Horizon 管理

VMware Horizon 2103

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

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

目錄

VMware Horizon 管理

1

《Horizon 管理》說明如何在 Horizon Console 中設定和管理 VMware Horizon®、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 VMware Horizon 元件和進行疑難排解。

VMware Horizon Console 是最新版本的 Web 介面，您可以透過它建立和管理虛擬桌面平台和已發佈的桌面平台和應用程式。

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 中管理 Cloud Pod 架構》文件。

主要對象

這些資訊適用於想要設定和管理 VMware Horizon 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

VMware Horizon Console 是 VMware Horizon 的 Web 介面，您可以透過它來建立和管理虛擬桌面平台及已發佈的桌面平台和應用程式。

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

本章節討論下列主題：

登入 Horizon Console

若要執行桌面平台或應用程式集區部署工作，或監控工作並進行疑難排解，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。
- 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 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。VMware 建議使用 FQDN，而非 IP 位址。

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。

備註 如果您使用較舊的網頁瀏覽器 (例如 Internet Explorer 11)，則會出現快顯視窗，其中顯示您應使用以取得 Horizon Console 最佳使用者體驗的網頁瀏覽器。您也可以在快顯視窗中按一下您慣用的網頁瀏覽器，以下載該網頁瀏覽器。

選項	說明
您已為連線伺服器設定 CA 簽署的憑證。	第一次連線時，您的網頁瀏覽器會顯示 VMware Horizon 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 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。

3 若要記住每次登入的使用者名稱，請選擇性地選取**記住使用者名稱**。

4 按一下**登入**。

後續步驟

您也可以在 Horizon Console 中的任何連結上按一下滑鼠右鍵，以在另一個網頁瀏覽器索引標籤中開啟。

Horizon Console 介面的使用提示

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

Horizon Console 包含許多常用的使用者介面功能。例如，每個頁面左側的導覽窗格，可將您導向至其他 Horizon Console 頁面。搜尋篩選器可以讓您選取與您要搜尋之物件相關的篩選準則。

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

表 2-1. Horizon Console 導覽和顯示功能

Horizon Console 功能	說明
在 Horizon Console 頁面中向後和向前導覽	按一下瀏覽器的**上一頁**按鈕，移至先前顯示的 Horizon Console 頁面。按一下**向前**按鈕以返回目前頁面。 若您在使用 Horizon Console 精靈或對話方塊時，按一下瀏覽器的**上一頁**按鈕，則會返回主要 Horizon Console 頁面。您在精靈或對話方塊中輸入的資訊將會遺失。
將 Horizon Console 頁面加入書籤	您可以在瀏覽器中將 Horizon Console 頁面加入書籤。

表 2-1. Horizon Console 導覽和顯示功能 (續)

Horizon Console 功能	說明
多欄排序	您可以使用多欄排序，以多種方式為 Horizon 物件排序。 按一下 Horizon Console 資料表頂端列的標題，可根據該標題按字母順序為 Horizon 物件排序。 若要以次要項目為 Horizon 物件排序，請按住 Ctrl 並點選其他標題。 您可以繼續按 Ctrl 加標題，依重要性遞減順序為資料表中的所有欄排序。 按 Ctrl+Shift 同時按一下標題，可取消選取排序項目。
自訂資料表欄	您可以隱藏選取的欄並鎖定第一欄，以自訂 Horizon Console 資料表欄的顯示方式。此功能可讓您對包含許多資料行的大型資料表控制其顯示方式。 在任一欄標題上按一下滑鼠右鍵，以顯示可讓您採取下列動作的內容功能表： ■ 隱藏所選欄。 ■ 自訂欄。對話方塊顯示資料表中的所有欄。您可以選取欄以顯示或隱藏。 ■ 鎖定第一欄。此選項可以在水平捲動包含許多欄的資料表時，強制顯示左欄。
選取 Horizon 物件並顯示 Horizon 物件詳細資料	在列出 Horizon 物件的 Horizon Console 資料表中，您可以選取物件或顯示物件詳細資料。 ■ 若要選取物件，請在資料表中物件列的任何地方按一下。頁面上方用來管理物件的功能表和命令會變得可供使用。 ■ 若要顯示物件詳細資料，請按兩下物件列中的左側儲存格。物件詳細資料會以新頁面顯示。 例如，在**詳細目錄 > 桌面平台**頁面上，按一下個別集區之資料列中的任一處，以啟用會影響集區的命令。 按兩下左側欄中的**識別碼**儲存格，以顯示包含集區詳細資料的新頁面。
展開對話方塊以檢視詳細資料	您可以展開 Horizon Console 對話方塊，以檢視資料表欄中的詳細資料，例如桌面平台名稱和使用者名稱。 若要展開對話方塊，請將滑鼠置於對話方塊右下角的點上方，然後拖曳角落。
在 Horizon 物件上顯示網頁瀏覽器作業的快顯功能表	您可以在 Horizon Console 資料表中的 Horizon 物件上按一下滑鼠右鍵，以顯示用來執行網頁瀏覽器作業的快顯功能表，例如在另一個索引標籤或視窗中開啟物件。

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 執行個體新增至 VMware Horizon 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

若要使用 VMware vSphere 虛擬機器作為遠端桌面平台，您必須將 VMware Horizon 設定為與 vCenter Server 通訊。

如需詳細資訊，請參閱《Horizon 安裝》文件中的〈將 vCenter Server 執行個體新增至 VMware Horizon〉。

從 VMware Horizon 中移除 vCenter Server 執行個體

您可以移除 VMware Horizon 與 vCenter Server 執行個體之間的連線。當您這麼做後，VMware Horizon 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 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 VMware Horizon 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**。

結果

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

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 VMware Horizon，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 VMware Horizon 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。

瞭解 VMware Horizon 服務

連線伺服器執行個體的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 VMware Horizon 服務。若您停止連線伺服器主機上的 VMware Horizon 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 VMware Horizon 功能沒有回應時，重新啟動服務。

停止和啟動 VMware Horizon 服務

連線伺服器執行個體的作業取決於系統上執行的數個服務。當您疑難排解 VMware Horizon 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 VMware Horizon 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 請停止連線伺服器主機上的 VMware Horizon 連線伺服器服務即可。請勿停止其他任何元件服務。

必要條件

自行熟悉在連線伺服器主機上執行的服務，如連線伺服器主機上的服務中所述。

程序

1 在命令提示字元處輸入 **`services.msc`** 以啟動 Windows 服務工具。

2 選取連線伺服器主機上的 VMware Horizon 連線伺服器服務，然後按一下**停止**、**重新啟動**或**啟動** (如果適用)。

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

VMware Horizon 的作業取決於在連線伺服器主機上執行的數個服務。

表 3-1. Horizon 連線伺服器主機服務

服務名稱	啟動類型	說明
VMware Horizon 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 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 指令碼主機服務。
VMware Horizon 架構元件	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。

表 3-1. Horizon 連線伺服器主機服務 (續)

服務名稱	啟動類型	說明
VMware Horizon 訊息匯流排元件	手動	在 VMware Horizon 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 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 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 安全閘道元件	手動	提供一般閘道服務。此服務必須永遠處於執行狀態。
VMware Horizon 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 Horizon LDAP 服務。此服務必須永遠處於執行狀態。在 VMware Horizon 升級期間，此服務可確保現有資料能正確移轉。

配置不受信任的網域

您可以在連線伺服器網域內新增沒有正式信任關係的使用者網域。設定連線伺服器網域與使用者網域之間的單向或雙向信任關係之後，通常會干擾使用者 Active Directory (AD) 基礎結構。您可以改為在個別網域中部署 VMware Horizon，並將其設定為不受信任的網域，以設定與使用者網域的通訊。

在某些情況下 (例如，當您擁有與內部部署使用者網域進行通訊的雲端主控連線伺服器網域時) 可以更輕鬆地設定以建立不受信任的關係。

您可以建立主要網域繫結帳戶，以設定連線伺服器網域與其他網域之間的不受信任關係。Horizon 會使用網域繫結帳戶在 Active Directory 中查詢和執行查閱。您也可以新增多個輔助帳戶，以防主要網域繫結帳戶變得無法存取或遭到鎖定。

當設定時，Horizon 會使用輔助網域繫結帳戶在 Active Directory 中查詢和執行查詢。

在 Horizon Console 中，您可以透過導覽至**設定 > 網域**，以檢視在**網域繫結**索引標籤上設定的不受信任網域和資訊，以及在**連線伺服器**索引標籤上連線伺服器網域信任關係。

當不受信任的網域成功設定，且稍後管理員建立不受信任網域與連線伺服器網域的正式信任關係 (單向或雙向) 時，不受信任的網域將會視為連線伺服器網域。不受信任的網域將不再顯示在**網域 > 網域繫結**中，且將會顯示在**網域 > 連線伺服器**索引標籤中。

網域繫結帳戶內容

當您建立網域繫結帳戶時，必須指定特定帳戶組態和 Active Directory (AD) 登錄內容。Horizon 會使用網域繫結帳戶作為主要服務帳戶，以連線至不受信任使用者網域的 Active Directory 伺服器並查詢 Active Directory。

表 3-2. 網域繫結帳戶內容

內容	說明
DNS 名稱	完整 Active Directory 網域名稱。
NetBIOS	Active Directory NetBIOS 網域名稱。
通訊協定	(無法編輯) LDAP 是唯一支援的通訊協定。
主要服務帳戶	主要網域繫結服務帳戶的認證： ■ **使用者名稱**。主要網域繫結管理員的使用者名稱。 ■ **密碼**。主要網域繫結管理員的密碼。
連接埠	預設連接埠是 389 (LDAP)。除非您使用的是非標準連接埠，否則不需要修改此文字方塊。
內容	與 DNS 網域名稱相關的 LDAP 命名內容。此欄位會自動從 DNS 名稱填入。例如，「dc=horizon,dc=example,dc=com」。
自動	選取此選項可自動探索網域控制站。
網域控制站 IP	指定要用來與此 Active Directory 通訊的網域控制站 IP。可以使用以逗號分隔的清單來提供多個 IP。
站台名稱	用於搜尋網域控制站或控制站的慣用站台。

新增網域繫結帳戶

新增主要網域繫結帳戶，以設定連線伺服器網域與不同網域之間的不受信任關係。

必要條件

- 確認您已準備好用於連線伺服器網域的 Active Directory。請參閱《Horizon 安裝》文件中的〈準備 Active Directory〉。
- 收集不受信任的網域繫結帳戶內容。請參閱網域繫結帳戶內容。
- 確認連線伺服器網域與目標使用者網域之間沒有任何正式信任關係。您可以導覽至**設定 > 網域**然後按一下**連線伺服器**索引標籤，以檢視連線伺服器網域的網域資訊。
- 確認您的 DNS 基礎結構可以成功解析來自每個連線伺服器的不受信任網域 FQDN。
- 確認連線伺服器機器與不受信任網域的網域控制站及時同步。

程序

1 在 Horizon Console 中，導覽至**設定 > 網域**。

2 按一下**網域繫結**索引標籤。

3 按一下**新增**以新增不受信任的網域繫結帳戶。

4 輸入受信任的網域繫結帳戶內容。

5 (選擇性) 選取**新增不受信任網域帳戶後新增輔助帳戶**以新增輔助網域繫結帳戶。

在**管理輔助帳戶**視窗中，按一下**新增**並輸入輔助網域繫結帳戶使用者的使用者名稱和密碼，然後按一下**確定**。

6 按一下**確定**。

結果

在**網域繫結**索引標籤上，您可以在**服務帳戶**資料行中檢視主要網域繫結戶。

後續步驟

新增輔助網域繫結帳戶。請參閱管理輔助網域繫結帳戶。

管理輔助網域繫結帳戶

新增主要網域繫結帳戶後，您可以新增、編輯和移除輔助網域繫結帳戶。您也可以新增多個輔助網域繫結帳戶。當設定時，如果主要網域繫結帳戶無法存取或遭到鎖定，則 Horizon 將會使用輔助網域繫結帳戶。

必要條件

確認您已新增網域繫結帳戶。請參閱新增網域繫結帳戶。

程序

1 在 Horizon Console 中，**導覽至設定 > 網域**。

2 按一下**網域繫結**索引標籤。

3 選取不受信任的網域。

4 按一下**管理輔助帳戶**。

5 輸入輔助帳戶的使用者名稱和密碼。

6 (選擇性) 按一下**新增**以新增另一個輔助帳戶，然後輸入輔助帳戶使用者的使用者名稱和密碼。

您也可以選擇性地編輯或移除輔助帳戶。按一下**編輯**以編輯輔助帳戶使用者的使用者名稱和密碼。按一下**移除**以移除輔助帳戶。

備註 輔助網域繫結帳戶使用者可以編輯密碼，但無法編輯輔助帳戶的使用者名稱。

7 按一下**確定**。

結果

在**網域繫結**索引標籤上，您可以在**輔助帳戶**資料行下方檢視新增的輔助帳戶數量。

進行用戶端工作階段的設定

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

為用戶端工作階段和連線設定選項

您可以設定全域設定，以確定用戶端工作階段和連線的運作方式。

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

您也可以將連線伺服器執行個體設定為在 Horizon 用戶端和遠端桌面平台之間，使用直接、非通道連線。請參閱《Horizon 安裝》文件中的〈建設定安全通道和 PCoIP 安全閘道〉。

必要條件

自行熟悉全域設定。請參閱用戶端工作階段的全域設定、用戶端工作階段和連線的全域安全性設定和用戶端工作階段的全域用戶端限制設定。

程序

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

2 選擇您要設定一般設定、安全性設定還是用戶端限制設定。

選項	說明
一般全域設定	在**一般設定**索引標籤中，按一下**編輯**。
全域安全設定	在**安全性設定**索引標籤中，按一下**編輯**。
全域用戶端限制設定	在**用戶端限制設定**索引標籤中，按一下**編輯**。

3 設定全域設定。

4 按一下**確定**。

後續步驟

您可以變更在安裝期間所提供的資料復原密碼。請參閱《Horizon 安全性》文件中的〈變更資料復原密碼〉。

用戶端工作階段的全域設定

一般全域設定可決定工作階段逾時長度、SSO 啟用與逾時限制、Horizon 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。您不需重新啟動連線伺服器或 Horizon Client。

表 3-3. 用戶端工作階段的一般全域設定

設定	說明
View API 工作階段逾時	決定 View API 工作階段會持續閒置多久的時間，View API 工作階段才會逾時。 **重要** 若將 View API 工作階段逾時設為很大的分鐘數，則會增加未經授權使用 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，View API 工作階段逾時為 10 分鐘。您可以將工作階段逾時設為 10 到 4320 分鐘 (72 小時)。
連線伺服器工作階段逾時	決定 Horizon Console 工作階段要持續閒置多久的時間，連線伺服器工作階段才會逾時。 **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。 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。 您可以設定的最小連線伺服器工作階段逾時為 2 分鐘，最大連線伺服器工作階段逾時為 4320 分鐘 (72 小時)。 若要覆寫**連線伺服器工作階段逾時**值，並針對閒置的 Horizon Console 工作階段要多久才會逾時設定您自己的使用者喜好設定，請在 Horizon Console 標頭中按一下**設定**。在**我的喜好設定**對話方塊中，輸入**連線伺服器工作階段逾時覆寫**的值。
強制中斷使用者連線	自使用者登入 VMware Horizon 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**。
單一登入 (SSO)	如果 SSO 已啟用，則 VMware Horizon 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 VMware Horizon 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 VMware Horizon Agent 6.0 或更新版本或 Horizon Agent 7.0 或更新版本時，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，使用者必須從連線伺服器中斷連線或結束 Horizon Client，然後重新連線至連線伺服器。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。

表 3-3. 用戶端工作階段的一般全域設定 (續)

設定	說明
支援應用程式的用戶端中斷應用程式的連線並捨棄閒置使用者的 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 VMware Horizon 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**，VMware Horizon 將永不會因為使用者無活動而中斷應用程式連線或捨棄 SSO 認證。 預設值為**永不**。
其他用戶端 捨棄 SSO 認證	指定分鐘數後捨棄 SSO 認證。此設定適用於不支援應用程式遠端處理的用戶端。如果設定為 **...分鐘後**，使用者必須在其登入 VMware Horizon 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，VMware Horizon 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 VMware Horizon Server 元件安裝所在的機器。 **備註** Horizon Agent 軟體無法與其他任何 VMware Horizon Server 軟體元件 (包括連線伺服器) 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，VMware Horizon 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。 啟用此設定也會影響 HTML Access 從 Workspace ONE 啟動時的行為。如需詳細資訊，請參閱 Workspace ONE 說明文件。 停用此設定時，認證會留在快取中。此功能依預設為停用。

表 3-3. 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伺服器資訊	啟用此安全性設定，可在 Horizon Client 中隱藏伺服器 URL 資訊。
在用戶端使用者介面中隱藏網域清單	啟用此安全性設定，可在 Horizon Client 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 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 安全性》文件。
啟用雙因素重新驗證	選取此設定以啟用在工作階段逾時後對使用者執行雙因素驗證的功能。

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 VMware Horizon 之間的 Horizon Client 連線和 Horizon Console 連線都需要 TLS。如果您的 VMware Horizon 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上設定非 TLS 連線。

表 3-4. 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 VMware Horizon 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。

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應用程式的啟動限定於特定用戶端和版本，以及向用戶端提供警告訊息。

在 Horizon Console 中，您可以導覽至**設定 > 全域設定 > 用戶端限制設定**，以設定全域用戶端限制設定。

用戶端限制適用於 Horizon Client 4.5.0 版或更新版本，但 Chrome 版 Horizon Client 除外 (必須是 4.8.0 版或更新版本)。已設定此功能時，特定或舊版 Horizon Client 的用戶端類型皆無法連線至遠端桌面平台和已發佈的應用程式。向特定用戶端版本顯示警告訊息的功能適用於 Horizon Client 2006 或更新版本。

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 VMware Horizon。

表 3-5. 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	針對**封鎖來自用戶端版本的連線**設定，請選取下列其中一個選項： ■ **早於**：指定最早的用戶端版本，以封鎖早於該版本的所有用戶端。 ■ **特定**：輸入特定版本 (以逗號分隔)，以在使用者使用這些用戶端版本連線時封鎖使用者。 針對**從特定用戶端版本連線時警告使用者**設定，請輸入以逗號分隔的版本，以警告從這些用戶端版本連線的使用者。依預設會啟用 Horizon Client 5.5.0 版的警告。您可以移除此版本以停用警告。
Linux 版 Horizon Client	針對**封鎖來自用戶端版本的連線**設定，請選取下列其中一個選項： ■ **早於**：指定最早的用戶端版本，以封鎖早於該版本的所有用戶端。 ■ **特定**：輸入特定版本 (以逗號分隔)，以在使用者使用這些用戶端版本連線時封鎖使用者。 針對**從特定用戶端版本連線時警告使用者**設定，請輸入以逗號分隔的版本，以警告從這些用戶端版本連線的使用者。依預設會啟用 Horizon Client 5.5.0 版的警告。您可以移除此版本以停用警告。
Mac 版 Horizon Client	針對**封鎖來自用戶端版本的連線**設定，請選取下列其中一個選項： ■ **早於**：指定最早的用戶端版本，以封鎖早於該版本的所有用戶端。 ■ **特定**：輸入特定版本 (以逗號分隔)，以在使用者使用這些用戶端版本連線時封鎖使用者。 針對**從特定用戶端版本連線時警告使用者**設定，請輸入以逗號分隔的版本，以警告從這些用戶端版本連線的使用者。依預設會啟用 Horizon Client 5.5.0 版的警告。您可以移除此版本以停用警告。
iOS 版 Horizon Client	針對**封鎖來自用戶端版本的連線**設定，請選取下列其中一個選項： ■ **早於**：指定最早的用戶端版本，以封鎖早於該版本的所有用戶端。 ■ **特定**：輸入特定版本 (以逗號分隔)，以在使用者使用這些用戶端版本連線時封鎖使用者。 針對**從特定用戶端版本連線時警告使用者**設定，請輸入以逗號分隔的版本，以警告從這些用戶端版本連線的使用者。依預設會啟用 Horizon Client 5.5.0 版的警告。您可以移除此版本以停用警告。
Android 版 Horizon Client	針對**封鎖來自用戶端版本的連線**設定，請選取下列其中一個選項： ■ **早於**：指定最早的用戶端版本，以封鎖早於該版本的所有用戶端。 ■ **特定**：輸入特定版本 (以逗號分隔)，以在使用者使用這些用戶端版本連線時封鎖使用者。 針對**從特定用戶端版本連線時警告使用者**設定，請輸入以逗號分隔的版本，以警告從這些用戶端版本連線的使用者。依預設會啟用 Horizon Client 5.5.0 版的警告。您可以移除此版本以停用警告。
UWP 版 Horizon Client	輸入 Horizon Client 版本號碼，以封鎖早於該版本的所有用戶端。
Chrome 版 Horizon Client	針對**封鎖來自用戶端版本的連線**設定，請選取下列其中一個選項： ■ **早於**：指定最早的用戶端版本，以封鎖早於該版本的所有用戶端。 ■ **特定**：輸入特定版本 (以逗號分隔)，以在使用者使用這些用戶端版本連線時封鎖使用者。 針對**從特定用戶端版本連線時警告使用者**設定，請輸入以逗號分隔的版本，以警告從這些用戶端版本連線的使用者。依預設會啟用 Horizon Client 5.5.0 版的警告。您可以移除此版本以停用警告。
Horizon Client 表示 HTML Access	輸入 Horizon Client 版本號碼，以封鎖早於該版本的所有用戶端。

表 3-5. 用戶端工作階段的全域用戶端限制設定 (續)

設定	說明
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。 如果網繭聯盟已存在，則屬性為 `DC=vdiglobal`。如果網繭聯盟不存在，則屬性為 `DC=vdi`。
用於已封鎖用戶端版本的訊息	輸入當使用者嘗試使用已封鎖的 Horizon Client 版本連線時，要向其顯示的訊息。訊息的字元長度限制為 1024。
警告訊息	輸入要向使用受限 Horizon Client 版本連線之使用者顯示的警告訊息。訊息的字元長度限制為 1024。

加入客戶經驗改進計劃

您可以設定 VMware Horizon 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**。

備註 除了為 CEIP 收集的資訊，VMware 可能還會收集作業資料。這表示 VMware 得監控並收集客戶和其使用者就軟體使用相關的組態、效能、使用量和耗用量資料，以利產品和服務的交付和作業 (統稱為「作業資料」)，如 VMware 隱私權注意事項中所述。

收集作業資料與 CEIP 完全無關，無論您是否已加入 CEIP，都可能會進行收集。您可以連絡 VMware 支援以停用作業資料的收集。

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，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 Active Directory、硬體和軟體需求的相關資訊，請參閱《Horizon 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。

備註 不建議使用 Internet Explorer 網頁瀏覽器來進行智慧卡驗證。如需建議和支援的網頁瀏覽器清單，請參閱《Horizon 安裝》文件中的〈Horizon Console 需求〉。

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
- 在 Horizon Connection Server 上設定智慧卡驗證
- 在第三方解決方案上設定智慧卡驗證
- 在 Horizon Console 中確認您的智慧卡驗證組態
- 使用智慧卡憑證撤銷檢查

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時，連線伺服器執行個體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，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 VMware 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機構，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會使用這項資訊來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機構，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。

   針對您要匯出的檔案，使用預設的檔案類型 CER。

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會使用這項資訊來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主機上的系統路徑。如需詳細資訊，請參閱《Horizon 安裝》文件。

程序

1. 在連線伺服器主機上，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 -storetype JKS

   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 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《Horizon 安裝》文件中的〈準備 Active Directory 以進行智慧卡驗證〉。

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。

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。

- 在連線伺服器主機上的 `locked.properties` 檔案中，確認 `useCertAuth` 內容設為 **`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。已安裝遠端桌面服務角色的 RDS 主機會自動支援智慧卡功能。因此，不需要安裝該功能。

- 檢查連線伺服器主機上 *磁碟機代號*:\ProgramData\VMware\log\ConnectionServer 中的記錄檔，以尋找指出智慧卡驗證已啟用的訊息。

  備註 此檔案路徑為一個符號連結，會重新導向至記錄檔的實際位置，即 *磁碟機代號*:\ProgramData\VMware\VDM\logs

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。

VMware Horizon 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上設定憑證撤銷檢查。必須可以從連線伺服器主機存取 CA。

您可以在相同連線伺服器執行個體上設定 CRL 和 OCSP。當您設定兩種憑證撤銷檢查類型時，系統會嘗試先使用 OCSP，如果 OCSP 失敗，再回復為使用 CRL。但如果 CRL 失敗，VMware Horizon 不會回復使用 OCSP。

- 透過 CRL 檢查登入

  當您設定 CRL 檢查時，VMware Horizon 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，VMware Horizon 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。VMware Horizon 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，VMware Horizon 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，VMware Horizon 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，VMware Horizon 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 VMware Horizon 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，VMware Horizon 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。VMware Horizon 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 VMware Horizon 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，VMware Horizon 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來讓您的變更生效。

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，VMware Horizon 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，VMware Horizon 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 VMware Horizon 無法存取 CRL，CRL 檢查則會失敗。

表 4-1. 智慧卡憑證撤銷檢查的屬性 (續)

內容	說明
allowCertCRLs	當此屬性設定為 **true** 時，VMware Horizon 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。VMware Horizon 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，VMware Horizon 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

VMware Horizon 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 VMware Horizon 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 Connection Server 執行個體設定成使用者必須使用 RSA SecurID 驗證或 RADIUS (遠端驗證撥入使用者服務) 驗證。

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

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

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

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

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

- 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 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。

結果

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 VMware Horizon 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 VMware Horizon 與 VMware Workspace ONE、VMware Workspace ONE Access，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 VMware Horizon 以與其搭配使用的相關資訊。啟用 SSO 後，登入 VMware Workspace ONE Access 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 Workspace ONE Access 或第三方裝置，您必須在 VMware Horizon 中建立 SAML 驗證器。SAML 驗證器包含 VMware Horizon 和 Workspace ONE、VMware Workspace ONE Access 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 Workspace ONE Access 整合

VMware Horizon 與 VMware Workspace ONE Access (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 Workspace ONE Access 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 Workspace ONE Access 與 VMware Horizon 整合後，每當使用者登入 VMware Workspace ONE Access 並按一下桌面平台或應用程式圖示時，VMware Workspace ONE Access 便會產生唯一的 SAML 構件。VMware Workspace ONE Access 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 Workspace ONE Access 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 Workspace ONE Access 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 Workspace ONE Access 與 VMware Horizon 整合涉及使用 VMware Horizon 資訊設定 VMware Workspace ONE Access，以及將 VMware Horizon 設定為委派責任以供 VMware Workspace ONE Access 驗證。

若要委派責任給 VMware Workspace ONE Access 以供驗證，則必須在 VMware Horizon 中建立 SAML 驗證器。SAML 驗證器包含 VMware Horizon 和 VMware Workspace ONE Access 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 Workspace ONE Access 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 Workspace ONE Access 將無法辨識您在 VMware Horizon 中設定的 SAML 驗證器，而您也無法在 VMware Workspace ONE Access 中設定集區。

在 Horizon Console 中設定 SAML 驗證器

若要從 VMware Workspace ONE Access 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 VMware Horizon 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 Workspace ONE Access 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 安裝》文件。
- 記下 Workspace ONE 伺服器、VMware Workspace ONE Access 伺服器或面向外部之負載平衡器的 FQDN 或 IP 位址。
- (選擇性) 若您使用 Workspace ONE 或 VMware Workspace ONE Access，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 Workspace ONE Access 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 Workspace ONE Access 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 Workspace ONE Access，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 Workspace ONE Access 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 Workspace ONE Access，此 URL 應指向 VMware Workspace ONE Access 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 VMware Horizon 和 VMware Workspace ONE Access 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 Workspace ONE Access 的 Proxy 支援

VMware Horizon 可為 VMware Workspace ONE Access (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 VMware Horizon 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：`dc=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common`。

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 Workspace ONE Access 管理員可設定存取原則，以限制對 VMware Horizon 中已授權的桌面平台和應用程式的存取。若要強制執行在 VMware Workspace ONE Access 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。

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。

結果

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 VMware 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。

設定未驗證使用者的工作流程

1 針對未驗證存取建立使用者。請參閱針對未驗證存取建立使用者。

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

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

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

設定未驗證使用者的規則和指導方針

- 未驗證存取不支援雙因素驗證 (例如 RSA 和 RADIUS) 和智慧卡驗證。
- 智慧卡驗證和未驗證存取互斥。即使先前已啟用未驗證存取，在連線伺服器中將智慧卡驗證設為**必要**時仍會停用。
- 未驗證存取不支援 VMware Workspace ONE Access 和 VMware App Volumes。
- PCoIP 和 VMware Blast 顯示通訊協定皆支援此功能。
- 未驗證存取功能不會驗證 RDS 主機的授權資訊。管理員必須設定和使用裝置授權。
- 未驗證存取功能不會保留任何使用者特定資料。使用者可以驗證應用程式的資料儲存需求。
- 您無法重新連線至未驗證應用程式工作階段。當使用者從用戶端中斷連線時，RDS 主機會自動登出本機使用者工作階段。
- 未驗證存取僅支援已發佈的應用程式。
- 從桌面平台集區發佈的應用程式不支援未驗證存取。
- Unified Access Gateway 應用裝置不支援未驗證存取。

- 系統不會保留未驗證使用者的使用者喜好設定。
- 虛擬桌面平台不支援未驗證使用者。
- 如果已使用 CA 簽署的憑證設定連線伺服器，且已啟用未驗證存取但未設定預設的未驗證使用者，則 Horizon Console 會將連線伺服器的狀態顯示為紅色。
- 如果安裝在 RDS 主機上的 Horizon Agent 已停用 `AllowSingleSignon` 群組原則設定，則未驗證存取功能將無法運作。管理員也可以控制是否要使用 `UnAuthenticatedAccessEnabled` Horizon Agent 群組原則設定來停用或啟用未驗證存取。`vdm_agent.admx` 範本檔中包含 Horizon Agent 群組原則設定。您必須將 RDS 主機重新開機，此原則才會生效。

針對未驗證存取建立使用者

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

必要條件

- 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**。

結果

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。請參閱啟用使用者未驗證存取。

啟用使用者未驗證存取

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

程序

1 在 Horizon 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。

搜尋未驗證存取工作階段

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

程序

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

2 在**工作階段**下拉式功能表中，選取**應用程式**以搜尋應用程式工作階段。

3 選取搜尋準則，然後開始搜尋。

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

備註 「上一個工作階段」是工作階段上次連線期間的持續時間 (以毫秒為單位)。如果工作階段目前已連線，則此為處於連線狀態之工作階段的持續時間。如果工作階段目前已中斷連線，則此為其上次連線期間的持續時間。

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

- 確認已建立未驗證存取使用者。如果預設的未驗證使用者是唯一的「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**。

   預設使用者具有尾碼「default」。
5. 按兩下已發佈的應用程式以啟動應用程式。

針對未驗證存取已發佈的應用程式設定登入減速

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

必要條件

- 確認您已為使用者啟用未驗證存取。
- 確認您擁有 Horizon Client 4.9 版或更新版本。

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，然後按一下**編輯**。
4. 按一下**驗證**索引標籤。

5 從**登入減速等級**下拉式功能表中，為未驗證存取登入選取減速等級。

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

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

早於 Horizon Client 4.8 之前的版本不相容。

7 按一下**確定**。

後續步驟

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

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 VMware Horizon 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 VMware Horizon 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 中管理 Cloud Pod 架構》文件。

備註 在遠端網繭中，具有混合登入密碼的未驗證存取使用者無法用作預設的未驗證存取使用者。如果您現有的未驗證存取使用者具有跨網繭使用者的混合登入密碼 (例如，在升級中)，則這些使用者在連線至不同的網繭時，可能會看到 Horizon Client 中的全域應用程式權利不一致。例如，即使建立使用者的網繭具有本機集區，且在連線至某些其他網繭時可能會顯示這些權利，跨網繭使用者仍可能無法看到全域應用程式權利。如果發生這種不一致，請移除這些跨網繭使用者。

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 Connection Server 執行個體進行驗證，以及使用 Kerberos 對遠端桌面平台進行驗證。不需要進一步驗證使用者。

為了支援此功能，使用者認證會儲存在連線伺服器執行個體與用戶端系統上。

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

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

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

  當您選取**接受以目前使用者身分登入**時，您可以啟用下列使用者設定：

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

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

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

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

「以目前使用者身分登入」功能的限制與需求如下：

- 當連線伺服器執行個體上的智慧卡驗證設為「必要」時，連線至連線伺服器執行個體時選取**以目前使用者身分登入**的使用者將會驗證失敗。這些使用者必須在登入連線伺服器時，以其智慧卡和 PIN 碼重新驗證。
- 用戶端登入系統的時間，必須與連線伺服器主機的時間同步。
- 如果在用戶端系統上修改預設的**從網路存取此電腦**使用者權限指派，則必須依照 VMware 知識庫 (KB) 文章 1025691 所述進行修改。

設定 True SSO

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

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

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

這項功能具有下列的限制：

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

您必須執行下列工作，為您的環境設定 True SSO：

1 設定企業憑證授權機構

2 建立與 True SSO 搭配使用的憑證範本

3 安裝和設定註冊伺服器

4 匯出註冊服務用戶端憑證

5 設定 SAML 驗證來與 True SSO 搭配使用

6 設定 Horizon 連線伺服器使用 True SSO

設定企業憑證授權機構

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

必要條件

如果您有現有的 Microsoft 憑證服務執行個體，請考慮是否要為 True SSO 設定子 CA。若要瞭解現有執行個體支援 True SSO 所需的變更，請參閱 VMware 知識庫 (KB) 文章 https://kb.vmware.com/s/article/2149312。

如果您沒有現有的 Microsoft 憑證服務執行個體，請參閱 Microsoft 說明文件以決定要使用的部署類型。若要查看 Microsoft 說明文件，請在 https://docs.microsoft.com 提供的 Microsoft 說明文件中搜尋字串「伺服器憑證部署概觀」。

若要部署新的根憑證授權機構，請在 https://docs.microsoft.com 提供的 Microsoft 說明文件中搜尋字串「安裝憑證授權機構」。

程序

1 開啟命令提示字元並輸入下列命令，以設定非持續性憑證處理的 CA：

```
certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

2 (選擇性) 輸入下列命令，忽略 CA 上的離線 CRL (憑證撤銷清單) 錯誤：

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

備註 若要防止撤銷檢查失敗，通常需進行此設定，因為 True SSO 所使用的根憑證授權機構通常會處於離線狀態。不過，如果您想要讓根憑證授權機構保持在線上狀態，您可以略過此設定。

3 輸入以下命令重新啟動服務：

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

後續步驟

建立憑證範本。請參閱建立與 True SSO 搭配使用的憑證範本 。

建立與 True SSO 搭配使用的憑證範本

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

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

必要條件

- 確認您有企業 CA 可用於建立本程序所述的範本。請參閱設定企業憑證授權機構。

- 確認您已備妥智慧卡驗證所需的 Active Directory。如需詳細資訊，請參閱《Horizon 安裝》文件。
- 建立註冊伺服器在網域和樹系中的安全群組，並將註冊伺服器的電腦帳戶加入該群組。

程序

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

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

b 以滑鼠右鍵按一下**智慧卡登入**範本，然後選取**複製**。

c 針對以下索引標籤進行以下變更：

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

d 按一下 [新範本的內容] 對話方塊中的**確定**。

e 關閉 [憑證範本主控台] 視窗。

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

備註 根據此範本核發憑證的所有憑證授權機構都需要執行此步驟。

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

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

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

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

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

1 按一下**新增**。

2 指定哪些電腦可註冊憑證。

3 針對這些電腦選取適用的核取方塊，給予電腦下列權限：讀取、註冊。

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

備註 根據此範本核發憑證的所有憑證授權機構都需要執行此步驟。

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

後續步驟

建立註冊服務。

安裝和設定註冊伺服器

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

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

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

必要條件

- 建立至少具備 4 GB 記憶體的 Windows Server 2012 R2、Windows Server 2016 或 Windows Server 2019 虛擬機器，或使用主控企業 CA 的虛擬機器。請勿使用做為網域控制站的機器。
- 確認虛擬機器上未安裝其他 Horizon 元件，包括連線伺服器、Horizon Client 或 Horizon Agent。
- 確認虛擬機器屬於 Horizon 部署之 Active Directory 網域的一部分。

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

程序

1 在您計劃用於註冊伺服器的機器上，將憑證嵌入式管理單元新增到 MMC：

a 開啟 MMC 主控台並選取**檔案 > 新增/移除嵌入式管理單元**

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

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

d 在 [新增或移除嵌入式管理單元] 視窗中，按一下**確定**。

2 核發註冊代理程式憑證：

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

b 在憑證註冊精靈中，接受預設值，直到進入 [要求憑證] 頁面。

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

d 接受其他精靈頁面上的預設值，並按一下最後一頁上的**完成**。

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

3 安裝註冊伺服器：

a 從 VMware 下載網站下載 Horizon Connection Server 安裝程式檔案，網址為 https://my.vmware.com/web/vmware/downloads。

在 [桌面平台及終端使用者運算] 下，選取 VMware Horizon 下載，其中包含連線伺服器。

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

c 在 [安裝選項] 頁面上，選取 **Horizon 註冊伺服器**，然後按**下一步**。

d 依照提示完成安裝。

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

後續步驟

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

匯出註冊服務用戶端憑證

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

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

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

必要條件

確認您具有連線伺服器。如需安裝指示，請參閱《Horizon 安裝》文件。如需升級指示，請參閱《Horizon 升級》文件。

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

程序

1 在叢集的其中一部連線伺服器機器上，將憑證嵌入式管理單元新增到 MMC 中：
   a 開啟 MMC 主控台並選取**檔案 > 新增/移除嵌入式管理單元**
   b 在**可用的嵌入式管理單元**下方，選取**憑證**然後按一下**新增**。
   c 在 [憑證嵌入式管理單元] 視窗中，選取**電腦帳戶**、按**下一步**，然後按一下**完成**。
   d 在 [新增或移除嵌入式管理單元] 視窗中，按一下**確定**。
2 在 MMC 主控台的左窗格中，展開 **VMware Horizon 憑證**資料夾並選取**憑證**資料夾。
3 在右窗格中，以滑鼠右鍵按一下具有易記名稱 **vdm.ec** 的憑證檔案，並選取**所有工作 > 匯出**。
4 在憑證匯出精靈中，接受預設值，包括保持選取**否，不要匯出私密金鑰**選項按鈕。
5 當系統提示您命名檔案時，請輸入檔案名稱，例如 **`EnrollClient`** (表示註冊服務用戶端憑證)，接著依照提示完成匯出憑證。

後續步驟

將憑證匯入註冊伺服器。請參閱在註冊伺服器上匯入註冊服務用戶端憑證。

在註冊伺服器上匯入註冊服務用戶端憑證

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

必要條件

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

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

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

程序

1 將適當的憑證檔案複製到註冊伺服器機器。

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

2 在註冊伺服器上，將憑證嵌入式管理單元新增到 MMC：

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

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

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

  d 在 [新增或移除嵌入式管理單元] 視窗中，按一下**確定**。

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

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

5 依照提示進行，並接受預設值以完成憑證的匯入作業。

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

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

後續步驟

設定用來將驗證委派給 VMware Workspace ONE Access 的 SAML 驗證器。請參閱設定 SAML 驗證來與 True SSO 搭配使用。

設定 SAML 驗證來與 True SSO 搭配使用

透過 True SSO 功能，使用者可以使用智慧卡、RADIUS 或 RSA SecurID 驗證登入 VMware Workspace ONE Access，且即使是第一次啟動遠端桌面平台或應用程式，也不會再收到提供 Active Directory 認證的提示。

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

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

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

必要條件

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

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，選取要與 SAML 驗證器建立關聯的伺服器執行個體，然後按一下**編輯**。

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

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

4 按一下**管理 SAML 驗證器**後，按一下**新增**。

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

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

6 按一下**確定**以儲存 SAML 驗證器組態。

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

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

7 在 Horizon Console 儀表板上的 [系統健全狀況] 區段中按一下**檢視**，然後選取**其他元件 > SAML 2.0 驗證器**，接著選取已新增的 SAML 驗證器，並驗證詳細資料。

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

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

後續步驟

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

如需 SAML 驗證運作方式的詳細資訊，請參閱使用 SAML 驗證。

設定 Horizon 連線伺服器使用 True SSO

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

此程序只需在叢集的其中一個連線伺服器上執行。

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

必要條件

- 確認可以具有管理員角色的使用者身分執行命令。您可以使用 Horizon Console，將管理員角色指派給使用者。請參閱第 8 章 設定角色型委派管理。
- 確認您擁有下列伺服器的完整網域名稱 (FQDN)：
  - 連線伺服器
  - 註冊伺服器

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

    如需詳細資訊，請參閱設定企業憑證授權機構。
- 確認您有網域的 Netbios 名稱或 FQDN。
- 請確認您已建立憑證範本。請參閱建立與 True SSO 搭配使用的憑證範本 。

- 確認您已建立 SAML 驗證器以將驗證委派給 VMware Workspace ONE Access。請參閱設定 SAML 驗證來與 True SSO 搭配使用。

程序

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

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

註冊伺服器隨即新增到全域清單中。

2 輸入命令來列出該註冊伺服器的資訊。

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

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

重要 您必須在下一個步驟中指定憑證授權機構的一般名稱。

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

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

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

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

4 輸入命令來探索可使用的 SAML 驗證器。

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

當您使用 Horizon Console 設定 VMware Workspace ONE Access 和連線伺服器之間的 SAML 驗證時，即會建立驗證器。

輸出中會顯示驗證器名稱並顯示是否已啟用 True SSO。

重要 您必須在下一個步驟中指定驗證器名稱。

5 輸入命令啟用驗證器，以使用 True SSO 模式。

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

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

後續步驟

在 Horizon Console 中，確認 True SSO 組態的健全狀況狀態。如需詳細資訊，請參閱使用儀表板來排解與 True SSO 有關的問題。

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

用於設定 True SSO 的命令列參考

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

公用程式的位置

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

語法和驗證

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

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

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

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

`vdmutil` 命令包括指定要用於驗證的使用者名稱、網域和密碼的驗證選項。

表 6-1. vdmutil 命令驗證選項

選項	說明
`--authAs`	Horizon 管理員使用者的名稱。請勿使用 *domain\username* 或使用者主體名稱 (UPN) 格式。
`--authDomain`	`--authAs` 選項中指定之 Horizon 管理員使用者的完整網域名稱或網域的 Netbios 名稱。
`--authPassword`	在 `--authAs` 選項中指定的 Horizon 管理員使用者的密碼。輸入 "*" 而非密碼會使 `vdmutil` 命令提示輸入密碼，並且不會在命令列上的命令歷程記錄中保留敏感的密碼。

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

命令輸出

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

用於管理註冊伺服器的命令

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

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

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

如需驗證選項的詳細資訊，請參閱 用於設定 True SSO 的命令列參考。

表 6-2. 用於管理註冊伺服器的 vdmutil truesso 命令選項

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

用於管理連接器的命令

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

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

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

如需驗證選項的詳細資訊，請參閱 用於設定 True SSO 的命令列參考。

表 6-3. 用於管理連接器的 vdmutil truesso 命令選項

選項	描述
`--create --connector --domain` *domain-fqdn* `--template` *template-name* `--primaryEnrollmentServer` *enroll-server1-fqdn* [`--secondaryEnrollmentServer` *enroll-server2-fqdn*] `--certificateServer` *CA-common-name* `--mode{enabled |disabled}`	為指定網域建立連接器，並設定連接器讓其使用以下設定： ■ *template-name* 是要使用之憑證範本的名稱。 ■ *enroll-server1-fqdn* 是要使用之主要註冊伺服器的 FQDN。 ■ *enroll-server2-fqdn* 是要使用之次要註冊伺服器的 FQDN。此設定為選用。 ■ *CA-common-name* 是要使用之憑證授權單位的一般名稱。這可以是以逗號分隔的 CA 清單。 若要確定特定註冊伺服器可以使用的憑證範本和憑證授權單位，您可以執行 `vdmutil` 命令並搭配 `--truesso --environment --list --enrollmentServer` *enroll-server-fqdn* `--domain` *domain-fqdn* 選項。
`--list --connector`	列出已建立連接器之網域的 FQDN。
`--list --connector --verbose`	列出具有連接器的所有網域，並針對每個連接器提供下列資訊： ■ 主要註冊伺服器 ■ 次要註冊伺服器 (若有) ■ 憑證範本的名稱 ■ 連接器已啟用還是停用 ■ 一個或多個 (若不只一個) 憑證授權單位伺服器的一般名稱
`--edit --connector` *domain-fqdn* [`--template` *template-name*] [`--mode{enabled |disabled]` [`--primaryEnrollmentServer` *enroll-server1-fqdn*] [`--secondaryEnrollmentServer` *enroll-server2-fqdn*] [`--certificateServer` *CA-common-name*]	針對為 *domain-fqdn* 所指定之網域所建立的連接器，可讓您變更下列任何一項設定： ■ *template-name* 是要使用之憑證範本的名稱。 ■ 模式可以是 `enabled` 或 `disabled`。 ■ *enroll-server1-fqdn* 是要使用之主要註冊伺服器的 FQDN。 ■ *enroll-server2-fqdn* 是要使用之次要註冊伺服器的 FQDN。此設定為選用。 ■ *CA-common-name* 是要使用之憑證授權單位的一般名稱。這可以是以逗號分隔的 CA 清單。
`--delete --connector` *domain-fqdn*	刪除已為 *domain-fqdn* 所指定之網域建立的連接器。

用於管理驗證器的命令

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

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

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

如需驗證選項的詳細資訊，請參閱 用於設定 True SSO 的命令列參考。

表 6-4. 用於管理驗證器的 vdmutil truesso 命令選項

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

True SSO 的進階組態設定

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

Horizon Agent 組態設定

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

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

ADMX 檔案可從 `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip` 中取得，而您可以從 VMware 下載網站下載該 zip 檔案，網址為 https://my.vmware.com/web/vmware/downloads。在 [桌面平台及終端使用者運算] 下，選取 VMware Horizon 下載，其中有包含 ZIP 檔案的 GPO 服務包。

表 6-5. 用於在 Horizon Agent 上設定 True SSO 的機碼

機碼	最小值與最大值	說明
Disable True SSO	N/A	將此機碼設定為 **true** 可停用代理程式上的功能。在群組原則中使用此設定可在集區層級停用 True SSO。預設值為 **false**。
Certificate wait timeout	10 - 120	指定憑證到達代理程式的逾時期間，以秒為單位。預設值為 **40**。
Minimum key size	1024 - 8192	金鑰的最小允許大小。預設值為 **1024**，表示依預設，如果金鑰大小小於 1024，則不能使用該金鑰。
All key sizes	N/A	可使用之金鑰大小的逗號分隔清單。最多可指定 5 個大小，例如：**1024,2048,3072,4096**。預設值為 **2048**。
Number of keys to pre-create	1 - 100	在提供遠端桌面平台和主控 Windows 應用程式的 RDS 伺服器上，預先建立的金鑰數目。預設值為 **5**。
Minimum validity period required for a certificate	N/A	重複使用某個憑證來重新連線使用者時所需的最短有效期間 (以分鐘為單位)。預設值為 **5**。

註冊伺服器組態設定

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

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

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

表 6-6. 用於在註冊伺服器上設定 True SSO 的登錄機碼

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

表 6-6. 用於在註冊伺服器上設定 True SSO 的登錄機碼 (續)

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

連線伺服器組態設定

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

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

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

表 6-7. 連線伺服器的進階 True SSO 設定

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

識別沒有 AD UPN 的 AD 使用者

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

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

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

例如，您可以新增下列篩選器：

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

連線伺服器會使用下列預設 LDAP URL 篩選器：

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

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

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

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

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

- "member"
- "memberOf"
- "distinguishedName"
- "telephoneNumber"
- "primaryGroupID"

使用 True SSO 和 Workspace ONE 解除鎖定桌面平台

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

必要條件

- 確認您擁有 VMware Horizon 7.8 版或更新版本。
- 確認您擁有 Windows 版 Horizon Client 5.0 或更新版本。
- 確認您擁有 Workspace ONE 19.03 版或更新版本。

程序

1. 啟用 Workspace ONE，並將其設定為與連線伺服器搭配使用。

   請參閱 Workspace ONE 說明文件網頁上的 Workspace ONE 說明文件。
2. 設定 Horizon Connection Server 以使用 True SSO。

   請參閱設定 Horizon 連線伺服器使用 True SSO。
3. 若要啟動虛擬或已發佈的桌面平台，請在 Workspace ONE 模式下連線至已設定 True SSO 的連線伺服器。請參閱 VMware Horizon Client 說明文件網頁上的 Horizon Client 說明文件。
4. 從 Workspace ONE 入口網站啟動虛擬或已發佈的桌面平台，讓使用者可透過 True SSO 使用單一登入。
5. 鎖定桌面平台。
6. 若要解除鎖定桌面平台，請選取 **VMware True SSO 使用者**，然後按一下**提交**。

   系統會將您重新導向至瀏覽器，以向 Workspace ONE 重新驗證。
7. 輸入已鎖定桌面平台的認證和密碼。

後續步驟

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

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

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

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

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

使用儀表板來排解與 True SSO 有關的問題

您可以使用 Horizon Console 中的系統健全狀況儀表板，以快速查看可能會影響 True SSO 功能的作業問題。

對於使用者而言，若在系統嘗試為使用者登入至遠端桌面平台或應用程式時 True SSO 停止運作，使用者會看見以下訊息：「使用者名稱或密碼不正確。」在按一下**確定**後，使用者就會看見登入畫面。使用者會在 Windows 登入畫面看到額外的動態磚，其標籤為 **VMware SSO 使用者**。若使用者擁有的 Active Directory 認證為具備權利的使用者所屬，使用者就能夠使用 AD 認證來登入。

在 Horizon Console 中，導覽至**監視器 > 儀表板**，接著在**系統健全狀況**窗格中按一下**檢視**，然後按一下 **True SSO** 索引標籤，以查看與 True SSO 有關的項目。

備註 True SSO 功能每分鐘僅提供一次資訊給儀表板。按一下右上角的重新整理圖示，則可立即重新整理資訊。

- 在 **True SSO** 索引標籤上，您可以查看使用 True SSO 的網域清單。

  您可以按一下網域名稱，查看下列資訊：為該網域設定的註冊伺服器清單、企業憑證授權機構清單、正在使用的憑證範本名稱，以及狀態。若有任何問題，[狀態] 欄位會說明問題的內容。

  若要將 [True SSO 網域詳細資料] 對話方塊中顯示的任何組態設定予以變更，請使用 `vdmutil` 命令列介面來編輯 True SSO 連接器。如需詳細資訊，請參閱用於管理連接器的命令。
- 您可以按一下以展開**其他元件 > SAML 2.0 驗證器**，來查看用於將驗證委派給 VMware Workspace ONE Access 執行個體所建立的 SAML 驗證器清單。您可以按一下驗證器名稱來檢查詳細資料和狀態。

備註 為能使用 True SSO，必須啟用 SSO 的全域設定。在 Horizon Console 中，選取**設定 > 全域設定**，並驗證已將 **Single Sign-On (SSO)** 設定為**已啟用**。

表 6-8. 連線伺服器到註冊伺服器連線狀態

狀態文字	說明
無法提取 True SSO 健全狀況資訊。	儀表板無法從連線伺服器執行個體擷取健全狀況資訊。
True SSO 組態服務無法連絡 <FQDN> 註冊伺服器。	在網繭中，系統已選擇其中一個連線伺服器執行個體以將組態資訊傳送給網繭使用的所有註冊伺服器。此連線伺服器執行個體將會每分鐘重新整理一次註冊伺服器組態。若組態工作無法更新註冊伺服器，就會顯示此訊息。如需其他資訊，請參閱註冊伺服器連線的表格。
無法連絡 <FQDN> 註冊伺服器以管理此連線伺服器上的工作階段。	目前的連線伺服器執行個體無法連線至註冊伺服器。系統僅會針對您的瀏覽器所指向的連線伺服器執行個體顯示此狀態。若網繭中有多個連線伺服器執行個體，您需要將瀏覽器變更為指向其他連線伺服器執行個體，才能檢查其狀態。如需其他資訊，請參閱註冊伺服器連線的表格。

表 6-9. 註冊伺服器連線

狀態文字	說明
此網域 <網域名稱> 不存在於 <FQDN> 註冊伺服器上。	已將 True SSO 連接器設定為使用此網域的此註冊伺服器，但尚未將註冊伺服器設定為連線至此網域。若此狀態維持超過一分鐘，您需要檢查目前負責將註冊組態重新整理之連線伺服器執行個體的狀態。
<FQDN> 註冊伺服器對網域 <網域名稱> 的連線仍在建立。	註冊伺服器還無法連線至此網域中的網域控制站。若此狀態維持超過一分鐘，您可能需要驗證從註冊伺服器到網域的名稱解析是否正確，且註冊伺服器和網域之間存在網路連線。
<FQDN> 註冊伺服器與網域 <網域名稱> 的連線正在停止或處於有問題的狀態。	註冊伺服器已連線至網域中的網域控制站，但無法從網域控制站讀取 PKI 資訊。若發生此情形，則表示實際的網域控制站可能有問題。若未正確設定 DNS，也可能發生此問題。請檢查註冊伺服器上的記錄檔，來查看註冊伺服器正嘗試使用哪個網域控制站，並驗證該網域控制站是否可完整運作。
<FQDN> 註冊伺服器尚未從網域控制站讀取註冊內容。	這是過渡狀態，只會在註冊伺服器啟動期間，或在將新網域新增至環境時才會顯示。此狀態持續的時間通常少於一分鐘。若此狀態持續超過一分鐘，則表示網路非常慢，或是發生問題造成網域控制站存取不易。
<FQDN> 註冊伺服器已讀取註冊內容至少一次，但有一段時間無法連線網域控制站。	只要註冊伺服器從網域控制站讀取到 PKI 組態，其便會每兩分鐘輪詢一次看看是否有變更。若已經有一小段時間無法連線到網域控制站 (DC)，就會設定此狀態。無法連絡 DC 通常可能表示註冊伺服器無法偵測到 PKI 組態中有任何變更。只要憑證伺服器仍可存取網域控制站，就仍可核發憑證。
<FQDN> 註冊伺服器已讀取註冊內容至少一次，但有一段時間無法連線網域控制站或存在其他問題。	若註冊伺服器已經很久無法連線到網域控制站，就會顯示此狀態。註冊伺服器接著會嘗試探索此網域的替代網域控制站。若憑證伺服器仍可存取網域控制站，就仍可核發憑證，但若此狀態維持超過一分鐘，則表示註冊伺服器已失去該網域所有網域控制站的存取權，且可能無法再核發憑證。

表 6-10. 註冊憑證狀態

狀態文字	說明
此網域的 <網域名稱> 樹系的有效註冊憑證未安裝在 <FQDN> 註冊伺服器上，或可能已到期	尚未安裝此網域的任何註冊憑證，或是憑證無效或已到期。註冊憑證必須由受樹系信任的企業 CA 核發，且此網域為該樹系的成員。驗證您已完成《Horizon 管理》文件中的步驟，其中說明了在註冊伺服器上安裝註冊憑證的方法。您也可以開啟 MMC、憑證管理嵌入式管理單元，來開啟本機電腦存放區。開啟個人憑證容器，並驗證是否已安裝憑證，以及憑證是否有效。您也可以開啟註冊伺服器記錄檔。註冊伺服器會記錄有關其找到之任何憑證的狀態的其他資訊。

表 6-11. 憑證範本狀態

狀態文字	說明
範本 <名稱> 不存在於 <FQDN> 註冊伺服器網域上。	檢查您指定的範本名稱是否正確。
此範本產生的憑證無法用來登入至 Windows。	此範本未啟用智慧卡的使用以及資料簽署。檢查您指定的範本名稱是否正確。請確認您已完成建立與 True SSO 搭配使用的憑證範本 中所述的步驟。
範本 <名稱> 已啟用智慧卡登入，但無法使用。	此範本已啟用智慧卡登入，但範本無法與 True SSO 搭配使用。檢查您指定的範本名稱是否正確，並確認您已執行建立與 True SSO 搭配使用的憑證範本 中所述的步驟。您也可以檢查註冊伺服器記錄檔，因為它會記錄範本中的哪項設定使得範本無法用於 True SSO。

表 6-12. 憑證伺服器組態狀態

狀態文字	說明
憑證伺服器 <CA 的 CN> 不存在於網域中。	驗證您指定的 CA 名稱是否正確。您必須指定一般名稱 (CN)。
憑證未在 NTAuth (企業) 存放區。	此 CA 並非企業 CA，或其 CA 憑證尚未新增至 NTAUTH 存放區。若此 CA 並非樹系成員，您必須手動將 CA 憑證新增至此樹系的 NTAUTH 存放區。

表 6-13. 憑證伺服器連線狀態

狀態文字	說明
<FQDN> 註冊伺服器未連線至憑證伺服器 <CA 的 CN>。	註冊伺服器未連線至憑證伺服器。若註冊伺服器才剛啟動，或是最近才將 CA 新增至 True SSO 連接器，則此狀態可能是過渡狀態。若狀態維持超過一分鐘，則表示註冊伺服器無法連線至 CA。確認名稱解析可正常運作，且您具備連線至 CA 的網路連線能力，且註冊伺服器的系統帳戶有存取 CA 的權限。
<FQDN> 註冊伺服器已連線至憑證伺服器 <CA 的 CN>，但憑證伺服器處於降級狀態	若 CA 在核發憑證時速度太慢，就會顯示此狀態。若 CA 維持此狀態，請檢查 CA 或 CA 所用之網域控制站的負載。 **備註** 若 CA 已標示為緩慢，該 CA 會維持此狀態，直到已順利完成至少一個憑證要求，且該憑證是在一般時間範圍內核發出去。
<FQDN> 註冊伺服器可以連線憑證伺服器 <CA 的 CN>，但服務無法使用。	若註冊伺服器與 CA 的連線處於作用中狀態，但 CA 無法核發憑證，就會發出此狀態。此狀態通常是過渡狀態。若 CA 沒有很快就變為可用，狀態就會變為已中斷連線。

具備權利的使用者和群組

7

您可以設定權利，來控制您的使用者可以存取哪些遠端桌面平台和應用程式。您可以設定受限制的權利功能，以根據當使用者選取桌面平台時所連線的 Horizon Connection Server 執行個體，來控制桌面平台存取權。您也可以對網路外部的一組使用者限制存取，使其無法在網路內連線至遠端桌面平台和發佈的應用程式。

如需在 Cloud Pod 架構環境中設定全域權利的相關資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

備註 為 Active Directory 中的使用者與群組授權時，您可以在整個目錄或特定網域中搜尋使用者與群組。在 Horizon Console 中，當您導覽至**使用者與群組**，並選取**整個目錄**選項時，連線伺服器會搜尋連線伺服器網域樹系中所有網域間的使用者與群組，並予以計數。任何不屬於連線伺服器網域樹系的網域，都會排除於**整個目錄**選項之外。若要在非連線伺服器網域樹系一部分的網域中搜尋使用者或群組，您必須明確選取這些網域，這同時適用於連線伺服器網域和不受信任的網域。

本章節討論下列主題：

在 Horizon Console 中將權利新增至桌面平台或應用程式集區

使用者必須有權使用桌面平台或應用程式集區，才能存取遠端桌面平台或應用程式。

必要條件

建立桌面平台或應用程式集區。

程序

1 選取桌面平台或應用程式集區。

選項	動作
為桌面平台集區新增權利	在 Horizon Console 中，選取**詳細目錄 > 桌面平台**，然後按一下桌面平台集區的名稱。
為應用程式集區新增權利	在 Horizon Console 中，選取**詳細目錄 > 應用程式**，然後按一下應用程式集區的名稱。

2 從**權利**下拉式功能表中選取**新增權利**。

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

備註 未驗證存取使用者會從篩選搜尋結果中排除。網域本機群組會在篩選後被排除在混合模式網域的搜尋結果之外。如果是在混合模式下設定您的網域，您無法將權利賦予網域本機群組中的使用者。

4 選取您要賦予哪些使用者或群組使用集區中桌面平台或應用程式的權利，並按一下**確定**。

5 按一下**確定**儲存變更。

在 Horizon Console 中從桌面平台或應用程式集區移除權利

您可以將權利從桌面平台或應用程式集區中移除，以防止特定的使用者或群組存取桌面平台或應用程式。

程序

1 選取桌面平台或應用程式集區。

選項	動作
為桌面平台集區新增權利	在 Horizon Console 中，選取**詳細目錄 > 桌面平台**，然後按一下桌面平台集區的名稱。
為應用程式集區新增權利	在 Horizon Console 中，選取**詳細目錄 > 應用程式**，然後按一下應用程式集區的名稱。

2 從**權利**下拉式功能表中選取**移除權利**。

3 選取您要移除其權利的使用者或群組，並按一下**移除**。

4 按一下**確定**儲存變更。

檢閱桌面平台或應用程式集區權利

您可以檢閱使用者或群組具有權利的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**，然後按一下使用者或群組名稱。

2 按一下**權利**索引標籤並檢閱使用者或群組具有權利的桌面平台或應用程式集區。

選項	動作
列出使用者或群組具有權利的桌面平台集區	按一下**桌面平台權利**。
列出使用者或群組具有權利的應用程式集區	按一下**應用程式權利**。

為獲授權集區設定捷徑

您可以為獲授權集區設定捷徑。當具備權利的使用者從 Windows 用戶端連線至連線伺服器執行個體時，Windows 版 Horizon Client 會將這些捷徑放置在使用者用戶端裝置、桌面平台或是兩者上的 [開始] 功能表中。您可以在建立或修改集區時設定捷徑。

您必須在捷徑設定期間選取類別資料夾或根 (/) 資料夾。您可以新增及命名您自己的類別資料夾。您最多可以設定四個資料夾層級。例如，您可以新增名為 Office 的類別資料夾，並為與工作相關的所有應用程式 (例如 Microsoft Office 和 Microsoft PowerPoint) 選取該資料夾。

在 Windows 10 用戶端裝置上，Horizon Client 會將類別資料夾和捷徑置於 [應用程式] 清單中。如果您為捷徑選取了根 (/) 資料夾，則 Horizon Client 會將捷徑直接放置於 [應用程式] 清單中。

在您建立捷徑後， **中集區的**應用程式捷徑 Horizon Console 欄中會出現核取記號。

依預設，Windows 版 Horizon Client 會在具備權利的使用者第一次連線至伺服器時提示他們安裝捷徑。您可以將 Windows 版 Horizon Client 設定為自動安裝捷徑或永不安裝捷徑，只要修改**在 Horizon Server 設定時會自動安裝捷徑**群組原則設定即可。如需詳細資訊，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。

依預設，每當使用者連線至伺服器時，系統會在使用者的 Windows 用戶端裝置上同步化您對捷徑所做的變更。Windows 使用者可以在 Horizon Client 中停用捷徑同步化功能。如需詳細資訊，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。

您也可以在建立或修改全域權利時設定捷徑。如需設定全域權利的相關資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

在 Horizon Console 中為桌面平台集區建立捷徑

您可以在 Horizon Console 中為已授權的桌面平台集區建立捷徑，讓桌面平台集區出現在 Windows 桌面平台、使用者 Windows 用戶端裝置或是兩者上的 [開始] 功能表中。您最多可以為捷徑指定四個類別資料夾層級。您可以在建立桌面平台集區時建立捷徑。您也可以在編輯桌面平台集區時建立和修改捷徑。

必要條件

根據您想要建立的桌面平台集區類型來決定如何進行集區設定。

程序

1 在 Horizon Console 中，按一下**詳細目錄 > 桌面平台**，然後按一下**新增**。

2 在**新增集區**精靈中，選取您要建立的桌面平台集區類型，然後按**下一步**。

3 依照精靈提示進入**桌面平台集區設定**頁面。

4 為桌面平台集區建立捷徑。

a 按一下 [類別資料夾] 的**瀏覽**按鈕。

b 選取**從資料夾清單選取類別資料夾**選項。

c 在**選取類別資料夾或建立新資料夾，以在用戶端裝置中放置此集區的捷徑**文字方塊中輸入資料夾名稱。

資料夾名稱最長可為 64 個字元。若要指定子資料夾，請輸入反斜線 (\) 字元，例如，`dir1\dir2\dir3\dir4`。您最多可以輸入四個資料夾層級。您無法在資料夾名稱的開頭或結尾使用反斜線，也無法組合兩個或多個反斜線。例如，`\dir1`、`dir1\dir2\`、`dir1\\dir2`，以及 `dir1\\\dir2` 皆無效。您無法輸入 Windows 保留關鍵字。

d 選取捷徑建立方法。

您可以選取一或兩個方法。

選項	說明
開始功能表/啟動器	在 Windows 用戶端裝置上建立 Windows [開始] 功能表捷徑。
桌面平台	在 Windows 用戶端裝置的桌面平台上建立捷徑。

e 若要儲存變更，請按一下**提交**。

5 依照精靈提示進入**即將完成**頁面，然後選取**此精靈完成後賦予使用者權利**，然後按一下**提交**。

6 在**新增權利**精靈中按一下**新增**，選取一或多個搜尋準則，接著按一下**尋找**以根據搜尋準則尋找使用者或群組，然後選取您要授權使用集區中桌面平台的使用者或群組，然後按一下**確定**。

針對**桌面平台集區**頁面上的桌面平台集區，核取記號會出現在**應用程式捷徑**資料行中。

在 Horizon Console 中為應用程式集區建立捷徑

您可以在 Horizon Console 中為已授權的應用程式建立捷徑，讓捷徑出現在 Windows 桌面平台、使用者 Windows 用戶端裝置或是兩者上的 [開始] 功能表中。您最多可以為捷徑指定四個類別資料夾層級。您可以在建立應用程式集區時建立捷徑。您也可以在編輯應用程式集區時建立捷徑。

在 Mac 用戶端上，如果您將 Mac 版 Horizon Client 設定為從本機系統上的應用程式資料夾執行已發佈的應用程式，並允許使用伺服器中的資料夾設定，則類別資料夾會出現在 Mac 用戶端裝置上的應用程式資料夾中。如需詳細資訊，請參閱《Mac 版 VMware Horizon Client 安裝和設定指南》文件。

必要條件

請參閱《在 Horizon 中設定已發佈的桌面平台和應用程式》和《在 Horizon 中設定虛擬桌面平台》文件：

- 設定 RDS 主機。
- 建立包含 RDS 主機的伺服器陣列。
- 如果您計劃手動新增應用程式集區，請收集應用程式的相關資訊。
- 將 Windows 版 Horizon Client 安裝在用戶端裝置上。

程序

1 在 Horizon Console 中，按一下**詳細目錄 > 應用程式**，然後按一下**新增**。

2 選取要建立的應用程式集區類型。

選項	說明
手動新增應用程式集區	輸入應用程式的相關資訊。
選取已安裝的應用程式	依名稱、安裝路徑或應用程式類型篩選以尋找應用程式，或從已安裝的應用程式清單中選取。

3 在**新增應用程式集區**精靈中，選取 RDS 伺服器陣列，輸入集區識別碼，以及應用程式的完整路徑名稱。

4 為應用程式集區建立捷徑。

a 按一下 [類別資料夾] 的**瀏覽**按鈕。

b 選取**從資料夾清單選取類別資料夾**選項。

c 從清單選取類別資料夾，或是在**選取類別資料夾或建立新資料夾，以在用戶端裝置中放置此集區的捷徑**文字方塊中輸入資料夾名稱。

資料夾名稱最長可為 64 個字元。若要指定子資料夾，請輸入反斜線 (\) 字元，例如，`dir1\dir2\dir3\dir4`。您最多可以輸入四個資料夾層級。您無法在資料夾名稱的開頭或結尾使用反斜線，也無法組合兩個或多個反斜線。例如，`\dir1`、`dir1\dir2\`、`dir1\\dir2`，以及 `dir1\\\dir2` 皆無效。您無法輸入 Windows 保留關鍵字。

備註 如果需要，非 Windows 用戶端可以將反斜線轉換為正斜線。

d 選取捷徑建立方法。

您可以選取一或兩個方法。

選項	說明
開始功能表/啟動器	在 Windows 用戶端裝置上建立 Windows [開始] 功能表捷徑。
桌面平台	在 Windows 用戶端裝置的桌面平台上建立捷徑。

e 若要儲存變更，請按一下**提交**。

5 選取**此精靈完成後賦予使用者權利**。

6 在**新增權利**精靈中按一下**新增**，選取一或多個搜尋準則，接著按一下**尋找**以根據搜尋準則尋找使用者或群組，然後選取您要授權使用集區中應用程式的使用者或群組，然後按一下**確定**。

針對**應用程式集區**頁面上的應用程式集區，核取記號會出現在**應用程式捷徑**資料行中。

實作桌面平台集區、已發佈的桌面平台和應用程式集區的用戶端限制

您可以限制僅特定用戶端電腦可存取授權的桌面平台集區、已發佈的桌面平台和應用程式集區。若要限制存取，您必須在 Active Directory 安全群組中新增可存取桌面平台集區、已發佈的桌面平台或應用程式的用戶端電腦名稱，然後再授權此群組使用集區。Active Directory 安全群組可包含屬於任何 AD 組織單位 (OU) 或預設電腦容器的用戶端電腦。

用戶端限制功能有某些需求和限制。

- 當您建立或修改桌面平台集區、已發佈的桌面平台或應用程式集區時，必須啟用用戶端限制原則。依預設會停用用戶端限制原則。如需已發佈的桌面平台集區和應用程式集區設定的相關資訊，請參閱《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。如需即時複製、完整複製和手動桌面平台集區設定的相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》文件。
- 當您建立或修改桌面平台集區、已發佈的桌面平台或應用程式集區的權利時，必須新增 Active Directory 安全群組，並使其包含可存取桌面平台集區、已發佈的桌面平台或應用程式集區的用戶端電腦名稱。
- 用戶端限制功能僅允許特定用戶端電腦存取桌面平台集區、已發佈的桌面平台和應用程式集區。它不會讓使用者存取未授權的桌面平台和應用程式集區。例如，若使用者未包含在應用程式集區權利中 (無論是作為使用者或使用者群組的成員)，即便該使用者的用戶端電腦隸屬於有權使用應用程式集區的 AD 安全群組，該使用者仍無法存取應用程式集區。
- 只有 Windows 用戶端電腦可支援用戶端限制功能。
- 為桌面平台集區、已發佈的桌面平台或應用程式集區啟用用戶端限制原則時，非 Windows 用戶端和 HTML Access 用戶端將無法從受限制的集區啟動桌面平台或應用程式。
- 用戶端限制功能只會限制來自 Windows 用戶端的新工作階段。此功能不會限制來自先前使用者工作階段的現有應用程式工作階段連線。
- 使用 Windows 版 Horizon Client 時，屬於 Active Directory 安全群組的用戶端電腦必須位於預設 AD 位置「CN=Computers」。

設定角色型委派管理

8

VMware Horizon 環境中的一個金鑰管理工作會用來決定誰可以使用 Horizon Console，以及這些使用者有權執行哪些工作。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。如果管理員沒有修改全域原則的權限，則當管理員登入 Horizon Console 時，全域原則頁面上的按鈕會停用，且無法修改全域原則。

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，以建立自己的自訂角色。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，您可能需要將角色套用至存取群組和/或聯盟存取群組 (僅限 Cloud Pod 架構環境)。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。

如需關於如何設定聯盟存取群組以委派全域權利管理的資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

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。

在 Cloud Pod 架構環境中，您可以設定聯盟存取群組以委派全域權利的管理。如需相關資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

- 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 8-1. 不同存取群組的不同管理員顯示此類組態的範例。

表 8-1. 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 8-2. 同一個存取群組的不同管理員顯示此類組態的範例。

表 8-2. 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。

瞭解權限和存取群組

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 8-3. [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 8-4. [存取群組] 索引標籤上針對 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 8-3. [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 8-3. [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，則 [繼承] 資料行中會顯示核取記號。

下表顯示當您選取「詳細目錄管理員」角色時，表 8-3. [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 8-5. 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

如需關於權限和聯盟存取群組的資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

管理管理員

擁有管理角色和權限之權限的使用者可以使用 Horizon Console 來新增和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 VMware Horizon 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。

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或伺服器陣列的管理員，請建立存取群組並將桌面平台集區或伺服器陣列移至該存取群組。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，然後按一下**確定**。

您可以按 Ctrl 或 Shift 鍵，選取多個使用者和群組。

5 按**下一步**，然後選取角色。

存取群組資料行表示角色是否套用至存取群組。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。

備註 即使服務台管理員和服務桌面平台管理員 (唯讀) 角色顯示為適用於存取群組，管理員仍僅能新增至根存取群組。

選項	動作
您選取的角色會套用至存取群組	按**下一步**，然後選取一或多個存取群組。
您要將角色套用至所有存取群組	按**下一步**，然後選取根存取群組。

如需聯盟存取群組的相關資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

6 按一下**完成**即可建立管理員使用者或群組。

結果

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。如果本機網繭是 Cloud Pod 架構環境的一部分，則超級管理員也擁有根聯盟存取群組的管理員角色。

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**。

結果

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 Cloud Pod 架構環境中，您可以新增、刪除和檢閱聯盟存取群組的權限。如需詳細資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

- 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。

在 Cloud Pod 架構環境中，您可以新增聯盟存取群組的權限。如需詳細資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

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。只有適用於存取群組的角色可供選取。 **備註** 即使服務台管理員和服務台管理員 (唯讀) 角色顯示為適用於存取群組，仍僅能在根存取群組上建立權限。

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。

在 Cloud Pod 架構環境中，您可以刪除聯盟存取群組的權限。如需詳細資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

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。

在 Cloud Pod 架構環境中，您可以檢閱聯盟存取群組的權限。如需詳細資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

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。

如需在 Cloud Pod 架構環境中管理和檢閱聯盟存取群組的相關資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

- 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、應用程式集區和伺服器陣列。

- 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**。

結果

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、應用程式集區和伺服器陣列。

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** 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

  如果自訂角色沒有任何權限，您可以移除該自訂角色。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。

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。

在 Cloud Pod 架構環境中，如果網繭是網繭聯盟的一部分，則角色更新時，系統可能會自動新增或刪除權限。如需詳細資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。當連線伺服器執行個體不是網繭聯盟的一部分時，系統不會自動建立或刪除權限。

必要條件

自行熟悉可用於建立自訂角色的管理員權限。請參閱 預先定義的角色和權限。

程序

1 在 Horizon 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

如果自訂角色沒有任何權限，您可以移除該自訂角色。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**。

預先定義的角色或具有權限的自訂角色無法使用**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至存取群組。在 Cloud Pod 架構環境中，僅包含全域權限的角色也無法套用至聯盟存取群組。

- 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。在 Cloud Pod 架構環境中，包含某些物件特定權限的角色適用於聯盟存取群組。

- 權限範圍

  管理員權限可以限制在範圍內。

- 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至存取群組或聯盟存取群組。聯盟存取群組僅可在 Cloud Pod 架構環境中使用。

表 8-6. Horizon Console 中預先定義的角色

角色	使用者功能	套用至存取群組	套用至聯盟存取群組
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。 管理員在存取群組或聯盟存取群組上具有此角色時，只能管理該存取群組或聯盟存取群組中的詳細目錄物件。 **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： ■ 使用 `vdmadmin`、`vdmimport` 以及 `lmvutil` 命令。	是	是
管理員 (唯讀)	■ 檢視 (但無法修改) 全域設定與詳細目錄物件。 ■ 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。 管理員在存取群組或聯盟存取群組上具有此角色時，只能檢視該存取群組或聯盟存取群組中的詳細目錄物件。	是	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) 全域原則及組態設定，但管理員角色與權限除外。	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	是
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	是

表 8-6. Horizon Console 中預先定義的角色 (續)

角色	使用者功能	套用至存取群組	套用至聯盟存取群組
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。 ■ 在自動集區和伺服器陣列上執行維護作業。 ■ 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。	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。	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至存取群組。在 Cloud Pod 架構環境中，僅包含全域權限的角色也無法套用至聯盟存取群組。

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 8-7. 全域權限

權限	使用者功能	預先定義的角色
收集作業記錄	收集集區、伺服器陣列或連線伺服器的作業記錄。	
主控台互動	登入並使用 Horizon Console。 **備註** VMware Horizon 會自動將**主控台互動**權限新增至新角色。此權限不會顯示在 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** VMware Horizon 會自動將**直接互動**權限新增至新角色。此權限不會顯示在 Horizon Console 的全域權限清單中。	管理員 管理員 (唯讀)
管理存取群組	新增和移除存取群組以及 Cloud Pod 架構 環境中的聯盟存取群組。	管理員 本機管理員
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。在 Cloud Pod 架構環境中，包含某些物件特定權限的角色適用於聯盟存取群組。

下表說明物件特定的權限。預先定義的角色管理員、本機管理員、服務台管理員和詳細目錄管理員包含這些權限。

表 8-8. 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, 應用程式集區, 伺服器陣列
賦予桌面平台和應用程式集區權利	新增和移除使用者權利。	桌面平台集區, 應用程式集區
管理 Cloud Pod 架構	設定和管理 Cloud Pod 架構環境，包括全域權利、站台、主站台和網繭。 若要管理 Cloud Pod 架構組態，管理員必須擁有根聯盟存取群組的此權限。	桌面平台集區、應用程式集區、伺服器陣列、機器、全域權利
管理全域工作階段	在 Cloud Pod 架構環境中管理全域工作階段。	全域工作階段
在自動桌面平台和伺服器陣列上管理維護作業	排程推送映像、排程維護以及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
管理服務台 (唯讀)	Horizon Help Desk Tool 的唯讀存取權、全域設定和全域原則，除了管理員和角色及 Cloud Pod 架構組態。	桌面平台集區、應用程式集區、伺服器陣列、機器、工作階段、全域權利、全域工作階段

權限範圍

管理員權限可以限制在範圍內。

範圍	說明
全域	具有此範圍的權限具有下列特性： ■ 不適用於存取群組。 ■ 不適用於 Cloud Pod 架構環境中的聯盟存取群組。 ■ 僅為本機網繭叢集的一部分。 ■ 與適用於本機網繭叢集的全域設定有關。
聯盟群組	具有此範圍的權限適用於 Cloud Pod 架構環境中的聯盟存取群組。
存取群組、聯盟群組	具有此範圍的權限適用於存取群組以及 Cloud Pod 架構環境中的聯盟存取群組。
本機網繭	具有此範圍的權限適用於存取群組，且將包全域權限。
全部	具有此範圍的權限適用於存取群組以及 Cloud Pod 架構環境中的聯盟存取群組，且將包含全域權限。

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 8-9. 內部權限

權限	說明	預先定義的角色
本機 (唯讀)	授與對詳細目錄物件、全域設定和全域原則的唯讀存取權。	管理員、管理員 (唯讀)、本機管理員、本機管理員 (唯讀)
完整 (唯讀)	授與所有設定的唯讀存取權。	管理員、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。	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)
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。	管理員、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)

管理完整複製和即時複製所需的最低 vCenter Server 權限

管理員必須具有特定的 vCenter Server 權限，才能管理完整複製和即時複製。

Horizon 管理員必須在 vCenter Server 中建立自訂角色，並選取下列權限，才能管理完整複製。下表列出在 vCenter Server 中執行基本作業所需的最低 vCenter Server 權限。

表 8-10. 完整複製權限

工作	vCenter Server 上針對完整複製的權限群組
■ 建立資料夾 ■ 刪除資料夾	**資料夾**
配置空間	**資料存放區**

表 8-10. 完整複製權限 (續)

工作	vCenter Server 上針對完整複製的權限群組
■ 組態 ■ 新增或移除裝置 ■ 進階 ■ 修改裝置設定 ■ 互動 ■ 關閉電源 ■ 開啟電源 ■ 重設 ■ 暫止 ■ 執行抹除或縮小作業 ■ 詳細目錄 ■ 新建 ■ 從現有資源建立 ■ 移除 ■ 正在佈建 ■ 自訂 ■ 部署範本 ■ 讀取自訂規格 ■ 複製範本 ■ 複製虛擬機器	**虛擬機器**
將虛擬機器指派給資源集區	**資源**
作為 vCenter Server (即使未使用 View 儲存加速器仍需要)	**全域**
(全部 – 如果您使用虛擬磁碟區的 Virtual SAN 資料存放區)	**設定檔驅動儲存區**
實作 View 儲存加速器以啟用 ESXi 主機快取：設定進階設定。	**主機**

表 8-11. 即時複製權限

工作	vCenter Server 上針對即時複製的權限群組
■ 建立資料夾 ■ 刪除資料夾	**資料夾**
■ 配置空間 ■ 瀏覽資料存放區	**資料存放區**

表 8-11. 即時複製權限 (續)

工作	vCenter Server 上針對即時複製的權限群組
■ 組態 ■ 新增或移除裝置 ■ 進階 ■ 修改裝置設定 ■ 變更 CPU 計數 ■ 變更記憶體 ■ 變更設定 ■ 變更資源 ■ 設定主機 USB 裝置 ■ 設定原始裝置 ■ 設定 mangedby ■ 顯示連線設定 ■ 擴充虛擬磁碟 ■ 查詢 Fault Tolerance 相容性 ■ 查詢未知檔案 ■ 從路徑重新載入 ■ 移除磁碟 ■ 重新命名 ■ 重設客體資訊 ■ 設定註解 ■ 切換磁碟變更追蹤 ■ 切換分支父系 ■ 升級虛擬機器相容性 ■ 互動 ■ 關閉電源 ■ 開啟電源 ■ 重設 ■ 暫止 ■ 執行抹除或縮小作業 ■ 連線裝置 ■ 詳細目錄 ■ 新建 ■ 從現有資源建立 ■ 移除 ■ 移動 ■ 登錄 ■ 解除登錄 ■ 快照管理 ■ 建立快照 ■ 移除快照 ■ 重新命名快照 ■ 還原快照	**虛擬機器**

表 8-11. 即時複製權限 (續)

工作	vCenter Server 上針對即時複製的權限群組
■ 正在佈建 ■ 自訂 ■ 部署範本 ■ 讀取自訂規格 ■ 複製範本 ■ 複製虛擬機器 ■ 允許磁碟存取	
將虛擬機器指派給資源集區	**資源**
■ 當做 vCenter Server 使用 ■ 啟用方法 ■ 停用方法 ■ 管理自訂屬性 ■ 設定自訂屬性	**全域**
■ 詳細目錄：修改叢集 ■ 實作 View 儲存加速器：設定進階設定	**主機**
指派	**網路**
(全部 – 如果您使用虛擬磁碟區的 Virtual SAN 資料存放區)	**設定檔驅動儲存區**
搭配使用 vTPM 與即時複製： ■ 複製 ■ 解密 ■ 直接存取 ■ 加密 ■ 管理 KMS ■ 移轉 ■ 登錄主機	**密碼編譯作業**

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。部分作業除了需要正在操作的物件存取權之外，還需要根存取群組或 Cloud Pod 架構 環境中聯盟根存取群組的權限。

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 8-12. 集區管理工作與權限

工作	所需的權限
啟用或停用伺服器陣列、桌面平台或應用程式集區。	**啟用伺服器陣列、桌面平台和應用程式集區**
將使用者權利賦予或取消賦予給集區。	**賦予桌面平台和應用程式集區權利**
新增集區。	**管理伺服器陣列及桌面平台和應用程式集區** **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。
排程推送映像、排程維護以及變更桌面平台集區和伺服器陣列的預設映像。	**在自動桌面平台和伺服器陣列上管理維護作業**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 8-13. 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**全域管理員視圖**頁面上管理管理員。

表 8-14. 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**
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**

用來管理遠端存取和未驗證存取的權限和角色

若要存取**使用者與群組**頁面上的**遠端存取**和**未驗證存取**索引標籤，管理員必須具有「全域組態及原則管理員 (唯讀)」角色。若要在這些索引標籤上執行作業，管理員必須具有「全域組態及原則管理員」角色，或至少具有**管理全域組態和原則**權限。

如果已啟用 Cloud Pod 架構功能，則為了在**未驗證存取**索引標籤上執行作業，管理員必須額外具有根聯盟存取群組上的**管理 Cloud Pod 架構**權限。

管理 Cloud Pod 架構環境的權限

管理員必須具有根聯盟存取群組上的**管理 Cloud Pod 架構**權限，才能在 Horizon Console 中或使用 `lmvutil` 命令管理 Cloud Pod 架構環境。

若要新增全域權利，管理員必須具有任何聯盟存取群組上的管理 Cloud Pod 架構權限。若要修改全域權利資料或刪除全域權利，管理員必須具有全域權利聯盟存取群組上的管理 Cloud Pod 架構權限。如果管理員具有自訂存取群組上的管理 Cloud Pod 架構權限，則列出的本機集區以及可新增的本機集區將根據自訂存取群組上詳細目錄權限授與的可見度而定。

如需詳細資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

管理存取群組和聯盟存取群組的權限

管理員必須具有根存取群組的**管理存取群組**權限，才能在 Horizon Console 中新增和移除存取群組。在 Cloud Pod 架構環境中，管理員必須具有**管理存取群組**權限，才能在 Horizon Console 中新增和移除聯盟存取群組。如果在自訂存取群組上授與特殊權限的權限，則權限僅會授與對**管理員**頁面的唯讀存取權。

管理工作階段和全域工作階段的權限

需要特定權限才能在 Horizon Console 中檢視工作階段和全域工作階段。

下表說明每種工作階段類型所需的權限。

工作階段類型	工作階段說明	所需的權限
SA	在資源上主控的工作階段不會用於 Cloud Pod 架構環境中的網繭聯盟。	在桌面平台集區或伺服器陣列的存取群組上具有存取群組、本機網繭或全部範圍的任何權限。
SB	在本機網繭叢集資源上主控，但由 Cloud Pod 架構環境中網繭聯盟所提供的工作階段。	在桌面平台集區或伺服器陣列的存取群組上具有存取群組、本機網繭或全部範圍的任何權限，或在全域權利存取群組上**管理全域工作階段**或**管理服務台 (唯讀)**。
SC	在遠端網繭叢集資源上主控，但由 Cloud Pod 架構環境中網繭聯盟提供的工作階段。	全域權利存取群組上的**管理全域工作階段**或**管理服務台 (唯讀)**。

SA 和 SB 類型的工作階段會在工作階段頁面上列出，不包含 Horizon Console 中的**搜尋工作階段**。下表說明在這些頁面上管理工作階段所需的權限。

作業	所需的權限
傳送訊息	在桌面平台集區或伺服器陣列的存取群組上**管理工作階段**。
中斷連線	在桌面平台集區或伺服器陣列的存取群組上**管理工作階段**。
登出	在桌面平台集區或伺服器陣列的存取群組上**管理工作階段**。
重新啟動桌面平台	在桌面平台集區或伺服器陣列的存取群組上**管理重新啟動作業**。
重設虛擬機器	在桌面平台集區或伺服器陣列的存取群組上**管理重新啟動作業**。

所有類型的工作階段都會在 Horizon Console 中的**搜尋工作階段**頁面上列出。下表說明管理這些工作階段所需的權限。

工作階段類型	作業	所需的權限
SA	傳送訊息、中斷連線、登出	在桌面平台集區或伺服器陣列的存取群組上**管理工作階段**。
SA	重新啟動桌面平台、重設虛擬機器	在桌面平台集區或伺服器陣列的存取群組上**管理重新啟動作業**。
SB	傳送訊息、中斷連線、登出	在工作階段任何全域權利的聯盟存取群組上**管理全域工作階段**，或在桌面平台集區或伺服器陣列的存取群組上**管理工作階段**。
SB	重新啟動桌面平台、重設虛擬機器	在工作階段任何全域權利的聯盟存取群組上**管理全域工作階段**，或在桌面平台集區或伺服器陣列的存取群組上**管理重新啟動作業**。
SC	任何作業	在工作階段任何全域權利的聯盟存取群組上**管理全域工作階段**。

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。

備註 Horizon Help Desk Tool 會根據管理委派支援聯盟存取群組，但不支援以存取群組為基礎的管理委派。若要存取 Horizon Help Desk Tool，您必須擁有根存取群組和任何聯盟存取群組的管理服務台 (唯讀) 權限。

表 8-15. 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。	在根存取群組上**管理服務台 (唯讀)**。
管理全域工作階段。	**管理全域工作階段**必須存在於全域工作階段所存在全域權利的任何聯盟存取群組上。
可以登入 Horizon Console。	**主控台互動** **備註** **主控台互動**會自動新增至新角色，且不會出現在 Horizon Console 中的全域權限清單中。
對來自本機網繭叢集之桌面平台或應用程式集區服務中的工作階段執行所有機器和工作階段相關命令。	在根存取群組上**管理機器**。
傳送訊息、中斷連線，以及登出從本機網繭叢集之桌面平台或應用程式集區服務的工作階段。	在根存取群組上**管理工作階段**。
傳送全域工作階段的訊息、中斷連線和登出作業。	**管理全域工作階段**必須存在於全域工作階段所存在全域權利的任何聯盟存取群組上。如果在本機網繭叢集的桌面平台集區或伺服器陣列上主控工作階段，則即使該工作階段是由全域權利所提供，若管理員在根存取群組上具有**管理工作階段**，則仍會允許該作業。
重新啟動和重設全域工作階段的作業。	**管理全域工作階段**必須存在於全域工作階段所存在全域權利的任何聯盟存取群組上。如果在本機網繭叢集的桌面平台集區或伺服器陣列上主控工作階段，則即使該工作階段是由全域權利所提供，若管理員在根存取群組上具有**管理重新啟動作業**，則仍會允許該作業。
重設並重新啟動本機工作階段的作業。	在根存取群組上**管理重新啟動作業**。
遠端協助作業。	在根存取群組上**遠端協助**。
結束遠端處理程序和應用程式。	在根存取群組上**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。	在根聯盟存取群組上**管理全域工作階段**。如果本機網繭不是網繭聯盟的一部分，則管理員必須在根存取群組上具有**管理全域工作階段**。此外，管理員必須在根存取群組上具有**管理重新啟動作業**、**管理工作階段**、**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**

一般管理工作和命令的權限和角色

管理員必須具備某些權限或角色，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和角色。

表 8-16. 一般管理工作和命令的權限和角色

工作	必要的權限或角色
新增或刪除存取群組或聯盟存取群組	**管理存取群組**
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 Agent 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** Horizon 會自動將**直接互動**權限新增至新角色。此權限不會顯示在 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 VMware Horizon 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 VMware Horizon 權限的使用者。
- 將擁有 VMware Horizon 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 VMware Horizon 組態設定的管理員。
- 建立聯盟存取群組以區隔敏感全域權利。將這些聯盟存取群組委派給限定人數的一組使用者管理。

設定 Horizon 元件的群組原則 9

您可以使用群組原則設定來設定特定 Horizon 元件的行為。

如需關於安裝 Horizon ADMX 範本檔案和編輯群組原則設定的一般資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

本章節討論下列主題：

VMware View Server 組態 ADMX 範本設定

VMware View Server 組態 ADMX (`vdm_server.admx`) 範本檔包含與連線伺服器相關的原則設定。

下表說明 VMware View Server 連線伺服器組態 ADMX 範本檔中的每個原則設定。此範本僅包含「電腦組態」設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View Server 組態**資料夾中。

表 9-1. VMware View Server 組態範本設定

設定	內容
Enumerate Forest Trust Child Domains	決定是否列舉伺服器所在網域所信任的每個網域。為了建立完整的信任鏈結，也要列舉每個信任的網域所信任的網域，在搜尋到所有信任的網域之前，程序才會以遞迴的方式繼續。此資訊會傳遞到連線伺服器，以確保用戶端在登入時可以使用所有信任的網域。 此內容依預設為啟用。停用時，只會列舉直接信任的網域，因此不會與遠端網域控制站建立連線。 **備註** 在網域關係複雜的環境 (例如，在其樹系中使用網域間具備信任的多個樹系結構的環境) 中，此程序可能需要幾分鐘才能完成。
Recursive Enumeration of Trusted Domains	決定是否列舉伺服器所在網域所信任的每個網域。若要建立完整的信任鏈結，也要列舉每個信任的網域所信任的網域，在搜尋到所有信任的網域之前，程序才會以遞迴的方式繼續。此資訊會傳遞到連線伺服器，讓用戶端在登入時，可以使用所有信任的網域。 此設定依預設為啟用。停用此設定時，只會列舉直接信任的網域，因此不會與遠端網域控制站建立連線。 在網域關係複雜的環境 (例如，在其樹系中使用網域間具備信任的多個樹系結構的環境) 中，此程序可能需要幾分鐘才能完成。
Windows Password Authentication Mode	選取 Windows 密碼驗證模式。 ■ KerberosOnly。使用 Kerberos 進行驗證。 ■ KerberosWithFallbackToNTLM。使用 Kerberos 進行驗證，但失敗時則退回使用 NTLM。 ■ Legacy。使用 NTLM 進行驗證，但失敗時則退回使用 Kerberos。用於支援舊版 NT 網域控制站。 預設為 KerberosOnly。

VMware View 一般組態 ADMX 範本設定

VMware View 一般組態 ADMX (vdm_common.admx) 範本檔包含所有 Horizon 元件通用的原則設定。這些範本僅包含「電腦組態」設定。

記錄組態設定

下表說明 VMware View 一般組態 ADMX 範本檔中的記錄組態原則設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View 一般組態 > 記錄組態**資料夾中。

表 9-2. VMware View 一般組態範本：記錄組態設定

設定	內容
Log Directory	指定記錄檔目錄的完整路徑。如果無法寫入該位置，則會使用預設位置。若是用戶端記錄檔，則會建立具有用戶端名稱的額外目錄。
Maximum debug log size in Megabytes	指定偵錯記錄可到達的大小上限 (MB)，記錄檔超過此上限後會關閉並建立新的記錄檔。
Maximum number of debug logs	指定要保留在系統上的偵錯記錄檔數目上限。當記錄檔到達其大小上限時，則不會新增其他項目而且會建立新的記錄檔。當先前的記錄檔數目到達此值時，則會刪除最舊的記錄檔。

表 9-2. VMware View 一般組態範本：記錄組態設定 (續)

設定	內容
Number of days to keep production logs	指定記錄檔保留在系統上的天數。若未設定值，會套用預設值且記錄檔會保留 7 天。
Send logs to a Syslog server	允許將 Horizon Server 記錄傳送至 Syslog 伺服器，例如 VMware vCenter Log Insight。將從設定此 GPO 之 OU 或網域中的所有 Horizon Server 中傳送記錄。 透過在 GPO 中 (連結至包含桌面平台的 OU) 啟用此設定，您可以將 Horizon Agent 記錄傳送到 Syslog 伺服器。 若要傳送記錄資料至 Syslog 伺服器，請啟用此設定，並指定記錄層級和伺服器完整網域名稱 (FQDN) 或 IP 位址。若不想使用預設連接埠 514，則可以指定替代連接埠。指定時請以分隔號 (|) 分隔每個元素。使用下列語法： `Log Level|Server FQDN or IP [|Port number(514 default)]` 例如：`Debug|192.0.2.2` **重要** Syslog 資料會在未經軟體式加密的情況下傳送到網路上。由於 Horizon Server 記錄可能包含敏感資料，因此請避免在不安全的網路上傳送 Syslog 資料。如果可能，請使用連結層安全性 (例如 IPsec) 來避免此資料可能會在網路上遭到監控的情況。

效能警示設定

表 9-3. VMware View 一般組態範本：效能警示設定會說明 VMware View 一般組態 ADMX 範本檔中的效能警示設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View 一般組態 > 效能警示**資料夾中。

表 9-3. VMware View 一般組態範本：效能警示設定

設定	內容
CPU and Memory Sampling Interval in Seconds	指定 CPU 和記憶體輪詢間隔 CPU。取樣間隔低，會導致輸出到記錄的層級變高。
Overall CPU usage percentage to issue log info	指定記錄系統總體 CPU 使用率的臨界值。當有多個處理器可使用時，此百分比表示合併的使用率。
Overall memory usage percentage to issue log info	指定記錄總體已認可系統記憶體使用率的臨界值。已認可系統記憶體是指已由處理器配置，而且作業系統已在分頁檔中認可實體記憶體或分頁插槽的記憶體。
Process CPU usage percentage to issue log info	指定記錄任何個別程序之 CPU 使用率的臨界值。

表 9-3. VMware View 一般組態範本：效能警示設定 (續)

設定	內容
Process memory usage percentage to issue log info	指定記錄任何個別程序之記憶體使用率的臨界值。
Process to check, comma separated name list allowing wild cards and exclusion	指定對應於要檢查之一或多個程序名稱的查詢清單 (以逗號分隔)。您可以在每個查詢內使用萬用字元來篩選清單。 ■ 星號 (*) 可符合零或更多字元。 ■ 問號 (?) 可符合單一字元。 ■ 驚嘆號 (!) 放在查詢開頭會排除該查詢所產生的任何結果。 例如，下列查詢會選取開頭為 **ws** 的所有程序，並排除結尾為 **sys** 的所有程序： **'! *sys,ws*'**

備註 效能警示設定僅適用於連線伺服器和 Horizon Agent 系統。這些設定不適用於 Horizon Client 系統。

安全性設定

表 9-4. VMware View 一般組態範本：安全性設定會說明 VMware View 一般組態 ADMX 範本檔中的安全性設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View 一般組態 > 安全性設定**資料夾中。

表 9-4. VMware View 一般組態範本：安全性設定

設定	內容
Only use cached revocation URLS	憑證撤銷檢查只能存取快取 URL。 如果未設定，預設為 false。
Revocation URL check timeout milliseconds	所有撤銷 URL 線擷取的累積逾時 (以毫秒為單位)。 未設定或將值設為 0 代表使用 Microsoft 預設處理。
Type of certificate revocation check	選取要完成的憑證撤銷檢查類型： ■ 無 ■ EndCertificateOnly ■ WholeChain ■ WholeChain 預設值為 WholeChainButRoot。

一般設定

表 9-5. VMware View 一般組態範本：一般設定會說明 VMware View 一般組態 ADMX 範本檔中的一般設定。所有設定都位在 [群組原則管理編輯器] 的**電腦組態 > 原則 > 系統管理範本 > VMware View 一般組態**資料夾中。

表 9-5. VMware View 一般組態範本：一般設定

設定	內容
Configure dump count on program error	限制可建立的傾印檔案數量。將**所要建立的傾印檔案上限**設定為任何數值。該值會依每個處理程序以及每個使用者的每個處理程序生效。如果將值設定為 0，則不會建立任何傾印檔案。如果未進行此設定，則可建立的傾印檔案數量為 128 個或無限制，取決於產生傾印檔案的處理程序。
Configure dump type on program error	指定可建立的傾印檔案大小。有效值如下： ■ **完整** - 產生完整的傾印。傾印包含處理程序的完整記憶體。完整傾印的大小相對較大。 ■ **小型** - 傾印包含產生堆疊追蹤的足夠資訊，並讓您能夠執行基本疑難排解步驟。傾印不包含完整記憶體，因此您無法擷取某些物件或物件名稱的相關資訊。傾印大小相對較小。 如果未進行此設定，則依預設會建立完整傾印。
Disk threshold for log and events in Megabytes	指定記錄和事件的最小剩餘磁碟空間臨界值。若未指定值，則預設值為 200。當達到指定的值時，事件記錄會停止。
Enable extended logging	決定記錄檔中是否包含追蹤和偵錯事件。
Override the default View Windows event generation	支援下列值： ■ 0 - 僅針對 View 事件產生事件記錄項目 (記錄訊息不會產生事件記錄項目) ■ 1 - 在 4.5 (及更早版本) 相容模式中產生事件記錄項目。標準 View 事件不會產生事件記錄項目。系統僅根據記錄檔文字產生事件記錄項目。 ■ 2 - 在 4.5 (及更早版本) 相容模式中產生事件記錄項目，同時包含 View 事件。

維護 Horizon 元件

10

若要讓 VMware Horizon 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 VMware Horizon 組態資料
- 還原 Horizon 連線伺服器組態資料

備份和還原 VMware Horizon 組態資料

您可以在 Horizon Console 中排程或執行自動備份，以備份您的 VMware Horizon 組態資料。您可以手動匯入已備份的 Horizon LDAP 檔案，以還原您的 VMware Horizon 組態。

您可以使用備份及還原功能，保留和移轉 VMware Horizon 組態資料。

備份 Horizon Connection Server 資料

完成連線伺服器的初始組態後，應該排程 VMware Horizon 組態資料的定期備份。您可以藉由使用 Horizon Console 來保留您的 VMware Horizon 資料。

VMware Horizon 會將 LDAP 連線伺服器組態資料儲存在 Horizon LDAP 存放庫中。

當您使用 Horizon Console 執行備份時，VMware Horizon 會備份 Horizon LDAP 組態資料。Horizon LDAP 資料會以加密的 LDAP 資料交換格式 (LDIF) 匯出。如需 Horizon LDAP 的說明，請參閱《Horizon 架構規劃》文件中的〈Horizon LDAP〉。

有幾種方法可執行備份。

- 排程自動備份或使用 **中的**立即備份 Horizon Console 功能，立即起始備份。請參閱排程 VMware Horizon 組態備份。
- 使用 `vdmexport` 公用程式，手動匯出 Horizon 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 Horizon 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` 工具僅能備份 Horizon 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 VMware Horizon 組態資料：

- VMware Horizon 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。VMware Horizon 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。

排程 VMware Horizon 組態備份

您可以排程定期備份 VMware Horizon 組態資料。VMware Horizon 會備份 Horizon 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 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 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 組態備份設定

VMware Horizon 可以定期備份您的連線伺服器資料。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 10-1. Horizon 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，VMware Horizon 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，VMware Horizon 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

您可以藉由匯出 Horizon 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 Horizon LDAP 組態資料匯出至加密的 LDIF 檔案。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。

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 Horizon LDAP 組態。已清理的組態資料中會遺失密碼與其他重大資訊。

結果

如需 vdmexport 命令的詳細資訊，請參閱匯出 LDAP 組態資料。

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。

如需關於匯入 LDIF 檔案的詳細資訊，請參閱還原 Horizon 連線伺服器組態資料。

還原 Horizon 連線伺服器組態資料

您可以手動還原由 VMware Horizon 備份的連線伺服器 LDAP 組態檔。

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 Connection Server 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 Horizon LDAP 存放庫。

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 VMware Horizon 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 VMware Horizon 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 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 Horizon LDAP 存放庫中。

如果您使用 Horizon Console 或預設的 vdmexport 命令備份您的 Horizon 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 Horizon LDAP 存放庫中會遺失重大的組態資訊。

如需備份 Horizon LDAP 存放庫的相關資訊，請參閱備份 Horizon Connection Server 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 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。

2 安裝一個連線伺服器執行個體。

3 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。

4 按一下**開始 > 命令提示字元**。

5 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。

6 匯入解密的 LDIF 檔案來還原 Horizon LDAP 組態。

  指定 `-f` 選項並搭配解密的 LDIF 檔案。例如：

7 解除安裝連線伺服器。

  僅解除安裝套件 VMware Horizon 連線伺服器。

8 重新安裝連線伺服器。

9 登入 Horizon Console 並驗證組態是否正確。

10 重新安裝複寫伺服器執行個體。

結果

`vdmimport` 命令會使用 LDIF 檔案中的組態資料更新連線伺服器中的 Horizon LDAP 存放庫。如需關於 `vdmimport` 命令的詳細資訊，請參閱《Horizon 安裝》文件。

備註 請確定要還原的組態與 vCenter Server 已知的虛擬機器相符。

設定 Kiosk 模式下的用戶端

11

您可以設定可從 VMware Horizon 取得桌面平台存取權的自動用戶端。

Kiosk 模式下的用戶端為精簡型用戶端或鎖定電腦，可執行 Horizon Client 以連線至連線伺服器執行個體，並啟動工作階段。使用者通常不需要登入即可存取用戶端裝置，雖然已發佈的桌面平台可能會要求其為某些應用程式提供驗證資訊。範例應用程式包括醫療資料輸入工作站、航空公司登機站、客戶自助服務點，以及可供大眾存取的資訊終端機。

您應確保桌面平台應用程式針對安全交易實施驗證機制、實體網路能防止竄改和窺探，以及和網路連線的所有裝置均受信任。

Kiosk 模式下的用戶端支援用於遠端存取的標準功能，例如將 USB 裝置自動重新導向至遠端工作階段，以及依據位置列印。

VMware Horizon 會使用彈性驗證功能，驗證 Kiosk 模式下的用戶端裝置，而非使用者。您可以設定連線伺服器執行個體，對符合以下條件的用戶端進行驗證：以 MAC 位址，或開頭是「custom-」字元或您在 ADAM 定義之替代首碼字串的使用者名稱，來自我識別的用戶端。若您將用戶端設定為具有自動產生的密碼，則無需指定密碼，即可在裝置上執行 Horizon Client。若您設定明確的密碼，則必須將此密碼指定至 Horizon Client。由於您通常會從指令碼執行 Horizon Client，而且密碼會以純文字形式顯示，您應該防範未獲授權的使用者讀取指令碼。

只有經您啟用、可對 Kiosk 模式下的用戶端進行驗證的連線伺服器執行個體，才能從符合以下條件的帳戶接受連線：開頭是「cm-」字元且後跟 MAC 位址，或開頭是「custom-」或您所定義的替代字串的帳戶。Horizon Client 不允許手動輸入採用這些形式的使用者名稱。

最佳做法是使用專用連線伺服器執行個體來處理 Kiosk 模式下的用戶端，並在 Active Directory 中為這些用戶端的帳戶建立專用的組織單位和群組。此做法不僅能隔開這些系統，避免未經授權的入侵，也能更方便設定和管理用戶端。

本章節討論下列主題：

將用戶端設定為 Kiosk 模式

若要設定 Active Directory 及 VMware Horizon 以支援處於 Kiosk 模式的用戶端，必須依序執行幾項工作。

必要條件

確認您有執行組態工作所需的權限。

- Active Directory 中用來變更網域使用者和群組帳戶的**網域管理**或**帳戶操作員**憑證。
- **管理員**、**詳細目錄管理員**，或使用 Horizon Console 將遠端桌面平台授權給使用者或群組的同等角色。
- **管理員**或執行 `vdmadmin` 命令的同等角色。

程序

1 針對 Kiosk 模式中的用戶端備妥 Active Directory 與 VMware Horizon

您必須設定 Active Directory 接受您建立用來驗證用戶端裝置的帳戶。只要您建立一個群組，您也必須將該群組授權給用戶端存取的桌面平台集區。您也可以備妥用戶端使用的桌面平台集區。

2 為 Kiosk 模式下的用戶端設定預設值

您可以使用 `vdmadmin` 命令，在 Active Directory 中為 kiosk 模式下的用戶端，設定組織單位、密碼到期和群組成員資格的預設值。

3 顯示用戶端裝置的 MAC 位址

如果您要建立以其 MAC 位址為基礎的用戶端帳戶，可以使用 Horizon Client 來搜索用戶端裝置的 MAC 位址。

4 在 Kiosk 模式下新增用戶端的帳戶

您可以使用 `vdmadmin` 命令，將用戶端的帳戶新增至連線伺服器群組的組態。新增用戶端後，啟用用戶端驗證的連線伺服器執行個體即可與該用戶端搭配使用。您也可以更新用戶端的組態，或從系統移除用戶端的帳戶。

5 以 Kiosk 模式啟用用戶端驗證

您可以使用 `vdmadmin` 命令，對嘗試透過連線伺服器執行個體連線至其遠端桌面平台的用戶端啟用驗證。

6 驗證 Kiosk 模式下的用戶端組態

您可以使用 `vdmadmin` 命令來顯示處於 Kiosk 模式的用戶端相關資訊，以及設定為驗證這類用戶端之連線伺服器執行個體的相關資訊。

7 在 Kiosk 模式下從用戶端連線至遠端桌面平台

您可以從命令列執行用戶端，或使用指令碼將用戶端連線至遠端工作階段。

針對 Kiosk 模式中的用戶端備妥 Active Directory 與 VMware Horizon

您必須設定 Active Directory 接受您建立用來驗證用戶端裝置的帳戶。只要您建立一個群組，您也必須將該群組授權給用戶端存取的桌面平台集區。您也可以備妥用戶端使用的桌面平台集區。

最佳做法是，建立另外的組織單位與群組，以減少您管理 Kiosk 模式用戶端的工作。您可以為不屬於任何群組的用戶端新增個別帳戶，但如果您設定的用戶端數量較多，這會產生很大的額外管理負荷。

程序

1 在 Active Directory 中，建立另外的組織單位與群組以搭配 Kiosk 模式的用戶端使用。

您必須為該群組指定 Windows 2000 之前的名稱。您使用此名稱來識別 `vdmadmin` 命令群組。

2 為客體虛擬機器建立映像或範本。

您可使用由 vCenter Server 管理的虛擬機器作為自動集區的範本、作為即時複製桌面平台集區的父系，或作為手動桌面平台集區中的虛擬機器。您也可以在客體作業系統上安裝與設定應用程式。

3 設定客體作業系統，讓用戶端保持自動時不會被鎖定。

VMware Horizon 會為在 Kiosk 模式中連線的用戶端隱藏登入前訊息。如果您需要事件去解除鎖定畫面並顯示訊息，您可以在客體作業系統上設定適當的應用程式。

4 在 Horizon Console 中，建立用戶端將使用的桌面平台集區，並將群組授權給此集區。

例如，您可以選擇建立浮動指派、即時複製桌面平台集區成為最適合您用戶端應用程式需求的桌面平台集區。

重要 請勿將用戶端或群組授權給多個桌面平台集區。如果您這麼做，VMware Horizon 會從獲得用戶端授權的集區隨機指派遠端桌面平台，並產生警告事件。

5 如果您要為用戶端啟用依據位置列印，請設定以下 Active Directory 群組原則設定：`AutoConnect Location-based Printing for VMware View`，此設定位於電腦設定下 `Software Settings` 資料夾中的 Microsoft 群組原則物件編輯器內。

6 設定其他您必須最佳化的原則，並保護用戶端的遠端桌面平台。

例如，您可能要覆寫當本機 USB 裝置啟動或插入時連線至遠端桌面平台的原則。依預設，Windows 版 Horizon Client 會為 Kiosk 模式中的用戶端啟用這些原則。

範例： 針對 Kiosk 模式中的用戶端備妥 Active Directory

公司內部網路的網域為 MYORG，其組織單位的辨別名稱為 OU=myorg-ou,DC=myorg,DC=com。在 Active Directory 中，您可以建立辨別名稱為 OU=kiosk-ou,DC=myorg,DC=com 的組織單位 kiosk-ou，並建立群組 kc-grp 以搭配 Kiosk 模式中的用戶端使用。

後續步驟

設定用戶端的預設值。

為 Kiosk 模式下的用戶端設定預設值

您可以使用 `vdmadmin` 命令，在 Active Directory 中為 kiosk 模式下的用戶端，設定組織單位、密碼到期和群組成員資格的預設值。

在用戶端將用來連線至其已發佈桌面平台的連線伺服器執行個體所在的群組中，您必須對其中一個連線伺服器執行個體執行 `vdmadmin` 命令。

設定密碼到期日和 Active Directory 群組成員資格的預設值後，這些設定都會由群組中的所有連線伺服器執行個體共用。

程序

- 為用戶端設定預設值。

```
            vdmadmin
            -Q
            -clientauth
            -setdefaults [-b authentication_arguments] [-ouDN] [ -expirepassword |
-noexpirepassword ] [-groupgroup_name | -nogroup]
```

選項	說明
-expirepassword	指定用戶端帳戶的密碼到期時間，與連線伺服器群組相同。如果未定義群組的到期時間，則密碼不會到期。
-group ***group_name***	對要新增用戶端帳戶的預設群組指定名稱。必須指定群組的名稱作為 Active Directory 的 Windows 2000 以前版本群組名稱。
-noexpirepassword	指定用戶端帳戶密碼不會過期。
-nogroup	清除預設群組的設定。
-ou ***DN***	指定預設組織單位 (用戶端帳戶即新增至其中) 的辨別名稱。 例如：OU=kiosk-ou,DC=myorg,DC=com **備註** 您不能使用此命令來變更組織單位的組態。

此命令會為連線伺服器群組中的用戶端更新預設值。

範例： 為 Kiosk 模式下的用戶端設定預設值

設定組織單位、密碼到期日及用戶端群組成員資格的預設值。

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword
-group kc-grp
```

後續步驟

為使用 MAC 位址來進行驗證的用戶端裝置找出其 MAC 位址。

顯示用戶端裝置的 MAC 位址

如果您要建立以其 MAC 位址為基礎的用戶端帳戶，可以使用 Horizon Client 來搜索用戶端裝置的 MAC 位址。

必要條件

在用戶端的主控台上登入。

程序

- 若要顯示 MAC 位址，請輸入適用於您平台的命令。

選項	動作
Windows	輸入 **C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo** 用戶端會使用您為其設定的預設連線伺服器執行個體。如果您未設定預設值，用戶端會提示您設定該值。 該命令會顯示 IP 位址、MAC 位址及用戶端裝置的機器名稱。
Linux	輸入 **vmware-view --printEnvironmentInfo -s *connection_server*** 您必須指定連線伺服器執行個體的 IP 位址或 FQDN，用戶端會用它來連線至桌面平台。 該命令會顯示 IP 位址、MAC 位址、機器名稱、網域、名稱、任何登入使用者的名稱和網域，以及用戶端裝置的時區。

後續步驟

新增用戶端帳戶。

在 Kiosk 模式下新增用戶端的帳戶

您可以使用 `vdmadmin` 命令，將用戶端的帳戶新增至連線伺服器群組的組態。新增用戶端後，啟用用戶端驗證的連線伺服器執行個體即可與該用戶端搭配使用。您也可以更新用戶端的組態，或從系統移除用戶端的帳戶。

在用戶端將用來連線至其已發佈桌面平台的連線伺服器執行個體所在的群組中，您必須對其中一個連線伺服器執行個體執行 `vdmadmin` 命令。

在 Kiosk 模式下新增用戶端時，VMware Horizon 將在 Active Directory 中建立用戶端的使用者帳戶。如果指定用戶端的名稱，此名稱的開頭必須是已辨識的首碼字串，例如 "custom-"，或者是在 ADAM 中定義的備用首碼字串，而且長度不可超過 20 個字元。如果您不指定用戶端的名稱，VMware Horizon 將從您為用戶端裝置所指定的 MAC 位址產生名稱。例如，如果 MAC 位址為 00:10:db:ee:76:80，則對應的帳戶名稱為 cm 00_10_db_ee_76_80。您僅能將這些帳戶用於您啟用以驗證用戶端的連線伺服器執行個體。

重要 請勿將一個指定的名稱用於多個用戶端裝置。未來版本可能不支援此組態。

程序

- 使用 -domain 及 -clientid 選項執行 vdmadmin 命令，指定用戶端的網域，以及用戶端的名稱或 MAC 位址。

```
vdmadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name -clientid
client_id [-password "password" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword]
[-group group_name | -nogroup] [-description "description_text"]
```

選項	說明
-clientid *client_id*	指定用戶端的名稱或 MAC 位址。
-description "*description_text*"	為 Active Directory 中的用戶端裝置建立帳戶的說明。
-domain *domain_name*	指定用戶端的網域。
-expirepassword	指定用戶端帳戶上密碼的到期時間與連線伺服器群組相同。如果未定義群組的到期時間，則密碼不會到期。
-genpassword	產生用戶端帳戶的密碼。如果您未指定 -password 或 -genpassword，這將是預設行為。 產生的密碼有 16 個字元，至少包含一個大寫字母、一個小寫字母、一個符號及一個數字，並且可包含重複的字元。如果需要強度更高的密碼，可使用 -password 選項指定密碼。
-group *group_name*	指定新增用戶端帳戶的群組名稱。必須指定群組的名稱作為 Active Directory 的 Windows 2000 以前版本群組名稱。如果您先前已設定預設群組，用戶端帳戶將新增至此群組。
-noexpirepassword	指定用戶端帳戶的密碼不到期。
-nogroup	指定用戶端帳戶不新增至預設群組。
-ou *DN*	指定新增用戶端帳戶的組織單位辨別名稱。 例如：OU=kiosk-ou,DC=myorg,DC=com
-password "*password*"	指定用戶端帳戶的明確密碼。

此命令將為指定網域及群組 (如果有) 中的用戶端建立 Active Directory 中的使用者帳戶。

範例： 新增用戶端的帳戶

使用 group kc-grp 的預設設定，將以用戶端 MAC 位址指定的用戶端帳戶新增至 MYORG 網域。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

使用自動產生的密碼，將以用戶端 MAC 位址指定的用戶端帳戶新增至 MYORG 網域。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword
```

新增具名用戶端的帳戶，並指定用於用戶端的密碼。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou
"OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

使用自動產生的密碼，新增具名用戶端的帳戶。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Kiosk11 -genpassword -ou
"OU=kiosk-ou,DC=myorg,DC=com" -description "Kiosk 11"
```

後續步驟

啟用用戶端驗證。

以 Kiosk 模式啟用用戶端驗證

您可以使用 `vdmadmin` 命令，對嘗試透過連線伺服器執行個體連線至其遠端桌面平台的用戶端啟用驗證。

在用戶端將用來連線至其遠端桌面平台的連線伺服器執行個體所在的群組中，您必須對其中一個連線伺服器執行個體執行 `vdmadmin` 命令。

雖然您啟用個別連線伺服器執行個體的驗證，但群組中所有連線伺服器執行個體會共用用戶端驗證的所有其他設定。您只需要為用戶端新增帳戶一次。在連線伺服器群組中，任何已啟用的連線伺服器執行個體都可以驗證用戶端。

如果計劃在 RDS 主機上搭配使用 Kiosk 模式和工作階段型桌面平台，您還必須將使用者帳戶新增至遠端桌面平台使用者群組。

程序

1 啟用連線伺服器執行個體上的用戶端驗證。

```
vdmadmin -Q -enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

選項	說明
-requirepassword	指定您需要用戶端提供密碼。 **重要** 如果您指定此選項，則連線伺服器執行個體無法驗證已自動產生密碼的用戶端。如果您變更連線伺服器執行個體的組態以指定此選項，則這類用戶端無法驗證自己，它們會失敗且出現以下錯誤訊息：使用者名稱不明或密碼不正確。
-s *connection_server*	指定要啟用用戶端驗證的連線伺服器執行個體的 NetBIOS 名稱。

此命令讓指定的連線伺服器執行個體能夠驗證用戶端。

2 如果已發佈的桌面平台是由 Microsoft RDS 主機提供的，請登入 RDS 主機並將使用者帳戶新增至遠端桌面平台使用者群組。

例如，在 VMware Horizon Server 上，將使用者帳戶 `custom-11` 授權給 RDS 主機上的工作階段型桌面平台。您必須登入 RDS 主機，透過前往**控制台 > 系統及安全性 > 系統 > 遠端設定 > 選取使用者 > 新增**，將使用者 `custom-11` 新增至遠端桌面平台使用者群組。

範例： 以 Kiosk 模式啟用用戶端驗證

啟用連線伺服器執行個體 csvr-2 的用戶端驗證。具有自動產生密碼的用戶端不須提供密碼即可自行驗證。

```
vdmadmin -Q -enable -s csvr-2
```

啟用連線伺服器執行個體 csvr-3 的用戶端驗證，需要用戶端對 Horizon Client 指定其密碼。具有自動產生密碼的用戶端無法自行驗證。

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

後續步驟

驗證連線伺服器執行個體與用戶端的組態。

驗證 Kiosk 模式下的用戶端組態

您可以使用 `vdmadmin` 命令來顯示處於 Kiosk 模式的用戶端相關資訊，以及設定為驗證這類用戶端之連線伺服器執行個體的相關資訊。

在用戶端將用來連線至其遠端桌面平台的連線伺服器執行個體所在的群組中，您必須對其中一個連線伺服器執行個體執行 `vdmadmin` 命令。

程序

- 顯示處於 Kiosk 模式之用戶端及用戶端驗證的相關資訊。

  ```
  vdmadmin
  -Q
  -clientauth
  -list [-b authentication_arguments] [-xml]
  ```

  此命令會顯示處於 Kiosk 模式之用戶端的相關資訊，以及已啟用用戶端驗證之連線伺服器執行個體的相關資訊。

範例： 顯示處於 Kiosk 模式之用戶端的相關資訊

以文字格式顯示用戶端的相關資訊。用戶端 cm-00_0c_29_0d_a3_e6 具有自動產生的密碼，且不需要使用者或應用程式指令碼對 Horizon Client 指定此密碼。用戶端 cm-00_22_19_12_6d_cf 擁有明確指定的密碼，且需要使用者提供。連線伺服器執行個體 CONSVR2 接受來自具有自動產生密碼之用戶端的驗證要求。CONSVR1 不接受 Kiosk 模式下用戶端的驗證要求。

```
C:\ vdmadmin -Q -clientauth -list
Client Authentication User List
================================
GUID              : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID          : cm-00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID          : cm-00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
```

```
Common Name                    : CONSVR1
Client Authentication Enabled : false
Password Required              : false

Common Name                    : CONSVR2
Client Authentication Enabled : true
Password Required              : false
```

後續步驟

確認用戶端可以連線至其遠端桌面平台。

在 Kiosk 模式下從用戶端連線至遠端桌面平台

您可以從命令列執行用戶端，或使用指令碼將用戶端連線至遠端工作階段。

您通常都是使用命令指令碼在已部署的用戶端裝置上執行 Horizon Client。

備註 在 Windows 或 Mac 用戶端上，依預設，當遠端桌面工作階段啟動時，如果其他應用程式或服務正在使用用戶端上的 USB 裝置，則不會自動轉送這些裝置。在所有用戶端上，預設不會轉送人機介面裝置 (HID) 和智慧卡讀卡機。

程序

- 若要連線至遠端工作階段，請輸入適用於您平台的命令。

選項	說明
Windows	輸入 **C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL *connection_server*] [-userName *user_name*] [-password *password*]** **-password***password* 指定用戶端帳戶的密碼。如果您已定義帳戶的密碼，則必須指定此密碼。 **-serverURL***connection_server* 指定連線伺服器執行個體的 IP 位址或 FQDN，Horizon Client 會使用該執行個體來連線至其遠端桌面平台。如果您不指定用戶端將用來連線至遠端桌面平台的連線伺服器執行個體的 IP 位址或 FQDN，則該用戶端就會使用您為其設定的預設連線伺服器執行個體。 **-userName***user_name* 指定用戶端帳戶的名稱。如果您不想讓用戶端使用 MAC 位址，而是使用以識別的首碼字串為開頭 (例如 "custom-") 的帳戶名稱來自行驗證，則必須指定此名稱。
Linux	輸入 **vmware-view --unattended -s *connection_server* [--once] [-u *user_name*] [-p *password*]** **--once** 指定您不想讓 Horizon Client 在發生錯誤時重新嘗試連線。 **重要** 您通常應指定此選項，並使用結束碼來處理錯誤。否則，可能會難以遠端結束 `vmware-view` 程序。 **-p***password* 指定用戶端帳戶的密碼。如果您已定義帳戶的密碼，則必須指定此密碼。 **-s***connection_server* 指定連線伺服器執行個體的 IP 位址或 FQDN，用戶端會使用該執行個體連線至其桌面平台。 **-u***user_name* 指定用戶端帳戶的名稱。如果您不想讓用戶端使用 MAC 位址，而是使用以識別的首碼字串為開頭 (例如 "custom-") 的帳戶名稱來自行驗證，則必須指定此名稱。

如果伺服器驗證 Kiosk 用戶端，且遠端桌面平台可用，則命令就會啟動遠端工作階段。

範例： 在 Kiosk 模式下於用戶端上執行 Horizon Client

在帳戶名稱採用本身 MAC 位址並具有自動產生的密碼的 Windows 用戶端上，執行 Horizon Client。

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended
-serverURL consvr2.myorg.com
```

使用指派的名稱和密碼在 Linux 用戶端上執行 Horizon Client。

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

Horizon Console 中的監控和疑難排解

12

您可以使用多種程序來監控、診斷和修正使用 VMware Horizon 時可能會遇到的問題。您可以使用 Horizon Help Desk Tool 進行監控和疑難排解、使用其他疑難排解程序調查及更正問題，或從「VMware 技術支援」獲得協助。

如需關於疑難排解桌面平台和桌面平台集區的相關資訊，請參閱《在 Horizon Console 中設定虛擬桌面平台》文件。

本章節討論下列主題：

在 Horizon Console 中使用 Horizon Help Desk Tool

Horizon Help Desk Tool 是一個可用來取得 VMware Horizon 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：

- VMware Horizon 的 Horizon Enterprise 版授權或 Horizon Apps Advanced 版授權。若要確認您具有正確的授權，請參閱《Horizon 管理》中的 < 在 Horizon Console 中變更產品授權金鑰或授權模式 > 。
- 用來儲存 VMware Horizon 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 安裝》文件。
- 用來登入 Horizon Help Desk Tool 的服務台管理員角色或服務台管理員 (唯讀) 角色。如需這些角色的詳細資訊，請參閱《Horizon 管理》中的 < 服務台工具工作的權限 > 。
- 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}
  ```

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 12-1. 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 12-2. 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。
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 12-3. 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 12-4. 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、虛擬或已發佈的桌面平台，以及 CPU 和記憶體的詳細資料。

Horizon Client

根據 Horizon Client 的類型顯示資訊，並且包含諸如使用者名稱、Horizon Client 的版本、用戶端機器的 IP 位址，以及用戶端機器的作業系統等詳細資料。

備註 如果您已升級 Horizon Agent，則必須也將 Horizon Client 升級至最新版本。否則將不會顯示 Horizon Client 的版本。如需關於升級 Horizon Client 的詳細資訊，請參閱《Horizon 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 12-5. 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。

表 12-5. 虛擬機器詳細資料 (續)

選項	說明
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。
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 12-6. 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)。

表 12-6. PCoIP 顯示通訊協定詳細資料 (續)

選項	說明
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 12-7. 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 12-8. 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 12-9. 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 12-10. 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 12-11. 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 12-12. 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

若要避免捲動整個工作階段程序清單，您可以在搜尋篩選器文字方塊中輸入程序名稱，以依名稱搜尋工作階段程序。

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 12-13. 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

若要避免捲動整個應用程式清單，您可以在搜尋篩選器文字方塊中輸入應用程式名稱，以依名稱搜尋應用程式。

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 12-14. 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 VMware 登入監視器

VMware 登入監視器可監控 Windows 使用者登入，以及報告效能度量，目的在於協助管理員、支援人員和開發人員疑難排解緩慢的登入效能。

度量包括登入時間、登入指令碼時間、CPU/記憶體使用量，以及網路連線速度。登入監視器也可以從其他 VMware 產品接收度量以提供登入程序的更多資訊。

支援的平台

登入監視器支援與 Horizon Agent 相同的 Windows 平台。

重要功能

登入監視器提供下列功能：

- 安裝為 Horizon Agent 的一部分。若要啟動服務，請參閱 KB 57051。
- 與 Horizon Help Desk Tool 計時分析工具整合。系統會彙總與登入相關的度量，並傳送至 Horizon Agent 事件資料庫。
- 可讓客戶將記錄上傳至檔案伺服器以便於存取。
- 與其他 VMware 產品整合，例如 App Volumes、UEM，以及將登入相關事件傳送至登入監視器的 Horizon Agent。登入監視器會在事件發生時記錄事件，以顯示登入流程中的事件及其持續多久。
- 監控相同機器上的並行登入。

記錄

登入監視器會寫入服務狀態訊息和使用者工作階段的記錄檔。依預設，所有記錄檔皆會寫入至 `C:\ProgramData\VMware\VMware Logon Monitor\Logs`。

- 主要記錄檔：主要的記錄檔 `vmlm.txt` 包含在監控登入之前和之後所傳入 vmlm 服務和工作階段事件的所有狀態訊息。檢查此記錄檔以判斷登入監視器是否正確執行。
- 工作階段記錄檔：工作階段記錄檔包含與使用者登入工作階段相關的所有事件。事件會在登入開始時在此記錄檔中啟動，且僅適用於單一使用者工作階段。記錄檔結尾處會寫入摘要，以提供最重要度量的概觀。檢查此記錄檔可疑難排解緩慢的登入。登入完成時，不會有進一步的事件寫入至工作階段記錄檔。

登入監視器度量

登入監視器會計算登入、群組原則、使用者設定檔，以及效能的相關度量。這些度量可提供系統管理員關於登入期間使用者系統的詳細檢視，以協助判斷效能瓶頸的根本原因。

表 12-15. 登入監視器度量

度量	參數	說明
登入時間	■ 啟動 ■ End ■ 時間總計	度量包括客體上登入開始的時間、登入完成的時間，以及載入設定檔和桌面平台顯示的時間，以及在客體上處理登入所耗費的時間總計。排除在客體外所耗費的任何時間。
工作階段開始到登入開始時間	時間總計	從 Windows 建立使用者工作階段直到登入開始之間的時間。
設定檔同步時間	時間總計	Windows 於登入期間耗費在協調使用者設定檔的時間。

表 12-15. 登入監視器度量 (續)

度量	參數	說明
殼層載入	■ 啟動 ■ End ■ 時間總計	Windows 會提供使用者殼層載入的開始時間。結束時間為總管視窗建立的時間。
登入到登錄區載入時間	時間總計	此度量提供從登入開始到載入使用者登錄區的時間總計。
Windows 資料夾重新導向	■ 啟動 ■ End ■ 時間總計	與 Windows 資料夾重新導向開始且完整套用時間，以及啟用 Windows 資料夾重新導向時間總計相關的度量。第一次套用資料夾重新導向，或如果正在將新檔案上傳到重新導向共用，則這個時間可能會很高。
群組原則時間	■ 使用者群組原則套用時間 ■ 電腦群組原則套用時間	與將群組原則套用至客體相關的度量，包括套用使用者群組原則和電腦群組原則所耗費的時間。
設定檔度量	■ 設定檔類型：本機、漫遊、暫存 ■ 設定檔大小：檔案數目、資料夾總數、MB 總計	與使用者設定檔相關的度量，指出使用者設定檔類型及其是否儲存在本機電腦、中央設定檔存放區上或在登出後刪除。 設定檔大小包含檔案數目、資料夾總數和使用者設定檔大小總計 (以 MB 為單位) 的度量。
設定檔大小分佈	■ 介於 0 到 1 MB 之間的檔案數目 ■ 介於 1 MB 到 10 MB 之間的檔案數目 ■ 介於 10 MB 到 100 MB 之間的檔案數目 ■ 介於 100 MB 到 1 GB 之間的檔案數目 ■ 介於 1 GB 到 10 GB 之間的檔案數目	使用者設定檔中各種大小範圍的檔案數目計數。
登入期間啟動的處理程序	■ 名稱 ■ 處理程序識別碼 ■ 父處理程序識別碼 ■ 工作階段識別碼	系統會針對每個處理程序從工作階段開始直到登入完成記錄這些值。
群組原則登入指令碼時間	時間總計	與執行群組原則登入指令碼報告執行群組原則登入指令碼所花費時間總計相關的度量。
群組原則 PowerShell 指令檔時間	時間總計	與執行群組原則 PowerShell 指令檔相關的度量，指出執行群組原則 PowerShell 指令檔所耗費的時間。
記憶體使用量	■ 可用的位元組：最小、最大、平均 ■ 已認可位元組：最小、最大、平均 ■ 分頁集區：最小、最大、平均	登入期間與記憶體使用量相關的 WMI 度量。取樣會在登入完成之前持續進行。預設為停用狀態。
CPU 使用率	■ 閒置 CPU：最小、最大、平均 ■ 使用者 CPU：最小、最大、平均 ■ 核心 CPU：最小、最大、平均	登入期間與 CPU 使用率相關的 WMI 度量。取樣會在登入完成之前持續進行。預設為停用狀態。

表 12-15. 登入監視器度量 (續)

度量	參數	說明
登入指令碼是否已同步？		報告群組原則登入指令碼會與登入同步執行或非同步執行。
網路連線狀態	■ 已捨棄 ■ 已還原	報告網路連線是否運作中或是中斷連線。
群組原則軟體安裝	■ 非同步：True/False ■ 錯誤碼 ■ 時間總計	與群組原則軟體安裝相關的度量，指出安裝與登入同步或非同步、安裝成功或失敗，以及使用群組原則安裝軟體所耗費的時間總計。
設定檔磁碟區的磁碟使用量	■ 使用者可用的磁碟空間 ■ 可用磁碟空間 ■ 磁碟空間總計	與存放使用者設定檔之磁碟區上磁碟使用量相關的度量。
網域控制站探索	■ 錯誤碼 ■ 時間總計	網域控制站相關度量。錯誤碼指出網域控制站是否出現故障。
估計的網路頻寬	頻寬	從事件識別碼 5327 所收集的值。
網路連線詳細資料	■ 頻寬 ■ 慢速連結臨界值 ■ 偵測到的慢速連結：True/False	從事件識別碼 5314 所收集的值。
影響登入時間的設定	■ 電腦\系統管理範本\登入\永遠在電腦啟動與登入時等待網路啟動 ■ 電腦\系統管理範本\登入\當使用者登入時執行這些程式 ■ 電腦\系統管理範本\使用者設定檔\等待漫遊使用者設定檔 ■ 電腦\系統管理範本\使用者設定檔\如果使用者有漫遊設定檔或遠端主目錄，設定網路的最大等待時間 ■ 電腦\系統管理範本\群組原則\設定登入指令碼延遲 ■ 使用者\系統管理範本\系統\登入\當使用者登入時執行這些程式 ■ 使用者\系統管理範本\系統\使用者設定檔\指定網路目錄僅在登入/登出時同步	
來自 Horizon Agent 的度量 (App Volumes)		與登入監視器進行互動的 VMware 產品會在登入監視器記錄檔中報告自訂度量。這些度量可協助判斷這些產品是否可能對登入時間造成負面影響。

登入監視器組態設定

您可以使用 Windows 登錄值來設定登入監視器設定。

登錄設定

若要變更組態設定，請導覽至登錄機碼 `HKLM\Software\VMware, Inc.\VMware Logon Monitor`。

表 12-16. 登入監視器組態值

登錄機碼	類型	說明
RemoteLogPath	REG_SZ	上傳記錄檔的遠端共用路徑。當記錄檔複製到遠端記錄檔共用時會位於 RemoteLogPath 登錄機碼指定的資料夾。範例：`\\server\share\%username%。%userdomain%`。登入監視器會視需要建立資料夾。預設為停用狀態。 ■ 遠端記錄檔資料夾的 UNC 路徑 ■ (選用) 如果未設定則記錄檔不會上傳。 ■ 支援選用的本機環境變數。
Flags	REG_DWORD	此值為影響登入監視器行為的位元遮罩。 ■ 設定或移除以啟用或停用 CPU 和記憶體度量的值為 0x4。預設為停用狀態。 ■ 設定或移除以啟用處理事件和登入指令碼度量的值為 0x8。預設為停用狀態。 ■ 設定以啟用或停用與 VMware Horizon 整合的值為 0x2。依預設為啟用。 ■ 設定以停用損毀傾印的值為 0x1。傾印會寫入至 `C:\ProgramData\VMware\VMware Logon Monitor\Data`。預設為停用狀態。 ■ 若要根據每位使用者在遠端路徑中建立資料夾，則需要設定的值為 0x10。預設為停用狀態。
LogMaxSizeMB	REG_DWORD	主要記錄檔的大小上限 (以 MB 為單位)。預設為 100 MB。
LogKeepDays	REG_DWORD	輪流利用主要記錄檔之前保留的天數上限。預設值為 7 天。

計時分析工具設定

登入監視器會與 Horizon Help Desk 計時分析工具整合。計時分析工具依預設為關閉。

- 若要啟用登入監視器以使用計時分析工具將事件寫入至事件資料庫，請執行 `vdmadmin -I -timingProfiler -enable`。
- 若要停用登入監視器以使用計時分析工具，請執行 `vdmadmin -I -timingProfiler -disable`。

使用 VMware Horizon 效能追蹤程式

VMware Horizon 效能追蹤程式是一種公用程式，它會在遠端桌面平台中執行，並監控顯示通訊協定與系統資源使用量的效能。您也可以建立應用程式集區，並以已發佈的應用程式形式執行 Horizon 效能追蹤程式。

設定 VMware Horizon 效能追蹤程式

您可以在遠端桌面平台中執行 Horizon 效能追蹤程式。您也可以已發佈的應用程式形式執行 Horizon 效能追蹤程式。

Horizon 效能追蹤程式功能

Horizon 效能追蹤程式會顯示下列功能的重要資料：

表 12-17. Horizon 效能追蹤程式功能

效能監控	詳細資料
通訊協定的特定資料	■ 編碼器名稱：用於顯示通訊協定的編碼器名稱 ■ 使用的頻寬：顯示通訊協定 (PCoIP 或 Blast) 取樣期間內傳入和傳出頻寬的平均整體頻寬 ■ 每秒畫面播放速率：一秒取樣期間內編碼的影像處理畫面數目 ■ 音訊開啟：音訊功能是否開啟 ■ 音訊已啟動：音訊功能是否已啟動 ■ CPU 使用率: ■ 編碼器 CPU：目前使用者工作階段中顯示通訊協定編碼器的 CPU 使用率 ■ 系統 CPU：系統的 CPU 使用率總計
傳輸類型	■ 用戶端至遠端工作階段：用於從用戶端到遠端對等的 UDP 或 TCP 通訊協定傳輸套件 ■ 遠端工作階段至用戶端：用於從遠端對等到用戶端的 UDP 或 TCP 通訊協定傳輸套件 ■ Horizon Connection Server：用來連線至連線伺服器執行個體的 UDP 或 TCP 通訊協定傳輸套件
系統健全狀況狀態	■ 估計頻寬：Horizon Client 和 Horizon Agent 之間的整體估計可用頻寬 ■ 來回行程：Horizon Agent 和 Horizon Client 之間的來回行程延遲時間 (以毫秒為單位)
工作階段內容	■ 伺服器詳細資料，例如 DNS 名稱、網域名稱、是否使用通道、URL、遠端 IP 位址 ■ 用戶端機器詳細資料，例如顯示器號碼、IP 位址、鍵盤和滑鼠配置、語言、時區
即時通訊協定開關	

備註 Horizon 效能追蹤程式僅在 Horizon Agent 於虛擬桌面平台工作階段上執行時才會收集和顯示資料。

Horizon 效能追蹤程式的系統需求

Horizon 效能追蹤程式支援下列組態。

表 12-18. Horizon 效能追蹤程式系統需求

系統	需求
虛擬桌面平台作業系統	所有支援 Horizon Agent 的作業系統，Linux 代理程式除外。
用戶端機器作業系統	支援所有 Horizon Client 版本，但不支援已發佈應用程式形式的 Linux 版 Horizon Client 和 Windows 10 UWP 版 Horizon Client。

表 12-18. Horizon 效能追蹤程式系統需求 (續)

系統	需求
顯示通訊協定	VMware Blast 和 PCoIP
.NET Framework	Horizon 效能追蹤程式需要 .NET Framework 4.0 版或更新版本。

安裝 Horizon 效能追蹤程式

Horizon 效能追蹤程式是 Horizon Agent 安裝程式中的自訂安裝選項。您必須選取該選項，因為依預設不會選取。Horizon 效能追蹤程式同時適用於 IPv4 和 IPv6。

您可以在虛擬桌面平台或 RDS 主機上安裝 Horizon 效能追蹤程式。如果您在 RDS 主機上安裝，可以將其發佈為已發佈的應用程式，並從 Horizon Client 執行已發佈的應用程式。請參閱《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

安裝會在桌面平台建立捷徑。

設定 Horizon 效能追蹤程式群組原則設定

您可以設定群組原則設定來變更預設設定。請參閱設定 Horizon Performance Tracker 群組原則設定。。

設定 Horizon Performance Tracker 群組原則設定。

若要設定 Horizon Performance Tracker，請在代理程式機器上安裝 Horizon Performance Tracker ADMX 範本檔 (`vdm_agent_perfTracker.admx`)，然後使用本機群組原則編輯器來進行原則設定。

為 Horizon 提供群組原則設定的所有 ADMX 檔案皆可在 `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip` 中取得，其中 *YYMM* 為行銷版本，*x.x.x* 是內部版本，而 *yyyyyyyy* 是組建編號。您可以從 VMware 下載網站下載此檔案，網址為 https://my.vmware.com/web/vmware/downloads。在 [桌面平台及終端使用者運算] 下，選取 VMware Horizon 下載，其中有包含 ZIP 檔案的 GPO 服務包。

程序

1. 從 `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip` 檔案解壓縮出 `vdm_agent_perfTracker.admx` 檔案，並將檔案複製至代理程式機器上的 `%systemroot%\PolicyDefinitions` 資料夾中。
2. 從 `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyyy`*`.zip` 檔案解壓縮出 `vdm_agent_perfTracker.adml` 檔案，並將檔案複製至代理程式機器上 `%systemroot%\PolicyDefinitions\` 資料夾的語言子資料夾中。

   例如，將 `vdm_agent_perfTracker.adml` 檔案的 `en_us` 版本複製到 `%systemroot%\PolicyDefinitions\en_us` 子資料夾中。
3. 啟動本機群組原則編輯器 (`gpedit.msc`)，然後導覽至**電腦組態 > 系統管理範本 > VMware Horizon Performance Tracker**。

4 編輯群組原則設定。

設定	說明
Horizon Performance Tracker 基本設定	啟用時，您可以設定 Horizon Performance Tracker 收集資料的頻率 (以秒為單位)。
啟用 Horizon Performance Tracker 在遠端桌面平台連線中自動啟動。	啟用時，當使用者登入至遠端桌面平台連線時，Horizon Performance Tracker 即會自動啟動。若要清除此喜好設定 GPO 設定，請選取**停用**。
啟用 Horizon Performance Tracker 在遠端應用程式連線中自動啟動	啟用時，當使用者登入至遠端應用程式連線時，Horizon Performance Tracker 即會自動啟動。若要清除此喜好設定 GPO 設定，請選取**停用**。

5 若要讓您的變更生效，請在代理程式機器上重新啟動 Horizon Performance Tracker。

執行 Horizon 效能追蹤程式

您可以使用 Horizon Client 在遠端桌面平台內執行 Horizon 效能追蹤程式，或將其執行為已發佈的應用程式。

如果您使用的 Horizon Client 平台支援多個工作階段，則可以從不同伺服器陣列執行多個 Horizon 效能追蹤程式已發佈的應用程式。在支援多個工作階段的 Windows 和 Mac 用戶端上，[概觀] 視窗中的機器名稱會識別已發佈應用程式的來源伺服器陣列。在 Android 和 iOS 用戶端和 HTML Access 上，一次僅支援一個開啟的工作階段。如果您從另一個伺服器陣列開啟第二個工作階段，則第一個工作階段會關閉。

必要條件

- 安裝和設定 Horizon 效能追蹤程式。請參閱設定 VMware Horizon 效能追蹤程式。
- 設定 Horizon 效能追蹤程式群組原則設定。請參閱設定 Horizon Performance Tracker 群組原則設定。。

程序

- 若要在遠端桌面平台中執行 Horizon 效能追蹤程式，請使用 Horizon Client 或 HTML Access 來連線至伺服器，並啟動遠端桌面平台。

  如果當遠端桌面平台開啟時 Horizon 效能追蹤程式不會自動啟動，您可以按兩下 Windows 桌面平台上的 **VMware Horizon 效能追蹤程式**捷徑，或以啟動任何 Windows 應用程式的相同方式來啟動 Horizon 效能追蹤程式。

  若要選取選項以顯示 [概觀] 視窗或浮動列並結束應用程式，請在遠端桌面平台系統匣中的 VMware Horizon 效能追蹤程式圖示上按一下滑鼠右鍵。

- 若要以已發佈的應用程式形式來執行 Horizon 效能追蹤程式，請使用 Horizon Client 或 HTML Access 連線至伺服器，並啟動 Horizon 效能追蹤程式已發佈的應用程式。

  您使用 Horizon 效能追蹤程式已發佈應用程式的方式，取決於您使用的用戶端類型。您無法使用 Linux 版 Horizon Client 或 Windows 10 UWP 版 Horizon Client 將 Horizon 效能追蹤程式執行為已發佈的應用程式。

  - 使用 Windows 版 Horizon Client 時，Windows 用戶端系統上的系統匣中會顯示 VMware Horizon 效能追蹤程式圖示。您可以按兩下此圖示在 Windows 用戶端上開啟 Horizon 效能追蹤程式。您可以用滑鼠右鍵按一下此圖示，選取選項以顯示 [概觀] 視窗或浮動列並結束應用程式。

- 使用 Mac 版 Horizon Client 時，Mac 用戶端系統的功能表列中會顯示 VMware Horizon 效能追蹤程式圖示。您可以按兩下此圖示在 Mac 用戶端上開啟 Horizon 效能追蹤程式。您也可以用滑鼠右鍵按一下此圖示，選取選項以顯示 [概觀] 視窗或浮動列並結束應用程式。
- 使用 Android 版 Horizon Client 或 iOS 版 Horizon Client 時，Horizon Client 中的 Unity Touch 側邊列會顯示 VMware Horizon 效能追蹤程式圖示。您可以輕觸並按住此圖示，選取選項以顯示 [概觀] 視窗和浮動列並結束應用程式。
- 使用 HTML Access 時，HTML Access 側邊列中會顯示 VMware Horizon 效能追蹤程式圖示。您可以用滑鼠右鍵按一下此圖示，然後選取選項以顯示 [概觀] 視窗或浮動列並結束應用程式。

後續步驟

如需 Horizon 效能追蹤程式顯示資料的相關資訊，請參閱設定 VMware Horizon 效能追蹤程式。

設定負載平衡器以進行 Horizon 連線伺服器健全狀況監控

若要監控 Horizon 連線伺服器上的負載平衡健全狀況，請遵循下列最佳做法。

若要避免大量的健全狀況檢查要求湧入連線伺服器，請將輪詢間隔設定為 30 秒，並將逾時設為該期間的兩或三倍。傳送探查至一個連線伺服器執行個體的負載平衡器不應超過兩個。

唯一支援的健全狀況檢查是 `favicon.ico` 的擷取。若要將探查的成本降至最低，請盡可能使用 `HEAD` 方法。無論檢查是否成功，您都必須在擷取之後捨棄連線，方法包括在要求中新增 Connection: close 標頭，或使用 HTTP/1.0 要求。以下是在負載平衡器的傳送字串中使用 `HEAD` 方法的範例：

```
HEAD /favicon.ico HTTP/1.1\r\nHost: \r\nConnection: Close\r\n
```

HTTP 狀態通常為 200。如果已以系統管理方式停用連線伺服器 (請參閱在 Horizon Console 中停用或啟用 Horizon 連線伺服器)，則狀態將為 503。

如需逾時設定和負載平衡器持續性值，請參閱逾時設定和負載平衡器持續性上的知識庫文章。

監控 VMware Horizon 元件

您可以使用 Horizon Console 儀表板快速調查 VMware Horizon 部署中的 VMware Horizon 與 vSphere 元件的狀態。

Horizon Console 會顯示 Cloud Pod 架構環境中的連線伺服器執行個體、事件資料庫、閘道、資料存放區、vCenter Server 執行個體、網域和工作階段的相關監控資訊。

備註 VMware Horizon 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。

如需在 Cloud Pod 架構環境中監控工作階段的相關資訊，請參閱《在 Horizon 中管理 Cloud Pod 架構》文件。

程序

1 Horizon Console 導覽器的頂端面板會顯示儀表板統計資料的摘要詳細資料，包括**工作階段**、**問題 vCenter 虛擬機器**、**問題 RDS 主機**、**事件**和**系統健全狀況**的最新重新整理日期和相關問題總數。

您可以按一下重新整理圖示以取得最新的儀表板統計資料。

您可以按一下問題號碼，以檢視更多關於元件問題的詳細資料。

- 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。
- 灰色問號表示元件狀態不明。

2 導覽至**監視 > 儀表板**。

系統健全狀況窗格會顯示有問題的系統元件的相關資訊。您可以按一下各個系統元件，以取得受影響的元件、狀態和問題說明的高階視圖。

3 若要檢視問題的詳細資訊，請按一下**檢視**，然後進行選取。

選項	敘述
元件	顯示服務元件的相關資訊。 若要檢視服務元件的相關資訊並執行疑難排解工作，請按一下**連線伺服器**、**閘道伺服器**、**事件資料庫**或 True SSO 索引標籤。 若要執行下列工作，請選取元件。 ■ 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執行個體，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執行個體，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。若要檢視伺服器陣列的詳細資訊 (包括屬於伺服器陣列的 RDS 主機)，請按一下伺服器陣列識別碼。
vSphere	顯示與 vSphere 相關的元件資訊。 若要檢視每個元件的相關資訊，請按一下**資料存放區**、**ESX 主機**和 vCenter Server 索引標籤。
其他元件	若要檢視每個元件的詳細資訊，請按一下**網域**、SAML 2.0 和**授權服務**索引標籤。 **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 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 若要查看長條圖以瞭解虛擬桌面、已發佈的桌面平台和已發佈應用程式的作用中、已中斷連線或閒置工作階段數目，請檢視**工作階段**窗格。

5 若要檢視工作階段，請按一下**工作階段**窗格中的**檢視**。

工作階段頁面會顯示工作階段的相關資訊。

6 若要檢視資料存放區，請按一下**工作負載**窗格中的**檢視**。

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情況。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。

備註 所有閘道設定均啟用後，Horizon Console 會顯示工作階段限制 (即允許的連線伺服器工作階段上限)，並將連線伺服器工作階段計數表示為此限制的百分比。閘道設定未啟用時，則不會指定任何工作階段限制，且會顯示連線伺服器工作階段的絕對數目。

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。

3 選取連線伺服器，然後按一下**檢視工作階段詳細資料**，以檢視此連線伺服器的閘道和非閘道通訊協定工作階段的數目，以及工作階段限制 (若有顯示)。

在管理連線的連線伺服器上，閘道通訊協定工作階段會透過 Blast 安全閘道、PCoIP 安全閘道或 HTTPS 安全通道進行傳遞。例如，連線伺服器可設定為使用 PCoIP 安全閘道連線，而 Horizon Client 則使用 PCoIP 通訊協定連線至連線伺服器。

在管理連線的連線伺服器上，非閘道通訊協定工作階段不會透過 Blast 安全閘道、PCoIP 安全閘道或 HTTPS 安全通道進行傳遞。例如，連線伺服器可設定為使用 HTTP(s) 安全通道連線，而 Horizon Client 則使用 PCoIP 通訊協定來連線至連線伺服器。

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。

監控永久授權使用量

在 Horizon Console 中，您可以監控在同時間連線至 VMware Horizon 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永久授權使用量。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。

VMware Horizon 提供兩個永久授權使用量模式，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，VMware Horizon 都會計算您環境中的具名使用者和並行使用者數目。

對於具名使用者，VMware Horizon 會計算已存取 VMware Horizon 環境的唯一使用者數目。如果某個具名使用者執行多個單一使用者桌面平台、已發佈的桌面平台和已發佈的應用程式，該使用者只會計算一次。

對於具名使用者，**使用設定**面板上的**目前**資料行會顯示首次設定 VMware Horizon 部署以來或上次重設具名使用者計數以後的使用者數目。**最高**資料行不適用於具名使用者。

對於並行使用者，VMware Horizon 會計算每個工作階段的單一使用者桌面平台連線數目。如果並行使用者執行多個單一使用者桌面平台，則每個連線的桌面平台工作階段會分開計算。

對於並行使用者，系統會計算每個使用者的已發佈桌面平台和應用程式連線數目。如果某個並行使用者執行多個已發佈的桌面平台工作階段和應用程式，即使不同的已發佈桌面平台或應用程式主控於不同的 RDS 主機上，使用者仍僅會計算一次。如果某個並行使用者執行單一使用者桌面平台和其他已發佈的桌面平台和應用程式，則使用者僅會計算一次。

對於並行使用者，**使用設定**面板上的**最高**資料行會顯示首次設定 VMware Horizon 部署以來或上次重設最高計數以後，並行桌面平台工作階段和已發佈的桌面平台及應用程式使用者的最高數目。

您可以監控協作工作階段的數目以及連線至工作階段的工作階段協作者數目。

- 作用中 - 協作工作階段：工作階段擁有者已邀請一或多個使用者加入工作階段的工作階段數目。範例：John 邀請了兩人加入其工作階段，而 Mary 邀請了一人加入其工作階段。無論是否有任何受邀者加入工作階段，此資料列的值皆為 2。
- 作用中 - 協作者總數：已連線至協作工作階段的使用者總數，包括工作階段擁有者和任何協作者。範例：John 邀請了兩人，但只有一人加入工作階段。Mary 邀請了一人，但該受邀者並未加入工作階段。此資料列的值為 3：John 的協作工作階段中有一個主要受邀者和一個次要受邀者，而 Mary 的協作工作階段有一個主要受邀者和零個次要受邀者。由於工作階段擁有者會納入計算，因此協作者總數保證永遠大於或等於協作工作階段總數。

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 VMware Horizon 功能，則可以使用 Horizon Console 來變更產品授權金鑰。根據您的 VMware Horizon 部署，您可以取得 VMware Horizon 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 VMware Horizon 執行時將授權新增至 VMware Horizon。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

- 若要讓 VMware Horizon 和附加元件功能成功運作，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 VMware Horizon。請參閱《Horizon 安裝》文件中的〈啟用 VMware Horizon 以進行訂閱授權和 Horizon 控制平面服務〉。**授權**面板會顯示關於 Horizon 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) 若要將 Horizon 網繭的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) 若要將 Horizon 網繭的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 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 版本，確認已啟用或停用元件授權。

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

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。

重設永久授權使用量資料

在 Horizon Console 中，您可以重設永久授權使用量資料，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。請參閱監控永久授權使用量。

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**。

在 VMware Horizon 中監控事件

事件資料庫會儲存連線伺服器主機或群組、Horizon Agent 與 Horizon 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、Oracle 或 PostgreSQL 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，請參閱事件資料庫資料表和結構描述。

備註 事件資料庫無法使用時，VMware Horizon 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 VMware Horizon 事件，讓分析軟體能夠存取事件資料。請參閱《Horizon 安裝》文件中的〈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 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 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、篩選事件，並依照一或多欄排序列出的事件。

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。

VMware Horizon 事件訊息

VMware Horizon 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 VMware Horizon 報告的事件類型。

表 12-19. VMware Horizon 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 VMware Horizon 的作業或組態所做的變更失敗或成功。
錯誤	報告 VMware Horizon 執行失敗的作業。
資訊	報告 VMware Horizon 內的一般作業。
警告	報告作業或組態設定中發生的小問題，這些小問題可能會在經過一段時間後導致更嚴重的問題。

如果您看到與「稽核失敗」、「錯誤」或「警告」事件相關的訊息，可能需要採取某些動作。若是「稽核成功」或「資訊」事件，則不需採取任何動作。

收集 VMware Horizon 的診斷資訊

您可以收集診斷資訊，以協助 VMware 技術支援診斷並解決 VMware Horizon 的相關問題。

您可以收集各種 VMware Horizon 元件的診斷資訊。收集這些資訊的方式取決於 VMware Horizon 元件。

- 建立 Horizon Agent 的資料收集工具服務包

  若要協助 VMware 技術支援疑難排解 Horizon Agent 的問題，您可能需要使用 `vdmadmin` 命令，來建立資料收集工具 (DCT) 服務包。您也可以手動取得 DCT 服務包，不需使用 `vdmadmin`。

- 使用 DCT 來收集遠端桌面平台功能和元件的記錄

  您可以在 Windows 版 Horizon Agent、Windows 版 Horizon Client、Mac 版 Horizon Client，或 Linux 版 Horizon Client 系統上，針對特定遠端桌面平台或所有遠端桌面平台功能的資料收集工具 (DCT) 服務包設定記錄層級和產生記錄檔。

- Windows 版 Horizon Client 記錄檔

  記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以使用群組原則設定來設定部分記錄檔的位置、詳細資訊和保留期間。

- Mac 版 Horizon Client 記錄檔

  記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以建立組態檔來設定詳細資訊等級。

- Linux 版 Horizon Client 記錄檔

  記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以建立組態檔來設定詳細資訊等級。

- 行動裝置上的 Horizon Client 記錄檔

  在行動裝置上，您可能必須安裝協力廠商程式，以導覽至包含記錄檔的目錄。行動用戶端具有用於傳送記錄服務包到 VMware 的組態設定。因為記錄可能影響效能，請在必須排解問題時才啟用記錄。

- Windows 機器上的 Horizon Agent 記錄檔

  記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以使用群組原則設定來設定部分記錄檔的位置、詳細資訊和保留期間。

- Linux 桌面平台記錄檔

  記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以建立組態檔來設定詳細資訊等級。

- 儲存 Windows 版 Horizon Client 的診斷資訊

  若您在使用 Windows 版 Horizon Client 時遇到問題，而且無法以一般網路疑難排解技巧加以解決，您可以儲存記錄檔複本和組態的相關資訊。

- 收集 Horizon 連線伺服器的診斷資訊

  您可以使用支援工具設定記錄層級，並產生 Horizon 連線伺服器的記錄檔。

- 從主控台收集 Horizon Agent、Horizon Client 或 Horizon 連線伺服器的診斷資訊

  如果您可直接存取主控台，即可使用支援指令碼，針對連線伺服器、Horizon Client 或執行 Horizon Agent 的遠端桌面平台產生記錄檔。這些資訊有助於 VMware 技術支援診斷由於這些元件造成的任何問題。

建立 Horizon Agent 的資料收集工具服務包

若要協助 VMware 技術支援疑難排解 Horizon Agent 的問題，您可能需要使用 `vdmadmin` 命令，來建立資料收集工具 (DCT) 服務包。您也可以手動取得 DCT 服務包，不需使用 `vdmadmin`。

為了方便使用，您可以在連線伺服器執行個體上使用 `vdmadmin` 命令，從遠端桌面平台要求 DCT 服務包。服務包會傳回至連線伺服器。

或者您可以登入特定遠端桌面平台，並執行 `support` 命令，在該桌面平台上建立 DCT 服務包。如果已開啟使用者帳戶控制 (UAC)，您就必須以這種方式取得 DCT 服務包。

程序

1 以具有所需權限的使用者身分登入。

選項	動作
在 Horizon 連線伺服器上使用 vdmadmin	以具有**管理員**角色的使用者身分，登入標準或複本執行個體連線伺服器。
在遠端桌面平台上	以具有系統管理員權限的使用者身分，登入遠端桌面平台。

2 開啟命令提示字元，並執行命令，以產生 DCT 服務包。

選項	動作
在 Horizon 連線伺服器上使用 vdmadmin	若要指定輸出服務包檔案、桌面平台集區及機器的名稱，請搭配 `-outfile`、`-d` 及 `-m` 選項使用 `vdmadmin` 命令。 `vdmadmin -A [-b authentication_arguments] -getDCT -outfile local_file -d desktop -m machine`
在遠端桌面平台上	將目錄變更為 `c:\Program Files\VMware\VMware View\Agent\DCT` 並執行下列命令： `support`

結果

命令會將服務包寫入指定的輸出檔案。

範例： 使用 vdmadmin 來建立 Horizon Agent 的服務包檔案

針對桌面平台集區 dtpool2 中的機器 machine1 建立 DCT 服務包，並將其寫入 zip 檔案 `C:\myfile.zip` 中。

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

後續步驟

如果您擁有現有支援要求，則可以藉由附加 DCT 服務包檔案來更新。

使用 DCT 來收集遠端桌面平台功能和元件的記錄

您可以在 Windows 版 Horizon Agent、Windows 版 Horizon Client、Mac 版 Horizon Client，或 Linux 版 Horizon Client 系統上，針對特定遠端桌面平台或所有遠端桌面平台功能的資料收集工具 (DCT) 服務包設定記錄層級和產生記錄檔。

預設安裝路徑

DCT 指令碼會安裝在下列目錄中，並從代理程式和用戶端安裝路徑執行。

- Windows 版 Horizon Agent：`C:\Program Files\VMware\VMware View\Agent\DCT\support.bat`
- Windows 版 Horizon Client：`C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat`
- Mac 版 Horizon Client：`/Applications/VMware Horizon Client.app/Contents/Library/dct/HorizonCollector.sh`
- Linux 版 Horizon Client：`/usr/bin/vmware-view-log-collector`

命令語法

使用下列命令針對每個平台執行 DCT 指令碼。

- Windows 版 Horizon Agent：`support.bat`
- Windows 版 Horizon Client：`support.bat`
- Mac 版 Horizon Client：`HorizonCollector.sh`
- Linux 版 Horizon Client：`vmware-view-log-collector`

支援的功能

下表所列的遠端桌面平台功能具有 JSON 組態檔，其中包含記錄層級設定、記錄收集設定和傾印收集設定。

這些服務適用於 Windows 版 Horizon Agent、Windows 版 Horizon Client、Mac 版 Horizon Client，和 Linux 系統版 Horizon Client，說明中另述特定例外。

對於接受功能名稱的命令列選項，請指定 [功能名稱] 資料行中顯示的名稱。

功能名稱	完整功能名稱
Blast	Blast **備註** 此服務僅適用於 Windows 版 Horizon Agent。
用戶端	用戶端 **備註** 此服務不適用於 Windows 版 Horizon Agent。
CDR	用戶端磁碟機重新導向
剪貼簿	剪貼簿重新導向
DPISync	DPI 同步
DnD	拖放 **備註** 此服務不適用於 Linux 版 Horizon Client。
FA	檔案類型關聯 **備註** 此服務不適用於 Linux 版 Horizon Client。
TSMMR	多媒體重新導向 **備註** 此服務不適用於 Mac 版 Horizon Client。
PCoIP	PCoIP
PerfTracker	Performance Tracker **備註** 此服務僅適用於 Windows 版 Horizon Agent。
PrintRedir	印表機重新導向
PublishedApp	已發佈的應用程式
RTAV	RTAV
ScannerRedirection	掃描器重新導向 **備註** 此服務不適用於 Mac 版 Horizon Client。
SerialPortRedirection	序列埠重新導向 **備註** 此服務不適用於 Mac 版 Horizon Client。
SmartCard	智慧卡重新導向
URLRedirection	URL 內容重新導向
USB	USB 重新導向

功能名稱	完整功能名稱
VDPService	VDPService
浮水印	數位浮水印

命令列選項

下表說明命令列選項和使用方式。

選項	用途	說明

-l	-l	列出 DCT 所支援所有功能和元件的記錄層級。
		例如，Windows 版 Horizon Client 命令 `support.bat -l` 的輸出會列出 DCT 控制的所有元件以及記錄層級狀態：
		`- Agent Core [INFO]`
		`- PCoIP [INFO]`
		`- Virtual Channel [INFO]`
		`- VDP Service [TRACE]`
		`- Remote Features`
		`- Client Drive Redirection [TRACE]`
		`- Clipboard Redirection [DEBUG]`
		`- Drag and Drop [TRACE]`
		`- DPI Synchronization [INFO]`
		`- File Type Association [INFO]`

	-l *feature1*,*feature2* ...	列出指定功能的記錄層級。
		例如，Windows 版 Horizon Client 命令 `support.bat -l CDR,DnD` 的輸出會列出用戶端磁碟機重新導向和拖放功能的記錄層級狀態：
		`- Client Drive Redirection [TRACE]`
		`- Drag and Drop [TRACE]`

選項	用途	說明

	-l -傾印	查詢已設定程序的傾印設定。
		例如，Windows 版 Horizon Client 命令 `support.bat -l -dumps` 的輸出會列出每個程序的名稱、傾印類型和傾印計數上限：
		`Process Name Dump Type Max Dump Count`
		`vmware-view.exe Full 128`
		`vmware-remotemks.exe Full 128`
		`vmware-appstub.exe Full 128`
		`horizon_client_service.exe Full NO LIMIT`
		備註 此命令僅適用於 Windows 版 Horizon Client。

	-l -傾印計數	查詢已設定程序的傾印計數。 **備註** 此命令僅適用於 Windows 版 Horizon Client。
	-l -傾印類型	查詢已設定程序的傾印類型。 **備註** 此命令僅適用於 Windows 版 Horizon Client。
-ld	-ld *feature1*,*feature2* ...	列出指定功能的記錄層級詳細資料。
-x	-x All:*level*	設定 DCT 所支援所有功能的記錄層級。有效的記錄層級如下： ■ 資訊 ■ 偵錯 ■ 追蹤 ■ 詳細
	-x *feature1*:*level1*,*feature2*:*level2* ...	設定指定功能或元件的記錄層級。 例如，Linux 版 Horizon Client 命令 `vmware-view-log-collector -x All:TRACE` 的輸出會將所有元件的記錄層級設定為追蹤。Linux 版 Horizon Client 命令 `vmware-view-log-collect -x DnD:INFO,CDR:TRACE` 的輸出會將拖放功能的記錄層級設定為資訊，並將用戶端磁碟機重新導向功能的記錄層級設定為追蹤。
-r	-r	將所有功能的記錄層級重設為安裝預設值。
-c	-c All	收集所有記錄。
	-c *feature1*,*feature2* ...	收集指定功能或元件的記錄。
-d	-d *directory1*	將 DCT 輸出重新導向至指定的目錄。
-f	-f *bundleName*	將記錄服務包檔案的完整名稱指定為 *bundleName*。

選項	用途	說明
-h	-h	顯示命令列選項的說明資訊，並列出 DCT 支援的功能和元件。
-del	-del -dumps All	刪除 DCT 所支援所有功能和元件的傾印。 **備註** 此命令僅適用於 Windows 版 Horizon Client。
	-del -dumps *feature1,feature2* ...	刪除指定功能的傾印。 例如，Windows 版 Horizon Client 命令 `support.bat -del -dumps Client,FA` 的輸出會刪除用戶端和檔案類型關聯功能的傾印檔案。 **備註** 此命令僅適用於 Windows 版 Horizon Client。

即時傾印

對於 Windows 版 Horizon Client 和 Windows 版 Horizon Agent，部分功能也支援即時傾印。此功能會根據組態檔設定傾印目標處理程序，並在記錄服務包中收集傾印。是否需要產生即時傾印，取決於功能的組態。

例如，如果您執行 Windows 版 Horizon Client 的命令 `support.bat -c`，則會出現此訊息：您可以選擇產生在此機器上所執行 `VMware Horizon Client` 處理程序的診斷傾印，但請注意，這些檔案可能會很大。如果您選擇 `Y`，則會針對與 Windows 版 Horizon Client 相關的現有處理程序產生傾印檔案。

Windows 版 Horizon Client 記錄檔

記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以使用群組原則設定來設定部分記錄檔的位置、詳細資訊和保留期間。

記錄檔位置

針對下表中的檔案名稱，*YYYY* 代表年，*MM* 為月，*DD* 為日，而 *XXXXXX* 為數字。

表 12-20. Windows 版 Horizon Client 記錄檔

記錄類型	目錄路徑	檔案名稱
安裝	`C:\Users\%username%\AppData\Local\Temp`	`vminst.log_XXXXXX_XXXXXX.txt` `vmmsi.log_XXXXXX_XXXXXX.txt`
PCoIP 用戶端 來自 `vmware-remotemks.exe` 處理程序	`C:\Users\%username%\AppData\Local\Temp`	`pcoip_client_YYYY_MM_DD_XXXXXX.txt` **備註** 您可以使用 GPO 來設定記錄層級，從 0 到 3 (最詳細)。請使用 View PCoIP 用戶端工作階段變數 ADMX 範本檔 `pcoip.admx`。此設定為**設定 PCoIP 事件記錄詳細資訊**。
Horizon Client UI 來自 `vmware-view.exe` 處理程序	`C:\Users\%username%\AppData\Local\VMware\VDM\Logs`	`vmware-horizon-viewclient-YYYY-MM-DD-XXXXXX.txt` **備註** 您可以使用 GPO 來設定記錄位置。請使用 View 一般組態 ADMX 範本檔 `vdm_common.admx`。

表 12-20. Windows 版 Horizon Client 記錄檔 (續)

記錄類型	目錄路徑	檔案名稱
Horizon Client 記錄 來自 vmware-view.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username-XXXXXX*	vmware-crtbora-*XXXXXX*.log
訊息架構	C:\Users\%*username*%\AppData\Local\VMware\VDM\Logs	log-*YYYY-MM-DD-XXXXXX*.txt debug-*YYYY-MM-DD-XXXXXX*.txt
遠端 MKS (mouse-keyboard-screen) 記錄 來自 vmware-remotemks.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	ViewMP-Client-*XXXXXX*.log vmware-mks-*XXXXXX*.log vmware-rdeSvc-*XXXXXX*.log vmware-vvaClient-*XXXXXX*.log
Tsdr 用戶端 來自 vmware-remotemks.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	vmware-ViewTsdr-Client-*XXXXXX*.log
Tsmmr 用戶端 來自 vmware-remotemks.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	vmware-ViewTsmmr-Client-*XXXXXX*.log
VdpService 用戶端 來自 vmware-remotemks.exe 處理程序	C:\Users\%*username*%\AppData\Local\Temp\vmware-*username*	vmware-vdpServiceClient-*XXXXXX*.log
WSNM 服務 來自 wsnm.exe 處理程序	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-*XXXXXX*.txt **備註** 您可以使用 GPO 來設定記錄位置。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。
USB 重新導向 來自 vmware-remotemks.exe 處理程序	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-*XXXXXX*.txt **備註** 您可以使用 GPO 來設定記錄位置。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。
序列埠重新導向 來自 vmwsprrdpwks.exe 處理程序	C:\ProgramData\VMware\VDM\Logs	Serial*.txt Netlink*.txt
掃描器重新導向 來自 ftscanmgr.exe 處理程序	C:\ProgramData\VMware\VDM\Logs	Scanner*.txt Netlink*.txt

記錄檔組態

您可以使用群組原則設定來進行下列組態變更：

- 針對 PCoIP 用戶端記錄，您可以設定記錄層級，從 0 到 3 (最詳細)。請使用 View PCoIP 用戶端工作階段變數 ADMX 範本檔 pcoip.admx。此設定為**設定 PCoIP 事件記錄詳細資訊**。
- 針對用戶端使用者介面記錄，設定記錄位置、詳細資訊和保留原則。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。

- 針對 USB 重新導向記錄，設定記錄位置、詳細資訊和保留原則。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。
- 針對 WSNM 服務記錄，設定記錄位置、詳細資訊和保留原則。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。

您也可以使用命令列命令來設定詳細資訊等級。導覽至 C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT 目錄，並輸入下列命令：

```
support.bat loglevels
```

將會顯示新的命令提示字元視窗，並提示您選取詳細資訊等級。

收集記錄服務包

您可以使用用戶端使用者介面或命令列命令將記錄收集到 ZIP 檔案，以便傳送該檔案給 VMware 技術支援。

- 在 Horizon Client 中，從**選項**功能表中選取**支援資訊**。在顯示的對話方塊中，按一下**收集支援資料**。
- 從命令列，導覽至 C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT 目錄，並輸入 support.bat 命令。

Mac 版 Horizon Client 記錄檔

記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以建立組態檔來設定詳細資訊等級。

記錄檔位置

表 12-21. Mac 版 Horizon Client 記錄檔

記錄類型	目錄路徑	檔案名稱
Horizon Client UI	~/Library/Logs/VMware Horizon Client	
PCoIP 用戶端	~/Library/Logs/VMware Horizon Client	
即時音訊視訊	~/Library/Logs/VMware	vmware-RTAV-pid.log
USB 重新導向	~/Library/Logs/VMware	
VChan	~/Library/Logs/VMware Horizon Client	
遠端 MKS (mouse-keyboard-screen) 記錄	~/Library/Logs/VMware	
Crtbora	~/Library/Logs/VMware	

記錄檔組態

Horizon Client 會在 Mac 用戶端的 ~/Library/Logs/VMware Horizon Client 目錄中產生記錄檔。管理員可在 Mac 用戶端上的 /Library/Preferences/com.vmware.horizon.plist 檔案中設定機碼，以設定記錄檔的數目上限以及可保留記錄檔的天數上限。

表 12-22. 用於記錄檔收集的 plist 機碼

機碼	說明
MaxDebugLogs	記錄檔的數目上限。上限值為 100。
MaxDaysToKeepLogs	可保留記錄檔的天數上限。此值沒有限制。

當您啟動 Horizon Client 時，系統將刪除與這些準則不相符的檔案。

如果未在 com.vmware.horizon.plist 檔案中設定 MaxDebugLogs 或 MaxDaysToKeepLogs 機碼，則記錄檔的預設數目為 5 個，可保留記錄檔的預設天數為 7 天。

Linux 版 Horizon Client 記錄檔

記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以建立組態檔來設定詳細資訊等級。

記錄檔位置

表 12-23. Linux 版 Horizon Client 記錄檔

記錄類型	目錄路徑	檔案名稱
安裝	/tmp/vmware-root/	.vmware-installer-pid.log vmware-vmis-pid.log
Horizon Client UI	/tmp/vmware-*username*/	vmware-horizon-client-pid.log
PCoIP 用戶端	/tmp/teradici-*username*/	pcoip_client_*YYYY_MM_DD_XXXXXX*.log
即時音訊視訊	/tmp/vmware-*username*/	vmware-RTAV-pid.log
USB 重新導向	/tmp/vmware-root/	vmware-usbarb-pid.log vmware-view-usbd-pid.log
VChan	/tmp/vmware-*username*/	VChan-Client.log **備註** 當您透過設定「export VMW_RDPVC_BRIDGE_LOG_ENABLED=1」啟用 RDPVCBridge 記錄時便會建立此記錄。
遠端 MKS (mouse-keyboard-screen) 記錄	/tmp/vmware-*username*/	vmware-mks-pid.log vmware-MKSVchanClient-pid.log vmware-rdeSvc-pid.log
VdpService 用戶端	/tmp/vmware-*username*/	vmware-vdpServiceClient-pid.log
Tsdr 用戶端	/tmp/vmware-*username*/	vmware-ViewTsdr-Client-pid.log

記錄檔組態

您可以使用組態內容 (`view.defaultLogLevel`) 來設定用戶端記錄檔的詳細資訊等級，從 0 (收集所有事件) 到 6 (僅收集嚴重事件)。

針對 USB 的特定記錄，您可以使用下列命令列命令：

```
vmware-usbarbitrator --verbose
vmware-view-usbd -o log:trace
```

收集記錄服務包

記錄收集器位於 `/usr/bin/vmware-view-log-collector`。若要使用記錄收集器，您必須具備執行權限。您可以從 Linux 命令列輸入下列命令來設定權限：

```
chmod +x /usr/bin/vmware-view-log-collector
```

您可以從 Linux 命令列輸入下列命令來執行記錄收集器：

`/usr/bin/vmware-view-log-collector`

行動裝置上的 Horizon Client 記錄檔

在行動裝置上，您可能必須安裝協力廠商程式，以導覽至包含記錄檔的目錄。行動用戶端具有用於傳送記錄服務包到 VMware 的組態設定。因為記錄可能影響效能，請在必須排解問題時才啟用記錄。

iOS 用戶端記錄檔

針對 iOS 用戶端，記錄檔位於 *`User Programs`*`/Horizon/` 下的 `tmp` 和 `Documents` 目錄中。若要導覽至這些目錄，您必須先安裝第三方應用程式，例如 iFunbox。

您可以透過開啟 Horizon Client 設定中的**記錄**設定來啟用記錄。在此設定啟用時，如果用戶端未預期地結束，或如果您結束用戶端然後重新啟動用戶端，記錄檔會合併並壓縮成單一 GZ 檔案。之後您可以透過電子郵件將服務包傳送給 VMware。如果您的裝置連接到 PC 或 Mac，您可以使用 iTunes 擷取記錄檔。

Android 用戶端記錄檔

針對 Android 用戶端，記錄檔位於 `Android/data/com.vmware.view.client.android/files/` 目錄中。若要導覽至此目錄，您必須先安裝第三方應用程式，例如 File Explorer 或 My Files。

依預設，只會在應用程式未預期地結束時建立記錄。您可以透過開啟 Horizon Client 設定中的**啟用記錄**設定來變更此預設值。若要透過電子郵件傳送記錄服務包給 VMware，您可以使用 Horizon Client 設定中的**傳送記錄**設定。

Chrome 用戶端記錄檔

Chrome 用戶端的記錄僅能透過 JavaScript 主控台取得。

Windows 機器上的 Horizon Agent 記錄檔

記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以使用群組原則設定來設定部分記錄檔的位置、詳細資訊和保留期間。

記錄檔位置

針對下表中的檔案名稱，*YYYY* 代表年，*MM* 為月，*DD* 為日，而 *XXXXXX* 為數字。

表 12-24. Windows 版 Horizon Client 記錄檔

記錄類型	目錄路徑	檔案名稱
安裝	C:\Users\%*username*%\AppData\Local\Temp	vminst.log_*XXXXXX*_*XXXXXX*.txt vmmsi.log_*XXXXXX*_*XXXXXX*.txt
Horizon Agent	*<Drive Letter>*:\ProgramData\VMware\VDM\logs	pcoip_agent_*YYYY_MM_DD_XXXXXX*.txt pcoip_agent_*YYYY_MM_DD_XXXXXX*.txt vmware-vdpServiceServer-*XXXXXX*.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-*XXXXXX*.txt **備註** 您可以使用 GPO 來設定記錄檔位置。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。

記錄檔組態

您可以使用下列方法來設定記錄選項。

- 使用群組原則設定來設定記錄位置、詳細資訊和保留原則。請使用 View 一般組態 ADMX 範本檔 vdm_common.admx。
- 使用命令列命令來設定詳細資訊等級。導覽至 C:\Program Files\VMware\VMware View\Agent\DCT 目錄，並輸入 support.bat loglevels。將會顯示新的命令提示字元視窗，並提示您選取詳細資訊等級。
- 將 vdmadmin 命令與 -A 選項搭配使用，以設定依 Horizon Agent 的記錄。如需指示，請參閱《Horizon 管理》文件。

收集記錄服務包

您可以使用命令列命令將記錄收集到 ZIP 檔案，以傳送該檔案給 VMware 技術支援。從命令列，導覽至 C:\Program Files\VMware\VMware View\Agent\DCT 目錄，並輸入 support.bat 命令。

Linux 桌面平台記錄檔

記錄檔可協助您對安裝、顯示通訊協定和功能元件的相關問題進行疑難排解。您可以建立組態檔來設定詳細資訊等級。

記錄檔位置

表 12-25. Linux 桌面平台記錄檔

記錄類型	目錄路徑
安裝	/tmp/vmware-root
Horizon Agent	/var/log/vmware
Horizon Agent	/usr/lib/vmware/viewagent/viewagent-debug.log

記錄檔組態

若要設定記錄，請編輯 /etc/vmware/config 檔案。

收集記錄服務包

您可以建立 Data Collection Tool (DCT) 服務包，該服務包會收集機器的組態資訊並記錄至壓縮的 tarball。在 Linux 桌面平台中開啟命令提示字元，並執行 dct-debug.sh 指令碼。

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

tarball 是在執行指令碼所在的目錄 (目前的工作目錄) 中產生。檔案名稱包含作業系統、時間戳記和其他資訊，例如 ubuntu-12-vdm-sdct-20150201-0606-agent.tgz。

此命令會從 /tmp/vmware-root 目錄和 /var/log/vmware 目錄收集記錄檔，並且也會收集下列系統記錄和組態檔：

- /var/log/messages*
- /var/log/syslog*
- /var/log/boot*.log
- /proc/cpuinfo, /proc/meminfo, /proc/vmstat, /proc/loadavg
- /var/log/audit/auth.log*
- /etc/hosts
- /etc/resolv.conf
- /etc/nsswitch.conf
- /var/log/Xorg*
- /etc/X11/xorg.conf
- /usr/lib/vmware/viewagent 中的核心檔案
- /var/crash/_usr_lib_vmware_viewagent* 中的任何損毀檔案

儲存 Windows 版 Horizon Client 的診斷資訊

若您在使用 Windows 版 Horizon Client 時遇到問題，而且無法以一般網路疑難排解技巧加以解決，您可以儲存記錄檔複本和組態的相關資訊。

您在儲存診斷資訊並與 VMware 技術支援聯絡之前，可以先嘗試解決 Windows 版 Horizon Client 的連線問題。如需詳細資訊，請參閱《在 Horizon 中設定虛擬桌面平台》文件中的〈Horizon Client 和 Horizon 連線伺服器之間的連線問題〉。

如需關於為其他 Horizon Client 平台收集支援資料的相關資訊，請參閱該平台的《安裝和設定指南》。以 Mac 版 Horizon Client 為例，請參閱《Mac 版 VMware Horizon Client 安裝和設定指南》。

程序

1 在 Horizon Client 中按一下**支援資訊**，或是在遠端桌面平台功能表，選取**選項 > 支援資訊**。

2 在**支援資訊**視窗中按一下**收集支援資料**，並在出現提示時按一下**是**。

命令視窗會顯示資訊收集進度。此程序可能需要幾分鐘時間。

3 在命令視窗中，藉由輸入您要據以測試 Horizon Client 組態之 Horizon 連線伺服器執行個體的 URL 來回應提示，如有需要，亦可選擇產生 VMware Horizon 程序的診斷傾印。

此資訊會寫入用戶端機器之桌面平台資料夾中的 zip 檔案。

4 在 VMware 網站的「支援」頁面提出支援要求，並附加輸出的 zip 檔案。

收集 Horizon 連線伺服器的診斷資訊

您可以使用支援工具設定記錄層級，並產生 Horizon 連線伺服器的記錄檔。

支援工具將收集連線伺服器的記錄資料。這些資訊有助於 VMware 技術支援診斷由於連線伺服器所造成的任何問題。支援工具並非用來收集 Horizon Client 或 Horizon Agent 的診斷資訊。您必須改用支援指令碼。請參閱從主控台收集 Horizon Agent、Horizon Client 或 Horizon 連線伺服器的診斷資訊。

必要條件

以具有**管理員**角色的使用者身分，登入連線伺服器的標準或複本執行個體。

程序

1 選取**開始 > 所有程式 > VMware > 設定 View 連線伺服器記錄層級**。

2 在**選擇**文字方塊中，輸入設定記錄層級的數值，並且按 Enter。

選項	說明
0	將記錄層級重設為預設值。
1	選取記錄的一般層級。
2	選取記錄的偵錯層級 (預設)。
3	選取完整記錄。

系統將以您選取的詳細資料層級，開始記錄資訊。

3 收集連線伺服器行為的充足資訊後，選取**開始 > 所有程式 > VMware > 產生 View 連線伺服器記錄服務包**。

支援工具會將記錄檔寫入連線伺服器執行個體的桌面平台上名為 `vdm-sdct` 的資料夾中。

4 在 VMware 網站的「支援」頁面提出支援要求，並附加輸出檔案。

從主控台收集 Horizon Agent、Horizon Client 或 Horizon 連線伺服器的診斷資訊

如果您可直接存取主控台，即可使用支援指令碼，針對連線伺服器、Horizon Client 或執行 Horizon Agent 的遠端桌面平台產生記錄檔。這些資訊有助於 VMware 技術支援診斷由於這些元件造成的任何問題。

必要條件

登入要收集資訊的系統。您必須以具有管理員權限的使用者身分登入。

- 對於 Horizon Agent，登入已安裝 Horizon Agent 的虛擬機器。
- 對於 Horizon Client，登入已安裝 Horizon Client 的系統。
- 對於連線伺服器，登入連線伺服器主機。

程序

1 開啟命令提示字元視窗，並針對要收集診斷資訊的 VMware Horizon 元件變更為適當的目錄。

選項	說明
Horizon Agent	切換至 `C:\Program Files\VMware View\Agent\DCT` 目錄。
Horizon Client	切換至 `C:\Program Files\VMware View\Client\DCT` 目錄。
連線伺服器	切換至 `C:\Program Files\VMware View\Server\DCT` 目錄。

如果並非將軟體安裝於預設目錄，請更改為適當的磁碟機代號及路徑。

2 輸入命令以執行支援指令碼。

```
.\support.bat [loglevels]
```

如果要啟用進階記錄，請指定 `loglevels` 選項，並且在提示時輸入記錄層級的數值。

選項	說明
0	將記錄層級重設為預設值。
1	選取記錄的一般層級。
2	選取記錄的偵錯層級 (預設)。
3	選取完整記錄。
4	選取 PCoIP 的資訊記錄 (僅限 Horizon Agent 及 Horizon Client)。
5	選取 PCoIP 的偵錯記錄 (僅限 Horizon Agent 及 Horizon Client)。

選項	說明
6	選取虛擬通道的資訊記錄 (僅限 Horizon Agent 及 Horizon Client)。
7	選取虛擬通道的偵錯記錄 (僅限 Horizon Agent 及 Horizon Client)。
8	選取虛擬通道的追蹤記錄 (僅限 Horizon Agent 及 Horizon Client)。

指令碼會將壓縮的記錄檔寫入桌面平台的資料夾 `vdm-sdct`。

3 在 VMware 網站的「支援」頁面提出支援要求，並附加輸出檔案。

在 Horizon Console 中收集記錄

您可以在 Horizon Console 中產生和記錄管理收集工作，以及下載連線伺服器、桌面平台集區和伺服器陣列的記錄服務包。

透過完整的管理權限，您可以查看和管理所有記錄收集工作作業，包括取消記錄建立要求，以及刪除其他使用者已完成的記錄收集工作。

不具完整權限的管理員只能查看、管理和取消自己起始的工作。

必要條件

您必須具有記錄收集權限，才能收集記錄。在 Horizon Console 中，導覽至**設定 > 管理員 > 角色權限 > 新增角色**。建立具有收集作業記錄權限的自訂角色，並將此角色新增至管理員的權限。

程序

1 在 Horizon Console 中，導覽至**疑難排解 > 記錄收集**。

2 在**收集**索引標籤上選取元件類型，然後按一下**尋找**。

元件類型包括：

- **連線伺服器**：選取連線伺服器。
- **代理程式**：從目前的網繭選取桌面平台集區。
- **代理程式 RDS**：從目前的網繭選取伺服器陣列。

3 從清單中選取元件，然後按一下**收集**。

[記錄收集狀態] 視窗會列出選取的元件，以及每個元件的記錄收集工作狀態。狀態包括已成功排入佇列的記錄，以及因錯誤而發生的失敗。您可以重新整理清單以查看狀態更新。

- 連線伺服器：如果連線伺服器是代理程式記錄收集工作的擁有者，則該連線伺服器的記錄收集工作可能會因為伺服器忙碌中，請稍後再試一次錯誤而失敗。
- 代理程式：在代理程式中完成記錄收集工作後，代理程式記錄服務包會複製到連線伺服器的本機檔案系統。

備註 如果已針對特定元件要求記錄，則會停用該元件以避免出現重複的記錄建立要求。

4 在**管理**索引標籤中，按一下**下載**資料行中的連結，以下載元件的記錄服務包。

記錄服務包會下載至使用者的本機檔案系統中。

5 若要刪除已完成的記錄收集工作的記錄服務包，請選取元件，然後按一下**刪除**。

在本機檔案系統上的記錄儲存區目錄中產生的記錄服務包將會刪除。刪除作業會刪除連線伺服器本機檔案系統上的記錄儲存區目錄 (預設目錄：`%PROGRAMDATA%/VMware/VDM/DCT`) 中儲存的記錄收集工作和相關聯的記錄服務包。

備註 您必須具有完整的管理權限，才能執行此作業。

6 若要取消已起始的記錄建立工作，請選取元件，然後按一下**取消**。您必須先取消處於錯誤狀態的工作才能起始下一個工作。

進行中和已完成工作的取消程序會根據元件而有所不同：

元件	進行中工作的程序	已完成工作的程序
連線伺服器	1 在背景中執行的程序會中止。 2 在記錄儲存區位置中產生的中繼檔案會刪除。 3 工作會刪除。 **備註** 如果在背景中執行的程序因錯誤而停止，則中止作業可能會失敗，而需要手動介入予以復原。	1 在記錄儲存區位置中產生的記錄服務包會刪除。 2 工作會刪除。
代理程式	1 連線伺服器會等待代理程式中的記錄收集完成。 2 代理程式記錄服務包會複製到連線伺服器。 3 記錄服務包會刪除。 4 工作會刪除。	1 儲存在記錄儲存區位置中的記錄服務包會刪除。 2 工作會刪除。

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 VMware Horizon 的問題。Skyline Collector 應用裝置會針對為記錄收集所設定的 VMware Horizon 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。

結果

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 VMware Horizon 的問題。

更新支援要求

您可以在支援網站上更新現有的支援要求。

在您提出支援要求之後，可能會收到由 VMware 技術支援寄來的電子郵件要求，請您提供 `support` 或 `svi-support` 指令碼的輸出檔。在您執行指令碼時，指令碼會告訴您輸出檔的名稱和位置。請回覆電子郵件訊息，並在回覆中附加輸出檔。

如果輸出檔太大，無法以附件包含在郵件中 (10MB 或以上)，請連絡 VMware 技術支援，告訴他們您的支援要求編號，同時索取 FTP 上傳指示。或者您也可以在支援網站上，將檔案附加至現有的支援要求。

程序

1 造訪 VMware 網站的「支援」頁面並登入。

2 按一下**支援要求記錄**，然後找出適用的支援要求編號。

3 更新支援要求，同時附加您藉由執行 `support` 或 `svi-support` 指令碼而取得的輸出。

傳送意見反應

Horizon Console 會定期顯示一個快顯視窗，要求您提供關於功能的意見反應。您可以選擇在快顯視窗中提供意見反應或不提供意見反應，或設定 Horizon Console 以選擇不提供意見反應。Horizon 團隊會參酌您提供的意見反應來改善產品。

程序

1 在 Horizon Console 標頭中，按一下**傳送意見反應**圖示。

如果您在 DMZ 環境中處於離線狀態，當您按一下**傳送意見反應**圖示時，將會顯示預先填入的電子郵件視窗。您可以使用範本電子郵件來提交您的意見反應。

2 在顯示的對話方塊中，按 [下一步]。

您可以選擇不傳送意見反應，也可以檢閱對話方塊中提供的 VMware 隱私權通知。如果您選擇不傳送意見反應，Horizon Console 將不會再顯示任何要求提供意見反應的快顯視窗。

3 填妥**傳送意見反應**視窗中的欄位，然後按一下**提交**。

對 VMware Horizon Server 憑證撤銷檢查進行疑難排解

如果無法對伺服器的 TLS 憑證執行憑證撤銷檢查，則用於安全 Horizon Client 連線的連線伺服器執行個體可能會在 Horizon Console 中顯示為紅色。

問題

Horizon Console 儀表板上的連線伺服器圖示為紅色。連線伺服器的狀態會顯示下列訊息：無法勾選伺服器的憑證。

原因

如果您的組織使用 Proxy 伺服器來進行網際網路存取，或是連線伺服器執行個體因防火牆或其他控制項，而無法與提供撤銷檢查的伺服器連線，則憑證撤銷檢查可能會失敗。

連線伺服器執行個體會對其本身的憑證執行憑證撤銷檢查。依預設，VMware Horizon 連線伺服器服務會以 `LocalSystem` 帳戶啟動。當它在 `LocalSystem` 底下執行時，連線伺服器執行個體無法使用在 Internet Explorer 設定的 Proxy 設定來存取 CRL DP URL 或 OCSP 回應者，以確定憑證的撤銷狀態。

您可以使用 Microsoft `Netshell` 命令，將 Proxy 設定匯入至連線伺服器執行個體，如此一來，伺服器即可存取網際網路上的憑證撤銷檢查站台。

解決方案

1. 在連線伺服器電腦上，使用**以系統管理員身分執行**設定開啟命令列視窗。

   例如，按一下**開始**，輸入 **cmd**，以滑鼠右鍵按一下 `cmd.exe` 圖示，然後選取**以系統管理員身分執行**。
2. 輸入 **netsh**，並按 Enter 鍵。
3. 輸入 **winhttp**，並按 Enter 鍵。
4. 輸入 **show proxy**，並按 Enter 鍵。

   `Netshell` 顯示 Proxy 已設定為 DIRECT (直接) 連線。透過這項設定，若組織使用 Proxy，連線伺服器電腦即無法連線至網際網路。
5. 設定 Proxy 設定。

   例如，在 `netsh winhttp>` 提示，輸入 **import proxy source=ie**。

   Proxy 設定會匯入至連線伺服器電腦。
6. 您可以輸入 **show proxy** 以確認 Proxy 設定。
7. 重新啟動 VMware Horizon 連線伺服器服務。
8. 在 Horizon Console 儀表板上，確認連線伺服器圖示為綠色。

智慧卡憑證撤銷檢查疑難排解

已連接智慧卡的連線伺服器執行個體無法對伺服器的 TLS 憑證執行憑證撤銷檢查，除非您已設定智慧卡憑證撤銷檢查。

問題

如果您的組織使用 Proxy 伺服器來進行網際網路存取，或是連線伺服器執行個體因防火牆或其他控制項，而無法與提供撤銷檢查的伺服器連線，則憑證撤銷檢查可能會失敗。

重要 請確定 CRL 檔案為最新。

原因

VMware Horizon 使用「憑證撤銷清單」(CRL) 和「線上憑證狀態通訊協定」(OCSP) 來支援憑證撤銷檢查。CRL 是核發憑證的 CA (憑證授權機構) 所發佈的撤銷憑證清單。OCSP 是用來取得 X.509 憑證的撤銷狀態的憑證驗證通訊協定。必須可以從連線伺服器主機存取 CA。只有在設定智慧卡憑證撤銷檢查時，才會發生此問題。請參閱使用智慧卡憑證撤銷檢查。

解決方案

1. 建立您自己專屬 (手動) 程序，從您使用的 CA 網站下載最新的 CRL 到 VMware Horizon Server 上的路徑。
2. 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`
3. 將 `locked.properties` 檔案中的 `enableRevocationChecking` 和 `crlLocation` 內容新增至儲存 CRL 的本機路徑。
4. 重新啟動連線伺服器服務來讓您的變更生效。

進一步疑難排解資訊

您可以在 VMware 知識庫文章中找到進一步的疑難排程資訊。

VMware 知識庫 (KB) 會持續更新，以提供 VMware 產品的疑難排解新資訊。

如需疑難排解的詳細資訊，請參閱 VMware 知識庫網站上的知識庫文章：

http://kb.vmware.com/selfservice/microsites/microsite.do

使用 vdmadmin 命令

13

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 VMware Horizon 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 VMware Horizon 作業報告

  您可以將 vdmadmin 命令與 -I 選項搭配使用，以列示 VMware Horizon 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 VMware Horizon 事件記錄訊息

  您可以將 vdmadmin 命令與 -I 選項搭配使用，將 VMware Horizon 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即時複製虛擬機器。VMware Horizon 會將 ESXi 主機導向至即時複製作業系統磁碟上的回收磁碟空間，不需等待作業系統磁碟上的未使用空間到達在 Horizon Console 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 VMware Horizon 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的項目

  您可以將 vdmadmin 命令與 -S 選項搭配使用，以移除 VMware Horizon 組態中的連線伺服器執行個體的項目。

- 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 Console，將**管理員**角色指派給使用者。請參閱第 8 章 設定角色型委派管理。

如果您以權限不足的使用者身分登入，而且您知道已獲指定**管理員**角色之使用者的密碼，則可以以該使用者身分，使用 -b 選項執行命令。當指定的使用者位於指定的網域內時，您可以指定 -b 選項以執行 vdmadmin 命令。下列 -b 選項的使用格式是相同的。

```
        -b username domain [password | *]
```

```
        -b username@domain [password | *]
```

```
        -b domain\username [password | *]
```

如果指定星號 (*) 而非指定密碼，系統會提示您輸入密碼，而且 vdmadmin 命令不會在命令列的命令歷程記錄中保留敏感的密碼。

您可以使用 -b 選項搭配所有命令選項，但 -R 和 -T 選項除外。

vdmadmin 命令輸出格式

有些 vdmadmin 命令選項可讓您指定輸出資訊的格式。

下表說明某些 vdmadmin 命令選項針對格式化輸出文字所提供的選項。

表 13-1. 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 VMware Horizon 的作業。

表 13-2. 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
-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 VMware Horizon 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 VMware Horizon 作業的報告。請參閱使用 -I 選項列示與顯示 VMware Horizon 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 VMware Horizon 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 VMware Horizon 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的項目。
-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管理員角色。請參閱使用 -U 選項顯示使用者的相關資訊。

表 13-2. 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] -getlogfilelogfile-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 13-3. 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 13-4. 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 VMware Horizon 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] -monitorid monitor_id -instanceid instance_id -xml [-w
| -n]
```

使用附註

下表會顯示 VMware Horizon 用來監控其元件健全狀況的健全狀況監視器。

表 13-5. 健全監視器

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，VMware Horizon 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 13-6. 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。
`-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 VMware Horizon 作業報告

您可以將 `vdmadmin` 命令與 `-I` 選項搭配使用，以列示 VMware Horizon 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
```

使用附註

您可以使用此命令顯示可用的報告與視圖，並顯示 VMware Horizon 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 VMware Horizon 記錄訊息。請參閱使用 -I 選項以 Syslog 格式產生 VMware Horizon 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 13-7. 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 VMware Horizon 事件記錄訊息

您可以將 `vdmadmin` 命令與 `-I` 選項搭配使用，將 VMware Horizon 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
```

使用附註

您可以使用此命令以 Syslog 格式產生 VMware Horizon 事件記錄檔訊息。在 Syslog 檔中，VMware Horizon 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 VMware Horizon 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。請參閱《Horizon 安裝》文件中的〈設定 Syslog 伺服器的事件記錄〉。

表 13-8. 可使用 Syslog 格式產生 VMware Horizon 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 VMware Horizon 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 VMware Horizon 事件。

```
vdmadmin -I -eventSyslog -disable
```

將 VMware Horizon 事件的 Syslog 輸出僅導向至本機系統。

```
vdmadmin -I -eventSyslog -enable -localOnly
```

將 VMware Horizon 事件的 Syslog 輸出僅導向至指定的路徑。

```
vdmadmin -I -eventSyslog -enable -path path
```

將 VMware Horizon 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 [-b authentication_arguments] -d desktop -m  machine -u domain\user
```

```
vdmadmin -L [-b authentication_arguments] -d desktop [-m machine | -u domain\user] -r
```

使用附註

VMware Horizon 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 VMware Horizon 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 VMware Horizon 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。

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 13-9. 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]
```

使用附註

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 Console 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 13-10. 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即時複製虛擬機器。VMware Horizon 會將 ESXi 主機導向至即時複製作業系統磁碟上的回收磁碟空間，不需等待作業系統磁碟上的未使用空間到達在 Horizon Console 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。

使用此選項之前，請先參閱《在 Horizon 中設定虛擬桌面平台》文件中的〈回收即時複製上的磁碟空間〉。此選項僅適用於 vSphere 6.7 之前的非 vSAN 資料存放區，此處會由 Horizon 執行空間回收作業。

選項

表 13-11. 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 VMware Horizon 開放給使用者的網域。

語法

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain
-add [-s connsvr]
```

```
vdmadmin -N [-b authentication_arguments] -domains -list [-w | -n] [-xml]
```

```
vdmadmin -N [-b authentication_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]
```

使用附註

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

VMware Horizon 下表顯示您可以指定用來設定網域篩選條件的選項。

表 13-12. 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。
-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 :
```

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，VMware Horizon 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 VMware Horizon 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。

VMware Horizon 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，VMware Horizon 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。VMware Horizon 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 13-13. 網域清單類型

網域清單類型	說明
搜尋排除清單	指定 VMware Horizon 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 VMware Horizon 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 VMware Horizon 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。VMware Horizon 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。

VMware Horizon 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，VMware Horizon 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 VMware Horizon 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
```

VMware Horizon 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 VMware Horizon 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 :
```

VMware Horizon 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，VMware Horizon 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 13-14. 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。
`-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 13-15. 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 13-15. 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] [-group
group_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"]
```

使用附註

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，VMware Horizon 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，VMware Horizon 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 VMware Horizon 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 13-16. 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。

表 13-16. 在 Kiosk 模式中設定用戶端的選項 (續)

選項	說明
`-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。VMware Horizon 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的項目

您可以將 vdmadmin 命令與 -S 選項搭配使用，以移除 VMware Horizon 組態中的連線伺服器執行個體的項目。

語法

```
vdmadmin -S [-b authentication_arguments] -r -s server
```

使用附註

為確保高可用性，VMware Horizon 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 VMware Horizon 組態內存留下來。

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 如果連線伺服器是 CPA 聯盟的一部分，請執行「新增或移除程式」工具，從 Windows Server 電腦中移除 Adam 執行個體 VMwareVDMDSG 程式。

4 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項目從組態中移除。

如果您要在已移除的系統上重新安裝 VMware Horizon，但不複寫原始群組的 VMware Horizon 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。

備註 如果您使用 vdmadmin -S 命令移除連線伺服器執行個體，而未如上所述在伺服器上完整解除安裝 LDAP 執行個體，則您可能會意外移除架構主節點，導致封鎖連線伺服器未來的升級和安裝。

選項

-s 選項可指定待移除的連線伺服器執行個體的 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} -owner domain\user -user domain\user [-password
password]
```

使用附註

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 Console 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並不需要。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 13-17. 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。

表 13-17. 提供次要認證的選項 (續)

選項	說明
-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 VMware Horizon 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。
- 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 13-18. 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 [-b authentication_arguments] -collisions [-resolve]
vdmadmin -X [-b authentication_arguments] -schemacollisions [-resolve] [-global]
vdmadmin -X [-b authentication_arguments] -seizeSchemaMaster
vdmadmin -X [-b authentication_arguments] -seizeSchemaMaster [-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 VMware Horizon 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 VMware Horizon 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 VMware Horizon 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 13-19. 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 13-20. 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。

下表顯示可指定用來解決 LDAP 結構描述主節點問題的選項。

表 13-21. 用來解決 LDAP 結構描述主節點問題的選項

選項	說明
`-seizeSchemaMaster`	將目前的節點設為叢集上的結構描述主節點。
`-global`	結構描述角色可從 Cloud Pod 架構 環境中的全域 Horizon LDAP 執行個體上取得。若未指定此選項，則會在本機 Horizon LDAP 執行個體上取得結構描述角色。

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
```

將目前的節點設為本機 LDAP 執行個體之叢集上的結構描述主節點。

```
vdmadmin -X -seizeSchemaMaster
```

將目前的節點設為 Cloud Pod 架構環境中全域 LDAP 執行個體之叢集上的結構描述主節點。

```
vdmadmin -X -seizeSchemaMaster -global
```

整合 VMware Horizon 與事件資料庫 14

您可以設定 VMware Horizon，將事件記錄到 Microsoft SQL Server、Oracle 或 PostgreSQL 資料庫。VMware Horizon 會記錄事件，例如使用者動作、管理員動作、報告系統失敗和錯誤的警示，以及統計取樣。

使用者動作包括記錄及啟動桌面平台和應用程式工作階段。管理員動作包括新增權利以及建立桌面平台和應用程式集區。統計取樣的其中一個範例是記錄 24 小時期間內的使用者數目上限。

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

本章節討論下列主題：

事件資料庫資料表和結構描述

VMware Horizon 會使用資料庫資料表來實作事件資料庫。事件資料庫會在這些資料表的名稱前面加上您在設定資料庫時定義的首碼。

事件資料庫資料表

下表顯示在 VMware Horizon 中實作事件資料庫的資料庫資料表。

表 14-1. 事件資料庫資料表

資料表名稱	說明
event	最近事件的中繼資料和搜尋最佳化資料。
event_data	最近事件的資料值。

表 14-1. 事件資料庫資料表 (續)

資料表名稱	說明
event_data_historical	所有事件的資料值。
event_historical	所有事件的中繼資料和搜尋最佳化資料。

VMware Horizon 會將事件的相關詳細資料記錄至所有資料庫資料表。寫入事件記錄經過特定期間後，VMware Horizon 會從 event 和 event_data 資料表刪除該記錄。您可以使用 Horizon Console 來設定資料庫要將記錄保留在 event 和 event_data 資料表中的期間。

重要 VMware Horizon 不會限制 event_historical 和 event_data_historical 資料表的成長。您必須為這些資料表實作空間管理原則。

唯一主索引鍵 EventID 會識別 VMware Horizon 記錄在 event 和 event_historical 資料表中的每個事件。VMware Horizon 會將每個事件的資料值記錄在 event_data 和 event_data_historical 資料表中。您可以在 EventID 資料行上連接 event 與 event_data 資料表或 event_ historical 與 event_data_historical 資料表，以取得事件的完整資訊集。

event 和 event_historical 資料表中的 [EventType]、[Severity] 和 [Time] 資料行可識別事件的類型和嚴重性及其發生的時間。

如需設定事件資料庫的相關資訊，請參閱《Horizon 安裝》文件。

備註 若要從歷史表格清除資料，請參閱 http://kb.vmware.com/kb/2150309。

事件資料庫結構描述

下表說明 event 和 event_historical 資料庫資料表的結構描述。

表 14-2. event 和 event_historical 資料表的結構描述

資料行名稱	Oracle 資料類型	SQL Server 資料類型	PostgreSQL 資料類型	說明
Acknowledged	SMALLINT	tinyint	整數	VMware Horizon 是否已確認事件。 ■ 0 = false ■ 1 = true
Applicationid	NVARCHAR2(512)	nvarchar(512)	character varying(512)	相關聯應用程式的識別碼。
DesktopId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	與集區相關聯的桌面平台識別碼。
EndpointId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	相關聯端點的識別碼。
EventID	INTEGER	int	整數	事件的唯一主索引鍵。
EventType	NVARCHAR2(512)	nvarchar(512)	character varying(512)	與訊息類別目錄中的項目相對應的事件名稱。例如 BROKER_USERLOGGEDIN。

表 14-2. event 和 event_historical 資料表的結構描述 (續)

資料行名稱	Oracle 資料類型	SQL Server 資料類型	PostgreSQL 資料類型	說明
FolderPath	NVARCHAR2(512)	nvarchar(512)	character varying(512)	包含相關聯物件之資料夾的完整路徑。
GroupId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Active Directory 中相關聯群組的 SID。
LUNId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	儲存相關聯物件之 LUN 的識別碼。
MachineId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	相關聯實體或虛擬機器的識別碼。
Module	NVARCHAR2(512)	nvarchar(512)	character varying(512)	引發事件的 VMware Horizon 元件。例如 Admin、Broker、Tunnel、Framework、Client 或 Agent。
ModuleAndEventText	NVARCHAR2(512)	nvarchar(512)	character varying(512)	包含的值針對屬性參數取代的事件訊息。
Node	NVARCHAR2(512)	nvarchar(512)	character varying(512)	虛擬裝置節點的名稱。
SessionId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	相關聯工作階段的識別碼。
嚴重性	NVARCHAR2(512)	nvarchar(512)	character varying(512)	嚴重性層級。例如資訊、警告、錯誤、AUDIT_SUCCESS 和 AUDIT_FAIL。
來源	NVARCHAR2(512)	nvarchar(512)	character varying(512)	事件來源的識別碼。
ThinappId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	相關聯 ThinApp 物件的識別碼。
時間	TIMESTAMP	datetime	不含時區的時間戳記	事件發生的時間，從 epoch 計算 (1970 年 1 月 1 日)。
UserDiskPathId	NVARCHAR2(512)	nvarchar(512)	character varying(512)	使用者磁碟的識別碼。
UserSID	NVARCHAR2(512)	nvarchar(512)	character varying(512)	Active Directory 中相關聯使用者的 SID。

下表說明 event_data 和 event_data_historical 資料庫資料表的結構描述。

表 14-3. event_data 和 event_data_historical 資料表的結構描述

資料行名稱	Oracle 資料類型	SQL Server 資料類型	PostgreSQL 資料類型	說明
BooleanValue	SMALLINT	tinyint	整數	布林值屬性的值。 ■ 0 = false ■ 1 = true
EventID	INTEGER	int	整數	事件的唯一主索引鍵。

表 14-3. event_data 和 event_data_historical 資料表的結構描述 (續)

資料行名稱	Oracle 資料類型	SQL Server 資料類型	PostgreSQL 資料類型	說明
IntValue	INTEGER	int	整數	整數屬性的值。
名稱	NVARCHAR2(512)	nvarchar(512)	character varying(512)	屬性名稱 (例如 UserDisplayName)。
StrBlobValue	NCLOB	nvarchar(max)	文字	超過 500 個字元的字串屬性值。
StrValue	NVARCHAR2(512)	nvarchar(512)	character varying(512)	字串屬性的值。針對其他類型的屬性，此資料行會包含字串形式的資料類型解譯。
TimeValue	TIMESTAMP	datetime	不含時區的時間戳記	日期和時間屬性的值。
類型	SMALLINT	tinyint	整數	屬性的資料類型。 ■ 0 = StrValue ■ 1 = IntValue ■ 2 = TimeValue ■ 3 = BooleanValue ■ 4 = StrBlobValue

下表顯示 timing_profiler 資料庫資料表的架構。

表 14-4. Timing_profiler 資料表的架構

資料行名稱	Oracle 資料類型	SQL Server 資料類型	PostgreSQL 資料類型	說明
EventId	NUMBER	int	整數	事件的唯一主索引鍵。
EventType	NVARCHAR2(512)	nvarchar(512)	字元有所不同	計時分析工具事件的類型。例如：TIMING_PROFILER_DESKTOP_RECONNECT。
內容	NCLOB	nvarchar(max)	文字	JSON 包含與此計時分析工具事件相關聯的各種屬性。
SessionId	NVARCHAR2(512)	nvarchar(512)	字元有所不同	與此事件相關聯的工作階段。
時間	TIMESTAMP	datetime	不含時區的時間戳記	事件發生的時間，從 epoch 計算 (1970 年 1 月 1 日)。
TimingProfilerTree	NCLOB	nvarchar(max)	文字	登入計時分析工具樹狀結構。
UserSid	NVARCHAR2(512)	nvarchar(512)	字元有所不同	涉及此事件的使用者。

Horizon Connection Server 事件

Horizon Connection Server 事件會報告連線伺服器的相關資訊，例如桌面平台和應用程式工作階段、使用者驗證失敗，以及佈建錯誤。

BROKER_DAILY_MAX_DESKTOP_SESSIONS 事件會報告 24 小時期間內的並行桌面平台工作階段數目上限。如果使用者同時執行多個桌面平台工作階段，則每個桌面平台工作階段會分開計數。

BROKER_DAILY_MAX_APP_USERS 事件會報告 24 小時期間內的並行應用程式使用者數目上限。如果使用者同時執行多個應用程式，則該使用者僅會計數一次。由於取樣每 5 分鐘執行一次，因此短期留存的工作階段可能不會包含在計數中。

BROKER_VC_DISABLED 和 BROKER_VC_ENABLED 事件會報告 VMware Horizon 用來追蹤 vCenter Server 執行個體之 vCenter 驅動程式的狀態。

BROKER_VC_STATUS_* 事件會報告 vCenter Server 執行個體的狀態。

下表列出連線伺服器的所有事件類型。

表 14-5. 連線伺服器事件

事件類型	嚴重性	ModuleAndEventText
BROKER_AGENT_OFFLINE	警告	機器${MachineName} 上執行的代理程式未回應查詢，因此將其標記為離線
BROKER_AGENT_ONLINE	警告	機器${MachineName} 上執行的代理程式正再次回應，但是未傳送啟動訊息
BROKER_APPLICATION_LAUNCH_FAILURE	錯誤	無法為使用者 ${UserDisplayName} 從集區 ${PoolId} 啟動: 處理此要求時，Broker 發生錯誤，請連絡支援部門以取得協助
BROKER_APPLICATION_MISSING	警告	至少有 ${ApplicationMissingCount} 個應用程式 (包括 ${ApplicationExecutable}) 未安裝在集區 ${PoolId} 中的 ${MachineName} 上
BROKER_APPLICATION_NOT_ENTITLED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${PoolId} 啟動: 使用者無權使用此集區
BROKER_APPLICATION_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${PoolId} 啟動: 不支援要求的通訊協定 ${ProtocolId}
BROKER_APPLICATION_REQUEST	資訊	使用者 ${UserDisplayName} 已要求應用程式 ${Application Id}
BROKER_APPLICATION_SESSION_REQUEST	資訊	使用者 ${UserDisplayName} 已從集區 ${PoolId} 要求了應用程式工作階段
BROKER_DAILY_MAX_DESKTOP_SESSIONS	資訊	${Time}: 在過去 24 小時中，並行桌面平台工作階段的數目上限為 ${UserCount}
BROKER_DAILY_MAX_APP_USERS	資訊	${Time}: 在過去 24 小時中，具有並行應用程式工作階段的使用者數目上限為 ${UserCount}
BROKER_DESKTOP_LAUNCH_FAILURE	錯誤	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 處理此要求時 Broker 發生錯誤，請連絡支援部門尋求協助
BROKER_DESKTOP_NOT_ENTITLED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 使用者無權使用此集區
BROKER_DESKTOP_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 不支援要求的通訊協定 ${ProtocolId}

表 14-5. 連線伺服器事件 (續)

事件類型	嚴重性	ModuleAndEventText
BROKER_DESKTOP_REQUEST	資訊	使用者 ${UserDisplayName} 要求集區 ${DesktopId}
BROKER_EVENT_HANDLING_STARTED	資訊	Broker ${BrokerName} 已開始處理事件
BROKER_EVENT_HANDLING_STOPPED	資訊	${BrokerName} 已停止處理事件
BROKER_MACHINE_ALLOCATED	資訊	使用者 ${UserDisplayName} 要求集區 ${DesktopId}，已配置機器 ${MachineName}
BROKER_MACHINE_ASSIGNED_UNAVAILABLE	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 指派的機器 ${MachineName} 無法使用
BROKER_MACHINE_CANNOT_CONNECT	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 無法使用 ${ProtocolId} 連線至機器 ${MachineName}
BROKER_MACHINE_CONFIGURED_VIDEO_SETTINGS	資訊	已成功設定集區 ${DesktopId} 中虛擬機器${MachineName} 的視訊設定
BROKER_MACHINE_NOT_READY	警告	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 機器 ${MachineName} 未準備就緒，無法接受連線
BROKER_MACHINE_OPERATION_DELETED	資訊	已刪除機器${MachineName}
BROKER_MACHINE_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 機器 ${MachineName} 不支援通訊協定 ${ProtocolId}
BROKER_MACHINE_PROTOCOL_UNAVAILABLE	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 機器 ${MachineName} 未報告通訊協定 ${ProtocolId} 準備就緒
BROKER_MACHINE_REJECTED_SESSION	警告	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 機器${MachineName} 拒絕啟動工作階段要求
BROKER_MACHINE_SESSION_TIMEDOUT	警告	使用者 ${UserDisplayName} 的工作階段已逾時
BROKER_MULTIPLE_DESKTOPS_FOR_KIOSK_USER	警告	使用者 ${UserDisplayName} 有權使用多個桌面平台集區
BROKER_POOL_CANNOT_ASSIGN	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 沒有可為其指定使用者的機器可供使用
BROKER_POOL_COMANAGER_REQUIRED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 沒有任何共同管理功能可供通訊協定 ${ProtocolId} 使用
BROKER_POOL_EMPTY	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 桌面平台集區為空白
BROKER_POOL_NO_MACHINE_ASSIGNED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 沒有為此使用者指定任何機器

表 14-5. 連線伺服器事件 (續)

事件類型	嚴重性	ModuleAndEventText
BROKER_POOL_NO_RESPONSES	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 桌面平台集區中的所有機器都沒有回應
BROKER_POOL_OVERLOADED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 所有回應的機器目前都在使用中
BROKER_POOL_POLICY_VIOLATION	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 此桌面平台集區不允許使用線上工作階段
BROKER_POOL_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 沒有支援通訊協定 ${ProtocolId} 的機器可供使用
BROKER_POOL_PROTOCOL_UNAVAILABLE	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 沒有報告通訊協定 ${ProtocolId} 已準備就緒的機器可供使用
BROKER_POOL_TUNNEL_NOT_SUPPORTED	AUDIT_FAIL	無法為使用者 ${UserDisplayName} 從集區 ${DesktopId} 啟動: 通訊協定 ${ProtocolId} 不支援通道
BROKER_PROVISIONING_ERROR_CONFIG_CLEARED	資訊	集區 ${DesktopId} 不再出現先前報告的組態問題
BROKER_PROVISIONING_ERROR_CONFIG_SET	錯誤	由於出現組態問題，因此集區 ${DesktopId} 發生佈建錯誤
BROKER_PROVISIONING_ERROR_DISK_CLEARED	資訊	集區 ${DesktopId} 不再出現先前報告的磁碟問題
BROKER_PROVISIONING_ERROR_DISK_SET	警告	由於出現磁碟問題，因此集區 ${DesktopId} 發生佈建錯誤
BROKER_PROVISIONING_ERROR_LICENCE_CLEARED	資訊	集區 ${DesktopId} 不再出現先前報告的授權問題
BROKER_PROVISIONING_ERROR_LICENCE_SET	錯誤	集區 ${DesktopId} 因授權問題而發生佈建錯誤
BROKER_PROVISIONING_ERROR_NETWORKING_CLEARED	資訊	集區 ${DesktopId} 不再出現先前報告的 Horizon Agent 網路問題
BROKER_PROVISIONING_ERROR_NETWORKING_SET	錯誤	集區 ${DesktopId} 因 Horizon Agent 的網路問題而發生佈建錯誤
BROKER_PROVISIONING_ERROR_RESOURCE_CLEARED	資訊	集區 ${DesktopId} 不再出現先前報告的資源問題
BROKER_PROVISIONING_ERROR_RESOURCE_SET	錯誤	集區 ${DesktopId} 因資源問題而發生佈建錯誤
BROKER_PROVISIONING_ERROR_TIMEOUT_CUSTOMIZATION_CLEARED	資訊	集區 ${DesktopId} 不再出現先前報告的自訂時發生逾時的問題
BROKER_PROVISIONING_ERROR_TIMEOUT_CUSTOMIZATION_SET	錯誤	集區 ${DesktopId} 因自訂作業逾時而發生佈建錯誤

表 14-5. 連線伺服器事件 (續)

事件類型	嚴重性	ModuleAndEventText
BROKER_PROVISIONING_ERROR_VM_CLONING	錯誤	機器${MachineName} 發生佈建錯誤: 機器複製失敗
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_ERROR	錯誤	機器${MachineName} 發生佈建錯誤: 機器自訂失敗
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_NETWORKING	錯誤	機器 ${MachineName} 發生佈建錯誤: 由於 Horizon Agent 與連線伺服器之間沒有網路通訊而導致自訂錯誤
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_TIMEOUT	錯誤	機器${MachineName} 發生佈建錯誤: 自訂作業逾時
BROKER_PROVISIONING_SVI_ERROR_RECONFIG_FAILED	錯誤	機器${MachineName} 發生佈建錯誤: 重新設定作業失敗
BROKER_PROVISIONING_SVI_ERROR_REFIT_ FAILED	錯誤	機器${MachineName} 發生佈建錯誤: 重新調整作業${SVIOperation} 失敗
BROKER_PROVISIONING_SVI_ERROR_REMOVING_VM	錯誤	機器${MachineName} 發生佈建錯誤: 無法從詳細目錄移除機器
BROKER_PROVISIONING_VERIFICATION_ FAILED_USER_ASSIGNED	警告	機器 ${MachineName} 的佈建驗證失敗: 已將使用者指定至集區 ${DesktopId} 中的機器
BROKER_PROVISIONING_VERIFICATION_ FAILED_USER_CANNOT_BE_ASSIGNED	警告	機器 ${MachineName} 的佈建驗證失敗: 由於集區 ${DesktopId} 不具持續性，因此無法指派使用者
BROKER_PROVISIONING_VERIFICATION_ FAILED_VMNAME_IN_USE	警告	機器 ${MachineName} 的佈建驗證失敗: 集區 ${DesktopId} 中已存在名稱為 ${MachineName} 的機器
BROKER_SVI_ARCHIVE_UDD_FAILED	AUDIT_FAIL	無法將使用者資料磁碟 ${UserDiskName} 封存至位置 ${SVIPath}
BROKER_SVI_ARCHIVE_UDD_SUCCEEDED	AUDIT_SUCCESS	已將使用者資料磁碟 ${UserDiskName} 封存至位置 ${SVIPath}
BROKER_SVI_ATTACH_UDD_FAILED	AUDIT_FAIL	無法將使用者資料磁碟 ${UserDiskName} 連接至虛擬機器 ${SVIVMID}
BROKER_SVI_ATTACH_UDD_SUCCEEDED	AUDIT_SUCCESS	已將使用者資料磁碟 ${UserDiskName} 連接至虛擬機器 ${SVIVMID}
BROKER_SVI_DETACH_UDD_FAILED	AUDIT_FAIL	無法中斷使用者資料磁碟 ${UserDiskName} 與虛擬機器 ${SVIVMID} 的連結
BROKER_SVI_DETACH_UDD_SUCCEEDED	AUDIT_SUCCESS	已中斷使用者資料磁碟 ${UserDiskName} 與虛擬機器 ${SVIVMID} 的連結
BROKER_USER_AUTHFAILED_ACCOUNT_ DISABLED	AUDIT_FAIL	由於帳戶已停用，因此使用者 ${UserDisplayName} 無法驗證
BROKER_USER_AUTHFAILED_ACCOUNT_ EXPIRED	AUDIT_FAIL	由於帳戶已到期，因此使用者 ${UserDisplayName} 無法驗證
BROKER_USER_AUTHFAILED_ACCOUNT_ LOCKED_OUT	AUDIT_FAIL	由於帳戶已鎖定，因此使用者 ${UserDisplayName} 無法驗證

表 14-5. 連線伺服器事件 (續)

事件類型	嚴重性	ModuleAndEventText
BROKER_USER_AUTHFAILED_ACCOUNT_ RESTRICTION	AUDIT_FAIL	由於存在帳戶限制，因此使用者 ${UserDisplayName} 無法驗證
BROKER_USER_AUTHFAILED_BAD_USER_ PASSWORD	AUDIT_FAIL	由於使用者名稱或密碼不正確，因此使用者 ${UserDisplayName} 無法驗證
BROKER_USER_AUTHFAILED_GENERAL	AUDIT_FAIL	使用者 ${UserDisplayName} 無法驗證
BROKER_USER_AUTHFAILED_NO_LOGON_ SERVERS	AUDIT_FAIL	由於無登入伺服器，因此使用者 ${UserDisplayName} 無法驗證
BROKER_USER_AUTHFAILED_PASSWORD_ EXPIRED	AUDIT_FAIL	由於密碼已到期，因此使用者 ${UserDisplayName} 無法驗證
BROKER_USER_AUTHFAILED_PASSWORD_ MUST_CHANGE	AUDIT_FAIL	由於必須變更密碼，因此使用者 ${UserDisplayName} 無法驗證
BROKER_USER_AUTHFAILED_SECUREID_ ACCESS_DENIED	AUDIT_FAIL	使用者 ${UserDisplayName} 存取 SecurID 遭拒
BROKER_USER_AUTHFAILED_SECUREID_ NEWPIN_REJECTED	AUDIT_FAIL	由於已拒絕新 PIN，因此使用者 ${UserDisplayName} 存取 SecurID 遭拒
BROKER_USER_AUTHFAILED_SECUREID_ WRONG_NEXTTOKEN	AUDIT_FAIL	由於輸入的下一個 Token 不正確，因此使用者 ${UserDisplayName} 存取 SecurID 遭拒
BROKER_USER_AUTHFAILED_SECUREID_ WRONG_STATE	AUDIT_FAIL	由於狀態不正確，因此使用者 ${UserDisplayName} 存取 SecurID 遭拒
BROKER_USER_AUTHFAILED_TIME_ RESTRICTION	AUDIT_FAIL	由於存在時間限制，因此使用者 ${UserDisplayName} 無法驗證
BROKER_USER_NOT_AUTHORIZED	AUDIT_FAIL	使用者 ${UserDisplayName} 已驗證，但是未取得執行作業的授權
BROKER_USER_NOT_ENTITLED	AUDIT_FAIL	使用者 ${UserDisplayName} 已驗證，但是無權使用任何集區
BROKER_USERCHANGEDPASSWORD	AUDIT_SUCCESS	使用者已變更 ${UserDisplayName} 的密碼
BROKER_USERLOGGEDIN	AUDIT_SUCCESS	使用者 ${UserDisplayName} 已登入
BROKER_USERLOGGEDOUT	AUDIT_SUCCESS	使用者 ${UserDisplayName} 已登出
BROKER_VC_DISABLED	資訊	位址為 ${VCAddress} 的 vCenter 已暫時停用
BROKER_VC_ENABLED	資訊	位址為 ${VCAddress} 的 vCenter 已啟用
BROKER_VC_STATUS_CHANGED_CANNOT_ LOGIN	警告	無法登入位址為 ${VCAddress} 的 vCenter
BROKER_VC_STATUS_CHANGED_DOWN	資訊	位址為 ${VCAddress} 的 vCenter 已關機
BROKER_VC_STATUS_CHANGED_INVALID_ CREDENTIALS	警告	位址為 ${VCAddress} 的 vCenter 擁有的認證無效
BROKER_VC_STATUS_CHANGED_NOT_YET_ CONNECTED	資訊	尚未連線至位址為 ${VCAddress} 的 vCenter

表 14-5. 連線伺服器事件 (續)

事件類型	嚴重性	ModuleAndEventText
BROKER_VC_STATUS_CHANGED_RECONNECTING	資訊	正在重新連線至位址為 ${VCAddress} 的 vCenter
BROKER_VC_STATUS_CHANGED_UNKNOWN	警告	位址為 ${VCAddress} 的 vCenter 狀態不明
BROKER_VC_STATUS_CHANGED_UP	資訊	位址為 ${VCAddress} 的 vCenter 已開機
BROKER_USER_LOCK_SSO		表示連線伺服器的 SSO 認證已因逾時或螢幕鎖定而遭到捨棄。事件文字：使用者 <網域名稱\使用者名稱> 的 SSO 認證已鎖定。
BROKER_LMV_REMOTE_POD_DESKTOP_LAUNCH		表示使用者的工作階段已重新導向至遠端網繭，用以在 CPA 環境中啟動桌面平台工作階段。事件文字：遠端網繭 <網繭名稱> 已從全域權利 <全域權利名稱> 為使用者 <使用者名稱> 啟動桌面平台。

Horizon Agent 事件

Horizon Agent 事件會報告 Horizon Agent 相關資訊，例如已登入或從特定機器中斷連線的使用者、Horizon Agent 是否已在特定機器上關閉，以及 Horizon Agent 是否已從特定機器將啟動訊息傳送至 Horizon Connection Server。

表 14-6. Horizon Agent 事件

事件類型	嚴重性	ModuleAndEventText
AGENT_CONNECTED	資訊	使用者 ${UserDisplayName} 已登入機器${MachineName} 上的新工作階段
AGENT_DISCONNECTED	資訊	使用者 ${UserDisplayName} 已與機器${MachineName} 中斷連線
AGENT_ENDED	資訊	使用者 ${UserDisplayName} 已登出機器${MachineName}
AGENT_PENDING	資訊	機器${MachineName} 上執行的代理程式已接受使用者 ${UserDisplayName} 的已配置工作階段
AGENT_PENDING_EXPIRED	警告	機器${MachineName} 上使用者 ${UserDisplayName} 的擱置工作階段已到期
AGENT_RECONFIGURED	資訊	已成功重新設定機器${MachineName}
AGENT_RECONNECTED	資訊	使用者 ${UserDisplayName} 已重新連線至機器${MachineName}
AGENT_RESUME	資訊	機器${MachineName} 上的代理程式已傳送繼續訊息
AGENT_SHUTDOWN	資訊	機器${MachineName} 上執行的代理程式已關閉，此機器將無法使用

表 14-6. Horizon Agent 事件 (續)

事件類型	嚴重性	ModuleAndEventText
AGENT_STARTUP	資訊	機器${MachineName} 上執行的代理程式已連絡連線伺服器，並已傳送啟動訊息
AGENT_SUSPEND	資訊	機器${MachineName} 上的代理程式已傳送暫止訊息

Horizon Console 事件

Horizon Console 事件會報告使用者在 Horizon Console 中所起始動作的相關資訊。

表 14-7. Horizon Console 事件

EventType	嚴重性	ModuleAndEventText
ADMIN_ADD_DESKTOP_ENTITLEMENT	AUDIT_SUCCESS	${UserDisplayName} 已授予對集區 ${DesktopId} 的 ${EntitlementDisplay} 權利
ADMIN_ADD_LICENSE	AUDIT_SUCCESS	${UserDisplayName} 已新增授權
ADMIN_ADD_LICENSE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法新增授權
ADMIN_ADD_PM	AUDIT_SUCCESS	${UserDisplayName} 已新增實體機器${MachineName} 至集區 ${DesktopId}
ADMIN_ADD_PM_FAILED	AUDIT_FAIL	${UserDisplayName} 無法新增實體機器 ${MachineName} 至集區 ${DesktopId}
ADMIN_ADMINSTRATOR_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法移除管理員 ${AdminPermissionEntity} 的所有權限
ADMIN_ADMINSTRATOR_REMOVED	AUDIT_SUCCESS	${UserDisplayName} 已移除管理員 ${AdminPermissionEntity} 的所有權限
ADMIN_CONNECTION_BROKER_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法更新連線 Broker ${BrokerId}
ADMIN_CONNECTION_BROKER_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已更新連線代理 ${BrokerId}: (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_CONNECTION_SERVER_BACKUP_FAILED	AUDIT_FAIL	${UserDisplayName} 無法啟動連線 Broker ${BrokerId} 的備份
ADMIN_CONNECTION_SERVER_BACKUP_INITIATED	AUDIT_SUCCESS	${UserDisplayName} 已起始連線 Broker ${BrokerId} 的備份
ADMIN_CONNECTION_SERVER_DISABLE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法停用連線 Broker ${BrokerId}
ADMIN_CONNECTION_SERVER_DISABLED	AUDIT_SUCCESS	${UserDisplayName} 正在停用連線 Broker ${BrokerId}
ADMIN_CONNECTION_SERVER_ENABLE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法啟用連線 Broker ${BrokerId}

表 14-7. Horizon Console 事件 (續)

EventType	嚴重性	ModuleAndEventText
ADMIN_CONNECTION_SERVER_ENABLED	AUDIT_SUCCESS	${UserDisplayName} 正在啟用連線 Broker ${BrokerId}
ADMIN_DATABASE_CONFIGURATION_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} 無法新增資料庫組態
ADMIN_DATABASE_CONFIGURATION_ ADDED	AUDIT_SUCCESS	${UserDisplayName} 已新增資料庫組態
ADMIN_DATABASE_CONFIGURATION_DELETE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法刪除資料庫組態
ADMIN_DATABASE_CONFIGURATION_DELETE_FAILED	AUDIT_SUCCESS	${UserDisplayName} 已刪除資料庫組態
ADMIN_DATABASE_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法更新資料庫組態
ADMIN_DATABASE_CONFIGURATION_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已更新資料庫組態
ADMIN_DEFAULT_DESKTOPPOOL_ASSIGN	AUDIT_SUCCESS	${UserDisplayName} 已將預設桌面的集區 ${DesktopId} 指定至 ${UserName}
ADMIN_DEFAULT_DESKTOPPOOL_ASSIGN_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將預設桌面的集區 ${DesktopId} 指定至 ${UserName}
ADMIN_DEFAULT_DESKTOPPOOL_UNASSIGN	AUDIT_SUCCESS	${UserDisplayName} 已移除至 ${UserName} 的預設桌面集區指定
ADMIN_DEFAULT_DESKTOPPOOL_UNASSIGN_FAILED	AUDIT_FAIL	${UserDisplayName} 無法移除至 ${UserName} 的預設桌面集區指定
ADMIN_DESKTOP_ADDED	AUDIT_SUCCESS	${UserDisplayName} 已新增集區 ${DesktopId}
ADMIN_DESKTOP_ASSIGN	AUDIT_SUCCESS	${UserDisplayName} 已將桌面${MachineName} 指定至 ${UserName}
ADMIN_DESKTOP_ASSIGN_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將桌面${MachineName} 指定至 ${UserName}
ADMIN_DESKTOP_EDITED	AUDIT_SUCCESS	${UserDisplayName} 已編輯集區 ${DesktopId} (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_DESKTOP_MAINTENANCE_MODE_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將桌面${MachineName} 更新為 ${MaintenanceMode} 維護模式
ADMIN_DESKTOP_MAINTENANCE_MODE_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已將桌面${MachineName} 更新為 ${MaintenanceMode} 維護模式
ADMIN_DESKTOP_UNASSIGN	AUDIT_SUCCESS	${UserDisplayName} 已移除對桌面${MachineName} 的指定
ADMIN_DESKTOP_UNASSIGN_FAILED	AUDIT_FAIL	${UserDisplayName} 無法移除對桌面${MachineName} 的指定

表 14-7. Horizon Console 事件 (續)

EventType	嚴重性	ModuleAndEventText
ADMIN_ENABLE_DESKTOP_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將集區 ${DesktopId} 設為 ${EnableStatus}
ADMIN_ENABLE_DESKTOP_SUCCEEDED	AUDIT_SUCCESS	${UserDisplayName} 已將集區 ${DesktopId} 設為 ${EnableStatus}
ADMIN_ENABLED_DESKTOP_PROVISION_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將集區 ${DesktopId} 的佈建設為 ${EnableStatus}
ADMIN_ENABLED_DESKTOP_PROVISION_SUCCEEDED	AUDIT_SUCCESS	${UserDisplayName} 已將集區 ${DesktopId} 的佈建設為 ${EnableStatus}
ADMIN_EVENT_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法更新事件組態
ADMIN_EVENT_CONFIGURATION_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已更新全域組態
ADMIN_FOLDER_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} 無法新增資料夾 ${AdminFolderName}
ADMIN_FOLDER_ADDED	AUDIT_SUCCESS	${UserDisplayName} 已新增資料夾 ${AdminFolderName}
ADMIN_FOLDER_CHANGE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將物件 ${ObjectID}(type=${ObjectType}) 變更為資料夾 ${AdminFolderName}
ADMIN_FOLDER_CHANGED	AUDIT_SUCCESS	${UserDisplayName} 已將物件 ${ObjectID}(type=${ObjectType}) 變更為資料夾 ${AdminFolderName}
ADMIN_FOLDER_DELETE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法刪除資料夾 ${AdminFolderName}
ADMIN_FOLDER_DELETED	AUDIT_SUCCESS	${UserDisplayName} 已刪除資料夾 ${AdminFolderName}
ADMIN_GLOBAL_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法更新全域組態
ADMIN_GLOBAL_CONFIGURATION_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已更新全域組態 (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_GLOBAL_POLICY_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法更新全域原則
ADMIN_GLOBAL_POLICY_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已更新全域原則 (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_PERFMON_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法更新效能監視組態
ADMIN_PERFMON_CONFIGURATION_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已更新效能監視組態

表 14-7. Horizon Console 事件 (續)

EventType	嚴重性	ModuleAndEventText
ADMIN_PERMISSION_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將角色 ${AdminRoleName} 對資料夾 ${AdminFolderName} 的權限新增至 ${AdminPermissionEntity}
ADMIN_PERMISSION_ADDED	AUDIT_SUCCESS	${UserDisplayName} 已將角色 ${AdminRoleName} 對資料夾 ${AdminFolderName} 的權限新增至 ${AdminPermissionEntity}
ADMIN_PERMISSION_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法從 ${AdminPermissionEntity} 移除角色 ${AdminRoleName} 對資料夾 ${AdminFolderName} 的權限
ADMIN_PERMISSION_REMOVED	AUDIT_SUCCESS	${UserDisplayName} 已從 ${AdminPermissionEntity} 移除角色 ${AdminRoleName} 對資料夾 ${AdminFolderName} 的權限
ADMIN_POOL_POLICY_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法更新集區 ${DesktopId} 原則
ADMIN_POOL_POLICY_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已更新集區 ${DesktopId} 原則 (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_REMOVE_DESKTOP_ENTITLEMENT	AUDIT_SUCCESS	${UserDisplayName} 已取消賦予集區 ${DesktopId} 的 ${EntitlementDisplay} 權利
ADMIN_REMOVE_DESKTOP_FAILED	AUDIT_FAIL	${UserDisplayName} 無法移除集區 ${DesktopId}
ADMIN_REMOVE_DESKTOP_SUCCEEDED	AUDIT_SUCCESS	${UserDisplayName} 已移除集區 ${DesktopId}
ADMIN_ROLE_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} 無法新增具備 ${AdminPrivilegeName} 權限的角色 ${AdminRoleName}
ADMIN_ROLE_ADDED	AUDIT_SUCCESS	${UserDisplayName} 已新增具備 ${AdminPrivilegeName} 權限的角色 ${AdminRoleName}
ADMIN_ROLE_PRIV_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將角色 ${AdminRoleName} 更新為權限 ${AdminPrivilegeName}
ADMIN_ROLE_PRIV_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已將角色 ${AdminRoleName} 更新為權限 ${AdminPrivilegeName}
ADMIN_ROLE_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法移除角色 ${AdminRoleName}
ADMIN_ROLE_REMOVED	AUDIT_SUCCESS	${UserDisplayName} 已移除角色 ${AdminRoleName}

表 14-7. Horizon Console 事件 (續)

EventType	嚴重性	ModuleAndEventText
ADMIN_ROLE_RENAME_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將角色 ${AdminRoleName} 重新命名為 ${AdminRoleNewName}
ADMIN_ROLE_RENAMED	AUDIT_SUCCESS	${UserDisplayName} 已將角色 ${AdminRoleName} 重新命名為 ${AdminRoleNewName}
ADMIN_SECURITY_SERVER_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} 無法新增安全伺服器 ${SecurityServerId}
ADMIN_SECURITY_SERVER_ADDED	AUDIT_SUCCESS	${UserDisplayName} 已新增安全伺服器 ${SecurityServerId}
ADMIN_SECURITY_SERVER_EDIT_FAILED	AUDIT_FAIL	${UserDisplayName} 無法編輯安全伺服器 ${SecurityServerId}
ADMIN_SECURITY_SERVER_EDITED	AUDIT_SUCCESS	${UserDisplayName} 已編輯安全伺服器 ${SecurityServerId} (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_SECURITY_SERVER_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法移除安全伺服器 ${SecurityServerId}
ADMIN_SECURITY_SERVER_REMOVED	AUDIT_SUCCESS	${UserDisplayName} 已移除安全伺服器 ${SecurityServerId}
ADMIN_SESSION_SENDMSG	AUDIT_SUCCESS	${UserDisplayName} 已將訊息 (${SessionMessage}) 傳送至工作階段 (使用者 ${UserName}，桌面${MachineName})
ADMIN_SESSION_SENDMSG_FAILED	AUDIT_FAIL	${UserDisplayName} 無法將訊息 (${SessionMessage}) 傳送至工作階段 ${ObjectId}
ADMIN_SVI_ADD_DEPLOYMENT_GROUP_FAILED	AUDIT_FAIL	無法新增 ${SVIParentVM} 的部署群組: ${SVISnapshot}
ADMIN_SVI_ADD_DEPLOYMENT_GROUP_SUCCEEDED	AUDIT_SUCCESS	已新增 ${SVIParentVM} 的部署群組 ${SVIDeploymentGroupID}: ${SVISnapshot}
ADMIN_SVI_ADD_UDD_FAILED	AUDIT_FAIL	無法新增使用者資料磁碟 ${UserDiskName}
ADMIN_SVI_ADD_UDD_SUCCEEDED	AUDIT_SUCCESS	已新增使用者資料磁碟 ${UserDiskName}
ADMIN_SVI_ADMIN_ADDED	AUDIT_SUCCESS	${UserDisplayName} 已新增 SVI QuickPrep 網域 ${SVIAdminFqdn}(${SVIAdminName})
ADMIN_SVI_ADMIN_REMOVED	AUDIT_SUCCESS	${UserDisplayName} 已移除 SVI QuickPrep 網域 (id=${SVIAdminID})

表 14-7. Horizon Console 事件 (續)

EventType	嚴重性	ModuleAndEventText
ADMIN_SVI_ADMIN_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已更新 SVI QuickPrep 網域 ${SVIAdminFqdn}(${SVIAdminName})
ADMIN_SVI_ATTACH_UDD_FAILED	AUDIT_FAIL	無法要求將使用者資料磁碟 ${UserDiskName} 連接至虛擬機器 ${SVIVMID}
ADMIN_SVI_ATTACH_UDD_SUCCEEDED	AUDIT_SUCCESS	已要求將使用者資料磁碟 ${UserDiskName} 連接至虛擬機器 ${SVIVMID}
ADMIN_SVI_DELETE_UDD_FAILED	AUDIT_FAIL	無法刪除使用者資料磁碟 ${UserDiskName}
ADMIN_SVI_DELETE_UDD_SUCCEEDED	AUDIT_SUCCESS	已刪除使用者資料磁碟 ${UserDiskName}
ADMIN_SVI_DETACH_UDD_FAILED	AUDIT_FAIL	無法要求中斷使用者資料磁碟 ${UserDiskName} 與虛擬機器 ${SVIVMID} 的連結
ADMIN_SVI_DETACH_UDD_SUCCEEDED	AUDIT_SUCCESS	已要求中斷使用者資料磁碟 ${UserDiskName} 與虛擬機器 ${SVIVMID} 的連結
ADMIN_SVI_REBALANCE_VM_FAILED	AUDIT_FAIL	無法重新平衡虛擬機器 ${SVIVMID}
ADMIN_SVI_REBALANCE_VM_SUCCEEDED	AUDIT_SUCCESS	已重新平衡虛擬機器 ${SVIVMID}
ADMIN_SVI_REFRESH_VM_FAILED	AUDIT_FAIL	無法重新整理虛擬機器 ${SVIVMID}
ADMIN_SVI_REFRESH_VM_SUCCEEDED	AUDIT_SUCCESS	已重新整理虛擬機器 ${SVIVMID}
ADMIN_SVI_RESYNC_VM_FAILED	AUDIT_FAIL	無法將虛擬機器 ${SVIVMID} 依照部署群組 ${SVIDeploymentGroupID} 重新同步
ADMIN_SVI_RESYNC_VM_SUCCEEDED	AUDIT_SUCCESS	已將虛擬機器 ${SVIVMID} 依照部署群組 ${SVIDeploymentGroupID} 重新同步
ADMIN_SVI_UPDATE_POOL_DEPLOYMENT_GROUP_FAILED	AUDIT_FAIL	無法將集區 ${DesktopId} 更新至部署群組 ${SVIDeploymentGroupID}
ADMIN_SVI_UPDATE_POOL_DEPLOYMENT_GROUP_SUCCEEDED	AUDIT_SUCCESS	已將集區 ${DesktopId} 更新至部署群組 ${SVIDeploymentGroupID}
ADMIN_SVI_UPDATE_UDD_FAILED	AUDIT_FAIL	無法更新使用者資料磁碟 ${UserDiskName}
ADMIN_SVI_UPDATE_UDD_SUCCEEDED	AUDIT_SUCCESS	已將使用者資料磁碟 ${UserDiskName} 集區設為 ${DesktopId}，並將使用者設為 ${UserName}
ADMIN_UNREGISTER_PM	AUDIT_SUCCESS	${UserDisplayName} 已取消註冊實體機器 ${MachineName}

表 14-7. Horizon Console 事件 (續)

EventType	嚴重性	ModuleAndEventText
ADMIN_UNREGISTER_PM_FAILED	AUDIT_FAIL	${UserDisplayName} 無法取消註冊實體機器 ${MachineName}
ADMIN_USER_INFO_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法使用 AD 伺服器更新 ${UserName} 的使用者資訊
ADMIN_USER_INFO_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已使用 AD 伺服器更新 ${UserName} 的使用者資訊
ADMIN_USER_POLICY_DELETE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法刪除使用者 ${UserName} 的集區 ${DesktopId} 覆寫原則
ADMIN_USER_POLICY_DELETED	AUDIT_SUCCESS	${UserDisplayName} 已刪除使用者 ${UserName} 的集區 ${DesktopId} 覆寫原則 (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_USER_POLICY_UPDATE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法更新使用者 ${UserName} 的集區 ${DesktopId} 原則
ADMIN_USER_POLICY_UPDATED	AUDIT_SUCCESS	${UserDisplayName} 已更新使用者 ${UserName} 的集區 ${DesktopId} 原則 (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_USERLOGGEDIN	AUDIT_SUCCESS	使用者 ${UserDisplayName} 已登入 Horizon Console
ADMIN_USERLOGGEDOUT	AUDIT_SUCCESS	使用者 ${UserDisplayName} 已登出 Horizon Console
ADMIN_VC_ADD_FAILED	AUDIT_FAIL	${UserDisplayName} 無法新增 VC 伺服器 ${VCAddress}
ADMIN_VC_ADDED	AUDIT_SUCCESS	${UserDisplayName} 已新增 VC 伺服器 ${VCAddress}
ADMIN_VC_EDITED	AUDIT_SUCCESS	${UserDisplayName} 已編輯 VC 伺服器 ${VCAddress} (${AttrChangeType}: ${AttrName} = ${AttrValue})
ADMIN_VC_LICINV_ALARM_DISABLED	AUDIT_SUCCESS	VC 伺服器 ${VCAddress} 上授權詳細目錄監視的警示已停用，因為所有主機都有桌面授權
ADMIN_VC_REMOVE_FAILED	AUDIT_FAIL	${UserDisplayName} 無法移除 VC 伺服器 ${VCAddress}
ADMIN_VC_REMOVED	AUDIT_SUCCESS	${UserDisplayName} 已移除 VC 伺服器 ${VCAddress}

事件訊息屬性

ModuleAndEventText 訊息會使用特定的屬性。若要判斷屬性的資料類型，您可以檢查其 event_data 或 event_data_historical 資料表中的類型資料行值。

表 14-8. ModuleAndEventText 訊息使用的屬性

屬性名稱	說明
AdminFolderName	需要特殊存取權限的資料夾名稱。
AdminPermissionEntity	需要特殊存取權限的物件名稱。
AdminPrivilegeName	管理權限的名稱。
AdminRoleName	管理角色的名稱。
AdminRoleNewName	管理角色的新名稱。
AttrChangeType	套用至一般屬性的變更類型。
AttrName	一般屬性的名稱。
AttrValue	一般屬性的值。
BrokerId	連線伺服器執行個體的識別碼。
BrokerName	連線伺服器執行個體的名稱。
DesktopDisplayName	桌面平台集區的顯示名稱。
DesktopId	桌面平台集區的識別碼。
EntitlementDisplay	桌面平台權利的顯示名稱。
MachineId	實體或虛擬機器的名稱。
MachineName	實體或虛擬機器的名稱。
MaintenanceMode	維護模式狀態。
ObjectID	詳細目錄物件的識別碼。
ObjectType	詳細目錄物件的類型。
PolicyDisplayName	原則的顯示名稱。
PolicyObject	原則物件的識別碼。
PolicyValue	原則物件的值。
ProtocolId	顯示通訊協定的識別碼。
SecurityServerId	安全伺服器的識別碼。
SVIAdminFqdn	QuickPrep 網域的 FQDN。
SVIAdminID	QuickPrep 網域的識別碼。
SVIAdminName	QuickPrep 網域的名稱。
時間	日期和時間值。
UserCount	24 小時期間內桌面平台使用者的數目上限。

表 14-8. ModuleAndEventText 訊息使用的屬性 (續)

屬性名稱	說明
UserDiskName	使用者資料磁碟的名稱。
UserDisplayName	DOMAIN\username 格式的使用者名稱。
UserName	Active Directory 中的使用者名稱。
VCAddress	vCenter Server 的 URL。

範例資料庫查詢和視圖

您可以查詢 event_historical 資料庫以顯示錯誤事件、警告事件和特定的最近事件。

備註 請將下列範例中的 dbo.VE_ 首碼取代為您事件資料庫適用的首碼。

列出錯誤事件

下列查詢會顯示 event_historical 資料表中的所有錯誤事件。

```
CREATE VIEW error_events AS
    (
    SELECT ev.EventID, ev.Time, ev.Module, ev.EventType, ev.ModuleAndEventText
        FROM dbo.VE_event_historical AS ev
        WHERE ev.Severity = 'ERROR'
    );
```

列出警告事件

下列查詢會顯示 event_historical 資料表中的所有警告事件。

```
CREATE VIEW warning_events AS
    (
    SELECT ev.EventID, ev.Time, ev.Module, ev.EventType, ev.ModuleAndEventText
        FROM dbo.VE_event_historical AS ev
        WHERE ev.Severity = 'WARNING'
    );
```

列出最近事件

下列查詢會列出與網域 MYDOM 中使用者 fred 相關聯的所有最近事件。

```
CREATE VIEW user_fred_events AS
    (
    SELECT ev.EventID, ev.Time, ev.Module, ev.EventType, ev.Severity, ev.Acknowledged
        FROM dbo.VE_event_historical AS ev,
            dbo.VE_event_data_historical AS ed
        WHERE ev.EventID = ed.EventID AND ed.Name = 'UserDisplayName' AND ed.StrValue =
```

```
            'MYDOM\fred'
    );
```

下列查詢會列出機器上代理程式關閉的所有最近事件。

```
CREATE VIEW agent_shutdown_events AS
    (
    SELECT ev.EventID, ev.Time, ed.StrValue
        FROM dbo.VE_event_historical AS ev,
            dbo.VE_event_data_historical AS ed
        WHERE ev.EventID = ed.EventID AND ev.EventType = 'AGENT_SHUTDOWN' AND
            ed.Name = 'MachineName'
    );
```

下列查詢會列出桌面平台因桌面平台集區是空的而無法啟動的所有最近事件。

```
CREATE VIEW desktop_launch_failure_events AS
    (
    SELECT ev.EventID, ev.Time, ed1.StrValue, ed2.StrValue
        FROM dbo.VE_event_historical AS ev,
            dbo.VE_event_data_historical AS ed1,
            dbo.VE_event_data_historical AS ed2
        WHERE ev.EventID = ed1.EventID AND ev.EventID = ed2.EventID AND
            ev.EventType = 'BROKER_POOL_EMPTY' AND
            ed1.Name = 'UserDisplayName' AND ed2.Name = 'DesktopId'
    );
```

下列查詢會列出管理員已移除桌面平台集區的所有最近事件。

```
CREATE VIEW desktop_pool_removed_events AS
    (
    SELECT ev.EventID, ev.Time, ed1.StrValue, ed2.StrValue
        FROM dbo.VE_event_historical AS ev,
            dbo.VE_event_data_historical AS ed1,
            dbo.VE_event_data_historical AS ed2
        WHERE ev.EventID = ed1.EventID AND ev.EventID = ed2.EventID AND
            ev.EventType = 'ADMIN_DESKTOP_REMOVED' AND
            ed1.Name = 'UserDisplayName' AND ed2.Name = 'DesktopId'
);
```

自訂 LDAP 資料

15

您可以使用 VMware 和 Microsoft 命令列工具，對 VMware Horizon 匯入和匯出 LDAP 組態資料。這些命令列工具會匯入和匯出 LDAP 資料交換格式 (LDIF) 組態檔中的 LDAP 組態資料。

此功能適用於想要執行自動大量組態作業的進階管理員。若要建立用來更新 VMware Horizon 組態的指令碼，請使用 Horizon PowerCLI 模組。

本章節討論下列主題：

LDAP 組態資料簡介

所有 VMware Horizon 組態資料皆儲存在 LDAP 目錄中。每個 Horizon Connection Server 的標準或複本執行個體皆包含本機 LDAP 組態存放庫，以及與每個連線伺服器執行個體之間的複寫協議。此安排可確保對一個存放庫的變更會自動複寫至所有其他存放庫。

當您使用 Horizon Console 修改 VMware Horizon 組態時，存放庫中的適當 LDAP 資料將隨之更新。例如，如果您新增桌面平台集區，則 VMware Horizon 會將使用者、使用者群組和權利的相關資訊儲存在 LDAP 中。連線伺服器執行個體會自動管理其他 LDAP 組態資料，並使用存放庫中的資訊來控制 VMware Horizon 作業。

您可以使用 LDIF 組態檔來執行多項工作，包括在連線伺服器執行個體之間傳輸組態資料，以及備份 VMware Horizon 組態以便能夠還原連線伺服器執行個體的狀態。

您也可以使用 LDIF 組態檔來定義大量 VMware Horizon 物件 (例如桌面平台集區)，並將那些物件新增至您的連線伺服器執行個體，而不需使用 Horizon Console 手動執行工作。

VMware Horizon 會執行 LDAP 存放庫的定期備份。

LDAP 組態資料會以 ASCII 純文字的形式傳輸，且符合網際網路工程任務推動小組 (IETF) RFC 2849 標準。

修改 LDAP 組態資料

您可以將 Horizon Connection Server 執行個體上的 LDAP 組態資料匯出至 LDIF 組態檔、修改 LDIF 組態檔，然後將修改的 LDIF 組態檔匯入其他連線伺服器執行個體中，以執行自動的大量組態作業。

您可以檢查匯出的 LDIF 組態檔內容，以便在 Horizon 中取得任何 LDAP 組態資料項目所適用的 LDIF 語法範例。例如，您可以擷取桌面平台集區的資料，並使用該資料作為建立大量桌面平台集區的範本。

匯出 LDAP 組態資料

您可以使用 vdmexport 命令列公用程式，將組態資料從標準或複本連線伺服器執行個體匯出至 LDIF 組態檔。

程序

1 以「管理員」或「管理員 (唯讀)」角色的使用者身分登入標準或複本連線伺服器執行個體。

您必須以具有「管理員」或「管理員 (唯讀)」角色的使用者身分登入，才能從 Horizon 組態存放庫中匯出組態資料。

2 在命令提示字元中輸入 vdmexport 命令。

依預設，vdmexport 命令列公用程式會安裝在 C:\Program Files\VMware\VMware View\Server\tools\bin 目錄中。

vdmexport 命令具有下列選項。

選項	敘述
-f	LDAP 備份的輸出檔案名稱。
-v	輸出檔案為逐字輸出 (未加密)。
-c	與 -v 選項類似，但機密屬性值未包括在輸出檔案中。
-k	僅輸出 kiosk 用戶端項目和相關 FSP。
-g	備份 Cloud Pod 架構 全域 LDAP，而非本機 LDAP。

例如，以下命令會將本機 LDIF 組態檔匯出。

```
vdmexport -f mylocalexport.LDF
```

下列命令會備份 Cloud Pod 架構 全域 LDAP。

```
vdmexport -f myglobalexport.LDF -g
```

結果

vdmexport 命令會將連線伺服器執行個體的組態寫入至您指定的檔案。如果您的角色權限不足而無法檢視組態存放庫中的資料，則命令會顯示錯誤。

在 LDIF 組態檔中定義桌面平台集區

您可以在 LDIF 組態檔中定義桌面平台集區，並匯入自訂的 LDIF 組態檔以建立大量桌面平台集區。

備註 您也可以為 LDAP 存放庫中定義的其他物件建立自訂的 LDIF 組態檔，其中包括全域組態設定、特定 Horizon Connection Server 執行個體或安全伺服器的組態設定，以及特定使用者的組態設定。

若要在 LDIF 組態檔中定義桌面平台集區，您必須將下列項目新增至檔案。

- 桌面平台集區中每個虛擬桌面平台的虛擬桌面平台虛擬機器項目
- 每個桌面平台集區的虛擬機器集區項目
- 定義桌面平台集區之權利的桌面平台應用程式項目

您可以將每個虛擬機器集區項目與一個桌面平台應用程式項目建立一對一關係的關聯。桌面平台應用程式項目無法在虛擬機器集區項目之間共用，且一個虛擬機器集區項目只能與一個桌面平台應用程式項目建立關聯。

下表說明您在修改 LDIF 組態檔中桌面平台集區定義時必須指定的屬性。

表 15-1. 用來定義桌面平台集區的重要屬性

項目	屬性	說明
虛擬桌面平台虛擬機器 虛擬機器集區 桌面平台應用程式	cn	項目的一般名稱。如果需要自動產生名稱，請指定全域唯一識別碼 (GUID) 字串。您可以使用任何可靠的 GUID 產生器，如 .NET 所提供的機制 (例如，在 Visual Basic 中呼叫 System.Guid.NewGuid().ToString())。
桌面平台應用程式	成員	有權存取桌面平台集區之 Active Directory (AD) 使用者和群組的清單。此屬性會以 Windows 安全性識別碼 (SID) 參考的格式進行指定。成員值 <SID=S-1-2-3-4> 表示 SID 值為 S-1-2-3-4 的 AD 使用者或群組。 在 LDIF 格式中，左角括弧 (<) 是保留字元，因此您必須在屬性名稱後面加上兩個冒號 (::)，並指定 Base 64 格式的 SID 值 (例如 PFNJRD1TLTEtMi0zLTQ+IA==)。此為多重值屬性，因此您可以在多行上使用此屬性，以代表 SID 清單中的每個項目。

範例 LDIF 組態檔桌面平台集區項目

下列範例節錄自 LDIF 組態檔。其中顯示稱為 Pool1 之桌面平台集區 (包含名為 VM1 和 VM2 的兩個虛擬桌面平台) 的範例項目。桌面平台集區項目會與同樣名為 Pool1 的桌面平台應用程式項目進行配對。

```
#
# Virtual Desktop VM entry VM1
#
DN: CN=vm1,OU=Servers,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-Server
objectClass: pae-WinServer
objectClass: pae-ThinWinServer
objectClass: pae-VM
cn: vm1
description: sample virtual desktop entry
pae-VmSuspended:: IA==
pae-OptIgnoreProcessList: 0
pae-MOID: vm-1
pae-VmState: READY
pae-ServerManaged: 1
pae-SSOEnabled: 1
pae-DisplayName: virtual desktop 1
pae-TunneledConnection: 1
```

```
pae-pwdEncryption: KERB5
ipHostNumber: vm1
pae-ClientProtVersion: 1
pae-WinDomain: NULL
pae-thinProto: XP_RDP
pae-Services: SESSION |, HEARTBEAT |, EVENTS |, USED |
pae-VmPath: /New Datacenter/vm/vm-1
pae-OptSuspendTimeout: 0
pae-OptDisconnectLimitTimeout: 0
pae-OptMaximumSessions: 0
pae-Disabled: 0

#
# Virtual Desktop VM entry VM2
#
DN: CN=vm2,OU=Servers,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-Server
objectClass: pae-WinServer
objectClass: pae-ThinWinServer
objectClass: pae-VM
cn: vm2
description: sample virtual desktop entry
pae-VmSuspended:: IA==
pae-OptIgnoreProcessList: 0
pae-MOID: vm-2
pae-VmState: READY
pae-ServerManaged: 1
pae-SSOEnabled: 1
pae-DisplayName: virtual desktop 2
pae-TunneledConnection: 1
pae-pwdEncryption: KERB5
ipHostNumber: vm2
pae-ClientProtVersion: 1
pae-WinDomain: NULL
pae-thinProto: XP_RDP
pae-Services: SESSION |, HEARTBEAT |, EVENTS |, USED |
pae-VmPath: /New Datacenter/vm/vm-2
pae-OptSuspendTimeout: 0
pae-OptDisconnectLimitTimeout: 0
pae-OptMaximumSessions: 0
pae-Disabled: 0
#
# Further Virtual Desktop VM entries as required
#
#
# VM Pool entry Pool1
#
DN: CN=Pool1,OU=Server Groups,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-ServerPool
cn: Pool1
pae-VCDN: CN=b180b93b-2dd3-4b58-8a81-b8534a4b7565,OU=VirtualCenter,OU=Properties,DC=vdi,
```

```
DC=vmware,DC=int
pae-MemberDN: CN=vm1,OU=Servers,DC=vdi,DC=vmware,DC=int
pae-MemberDN: CN=vm2,OU=Servers,DC=vdi,DC=vmware,DC=int
pae-VmPowerPolicy: remainon
pae-VmProvEnabled: 1
pae-VmProvSuspendOnError: 1
pae-VmStartClone: 1
pae-VmPoolCalculatedValues: 1
pae-ServerPoolType: 0
pae-VmMinimumCount: 0
pae-VmHeadroomCount: 0
pae-VmMaximumCount: 0
pae-Disabled: 0

#
# Desktop Application entry Pool1 -- one entry is required for each VM Pool
#
DN: CN=Pool1,OU=Applications,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-Entity
objectClass: pae-App
objectClass: pae-WinApp
objectClass: pae-ThinWinApp
objectClass: pae-DesktopApplication
cn: Pool1
member:: PFNJRD1TLTEtMi0zLTQ+IA==
pae-Icon: /thinapp/icons/desktop.gif
pae-URL: \
pae-Servers: CN=Pool1,OU=Server Groups,DC=vdi,DC=vmware,DC=int
pae-ServerProtocolLevel: OSX_NETOP
pae-ServerProtocolLevel: OS2_NETOP
pae-ServerProtocolLevel: NT4_NETOP
pae-ServerProtocolLevel: WIN2K_NETOP
pae-ServerProtocolLevel: NT4_RDP
pae-ServerProtocolLevel: WIN2K_RDP
pae-ServerProtocolLevel: XP_RDP
pae-Disabled: 0
```

匯入 LDAP 組態資料

您可以使用 `vdmimport` 命令將 LDIF 組態檔中的組態資料匯入至標準或複本連線伺服器執行個體。

必要條件

- 將 LDAP 組態資料匯出至 LDIF 組態檔。請參閱匯出 LDAP 組態資料。
- 如果您要匯入 Cloud Pod 架構全域 LDIF 組態檔，請確認已在連線伺服器執行個體上初始化 Cloud Pod 架構 功能。

程序

1 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。

  您必須以具有管理員角色的使用者身分登入，才能將組態資料匯入 Horizon 組態存放庫中。

2 在命令提示字元中輸入 vdmimport 命令。

依預設，vdmimport 命令列公用程式會安裝在 C:\Program Files\VMware\VMware View\Server\tools\bin 目錄中。

vdmimport 命令具有下列選項。

選項	敘述
-f	輸入檔案名稱。
-i	顯示與指定的 LDIF 組態檔有關的檔案資訊。
-d	將指定的 LDIF 組態檔解密。
-p	指定將加密的 LDIF 組態檔解密時所使用的復原密碼。在出現提示時輸入 "" 作為密碼。
-g	指定還原是針對 Cloud Pod 架構環境而執行。

例如，下列命令會將本機 LDIF 組態檔解密並匯入。

```
vdmimport -d -p mypassword -f MyEncryptedxport.LDF > MyDecryptedexport.LDF
```

```
vdmimport -f MyDecryptedexport.LDF
```

下列命令會將 Cloud Pod 架構全域 LDIF 組態檔解密並匯入。

```
vdmimport -d -p mypassword -f MyEncryptedCPAexport.LDF > MyDecryptedCPAexport.LDF
```

```
vdmimport -g -f MyDecryptedCPAexport.LDF
```

結果

vdmimport 命令執行後，連線伺服器執行個體的組態會以該檔案中的資料進行更新，且會顯示已成功更新的記錄數目。如果有部分記錄因為您角色的權限不足而無法更新，則會出現錯誤。

將 VMware Horizon 部署連線至 Horizon Control Plane

16

VMware Horizon 可讓您靈活地在內部部署、雲端主控環境，或兩者的混合環境中部署虛擬桌面平台和應用程式。

無論您的虛擬桌面平台和應用程式在何處執行，您都可以選擇性地將 VMware Horizon 執行個體連線至 Horizon Control Plane，並獲得下列服務和優點。

- Horizon Cloud 管理員主控台在內部部署和多雲端部署間提供單一的整合主控台，可與承租人的雲端連線網繭機群搭配運作。
- Horizon Universal Broker 是雲端式代理技術，用來管理多雲端指派的虛擬資源並將其配置給您的使用者。
- 雲端監控服務 (CMS) 是 Horizon 控制平面中提供的一項中心服務。CMS 可讓您監控雲端連線網繭機群內和其間的容量、使用量和健全狀況，無論個別網繭所在的部署環境為何。
- Horizon 映像管理服務是一項雲端式服務，可讓您以簡便且自動化的方式管理雲端連線 Horizon 網繭中的桌面指派 (例如桌面平台集區和伺服器陣列) 所使用的系統映像。

Horizon Control Plane 已啟用訂閱授權。您也必須使用 Horizon Cloud Connector 虛擬應用裝置，將您的 VMware Horizon 部署與 Horizon Control Plane 連線。如需關於訂閱授權的詳細資訊，請參閱《Horizon 安裝》文件中的〈啟用 VMware Horizon 以進行訂閱授權和 Horizon Control Plane 服務〉。

《Horizon 架構規劃》文件提供部署 VMware Horizon 的概觀和需求。如需 Horizon Control Plane 的相關資訊，請參閱 VMware Horizon Cloud Service 說明文件中的 Horizon Cloud 簡介。

使用 Horizon PowerCLI 模組

17

Horizon PowerCLI 模組包含您可以用來在 Horizon 元件上執行各種管理工作的 Horizon PowerCLI Cmdlet。您可以使用 Horizon PowerCLI 搭配 API 規格，建立以社群為基礎的開放原始碼指令碼。

您可以在安裝 VMware PowerCLI 時安裝 Horizon PowerCLI 模組。

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

如需用來建立進階功能和指令碼以用於 Horizon PowerCLI 之 API 規格的相關資訊，請參閱 https://code.vmware.com/apis/405/view 的 View API 參考。

如需關於能用來建立自有 Horizon PowerCLI 指令碼之範例指令碼的詳細資訊，請造訪 https://github.com/vmware/PowerCLI-Example-Scripts 的 PowerCLI 社群。

本章節討論下列主題：

設定 Horizon PowerCLI 模組

您可以使用 VMware PowerCLI 來設定 Horizon PowerCLI 模組，並使用 Horizon PowerCLI Cmdlet 來連線或自連線伺服器中斷連線。連線至連線伺服器後，您可以撰寫用來叫用 Horizon API 的 PowerShell 指令碼。

程序

1 安裝 VMware PowerCLI。

從 PowerShell 資源庫安裝 VMware PowerCLI。若要安裝 VMware PowerCLI，請在 Windows PowerShell 提示字元中執行下列命令：

```
Install-Module -Name Vmware.PowerCLI
```

此命令會將所有 VMware PowerCLI 模組安裝到 Windows PowerShell。`VMware.VimAutomation.HorizonView` 模組即為 Horizon PowerCLI 模組。

您也可以從 https://code.vmware.com/web/dp/tool/vmware-powercli 下載並安裝 VMware PowerCLI。

如需關於如何安裝 VMware PowerCLI 的詳細資訊，請參閱 https://code.vmware.com/web/dp/tool/vmware-powercli 中的《VMware PowerCLI 使用者指南》。

2 在 Windows PowerShell 工作階段中匯入名為 `VMware.VimAutomation.HorizonView` 的 Horizon PowerCLI 模組。

使用下列命令將 `VMware.VimAutomation.HorizonView` 匯入至 Windows PowerShell 工作階段：

```
Import-Module -Name VMware.VimAutomation.HorizonView
```

`VMware.VimAutomation.HorizonView` 包含您可以用來連線至連線伺服器或與連線伺服器中斷連線的 `Connect-HVServer` 和 `Disconnect-HVServer` Cmdlet。

3 從 GitHub 存放庫提取範例指令碼。

使用 `Connect-HVServer` Cmdlet 連線至連線伺服器的 Horizon API 服務後，您可以執行用來叫用 Horizon API 的 PowerShell 指令碼。如需關於 Horizon API 的詳細資訊，請參閱 https://code.vmware.com/apis/405/view 中的《View API 參考》說明文件。

Horizon PowerCLI 模組的範例指令碼可在 https://github.com/vmware/PowerCLI-Example-Scripts 中的 [模組] 區段中以 `VMware.Hv.Helper` 模組的形式取得。

後續步驟

請直接使用範例指令碼或修改指令碼以符合您的自動化需求。除了範例指令碼，您也可以根據自己的需求開發用來叫用 Horizon API 的新指令碼。請參閱執行範例 Horizon PowerCLI 指令碼。

執行範例 Horizon PowerCLI 指令碼

您可以使用可叫用 Horizon API 的範例指令碼，並使用這些指令碼來執行管理員工作。您也可以根據自己的需求修改這些指令碼，以執行管理工作。

必要條件

- 完成安裝 VMware PowerCLI 和設定 Horizon PowerCLI 模組的步驟。請參閱設定 Horizon PowerCLI 模組 。

程序

1 從位於 https://github.com/vmware/PowerCLI-Example-Scripts 的 [模組] 區段下載 `VMware.Hv.Helper` 模組。

2 使用 `$env:PSModulePath` 命令來找出 Windows PowerShell 工作階段中的模組路徑，並將 `VMware.Hv.Helper` 模組複製到該位置。

3 使用下列命令來將 VMware.Hv.Helper 模組載入至您的 Windows PowerShell 工作階段，並開始使用指令碼。

```
 Get-Module -ListAvailable 'Vmware.Hv.Helper' | Import-Module; Get-Command -Module
'VMware.Hv.Helper'
```