訊協定連線在完成登入程序期間所花費的時間總計。 ■ **登入指令碼**。登入指令碼從開始執行到完成所花費的時間總計。 ■ **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。如果未設定全域原則，則 **GPO 載入**登入區段時間為 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。針對新工作階段會顯示 **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。
- 如果工作階段為 Linux 桌面平台工作階段，則不會顯示 **GPO 載入**和**設定檔載入**區段。
- 當桌面平台工作階段連線時，登入資料可能不會立即可用。登入資料會在幾分鐘後顯示。

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。

對於 RDS 主機工作階段，**處理程序**索引標籤會顯示目前使用者或目前系統處理程序啟動的目前 RDS 主機工作階段處理程序。

表 14-13. 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。 您無法結束可能會在**處理程序**索引標籤中列出的重要處理程序，例如 Windows 核心處理程序。如果您要結束某個重要處理程序，則 Horizon Help Desk Tool 會顯示一則訊息，表示其無法結束此系統處理程序。

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。針對 Linux 桌面平台工作階段，您無法存取**應用程式**索引標籤。

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。

您可以為使用者結束應用程式程序。若要結束應用程式程序，請按一下**結束應用程式**，然後按一下**確定**以確認變更。

備註 如果應用程式正在擱置使用者互動 (例如有未儲存的資料)，或者由於其他例外狀況，結束應用程式程序的作業可能會失敗。但是，在您結束應用程式時，Horizon Help Desk Tool 不會顯示任何成功或失敗訊息。

表 14-14. 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。 **備註** 此功能不適用於 Linux 桌面平台使用者。 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。
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 vdmadmin 命令

15

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#unique_9。

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 15-1. 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 15-2. 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_186。
-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 15-2. 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 15-3. 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 15-4. 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 15-5. 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 15-6. 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 15-6. 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 15-7. 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 15-8. 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 15-9. 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 15-10. 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 #unique_203。
- 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 15-11. 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 15-12. 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 15-12. 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 15-13. 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 15-14. 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 15-14. 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 15-15. 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 15-15. 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 15-16. 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 [-passwordpassword]
```

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 15-17. 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 15-18. 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 15-19. 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 15-20. 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
```