在 VMware Identity Manager 中設定資源

修改日期 2017 年 11 月 3 日

VMware Identity Manager 2.9.1

vmware®

您可以在 VMware 網站上找到最新的技術說明文件，網址為:

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

如果您對此文件有何想法，請將您的回應意見提交至：

docfeedback@vmware.com

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

內容

關於在 VMware Identity Manager 中設定資源

*在 VMware Identity Manager 中設定資源*提供關於如何新增資源至 VMware Identity Manager 目錄的指示。指示包括透過使用者的系統 (例如透過其桌面平台和行動裝置) 自訂資源並進行使用的相關資訊。支援的資源包括 Web 應用程式、擷取為 ThinApp® 套件的 Windows 應用程式、View 桌面平台和應用程式集區，以及 Citrix 發行的資源。

主要對象

此資訊適用於設定和管理 VMware Identity Manager 資源的任何人。該資訊是針對熟悉虛擬機器技術且富有經驗的 Windows 或 Linux 系統管理員而撰寫。

在 VMware Identity Manager 中設定資源的簡介

1

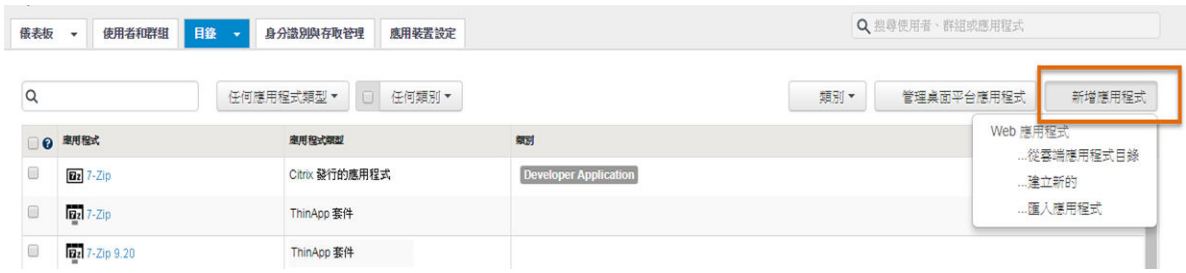
在安裝並設定 VMware Identity Manager 後，若要讓使用者能夠存取支援的資源，您必須在 VMware Identity Manager 管理主控台中啟用該資源。除了 Web 應用程式以外，在使用其他各個資源類型時，您都需要整合 VMware Identity Manager 與其他產品或元件。

您可以將下列類型的資源與 VMware Identity Manager 整合：

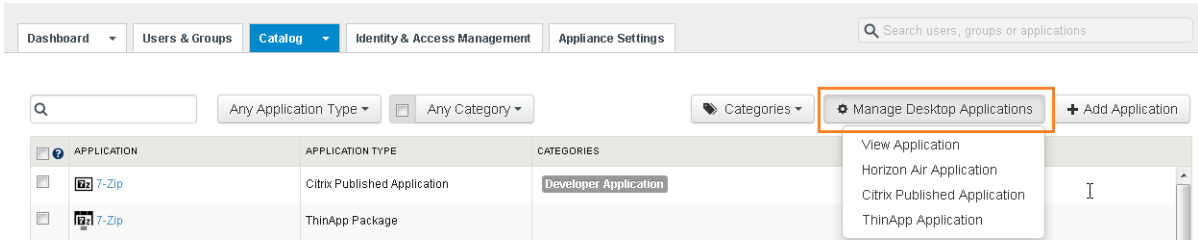
- Web 應用程式
- VMware Horizon® Cloud Service® 應用程式和桌面平台
- Horizon 7、Horizon 6 和 View 桌面平台和應用程式集區
- Citrix 發佈的資源
- ThinApp 封裝應用程式

您可以從管理主控台中的**目錄**索引標籤整合這些資源。

若要整合 Web 應用程式，您可以使用**目錄**索引標籤中的**新增應用程式**功能表。



若要整合並啟用 Horizon 7、Horizon 6 或 View 桌面平台和應用程式集區、VMware Horizon Cloud Service 桌面平台和應用程式、Citrix 發佈的資源或 ThinApp 封裝應用程式，您可以使用**目錄**索引標籤中的**管理桌面平台應用程式**功能表。



您可以在**目錄 > 設定**頁面中管理整合資源的全域設定。您可以透過選取**目錄**索引標籤中的應用程式，以管理個別應用程式的設定。

提供 Web 應用程式的存取權

2

在 VMware Identity Manager 服務中，您可以新增組織的外部 Web 應用程式並授權使用者存取它們。

若要讓使用者可透過服務存取 Web 應用程式，請確認符合下列需求：

- 如果您將 Web 應用程式設定為使用聯盟通訊協定，請使用 SAML 1.1、SAML 2.0 或 WS-Federation 1.2。將 Web 應用程式設定為使用聯盟通訊協定並非先決條件。
- 您打算要授與 Web 應用程式權利的使用者，即為該應用程式的登錄使用者，或是您想要為該應用程式設定佈建配接器 (如果適用)，以便將 VMware Identity Manager 使用者佈建在應用程式中。
- 如果 Web 應用程式是多承租人應用程式，服務會指向您的應用程式執行個體。

本章節討論下列主題:

將 Web 應用程式新增至組織的目錄

您可以將組織的 Web 應用程式新增至您的目錄，並且讓這些應用程式可供使用者和群組存取。

當您將 Web 應用程式的項目新增至目錄時，您會建立應用程式記錄，並設定 Web 應用程式的位址。VMware Identity Manager 服務會使用應用程式記錄作為範本，以建立 Web 應用程式的安全連線。

您可以使用下列方法，從 [目錄] 索引標籤將 Web 應用程式的應用程式記錄新增至您的目錄。

方法	說明
從雲端應用程式目錄	常用的企業 Web 應用程式類型會列在雲端應用程式目錄中。這些應用程式已完成部分設定。您必須完成其餘的應用程式記錄表單。
建立新的 Web 應用程式	您可以將未列在雲端應用程式目錄中的 Web 應用程式新增至您的目錄。這些 Web 應用程式的應用程式記錄具有比雲端應用程式目錄中的應用程式更高的通用性。您可以輸入應用程式說明和組態資訊，以建立應用程式記錄。
匯入 ZIP 或 JAR 檔案	您可以匯入先前在服務中設定的 Web 應用程式。您可以使用此方法，將預備部署移動至生產環境。在此情況下，您會從預備部署以 ZIP 檔案形式匯出 Web 應用程式。然後將 ZIP 檔案匯入至生產部署。

將 Web 應用程式新增至目錄後，您可以設定權利、存取原則、授權和佈建資訊。

Web 應用程式會新增至管理主控台。請以指派自您的 Active Directory 或 LDAP 目錄的管理員使用者角色登入。

從雲端應用程式目錄新增 Web 應用程式至您的目錄

雲端應用程式目錄已填入 Web 應用程式。這些應用程式在其應用程式記錄中包括部分資訊。從雲端應用程式目錄新增 Web 應用程式至您的目錄時，您必須提供其他資訊來完成應用程式記錄。您可能也需要與您的 Web 應用程式客戶代表合作，完成其他必要的設定。

雲端應用程式目錄中的許多應用程式使用安全性聲明標記語言 (SAML 1 或 SAML 2) 來交換驗證和授權資料，以確認該使用者可以存取 Web 應用程式。

新增 Web 應用程式至目錄時，您會建立間接指向 Web 應用程式的項目。該項目是透過應用程式記錄來定義，該記錄為包括連至 Web 應用程式的 URL 的表單。

您可以套用存取原則來控制使用者對應用程式的存取權。如果您不想要使用預設存取原則，請建立新原則。請參閱《*VMware Identity Manager 管理指南*》，以取得管理存取原則的相關資訊。

程序

1 在管理主控台中，按一下**目錄**索引標籤。

2 按一下**新增應用程式 > Web 應用程式 ...從雲端應用程式目錄**。

3 按一下您要新增的 Web 應用程式的圖示。

應用程式記錄會新增至您的目錄，隨即顯示 [詳細資料] 頁面，其中含有已指定的名稱和驗證設定檔。

4 (選擇性) 根據組織的需求，自訂 [詳細資料] 頁面上的資訊。

頁面上的項目隨即會填入 Web 應用程式的特定資訊。

視應用程式而定，您可以編輯部分項目。

表單項目	說明
名稱	應用程式的名稱。
說明	使用者可以讀取的應用程式的說明。
需要 VMware 瀏覽器	啟用此核取方塊可要求透過 iOS 和 Android 裝置上的 Workspace ONE 應用程式存取此應用程式時，僅能在 VMware 瀏覽器中加以開啟。
圖示	按一下**瀏覽**來上傳應用程式的圖示。支援 PNG、JPG 和 ICON 檔案格式的圖示，最大為 4 MB。 您上傳的應用程式圖示必須至少為 180 x 180 像素。如果圖示太小，則系統不會顯示。在該情況下，會顯示 Workspace ONE 圖示。
類別	若要允許應用程式顯示在目錄資源的類別搜尋中，請從下拉式功能表選取類別。您必須先前已建立類別。

5 按一下**儲存**。

6 按一下**組態**，編輯應用程式記錄的組態詳細資料，然後按一下**儲存**。

表單上的部分項目隨即會預先填入 Web 應用程式的特定資訊。部分預先填入的項目可供編輯，但其他則無法編輯。要求的資訊因應用程式而有所不同。

對於部分應用程式，表單會具有「應用程式參數」區段。如果應用程式的該區段存在，並且區段中的參數沒有預設值，請提供值以允許應用程式啟動。如果已提供預設值，您可以編輯該值。

7 選取**權利**、**授權**和**佈建**索引標籤，並視情況來自訂資訊。

索引標籤	說明
權利	授權使用者和群組使用應用程式。最初設定應用程式時或日後隨時可以設定權利。
存取原則	套用存取原則來控制使用者對應用程式的存取權。
授權	設定授權追蹤。新增授權資訊，供應用程式在報告中追蹤授權使用。
佈建	選取佈建配接器 (如果適用)。 佈建可從單一位置提供自動應用程式使用者管理。佈建配接器可允許 Web 應用程式在需要時從 VMware Identity Manager 服務擷取特定資訊。例如，若要啟用 Google Apps 的自動使用者佈建，Google Apps 資料庫中必須存在使用者帳戶資訊，例如使用者名稱、名字和姓氏。應用程式可能需要其他資訊，例如群組成員資格和授權角色資訊。 如需詳細資訊，請參閱使用佈建配接器。

下一個

如需關於為 Web 應用程式新增使用者和群組權利的詳細資料，請參閱讓使用者和群組有權使用 Web 應用程式。

透過匯入 ZIP 或 JAR 檔案新增 Web 應用程式至您的目錄

您可以將先前在 VMware Identity Manager 服務中設定的 Web 應用程式匯入到您的目錄。例如，您可能想要從您的預備環境匯入應用程式到您的生產環境。

此程序牽涉到從服務匯出應用程式服務包，並將它匯入至新環境。應用程式可能需要進一步的設定，特別是如果您是在原始環境中徹底測試了組態值。若要在匯入應用程式之後進一步設定 Web 應用程式，請參閱從雲端應用程式目錄新增 Web 應用程式至您的目錄或藉由建立新的應用程式記錄將 Web 應用程式新增至您的目錄。

程序

1 登入要從其匯出 Web 應用程式之服務的管理主控台。

2 按一下**目錄**索引標籤。

3 按一下**任何應用程式類型 > Web 應用程式**。

4 按一下要匯出之 Web 應用程式的圖示。

5 按一下**匯出**。

6 將壓縮的應用程式服務包儲存到您的本機系統。

7 登入要匯入 Web 應用程式之服務的管理主控台。

8 按一下**目錄**索引標籤。

9 按一下**新增應用程式 > Web 應用程式 ...匯入應用程式**。

10 按一下**瀏覽**，瀏覽至您將應用程式服務包儲存為 ZIP 檔案的本機系統位置，接著選取檔案，然後按一下**提交**。

11 視需要編輯 [詳細資料]、[組態]、[權利]、[存取原則]、[授權] 和 [佈建] 頁面上的資訊。

下一個

如需關於為 Web 應用程式新增使用者和群組權利的詳細資料，請參閱讓使用者和群組有權使用 Web 應用程式。如需佈建配接器的相關資訊，請參閱使用佈建配接器。

讓使用者和群組有權使用 Web 應用程式

將 Web 應用程式新增至您的目錄後，您可以為使用者和群組賦予應用程式的權利。

您可以將 Web 應用程式授權給 VMware Identity Manager 使用者。在您為使用者賦予 Web 應用程式的權利後，使用者將可檢視應用程式，並可從 Workspace ONE 入口網站加以啟動。如果您移除權利，使用者即無法檢視或啟動應用程式。

在許多情況下，要為使用者賦予 Web 應用程式的權利，最有效的方式是將 Web 應用程式權利新增至使用者群組。不過，在特定情況下，為個別使用者賦予 Web 應用程式的權利，是較恰當的作法。

程序

1 登入管理主控台。

2 為使用者賦予 Web 應用程式的權利。

方法	說明
存取 Web 應用程式，然後為使用者或群組賦予應用程式的權利。	a 按一下**目錄**索引標籤。 b 按一下**任何應用程式類型 > Web 應用程式**。 c 按一下要為使用者和群組賦予權利的 Web 應用程式。 Web 應用程式的資訊頁面會顯示依預設選取的**權利**索引標籤。群組權利和使用者權利會列於不同的表格中。 d 按一下**新增群組權利**或**新增使用者權利**。 e 輸入群組或使用者的名稱。 您可以開始輸入搜尋字串並讓自動完成功能列出選項，以搜尋使用者或群組，或者，您可以按一下**瀏覽**以檢視完整清單。 f 使用下拉式功能表，選取 Web 應用程式的啟動方式。 ■ **自動**會依預設在使用者下次登入 Workspace ONE 入口網站時，將應用程式顯示在 [啟動器] 頁面中。 ■ **使用者啟動**會要求使用者必須在 Workspace ONE 入口網站的 [目錄] 頁面中選取應用程式，並將其新增至 [啟動器] 頁面才能啟動應用程式。 g 按一下**儲存**。
存取使用者或群組，然後將 Web 應用程式權利新增至該使用者或群組。	a 按一下**使用者和群組**索引標籤。 b 按一下**使用者**索引標籤或**群組**索引標籤。 c 按一下使用者或群組的名稱。 d 按一下**應用程式**索引標籤，然後按一下**新增權利**。 e 在**應用程式類型**下拉式清單中，選取 **Web 應用程式**。 f 選取您要為使用者或群組賦予權利之 Web 應用程式旁的核取方塊。 g 在**部署**資料行中，選取每個 Web 應用程式的啟動方式。 ■ **自動**會依預設在使用者下次登入 Workspace ONE 入口網站時，將應用程式顯示在 [啟動器] 頁面中。 ■ **使用者啟動**會要求使用者必須在 Workspace ONE 入口網站的 [目錄] 頁面中選取應用程式，並將其新增至 [啟動器] 頁面才能啟動應用程式。 h 按一下**儲存**。

選取的使用者或群組此時會被賦予使用 Web 應用程式的權利。

使用佈建配接器

佈建可從單一位置提供自動應用程式使用者管理。佈建配接器可讓 Web 應用程式視需要從 VMware Identity Manager 服務擷取特定資訊。例如，如果對 Google Apps 啟用自動使用者佈建，便可從 VMware Identity Manager 服務擷取必要的使用者帳戶資訊，例如使用者名稱、名字和姓氏。

如果對 Web 應用程式啟用佈建，當您在 VMware Identity Manager 服務中將應用程式授權給使用者，該使用者就會佈建至 Web 應用程式。

VMware Identity Manager 服務目前包含適用於這些應用程式的佈建配接器。

- Google Apps

  請參閱範例：使用 Google Apps 佈建配接器。

- Office 365

- Socialcast

設定佈建配接器

佈建配接器適用於部分 Web 應用程式。佈建配接器可讓您在 Web 應用程式中佈建 VMware Identity Manager 使用者。

程序

1 在管理主控台中，按一下**目錄**索引標籤。

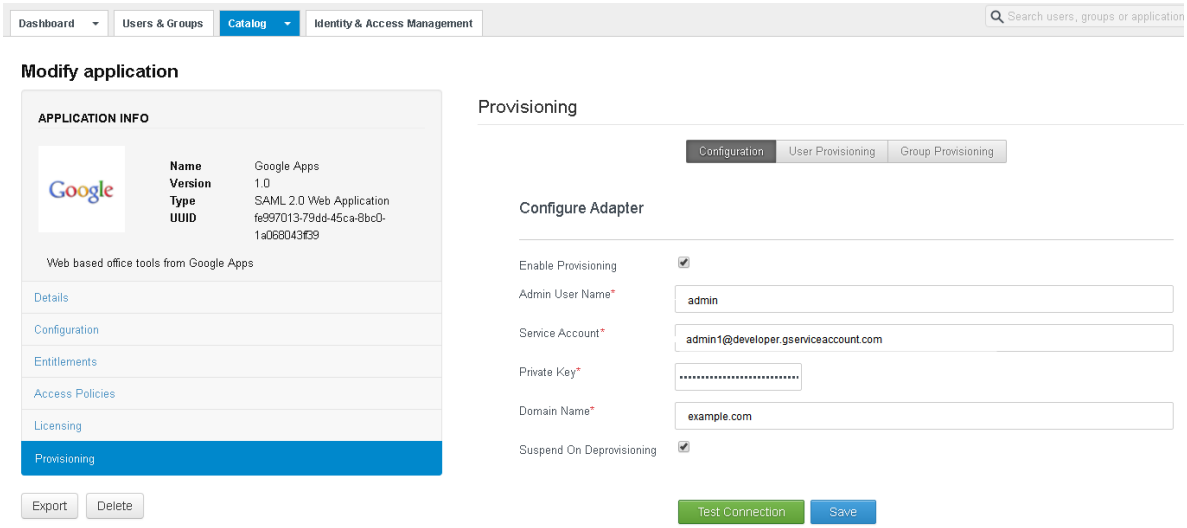
2 按一下 Web 應用程式，例如 Google Apps。

3 在 [修改] 應用程式頁面中，按一下**佈建**。

4 設定佈建。

選項	說明
組態索引標籤	設定佈建配接器。 a 按一下**啟用佈建**。 b 輸入 Web 應用程式帳戶資訊。 所需的資訊會隨著應用程式而有所不同。以 Google Apps 為例，您必須輸入 Google 服務帳戶資訊。
使用者佈建索引標籤	指定用來在 Web 應用程式中佈建使用者的屬性。具有值的屬性才可使用。您可以將屬性對應至 VMware Identity Manager 使用者屬性，或輸入其他值。某些屬性是必要的，表示這些屬性必須要有值。 ■ 若要指定或變更屬性的值，請按一下該屬性旁的編輯圖示、選取或輸入值，然後按一下**儲存**。 下拉式清單中所列的運算式，即為 [身分識別與存取管理] > [設定] > [使用者屬性] 頁面中所列的運算式。若要在下拉式清單中新增項目，請將其新增至 [使用者屬性] 頁面。您也可以直接輸入值。 對於某些屬性，您可以指定多個值。 ■ 若要刪除屬性對應，請按一下屬性旁的刪除圖示。
群組佈建索引標籤	對於支援群組佈建的佈建配接器，才會顯示**群組佈建**索引標籤。您必須選取要在 Web 應用程式中佈建的 VMware Identity Manager 群組，然後輸入必要資訊。群組會立即佈建。

例如：



在佈建配接器設定後，系統會啟用佈建。

當您將 VMware Identity Manager 中的 Web 應用程式授權給使用者時，該使用者也會建立於 Web 應用程式中。如果權利的部署類型是 [自動]，則會立即佈建使用者。如果部署類型是 [使用者啟動]，則會在使用者將 Web 應用程式新增至 Workspace ONE 入口網站中的 [啟動器] 頁面時，進行使用者的佈建。

當您將群組新增至 [群組佈建] 索引標籤時，將會立即佈建這些群組。

啟用或停用佈建配接器

您可以在設定 Web 應用程式佈建配接器之後加以啟用或停用。如果佈建配接器已啟用，當您將 VMware Identity Manager 服務中的 Web 應用程式授權給使用者時，該使用者也會建立於 Web 應用程式中。如果您不想將使用者佈建於 Web 應用程式中，您可以停用佈建配接器。

先決條件

您已設定佈建配接器。

程序

1 在管理主控台中按一下**目錄**索引標籤，然後選取 Web 應用程式。

2 在 [修改] 應用程式頁面中，按一下**佈建**。

3 在**組態**索引標籤中，選取**啟用佈建**核取方塊以啟用配接器，或取消選取該核取方塊以停用配接器。

檢視佈建狀態報告

如果為 Web 應用程式啟用了佈建，您將可檢視該應用程式的「佈建狀態」報告。此報告會列出在應用程式中佈建的使用者、每個使用者的佈建狀態、任何錯誤訊息，以及使用者最後一個事件的結果。

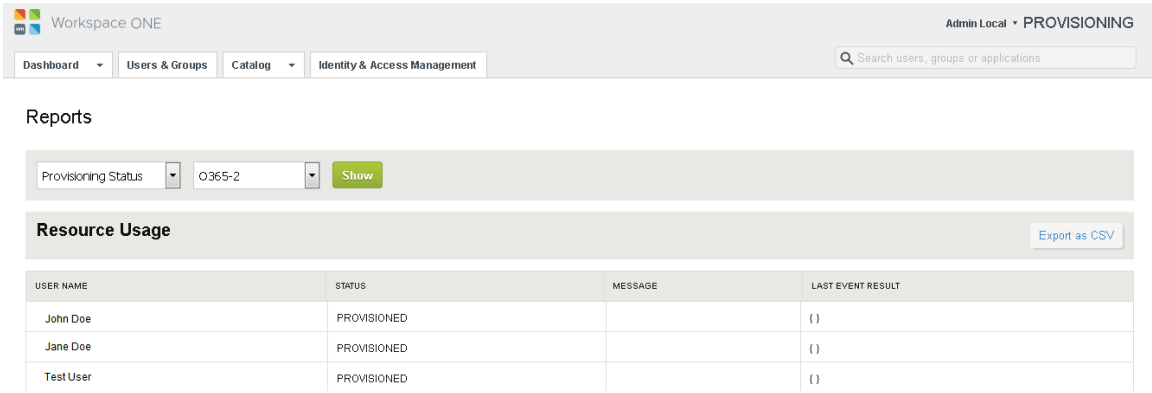
程序

1 在管理主控台內，按一下**儀表板**索引標籤上的箭頭，然後選取**報告**。

2 在 [報告] 頁面中，從下拉式功能表選取**佈建狀態**。

3 選取您要檢視其報告的應用程式，然後按一下**顯示**。

例如：



範例：使用 Google Apps 佈建配接器

您可以使用 Google Apps 佈建配接器，以自動從 VMware Identity Manager 服務在 Google 中佈建使用者。在啟用佈建功能後，每當您針對服務中的 Google Apps 權利授權某個使用者時，該名使用者將在 Google 中建立。您也可以使用配接器將群組佈建在 Google 中。

設定 Google 服務帳戶

您必須先建立 Google 服務帳戶，才可在 VMware Identity Manager 中啟用 Google Apps 佈建配接器。

程序

1 建立 Google 服務帳戶及其認證。

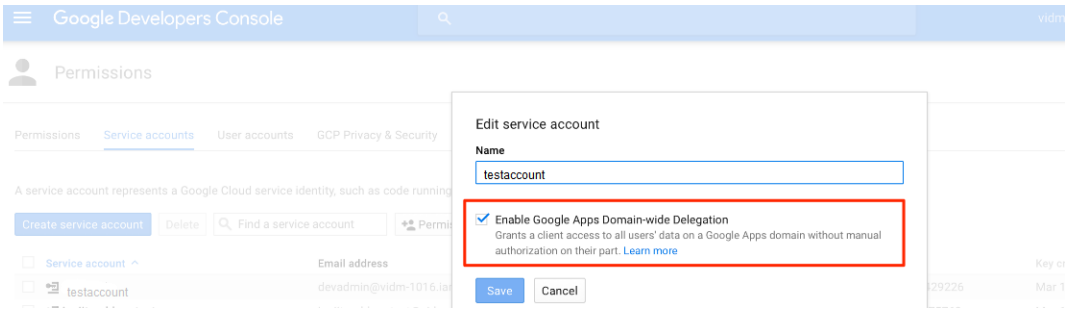
您將需要服務帳戶的用戶端識別碼、電子郵件地址和私密金鑰檔案才能啟用佈建。

2 建立 Google 服務帳戶後，請啟用 Google Apps 全網域委派。

a 在 API Manager 的**認證 > 建立認證**頁面中，按一下**管理服務帳戶**。

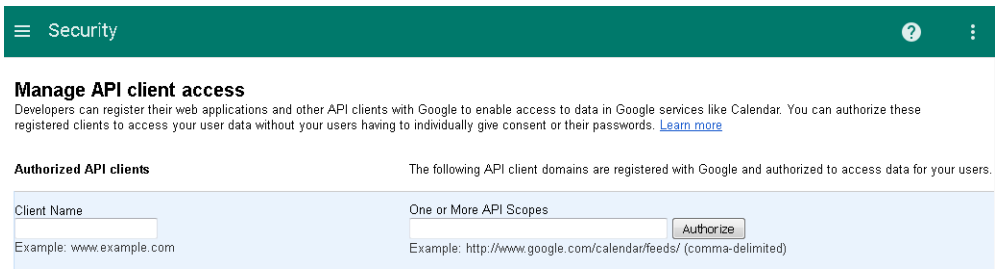
b 按一下您服務帳戶旁的 ⋮ 圖示，並選取**編輯**。

c 選取**啟用 Google Apps 全網域委派功能**核取方塊，然後按一下**儲存**。



3 從 Google 管理控制台中的**安全性 > 進階設定 > 驗證 > 管理 API 用戶端存取權**頁面，將 Google Apps 全網域授權委派給您的服務帳戶。如需詳細資訊，請參閱 Google 說明文件。

當您將全網域授權委派給服務帳戶時，請為**一或多個 API 範圍**欄位輸入下列值：
`https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.user.alias.readonly,https://www.googleapis.com/auth/admin.directory.user.alias,https://www.googleapis.com/auth/admin.directory.user,https://www.googleapis.com/auth/admin.directory.group.readonly,https://www.googleapis.com/auth/admin.directory.group.member.readonly,https://www.googleapis.com/auth/admin.directory.group.member,https://www.googleapis.com/auth/admin.directory.group`



現在，您可以在 VMware Identity Manager 服務中啟用佈建。

下一個

在 VMware Identity Manager 服務中設定 Google Apps 佈建配接器。

設定 Google Apps 佈建配接器

設定 Google Apps 佈建配接器，從 VMware Identity Manager 服務將使用者和群組佈建在 Google 中。

在啟用佈建功能後，每當您針對服務中的 Google Apps 權利授權某個使用者時，該名使用者也將在 Google 中建立。您也可以將群組佈建在 Google 中。

程序

1 登入 VMware Identity Manager 管理主控台。

2 按一下**目錄**索引標籤。

3 按一下 **Google Apps**。

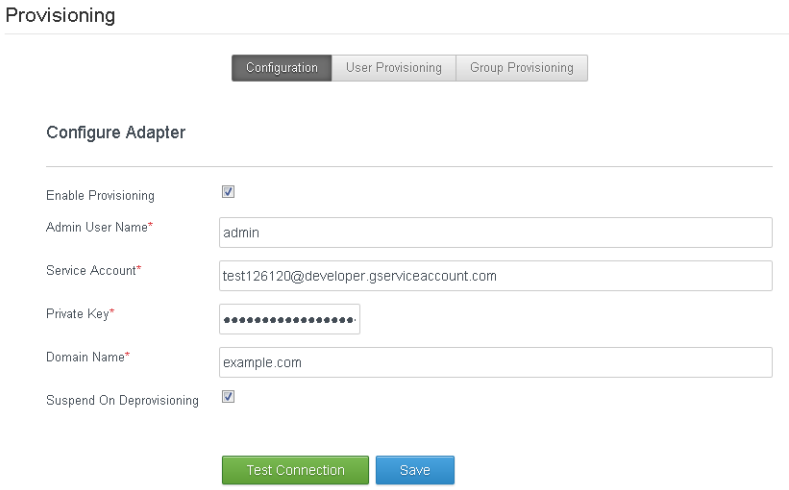
4 在 [修改] 應用程式頁面中，按一下**佈建**。

5 在**組態**索引標籤中，設定佈建配接器。

選項	說明
啟用佈建	選取此選項。
管理員使用者名稱	您的 Google Apps 管理員使用者名稱。請勿包含網域名稱。 例如：**admin**

選項	說明
服務帳戶	服務帳戶的用戶端電子郵件。 您可以從金鑰檔案中取得用戶端電子郵件。
私密金鑰	複製並貼上服務帳戶的私密金鑰。
網域名稱	您的公司的網域名稱。 例如：**example.com**
暫停取消佈建	如果您在移除使用者對 Google Apps 的權利時，要讓使用者在 Google 中處於暫停狀態，請選取此選項。

例如



6 按一下**測試連線**。

如果連線成功，頁面頂端將會顯示「已建立對 Google 服務的連線」訊息。

7 按一下**儲存**。

佈建隨即啟用。當您針對 Google Apps 授權使用者時，如果該使用者不存在於 Google 中，則會建立該使用者。

下一個

若要完成使用者佈建設定，請指定用來在 Google 中佈建使用者的屬性。

在 Google 中佈建使用者

若要在 Google 中佈建使用者，您必須設定 Google Apps 配接器、啟用佈建，然後指定用來在 Google 中佈建使用者的屬性。

其中 Google 屬性的清單可供使用。針對您要使用的屬性，指定其屬性對應。您可以將屬性對應至 VMware Identity Manager 使用者屬性，或輸入其他值。

以下是佈建至 Google 之使用者所需的屬性。這些屬性具有預設值。

- 使用者名稱
- 名字

- 姓氏

先決條件

您已設定 Google Apps 佈建配接器並啟用佈建。請參閱設定 Google Apps 佈建配接器。

程序

1 在 [Google Apps 佈建] 頁面中，按一下**使用者佈建**索引標籤。

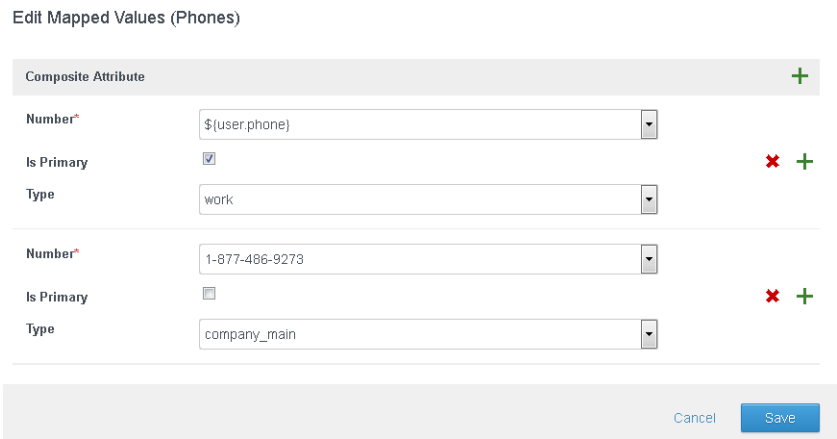
2 藉由設定屬性值，選取要用來在 Google 中佈建使用的屬性。

a 按一下屬性旁的編輯圖示。

b 選取或輸入一個值。

下拉式清單中的運算式，即為 [身分識別與存取管理] > [設定] > [使用者屬性] 頁面中所列的運算式。如果您想將任何運算式新增至清單中，請將其新增至 [使用者屬性] 頁面。您也可以直接輸入值。

對於某些屬性，您可以指定多個值。按一下位於右上方的 **+** 圖示以新增其他值。例如，您可以為**電話**屬性指定多個電話號碼。



c 按一下**儲存**。

3 若要刪除屬性對應，請按一下屬性旁的刪除圖示。

當使用者佈建在 Google 中時，系統不會使用沒有值的屬性。

使用者佈建現在已完成設定。當您針對 Google Apps 授權使用者時，如果該使用者不存在於 Google 中，則會建立該使用者。

備註 當您將 Google Apps 授權給使用者時，如果您將部署類型設為 [自動]，則會立即佈建使用者。如果您將部署類型設為 [使用者啟動]，則系統會在使用者將 Google Apps 新增至 Workspace ONE 入口網站中的 [啟動器] 頁面時進行使用者的佈建。

在 Google 中佈建群組

您可以使用 Google Apps 佈建配接器，透過 VMware Identity Manager 服務在 Google 中佈建群組。您可以選取您的任何 VMware Identity Manager 群組以進行佈建，無論群組是在本機建立，或是從您的企業目錄同步。群組會建立於 Google 中，且其中會新增群組成員的電子郵件地址。

Google 中的群組可作為郵寄清單。這些群組也可用來管理對文件、站台、行事曆等項目的存取。

在 Google 中佈建群組後，您可以像任何其他 Google 群組一樣管理這些群組。例如，您可以新增或刪除使用者。

先決條件

您已設定 Google Apps 佈建配接器並啟用佈建。請參閱設定 Google Apps 佈建配接器。

程序

1 在 VMware Identity Manager 管理主控台中，按一下**目錄**索引標籤。

2 按一下 **Google Apps**。

3 在 [修改] 應用程式頁面中，按一下**佈建**。

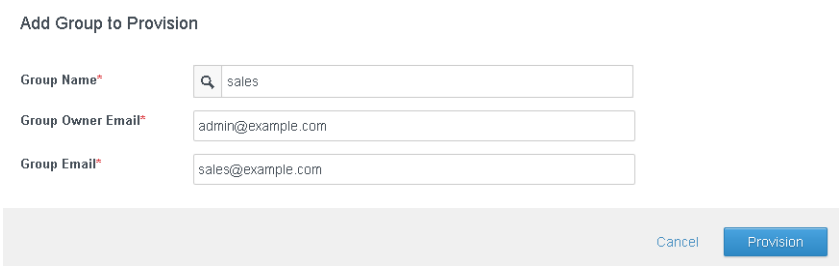
4 在 [佈建] 頁面中，按一下**群組佈建**索引標籤。

5 按一下**新增要佈建的群組**。

6 在顯示的 [新增要佈建的群組] 頁面中，輸入下列資訊。

選項	說明
群組名稱	輸入您要在 Google 中佈建之 VMware Identity Manager 群組的名稱。您可以開始輸入以搜尋群組。
群組擁有者電子郵件	輸入群組擁有者的電子郵件地址。
群組電子郵件	為 Google 中的群組輸入電子郵件地址。群組將會以此電子郵件地址在 Google 中建立。電子郵件地址必須是新的，或屬於現有的 Google 群組。它不可屬於使用者。 如果 Google 中已存在包含此電子郵件地址的群組，則您所選取的 VMware Identity Manager 群組成員將會新增至該群組。 **重要事項** 請確定電子郵件地址的網域符合您在**組態**索引標籤的**網域名稱**文字方塊中指定的網域。

例如：



7 按一下**佈建**。

群組在 Google 中佈建時會使用與 VMware Identity Manager 群組相同的名稱，以及您所指定的電子郵件地址。佈建狀態會顯示在**群組佈建**索引標籤中。

下一個

若要確認群組已在 Google 中佈建，請執行下列步驟。

1 登入 Google 管理控制台。

2 按一下**群組**圖示。

您可能需要按一下頁面底部的**更多控制項**，才能看見**群組**圖示。

3 選取新群組以檢視詳細資料。

取消佈建 Google 中的群組

您可以從 VMware Identity Manager 服務中取消佈建先前在 Google 中佈建的群組。取消佈建某群組，會使該群組從 Google 中刪除。

先決條件

確認已在 VMware Identity Manager 服務中設定 Google Apps 佈建配接器。請參閱設定 Google Apps 佈建配接器。

程序

1 在 VMware Identity Manager 管理主控台中，按一下**目錄**索引標籤。

2 按一下 **Google Apps**。

3 在 [修改] 應用程式頁面中，按一下**佈建**，然後按一下**群組佈建**索引標籤。

4 在表格中，選取您要取消佈建之群組旁的核取方塊，然後按一下**取消佈建**。

群組會從 Google 中刪除。它也會從 [群組佈建] 頁面中移除。

啟用或停用 Google Apps 佈建配接器

在啟用 Google Apps 佈建配接器後，每當您將 Google Apps 授權給使用者時，該名使用者也將在 Google 中建立。如果您不想將使用者佈建至 Google，您可以停用佈建配接器。

程序

1 在管理主控台中，按一下**目錄**索引標籤。

2 按一下 **Google Apps**。

3 在 [修改] 應用程式頁面中，按一下**佈建**。

4 在 [佈建] 頁面中，按一下**組態**索引標籤 (如果未選取)。

5 選取**啟用佈建**核取方塊以啟用配接器，或取消選取該核取方塊以停用配接器。

6 按一下**儲存**。

其他資訊

其他資訊提供有關設定 SAML 式單一登入至特定 Web 應用程式 (例如 Office 365 和 Google Apps) 的相關資訊。內含佈建配接器的相關資訊 (如果適用)。

請參閱 VMware Identity Manager 整合說明文件網站。

提供存取 View、Horizon 6 或 Horizon 7 桌面平台與應用程式集區

3

透過整合您的組織的 View、Horizon 6 或 Horizon 7 環境與您的 VMware Identity Manager 部署，您讓 VMware Identity Manager 使用者能夠使用 Workspace ONE 入口網站來存取其獲授權的 View 桌面平台與應用程式集區。您可以整合獨立的 View 網繭 (包含 View 連線伺服器執行個體)，以及網繭聯盟 (包含多個網繭且可跨越多個站台和資料中心)。

您會在 View 管理員介面中部署和管理桌面平台與應用程式集區。您也會在 View 中建立 Active Directory 使用者和群組的權利。將 View 網繭或網繭聯盟與您的 VMware Identity Manager 服務整合時，您會將這些資源和權利的相關資訊同步至 VMware Identity Manager。在 VMware Identity Manager 管理主控台中，您可以查看使用者和群組與其獲授權之 View 集區之間的關聯。

如需設定 View 的相關資訊，請參閱 View、Horizon 6 或 Horizon 7 文件。

支援的版本

VMware Identity Manager 支援下列版本和功能。

- View 5.3 和更新版本支援整合獨立 View 網繭。
- Horizon 6.2 和更新版本支援使用「Cloud Pod 架構」功能建立的整合網繭聯盟。
- Horizon 6.1.1 和更新版本支援 HTML Access。
- Horizon 7.x 支援憑證 SSO。

另請參閱《VMware 產品互通性對照表》以取得最新的支援資訊。

本章節討論下列主題:

- 允許使用者在 VMware Identity Manager 中重設其 View 桌面平台
- 設定特定應用程式和桌面平台的存取原則
- 在非持續性 View 桌面平台中減少資源使用並增加 VMware Identity Manager 桌面平台的效能

整合獨立的 View 網繭

若要整合獨立的 View 網繭，您必須在 VMware Identity Manager 管理主控台中新增 View 連線伺服器詳細資料，並且與 View 連線伺服器同步。

在 VMware Identity Manager 管理主控台中執行任何整合工作之前，請先設定 View。您會在 View 中建立及設定 View 集區，而不是在 VMware Identity Manager 中。您也可以在 View 中設定 Active Directory 使用者和群組的權利。

View 的整合涉及下列高層級的工作。

- 部署及設定 View。
- 使用為 Active Directory 使用者和群組設定的權利，部署 View 桌面平台和應用程式集區。
- 在 VMware Identity Manager 管理主控台的**使用者屬性**頁面上，啟用 userPrincipalName 屬性。
- 使用目錄同步功能，將有權使用 View 連線伺服器執行個體之 View 集區的 Active Directory 使用者和群組，同步至 VMware Identity Manager 服務。

  稍後，當您將 View 網繭新增至 VMware Identity Manager 時，也可以選取 [執行目錄同步] 選項。此選項會指定在 VMware Identity Manager 目錄中遺失任何有權使用 View 連線伺服器執行個體中 View 集區的使用者和群組時，讓目錄同步作為 View 同步的一部分來執行。
- 如果您想要同步任何 View 連線伺服器 5.x 執行個體，或使用 [執行目錄同步] 選項，請將 VMware Identity Manager 加入與 View 相同的 Active Directory 網域中。這兩個組態都會使用替代的同步方法，而這需要加入網域。
- 將 View 網繭新增至 VMware Identity Manager。
- 在 View 連線伺服器上設定 SAML 驗證器。在驗證器組態頁面上，一律須使用 VMware Identity Manager FQDN。

設定 View

若要在 VMware Identity Manager 中使用 View，您必須先安裝和設定 View。

VMware Identity Manager 支援 View 5.3 和更新版本。另請參閱《VMware 產品互通性對照表》以取得最新的支援資訊。

備註 Horizon 6.1.1 和更新版本支援 HTML Access。

設定 View 時，請確保您符合下列需求。

- 在預設連接埠 443 或自訂連接埠上部署 View 連線伺服器。

- 針對您的 View 設定中的每個 View 連線伺服器，請確認您擁有可以在反向查詢期間解析的 DNS 項目和 IP 位址。VMware Identity Manager 要求對 View 連線伺服器、View 安全伺服器和負載平衡器進行反向查詢。如果未正確設定反向對應，VMware Identity Manager 與 View 的整合會失敗。
- 以對 Active Directory 使用者和群組設定的權利來部署和設定 View 集區和桌面平台。確保使用者具有正確的權利。
- 設定桌面平台集區時，請確保 [遠端設定] 中，您將**中斷連線之後自動登出**選項設定為 1 或 2 分鐘，而不是**立即**。
- 確保您在 View 的根資料夾中建立 View 集區。如果您在根資料夾以外的資料夾建立 View 集區，VMware Identity Manager 會無法查詢這些 View 集區和權利。
- 建議您在 View 連線伺服器上，將 SAML 中繼資料到期期限延長為 90 天。如需相關資訊，請參閱在 View 連線伺服器上變更服務提供者中繼資料的到期期限。

加入 Active Directory 網域

在與 View 整合之前，如果您預計要同步任何 View 連線伺服器 5.x 執行個體或使用 [執行目錄同步] 選項，則必須先將 VMware Identity Manager 加入用於 View 的 Active Directory 網域中。這兩個組態都會使用替代的同步方法，而這需要加入網域。

先決條件

- 確認您具有 Active Directory 網域名稱、使用者名稱和密碼，以及可加入網域的權限。

  如需加入網域的詳細資訊，請參閱*《安裝及設定 VMware Identity Manager》*中的〈整合 Active Directory〉。
- 確認 VMware Identity Manager [使用者屬性] 頁面中的 **userPrincipalName** 屬性已啟用。在管理主控台中按一下**身分識別與存取管理 > 設定 > 使用者屬性**，即可存取此頁面。
- 確認已使用目錄同步，將具備 View 集區權利的使用者和群組同步至 VMware Identity Manager。
- 如果適用，建立連往 Active Directory 中多網域或受信任多樹系網域的連線。請參閱*《VMware Identity Manager 安裝與設定》*。

程序

1. 登入 管理主控台。
2. 按一下**身分識別與存取管理**。
3. 按一下**設定**。
4. 在 [連接器] 頁面中，按一下適當目錄旁的**加入網域**。

5 輸入 Active Directory 網域的資訊，然後按一下**加入網域**。輸入您的網域資訊時，請勿使用非 ASCII 字元。

選項	說明
網域	選取要加入的網域，或選取**自訂網域**並輸入網域名稱。請確定您輸入的是完整的 Active Directory 網域名稱，例如 **`server.example.com`**。 **備註** Active Directory FQDN 必須位在與 View 連線伺服器相同的網域中。否則，您的部署會失敗。
網域使用者	輸入 Active Directory 中有權將系統加入至該 Active Directory 網域之帳戶的使用者名稱。
網域密碼	輸入與 **AD 使用者名稱**相關聯的密碼。VMware Identity Manager 不會儲存此密碼。
要加入之網域的組織單位 (OU)	(選擇性) 要加入的組織單位 (OU)。此選項會將機器加入至指定的 OU，而非預設的電腦 OU。 例如，**ou=testou,dc=test,dc=example,dc=com**。

6 若要在多網域環境中設定 View 整合，請確認 VMware Identity Manager 和 View Server 加入相同的網域。

下一個

新增 View 網繭至 VMware Identity Manager。

將 Horizon View 網繭新增至 VMware Identity Manager 和同步資源

您可以新增多個 View 網繭至 VMware Identity Manager。在您新增網繭後，請為不同的網繭設定用戶端存取 URL。

您會在 VMware Identity Manager 管理主控台的 [View 集區] 頁面新增 View 網繭。您可以隨時回到此頁面來修改 View 組態，或是新增或移除 View 網繭。

先決條件

對於每個 View 網繭，您需要具有管理員角色之使用者的認證。

程序

1 登入 VMware Identity Manager 管理主控台。

2 按一下**目錄**索引標籤。

3 按一下**管理資源類型**，然後選取 **View 應用程式**。

4 選取**啟動 View 集區**核取方塊。

5 針對您要新增的每個 View 網繭，按一下**新增 View 網繭**。

6 提供每個 View 網繭的特定組態資訊。

連線伺服器	輸入 Horizon 連線伺服器執行個體的完整主機名稱，例如 connectionserver.example.com。網域名稱必須完全符合 Horizon 連線伺服器執行個體所加入的網域名稱。
使用者名稱	輸入用於此 View 網繭的管理員使用者名稱。使用者必須具有 View 中的管理員角色。
密碼	輸入用於此 View 網繭的管理員密碼。
使用第三方身分識別提供者的智慧卡驗證	如果使用者使用智慧卡驗證 (而非密碼) 來登入此 View 網繭，請選取核取方塊。
已在 Horizon View 上啟用 True SSO	此選項僅適用於支援 True SSO 功能的 Horizon 版本。 在 View 中設定 True SSO 時，使用者不需要密碼即可登入其 Windows 桌面平台。不過，如果使用者使用非密碼驗證方法 (例如 SecurID) 登入 VMware Identity Manager，則當使用者啟動其 Windows 桌面平台時，系統會提示他們輸入密碼。您可以選取此選項以防止在該案例中向使用者顯示密碼對話方塊。
同步本機權利	如果已為網繭設定本機權利，請選取此選項。

7 在**部署類型**下拉式清單中，選取讓使用者入口網站中的使用者能夠使用 View 資源的方式。

- **使用者啟動**：View 資源會新增至 Workspace ONE 中的 [目錄] 頁面。若要使用資源，使用者必須將資源從 [目錄] 頁面移至 [啟動器] 頁面。
- **自動**：View 資源會直接新增至 Workspace ONE 中的 [啟動器] 頁面，立即供使用者使用。

您在此處選取的部署類型，即為對您的 View 整合中所有資源的所有使用者權利進行套用的全域設定。您可以在資源的 [權利] 頁面上，針對各個資源修改個別使用者或群組的部署類型。

建議您將全域部署類型設為**使用者啟動**。接著，您可以針對各個資源修改特定使用者或群組的設定。

如需關於設定部署類型的詳細資訊，請參閱設定 View 權利的部署類型。

8 選取**不要同步重複的應用程式**核取方塊，可防止從多個伺服器同步重複的應用程式。

在多個資料中心部署 VMware Identity Manager 時，系統會在多個資料中心中設定相同的資源。選取此選項，可防止您的 VMware Identity Manager 目錄中出現重複的桌面平台或應用程式集區。

9 選取**設定 5.x 連線伺服器**核取方塊 (如果您在此頁面上設定的任何 View 連線伺服器執行個體是 5.*x* 版)。

選取此選項，可讓您以替代方式同步 View 5.*x* 所需的資源。

備註 如果您選取**執行目錄同步**選項，**設定 5.x 連線伺服器**選項也將自動選取，因為這兩個選項都依存於同步資源的替代方式。

10 如果您想要在 VMware Identity Manager 目錄中遺漏了任何有權使用 View 連線伺服器執行個體之 View 集區的使用者和群組時，讓目錄同步作為 View 同步的一部分來執行，請選取**執行目錄同步**核取方塊。

[執行目錄同步] 選項不會套用至「Cloud Pod 架構」網繭聯盟。如果 VMware Identity Manager 目錄中遺失具有全域權利的使用者和群組，則不會觸發目錄同步。

透過此程序進行同步的使用者和群組，可如同由 VMware Identity Manager 目錄同步新增的任何其他使用者一般進行管理。

重要事項 使用 [執行目錄同步] 選項時，View 同步會比較耗時。

備註 選取此選項時，**設定 5.x 連線伺服器**選項也將自動選取，因為這兩個選項都依存於同步資源的替代方式。

11 從**選擇 View 集區同步頻率**下拉式清單中，選取您要從 View 連線伺服器執行同步的頻率。

您可以設定一般的同步排程，或選擇手動同步。如果您選擇**手動**，則每當 View 資源或權利中發生變更時，您必須回到此頁面並按一下**立即同步**。

12 從**選取預設啟動用戶端**下拉式清單中，選取用以啟動 View 應用程式或桌面平台的預設用戶端。

選項	說明
無	系統不會在管理員層級設定預設喜好設定。如果此選項設為**無**，且使用者喜好設定也未設定，則系統會使用 View 的**預設顯示通訊協定**設定來決定如何啟動桌面平台或應用程式。
瀏覽器	View 桌面平台和應用程式依預設會在 Web 瀏覽器中啟動。使用者喜好設定 (若已設定) 會覆寫此設定。
用戶端	View 桌面平台和應用程式依預設會在 Horizon Client 中啟動。使用者喜好設定 (若已設定) 會覆寫此設定。

此設定會套用至 View 整合中的所有使用者和所有資源。

預設啟動用戶端設定會依照下列順序套用喜好設定 (由最高排到最低)：

a 使用者喜好設定，設定於 Workspace ONE 入口網站中。此選項無法在 Workspace ONE 應用程式中使用。

b Administrator 的**選取預設啟動用戶端**設定，設定於 VMware Identity Manager 管理主控台的 [View 集區] 頁面中。

c 適用於桌面平台或應用程式集區的 Horizon View **遠端顯示通訊協定 > 預設顯示通訊協定**設定，設定於 Horizon Administrator 中。例如，當顯示通訊協定設為 PCoIP 時，應用程式或桌面平台會在 Horizon Client 中啟動。

13 按一下**儲存**。

14 按一下**立即同步**。

每當您在 View 中變更設定 (例如新增權利或新增使用者) 時，皆需同步才能將變更填入 VMware Identity Manager。

15 設定 View 網繭的用戶端存取 URL。

a 按一下**身分識別與存取管理**索引標籤，然後按一下**設定**。

b 按一下**網路範圍**。

c 選取網路範圍。

d 在 [編輯網路範圍] 頁面中，於 **View 網繭**區段，輸入該網路範圍的 View 網繭用戶端存取 URL 主機名稱和連接埠號碼。

e 在 **IP 範圍**區段，指定要套用設定的 IP 範圍。

f 按一下**儲存**。

另請參閱為自訂網路範圍啟用多個用戶端存取 URL。

設定 SAML 驗證

若要從 VMware Identity Manager 服務啟動 View、Horizon 6、Horizon 7 應用程式或桌面平台並擁有從 VMware Identity Manager 通往應用程式或桌面平台的單一登入，您必須在 View 部署的所有 View 連線伺服器執行個體中設定 SAML 驗證。

如果您的組織使用透過第三方身分識別提供者的智慧卡驗證來檢視 View 資源，請勿執行該項工作。

程序

1 以具備管理員角色的使用者身分登入 View Administrator Web 介面。

2 針對 View 部署中的每個 View 連線伺服器執行個體設定 SAML 驗證。在驗證器組態頁面上，您必須使用 VMware Identity Manager 服務的完整網域名稱。

重要事項 View 和 VMware Identity Manager 必須處於時間同步狀態。如果 View 和 VMware Identity Manager 未處於時間同步狀態，當您嘗試啟動 View 應用程式或桌面平台時，會出現無效的 SAML 訊息。

下一個

您必須建立 VMware Identity Manager 和 View 連線伺服器之間的 SSL 信任，並且加以維護。

建立或更新 VMware Identity Manager 與 View 連線伺服器之間的 SSL 信任

首先，您必須在 View 連線伺服器上接受 SSL 憑證，以建立 VMware Identity Manager 與 View 連線伺服器之間的信任。如果您在整合之後變更 View 連線伺服器上的 SSL 憑證，則必須返回 VMware Identity Manager 並重新建立該信任。

先決條件

- 確認 View 具有已安裝的 SSL 憑證。依預設，View 會有自我簽署憑證。
- 在 View 中，將 View 連線伺服器的憑證變更為根簽署憑證。如需設定 View 連線伺服器執行個體或安全伺服器以使用新憑證的相關資訊，請參閱 VMware View 文件。
- 在 View 連線伺服器上設定 SAML 驗證。在驗證器組態頁面上，一律須使用 VMware Identity Manager FQDN。

備註 如果您使用第三方身分識別提供者從 VMware Identity Manager 存取 View 桌面平台，則 View 連線伺服器上的 SAML 驗證必須設定為 `allowed`。

程序

1 在 VMware Identity Manager 管理主控台中，按一下**目錄**索引標籤。

2 按一下**管理資源類型**，然後選取 **View 應用程式**。

3 按一下 [複寫的伺服器群組] 旁的**更新 SSL 憑證**連結。

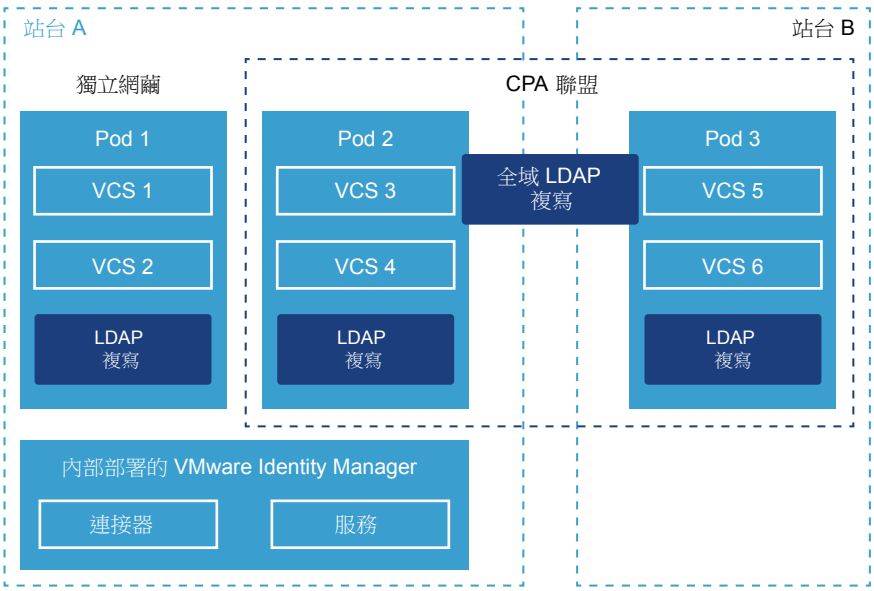
4 在 [憑證資訊] 頁面上，按一下**接受**。

如果 VMware Identity Manager 憑證在初始設定後有所變更，則您必須從 View 重新接受 SAML 驗證器。如果 View 憑證有所變更，則必須在 VMware Identity Manager 中接受 SSL 憑證。

整合 View Cloud Pod 架構 (CPA) 部署

除了將獨立 View 網繭與 VMware Identity Manager 整合，您也可以整合 View Cloud Pod 架構 (CPA) 部署。

圖 3-1 將 View 網繭聯盟與 VMware Identity Manager 整合



View Cloud Pod 架構功能可將多個 View 網繭連結起來，形成單一大型桌面平台和應用程式代理與管理環境，稱為網繭聯盟。網繭聯盟可跨越多個站台和資料中心。

您可將一或多個網繭聯盟與 VMware Identity Manager 服務整合。請注意，網繭聯盟是在 View 中建立和管理，對於網繭聯盟之桌面平台和應用程式集區的使用者和群組權利也是在 View 中設定。您需將資源和權利同步至 VMware Identity Manager。

網繭聯盟具備全域權利，可供您授權使用者從網繭聯盟中的任何網繭存取桌面平台和應用程式。全域權利可以包含來自聯盟中多個網繭的資源。例如，全域桌面平台權利可以包含來自三個不同資料中心中三個不同網繭的桌面平台集區。網繭聯盟中的個別網繭也能設定本機權利。您可以同時將全域和本機權利同步至 VMware Identity Manager。

將 View 網繭聯盟與 VMware Identity Manager 服務整合，牽涉到 VMware Identity Manager 管理主控台中的下列高階工作：

- 新增組成網繭聯盟的所有網繭，指定每個網繭的 View 連線伺服器。

  雖然 VMware Identity Manager 可以同步網繭聯盟中任何網繭的全域權利，但仍需連線至每個網繭以便同步 SAML 驗證所需的中繼資料。它也需要連線至網繭以便同步本機權利 (如果適用)。

- 新增網繭聯盟詳細資料，並指定全域啟動 URL。全域啟動 URL 通常是全域負載平衡器 URL，用來啟動全域授權的桌面平台和應用程式。

  您可為特定的網路範圍自訂全域啟動 URL，例如為內部和外部存取進行自訂。

- 將網繭聯盟的資源和權利同步至 VMware Identity Manager 服務。

  備註 系統僅會同步在網繭聯盟中具備「所有站台」範圍原則的全域權利。「所有站台」範圍原則會將搜尋應用程式或桌面平台的範圍設定為網繭聯盟中的所有網繭。

- 透過設定特定網路範圍的用戶端存取 URL，自訂全域啟動 URL。這些 URL 將用來啟動網繭聯盟中的全域授權資源。依預設，您在新增聯盟時指定的全域啟動 URL 將做為所有網路範圍的全域啟動 URL。
- 為網繭聯盟中已設定本機權利的每個網繭，指定用戶端存取 URL。這些 URL 將用來啟動網繭中的本機授權的桌面平台和應用程式。用戶端存取 URL 可以是 View 連線伺服器 URL、安全伺服器 URL 或負載平衡器 URL。用戶端存取 URL 是針對特定的網路範圍而設定。依預設，您在新增網繭時指定的 View 連線伺服器，將做為所有網路範圍的用戶端存取 URL。

將網繭聯盟與 VMware Identity Manager 服務整合時，服務會進行下列步驟：

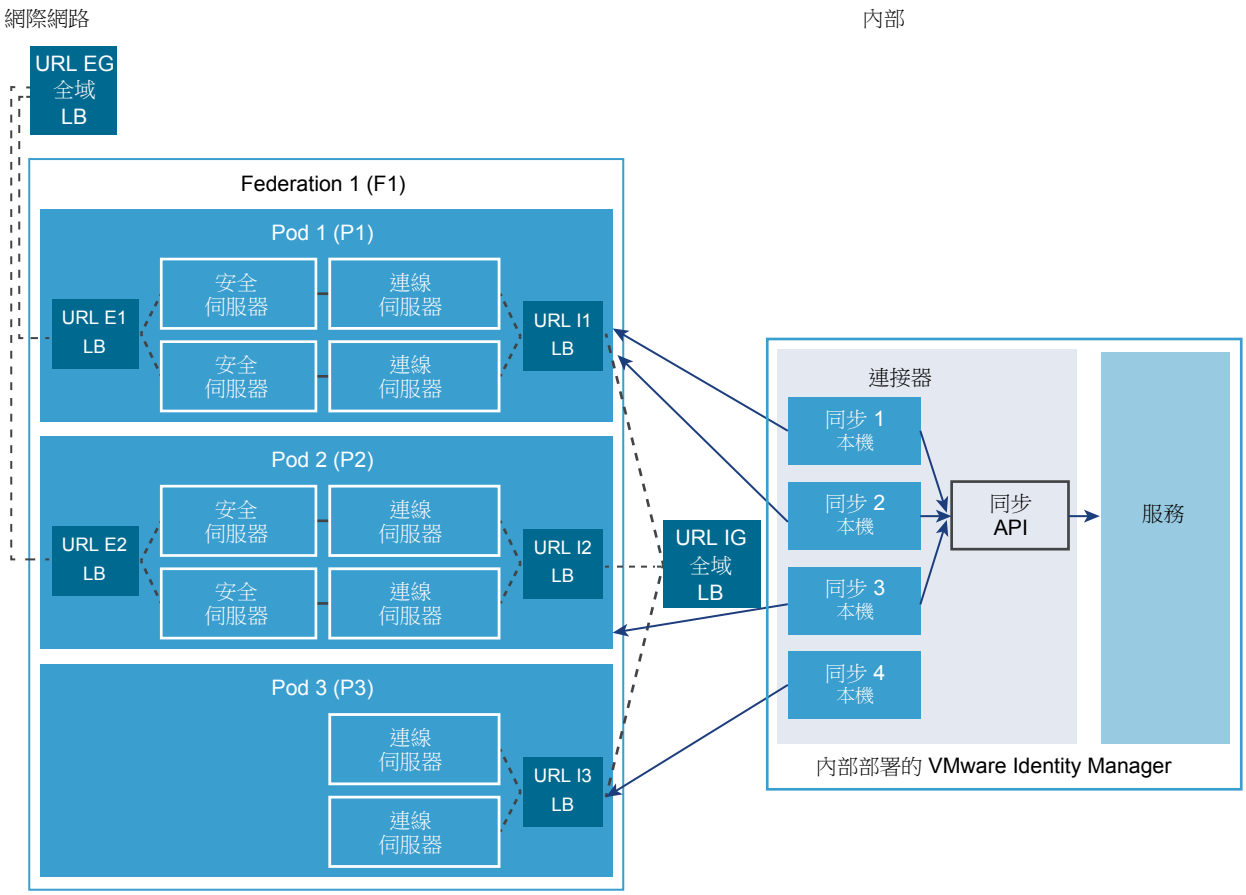
- 同步網繭聯盟中具備「所有站台」範圍原則的所有全域權利。
- 同步隸屬於網繭聯盟之網繭中的本機權利 (如果已選取)。
- 同步網繭聯盟中所有 View 連線伺服器的中繼資料。
- 允許使用者從 Workspace ONE 入口網站存取其 View 應用程式和桌面平台。

使用者存取可以從 Workspace ONE 入口網站存取其 View 應用程式和桌面平台。使用者獲授權的所有資源 (無論是透過全域權利或本機權利獲得) 都會顯示出來。應用程式和桌面平台是在 Horizon Client 中啟動。當使用者啟動本機授權的應用程式或桌面平台，則會從 View 連線伺服器啟動至使用者連線的 Horizon Client。全域授權的資源則是從資源所位在的 View 連線伺服器啟動。

Cloud Pod 架構部署範例

下圖顯示 Cloud Pod 架構部署範例以及其如何與 VMware Identity Manager 服務整合。

圖 3-2 Cloud Pod 架構部署範例



本圖說明網繭聯盟部署範例。在 Horizon 6 中建立一個名為 Federation 1 的網繭聯盟。它有三個網繭：Pod 1、Pod 2 和 Pod 3。Pod 1 和 Pod 2 針對每個 View 連線伺服器設定為使用安全伺服器執行個體，一個外部負載平衡器用於外部存取，以及一個內部負載平衡器用於內部存取。Pod 3 設定為使用一個內部負載平衡器，僅用於內部存取。整體而言，網繭聯盟具有一個外部全域負載平衡器以及一個內部全域負載平衡器。

桌面平台和應用程式集區會部署在網繭上。為 Federation 1 設定全域權利，並為個別網繭設定本機權利。

Federation 1 與 VMware Identity Manager 服務整合。VMware Identity Manager 服務會從 Federation 1 同步全域權利以及本機權利。由於全域權利會在每個網繭中進行複寫，因此會從 Pod 1 同步全域權利。另外也會從 Pod 1、Pod 2 和 Pod 3 同步本機權利。

使用者可以在 VMware Identity Manager Workspace ONE 入口網站中檢視他們獲授權的所有桌面平台和應用程式 (無論是透過全域權利或本機權利獲得的)。當使用者啟動桌面平台或應用程式時，如果該資源屬於全域權利的一部分，則啟動要求會根據使用者的網路範圍，前往外部或內部全域負載平衡器 (URL EG 或 URL IG)。如果資源來自本機權利，啟動要求會根據使用者的網路範圍，前往該資源部署所在之網繭的內部或外部負載平衡器。例如，若是 Pod 2 上的資源，要求會前往 URL I2 或 URL E2。

整合 View 網繭聯盟的需求

將 View 網繭聯盟與 VMware Identity Manager 整合具有下列需求。

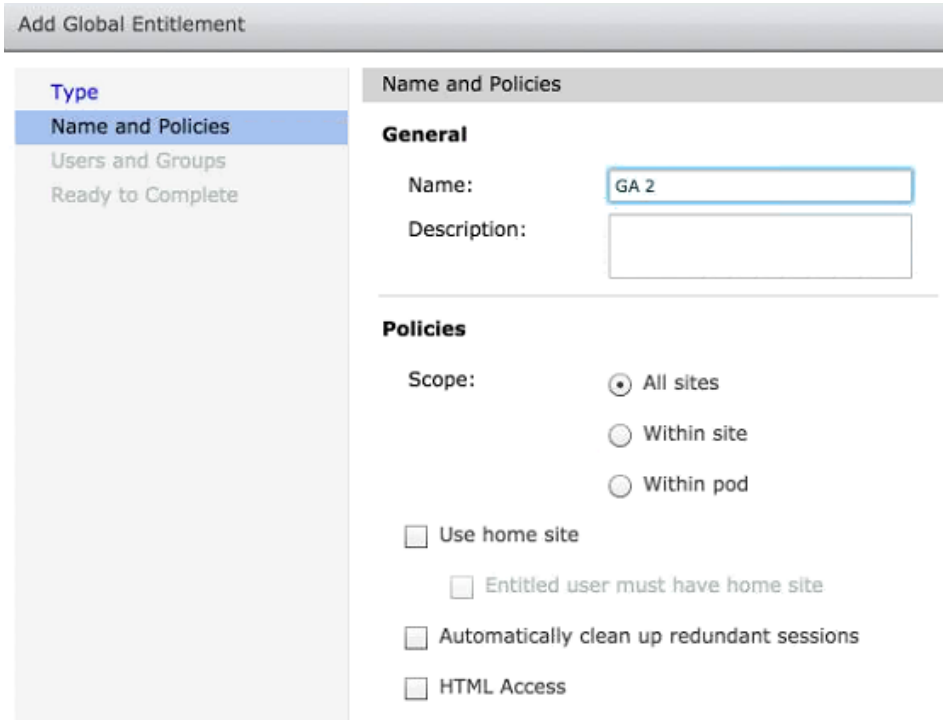
- VMware Identity Manager 在 Horizon 6.2 及更新版本中針對應用程式和桌面平台支援 Cloud Pod 架構功能。
- 您最多可將 10 個網繭聯盟與 VMware Identity Manager 服務整合。每個聯盟最多可包含 7 個網繭。
- 將 View 連線伺服器執行個體部署在預設連接埠 443 或自訂連接埠上。
- 確認 View 環境中的每個 View 連線伺服器執行個體都具有可在反向對應期間解析的 DNS 項目和 IP 位址。VMware Identity Manager 需要 View 連線伺服器、View 安全伺服器和負載平衡器執行個體的反向對應。如果未正確設定反向對應，VMware Identity Manager 與 View 的整合會失敗。
- 服務元件 VMware Identity Manager 連接器必須能夠連接網繭聯盟中的所有 View 連線伺服器執行個體。
- 網繭聯盟中的所有 View 連線伺服器執行個體都必須設定 SAML 驗證，並將 VMware Identity Manager 服務指定為身分識別提供者。您必須在 URL 中使用服務的完整網域名稱。

  如需詳細資訊，請參閱設定 SAML 驗證。

  建議您在 View 連線伺服器執行個體上，將 SAML 中繼資料到期期限延長為 90 天。如需相關資訊，請參閱在 View 連線伺服器上變更服務提供者中繼資料的到期期限。
- View 連線伺服器憑證將與 VMware Identity Manager 同步。
- 將應用程式和桌面平台集區部署在 View 網繭中。
  - 設定桌面平台集區時，請確保 [遠端設定] 中，您將**中斷連線之後自動登出**選項設定為 1 或 2 分鐘，而不是**立即**。
  - 確保您在 View 的根資料夾中建立 View 集區。如果將 View 集區建立在根資料夾以外的資料夾，VMware Identity Manager 將無法查詢這些 View 網繭和權利。

  如果在與 VMware Identity Manager 整合後新增或移除應用程式或桌面平台集區，您必須再次同步，這些變更才會出現在 VMware Identity Manager 服務中。
- 在與 VMware Identity Manager 服務整合前，您必須先從其中一個網繭初始化 Cloud Pod 架構功能，並將其他所有網繭都加入聯盟，藉以在 View 環境中建立網繭聯盟。當網繭加入聯盟時，全域權利就會複寫至網繭上。

  與 VMware Identity Manager 服務整合後，如果您在網繭聯盟中加入或移除網繭，則必須在 VMware Identity Manager 管理主控台中編輯網繭聯盟詳細資料以新增或移除網繭、儲存變更，然後再次同步。
- 在 View 環境中，於網繭聯盟中建立全域權利以將桌面平台和應用程式授權給 Active Directory 使用者或群組。
- 您想與 VMware Identity Manager 同步的全域權利必須設定**所有站台**範圍原則。具備其他範圍原則的權利都不會加以同步。



- 若要讓使用者在 Web 瀏覽器中啟動桌面平台或應用程式，請在 View 中為全域權利選取 HTML Access 選項。
- (選用) 視需要在網繭上建立本機權利。

如需關於設定 View 的詳細資訊，請參閱 Horizon 6 或 Horizon 7 說明文件。

設定您的 VMware Identity Manager 環境

設定您的 View 環境之後，您必須設定 VMware Identity Manager 環境，之後才能將網繭聯盟與服務整合。

先決條件

- 您的使用者名稱和密碼具備權限，可加入搭配 View 使用的 Active Directory 網域。如需加入網域所需之權限的相關資訊，請參閱《*安裝及設定 VMware Identity Manager*》中的〈與 Active Directory 整合〉。

程序

1 確認 VMware Identity Manager [使用者屬性] 頁面中的屬性 **userPrincipalName** 標示為必要。

   a 在管理主控台，按一下**身分識別與存取管理**索引標籤。

   b 按一下**設定**，然後選取 **使用者屬性**索引標籤。

   c 如果 **userPrincipalName** 屬性的**必要**核取方塊未選取，請加以選取。

   重要事項 必須在建立 VMware Identity Manager 目錄之前執行此動作。建立目錄之後，即無法將使用者屬性變更為必要。

2 透過目錄同步，將具有您的 View 環境中全域或本機權利的使用者和群組從 Active Directory 同步到 VMware Identity Manager 服務。

   a 若要檢視目前的使用者和群組，請按一下**使用者和群組**索引標籤。

   b 選取**身分識別與存取管理 > 目錄**索引標籤。

   c 選取適當的目錄。

   d 視需要修改目錄設定，然後按一下**立即同步**。

3 如果適用，建立連往 Active Directory 中多網域或受信任多樹系網域的連線。如需相關資訊，請參閱*安裝及設定 VMware Identity Manager*。

4 如果您要同步任何 View 連線伺服器 5.*x* 執行個體或是打算使用 [執行目錄同步] 選項，請將 VMware Identity Manager 目錄加入與 View 相同的 Active Directory 網域。這兩個組態都會使用替代的同步方法，而這需要加入網域。

   a 按一下**身分識別與存取管理**索引標籤。

   b 按一下**設定**，然後選取 **連接器**索引標籤。

   c 按一下適當目錄旁的**加入網域**。

   d 輸入 Active Directory 網域的資訊，然後按一下**加入網域**。輸入您的網域資訊時，請勿使用非 ASCII 字元。

選項	說明
網域	選取要加入的網域，或選取**自訂網域**並輸入網域名稱。請確定您輸入的是完整的 Active Directory 網域名稱，例如 **`server.example.com`**。 **備註** Active Directory FQDN 必須與 View 連線伺服器執行個體位於相同的網域中。否則，您的部署會失敗。
網域使用者	輸入有權將系統加入至該 Active Directory 網域之 Active Directory 使用者的使用者名稱。
網域密碼	輸入使用者的密碼。VMware Identity Manager 不會儲存此密碼。
要加入之網域的組織單位 (OU)	(選擇性) 要加入的組織單位 (OU)。此選項會將機器加入至指定的 OU，而非預設的電腦 OU。 例如，**ou=testou,dc=test,dc=example,dc=com**。

   e 確認 VMware Identity Manager 和 View 伺服器加入至相同網域。

新增雲端網繭聯盟和同步資源

若要新增網繭聯盟，您會先新增屬於網繭聯盟的所有網繭，然後新增網繭聯盟詳細資料、為全域權利指定全域啟動 URL，接著同步權利，並為特定網路範圍設定用戶端存取 URL。

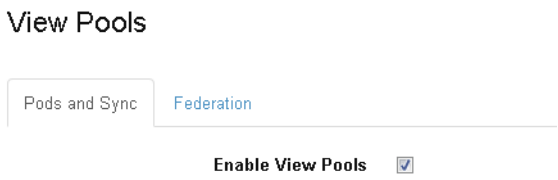
先決條件

- 遵循整合 View 網繭聯盟的需求中所述的需求來設定您的 View 環境。
- 根據設定您的 VMware Identity Manager 環境中所述的需求來設定您的 VMware Identity Manager 執行個體。

- 對於每個 View 網繭，您需要具有管理員角色之使用者的認證。

程序

1. 在管理主控台中，按一下**目錄**索引標籤。
2. 按一下**管理桌面平台應用程式**，然後選取 **View 應用程式**。
3. 在**網繭和同步**索引標籤中，選取**啟動 View 集區**核取方塊 (如果尚未核取)。

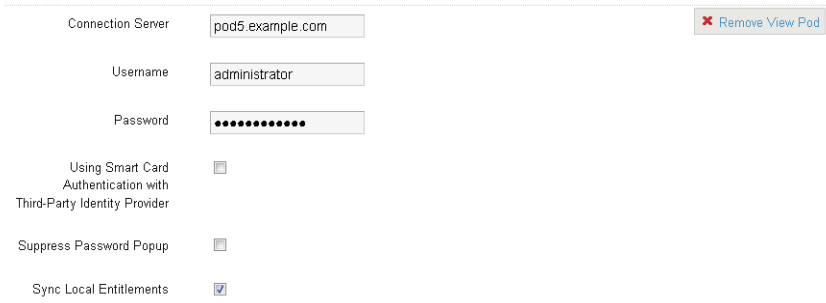


4 新增屬於雲端網繭聯盟的所有 View 網繭，一次新增一個。

a 提供 View 網繭的詳細資料。

選項	說明
連線伺服器	輸入 Horizon 連線伺服器執行個體的完整網域名稱 (FQDN)，例如 pod5server.example.com。網域名稱必須符合 Horizon 連線伺服器執行個體所加入的網域名稱。
使用者名稱	網繭的管理員使用者名稱。使用者必須具有 View 中的管理員角色。
密碼	網繭的管理員密碼。
使用第三方身分識別提供者的智慧卡驗證	如果使用者使用智慧卡驗證 (而非密碼) 來登入此 View 網繭，請選取核取方塊。
已在 Horizon View 上啟用 True SSO	此選項僅適用於支援 True SSO 功能的 Horizon 版本。 在 View 中設定 True SSO 時，使用者不需要密碼即可登入其 Windows 桌面平台。不過，如果使用者使用非密碼驗證方法 (例如 SecurID) 登入 VMware Identity Manager，則當使用者啟動其 Windows 桌面平台時，系統會提示他們輸入密碼。您可以選取此選項以防止在該案例中向使用者顯示密碼對話方塊。
同步本機權利	如果已為網繭設定本機權利，請選取此核取方塊。

例如：



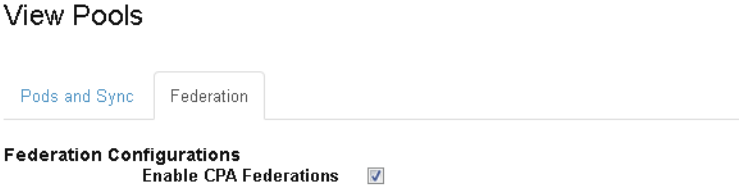
b 按一下**新增 View 網繭**，並新增下一個網繭。

c 重複這些步驟，直到您在雲端網繭聯盟中新增所有網繭為止。

5 按一下**儲存**。

隨即顯示每個網繭中的複寫伺服器。

6 按一下**聯盟**索引標籤，並選取**啟動 CPA 聯盟**核取方塊。



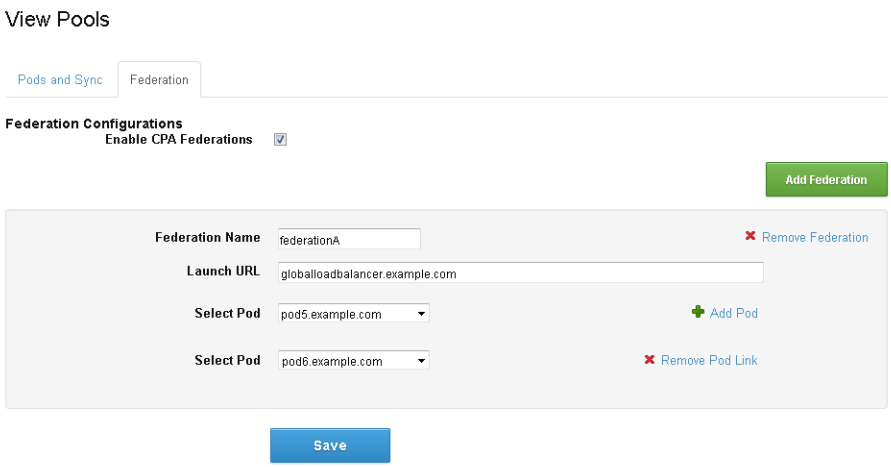
7 在**聯盟名稱**欄位中，輸入雲端網繭聯盟的名稱。

8 在**啟動 URL** 欄位中，輸入用來啟動全域授權桌面平台或應用程式的全域啟動 URL。例如，**federationA.example.com**。

啟動 URL 通常是雲端網繭聯盟的全域負載平衡器 URL。您可以在稍後的組態程序中，為特定網路範圍自訂啟動 URL。

9 選取屬於雲端網繭聯盟的網繭。

您在**網繭和同步**索引標籤中新增的所有網繭會在下拉式清單中列出。



10 按一下**新增網繭**並選取屬於雲端網繭聯盟的所有網繭，一次選取一個。

11 按一下**儲存**。

12 按一下**網繭和同步**索引標籤，捲動至頁面的底部，並為您的組態設定部署和同步選項。

選項	說明
部署類型	選取讓使用者能夠使用 View 資源的方法。 ■ **使用者啟動**：VMware Identity Manager 會將 View 資源新增至 Workspace ONE 中的 [目錄] 頁面。若要使用資源，使用者必須將資源從 [目錄] 頁面移至 [啟動器] 頁面。 ■ **自動**：VMware Identity Manager 會將資源直接新增至 [啟動器] 頁面，以供使用者立即使用。 您在此處選取的部署類型，即為對您的 View 整合中所有資源的所有使用者權利進行套用的全域設定。您可以在資源的 [權利] 頁面上，針對各個資源修改個別使用者或群組的部署類型。 建議您將全域部署類型設為**使用者啟動**。接著，您可以針對各個資源修改特定使用者或群組的設定。 如需關於設定部署類型的詳細資訊，請參閱設定 View 權利的部署類型。
不要同步重複的應用程式	如果您想要防止從多個伺服器同步重複的應用程式，請選取此選項。在多個資料中心部署 VMware Identity Manager 時，系統會在多個資料中心中設定相同的資源。選取此選項，可防止您的 VMware Identity Manager 目錄中出現重複的桌面平台或應用程式集區。

<table>
<tr><th>選項</th><th>說明</th></tr>
<tr><td>設定 5.x 連線伺服器</td><td>如果您在此頁面上設定的任何 View 連線伺服器執行個體是 5.x 版，請選取此核取方塊。
選取此選項，可讓您以替代方式同步 View 5.x 所需的資源。

備註 如果您選取執行目錄同步選項，設定 5.x 連線伺服器選項也將自動選取，因為這兩個選項都依存於同步資源的替代方式。</td></tr>
<tr><td>執行目錄同步</td><td>如果您想要在 VMware Identity Manager 目錄中遺漏了任何有權使用 Horizon 連線伺服器 執行個體之 View 集區的使用者和群組時，讓目錄同步作為 View 同步的一部分來執行，請選取此核取方塊。
[執行目錄同步] 選項僅適用於本機權利。它不適用於全域權利。如果 VMware Identity Manager 目錄中遺失具有全域權利的使用者和群組，則不會觸發目錄同步。
透過此程序進行同步的使用者和群組，可如同由 VMware Identity Manager 目錄同步新增的任何其他使用者一般進行管理。

重要事項 使用 [執行目錄同步] 選項時，View 同步會比較耗時。

備註 選取此選項時，設定 5.x 連線伺服器選項也將自動選取，因為這兩個選項都依存於同步資源的替代方式。</td></tr>
<tr><td>選擇 View 集區同步頻率</td><td>選取您要 View 資源和權利進行同步的頻率。您可以設定一般的同步排程，或選擇手動同步。如果您選擇手動，則每當 View 資源或權利中發生變更時，您必須回到此頁面並按一下立即同步。</td></tr>
<tr><td>選取預設啟動用戶端</td><td>選取用以啟動 View 應用程式或桌面平台的預設用戶端。
<table><tr><th>選項</th><th>說明</th></tr><tr><td>無</td><td>系統不會在管理員層級設定預設喜好設定。如果此選項設為無，且使用者喜好設定也未設定，則系統會使用 View 的預設顯示通訊協定設定來決定如何啟動桌面平台或應用程式。</td></tr><tr><td>瀏覽器</td><td>View 桌面平台和應用程式依預設會在 Web 瀏覽器中啟動。使用者喜好設定 (若已設定) 會覆寫此設定。</td></tr><tr><td>用戶端</td><td>View 桌面平台和應用程式依預設會在 Horizon Client 中啟動。使用者喜好設定 (若已設定) 會覆寫此設定。</td></tr></table>此設定會套用至 View 整合中的所有使用者和所有資源。
預設啟動用戶端設定會依照下列順序套用喜好設定 (由最高排到最低)：
a 使用者喜好設定，設定於 Workspace ONE 入口網站中。此選項無法在 Workspace ONE 應用程式中使用。
b Administrator 的選取預設啟動用戶端設定，設定於 VMware Identity Manager 管理主控台的 [View 集區] 頁面中。
c 適用於桌面平台或應用程式集區的 Horizon View 遠端顯示通訊協定 > 預設顯示通訊協定設定，設定於 Horizon Administrator 中。例如，當顯示通訊協定設為 PCoIP 時，應用程式或桌面平台會在 Horizon Client 中啟動。</td></tr>
</table>

13 按一下**儲存**。

14 按一下**立即同步**。

每當您在 View 中變更資訊 (例如新增權利或新增使用者) 時，您需要同步才能將變更填入 VMware Identity Manager。

15 在頁面右上角，按一下**管理主控台**。

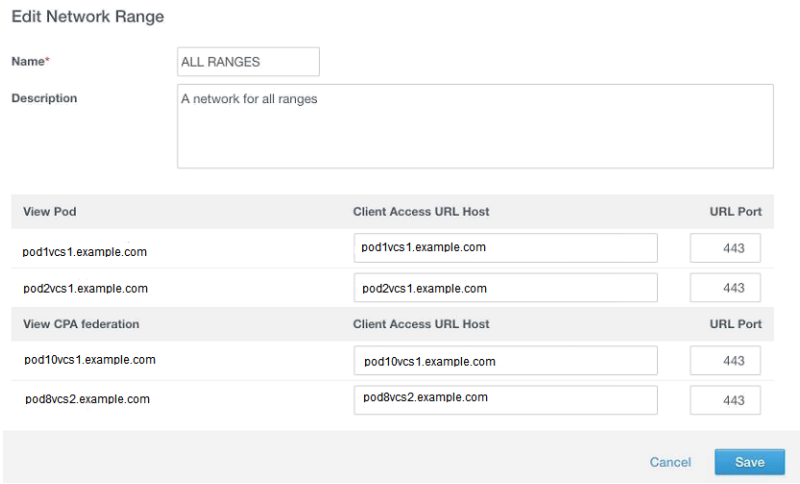
16 按一下**身分識別與存取管理**索引標籤，然後按一下頁面右側的**設定**。

17 按一下**網路範圍**索引標籤。

18 為特定網路範圍自訂啟動 URL。例如，通常會為內部和外部存取設定不同的啟動 URL。

a 選取網路範圍。您可以選取現有網路範圍或建立新的網路範圍。您也可以編輯預設的**所有範圍**網路範圍。

隨即顯示 [編輯網路範圍] 頁面。**View CPA 聯盟**區段會列出您在**聯盟**索引標籤中所新增網繭聯盟的全域啟動 URL。如果您新增多個網繭聯盟，則全部會列出。**View 網繭**區段會列出**網繭和同步**索引標籤中已選取**同步本機權利**選項的所有 View 網繭。



b 在 **View CPA 聯盟**區段中，針對全域啟動 URL，指定伺服器的完整網域名稱，則來自此網路範圍的全域權利的啟動要求將會導向至該伺服器。這通常是 View 網繭聯盟部署的全域負載平衡器 URL。

例如：**lb.example.com**

全域啟動 URL 可用來啟動全域授權的資源。

c 在 **View 網繭**區段中，針對每一個 View 網繭執行個體，指定伺服器的完整網域名稱，則來自此網路範圍的本機權利的啟動要求將會導向至該伺服器。您可以指定 View 連線伺服器執行個體、負載平衡器或安全伺服器。例如，如果您要編輯提供內部存取的範圍，您將為網繭指定內部負載平衡器。

例如：**lb.example.com**

用戶端存取 URL 用來從網繭啟動本機授權的資源。

另請參閱為自訂網路範圍啟用多個用戶端存取 URL。

設定 SAML 驗證

若要從 VMware Identity Manager 服務啟動 View、Horizon 6、Horizon 7 應用程式或桌面平台並擁有從 VMware Identity Manager 通往應用程式或桌面平台的單一登入，您必須在 View 部署的所有 View 連線伺服器執行個體中設定 SAML 驗證。

如果您的組織使用透過第三方身分識別提供者的智慧卡驗證來檢視 View 資源，請勿執行該項工作。

程序

1 以具備管理員角色的使用者身分登入 View Administrator Web 介面。

2 針對 View 部署中的每個 View 連線伺服器執行個體設定 SAML 驗證。在驗證器組態頁面上，您必須使用 VMware Identity Manager 服務的完整網域名稱。

重要事項 View 和 VMware Identity Manager 必須處於時間同步狀態。如果 View 和 VMware Identity Manager 未處於時間同步狀態，當您嘗試啟動 View 應用程式或桌面平台時，會出現無效的 SAML 訊息。

下一個

您必須建立 VMware Identity Manager 和 View 連線伺服器之間的 SSL 信任，並且加以維護。

建立或更新 VMware Identity Manager 與 View 連線伺服器之間的 SSL 信任

首先，您必須在 View 連線伺服器上接受 SSL 憑證，以建立 VMware Identity Manager 與 View 連線伺服器之間的信任。如果您在整合之後變更 View 連線伺服器上的 SSL 憑證，則必須返回 VMware Identity Manager 並重新建立該信任。

先決條件

- 確認 View 具有已安裝的 SSL 憑證。依預設，View 會有自我簽署憑證。
- 在 View 中，將 View 連線伺服器的憑證變更為根簽署憑證。如需設定 View 連線伺服器執行個體或安全伺服器以使用新憑證的相關資訊，請參閱 VMware View 文件。
- 在 View 連線伺服器上設定 SAML 驗證。在驗證器組態頁面上，一律須使用 VMware Identity Manager FQDN。

備註 如果您使用第三方身分識別提供者從 VMware Identity Manager 存取 View 桌面平台，則 View 連線伺服器上的 SAML 驗證必須設定為 `allowed`。

程序

1 在 VMware Identity Manager 管理主控台中，按一下**目錄**索引標籤。

2 按一下**管理資源類型**，然後選取 **View 應用程式**。

3 按一下 [複寫的伺服器群組] 旁的**更新 SSL 憑證**連結。

4 在 [憑證資訊] 頁面上，按一下**接受**。

如果 VMware Identity Manager 憑證在初始設定後有所變更，則您必須從 View 重新接受 SAML 驗證器。如果 View 憑證有所變更，則必須在 VMware Identity Manager 中接受 SSL 憑證。

為自訂網路範圍啟用多個用戶端存取 URL

如果您的公司對不同的網路範圍使用了多個用戶端存取 URL，則您必須編輯預設網路範圍，讓使用者能夠連線到正確的用戶端存取 URL 和連接埠號碼。如果這些設定未更新，Horizon Client 將不會啟動。

程序

1. 登入 VMware Identity Manager 管理主控台。
2. 按一下**身分識別與存取管理**索引標籤。
3. 在右側按一下**設定**，然後按一下**網路範圍**。
4. 按一下要修改的網路範圍。

   [編輯網路範圍] 頁面隨即出現。只有在您已整合 Cloud Pod 架構 (CPA) 部署 (也稱為網繭聯盟) 時，**View CPA 聯盟**區段才會出現。此區段會列出您在 [View 集區] 頁面的**聯盟**索引標籤中為網繭聯盟指定的全域啟動 URL。**View 網繭**區段會列出所有已選取**同步本機權利**選項的 View 網繭。
5. 使用您的公司組態，在**用戶端存取 URL 主機**和 **URL 連接埠**欄位中指定用戶端存取 URL 和連接埠。

   例如：**pod6.mycompany.com**
6. 確認您環境中的每個網路範圍都包含用戶端存取 URL。

重要事項 如果遺漏了網路範圍，透過該網路範圍啟動的使用者可能會遇到問題。

檢視 View 桌面平台和應用程式集區的連線資訊

您可以檢視關於 VMware Identity Manager 和 View 桌面平台或應用程式集區連線的資訊。

程序

1. 登入 管理主控台。
2. 按一下**目錄**索引標籤。
3. 若要檢視桌面平台集區，按一下**任何應用程式類型 > View 桌面平台集區**。若要檢視桌面平台集區，按一下**任何應用程式類型 > View 主控應用程式**。
4. 按一下 View 應用程式或桌面平台集區的名稱。
5. 按一下左側的**詳細資料**。
6. 檢視包含從 View 連線伺服器執行個體擷取的屬性的連線資訊。

   查看關於這些屬性的 View 說明文件詳細資料。

檢視 View 桌面平台與應用程式集區的使用者和群組權利

您可以查看 VMware Identity Manager 使用者和群組獲授權的 View 集區。

先決條件

- 從 View 連線伺服器執行個體同步資訊和相關的權利至 VMware Identity Manager。您可以在 管理主控台 中的 [View 集區] 頁面上，透過按一下**立即同步**來強制進行同步。

程序

1 登入 管理主控台。

2 檢視 View 桌面平台與應用程式集區的使用者和群組權利。

選項	動作
列出獲授權使用特定 View 桌面平台集區的使用者和群組。	a 按一下**目錄**索引標籤。 b 按一下**任何應用程式類型 > View 桌面平台集區**或 **View 主控應用程式**。 c 按一下您想要列出其權利的 View 集區的圖示。 依預設會選取**權利**索引標籤。群組權利和使用者權利會列於不同的表格中。
特定使用者或群組的 View 桌面平台與應用程式集區權利的清單。	a 按一下**使用者和群組**索引標籤。 b 按一下**使用者**索引標籤或**群組**索引標籤。 c 按一下個別使用者或群組的名稱。 d 按一下**應用程式**索引標籤。 隨即列出使用者或群組獲授權的 View 桌面平台與應用程式集區。

設定 View 權利的部署類型

您可以設定 View 資源的部署類型，以決定如何讓使用者能夠在 Workspace ONE 中使用這些資源。將部署類型設為 [使用者啟動] 之後，系統會將資源新增至 [目錄] 頁面。若要使用資源，使用者必須將資源從 [目錄] 頁面移至 [啟動器] 頁面。將部署類型設為 [自動] 之後，系統會將資源直接新增至 [啟動器] 頁面，以立即供使用者使用。

您可以設定不同層級的部署類型。

- 全域層級

  全域設定會套用至您的部署中所有 View 資源的所有使用者權利。您可以在第一次整合 View 資源與 VMware Identity Manager 時，從 [View 集區] 頁面指定全域部署類型。在初始整合之後，您可以從相同的頁面修改全域設定。請注意，如果您在初始整合後變更了全域設定，新的設定將僅會套用至同步的新權利。若要修改現有的權利，您可以變更個別資源層級的設定。

  備註 建議您將全域部署類型設為 [使用者啟動]。在一般情況下，您會先將全域設定設為 [使用者啟動]，再將其修改為針對特定使用者和群組權利進行啟用。

- 使用者或群組權利層級

  您也可以針對特定的使用者和群組，在個別的應用程式或桌面平台層級上設定部署類型。此設定會覆寫全域設定。此設定在後續同步期間將不會變更。

在同步期間，系統不會變更現有權利的部署類型。對於同步中的新權利，系統會套用全域設定。

備註 當資源啟動後，也就是資源顯示在使用者的 [啟動器] 頁面後，它將持續顯示在 [啟動器] 頁面中，除非使用者加以刪除。對部署類型所做的任何變更，皆不會將該資源從 [啟動器] 頁面中移除。

程序

1 若要設定全域層級的部署類型，請執行下列步驟。

a 按一下**目錄**索引標籤，然後選取**管理桌面平台應用程式 > View 應用程式**。

b 選取**網繭和同步**索引標籤。

c 在**部署類型**欄位中，選取**使用者啟動**或**自動**。

備註 建議您將全域部署類型設為**使用者啟動**。

d 按一下**儲存**。

這些設定將從下次同步時開始套用至所有新的權利。

2 若要為特定的使用者或群組權利設定部署類型，請執行下列步驟。

a 按一下**目錄**索引標籤。

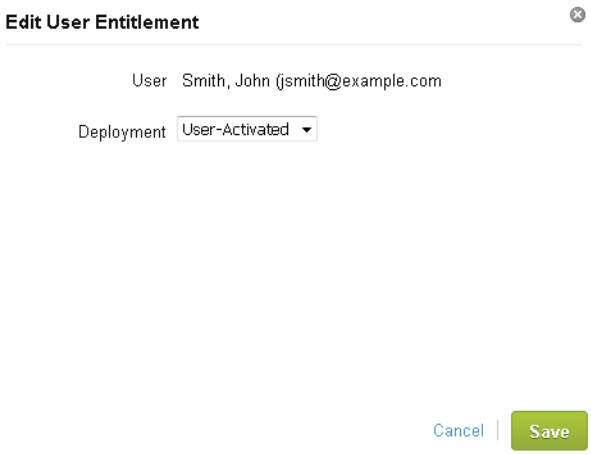
b 按一下要編輯權利的應用程式或桌面平台。

c 按一下**權利**，以顯示應用程式的 [權利] 頁面。

您可以在**部署**資料行中檢視使用者和群組權利目前的部署設定。

d 在您要編輯的權利旁，按一下**編輯**。

e 在 [編輯使用者權利] 對話方塊中，選取權利的部署類型。



f 按一下**儲存**。

設定使用者或群組權利層級的部署類型時，將具有高於全域部署類型設定的優先順序，且在同步期間將不會遭到修改。

檢視 View 桌面平台和應用程式的啟動選項

根據在 View 中設定桌面平台或應用程式的方式，View 桌面平台和應用程式可以在 Horizon Client 或 Web 瀏覽器中從 Workspace ONE 啟動。如果僅將 View 桌面平台或應用程式設定用於 Horizon Client，使用者就必須在其系統上安裝 Horizon Client。

View 的 HTML Access 功能可提供 View 管理員將 View 桌面平台或應用程式設定用於瀏覽器的選項。此項設定在 View 中完成，VMware Identity Manager 中無須進行任何設定。在 Horizon 7 中，由**允許在此伺服器陣列上使用桌面平台和應用程式的 HTML Access** 設定會決定 VMware Identity Manager 中的使用者是否可選擇在瀏覽器中從該伺服器陣列啟動桌面平台或應用程式。

VMware Identity Manager 對 Horizon 6.1.1 及更新版本提供 HTML Access 支援。

VMware Identity Manager 也支援 View 對 Horizon Client 提供支援的所有顯示通訊協定。對於 Horizon 7，除了 PCoIP 和 RDP for Horizon Client 4.0，VMware Identity Manager 另外也支援 Blast 通訊協定。當 VMware Identity Manager 使用者在 Horizon Client 中啟動桌面平台或應用程式，Horizon Client 會使用在 View 中為伺服器陣列設定的通訊協定。

備註 在 View 中，除了設定預設顯示通訊協定，管理員也能指定是否允許使用者選擇顯示通訊協定。如果您想支援不支援預設通訊協定的 Horizon Client 版本，則建議您允許使用者選擇顯示通訊協定。否則，將無法啟動應用程式或桌面平台。

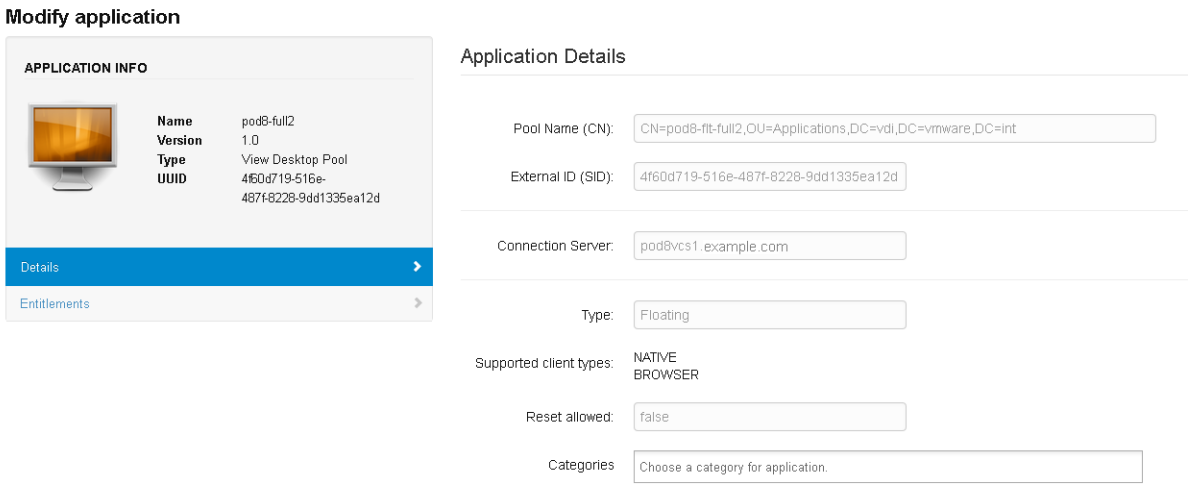
如需設定顯示通訊協定和啟動選項的相關資訊，請參閱 Horizon 7、Horizon 6 或 View 說明文件。

在 VMware Identity Manager 管理主控台中，您可查看 View 桌面平台或應用程式支援的啟動選項。

程序

1. 登入 VMware Identity Manager 管理主控台。
2. 按一下**目錄**索引標籤。
3. 若要顯示桌面平台集區，請按一下**任何應用程式類型 > View 桌面平台集區**。若要顯示應用程式，請按一下**任何應用程式類型 > View 主控應用程式**。
4. 按一下 View 應用程式或桌面平台的名稱。
5. 按一下左側的**詳細資料**。

   支援的用戶端類型欄位會顯示啟動選項。



此欄位的值可以是**原生**或**瀏覽器**，或兩者。如果僅列出**原生**，則只能從 Horizon Client 啟動桌面平台或應用程式。使用者必須先在其系統上安裝 Horizon Client，才能從 Workspace ONE 啟動應用程式。如果有列出**瀏覽器**，則使用者可以在瀏覽器中啟動應用程式或桌面平台。如果兩者都指定，則使用者可以選取啟動應用程式的方式。

備註 對於 Horizon 7 整合，必須在 Horizon 7 中啟用**允許在此伺服器陣列上使用桌面平台和應用程式的 HTML Access** 選項，**瀏覽器**選項才會出現在**支援的用戶端類型**清單中。

啟動 View 桌面平台或應用程式

使用者可以從 Workspace ONE 入口網站或應用程式啟動 View 桌面平台或應用程式。

根據在 View 中設定應用程式或桌面平台的方式，這些資源可在 Horizon Client 或瀏覽器中啟動。對於只能在 Horizon Client 中啟動的應用程式或桌面平台，使用者必須在其系統上安裝 Horizon Client。對於可以在 Horizon Client 或瀏覽器中啟動的應用程式和桌面平台，使用者可以選取啟動方法。

使用者也可在 Workspace ONE 入口網站的**喜好設定**頁面中設定其預設啟動喜好設定。此使用者喜好設定會覆寫在管理員層級上設定的任何預設啟動喜好設定。

備註 使用者無法在 Workspace ONE 應用程式中設定預設啟動喜好設定。

先決條件

根據在 View 中設定應用程式或桌面平台的方式，使用者可能需要安裝 Horizon Client。

如需受支援的 Horizon Client 版本，請參閱《VMware 產品互通性對照表》，網址為：http://www.vmware.com/resources/compatibility/sim/interop_matrix.php。

程序

1 登入 Workspace ONE 入口網站。

2 以滑鼠右鍵按一下您要使用的桌面平台或應用程式，然後檢查啟動選項可供使用。

如果啟動選項無法使用，表示連結已停用。

3 如果系統要求且您尚未在系統上安裝 Horizon Client，請進行安裝。

4 以滑鼠右鍵按一下桌面平台或應用程式，然後選取**在瀏覽器中啟動**或**在用戶端中啟動**。

如果選擇**瀏覽器**選項，應用程式或桌面平台會在瀏覽器中啟動。如果您使用的是 Horizon 6.1.1 或更新版本，瀏覽器視窗也會顯示 HTML Access 系統匣。

備註 如果 View 連線伺服器執行個體上的 SAML 中繼資料已到期，則應用程式或桌面平台將不會啟動。若要解決此問題，您必須再次將 View 資源同步至 VMware Identity Manager。在管理主控台的 [View 集區] 頁面中，按一下**立即同步**。

允許使用者在 VMware Identity Manager 中重設其 View 桌面平台

視您設定 View 和 VMware Identity Manager 的方式而定，使用者可以使用 應用程式入口網站 來重設沒有回應的 View 桌面平台。

當您設定 View 以允許使用者重設其桌面平台時，組態會同時套用至 View 和 VMware Identity Manager。

先決條件

- 設定 View 以允許使用者重設其桌面平台。請參閱 View、Horizon 6 或 Horizon 7 的說明文件，特別是*《View 管理》*指南。
- 為確保特定 View 桌面平台可由使用者重設，相關網繭的用戶端存取 URL 應該具有信任的憑證。如果 URL 具有根簽署或自我簽署憑證，請設定 VMware Identity Manager 以信任那些憑證。請參閱*《VMware Identity Manager 安裝與設定》*，以取得套用根憑證的相關資訊。

程序

- (選擇性) 確認 VMware Identity Manager 將指定的桌面平台列為可由使用者重設。
  a 在管理主控台中，選取**目錄**索引標籤。
  b 在**任何應用程式類型**下拉式功能表中，選取 **View 桌面平台集區**。
  c 按一下桌面平台的名稱。
  d 按一下**詳細資料**。
  e 確認**允許重設**設定是設為 **true**。

  如果設定為 **false**，則 View 未設定為允許使用者重設桌面平台。

下一個

如果 View 桌面平台日後變得沒有回應，您或使用者可以在 應用程式入口網站 中透過以滑鼠右鍵按一下沒有回應的桌面平台，然後按一下**重設桌面平台**來重設桌面平台。

設定特定應用程式和桌面平台的存取原則

預設存取原則集會套用至您的目錄中的所有應用程式和桌面平台。您也可以設定個別應用程式或桌面平台集區的存取原則，這將會覆寫預設存取原則。

您可以從 [原則] 頁面將存取原則套用至一或多個應用程式和桌面平台，或從 [應用程式組態] 頁面中選取特定應用程式的存取原則。

如需存取原則的詳細資訊，請參閱《*VMware Identity Manager 管理指南*》。

程序

1 若要從 [原則] 頁面將存取原則套用至應用程式和桌面平台，請遵循下列步驟。

   a 導覽至 [身分識別與存取管理] > [管理] > [原則] 頁面。

   b 按一下原則加以編輯，或按一下**新增原則**以建立新原則。

   c 在原則頁面中，編輯或定義原則。

   d 在**套用到**區段中，選取要套用原則的應用程式。

   e 按一下**儲存**。

2 若要從 [應用程式組態] 頁面中選取特定應用程式的存取原則，請遵循下列步驟。

   a 按一下**目錄**索引標籤。

   b 按一下應用程式。

   c 按一下左窗格中的**存取原則**。

   d 選取應用程式的存取原則，然後按一下**儲存**。

在非持續性 View 桌面平台中減少資源使用並增加 VMware Identity Manager 桌面平台的效能

在非持續性桌面平台 (亦即無狀態桌面平台) 中使用 Workspace ONE 入口網站時，若要減少資源使用並增加效能，您可以使用針對在非持續性 View 桌面平台中使用而最佳化的設定，來設定用戶端。

問題

當非持續性 View 桌面平台在 View 桌面平台中安裝了 VMware Identity Manager 桌面平台應用程式時，每次使用者啟動工作階段即會增加使用的資源數量，例如儲存區 I/O。

原因

非持續性 View 桌面平台原本即為無狀態。這類 View 桌面平台也稱為浮動桌面平台，而重新撰寫浮動桌面平台或從集區提供使用者新桌面平台時，您可以建立新工作階段。除非使用在非持續性桌面平台的 VMware Identity Manager 桌面平台應用程式是使用針對此案例最佳化的設定而進行設定，否則使用者在存取 ThinApp 套件時，可能會遇到效能降級。

一般來說，您會使用命令列安裝程式選項來設定 View 桌面平台的 VMware Identity Manager 桌面平台應用程式。請參閱 VMware Identity Manager 桌面平台的命令列安裝程式選項。

解決方案

- 使用建議的命令列安裝程式選項，在用於非持續性 View 桌面平台的範本中安裝 VMware Identity Manager 桌面平台應用程式。

/v 安裝程式選項	說明
ENABLE_AUTOUPDATE = 0	防止將 VMware Identity Manager 桌面平台應用程式自動更新為較新的版本。一般來說，您的 View 管理員會在範本中更新應用程式。
INSTALL_MODE = RUN_FROM_SHARE	如果您計劃讓使用者使用這些 View 桌面平台中的 ThinApp 套件，請使用此選項，讓 ThinApp 套件從伺服器串流 (而非下載) 到 Windows 系統。

以下是使用針對非持續性 View 桌面平台的最佳化組態 (其中預期使用者會使用 ThinApp 套件) 來安裝 VMware Identity Manager 桌面平台應用程式的範例。WORKSPACE_SERVER 選項會指定此安裝的 VMware Identity Manager 伺服器。

```
VMware-Identity-Manager-Desktop-n.n.n-nnnnnnn.exe /v WORKSPACE_SERVER="https://server.company.com"
ENABLE_AUTOUPDATE=0 INSTALL_MODE=RUN_FROM_SHARE
```

提供 VMware Horizon Cloud Service 的存取權

4

搭配主控或內部部署基礎結構的 VMware Horizon Cloud Service 可以與 VMware Identity Manager 服務整合。

將 Horizon Cloud 與 VMware Identity Manager 服務整合，可讓使用者能夠從 Workspace ONE 入口網站或應用程式存取其有權使用的 Horizon Cloud 應用程式和桌面平台。如此一來，使用者可以從單一位置跨裝置存取其所有的應用程式。

桌面平台和應用程式集區 (也稱為指派) 會設定在 Horizon Cloud 承租人中。您也需要在 Horizon Cloud 承租人中 (而非在 VMware Identity Manager 服務中) 設定使用者和群組權利。您必須從 Active Directory 將這些使用者和群組同步到 VMware Identity Manager 服務，之後才能與 Horizon Cloud 承租人整合。

整合 Horizon Cloud 承租人與 VMware Identity Manager 之後，您將可在 VMware Identity Manager 管理主控台中檢視 Horizon Cloud 桌面平台和應用程式。您也可以檢視使用者和群組權利。

您可以設定同步排程，以定期將資源和權利從 Horizon Cloud 承租人同步到 VMware Identity Manager 服務。

使用者可從 Workspace ONE 入口網站或應用程式啟動其有權使用的桌面平台和應用程式。這些桌面平台和應用程式可在瀏覽器中透過 HTML 進行存取，或在 VMware Horizon® Client™ 中透過支援的顯示通訊協定進行存取。支援 Horizon Client 3.4 版和更新版本。

本章節討論下列主題:

整合 Horizon Cloud 桌面平台和應用程式

若要將 Horizon Cloud 桌面平台和應用程式與 VMware Identity Manager 服務整合，您需要在 VMware Identity Manager 管理主控台中新增 Horizon Cloud 承租人詳細資料，並且從 Horizon Cloud 承租人同步資源和權利。您也需要設定 SAML 驗證，以啟用 Horizon Cloud 承租人與 VMware Identity Manager 服務之間的信任關係。

整合的先決條件

整合 Horizon Cloud 與 VMware Identity Manager 之前，請確定您符合先決條件。

- 確認您具有下列安裝：
  - 一個以內部部署方式部署的 VMware Identity Manager
  - 一個可由 VMware Identity Manager 服務存取的 Horizon Cloud 承租人。請與您的 Horizon Cloud 代表合作以安裝此項目。

    重要事項 您的 VMware Identity Manager 部署和 Horizon Cloud 承租人必須要有 VPN 連線才可正常運作。
  - 如果您使用其他外部連接器，請確定您使用的是 2016.1.1 版或更新版本。
- 確認您的 Horizon Cloud 承租人符合下列需求。
  - 承租人名稱必須是完整網域名稱 (FQDN)，而不只有主機名稱。例如，使用 `server-ta1.example.com` 而非 `server-ta1`。
  - 承租人應用裝置必須具備由 CA 簽發的有效簽署憑證。不支援自我簽署憑證。憑證必須符合承租人應用裝置的 FQDN。
  - 如果您建立了 VMware Identity Manager 目錄，並以 UPN 作為搜尋屬性，而您想要從 Horizon Cloud 承租人同步靜態桌面平台集區，則您的服務提供者必須為承租人啟用 UPN 並重新啟動承租人應用裝置，否則使用者將無法啟動靜態桌面平台。
- 確定 Horizon Cloud 承租人和 VMware Identity Manager 服務處於時間同步狀態。若未處於時間同步狀態，則當使用者啟動 Horizon Cloud 桌面平台和應用程式時，可能會發生無效 SAML 錯誤。
- 在 Horizon Cloud 承租人管理主控台中，建立並設定桌面平台和應用程式集區 (也稱為指派)。您可以在 Horizon Cloud 承租人中建立下列類型的集區：
  - 動態桌面平台集區 (也稱為浮動桌面平台指派)
  - 靜態桌面平台集區 (也稱為專用桌面平台指派)
  - 搭配桌面平台的工作階段型集區 (也稱為工作階段桌面平台指派)
  - 搭配應用程式的工作階段型集區 (也稱為遠端應用程式指派)

  如需集區類型的詳細資訊，請參閱 Horizon Air 說明文件。

  適用下列限制。
  - 您僅能從單一 Horizon Cloud 承租人同步至 VMware Identity Manager。
- 在 Horizon Air 承租人管理主控台中，設定 Horizon Cloud 桌面平台和應用程式的使用者和群組權利。

  備註 只有屬於已登錄群組之使用者的權利才會進行同步。不屬於任何群組的使用者，將無法在 VMware Identity Manager 中看見其權利。
- 在 VMware Identity Manager 管理主控台中，確定擁有這些權利的使用者和群組已從 Active Directory 同步至使用目錄同步的 VMware Identity Manager。

在 VMware Identity Manager 中啟用 Horizon Cloud 桌面平台和應用程式

若要將 Horizon Cloud 桌面平台和應用程式與 VMware Identity Manager 服務整合，您必須在 VMware Identity Manager 管理主控台中新增 Horizon Cloud 承租人詳細資料，並且將資源和權利從 Horizon Cloud 承租人同步至 VMware Identity Manager 服務。

備註 如果您已在高可用性案例中設定多個連接器，則必須在所有連接器中設定 Horizon Cloud 整合。您可以在其中一個連接器上設定自動同步排程，但必須在其他連接器上設定手動同步。

先決條件

- 確認已符合 整合的先決條件中所說明的必要條件。
- 確認 Horizon Cloud 承租人名稱是完整網域名稱 (FQDN)。例如，*server-ta1-1.example.com* (而不是 *server-ta1-1*)。
- 確認 v 承租人應用裝置已安裝來自 CA 的有效 SSL 憑證。不支援自我簽署憑證。憑證必須符合承租人應用裝置的 FQDN。

程序

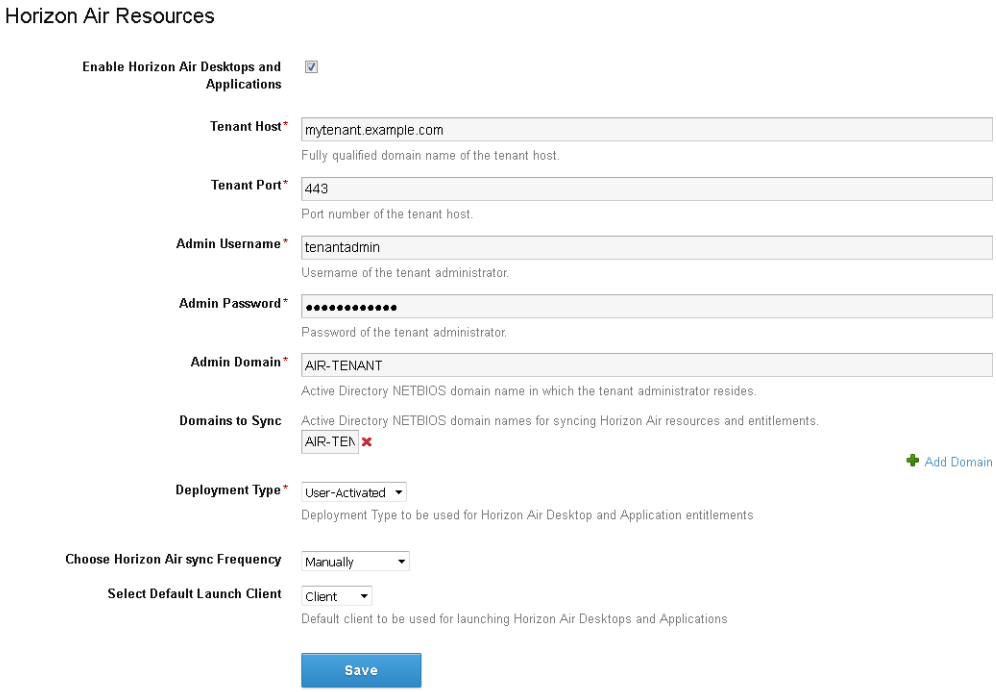
1. 登入 VMware Identity Manager 管理主控台。
2. 在**目錄**索引標籤中，選取**管理桌面平台應用程式 > Horizon Cloud**。
3. 選取**啟用 Horizon Cloud 桌面平台和應用程式**核取方塊。
4. 輸入環境的資訊。

   重要事項 輸入您的網域資訊時，請勿使用非 ASCII 字元。

選項	說明
承租人主機	承租人主機的完整網域名稱。例如：`tenant1.example.com`
承租人連接埠	承租人主機的連接埠號碼。例如：`443`
管理員使用者名稱	承租人管理員帳戶的使用者名稱。例如：`tenantadmin`
管理員密碼	承租人管理員帳戶的密碼。
管理員網域	承租人管理員所在的 Active Directory NETBIOS 網域名稱。
要同步的網域	用來同步 Horizon Cloud 資源和權利的 Active Directory NETBIOS 網域名稱。 **備註** 此欄位須區分大小寫。輸入名稱時，請確實使用適當的大小寫。

<table>
<tr><th>選項</th><th>說明</th></tr>
<tr><td>部署類型</td><td>選取讓使用者能夠使用 Horizon Cloud 資源的方法。
使用者啟動：Horizon Cloud 資源會新增至 Workspace ONE 中的 [目錄] 頁面。若要使用資源，使用者必須將資源從 [目錄] 頁面移至 [啟動器] 頁面。
自動：Horizon Cloud 資源會直接新增至 Workspace ONE 中的 [啟動器] 頁面，立即供使用者使用。
您在此處選取的部署類型，即為對您的 Horizon Cloud 整合中所有資源的所有使用者權利進行套用的全域設定。您可以在資源的 [權利] 頁面上，針對各個資源修改個別使用者或群組的部署類型。
建議您將全域部署類型設為使用者啟動。接著，您可以針對各個資源修改特定使用者或群組的設定。
如需關於設定部署類型的詳細資訊，請參閱設定 Horizon Cloud 權利的部署類型。</td></tr>
<tr><td>選擇 Horizon Air 同步頻率</td><td>同步 Horizon Cloud 資源和權利的頻率。您可以設定一般的同步排程，或選擇手動同步。如果您選擇手動，則每當 Horizon Cloud 資源或權利中發生變更時，您就必須回到此頁面並按一下立即同步。</td></tr>
<tr><td>選取預設啟動用戶端</td><td>選取用以啟動 Horizon Cloud 應用程式或桌面平台的預設用戶端。<table><tr><th>選項</th><th>說明</th></tr><tr><td>無</td><td>系統不會在管理員層級設定預設喜好設定。如果此選項設為無，且使用者喜好設定也未設定，則系統會使用 Horizon Cloud 預設通訊協定設定來決定如何啟動桌面平台或應用程式。</td></tr><tr><td>瀏覽器</td><td>Horizon Cloud 桌面平台和應用程式依預設會在 Web 瀏覽器中啟動。使用者喜好設定 (若已設定) 會覆寫此設定。</td></tr><tr><td>用戶端</td><td>Horizon Cloud 桌面平台和應用程式依預設會在 Horizon Client 中啟動。使用者喜好設定 (若已設定) 會覆寫此設定。</td></tr></table>此設定會套用至 Horizon Cloud 整合中的所有使用者和所有資源。
預設啟動用戶端設定會依照下列順序套用喜好設定 (由最高排到最低)：<ol type="a">
使用者喜好設定，設定於 Workspace ONE 入口網站中。此選項不適用於 Workspace ONE 應用程式。
管理員的選取預設啟動用戶端設定，設定於 VMware Identity Manager 管理主控台的 [Horizon Cloud 資源] 頁面中。
Horizon Cloud 預設通訊協定設定。</td></tr>
</table>

例如：



5 按一下**儲存**。

6 按一下**立即同步**，將資源和權利從 Horizon Cloud 承租人同步至 VMware Identity Manager 服務。

下一個

設定 SAML 驗證。

設定 SAML 驗證

設定 SAML 驗證以啟用服務提供者 (Horizon Cloud 承租人) 與身分識別提供者 (VMware Identity Manager) 之間的信任。

若要設定 SAML 驗證，您必須在 VMware Identity Manager 管理主控台中建立 Horizon Cloud 承租人的聯盟構件，並在 Horizon Cloud 承租人中設定 SAML 驗證。

建立 Horizon Cloud 的聯盟構件

若要設定 SAML 驗證，您必須建立 Horizon Cloud 承租人的聯盟構件。

先決條件

向服務提供者確認以下事項：

- Horizon Cloud 承租人名稱是完整網域名稱 (FQDN)。例如，*server-ta1-1.example.com* (而不是 *server-ta1-1*)。
- Horizon Cloud 承租人應用裝置已安裝來自 CA 的有效 SSL 憑證。不支援自我簽署憑證。憑證必須符合承租人應用裝置的 FQDN。

程序

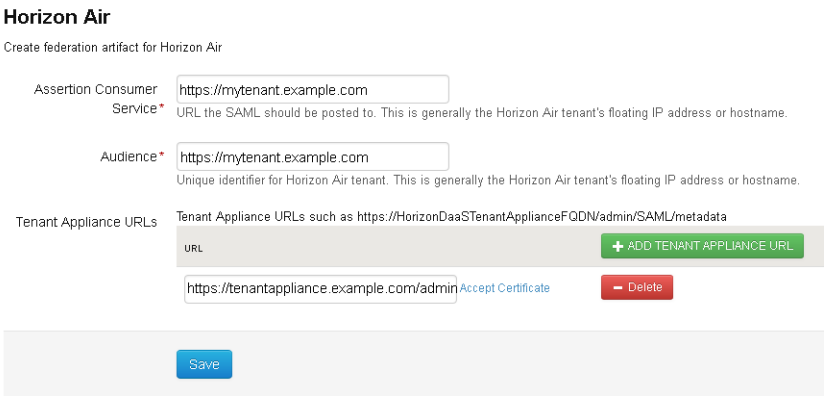
1 在 VMware Identity Manager 管理主控台內，按一下**目錄**索引標籤中的箭頭，接著選取**設定**。

2 在左窗格中，選取 **Horizon Cloud**。

3 輸入環境資訊以建立聯盟構件。

設定	說明
宣告取用者服務	張貼 SAML 宣告的目的地 URL。此 URL 通常是 Horizon Cloud 承租人的浮動 IP 或 Access Point URL。例如，https://mytenant.example.com。
對象	Horizon Cloud 承租人的唯一識別碼。此 URL 通常是 Horizon Cloud 承租人的浮動 IP 或 Access Point URL。例如，https://mytenant.example.com。
承租人應用裝置 URL	Horizon Cloud 承租人應用裝置的 URL，其格式為 https://*TenantApplianceFQDN*/admin/SAML/metadata。如果您擁有多個承租人應用裝置，請按一下**新增承租人應用裝置 URL** 來新增 URL。 如果承租人應用裝置位在浮動 IP 或 Access Point 應用裝置後方，請依照下列格式指定浮動 IP 或 Access Point 應用裝置 URL：https://*FloatingIPorAccessPointFQDN*/admin/SAML/metadata。

例如：



4 按一下各個 Horizon Cloud 承租人應用裝置 URL 旁的**接受憑證**連結以接受憑證。

重要事項 如果您在整合後變更 Horizon Cloud 承租人應用裝置上的 SSL 憑證，則必須返回此頁面並再次接受憑證以重新建立信任。

5 按一下**儲存**。

下一個

設定 Horizon Cloud 承租人中的 SAML 驗證。

設定 Horizon Cloud 承租人中的 SAML 驗證

在 VMware Identity Manager 管理主控台中建立聯盟構件後，請設定 Horizon Cloud 承租人中的 SAML 驗證。

備註 如果您的組織使用透過第三方身分識別提供者的智慧卡驗證來檢視 View 資源，請勿設定 SAML 驗證。

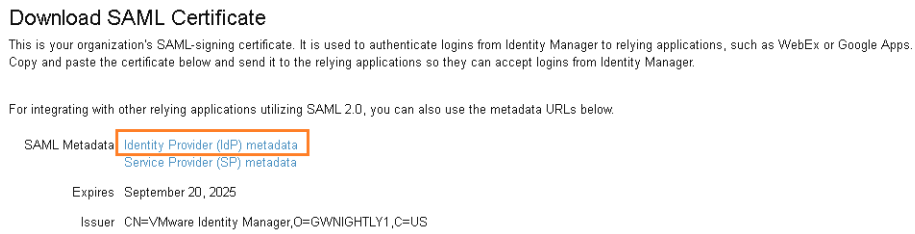
備註 Horizon Cloud 承租人應用裝置和 VMware Identity Manager 必須處於時間同步狀態。如果它們未處於時間同步狀態，當您嘗試啟動 Horizon Cloud 桌面平台和應用程式時，會顯示無效的 SAML 訊息。

程序

1 在 VMware Identity Manager 管理主控台內，按一下**目錄**索引標籤上的箭頭，接著選取**設定**。

2 在左窗格中按一下 **SAML 中繼資料**。

3 按一下**身分識別提供者 (IdP) 中繼資料**連結。



4 記下瀏覽器網址列中的 URL，如 https://*VMwareIdentityManagerFQDN*/SAAS/API/1.0/GET/metadata/idp.xml。

5 登入 Horizon Cloud 承租人。

6 導覽至**設定 > 一般設定 > 編輯**。

7 在 **IDM** 區段中，輸入必要的資訊。

選項	說明
IDM URL	您在步驟 4 中複製的 VMware Identity ManagerIdP 中繼資料。
逾時 SSO 權杖	(選用) 使 SSO 權杖逾時的時間長度 (以分鐘為單位)。
資料中心	Horizon Cloud 資料中心名稱。例如 Horizon。
承租人位址	Horizon Cloud 承租人位址。指定 Horizon Cloud 承租人應用裝置的浮動 IP 位址或主機名稱，或 Access Point IP 位址或主機名稱。例如 mytenant.example.com。

您的整合作業已完成。現在，您可以在 VMware Identity Manager 管理主控台中檢視 Horizon Cloud 桌面平台和應用程式集區，而使用者可以啟動他們有權使用的資源。

自訂 Horizon Cloud 整合的使用者識別碼

您可以自訂在使用者啟動 Horizon Cloud 應用程式和桌面平台時要在 SAML 回應中使用的使用者識別碼。依預設會使用「使用者主體名稱」。您可以選擇使用其他名稱識別碼格式 (例如 sAMAccountName 或電子郵件地址)，並自訂其中的值。

在下列情況中，選取名稱識別碼格式的功能相當實用：

- 同步來自多個子網域的使用者時，使用者主體名稱無法正常運作。您可以使用不同的名稱識別碼格式 (例如 sAMAccountName 或電子郵件地址) 以唯一識別使用者。

重要事項 確定 Horizon Cloud 和 VMware Identity Manager 中的名稱識別碼格式設定相同。

先決條件

您已在 [Horizon Cloud 資源] 頁面中啟用並設定 Horizon Cloud 整合 (該頁面可從**目錄 > 管理桌面平台應用程式 > Horizon Cloud** 存取)。

程序

1 在 VMware Identity Manager 管理主控台內，按一下**目錄**索引標籤中的箭頭，接著選取**設定**。

2 按一下左側的 **Horizon Cloud**。

3 在 Horizon Cloud 頁面中，指定要使用的名稱識別碼格式。

選項	說明
名稱識別碼格式	選取名稱識別碼格式，例如電子郵件地址或使用者主體名稱。預設值為**未指定 (使用者名稱)**。
名稱識別碼值	按一下**選取建議值**並從預先定義的值清單中選擇，或按一下**自訂值**並輸入值。預設值為 **${user.userPrincipalName}**。

4 按一下**儲存**。

下一個

在您每次進行變更並按一下 Horizon Cloud 資源整合頁面中的**儲存**後 (該頁面可從**目錄 > 管理桌面平台應用程式 > Horizon Cloud** 存取)，請返回**目錄 > 設定 > Horizon Cloud** 頁面確認設定，然後再按一次**儲存**。

如果儲存此頁面上的設定時發生錯誤，請按一下**重設**，接著再次輸入組態詳細資料，然後按一下**儲存**。

同步 Horizon Cloud 桌面平台和應用程式與 VMware Identity Manager

當您初始整合 Horizon Cloud 與 VMware Identity Manager 時，您需要將資源和權利從 Horizon Cloud 承租人同步至 VMware Identity Manager 服務。若您設定同步排程，則系統後續會定期同步資源和權利。此外，您可以隨時使用**立即同步**選項將更新同步至 VMware Identity Manager。

程序

1 登入 VMware Identity Manager 管理主控台。

2 在**目錄**索引標籤中，按一下**管理桌面平台應用程式 > Horizon Cloud**。

3 按一下**立即同步**。

4 (選用) 若要指定定期同步排程，請選取**選擇 Horizon Cloud 同步頻率**欄位中的一個選項，然後按一下**儲存**。

檢視 Horizon Cloud 桌面平台和應用程式集區的詳細資料

在 VMware Identity Manager 管理主控台中，您可以檢視已同步 Horizon Cloud 桌面平台和應用程式集區的相關資訊。

程序

1 登入 VMware Identity Manager 管理主控台。

2 按一下**目錄**索引標籤。

3 按一下**任何應用程式類型**，並選取 **Horizon Cloud 桌面平台**或 **Horizon Cloud 應用程式**。

4 選取桌面平台或應用程式集區。

5 按一下**詳細資料**。

系統會顯示從 Horizon Cloud 承租人中擷取的屬性。如需這些屬性的相關資訊，請參閱 Horizon Cloud 說明文件。

檢視 Horizon Cloud 桌面平台和應用程式的使用者和群組權利

在 VMware Identity Manager 管理主控台中，您可以檢視特定使用者和群組的 Horizon Cloud 權利。

Horizon Cloud 資源的使用者和群組權利會在 Horizon Cloud 承租人管理介面中設定，且無法從 VMware Identity Manager 管理主控台修改。

先決條件

若要檢視最新資訊，請同步 Horizon Cloud 桌面平台和應用程式。您可以藉由選取**目錄 > 管理桌面平台應用程式 > Horizon Cloud** 以前往 [Horizon Air 資源] 頁面，然後按一下**立即同步**來強制執行同步。

程序

1 登入 VMware Identity Manager 管理主控台。

2 檢視 Horizon Cloud 桌面平台和應用程式的使用者和群組權利。

選項	動作
列出有權使用特定 Horizon Cloud 桌面平台或應用程式集區的使用者和群組。	a 按一下**目錄**索引標籤。 b 按一下**任何應用程式類型 > Horizon Cloud 桌面平台**或 **Horizon Cloud 應用程式**。 c 選取您想要列出其權利的集區。 依預設會選取**權利**索引標籤。群組權利和使用者權利會列於不同的表格中。
特定使用者或群組之 Horizon Cloud 桌面平台和應用程式集區權利的清單。	a 按一下**使用者和群組**索引標籤。 b 按一下**使用者**索引標籤或**群組**索引標籤。 c 按一下個別使用者或群組的名稱。 d 按一下**應用程式**索引標籤。 隨即列出使用者或群組獲授權的 Horizon Cloud 桌面平台與應用程式集區。

設定特定應用程式和桌面平台的存取原則

預設存取原則集會套用至您的目錄中的所有應用程式和桌面平台。您也可以設定個別應用程式或桌面平台集區的存取原則，這將會覆寫預設存取原則。

您可以從 [原則] 頁面將存取原則套用至一或多個應用程式和桌面平台，或從 [應用程式組態] 頁面中選取特定應用程式的存取原則。

如需存取原則的詳細資訊，請參閱《*VMware Identity Manager 管理指南*》。

程序

1 若要從 [原則] 頁面將存取原則套用至應用程式和桌面平台，請遵循下列步驟。

a 導覽至 [身分識別與存取管理] > [管理] > [原則] 頁面。

b 按一下原則加以編輯，或按一下**新增原則**以建立新原則。

c 在原則頁面中，編輯或定義原則。

d 在**套用到**區段中，選取要套用原則的應用程式。

e 按一下**儲存**。

2 若要從 [應用程式組態] 頁面中選取特定應用程式的存取原則，請遵循下列步驟。

a 按一下**目錄**索引標籤。

b 按一下應用程式。

c 按一下左窗格中的**存取原則**。

d 選取應用程式的存取原則，然後按一下**儲存**。

設定 Horizon Cloud 權利的部署類型

您可以設定 Horizon Cloud 資源的部署類型，以決定如何讓使用者能夠使用這些資源。將部署類型設為 [使用者啟動] 之後，系統會將資源新增至 Workspace ONE 中的 [目錄] 頁面。若要使用資源，使用者必須將資源從 [目錄] 頁面移至 [啟動器] 頁面。將部署類型設為 [自動] 之後，系統會將資源直接新增至 [啟動器] 頁面，以立即供使用者使用。

您可以設定不同層級的部署類型。

- 全域層級

  全域設定會套用至您的部署中所有 Horizon Cloud 資源的所有使用者權利。您可以在第一次整合 Horizon Cloud 資源與 VMware Identity Manager 時，使用 [Horizon Air 資源] 頁面指定全域部署類型。在初始整合之後，您可以從相同的頁面修改全域設定。請注意，如果您在初始整合後變更了全域設定，新的設定將僅會套用至同步的新權利。若要修改現有的權利，您可以變更個別資源層級的設定。

  備註 建議您將全域部署類型設為 [使用者啟動]。在一般情況下，您會先將全域設定設為 [使用者啟動]，再將其修改為針對特定使用者和群組權利進行啟用。

- 使用者或群組權利層級

  您也可以針對特定的使用者和群組，在個別的應用程式或桌面平台層級上設定部署類型。此設定會覆寫全域設定。此設定在後續同步期間將不會變更。

在同步期間，系統不會變更現有權利的部署類型。對於同步中的新權利，系統會套用全域設定。

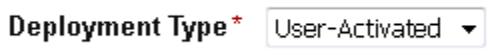
備註 當資源啟動後，也就是資源顯示在使用者的 [啟動器] 頁面後，它將持續顯示在 [啟動器] 頁面中，除非使用者加以刪除。對部署類型所做的任何變更，皆不會將該資源從 [啟動器] 頁面中移除。

程序

1 若要設定全域層級的部署類型，請執行下列步驟。

  a 按一下**目錄**索引標籤，然後選取**管理桌面平台應用程式 > Horizon Cloud**。

  b 在 [Horizon Cloud 資源] 頁面的**部署類型**欄位中，選取**使用者啟動**或**自動**。



  備註 建議您將全域部署類型設為**使用者啟動**。

  c 按一下**儲存**。

  這些設定將從下次同步時開始套用至所有新的權利。

2 若要為特定的使用者或群組權利設定部署類型，請執行下列步驟。

  a 按一下**目錄**索引標籤。

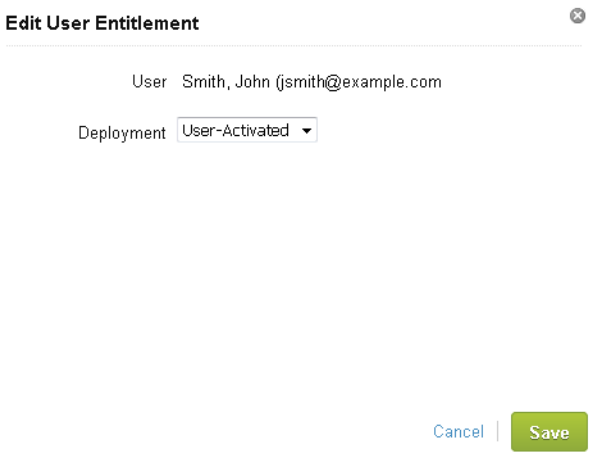
  b 按一下要編輯權利的應用程式或桌面平台。

c 按一下**權利**，以顯示應用程式的 [權利] 頁面。

您可以在**部署**資料行中檢視使用者和群組權利目前的部署設定。

d 在您要編輯的權利旁，按一下**編輯**。

e 在 [編輯使用者權利] 對話方塊中，選取權利的部署類型。



f 按一下**儲存**。

設定使用者或群組權利層級的部署類型時，將具有高於全域部署類型設定的優先順序，且在同步期間將不會遭到修改。

啟動 Horizon Cloud 桌面平台或應用程式

使用者可登入 Workspace ONE 入口網站或應用程式，並啟動他們有權使用的 Horizon Cloud 桌面平台和應用程式。

根據在 Horizon Cloud 承租人中設定應用程式或桌面平台的方式，這些資源可在 Horizon Client 或瀏覽器中啟動。對於只能在 Horizon Client 中啟動的應用程式或桌面平台，使用者必須在其系統上安裝 Horizon Client。對於可以在 Horizon Client 或瀏覽器中啟動的應用程式和桌面平台，使用者可以選取啟動方法。

使用者也可在 Workspace ONE 入口網站的**喜好設定**頁面中設定其預設啟動喜好設定。此使用者喜好設定會覆寫在管理員層級上設定的任何預設啟動喜好設定。

備註 使用者無法在 Workspace ONE 應用程式中設定預設啟動喜好設定。

程序

1 登入 Workspace ONE 入口網站。

2 以滑鼠右鍵按一下您要使用的桌面平台或應用程式，然後檢查啟動選項可供使用。

如果啟動選項無法使用，表示連結已停用。

3 如有需要，請在您的系統上安裝 Horizon Client。

4 以滑鼠右鍵按一下桌面平台或應用程式，然後選取**在瀏覽器中啟動**或**在用戶端中啟動**。

提供對 VMware ThinApp 套件的存取權

5

使用 VMware Identity Manager，您可集中發佈與管理 ThinApp 套件。ThinApp 套件是用於 Windows 系統的虛擬化 Windows 應用程式。Windows 系統上已安裝 VMware Identity Manager 桌面平台 應用程式的已授權使用者，可以在其 Windows 系統上啟動並使用獲授權的 ThinApp 套件。

在 ThinApp 擷取和建置程序中，您會透過 Windows 應用程式建立虛擬應用程式。該虛擬 Windows 應用程式可以在 Windows 系統上執行，而該系統不需安裝原始 Windows 應用程式。 ThinApp 套件是透過在 Windows 應用程式上執行 ThinApp 擷取和建置程序所產生之虛擬應用程式檔案的組合。套件包含可存取 Windows 應用程式的主要資料容器檔案和進入點檔案。

不是每個 ThinApp 套件都與 VMware Identity Manager 相容。當您擷取 Windows 應用程式時，ThinApp 擷取和建立程序中的預設設定會建立 VMware Identity Manager 無法發佈和管理的套件。藉由在擷取和建置程序期間設定適當的參數，您會建立 VMware Identity Manager 可以發佈和管理的 ThinApp 套件。 請參閱 VMware ThinApp 文件，以取得有關 ThinApp 功能以及可用來建立與 VMware Identity Manager 相容之套件的適當參數的詳細資訊。

將 VMware Identity Manager 與 ThinApp 存放庫整合後，您可在目錄中看到來自存放庫且 VMware Identity Manager 可以發佈和管理的 ThinApp 套件。在 VMware Identity Manager 目錄中看到 ThinApp 套件後，您便可將這些 ThinApp 套件授權給使用者和群組，也能選擇設定每個套件的授權追蹤資訊。

本章節討論下列主題:

整合 VMware ThinApp 套件

若要使用 VMware Identity Manager 來發佈及管理以 VMware® ThinApp® 封裝的應用程式，您必須具有包含 ThinApp 套件的 ThinApp 存放庫、指向該存放庫，然後同步套件。同步程序完成後，ThinApp 套件即可在您的 VMware Identity Manager 目錄中使用，且您可以將其權利賦予您的 VMware Identity Manager 使用者和群組。

ThinApp 會將應用程式從基礎作業系統及其程式庫和架構中解除，並且將應用程式綁定到稱為應用程式套件的單一可執行檔，以進行應用程式虛擬化。若要由 VMware Identity Manager 管理，這些套件必須以適當的選項啟用。例如，在 [ThinApp 設定擷取] 精靈中，選取**使用 Workspace 進行管理**核取方塊。如需 ThinApp 功能以及如何讓應用程式可由 VMware Identity Manager 管理的詳細資訊，請參閱 VMware ThinApp 文件。

一般而言，在 VMware Identity Manager 環境的整體安裝和設定程序中，您必須執行將 VMware Identity Manager 連線到存放庫及同步套件的步驟。ThinApp 存放庫必須是可由 VMware Identity Manager 使用統一命名慣例 (UNC) 路徑來存取的網路共用。VMware Identity Manager 會定期與這個網路共用同步，以取得 VMware Identity Manager 發佈及管理套件所需的 ThinApp 套件中繼資料。請參閱 VMware Identity Manager 對 ThinApp 套件和網路共用存放庫的需求。

網路共用可以是通用網際網路檔案系統 (CIFS) 或分散式檔案系統 (DFS) 共用。DFS 共用可以是單一伺服器訊息區 (SMB) 檔案共用，或組織成分散式檔案系統的多個 SMB 檔案共用。支援在 NetApp 儲存區系統上執行的 CIFS 和 DFS 共用。

VMware Identity Manager 對 ThinApp 套件和網路共用存放庫的需求

當您從 VMware Identity Manager 擷取並儲存 ThinApp 應用程式以進行發佈時，您必須符合特定需求。

對 ThinApp 套件的需求

若要建立或重新封裝可由 VMware Identity Manager 管理的 ThinApp 套件，您必須使用 VMware Identity Manager 所支援的 ThinApp 版本。VMware Identity Manager 支援 ThinApp 4.7.2 和更新版本。如需支援版本的更新資訊，請參閱*《VMware 產品互通性對照表》*，網址是 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php。

您必須具有可由 VMware Identity Manager 管理的 ThinApp 套件。在 ThinApp 的擷取和建置程序中，您可以建立可由 VMware Identity Manager 管理的套件，或是它無法管理的套件。例如，當您使用 [ThinApp 設定擷取] 精靈來擷取應用程式時，您可以藉由選取**使用 Workspace 進行管理**核取方塊，建立可由 VMware Identity Manager 管理的套件。請參閱 VMware ThinApp 文件，以取得有關 ThinApp 功能以及可用來建立與 VMware Identity Manager 相容之套件的適當參數的詳細資訊。

針對現有的 ThinApp 套件，您可以使用 `relink – h` 命令為 VMware Identity Manager 啟用套件。如需如何將現有 ThinApp 套件轉換為可由 VMware Identity Manager 管理之套件的相關資訊，請參閱*《VMware Identity Manager 管理指南》*。

您必須將 ThinApp 套件儲存在網路共用上，且該位置必須依據組織的需求，符合網路共用類型、存放庫存取和所需 ThinApp 套件部署模式之組合的需求。

對網路共用存放庫的需求

ThinApp 套件必須位於網路共用 (也稱為 ThinApp 套件存放庫) 上。網路共用必須可使用統一命名慣例 (UNC) 路徑，從用來存取 ThinApp 套件的 VMware Identity Manager 桌面平台 應用程式執行所在的每個系統來存取。例如，主機 `server` 上名為 `appshare` 的網路共用，可使用 UNC 路徑 `\\server\appshare` 來存取。網路共用資料夾的完整主機名稱必須可從 VMware Identity Manager 解析。

網路共用可以是通用網際網路檔案系統 (CIFS) 或分散式檔案系統 (DFS) 共用。DFS 共用可以是單一伺服器訊息區 (SMB) 檔案共用，或組織成分散式檔案系統的多個 SMB 檔案共用。支援在 NetApp 儲存區系統上執行的 CIFS 和 DFS 共用。

網路共用必須符合您為 VMware Identity Manager 設定用來存取 ThinApp 套件存放庫的存取類型所適用的準則：網域型存取或帳戶型存取。存取類型將決定下列項目有哪些可行的組合：

- 您要為 ThinApp 套件存放庫使用 CIFS 網路共用還是 DFS 網路共用。
- 您是否必須將 VMware Identity Manager 和網路共用的主機加入至相同的 Active Directory 網域。
- 使用者的 Windows 系統是否必須加入 Active Directory 網域，以使用 ThinApp 套件。
- 安裝的 VMware Identity Manager 桌面平台 應用程式經設定用來取得及執行虛擬化應用程式 (在安裝應用程式的 Windows 系統上) 的 ThinApp 套件安裝模式。在使用者的 Windows 系統上使用的套件安裝模式，會在安裝程序期間將 VMware Identity Manager 桌面平台 應用程式安裝至該 Windows 系統時進行設定。此套件安裝模式會決定該 Windows 系統所使用的 ThinApp 部署模式、下載模式或串流模式。

存取類型	網路共用類型	對 VMware Identity Manager 的需求	使用者 Windows 系統的需求
網域型存取	在使用網域型存取時，您可以對 ThinApp 套件存放庫使用 CIFS 共用。 網域型存取無法使用 DFS 共用。如果您有 DFS 共用，您必須使用帳戶型存取。	您必須將 VMware Identity Manager 加入至 Active Directory 網域，使其能夠加入 Windows 網路共用並存取套件。 如需如何設定 VMware Identity Manager 以加入網域的詳細資訊，請參閱《*VMware Identity Manager 安裝與設定*》中有關於設定 Kerberos 的資訊。 **備註** Windows 驗證不是必要的。 網路共用必須根據電腦帳戶，支援驗證與檔案權限。VMware Identity Manager 可使用網域中 VMware Identity Manager 的電腦帳戶存取網路共用。 您必須設定網路共用的資料夾和檔案權限，使權限的組合允許網域中 VMware Identity Manager 的電腦帳戶進行讀取存取。	使用者的 Windows 系統必須加入 Active Directory 網域，該使用者才能使用其授權的 ThinApp 套件。 下列系統必須全部加入相同的網域： ■ 使用者的 Windows 系統 ■ VMware Identity Manager ■ 含有 ThinApp 套件之網路共用磁碟機的主機 在使用網域型存取時，ThinApp 套件會有下列安裝模式可使用。 ■ COPY_TO_LOCAL。使用此安裝模式時，套件會下載至用戶端 Windows 系統。此安裝模式對應於將 ThinApp 下載模式用於虛擬化應用程式。用來登入用戶端 Windows 系統的帳戶，就是用來將套件從網路共用複製到用戶端 Windows 系統的使用者帳戶，該帳戶必須具有從該網路共用讀取套件及複製檔案的權限。在套件下載至用戶端 Windows 系統，且使用者啟動套件之後，虛擬化應用程式即會在用戶端 Windows 系統上本機執行。 ■ RUN_FROM_SHARE。使用此安裝模式時，套件不會下載至用戶端 Windows 系統。使用者會使用本機桌面平台上的捷徑啟動套件，而虛擬化應用程式會透過 ThinApp 串流模式從網路共用執行。用來登入用戶端 Windows 系統的帳戶，就是用來從網路共用執行套件的使用者帳戶，該帳戶必須具有從該網路共用讀取及執行檔案的權限。 **備註** RUN_FROM_SHARE 最適用於隨時都具有 ThinApp 套件之網路共用連線的 Windows 系統。最符合前述條件的 Windows 系統是 View 桌面平台，因為它隨時都連線至其網域。View 桌面平台具有浮動 (或無狀態) 的特性，能夠巧妙運用 RUN_FROM_SHARE 來避免因為下載套件至 Windows 系統所產生的資源耗用。 依預設，當您藉由執行用戶端安裝程式的圖形化版本將 VMware Identity Manager 桌面平台 應用程式安裝至 Windows 系統時，COPY_TO_LOCAL 安裝模式會設定為預設安裝模式。若要將不同的安裝模式設定為套件的預設安裝模式，您必須使用命令列執行用戶端安裝。請參閱 VMware Identity Manager 桌面平台的命令列安裝程式選項。
帳戶型存取	在使用帳戶型存取時，您可以對 ThinApp 套件存放庫使用 CIFS 共用或 DFS 共用。	您必須將 VMware Identity Manager 設定成使用共用使用者帳戶和密碼，以存取網路共用和套件。 共用使用者帳戶和密碼是對網路共用資料夾的 UNC 路徑具有讀取權限的任何組合。	使用者的 Windows 系統不需要加入 Active Directory 網域，該使用者即可使用其授權的 ThinApp 套件。Windows 驗證不是必要的。 使用者的 Windows 系統、VMware Identity Manager 和含有 ThinApp 套件之網路共用的主機不需要加入相同的 Active Directory 網域。

存取類型	網路共用類型	對 VMware Identity Manager 的需求	使用者 Windows 系統的需求
		您無須將 VMware Identity Manager 加入至 Active Directory 網域即可存取網路共用。 **備註** 在管理主控台中，您必須先完成 [加入網域] 頁面，才能使用 [ThinApp 套件] 頁面。 **備註** 如果您要使用 NetApp 共用，則需要帳戶型存取。	設定為帳戶型存取時，ThinApp 套件會有下列安裝模式可使用。 ■ 如果使用者的 Windows 系統未加入網域，則用戶端必須使用 HTTP_DOWNLOAD 安裝模式取得虛擬化應用程式。此安裝模式對應於將 ThinApp 下載模式用於虛擬化應用程式。 VMware Identity Manager 會使用共用使用者帳戶從存放庫中擷取套件。 ■ 如果使用者將 Windows 系統加入至網域，用戶端將可使用 COPY_TO_LOCAL 安裝模式或 RUN_FROM_SHARE 安裝模式來執行使用者的授權 ThinApp 套件。用來登入用戶端 Windows 系統的帳戶，就是用來從網路共用取得套件的使用者帳戶，該帳戶必須具有該網路共用的適當權限。 如果使用者的 Windows 系統有時可能加入網域，有時則否，您可以啟用 COPY_TO_LOCAL 模式和 AUTO_TRY_HTTP 選項來安裝用戶端，只要針對帳戶型存取設定 VMware Identity Manager 即可。 使用此組態時，用戶端會先嘗試使用 COPY_TO_LOCAL 模式來下載套件。如果 Windows 系統當時未加入網域，則複製套件的嘗試將會失敗。不過，在啟用 AUTO_TRY_HTTP 選項後，用戶端將會立即嘗試使用 HTTP 來下載套件。當您藉由執行用戶端安裝程式的圖形化版本將 VMware Identity Manager 桌面平台 應用程式安裝至 Windows 系統時，預設會使用此一 COPY_TO_LOCAL 加上 AUTO_TRY_HTTP 的組合。 必須針對帳戶型存取設定 VMware Identity Manager，使用 HTTP_DOWNLOAD 模式下載套件的嘗試才能成功。

此外，ThinApp 套件存放庫必須根據此處說明的狀況符合下列準則。

- 當您的設定牽涉到加入 Active Directory 網域的系統時，請確定斷續的命名空間不會使網域成員電腦無法存取代管 ThinApp 套件的網路共用。當 Active Directory 網域名稱不同於該網域中的機器所使用的 DNS 命名空間時，就會發生斷續的命名空間。
- 您必須設定網路共用的檔案和共用權限，為您要使其透過 COPY_TO_LOCAL 或 RUN_FROM_SHARE 選項執行 ThinApp 應用程式的使用者提供執行應用程式所需的讀取權限和功能。

例如，對於您要使其以串流模式執行 ThinApp 應用程式之使用者的 Active Directory 使用者帳戶，將共用資料夾權限設定為**讀取**、並將 NTFS 權限設定為**讀取和執行**，將可為這些使用者提供執行應用程式所需的讀取權限和功能。

必須要有**讀取和執行**的 NTFS 權限設定，才能使用 ThinApp 串流模式執行 ThinApp 應用程式，這對應於 VMware Identity Manager 桌面平台 應用程式的 RUN_FROM_SHARE 安裝模式。如果您的組織需要將 NTFS 權限設定為**讀取**，您的使用者可以對虛擬化應用程式使用 ThinApp 下載模式。ThinApp 下載模式對應於使用 COPY_TO_LOCAL 安裝模式或 HTTP_DOWNLOAD 安裝模式來安裝 Windows 用戶端。無論使用前述何種安裝模式，應用程式都會下載至 Windows 系統並且在本機啟動。

CIFS 和 DFS 網路共用都必須將 ThinApp 套件組織在命名空間下之目錄的個別子目錄中，而不是命名空間本身的子目錄中，例如 `\\server\appshare\thinapp1`、`\\server\appshare\thinapp2` 等等。請參閱 為 VMware Identity Manager 管理的 ThinApp 套件建立網路共用。

為 VMware Identity Manager 管理的 ThinApp 套件建立網路共用

如果要啟用 VMware Identity Manager 的 VMware ThinApp 管理功能，以及讓使用者從目錄存取 ThinApp 套件，您必須建立網路共用並將 ThinApp 套件儲存在該網路共用資料夾內。

VMware Identity Manager 會從網路檔案共用取得所需之 ThinApp 套件的相關中繼資料。

先決條件

- 確認 ThinApp 套件符合 VMware Identity Manager 需求。
- 確認您擁有在 IT 環境中建立符合 VMware Identity Manager 對 ThinApp 套件之需求的適當存取權限。

程序

1. 建立符合 ThinApp 套件之 VMware Identity Manager 需求的網路共用。
2. 在網路共用中，為每個 ThinApp 套件建立一個網路共用子資料夾。

   一般來說，您會將子資料夾命名為符合 ThinApp 應用程式的名稱，或指出資料夾中包含的應用程式。例如，如果在名為 `server` 主機上的網路共用名為 `appshare`，並且應用程式稱為 `abceditor`，則 ThinApp 套件的子資料夾為 `\\server\appshare\abceditor`。

   備註 使用 VMware Identity Manager 為要發佈的 ThinApp 套件建立您的網路共用子資料夾名稱時，請勿使用非 ASCII 字元。不支援非 ASCII 字元。
3. 將每個 ThinApp 套件的檔案 (如 EXE 和 DAT 檔案) 複製到為套件之虛擬化應用程式命名的子資料夾。

   複製檔案後，您將擁有一組子資料夾，以及與下列檔案相似的檔案：

   - `\\server\appshare\abceditor\abceditor.exe`
   - `\\server\appshare\abceditor\abceditor.dat`

下一個

設定 VMware Identity Manager 對 ThinApp 套件的存取。

設定 VMware Identity Manager 對 ThinApp 套件的存取

若要設定 VMware Identity Manager 以將 ThinApp 套件的存取權限提供給使用者，您必須啟用 VMware Identity Manager 以尋找儲存的 ThinApp 套件，以及與 VMware Identity Manager 同步套件。

先決條件

- 利用適當組態建立網路共用，並將 ThinApp 套件儲存在該網路共用中的適當位置。請參閱 為 VMware Identity Manager 管理的 ThinApp 套件建立網路共用。
- 確認您已備妥 ThinApp 套件所在之網路共用資料夾的 UNC 路徑。
- 確認您擁有 Active Directory 網域名稱，以及在該 Active Directory 中擁有加入網域之權限的帳戶使用者名稱和密碼。即便使用帳戶型存取，管理主控台仍會要求您先完成 [加入網域] 頁面，之後才能使用 [ThinApp 套件] 頁面。

  若要啟用網域型存取，您還必須將 VMware Identity Manager 加入 ThinApp 套件存放庫加入的 Active Directory 網域。確認您擁有網路共用使用之網域的 Active Directory 網域名稱，以及在該 Active Directory 中擁有加入網域之權限的帳戶使用者名稱和密碼。Active Directory 帳戶的作用在於將 VMware Identity Manager 加入網域。
- 在啟用帳戶型存取時，請確認您擁有具備網路共用讀取權限的使用者名稱和密碼。請參閱 VMware Identity Manager 對 ThinApp 套件和網路共用存放庫的需求。

  備註 除非您想要將所有執行階段狀況下對 ThinApp 套件的使用限制為加入網域的 Windows 系統，否則除了網域型存取之外，您也應該要啟用帳戶型存取。對於使用者未將 Windows 系統加入網域但需要使用其授權 ThinApp 套件的執行階段狀況，這樣的組合能提供最大支援彈性。

程序

1 加入 Active Directory 網域。

   a 登入 管理主控台。

   b 選取**身分識別與存取管理**索引標籤。

   c 按一下**設定**。

d 在 [連接器] 頁面中，按一下適當連接器列中的**加入網域**。

e 在 [加入網域] 頁面上，輸入 Active Directory 網域的資訊，然後按一下**加入網域**。

重要事項 在輸入 Active Directory (AD) 網域名稱、AD 使用者名稱或 AD 密碼時，請勿使用非 ASCII 字元。管理主控台中的上述輸入欄位不支援非 ASCII 字元。

選項	說明
AD 網域	輸入 Active Directory 的完整網域名稱。例如，**HS.TRDOT.COM**。
AD 使用者名稱	輸入 Active Directory 中有權將系統加入至該 Active Directory 網域之帳戶的使用者名稱。
AD 密碼	輸入與 **AD 使用者名稱**相關聯的密碼。VMware Identity Manager 不會儲存此密碼。

重要事項 每次匯入 VMware Identity Manager 組態時，您都必須將 VMware Identity Manager 重新加入網域。

[加入網域] 頁面會重新整理，顯示目前已加入網域的訊息。

2 啟用儲存之 ThinApp 套件的存取。

a 選取**目錄**索引標籤。

b 按一下**管理桌面平台應用程式**，然後選取 **ThinApp 應用程式**。

c 選取**啟動封裝應用程式**核取方塊。

d 填寫資訊並按一下**儲存**。

重要事項 輸入此頁面上的欄位資訊時，請勿使用非 ASCII 字元。管理主控台中的上述輸入欄位不支援非 ASCII 字元。

選項	說明
路徑	以 UNC 路徑格式輸入 ThinApp 套件資料夾所在之共用資料夾的路徑 (`\\server\share\subfolder`)。例如：`\\DirectoryHost\ThinAppFileShare`。對於 *DirectoryHost*，請提供主機名稱，而非 IP 位址。 對於 CIFS 和 DFS 網路共用兩者，此路徑必須是命名空間下的目錄，不是命名空間本身。
選擇頻率	選取您希望 VMware Identity Manager 同步與 VMware Identity Manager 同在網路共用位置之 ThinApp 套件相關資訊的間隔。 若為每週間隔，請設定同步發生之日的日期和時間。若為每日間隔，請設定時間。
啟用帳戶型存取	如果您想要使用帳戶型存取，請選取此選項。 **備註** 如果您的 ThinApp 套件存放庫是 DFS 網路共用，您必須選取此選項。如果您希望使用者能在未加入網域之 Windows 系統上使用其授權 ThinApp 套件，必須啟用帳戶型存取。 **備註** 如果您使用 NetApp 共用，必須啟用帳戶型存取。
共用使用者	輸入擁有網路共用讀取權限之使用者帳戶的使用者名稱。當您選取**啟動帳戶型存取**時，需要使用這項資訊。
共用密碼	輸入與**共用使用者**使用者帳戶相關聯的密碼。

指出值已儲存的訊息隨即會出現，且上個同步狀態的摘要也會出現。

3 按一下**立即同步**以與 VMware Identity Manager 同步 ThinApp 套件。

完成同步處理所需的時間取決於 ThinApp 套件的數目。

當同步程序完成時，同步的 ThinApp 套件清單隨即會出現。

VMware Identity Manager 的設定現已完成，您可以授權群組和使用者使用 ThinApp 套件，讓他們也可以使用安裝在 Windows 系統上的 VMware Identity Manager 桌面平台 應用程式執行其授權的 ThinApp 套件。

下一個

授權群組和使用者使用 ThinApp 套件。請參閱 *《VMware Identity Manager 管理指南》*。

為使用者和群組賦予 ThinApp 套件的權利

您可以為使用者和群組賦予以 ThinApp 套件的形式擷取之 Windows 應用程式的權利。

您只能為 VMware Identity Manager 使用者 (從您的目錄伺服器匯入的使用者) 賦予 ThinApp 套件的權利。在您為使用者賦予 ThinApp 套件的權利後，使用者將可檢視應用程式，並可在系統上從 VMware Identity Manager 桌面平台 應用程式加以啟動。如果您移除權利，使用者即無法檢視或啟動應用程式。

一般而言，要為使用者賦予 ThinApp 套件的權利，最有效的方式是將 ThinApp 套件權利新增至使用者群組。在特定情況下，為個別使用者賦予 ThinApp 套件的權利，是較恰當的作法。

先決條件

設定 VMware Identity Manager，以將 ThinApp 套件同步至您的 VMware Identity Manager 目錄。ThinApp 套件同步至您的目錄時，您可以將其權利賦予給使用者和群組。

使用管理主控台將 ThinApp 套件同步至您的目錄。您無法從管理主控台將 ThinApp 套件直接新增至您的目錄。

程序

1 登入 管理主控台。

2 為使用者賦予 ThinApp 套件的權利。

選項	說明
存取 ThinApp 套件，然後為使用者或群組賦予套件的權利。	a 按一下**目錄**索引標籤。 b 按一下**任何應用程式類型 > ThinApp 套件**。 c 按一下要為使用者和群組賦予權利的 ThinApp 套件。 依預設會選取**權利**索引標籤。群組權利會列在一個表格中，使用者權利則列於另一個表格。 d 按一下**新增群組權利**或**新增使用者權利**。 e 輸入群組或使用者的名稱。 您可以開始輸入搜尋字串並讓自動完成功能列出選項，以搜尋使用者或群組。您可以按一下**瀏覽**以檢視完整清單。 f 在下拉式功能表中，選取 ThinApp 套件的啟動方法。 **自動** 使用者可在下次登入 VMware Identity Manager 桌面平台 應用程式時直接存取 ThinApp 套件。 **使用者啟動** 使用者必須在 VMware Identity Manager 桌面平台 應用程式中啟動 ThinApp 套件，才能使用應用程式。 g 按一下**儲存**。
存取使用者或群組，然後將 ThinApp 套件權利新增至該使用者或群組。	a 按一下**使用者和群組**索引標籤。 b 按一下**使用者**索引標籤或**群組**索引標籤。 c 按一下個別使用者或群組的名稱。 d 按一下**應用程式**索引標籤。 e 按一下**新增權利**。 f 在**應用程式類型**下拉式清單中，選取 **ThinApp 套件**。 g 按一下要為使用者或群組授權之 ThinApp 套件旁的核取方塊。 h 在**部署**資料行中，選取 ThinApp 套件的啟動方法。 **自動** 使用者可在下次登入 VMware Identity Manager 桌面平台 應用程式時直接存取 ThinApp 套件。 **使用者啟動** 使用者必須在 VMware Identity Manager 桌面平台 應用程式中啟動 ThinApp 套件，才能使用應用程式。 i 按一下**儲存**。

選取的使用者或群組此時會被賦予使用 ThinApp 套件的權利。

下一個

確認 VMware Identity Manager 桌面平台 應用程式已安裝在使用者的 Windows 系統上。

使用 VMware Identity Manager 發佈及管理 ThinApp 套件

您的 VMware Identity Manager 使用者必須在其 Windows 系統上安裝並執行 VMware Identity Manager 桌面平台 應用程式，才能執行其使用 VMware Identity Manager 完成登錄的 ThinApp 套件。

ThinApp 套件是虛擬化 Windows 應用程式。ThinApp 套件會發佈至 Windows 系統，登入 Windows 系統的使用者可啟動及執行已在該 Windows 系統上登錄的這些 ThinApp 套件。VMware Identity Manager 可發佈及管理與 VMware Identity Manager 相容的 ThinApp 套件。

若要成功地在使用者登入的 Windows 工作階段中啟動並執行其中一個虛擬化應用程式，必須符合下列要素：

- 已透過 VMware Identity Manager 登錄虛擬化應用程式的 ThinApp 套件以供該使用者使用。
- 該 Windows 系統上有特定的 DLL 可供使用。
- `hws-desktop-client.exe` 程序執行中。

在相容的 ThinApp 套件建立後，依設定會在已登入的使用者在其登入的 Windows 工作階段中啟動虛擬化應用程式時載入特定 DLL。此時，虛擬化應用程式會嘗試載入 DLL。在 DLL 載入時，它會嘗試向本機安裝的 VMware Identity Manager 桌面平台 應用程式驗證該 ThinApp 套件是否已在 Windows 桌面平台上為該使用者進行登錄。本機安裝的 VMware Identity Manager 桌面平台 應用程式會直接判斷該應用程式是否已為該使用者登錄，而無須與 VMware Identity Manager 通訊。如果應用程式已在該 Windows 桌面平台上為該使用者登錄，VMware Identity Manager 桌面平台 應用程式會確認它上次與 VMware Identity Manager 同步的時間。如果 VMware Identity Manager 桌面平台 應用程式確認距離上次同步的時間未超過為已安裝的用戶端設定的離線寬限期，則用戶端會允許應用程式執行。

由於只有在已安裝 VMware Identity Manager 桌面平台 應用程式時，Windows 系統上才會有 DLL 可供使用，且由於在 VMware Identity Manager 桌面平台 應用程式執行於該系統時，會執行 `hws-desktop-client.exe` 程序，因此必須在 Windows 系統上安裝 VMware Identity Manager 桌面平台 應用程式，才能執行由 VMware Identity Manager 發佈及管理的 ThinApp 套件。

部署 VMware Identity Manager 桌面平台 應用程式以使用 ThinApp 套件

VMware Identity Manager 桌面平台 應用程式可藉由按兩下其安裝程式 EXE 檔案、使用命令列選項執行可執行檔，或執行使用命令列選項的指令碼來安裝。必須具有本機管理員權限，才可安裝應用程式。如需藉由按兩下安裝程式 EXE 檔案來安裝 VMware Identity Manager 桌面平台 應用程式的相關資訊，請參閱 *《VMware Identity Manager 使用者指南》*。

已安裝之應用程式的組態會決定由 VMware Identity Manager 發佈的 ThinApp 套件如何部署至該 Windows 系統。依預設，在藉由按兩下安裝程式 EXE 檔案來安裝 VMware Identity Manager 桌面平台 應用程式時，用戶端會設定成使用 COPY_TO_LOCAL 部署模式 (啟用 AUTO_TRY_HTTP 選項) 來部署 ThinApp 套件。這些預設安裝程式選項會產生所謂的下載部署模式。透過 COPY_TO_LOCAL 和 AUTO_TRY_HTTP 預設設定，用戶端應用程式會先嘗試藉由將 ThinApp 套件複製到 Windows 系統端點的方式加以下載，如果此嘗試失敗，用戶端應用程式會嘗試使用 HTTP 來下載 ThinApp 套件。

如果為 VMware Identity Manager 設定了對 ThinApp 存放庫的帳戶型存取，用戶端應用程式將可使用 HTTP 來下載 ThinApp 套件。在 ThinApp 套件下載至本機 Windows 系統後，使用者即可在本機系統上執行虛擬化應用程式。

若要避免虛擬化應用程式下載至本機 Windows 系統而使用 Windows 系統上的空間，您可以讓使用者藉由使用所謂的串流部署模式從網路共用來執行 ThinApp 套件。若要讓您的使用者透過串流模式執行 ThinApp 套件，您必須使用命令列安裝程序在 Windows 系統上安裝 VMware Identity Manager 桌面平台 應用程式。安裝程式具有命令列選項，可讓您用來設定 ThinApp 套件的執行階段部署模式。若要設定執行階段部署模式以串流處理 ThinApp 套件，請使用 RUN_FROM_SHARE 安裝程式選項。

將 VMware Identity Manager 桌面平台 應用程式安裝至多個 Windows 系統的方法之一，是使用指令碼以無訊息的方式將應用程式安裝至 Windows 系統。您可以用無訊息的方式同時將用戶端安裝至多個 Windows 系統。

備註 無訊息安裝在安裝程序期間不會顯示訊息或視窗。

您必須在指令碼中設定一個值，指出以該指令碼安裝的用戶端是要使用 ThinApp 串流模式來部署 ThinApp 套件，還是使用 RUN_FROM_SHARE 選項或其中一個 ThinApp 下載模式 (例如 COPY_TO_LOCAL 或 HTTP_DOWNLOAD 選項) 來部署。

為 Windows 端點上的 ThinApp 套件決定適當的部署模式

Windows 端點上的 VMware Identity Manager 桌面平台 應用程式組態會決定使用 VMware Identity Manager 發佈的 ThinApp 套件將會使用 ThinApp 串流模式、RUN_FROM_SHARE 還是其中一個 ThinApp 下載模式 (COPY_TO_LOCAL 或 HTTP_DOWNLOAD) 來部署。當您建立以無訊息方式將 VMware Identity Manager 桌面平台 應用程式安裝至 Windows 端點 (例如桌上型電腦和筆記型電腦) 的指令碼時，您會設定用來設定 ThinApp 套件部署模式的選項。請考量網路延遲性等細節，選擇所選端點的網路環境最適用的部署模式。

使用串流模式時，當 VMware Identity Manager 桌面平台 應用程式與 VMware Identity Manager 同步時，用戶端會為 ThinApp 套件的虛擬化 Windows 應用程式將應用程式捷徑下載至 Windows 桌面平台，且在使用者啟動 ThinApp 套件時，虛擬化 Windows 應用程式將會從 ThinApp 套件所在的檔案共用位置執行。

因此，串流模式適用於一律會連線到網路共用的系統，例如 View 桌面平台。

在下載模式下，第一次使用或更新 ThinApp 套件時，使用者必須先等候 ThinApp 套件下載至 Windows 系統，並建立捷徑。在首次下載後，使用者即可在本機 Windows 系統上啟動及執行虛擬化 Windows 應用程式。

重要事項 對於非持續性 View 桌面平台 (也稱為浮動或無狀態 View 桌面平台)，您應在安裝用戶端時使用命令列安裝程式選項 `/v INSTALL_MODE=RUN_FROM_SHARE` 將用戶端設定成使用 ThinApp 串流模式。RUN_FROM_SHARE 選項可提供在浮動 View 桌面平台中使用 ThinApp 套件的最佳執行階段體驗。請參閱 VMware Identity Manager 桌面平台的命令列安裝程式選項。

表格 5-1. 擷取為 ThinApp 套件之虛擬化應用程式的 ThinApp 部署模式

模式	說明
ThinApp 串流模式	在 ThinApp 串流模式中，虛擬化應用程式會在每次啟動時進行串流處理。此方法可避免使用桌面平台中要用來將虛擬化應用程式複製到桌面平台的磁碟空間。桌面平台必須連線到 ThinApp 套件的網路共用，應用程式才能執行。 下列環境可提供必要的一致性和穩定性： ■ 可穩定連線到 ThinApp 套件所在之檔案共用位置的 View 桌面平台 (無狀態或持續性)。 ■ 使用者具有不是 View 桌面平台、由多個使用者共用的 Windows 桌面平台。此狀態可避免在磁碟上累積下載的使用者特定應用程式，並可提供應用程式的快速存取，而不會導致使用者特定下載的延遲。 使用者用來登入 Windows 系統的帳戶，會用來從網路共用取得 ThinApp 套件。該帳戶在網路共用上必須具有適當的權限，以讀取及執行網路共用上的檔案。
ThinApp 下載模式	在 ThinApp 下載模式中，應用程式會下載至 Windows 端點。使用者會在端點上的本機位置執行虛擬化應用程式。在下列情況下，您可能會想要使用 ThinApp 下載模式： ■ 持續性 View 桌面平台 ■ 連接 LAN 但會定期離線的桌面平台 ■ 網路延遲性不佳的 LAN VMware Identity Manager 提供兩種形式的 ThinApp 下載模式：COPY_TO_LOCAL 和 HTTP_DOWNLOAD。如果為用戶端設定了 COPY_TO_LOCAL，則 Windows 端點必須加入至與檔案共用相同的網域，除非 AUTO_TRY_HTTP 選項已啟用，並且為 VMware Identity Manager 設定了 ThinApp 套件網路共用的帳戶型存取。 在 AUTO_TRY_HTTP 選項已啟用，並且為 VMware Identity Manager 設定了帳戶型存取時，如果 Windows 端點未加入至相同網域，且第一次嘗試下載 ThinApp 套件失敗，VMware Identity Manager 桌面平台 應用程式將會自動嘗試使用 HTTP 通訊協定來下載 ThinApp 套件，如同使用 HTTP_DOWNLOAD 模式。使用 HTTP_DOWNLOAD 時，Windows 端點無須加入至與檔案共用相同的網域。不過，在使用 HTTP_DOWNLOAD 時，複製和同步的所需時間將會遠高於使用 COPY_TO_LOCAL 時。 **重要事項** 如果 VMware Identity Manager 未啟用帳戶型存取，則無法使用 HTTP 通訊協定進行下載，即使 AUTO_TRY_HTTP 已啟用或用戶端已設定 HTTP_DOWNLOAD 選項亦然。 使用 COPY_TO_LOCAL 時，使用者用來登入 Windows 系統的帳戶，會用來從網路共用取得 ThinApp 套件。該帳戶在網路共用上必須具有適當的權限，以從網路共用讀取及複製檔案。使用 HTTP_DOWNLOAD 時，您在設定 VMware Identity Manager 對 ThinApp 套件網路共用的存取時在管理主控台中輸入的共用使用者帳戶，將是用來下載 ThinApp 套件的帳戶。該共用使用者帳戶在 ThinApp 套件的網路共用上必須具有讀取權限，以從網路共用複製檔案。

ThinApp 套件的網路共用必須符合您為 Windows 端點設定之部署模式的適當需求。請參閱 *《VMware Identity Manager 安裝與設定》*。

離線寬限期和 ThinApp 套件

離線寬限期是指允許在 Windows 系統啟動和執行虛擬化應用程式，且無須與 VMware Identity Manager 同步的一段期間。

ThinApp 套件是虛擬化的 Windows 應用程式，VMware Identity Manager 可將這些應用程式發佈到 Windows 系統。當 VMware Identity Manager 發佈 ThinApp 套件至使用者首次登入的 Windows 系統，套件的虛擬化應用程式會登錄至該 Windows 系統以供該使用者使用。系統會在 Windows 桌面平台上新增適當捷徑，使用者可以依照該系統上所安裝標準 Windows 應用程式的方法，使用該捷徑啟動虛擬化應用程式。

當使用者啟動其中一個由 VMware Identity Manager 部署至 Windows 系統的虛擬化應用程式，ThinApp 套件會要求從系統上執行之 ThinApp 代理程式執行的權限。ThinApp 代理程式會確認下列條件。

- 確認應用程式是否已為登入使用者在此 Windows 系統上進行登錄。
- 確認 Windows 系統是否已在允許的離線寬限期內與 VMware Identity Manager 同步。

如果符合上述兩個條件，ThinApp 代理程式就會允許虛擬化應用程式執行。

VMware Identity Manager 桌面平台應用程式與 VMware Identity Manager 同步的頻率由 POLLINGINTERVAL 安裝程式選項設定。依預設，頻率為每隔 5 分鐘進行同步。離線寬限期依預設會設定為 30 天。如果 Windows 系統在 30 天時間範圍內的任意時間具備可連線至 VMware Identity Manager 的網路連線，則應用程式可與 VMware Identity Manager 同步，且虛擬化應用程式可以執行。

但是，如果 Windows 系統不具備可連線至 VMware Identity Manager 的網路連線，應用程式就無法與 VMware Identity Manager 同步。該 Windows 系統上登錄的虛擬化應用程式可在離線系統上執行，直到離線寬限期設定的時間為止。

在 VMware Identity Manager 中部署後更新受管理的 ThinApp 套件

在將 ThinApp 套件新增至組織目錄並將該 ThinApp 套件授權給 VMware Identity Manager 使用者後，您的組織可能會想更新該套件，讓使用者使用更新或重建的 ThinApp 套件版本，而無須將使用者從目前套件解除授權然後再授權他們使用更新的套件。

當有 ThinApp 套件之 Windows 應用程式的更新版本發行時，或是該應用程式的製作者變更了套件所用參數值時，就可能會有更新的 ThinApp 套件版本可用。

ThinApp 4.7.2 和更新版本提供 VMware Identity Manager 中所用 ThinApp 套件的更新機制。此 ThinApp 更新機制不同於 VMware Identity Manager 環境外部所用 ThinApp 套件的其他更新機制。更新的 ThinApp 套件必須是使用此機制更新，您才能在 VMware Identity Manager 中部署更新後的套件而且讓使用者自動看到更新的版本。

對於在 VMware Identity Manager 中受管理的 ThinApp 套件，VMware Identity Manager 會使用兩個 Package.ini 參數來判斷某個套件是否為其他套件的更新版本。

AppID

VMware Identity Manager 中 ThinApp 套件的唯一識別碼。套件應用程式的所有進入點 (可執行檔) 都會獲指派相同的 AppID。ThinApp 套件與您組織的 VMware Identity Manager 目錄同步之後，套件的 `AppID` 會顯示在 ThinApp 套件資源頁面的 GUID 資料行中。此值由英數字元的字元組組成，每一組破折號之間以破折號分隔，例如以下範例所示：

```
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
```

	VMware Identity Manager 會將 AppID 相同的任何 ThinApp 套件視為相同應用程式的版本。
VersionID	ThinApp 套件的版本編號。VMware Identity Manager 使用 VersionID 來追蹤受管理 ThinApp 套件的不同版本。您可以將 VersionID 值增量一 (1) 來表示 ThinApp 套件是另一個套件的更新，並保持相同的 AppID。

請將更新後的套件放在為受管理 ThinApp 套件所設定之網路共用資料夾中的新資料夾。請參閱*《安裝及設定 VMware Identity Manager》*。當 VMware Identity Manager 對網路共用資料夾執行排程的同步，並遇到與另一個應用程式具有相同 AppID 的應用程式時，系統就會比較 VersionID 值。它會將 VersionID 值最高的 ThinApp 套件當做最新的更新。VMware Identity Manager 會自動將先前的使用者權利併入 VersionID 值最高的 ThinApp 套件，再同步使用者系統上的捷徑，使其指向更新的套件。

重要事項 標準 ThinApp InventoryName 參數對於成功的受管理 ThinApp 套件更新非常重要。舊的和更新的 ThinApp 套件都必須具有相同的 InventoryName 參數值。如果建立 ThinApp 套件的人在套件中變更了 InventoryName，之後建立更新套件，您需確認 InventoryName 值符合更新內容，才能在 VMware Identity Manager 中正確運作。

如需 ThinApp 套件之 Package.ini 檔案中所使用各種參數的詳細資料，請參閱*《ThinApp Package.ini 參數參考指南》*。

更新受管理的 ThinApp 套件

更新已受 VMware Identity Manager 管理的 ThinApp 套件，而您的組織目錄內包含多個步驟。更新的 ThinApp 套件可能由您組織中的其他群組提供。為確保 VMware Identity Manager 能自動使用更新的套件，以替代已授權使用者現有的套件，您必須確保更新的套件在建立時，也使用與目前套件相同的 AppID，並擁有比現有套件 VersionID 值還高的 VersionID 值，且能由 VMware Identity Manager 啟用管理。

先決條件

確認您擁有管理 ThinApp 套件所在位置的存取權，並能在那個位置建立子資料夾。

下一個

您的 VMware Identity Manager 目錄在下一個 ThinApp 套件同步後，會顯示新版本的更新 ThinApp 套件。如果您想要在 ThinApp 套件的資源頁面看到所反映的新版本，您可以使用管理主控台的 [封裝應用程式 - ThinApp] 頁面手動同步。

取得受管理之 ThinApp 套件的 AppID 和 VersionID 值

若要確保 VMware Identity Manager 會自動使用更新的 ThinApp 套件，而不會使用目前的套件，則必須使用目前受管理之 ThinApp 套件的 AppID 和高於目前版本的 VersionID 值來建立更新的 ThinApp 套件。

使用 Setup Capture 程序來建立更新的 ThinApp 套件時，Setup Capture 程式會從現有 ThinApp 套件的可執行檔中自動擷取 AppID 值，而 VersionID 值也會自動累加。不過，更新之 ThinApp 套件的建立者可使用不同的方法來建立更新的套件。未使用 Setup Capture 程序來建立更新的 ThinApp 套件時，套件建立者必須取得目前由 VMware Identity Manager 管理之 ThinApp 套件的 AppID 和 VersionID 值。AppID 和 VersionID 值會在管理主控台中顯示於 ThinApp 套件之資源頁面的頁面上。

程序

1. 按一下**目錄**索引標籤。
2. 按一下**任何應用程式類型 > ThinApp 套件**。
3. 按一下 ThinApp 套件，以開啟其資源頁面。
4. 按一下**詳細資料**。
5. 記下 [詳細資料] 頁面上的**版本**欄位所列的值。
6. 按一下 **ThinApp 套件**，以顯示 [ThinApp 套件] 頁面。
7. 記下 GUID 資料行所列的 AppID 值。

   GUID 資料行所列的值，即為 VMware Identity Manager 用來識別此 ThinApp 套件的值。

下一個

更新之 ThinApp 套件的建立者應完成建立更新的 ThinApp 套件中的步驟。

建立更新的 ThinApp 套件

目前受管理之 ThinApp 套件的 AppID 和 VersionID 值可用來建立更新的套件。更新的套件使用相同的 AppID 值和較高的 VersionID 值。

有時候，組織中的其他團隊會提供更新的 ThinApp 套件給您。建立更新之 ThinApp 套件的人員可使用下文描述的任一方法。

先決條件

完成取得受管理之 ThinApp 套件的 AppID 和 VersionID 值中的步驟，藉此確認目前的 ThinApp 套件具有 AppID 和 VersionID 值。

確認 ThinApp 程式的版本與 VMware Identity Manager 的版本相容。如需特定 ThinApp 版本的相關資訊，請參閱《*VMware 產品互通性對照表*》，網址為：http://www.vmware.com/resources/compatibility/sim/interop_matrix.php。

程序

- 使用 VMware Identity Manager 支援的 ThinApp 程式版本，以便使用任一可用方法來建立更新的 ThinApp 套件。

選項	說明
使用 Setup Capture 重新擷取	當 VMware Identity Manager 管理之現有 ThinApp 套件的專案資料夾無法使用時，請使用本方法。若要利用 Setup Capture 來建立更新的套件，您只需要以下項目： ■ 現有 ThinApp 套件的應用程式可執行檔 ■ 應用程式安裝程式 ■ VMware Identity Manager 支援的 Setup Capture 和 ThinApp 程式版本。 在擷取過程中，選取以 VMware Identity Manager 管理套件，且套件是現有基本 ThinApp 套件的更新。瀏覽至包含目前受管理之 ThinApp 套件可執行檔的資料夾。指向該資料夾，而非指向特定可執行檔。 利用這個方法，您不需在建立更新的套件之前取得 `AppID` 或 `VersionID` 值。在將套件指定為更新套件，並在 Setup Capture 中指向舊版本後，擷取程序會讀取舊版套件中的 `AppID`，再重複使用於更新的套件中。程序也會為更新之套件提供累加的 `VersionID`，以及指派相同的 `InventoryName`。
手動更新 Package.ini 檔案，然後重建套件。	當您沒有應用程式安裝程式可供重新擷取程序使用，或當您需要將套件更新為較新的 ThinApp 版本，且打算更新的內容超過 `relink` 命令的處理範圍時，請使用本方法。由於重建套件會併入新版本 ThinApp 既有之檔案系統和登錄的變更，因此重建作業會收集這些變更 (例如，當新版 ThinApp 提供您想要設定的新 Package.ini 參數時)。 若要將新套件標示為更新，請在 Package.ini 檔案的 `[Build Options]` 區段中編輯以下 VMware Identity Manager 參數： ■ 設定 `AppID` 參數的值，使其符合目前受管理之 ThinApp 應用程式的 `AppID` 值。您不能將 genid 的值重複用於 `AppID`，因為這樣系統就會為更新的套件產生新的 `AppID` 值，而 VMware Identity Manager 不會將新套件視為現有套件的更新。 ■ 將 `VersionID` 參數的值累加為高於目前受管理之 ThinApp 套件之值的整數。如果目前受管理之套件沒有已設定的 `VersionID` 參數，則該參數的值依預設為 1；您可以在 Package.ini 中為 `VersionID` 參數新增文字行，並將其值設定為 2 (`VersionID = 2`)。 ■ 確認 `InventoryName` 參數值符合目前受管理之套件的 `InventoryName` 值。目前之套件和更新之套件的 `InventoryName` 值必須相同。
使用 `relink –h` 命令搭配 AppID 和 VersionID 選項。	在下列情況中，您可以使用這個方法： ■ 您沒有應用程式的專案資料夾。 ■ 您已在 VMware Identity Manager 環境之外擷取、建置及測試套件，只剩下為 VMware Identity Manager 啟用更新的套件，以及將其放置在 VMware Identity Manager 使用之網路共用中的步驟。 ■ 您更新套件僅為更新套件的 ThinApp 執行階段，以併入新版 ThinApp 提供的錯誤修正。 例如，如果您已變更虛擬應用程式的專案目錄 (包括 Package.ini 檔案)、重建套件及測試套件，測試環境可能不是 VMware Identity Manager。更新應用程式的最後階段是為 VMware Identity Manager 啟用應用程式。此時，最簡單的途徑是使用 `relink –h` 命令，而不是重新擷取或重建。 **備註** 當您針對 ThinApp 套件執行 `relink –h` 命令時，ThinApp 執行階段一律會更新。

選項	說明
	您可以從 ThinApp Program Files 目錄執行重新連結命令，以便取得命令語法的說明。 當現有 ThinApp 套件已啟用以供 VMware Identity Manager 使用時，您可以執行下列命令來重複使用套件的現有 AppID 及累加 VersionID： `relink –h –VersionID + executable–folder/*.*` *executable-folder* 是含有要更新之 ThinApp 套件可執行檔的資料夾。 **重要事項** 在 VMware Identity Manager 中，當您使用 relink 命令時，無法將其直接指向 ThinApp 套件使用之網路共用中的套件可執行檔資料夾。該命令會在更新 ThinApp 執行階段時將舊有的可執行檔轉換成 BAK 檔案，再將這些 BAK 檔案和新檔案寫入資料夾。由於網路共用通常不允許寫入，因此您必須將重新連結指向可執行檔資料夾的複本。 如需 relink 命令的其他使用案例，包括啟用 ThinApp 套件以在 VMware Identity Manager 環境中使用，請參閱 VMware 知識庫文章：http://kb.vmware.com/kb/2021928。

您擁有一組用於更新之 ThinApp 套件的檔案 (EXE 檔案，也可選用 DAT 檔案)。

下一個

完成將更新的 ThinApp 套件複製到網路共用中的步驟，將檔案複製到網路共用中的新子資料夾。

將更新的 ThinApp 套件複製到網路共用

建立更新的 ThinApp 套件後，您需要將適當檔案複製到網路共用中與現有子資料夾相同階層的新子資料夾內。

先決條件

確認您已完成 建立更新的 ThinApp 套件 中的步驟並累加 VersionID 值，以備妥更新之 ThinApp 套件的檔案。

確認您擁有網路共用的存取權限，而且可以建立子資料夾及複製檔案到子資料夾內。

程序

1 在網路共用資料夾內，為更新的 ThinApp 套件建立新子資料夾。

保留欲更新之 ThinApp 套件的現有子資料夾，並且避免修改其內容。

在下一個排程的同步作業後，當 VMware Identity Manager 識別出新套件擁有相同的 AppID 值和較高的 VersionID 值時，會忽略舊有的套件。

一般來說，您會將子資料夾命名為符合 ThinApp 應用程式的名稱，或指出資料夾中包含的應用程式。例如，如果在名為 server 主機上的網路共用名為 *appshare*，並且應用程式稱為 *abceditor*，則 ThinApp 套件的子資料夾為 \\server\appshare\abceditor。

備註 使用 VMware Identity Manager 為要發佈的 ThinApp 套件建立您的網路共用子資料夾名稱時，請勿使用非 ASCII 字元。不支援非 ASCII 字元。

2 將更新之 ThinApp 套件的 EXE 和 DAT 檔案複製到新子資料夾。

3 (選擇性) 如果您不想要等到下一個排程的同步時間，可以使用 管理主控台 的 [封裝應用程式 - ThinApp] 頁面，以手動方式同步 VMware Identity Manager 與網路共用。

當 VMware Identity Manager 執行與網路共用資料夾之間的排程同步作業，並發現 `AppID` 值與另一個應用程式相同的應用程式時，它會比較 `VersionID` 值。它會將 `VersionID` 值最高的 ThinApp 套件當做最新的更新。VMware Identity Manager 會自動將先前的使用者權利併入 `VersionID` 值最高的 ThinApp 套件，再同步使用者系統上的捷徑，使其指向更新的套件。

從 VMware Identity Manager 刪除 ThinApp 套件

您可以從 VMware Identity Manager 永久移除 ThinApp 套件。

當您從 VMware Identity Manager 刪除 ThinApp 套件時，便會永久移除套件。除非您在 VMware Identity Manager 中再次新增 ThinApp 套件，否則無法再授權使用者使用該套件。

程序

1 針對連線至 VMware Identity Manager 的 ThinApp 套件存放庫，從網路檔案共用刪除 ThinApp 套件子資料夾。

2 從 VMware Identity Manager 刪除應用程式。

a 登入 管理主控台。

b 按一下**目錄**索引標籤。

c 按一下**任何應用程式類型 > ThinApp 套件**。

d 搜尋要刪除的 ThinApp 套件。

e 按一下 ThinApp 套件名稱以顯示其資源頁面。

f 按一下**刪除**並閱讀訊息，如果您同意，請按一下**是**。

ThinApp 套件將不再存在於 VMware Identity Manager 目錄中。

使現有的 ThinApp 套件與 VMware Identity Manager 相容

您可以將 ThinApp 套件從與 VMware Identity Manager 不相容的套件轉換為可由 VMware Identity Manager 散佈及管理的套件。您可以使用下列其中一種方法：使用 ThinApp 4.7.2 `relink` 命令、在編輯專案的 `Package.ini` 檔案以新增必要的 VMware Identity Manager 參數之後，從套件的 ThinApp 專案檔重新建置套件，或是重新擷取已在 ThinApp Setup Capture 程式中選取適當 VMware Identity Manager 設定的 Windows 應用程式。

備註 與 VMware Identity Manager 相容的 ThinApp 套件只能用於 VMware Identity Manager 部署。只有已安裝 VMware Identity Manager 桌面平台 應用程式的 VMware Identity Manager 使用者才可啟動及執行這些已啟用的套件。在執行階段，ThinApp 套件會載入具體指明的 DLL，並使用該 DLL 確認使用者對 VMware Identity Manager 的權利。由於 DLL 是隨著 VMware Identity Manager 桌面平台 應用程式而安裝的，因此這類 ThinApp 套件只能在已安裝 VMware Identity Manager 桌面平台 應用程式的 Windows 系統上執行。

先決條件

確認您可以存取您所選方法的必要項目。

- 如果您要使用 `relink` 命令，請確認您具有所要轉換之 ThinApp 套件的可執行檔，以及 ThinApp 4.7.2 `relink.exe` 應用程式。
- 如果您要更新 ThinApp 專案的 `Package.ini` 檔案並重新建置套件，請確認您具有 ThinApp 4.7.2 程式要重新建置套件所需的專案檔。
- 如果您要重新擷取 Windows 應用程式，請確認您具有 ThinApp 4.7.2 Setup Capture 程式和應用程式安裝程式，以及該程式要重新擷取應用程式所需的其他項目。如需詳細資訊，請參閱*《ThinApp 使用者指南》*。

確認您可以存取 VMware Identity Manager 所使用的 ThinApp 網路共用，而且可以對此網路共用來建立子資料夾及複製檔案。

程序

- 使用 VMware Identity Manager 支援的 ThinApp 程式版本，透過任一可用方法建立相容的 ThinApp 套件。

選項	說明
使用 `relink -h` 命令。	使用 `relink -h` 命令是最簡單的方法。您必須使用 ThinApp 4.7.2 或更新版本的 relink.exe 程式。在下列情況中，您可以使用這個方法： ■ 您無法使用重新建置方法，因為您沒有專案資料夾。 ■ 使用 Setup Capture 重新擷取應用程式太過費時。 ■ 您沒有使用 Setup Capture 進行重新擷取所需的應用程式安裝程式。 **備註** 當您針對 ThinApp 套件執行 `relink -h` 命令時，ThinApp 執行階段一律會更新。 您可以從 ThinApp Program Files 目錄執行重新連結命令，以便取得命令語法的說明。 若要建立相容的套件，請使用基本的命令語法： `relink -h executable-folder/*.*` 其中，*executable-folder* 是您要更新之 ThinApp 套件的可執行檔所在的資料夾。 **重要事項** 在 VMware Identity Manager 中，當您使用 `relink` 命令時，無法將其直接指向 ThinApp 套件使用之網路共用中的套件可執行檔資料夾。該命令會在更新 ThinApp 執行階段時將舊有的可執行檔轉換成 BAK 檔案，再將這些 BAK 檔案和新檔案寫入資料夾。由於網路共用通常不允許寫入，因此您必須將重新連結指向可執行檔資料夾的複本。 如需 `relink` 命令的其他使用案例，請參閱 http://kb.vmware.com/kb/2021928 上的 VMware 知識庫文章。

以必要的參數手動更新 Package.ini 檔案，然後重新建置套件。	當您沒有重新擷取程序的應用程式安裝程式時、當您不想執行重新擷取應用程式所需的前置設定時，或是當您想要從較新的 ThinApp 版本併入 `relink` 命令未能提供的功能時，請使用此方法。由於重建套件會併入新版本 ThinApp 既有之檔案系統和登錄的變更，因此重建作業會收集這些變更 (例如，當新版 ThinApp 提供您想要設定的新 Package.ini 參數時)。
	在 Package.ini 檔案的 `[Build Options]` 區段中，新增下列參數：
	`;--- VMware Identity Manager Parameters ---`
	`AppID=genid`
	`NotificationDLLs=hzntapluginlugin.dll`
	hzntaplugin.dll 是 ThinApp 執行階段所呼叫的 DLL，用來確認 VMware Identity Manager 使用者使用虛擬化應用程式的權利。
	您可以選擇性地加入 `HorizonOrgURL` 參數，並將其設為您的 VMware Identity Manager 完整網域名稱。請參閱 *《VMware Identity Manager 安裝與設定》*。

使用 Setup Capture 重新擷取，並選取必要的 VMware Identity Manager 設定。	在較適合重新擷取應用程式，而非使用其他方法時，請使用此方法。若要使用 ThinApp Setup Capture 建立相容的套件，請在精靈中選取適當的設定，以在擷取程序執行期間使用 VMware Identity Manager 來管理套件。如需擷取程序的詳細資訊，請參閱 *《ThinApp 使用者指南》*。

您已有可由 VMware Identity Manager 散佈及管理的 ThinApp 套件檔案集 (EXE 檔案和選用的 DAT 檔案)。

下一個

如需將 ThinApp 套件新增至網路共用的步驟，請參閱為 VMware Identity Manager 管理的 ThinApp 套件建立網路共用。

變更 ThinApp 套件共用資料夾

設定您 ThinApp 套件的 VMware Identity Manager 存取權之後，您的 IT 環境可能會變更，以致於您的 ThinApp 套件位在新的位置。發生此情況時，請在管理主控台中，將路徑更新為新位置。

先決條件

確認新網路共用位置遵守如 VMware Identity Manager 對 ThinApp 套件和網路共用存放庫的需求 中所述的網路共用需求。

程序

1. 登入 管理主控台。
2. 選取**目錄**索引標籤。
3. 按一下**管理桌面平台應用程式**，然後選取 **ThinApp 應用程式**。
4. 使用 UNC 路徑格式，將**路徑**文字方塊中的值變更為 ThinApp 套件所在的新共用資料夾。
5. (選擇性) 如果先前的網路共用為 CIFS 共用，而新共用為 DFS 共用，請選取**啟用帳戶型存取**核取方塊，並輸入對該網路共用具有讀取存取權的使用者的名稱和密碼。
6. 按一下**儲存**。

設定特定應用程式和桌面平台的存取原則

預設存取原則集會套用至您的目錄中的所有應用程式和桌面平台。您也可以設定個別應用程式或桌面平台集區的存取原則，這將會覆寫預設存取原則。

您可以從 [原則] 頁面將存取原則套用至一或多個應用程式和桌面平台，或從 [應用程式組態] 頁面中選取特定應用程式的存取原則。

如需存取原則的詳細資訊，請參閱《*VMware Identity Manager 管理指南*》。

程序

1. 若要從 [原則] 頁面將存取原則套用至應用程式和桌面平台，請遵循下列步驟。
   a. 導覽至 [身分識別與存取管理] > [管理] > [原則] 頁面。
   b. 按一下原則加以編輯，或按一下**新增原則**以建立新原則。
   c. 在原則頁面中，編輯或定義原則。
   d. 在**套用到**區段中，選取要套用原則的應用程式。
   e. 按一下**儲存**。

2 若要從 [應用程式組態] 頁面中選取特定應用程式的存取原則，請遵循下列步驟。

a 按一下**目錄**索引標籤。

b 按一下應用程式。

c 按一下左窗格中的**存取原則**。

d 選取應用程式的存取原則，然後按一下**儲存**。

設定 VMware Identity Manager 桌面平台

6

VMware Identity Manager 使用者必須先在他們的 Windows 系統上安裝及執行 VMware Identity Manager 桌面平台 應用程式，隨後才能執行以 VMware Identity Manager 註冊的 ThinApp 套件。

VMware Identity Manager 桌面平台 應用程式可透過按兩下安裝程式可執行檔並使用安裝精靈、使用命令列選項來執行可執行檔，或執行使用命令列選項的指令碼來進行安裝。安裝應用程式需要本機管理員權限。

在 Windows 端點上，VMware Identity Manager 桌面平台 應用程式的組態會決定透過 VMware Identity Manager 散佈的 ThinApp 套件要使用 ThinApp 串流模式、RUN_FROM_SHARE 或任一個 ThinApp 下載模式 (COPY_TO_LOCAL 或 HTTP_DOWNLOAD) 來部署。當您建立指令碼以利用無訊息方式將 VMware Identity Manager 桌面平台 安裝到 Windows 端點 (如桌上型和筆記型電腦) 時，需要配置用來設定 ThinApp 套件部署模式的選項。請選擇最適合選定端點之網路環境的部署模式，並將網路延遲之類的詳細資料納入考量。

備註 VMware Identity Manager 桌面平台 應用程式安裝期間如果有任何開啟的瀏覽器視窗，可能會導致從使用者入口網站啟動 ThinApp 套件時發生問題。請在安裝應用程式之前關閉所有瀏覽器視窗，或在安裝應用程式之後立即重新啟動瀏覽器。請參閱 無法從使用者入口網站啟動 ThinApp 套件。

本章節討論下列主題:

VMware Identity Manager 桌面平台的命令列安裝程式選項

使用命令列或部署指令碼執行其安裝程式時，您可以為 VMware Identity Manager 桌面平台 應用程式設定各種選項。

VMware Identity Manager 桌面平台 安裝程式的可用命令列選項

將用戶端應用程式的安裝程式 .exe 檔案下載至 Windows 系統之後，您可以透過執行下列命令來查看安裝選項的清單：

```
VMware-Identity-Manager-Desktop-n.n.n-nnnnnnn /?
```

其中，*n.n.n-nnnnnnn* 代表檔案的版本和組建編號。對話方塊隨即顯示，列出使用命令列或部署指令碼來安裝用戶端應用程式的可用安裝選項。

表格 6-1. 安裝程式命令列選項

安裝程式選項	值	說明
/?		顯示安裝程式命令列選項。
/a		執行管理模式安裝。 如需詳細資訊，請參閱 Windows Installer 說明文件。
/a	*現有管理模式安裝的完整路徑*	修補現有管理模式安裝。
/s		安裝期間隱藏初始化對話方塊。 若要以無訊息模式安裝，請使用 `/s /v/qn`。 在無訊息模式中，安裝期間不會出現訊息、對話方塊或提示。您通常會在建立部署指令碼時使用此選項來執行安裝程式。
/v	*金鑰值組*	傳遞至安裝程式的一組參數，以金鑰值組形式指定。使用格式 `key=value`。這些引數可設定一般 ThinApp 套件和 VMware Identity Manager 桌面平台的執行階段選項。
/c		清除安裝登錄資訊。
/l	[*記錄檔的完整路徑*]	執行詳細記錄並儲存至指定的記錄檔。 如果不指定記錄檔，則會使用預設的登入 %TEMP%。
/x		解壓縮安裝程式至 %TEMP% 資料夾。

/v 選項的金鑰值組

您可以對 /v 安裝程式選項使用下列金鑰值組。

表格 6-2. /v 安裝程式命令列選項的機碼

機碼	值	說明

WORKSPACE_SERVER	*VMware Identity Manager 服務的主機名稱或 URL*	提供 VMware Identity Manager 服務主機名稱或 URL，以允許 VMware Identity Manager 桌面平台 應用程式與服務通訊。HTTPS 是必要的通訊協定。將值含括在引號內。
		使用以下格式：
		`WORKSPACE_SERVER="https://VMwareIdentityManagerFQDN"`
		或
		`WORKSPACE_SERVER="VMwareIdentityManagerHostName"`
		例如：
		`WORKSPACE_SERVER="https://myserver.mycompany.com"`
		`WORKSPACE_SERVER="myserver"`

INSTALL_MODE	下列之一：
	`COPY_TO_LOCAL`
	`HTTP_DOWNLOAD`
	`RUN_FROM_SHARE`
		針對 VMware Identity Manager 桌面平台 應用程式如何在執行階段取得 ThinApp 套件設定部署模式。ThinApp 套件為虛擬化的 Windows 應用程式。ThinApp 套件位於與 VMware Identity Manager 整合的網路共用上。
		■ COPY_TO_LOCAL：使用者的獲授權套件會使用檔案複製下載至用戶端 Windows 系統。使用者啟動 ThinApp 套件時，虛擬化應用程式會在該本機系統上執行。在使用者第一次下載和使用獲授權的 ThinApp 套件之前，若要繼續同步套件至用戶端 Windows 系統，用戶端 Windows 系統必須加入 ThinApp 套件之網路共用所加入的相同 Active Directory 網域。用來登入 Windows 系統的使用者帳戶，即為用來從網路共用取得 ThinApp 套件的帳戶。該帳戶必須具有網路共用上的適當權限，才能從網路共用讀取和複製檔案。
		■ HTTP_DOWNLOAD：使用者的獲授權套件會使用 HTTP 通訊協定下載至用戶端 Windows 系統。使用者啟動 ThinApp 套件時，虛擬化應用程式會在該本機系統上執行。VMware Identity Manager 桌面平台 應用程式會使用使用者的 VMware Identity Manager 系統帳戶來向 VMware Identity Manager 驗證，以取得使用者獲授權的套件清單以進行下載。管理主控台 中所提供針對 ThinApp 套件的網路共用啟用帳戶型存取的共用使用者帳戶，即為 VMware Identity Manager 用來從存放庫存取 ThinApp 套件的帳戶。VMware Identity Manager 的該共用使用者帳戶需要網路共用上的讀取權限。使用者用來登入用戶端 Windows 系統的帳戶，以及使用者的 VMware Identity Manager 系統帳戶不需要具備網路共用上的任何權限。用戶端 Windows 系統不需加入 ThinApp 套件的網路共用所加入的相同網域。此下載方法通常比使用其他模式更為緩慢。此模式的優點是用戶端 Windows 系統不需加入 Active Directory 網域來取得和執行虛擬化應用程式。
		重要事項 為了讓 HTTP_DOWNLOAD 選項運作，VMware Identity Manager 中的 ThinApp 套件整合必須針對帳戶型存取進行設定。請參閱 *《VMware Identity Manager 安裝與設定》*。
		重要事項 在 Windows 2008 R2 或 Windows 7 上使用 VMware Identity Manager 2.6 和更新版本時，HTTP_DOWNLOAD 選項將無法運作，除非您在 VMware Identity Manager 中啟用 TLS 1.0，或在 Windows 2008 R2 或 Windows 7 系統中啟用 TLS 1.1 或 1.2。若要在 VMware Identity Manager 中啟用 TLS 1.0，請參閱知識庫文章 2144805。若要在 Windows 系統上啟用 TLS 1.1 或 1.2，請參閱 https://support.microsoft.com/en-us/kb/3140245 中的 Microsoft 說明文件。
		■ RUN_FROM_SHARE：虛擬化應用程式會在使用者啟動 ThinApp 套件時，從網路共用串流到用戶端 Windows 系統。RUN_FROM_SHARE 選項最適合的情況為 ThinApp 套件位於隨時可連線至網路共用的 Windows 系統，因為 ThinApp 套件不在 Windows 系統上，並且虛擬化應用程式只會在 Windows 系

表格 6-2. /v 安裝程式命令列選項的機碼 (繼續)

機碼	值	說明
		統可以連線至網路共用時執行。用戶端 Windows 系統必須加入 ThinApp 套件的網路共用所加入的相同 Active Directory 網域。用來登入 Windows 系統的使用者帳戶，即為用來從網路共用取得 ThinApp 套件的帳戶。該帳戶在網路共用上必須具有適當的權限，以讀取及執行網路共用上的檔案。 預設值為 COPY_TO_LOCAL。 針對所有模式，網路共用必須設定適當的檔案和共用權限。請參閱 *《VMware Identity Manager 安裝與設定》*。 **重要事項** 在浮動 View 桌面平台中安裝 VMware Identity Manager 桌面平台 時，請使用 RUN_FROM_SHARE 選項以避免複製 ThinApp 套件到那些無狀態 View 桌面平台系統。 使用其中一個組態安裝 VMware Identity Manager 桌面平台 應用程式時，登入 Windows 系統的使用者帳戶必須具有網路共用上的適當檔案和共用權限，才能夠取得 ThinApp 套件： ■ RUN_FROM_SHARE 選項 ■ COPY_TO_LOCAL 選項，也未啟用 AUTO_TRY_HTTP 選項，並且在 VMware Identity Manager 中設定帳戶型存取
POLLING_INTERVAL	*頻率 (以秒為單位)*	設定在安裝的 VMware Identity Manager 桌面平台 應用程式和 VMware Identity Manager 之間同步化的頻率 (以秒為單位)，以檢查是否有新的 ThinApp 套件或權利。如果未指定，則會套用 300 秒 (5 分鐘) 的預設值。 例如： `POLLING_INTERVAL=600`
ENABLE_AUTOUPDATE	0 或 1	啟用或停用自動更新檢查和下載活動。如果已啟用，安裝的 VMware Identity Manager 桌面平台 應用程式會自動檢查是否有更新的應用程式可供下載。如果有更新版本可供使用，VMware Identity Manager 桌面平台 應用程式會自動下載並自行更新為更新版本。此選項依預設為啟用。 將此變數的值設定為 0 可停用自動更新。如果未指定，則會套用 1 的預設值。 自動更新的安裝需要管理員權限。
SHARED_CACHE	0 或 1	判斷 ThinApp 套件快取是否位於要安裝用戶端應用程式的 Windows 系統的通用資料夾。將此變數的值設定為 1，可指定 Windows 系統上的所有使用者帳戶共用一個通用快取位置。依預設，通用的資料夾為 `%ProgramData%\VMware\Identity Manager Desktop\thinapp`。 如果未指定，則會套用預設值 0，並且每個 Windows 使用者帳戶可擁有自己的快取，而其預設位置為 `%LOCALAPPDATA%\VMware\Identity Manager Desktop\thinapp`。 **備註** 如果您指定共用快取，則 VMware Identity Manager 桌面平台 應用程式不會從此共用快取自動刪除 ThinApp 套件。因為 SHARED_CACHE=1 表示 Windows 系統上的所有使用者帳戶會共用相同的位置，而套件必須保持在共用位置，讓獲授權的使用者可以使用它們，即使您取消授權一個使用者也是如此。從 ThinApp 套件取消授權使用者時，VMware Identity Manager 桌面平台 應用程式會為該使用者取消登錄該套件。該 Windows 系統上其他獲授權的使用者可以繼續使用 ThinApp 套件。如果該 Windows 系統上沒有使用者帳戶獲授權可使用 ThinApp 套件，您可以手動刪除通用快取以回收空間。在快取位置下，每個 ThinApp 套件都有自己的資料夾。

表格 6-2. /v 安裝程式命令列選項的機碼 (繼續)

機碼	值	說明
CACHE_DIR	*資料夾的路徑*	設定如果使用 HTTP_DOWNLOAD 或 COPY_TO_LOCAL 安裝模式，將在本機快取 ThinApp 套件的位置。此值會針對每個系統 (非每個使用者) 而設定，因此您必須使用環境變數 (例如 %LOCALAPPDATA%) 來選取使用者的特定位置。務必在命令列逸出 % 字元，以避免立即展開。例如： `CACHE_DIR=^%LOCALAPPDATA^%\cache`
AUTO_TRY_HTTP	0 或 1	使用 COPY_TO_LOCAL 選項安裝 VMware Identity Manager 桌面平台 應用程式，並且針對 VMware Identity Manager 設定帳戶型存取時，如果第一個下載嘗試失敗，AUTO_TRY_HTTP 選項會判斷用戶端是否應該使用 HTTP 通訊協定自動嘗試下載使用者獲授權的 ThinApp 套件，類似於 HTTP_DOWNLOAD 選項。此選項依預設為啟用。將此選項的值設定為 0 可停用自動嘗試 HTTP 通訊協定進行下載。 **重要事項** 為了讓 AUTO_TRY_HTTP 選項運作，VMware Identity Manager 中的 ThinApp 套件整合必須針對帳戶型存取進行設定。請參閱 VMware Identity Manager 對 ThinApp 套件和網路共用存放庫的需求。
INSTALL_MODULES	`thinapp`	用來指定要安裝模組的逗號分隔清單。目前，只有 `thinapp` 模組可供使用。

MIGRATE_ACTION	下列之一：
	`MOVE`
	`COPY`
	`NONE`
		如果已安裝舊版 Workspace for Windows 應用程式，安裝程式會從舊版應用程式將資料和設定移轉至新應用程式。預設值為 `MOVE`。
		視您指定的值而定，系統會移動、複製或忽略下列設定。
		快取的 ThinApp 套件
		下載的 ThinApp 套件將從 Workspace for Windows 快取 `%LOCALAPPDATA%\VMware\Horizon ThinApp\PackageCache` 複製到新快取位置 `%LOCALAPPDATA%\VMware\Identity Manager Desktop\thinapp`。將變更快取資料夾內的資料夾名稱。
		重要事項 安裝期間針對 VMware Identity Manager 所設定的內容，比針對那些內容所移轉的值具有優先權。例如，如果 Workspace for Windows 中的 INSTALL_MODE 設為 COPY_TO_LOCAL，並且在安裝 Identity Manager 桌面平台時您指定 `/v INSTALL_MODE=HTTP_DOWNLOAD`，則 INSTALL_MODE 會設為 HTTP_DOWNLOAD。

範例 6-1. 使用 VMware Identity Manager 桌面平台 命令列安裝程式選項

如果您的 VMware Identity Manager 執行個體具有 https://*identitymanagerFQDN* 的 URL，並且 VMware Identity Manager 已針對帳戶型存取您的 ThinApp 套件的網路共用而設定，而您想要使用這些選項以無訊息方式安裝 VMware Identity Manager 桌面平台 應用程式至該 VMware Identity Manager 執行個體的多個桌面平台：

- ThinApp 安裝選項設為 HTTP_DOWNLOAD，因為您預期這些 Windows 系統將不會加入網域。VMware Identity Manager 已適當地針對 ThinApp 套件網路共用的帳戶型存取進行設定。
- 用戶端會每隔 60 秒使用 VMware Identity Manager 檢查是否有新套件和權利。

您將建立叫用下列命令的指令碼：

```
VMware-Identity-Manager-Desktop-n.n.n-nnnnnnn.exe /s
   /v/qn WORKSPACE_SERVER="https://identitymanagerFQDN" INSTALL_MODE=HTTP_DOWNLOAD POLLING_INTERVAL=60
```

其中，您會將檔案名稱的 *n.n.n-nnnnnnn* 部分取代為符合您下載的 VMware Identity Manager 桌面平台 安裝程式的名稱。

將具有相同設定的 VMware Identity Manager 桌面平台 應用程式安裝至多個 Windows 系統

若要將 VMware Identity Manager 桌面平台 應用程式部署至多個 Windows 系統，並將相同的組態設定套用至這些系統，您可以使用命令列安裝選項，實作會安裝 VMware Identity Manager 桌面平台 應用程式的指令碼。

重要事項 以無訊息方式部署 VMware Identity Manager 桌面平台 時，將不會在畫面上顯示錯誤訊息。若要在無訊息安裝期間查看錯誤，請監控 `%TEMP%` 資料夾，檢查其中是否有新的 `vminst.XXXXXX.log` 檔案。失敗的無訊息安裝的錯誤訊息會出現在這些檔案中。

一般而言，此部署案例會用在屬於 View 桌面平台的 Windows 系統上。如需用於非持續性 (也稱為浮動或無狀態) View 桌面平台之設定的說明，請參閱 在非持續性 View 桌面平台中減少資源使用並增加 VMware Identity Manager 桌面平台的效能。

先決條件

- 確認 Windows 系統所執行的 Windows 作業系統支援您所安裝的 VMware Identity Manager 桌面平台 應用程式版本。請參閱《*VMware Identity Manager 使用者指南*》或版本說明。
- 確認 Windows 系統已安裝受支援的瀏覽器。
- 如果您在建立部署指令碼之前需要執行命令以熟悉可用選項的功能，請確認您具有可用來執行該命令的 Windows 系統。列出選項的命令只能在 Windows 系統上使用。請參閱 VMware Identity Manager 桌面平台的命令列安裝程式選項。

程序

1. 取得 VMware Identity Manager 桌面平台 安裝程式的可執行檔，並在您要在其中以無訊息方式執行安裝程式的系統上找出該可執行檔。

   取得此可執行檔的方法之一，是使用 VMware Identity Manager 系統的下載頁面加以下載。如果您已將 VMware Identity Manager 系統設定成從下載頁面提供 Windows 應用程式安裝程式，則可藉由在瀏覽器中開啟下載頁面的 URL 來下載可執行檔。

2 使用安裝程式的命令列選項，建立符合您的組織需求的部署指令碼。

舉例來說，您可以使用的指令碼包括 Active Directory 群組原則指令碼、登入指令碼、VB 指令碼、批次檔、SCCM 等等。

例如，如果您的 VMware Identity Manager 執行個體的 URL 為 https://*identitymanagerFQDN*，而您想要將 ThinApp 部署模式設定為下載模式，並且讓 VMware Identity Manager 桌面平台 應用程式每 60 秒與伺服器同步一次，而以無訊息方式將 Windows 用戶端安裝至您預期會在網域以外使用的 Windows 系統，則您應建立會呼叫下列命令的指令碼：

```
VMware-Identity-Manager-Desktop-n.n.n-nnnnnnn.exe /s
/v /qn WORKSPACE_SERVER="https://identitymanagerFQDN" INSTALL_MODE=HTTP_DOWNLOAD
POLLING_INTERVAL=60
```

其中，您應取代檔案名稱的 *n.n.n-nnnnnnn* 部分，使其符合您已下載之檔案的名稱。

3 對 Windows 系統執行部署指令碼。

如果無訊息安裝成功，VMware Identity Manager 桌面平台 應用程式即會部署至 Windows 系統。登入這些 Windows 系統的使用者，可以從這些系統存取其授權資產。

備註 使用者的授權 ThinApp 套件會進行串流處理或下載，然後在輪詢間隔經過之後快取至使用者的 Windows 系統。因此，使用者在登入 VMware Identity Manager 使用者入口網站時，可能會看見其中顯示了 ThinApp 套件。在用戶端於下一個輪詢間隔同步應用程式之前，ThinApp 套件將不會啟動。

下一個

試著執行某些一般使用者工作，確認 VMware Identity Manager 桌面平台 已正確安裝在 Windows 系統上。

將 VMware Identity Manager 桌面平台安裝程式檔案新增至 VMware Identity Manager 虛擬應用裝置

發行新版本的 VMware Identity Manager 桌面平台時，您會從 VMware Downloads 頁面複製和安裝 zip 檔案至您部署中的每個 VMware Identity Manager 虛擬應用裝置。您會執行 `check-client-updates.pl` 命令來部署安裝程式檔案，並重新啟動每個虛擬應用裝置上的 Tomcat 服務。

先決條件

- 使用者必須具有其電腦上的管理員權限，才能安裝和自動更新 VMware Identity Manager 桌面平台應用程式。如果使用者沒有管理員權限，您可以使用軟體發佈工具來發佈和更新應用程式給您的使用者。
- 排程會在維護時段期間將這些安裝程式檔案新增至 VMware Identity Manager 虛擬應用裝置，因為虛擬應用裝置會重新啟動，並且這可能會中斷使用者存取。

程序

1 從 My VMware Downloads 頁面下載 VMware Identity Manager 桌面平台 zip 檔案到可存取 VMware Identity Manager 虛擬應用裝置的電腦。

2 將 zip 檔案複製到虛擬應用裝置中的暫存位置。例如：

```
scp filen.n.n-nnnnnnn.zip root@identitymanager-va.com:/tmp/
```

3 以根使用者身分登入虛擬應用裝置。

4 解壓縮和安裝新 zip 檔案到下載目錄。

```
/usr/local/horizon/scripts/check-client-updates.pl --install --clientfile /tmp/file.n.n.n-nnnnn.zip
```

此指令碼會自動解壓縮該檔案，並將 Windows 電腦適用的 VMware Identity Manager 桌面平台安裝程式檔案複製到 `/opt/vmware/horizon/workspace/webapps/ROOT/client` 目錄。它會自動更新到 `/opt/vmware/horizon/workspace/webapps/ROOT/client/cds` 目錄，並更新下載連結的 URL 參數值。

5 重新啟動虛擬應用裝置上的 Tomcat 服務。

6 針對您環境中的每個 VMware Identity Manager 虛擬應用裝置重複這些步驟。

使用者可以透過其 VMware Identity Manager 帳戶或透過下載連結 (https://*IdentityManagerFQDN*/download) 下載 Identity Manager 桌面平台應用程式。使用者的 Identity Manager 桌面平台應用程式會在使用者下載新版本時自動更新。

使用命令列 hws-desktop-ctrl.exe 應用程式

VMware Identity Manager 桌面平台 應用程式包含命令列應用程式 hws-desktop-ctrl.exe，可供您用來在使用者的 Windows 系統上執行與使用 ThinApp 套件相關的作業。

VMware Identity Manager 桌面平台 應用程式的安裝程序會在安裝 VMware Identity Manager 桌面平台 應用程式所在之 Windows 目錄位置中的 `HorizonThinApp` 資料夾中安裝 hws-desktop-ctrl.exe。

若要使用 hws-desktop-ctrl.exe 應用程式來執行其支援的其中一個命令，請使用下列格式。

```
hws-desktop-ctrl.exe command options
```

命令	說明
`hws-desktop-ctrl.exe recheck`	此命令會立即針對與登入 VMware Identity Manager 桌面平台 應用程式之使用者帳戶相關聯的 ThinApp 套件執行權利檢查。系統會同步任何新授權或更新的 ThinApp 套件。
`hws-desktop-ctrl.exe set InstallMode=install_mode`	此命令會變更用於此 Windows 系統上 ThinApp 套件的 ThinApp 部署模式。因為此命令會變更與 ThinApp 部署模式相關聯的登錄機碼，只有具備適當登錄權限的管理員可以使用此命令變更安裝模式。 *install_mode* 可用的值為： ■ `CopyToLocal` ■ `RunFromShare` ■ `HttpDownload`

命令	說明
`hws-desktop-ctrl.exe authorize guid=`*`ThinApp_GUID`* `path=`*`package_path`*	此命令會驗證是否可以啟動 ThinApp 套件。此命令不會實際啟動 ThinApp 套件。提供 ThinApp 套件的 GUID 和套件的可執行檔路徑。如果對 Windows 用戶端系統上的套件使用 ThinApp 下載模式，則路徑相對於本機快取根資料夾，即為相對於存放庫根路徑的路徑。範例為 `hws-desktop-ctrl.exe authorize guid= 436E1D7D-552C-4F70-8197-DB1B05D30394 path="FileZilla Client 3.3.2/FileZilla.exe"` 您可以在 管理主控台 中的資源頁面上查看 ThinApp 套件的 GUID、應用程式路徑，以及可執行檔名稱。
`hws-desktop-ctrl.exe quit`	此命令會讓 VMware Identity Manager 桌面平台 應用程式完全結束。
`hws-desktop-ctrl.exe launch app=`*`package_path`* `url=`*`launch_url`*	此命令是用來手動啟動 ThinApp 套件，其中，*package_path* 為套件的可執行檔路徑，而 *launch_url* 為該套用的 VMware Identity Manager 通訊協定 URL，格式為 `horizon://package_path`。範例為 `hws-desktop-ctrl.exe launch app="FileZilla Client 3.3.2/FileZilla.exe" url="horizon://FileZilla Client 3.3.2/FileZilla.exe"` 使用者通常不會使用此命令，他們可以從 Workspace ONE 入口網站中啟動其獲授權的 ThinApp 套件。此命令通常用於偵錯。

提供存取 Citrix 發佈的資源

7

您可以整合 Citrix 部署與 VMware Identity Manager，讓 Workspace ONE 使用者存取 Citrix 發佈的資源。

本章節討論下列主題:

概觀

您可以透過整合 Citrix 部署與 VMware Identity Manager，讓 Workspace ONE 使用者能夠存取 Citrix 發佈的資源。Citrix 發佈的資源包含 Citrix XenApp 和 XenDesktop 伺服器陣列內的應用程式和桌面平台。桌面平台也稱為 Citrix 發佈的傳遞群組。

使用者可從 Workspace ONE 入口網站或應用程式啟動 Citrix 發佈的應用程式和桌面平台。他們必須在其系統和裝置上安裝 Citrix Receiver 才能存取他們有權使用的資源。

您可以在 Citrix 中管理 Citrix 發佈的應用程式和桌面平台，以及授與使用者對這些資源的權利。在 VMware Identity Manager 管理主控台中，您可以檢視資源及其權利。

您也可以從 VMware Identity Manager 編輯 ICA 工作階段設定，例如控制解析度或壓縮的設定。您可以為 VMware Identity Manager 目錄中的所有 Citrix 資源或為個別 Citrix 資源全域進行設定。

VMware Identity Manager 支援包含 Citrix Netscaler 的 Citrix 部署。

支援的版本

- VMware Identity Manager 支援 XenApp 5.0、6.0、6.5 和 7.x 以及 XenDesktop 7.x。
- Integration Broker 是可與 Citrix 部署通訊的 VMware Identity Manager 元件，其支援的作業系統為 Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2。

- 若要使用 Citrix StoreFront ReST API，則需要 Integration Broker 2.9.1 或更新版本。
- 若要使用 XenApp 7.x 或 XenDesktop 7.x，則需要 Integration Broker 2.6 或更新版本。
- 若要使用 Netscaler 功能，則需要 Integration Broker 2.4 或更新版本。

備註　建議使用 VMware Identity Manager 及其元件的最新可用版本。

Citrix 整合所需的元件

若要整合 Citrix 部署與 VMware Identity Manager 服務，您將需要下列元件。

- 以內部部署方式安裝的 VMware Identity Manager 執行個體。
- 以內部部署方式安裝在支援之 Windows 伺服器上的 Integration Broker 執行個體。Integration Broker 是 VMware Identity Manager 的元件之一，也是負責與 Citrix 伺服器陣列通訊的元件。

  您可以從 https://my.vmware.com 下載 Integration Broker。
- 內部部署的 Citrix 部署。

在部署元件時，請確定您符合下列需求：

- VMware Identity Manager 服務必須能夠與 Integration Broker 通訊。如果您部署多個服務應用裝置執行個體，請確定這些執行個體全都可與 Integration Broker 通訊。
- Integration Broker 必須能夠與 Citrix 伺服器陣列通訊。

備註　建議使用 VMware Identity Manager 及其元件的最新可用版本。

高階整合設計

VMware Identity Manager 會使用 Integration Broker 和其他元件將 Citrix 發佈的資源同步至 VMware Identity Manager，以及從 Workspace ONE 入口網站或應用程式啟動資源。

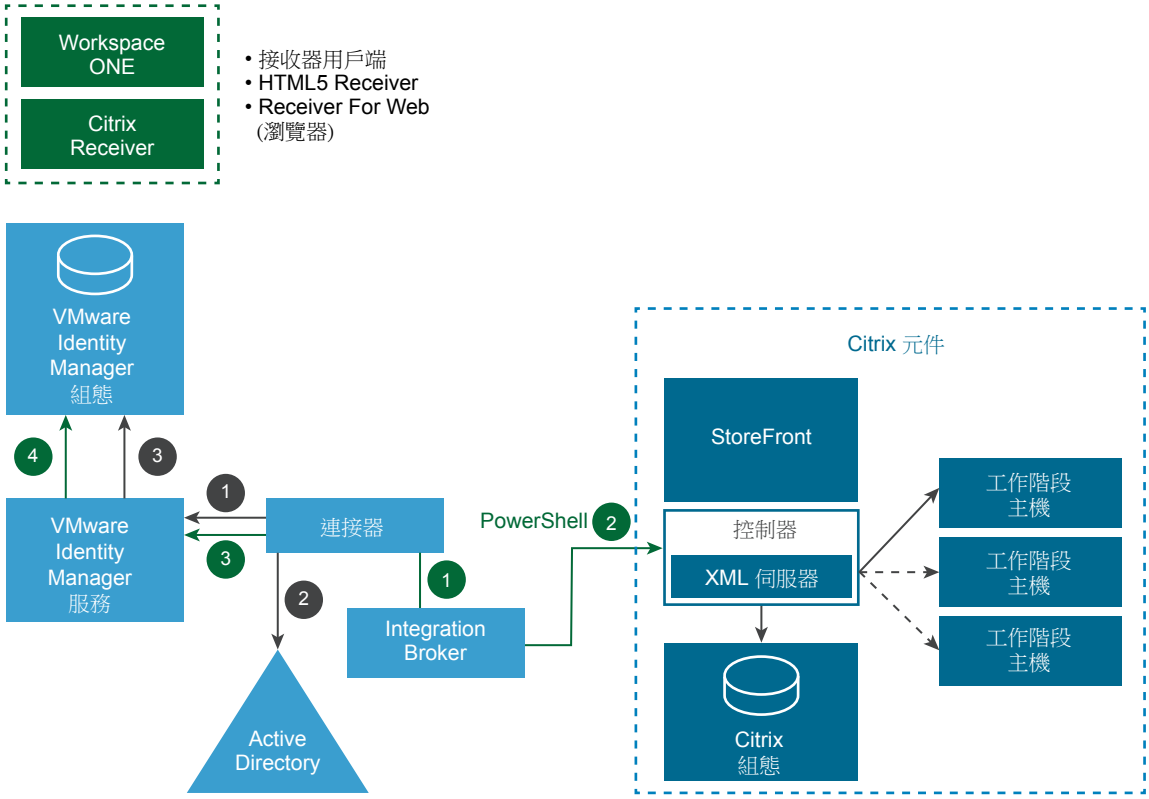
Citrix 發佈的資源和權利的同步化

VMware Identity Manager 會將 Citrix 發佈的應用程式和桌面平台以及使用者權利從 Citrix 伺服器陣列同步化至 VMware Identity Manager 服務。您可以設定同步排程以定期同步資源和權利。

Citrix 伺服器陣列是 VMware Identity Manager 中所有受支援作業的單一事實來源。您可以在 Citrix 中管理資源，以及授與使用者對這些資源的權利。

在 Citrix 伺服器陣列中新增、變更或刪除資源或權利時，相關資訊將會在同步之後更新於 VMware Identity Manager 中。

同步化架構圖

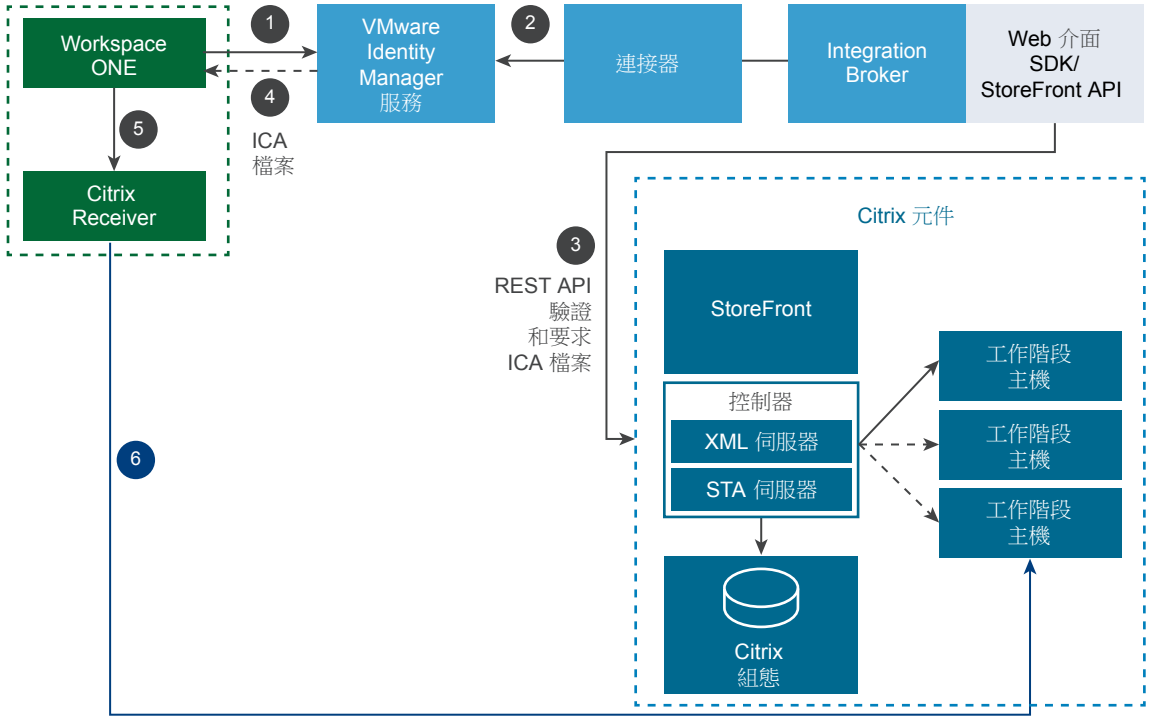


- VMware Identity Manager Connector 會將使用者和群組從您的企業目錄同步至 VMware Identity Manager 服務。
- Citrix 發佈的資源和權利會使用連接器、Integration Broker 和 PowerShell SDK 從 Citrix 伺服器陣列同步至 VMware Identity Manager。

啟動 Citrix 發佈的應用程式和桌面平台

VMware Identity Manager 會使用 Integration Broker 元件和 Citrix Web Interface SDK 或 Citrix StoreFront REST API，從 Workspace ONE 入口網站或應用程式啟動 Citrix 發佈的應用程式。您可以設定 Citrix 發佈之資源的內部和外部存取。使用者必須在其系統或裝置上安裝 Citrix Receiver，才能啟動應用程式和桌面平台。

啟動架構圖 (內部存取)



1 使用者從 Workspace ONE 入口網站或應用程式啟動 Citrix 發佈的應用程式或桌面平台。

2 要求會傳送至 VMware Identity Manager 服務、連接器和 Integration Broker。

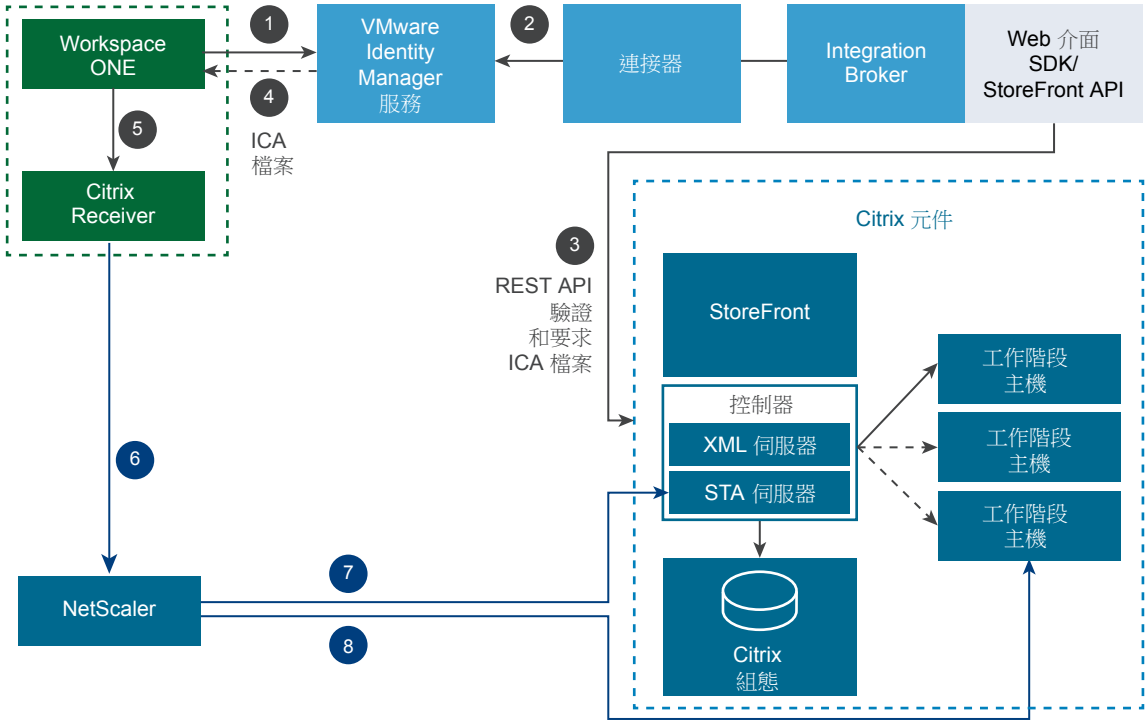
3 Integration Broker 會透過 Web Interface SDK 或 StoreFront REST API 與 Citrix 伺服器陣列通訊，以驗證和要求 ICA 檔案。

4 ICA 檔案會在擷取後傳遞至 Workspace ONE 入口網站或應用程式。

5 ICA 檔案會傳遞至 Citrix Receiver。

6 Citrix Receiver 會啟動應用程式或桌面平台。

啟動架構圖 (外部存取)



1 使用者從 Workspace ONE 入口網站或應用程式啟動 Citrix 發佈的應用程式或桌面平台。

2 要求會傳送至 VMware Identity Manager 服務、連接器和 Integration Broker。

3 Integration Broker 會透過 Web Interface SDK 或 StoreFront REST API 與 Citrix 伺服器陣列通訊，以驗證和要求 ICA 檔案。

4 ICA 檔案會在擷取後傳遞至 Workspace ONE 入口網站或應用程式。

5 ICA 檔案會傳遞至 Citrix Receiver。

6 Citrix Receiver 會與 Netscaler 通訊。

7 NetScaler 會透過 STA 票證與 Citrix STA 伺服器通訊，並取得 Citrix 工作階段伺服器資訊。

8 NetScaler 會與 Citrix 工作階段主機伺服器通訊，並建立應用程式啟動的工作階段。

> **備註** 在 7.x 版中，Citrix 工作階段主機伺服器為 Citrix VDA 伺服器。在 6.5 版中，則為 Citrix Worker 伺服器。

使用 StoreFront REST API 或 Web Interface SDK 進行啟動

Integration Broker 可以使用 Citrix Web Interface SDK 和 Citrix StoreFront REST API 與 Citrix 部署通訊，以啟動應用程式或桌面平台。使用 StoreFront REST API 時，Integration Broker 的行為會類似於 REST 用戶端。Web Interface SDK 和 StoreFront REST API 可用來從 Citrix 部署產生 ICA 檔案，並使用該檔案進行驗證。

您可以藉由在 VMware Identity Manager 管理主控台的 Citrix 組態頁面中選取或取消選取 [使用 StoreFront] 核取方塊，以指定所要使用的選項。

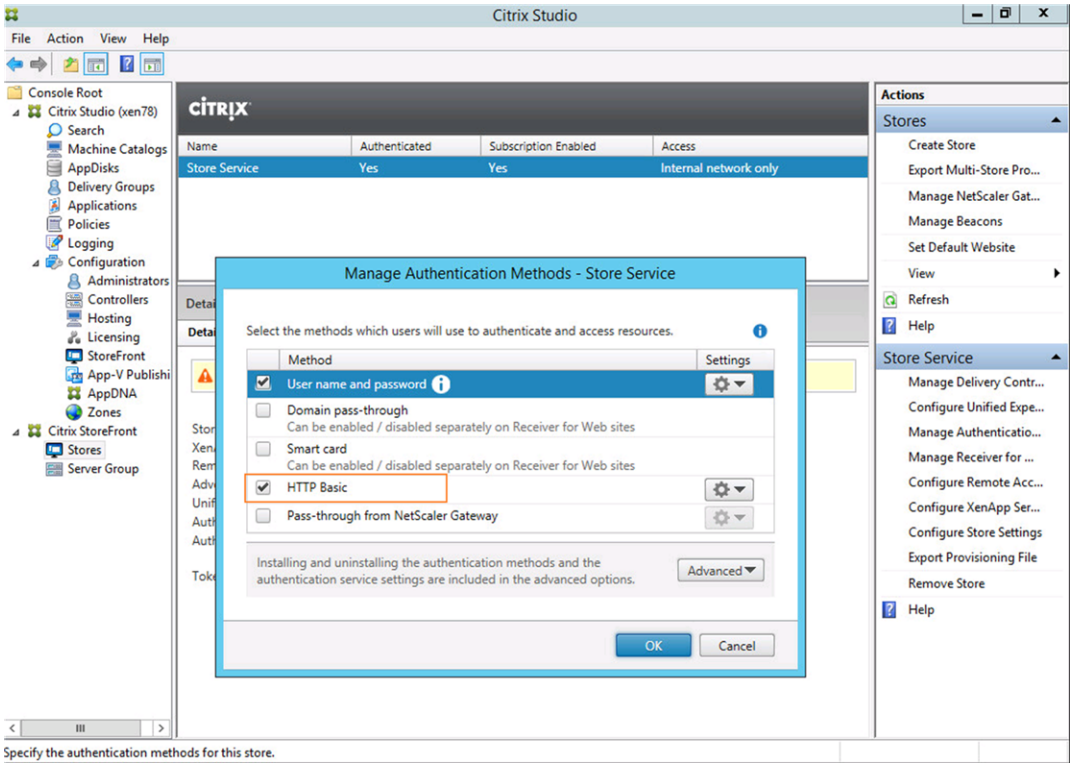
Integration Broker 執行個體可同時使用 Web Interface SDK 和 StoreFront REST API。如果您要使用 Web Interface SDK 與一個 Citrix 伺服器陣列通訊，而使用 StoreFront REST API 與另一個 Citrix 伺服器陣列通訊，請視需要選取或取消選取 [使用 StoreFront] 核取方塊。

若要使用 VMware Identity manager 2.9.1 和更新版本中所提供的 StoreFront REST API 選項，請確定符合下列需求。

- 安裝 Integration Broker 2.9.1 或更新版本。
- 確定使用的 XenApp 或 XenDesktop 版本支援 StoreFront。
- 確定 Integration Broker 可與 StoreFront 伺服器通訊。

  當您啟用 StoreFront REST API 時，Integration Broker 會與 StoreFront 伺服器通訊以產生 ICA 檔案。
- 在 Citrix StoreFront 儲存區中將 [HTTP 基本驗證] 啟用為驗證方法。只有內部存取才需要這麼做。

  警告 若您並未啟用 [HTTP 基本驗證]，則驗證將會失敗。



備註 若要使用 StoreFront REST API，您不需將任何其他檔案下載或複製到您的安裝。

Citrix 整合的必要條件

在 VMware Identity Manager 管理主控台中設定 Citrix 伺服器陣列詳細資料之前，您必須先完成某些必要工作。您必須在支援的 Windows Server 上部署及設定 Integration Broker (VMware Identity Manager 的元件)，並設定 Citrix PowerShell 遠端功能，以啟用 Integration Broker 與 Citrix 伺服器陣列之間的通訊。

高階工作包括下列項目：

- 準備 Windows Server 以安裝 Integration Broker。
  - 新增角色和功能。
  - 安裝 Microsoft J# 2.0 可轉散發套件。

    如果您打算使用 Storefront ReST API (而非 Citrix Web Interface SDK) 以連線至 Citrix 伺服器陣列，則不需要 Microsoft J# 2.0。
- 安裝 Integration Broker。
  - 下載並安裝 Integration Broker。
  - 設定 Integration Broker 的 IIS 管理員設定。
  - 設定 Integration Broker 的 HTTPS 繫結。
- 設定 Citrix PowerShell 遠端功能，以啟用 Integration Broker 伺服器與 Citrix 伺服器陣列之間的遠端引動過程。
  - 在 Integration Broker 伺服器上安裝 Citrix PowerShell SDK。
  - 在 Citrix 伺服器 (僅限 Citrix 6.0 和 5.0) 上啟用 PowerShell 遠端功能。
- 下載並複製 Citrix Web Interface SDK dll 檔案。

  如果您打算使用 Storefront ReST API 以連線至 Citrix 伺服器陣列，則不需要 Citrix Web Interface SDK。

關於部署 Integration Broker

Integration Broker 是 VMware Identity Manager 的元件之一，可用來與 Citrix 伺服器陣列通訊。您可以透過內部部署的方式，將 Integration Broker 安裝在支援的 Windows Server 上。

部署 Integration Broker 時，請遵循下列準則。

- 您可以將 Integration Broker 安裝在 Windows Server 2008 R2、Windows Server 2012 或 Windows Server 2012 R2 上。
- 若要使用 NetScaler 功能，您必須安裝 Integration Broker 2.4 或更新版本。針對 XenApp 或 XenDesktop 7.x，您必須安裝 Integration Broker 2.6 或更新版本。若要使用 Citrix StoreFront REST API，您必須安裝 Integration Broker 2.9.1 或更新版本。
- VMware Identity Manager 連接器必須能夠與 Integration Broker 通訊。如果您設定了多個連接器執行個體，請確定它們全都可與 Integration Broker 通訊。
- 單一 Integration Broker 執行個體可支援多個 Citrix 5.x、6.x 和 7.x 環境。

- 如果您要在 Windows 上使用 VMware Enterprise Systems Connector，請注意下列事項。
  - 從 My VMware 上的 VMware Identity Manager 產品頁面下載 Integration Broker。
  - 建議您將 Integration Broker 和 VMware Enterprise Systems Connector 安裝在不同的伺服器上。
  - 如果您要在與連接器相同的伺服器上安裝 Integration Broker，請確定 HTTP 和 HTTPS 繫結連接埠不會與 VMware Identity Manager Connector 元件使用的連接埠相衝突。

    VMware Identity Manager Connector 元件一律會使用連接埠 80。此外也會使用 443，除非在安裝期間設定了不同的連接埠。
  - 系統會在連接器安裝期間產生自我簽署憑證。如果您在與連接器相同的伺服器上安裝 Integration Broker，則可以使用此憑證。請安裝 Microsoft 商店中的憑證，並將其用於 HTTPS 繫結。

開始之前，您也需要規劃部署策略。

- 考量您是否將使用多個 Integration Broker 執行個體。多個執行個體有助於達成高可用性和負載平衡。
  - 若要達到高可用性，請設定具有兩個以上 Integration Broker 執行個體的叢集。您可以視需求使用相同的叢集來同步資源和權利以及啟動資源，或設定不同的叢集。
  - 如果您的部署需分配大量流量，請增加用來啟動資源的 Integration Broker 執行個體數目。
- 考量您是否將使用負載平衡器。

  如果您的部署會用到多個 Integration Broker 執行個體做為高可用性或負載平衡用途，請考慮將它們安裝在一或多個負載平衡器後面。

準備 Windows Server 以安裝 Integration Broker。

安裝 Integration Broker 之前，您必須設定 Windows 伺服器。

Integration Broker 伺服器支援下列作業系統。

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

備註 請參閱 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 上的 VMware 產品互通性對照表，以瞭解支援版本的最新相關資訊。

新增 Windows Server 角色和功能

在 Integration Broker 伺服器中新增必要的角色、功能和角色服務。

備註 此程序中的步驟涉及 Windows Server 2012 R2 或 Windows Server 2012 使用者介面。如有 Windows Server 2008 R2 的任何差異，也會加以說明。

先決條件

- 確認 Windows Server 2008 R2、Windows Server 2012 或 Windows Server 2012 R2 已安裝最新更新。若要檢查更新，請選取**控制台 > Windows Update**。

- 如有必要，請建立應用程式集區。您可以使用預設應用程式集區，也可以建立專用於 Integration Broker 的應用程式集區。

程序

1 選取**開始 > 伺服器管理員**。

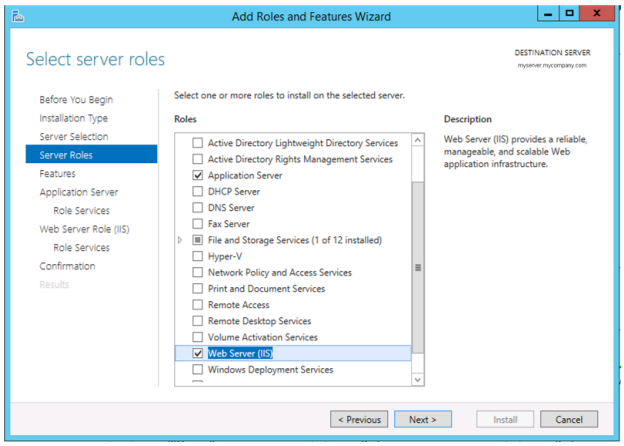
2 在伺服器管理員中，選取**管理 > 新增角色及功能**。

3 在 [新增角色及功能] 精靈中按**下一步**，直到**伺服器角色**頁面顯示。

4 選取下列角色，然後按**下一步**。

角色
- 應用程式伺服器
- 檔案和儲存服務
- 網頁伺服器 (IIS)

備註 當您選取 [網頁伺服器 (IIS)] 時，將會顯示一個方塊以提示您確認網頁伺服器 (IIS) 所需的功能。確認**管理工具**已包含在內，然後按一下**新增功能**。



5 在 [功能] 頁面中，選取下列功能。

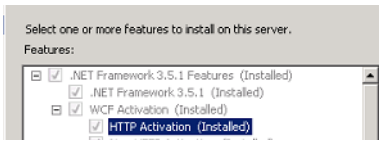
功能

- .NET Framework 3.5 功能
  - .NET Framework 3.5 (包括 .NET 2.0 和 3.0)
  - HTTP 啟動

    當您選取 [HTTP 啟動] 時，將會顯示一個方塊以提示您確認「HTTP 啟動」所需的功能。按一下**新增功能**。

備註 在 Windows Server 2008 R2 上，您可以選取下列選項：

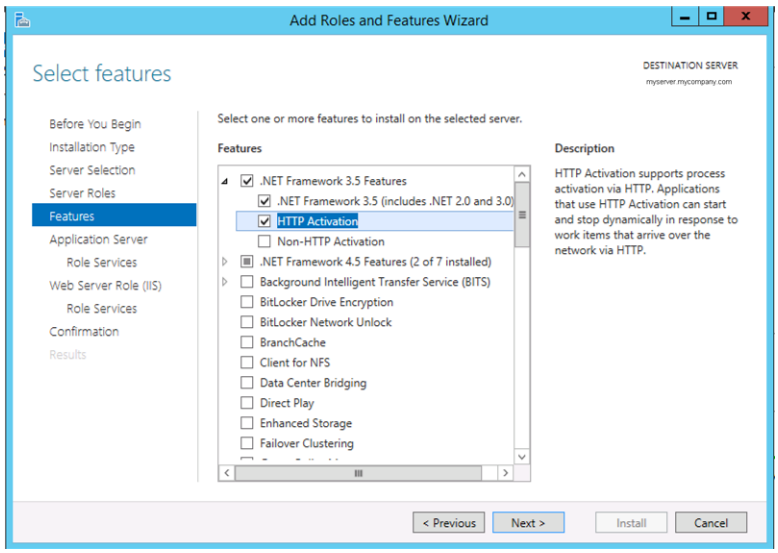
- .NET Framework 3.5 功能
  - .NET Framework 3.5
  - WCF 啟動
    - HTTP 啟動



- 可裝載 IIS 的 Web 核心
- Windows 處理序啟用服務
- WinRM IIS 延伸模組

例如：

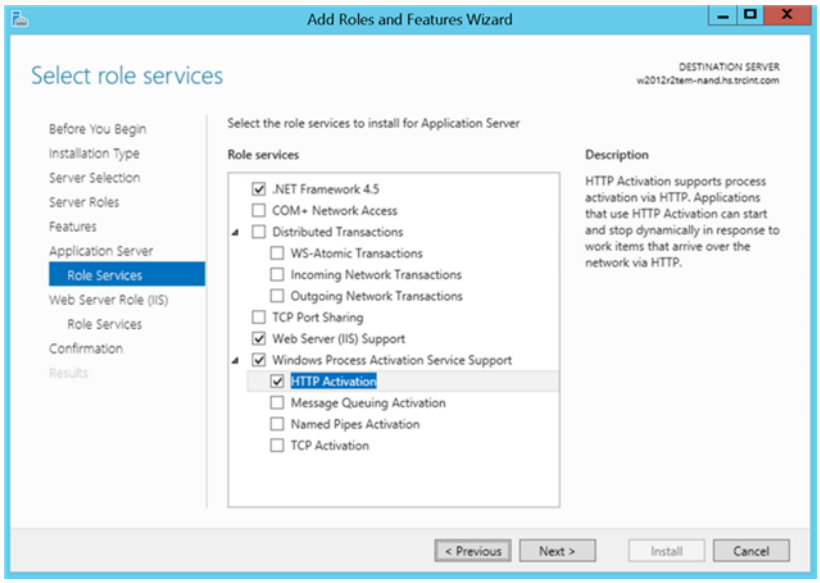
圖 7-1 Windows Server 2012 R2



6 按**下一步**，然後再按一次**下一步**，以顯示 [應用程式伺服器角色服務] 頁面。

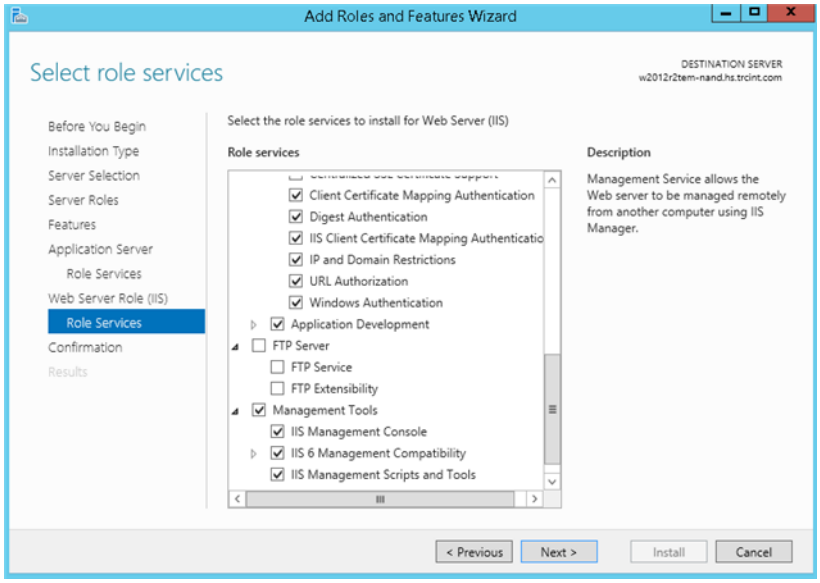
7 在 [應用程式伺服器角色服務] 頁面中，選取下列角色服務。

應用程式伺服器角色服務	**應用程式伺服器角色服務** ■ .NET Framework 4.5 (如果已預先選取，請勿加以變更) ■ 網頁伺服器 (IIS) 支援 **備註** 當您選取 [網頁伺服器 (IIS)] 時，將會顯示一個方塊以提示您確認網頁伺服器 (IIS) 所需的功能。按一下**新增功能**。 ■ Windows 處理序啟用服務支援 ■ HTTP 啟動 例如：



8 按**下一步**，然後再次按一次**下一步**，以顯示 [網頁伺服器角色 (IIS) 角色服務] 頁面。

9 在 [網頁伺服器角色 (IIS) 角色服務] 頁面中，選取下列角色服務。

網頁伺服器角色 (IIS) 角色服務	■ 網頁伺服器 ■ 接受預設選取項目 ■ 啟用下列選項： ■ 管理工具 ■ IIS 管理主控台 ■ IIS 6 管理相容性 例如： 

10 按**下一步**。

11 按一下**安裝**。

12 安裝完成後，按一下**關閉**以關閉 [新增角色及功能] 精靈。

下一個

如有必要，請安裝 Microsoft Visual J# 2.0 可轉散發套件。

安裝 Microsoft Visual J# 2.0 64 位元可轉散發套件

下載並安裝 Microsoft Visual J#® 2.0 64 位元可轉散發套件 - 第二版。如果您打算使用 Citrix Storefront REST API (而非 Citrix Web Interface SDK) 以連線至 Citrix 伺服器陣列，則不需要執行此步驟。

程序

1 從 Microsoft 網站下載 Microsoft Visual J# 2.0 64 位元可轉散發套件 - 第二版。

2 按兩下 vjredist.exe 檔案，然後遵循精靈指示來安裝套件。

部署 Integration Broker

若要部署 Integration Broker，您必須在支援的 Windows 伺服器上下載並安裝 Integration Broker，接著為其進行 IIS 管理員設定，然後設定 HTTPS 和 HTTP 繫結。

安裝 Integration Broker

在您設定的 Windows 伺服器上安裝 Integration Broker。

先決條件

- 準備 Windows 伺服器。請參閱準備 Windows Server 以安裝 Integration Broker。
- 從 My VMware 上的 VMware Identity Manager 產品頁面下載 Integration Broker。

程序

1. 以 Windows 管理員身分登入。
2. 按一下 `setup.exe` 檔案以執行 Integration Broker 安裝程式。
3. 接受使用者授權合約。
4. 選取要用來安裝 Integration Broker 的 Web 位置。
5. (選擇性) 如果您已為 Integration Broker 建立個別的應用程式集區，請選取該應用程式集區。

   警告 請勿變更**虛擬目錄**名稱。

6. 按**下一步**，完成 Integration Broker 的安裝。

下一個

設定 IIS 管理員設定。

設定 IIS 管理員設定

設定 Integration Broker 所需的 IIS 管理員設定。

備註 此程序中的步驟所參照的是 Windows Server 2012 或 Windows Server 2012 R2 使用者介面。如有任何 Windows Server 2008 R2 方面的差異，也會在此列出。

先決條件

身分識別使用者的認證。身分識別使用者必須符合下列需求：

- 網域使用者
- 在 Integration Broker 伺服器上啟用 PowerShell 遠端功能的權限：
  a. 以管理員身分啟動 PowerShell 的權限
  b. 執行 `Enable-PSRemoting`

- Citrix 伺服器上的下列角色之一：
  - 至少唯讀管理員 (7.x 版) 或僅限檢視管理員 (6.x 版)
  - 有權執行下列 PowerShell Cmdlet 的自訂管理員角色。這些 Cmdlet 可用來從 Citrix 伺服器陣列中擷取應用程式、伺服器、伺服器陣列和圖示資訊。

    在 XenApp 6.5 上：

    ```
    Get-XAApplication
    Get-XAServer
    Get-XAAccount
    Get-XAApplicationIcon
    Get-XAFarm
    ```

    在 XenApp 或 XenDesktop 7.x 上：

    ```
    Get-BrokerApplication
    Get-BrokerIcon
    Get-BrokerDesktopGroup
    Get-BrokerAccessPolicyRule
    Get-BrokerAppEntitlementPolicyRule
    Get-BrokerIcon
    Get-BrokerEntitlementPolicyRule
    ```

程序

1 按一下**開始 > 伺服器管理員**。

2 在 [伺服器管理員] 中，選取**工具 > Internet Information Services (IIS) 管理員**。

3 在 [IIS 管理員] 中，設定您在安裝 Integration Broker 時所選取的應用程式集區。

Tip 若要確認正確的應用程式集區，請按一下左窗格中的**應用程式集區**，接著在應用程式集區上按一下滑鼠右鍵並選取 **View 應用程式**，然後確認 Integration Broker 顯示在清單中。

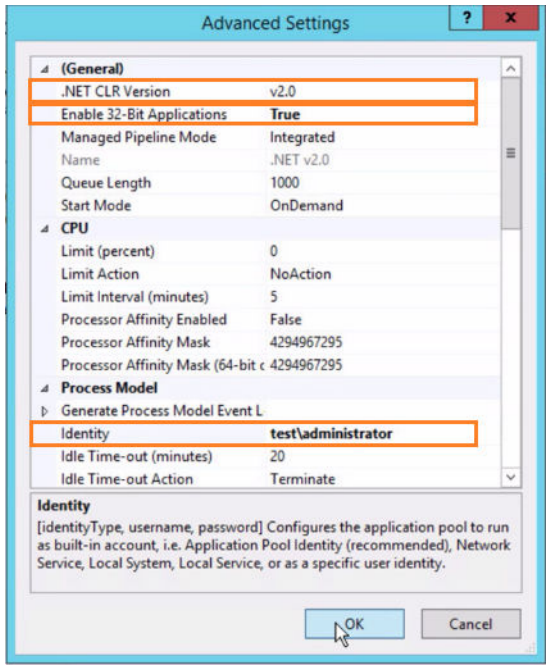
a 在左窗格中，按一下**應用程式集區**。

b 選取您要用於 Integration Broker 的應用程式集區。

c 在右窗格中按一下**進階設定**。

d 在 [進階設定] 對話方塊中，進行下列設定。

選項	說明
.NET CLR 版本	確認值為 **v2.0**。 **備註** 在 Windows 2012 和 Windows 2012 R2 中，應用程式集區依預設可能已設定為不同的 .NET 版本。請確定您將其設定為 v2.0。
啟用 32 位元應用程式	將值設為 **True**。
身分識別	1 按一下**身分識別**。 2 按一下 **...** 圖示。 3 在開啟的 [應用程式集區身分識別] 對話方塊中，按一下**自訂帳戶**，然後按一下**設定**。 4 輸入身分識別使用者的使用者名稱和密碼。請參閱＜必要條件＞一節中的身分識別使用者需求。 5 按一下**確定**，然後再次按一下**確定**。



e 按一下**確定**，關閉 [進階設定] 對話方塊。

設定 Integration Broker 的 HTTPS 站台繫結。

您必須設定 Integration Broker 的 HTTPS 站台繫結。若要設定繫結，您需要 Integration Broker 伺服器的 SSL 憑證。您可以從憑證授權機構取得憑證，或建立自我簽署憑證。

備註 如果您在 Windows 上使用 ，且要在與連接器相同的伺服器上安裝 Integration Broker，請確定 HTTP 和 HTTPS 繫結連接埠不會與 VMware Identity Manager Connector 元件使用的連接埠相衝突。

VMware Identity Manager Connector 元件一律會使用連接埠 80。此外也會使用 443，除非在安裝期間設定了不同的連接埠。如需所使用連接埠的詳細資訊，請參閱《*VMware Enterprise Systems Connector 安裝和設定*》。

建議您將 Integration Broker 和 VMware Enterprise Systems Connector 安裝在不同的伺服器上。

先決條件

- 取得 Integration Broker 伺服器的 SSL 憑證。您可以從憑證授權機構取得憑證，或建立自我簽署憑證。在 Integration Broker 伺服器的 Microsoft 存放區中安裝憑證。

  請參閱範例：使用 IIS 管理員建立自我簽署憑證和範例：使用 OpenSSL 建立自我簽署憑證。

  備註 如果您在 Windows 上使用 VMware Enterprise Systems Connector，且將 Integration Broker 安裝在與連接器相同的伺服器上，則可以使用連接器安裝期間產生的自我簽署憑證。請安裝 Microsoft 商店中的憑證，並將其用於 HTTPS 繫結。

- 如果您使用內部 CA 建立憑證，若要讓 VMware Identity Manager 能夠信任此憑證，則必須在**終止負載平衡器上的 SSL** 索引標籤上，透過 https://*vidmHostname*:8443/cfg/ssl 上傳內部 CA 的根憑證，其中，*vidmHostname* 是設定 Citrix 整合的 VMware Identity Manager 執行個體。在 SaaS 環境中，移至 https://*connectorHostname*:8443/cfg/ssl。

程序

1 在 [IIS 管理員] 的左窗格中，按一下您在其下安裝 Integration Broker 的網站。

Tip 若要確認正確的網站，您可以展開左窗格中的站台，並檢查其下列出的 Integration Broker。

2 在右窗格的**編輯站台**下，按一下**繫結**。

3 使用您建立的憑證新增 HTTPS 繫結。

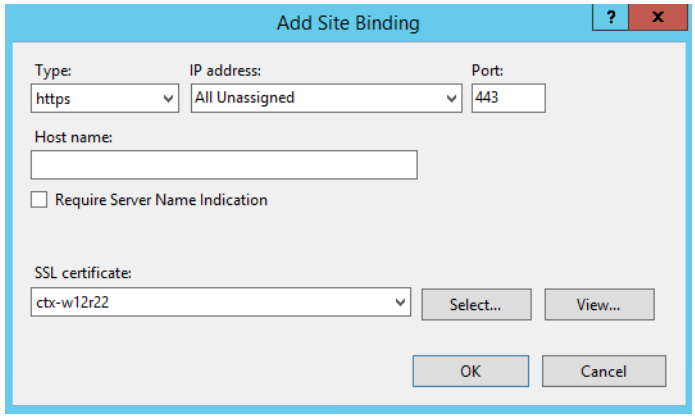
   a 按一下**新增**。

   b 在**類型**欄位中，選取 **https**。

   c 如果您使用 IIS 8.0 或更新版本，請確認**主機名稱**欄位是空的。其中不得包含任何值。

d 在 **SSL 憑證**欄位中，選取您已建立的 SSL 憑證。

例如：



e 按一下**確定**。

4 重新啟動 IIS。

a 以管理員身分開啟 [命令提示字元] 視窗。

b 輸入 `iisreset`。

下一個

確認繫結。

- 在瀏覽器的網址列輸入 http://*hostname* /IB/API/RestServiceImpl.svc/ibhealthcheck，藉此確認 HTTP 繫結會產生預期的輸出。

  預期的輸出：

  ```
  All ok
  ```

- 在瀏覽器的網址列輸入 https://*hostname* /IB/API/RestServiceImpl.svc/ibhealthcheck，藉此確認 HTTPS 繫結會產生預期的輸出。

  預期的輸出：

  ```
  All ok
  ```

備註 在 Internet Explorer 中不會直接顯示 `All ok` 輸出。但會下載輸出檔案。請開啟檔案以檢視輸出。

範例：使用 IIS 管理員建立自我簽署憑證

您可以使用 IIS 管理員建立 Integration Broker 伺服器的自我簽署憑證。

程序

1 啟動 [IIS 管理員]。

2 導覽至**伺服器憑證**。

3 在右窗格中的**動作**下，選取**建立自我簽署憑證**。

4 依照精靈指示以產生自我簽署憑證。

憑證會自動安裝在 Integration Broker 伺服器的 Microsoft 存放區中。

下一個

請將憑證用於 Integration Broker 網站的 HTTPS 繫結。

範例：使用 OpenSSL 建立自我簽署憑證

以下指示提供如何使用 Integration Broker 之 OpenSSL 設定自我簽署憑證的範例。

程序

1 建立 Integration Broker 伺服器的自我簽署憑證。

2 建立 `ibcerts` 資料夾以當做工作目錄。

3 使用 `vi openssl_ext.conf` 命令建立組態檔案。

a 複製以下 OpenSSL 命令並貼到組態檔案。

```
# openssl x509 extfile params
extensions = extend
[req] # openssl req params
prompt = no
distinguished_name = dn-param
[dn-param] # DN fields
C = US
ST = CA
O = VMware (Dummy Cert)
OU = Horizon Workspace (Dummy Cert)
CN = hostname (安裝 Integration Broker 的虛擬機器主機名稱。)
emailAddress = EMAIL PROTECTED
[extend] # openssl extensions
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always
keyUsage = digitalSignature,keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
[policy] # certificate policy extension data
```

備註 儲存檔案之前，請先輸入 CN 值。

b 執行此命令以產生私密金鑰。

```
openssl genrsa -des3 -out server.key 1024
```

c 輸入 *server.key* 的複雜密碼 (如 *vmware*)。

d 將 server.key 檔案重新命名為 server.key.orig。

```
mv server.key server.key.orig
```

e 移除與金鑰相關聯的密碼。

```
openssl rsa –in server.key.orig –out server.key
```

4 利用產生的金鑰建立 CSR (憑證簽署要求)。server.csr 會儲存在工作目錄中。

```
openssl req –new –key server.key –out server.csr –config ./openssl_ext.conf
```

5 簽署 CSR。

```
openssl x509 –req –days 365 –in server.csr –signkey server.key –out server.crt –extfile
openssl_ext.conf
```

預期的輸出隨即顯示。

```
Signature ok subject=/C=US/ST=CA/O=VMware (Dummy Cert)/OU=Horizon Workspace
(Dummy Cert)/CN=w2–hwdog–xa.vmware.com/emailAddress=EMAIL PROTECTED Getting
Private key
```

6 建立 P12 格式。

```
openssl pkcs12 –export –in server.crt –inkey server.key –out server.p12
```

a 出現提示時按 **Enter** 以取得匯出密碼。

重要事項 請勿輸入密碼。

預期的輸出為 server.p12 檔案。

b 將 server.p12 檔案移動至安裝 Integration Broker 的 Windows 機器上。

c 在 [命令提示字元] 中輸入 **mmc**。

d 按一下**檔案 > 新增或移除嵌入式管理單元**。

e 在 [嵌入式管理單元] 視窗中，依序按一下**憑證**和**新增**。

f 選取**電腦帳戶**選項按鈕。

7 將憑證匯入根和個人存放區憑證。

a 在對話方塊中選取**所有檔案**。

b 選取 server.p12 檔案。

c 按一下**可匯出**核取方塊。

d 將密碼保留空白。

e 接受後續步驟的預設值。

8 將憑證複製到相同 mmc 主控台中的 [信任的根 CA]。

9 確認憑證內容包含以下元素。

- 私密金鑰
- 主體屬性中的 CN 與 Integration Broker 主機名稱相符
- 啟用用戶端和伺服器驗證的擴充金鑰使用方法屬性

啟用 Citrix PowerShell 遠端功能

您必須設定 Citrix PowerShell 遠端功能，以啟用 Integration Broker 與 Citrix 伺服器陣列之間的遠端引動。

若要設定 Citrix PowerShell 遠端功能，則需要 Integration Broker 伺服器上安裝 Citrix PowerShell SDK，並確認已在 Citrix 伺服器上啟用 PowerShell 遠端功能。

在 Integration Broker 伺服器上，您必須安裝適當版本的 Citrix PowerShell SDK。如果您連線至多個版本的 Citrix 伺服器陣列，請在 Integration Broker 伺服器上安裝所有必要的 Citrix PowerShell SDK 版本，因為 SDK 不具回溯相容性。

您必須在 Citrix 伺服器上啟用 PowerShell 遠端功能，使 Integration Broker 伺服器能夠連線至這些伺服器並擷取必要的資訊，例如資源資訊、權利和圖示。您僅需要在將於 VMware Identity Manager 中設定的傳遞控制器或 XML Broker 上啟用 PowerShell 遠端功能，而不需要在伺服器陣列中的所有伺服器上啟用。在 XenApp 或 XenDesktop 7.x 中，這些是也用作 XML Broker 的傳遞控制器。在 Citrix 伺服器陣列 6.5、6.0 或 5.0 中，這些是 XML Broker 伺服器。

針對 Citrix 伺服器陣列 6.0 和 5.0 版，Citrix PowerShell 遠端功能需要安全 HTTPS 通道才能進行遠端呼叫。請確定 Citrix 傳遞控制器或 XML 代理具有有效的 SSL 憑證。

在 Integration Broker 伺服器上安裝 Citrix PowerShell SDK

您必須在 Integration Broker 伺服器上安裝 Citrix PowerShell SDK，才能啟用 Integration Broker 伺服器與 Citrix 伺服器陣列之間的連線。

下載並安裝要與 VMware Identity Manager 整合之 Citrix 伺服器陣列的對應 Citrix PowerShell SDK 版本。如果您連線至多個版本的 Citrix 伺服器陣列，請在 Integration Broker 伺服器上安裝所有必要的 Citrix PowerShell SDK 版本，因為 SDK 不具回溯相容性。

程序

1 登入 Integration Broker 伺服器。

2 如果您連線至 XenApp 或 XenDesktop 7.x，請遵循下列步驟。

   a 在 Integration Broker 伺服器上下載並安裝 Citrix Studio。

   b 確認安裝。

      1 以管理員身分開啟 Windows PowerShell。

      2 輸入此命令：

      ```
      Add-PSSnapin Citrix*
      ```

      3 輸入下列命令：

      ```
      Get-BrokerDesktopGroup -AdminAddress CitrixDeliveryController
      Get-ConfigSite -AdminAddress CitrixDeliveryController
      ```

      備註 如果發生驗證錯誤，請以 `set-executionpolicy remotesigned` 命令設定執行原則，然後再次嘗試命令。

3 如果您連線至 Citrix 伺服器陣列 6.5.x，請遵循下列步驟。

   a 在 Integration Broker 伺服器上下載並安裝 Citrix PowerShell SDK 6.5。

   b 確認安裝。

      1 Open **Program Files > Citrix PowerShell Module**。

      2 輸入此命令：

      ```
      Get-XAApplication -ComputerName CitrixServer
      ```

      確認清單包含由 Citrix 主控的所有應用程式。

      備註 如果命令失敗，請確認 XenApp Commands Remoting 服務目前執行於 Citrix 伺服器上。

4 如果您連線至 Citrix 伺服器陣列 6.0 或 5.0，請在 Integration Broker 伺服器上下載並安裝 Citrix PowerShell SDK 6.0 或 5.0，視您的 Citrix 伺服器陣列版本而定。

在 Citrix 伺服器陣列上啟用 Citrix PowerShell 遠端功能

如有必要，請在 Citrix 伺服器陣列上啟用 Citrix PowerShell 遠端功能。

- 在 Citrix XenApp 或 XenDesktop 7.x 上，確認 VMware Identity Manager 將連線的「傳遞控制器」上已啟用 PowerShell 遠端功能。
- 在 Citrix 6.5 上，確認 Citrix XenApp Commands Remoting 服務執行於 VMware Identity Manager 將連線的 XML Broker 上。
- 在 Citrix 6.0 或 5.0 上，啟用 PowerShell 遠端功能。請參閱在 Citrix 伺服器陣列 5.0 或 6.0 上設定 Citrix PowerShell 遠端功能。

在 Citrix 伺服器陣列 5.0 或 6.0 上設定 Citrix PowerShell 遠端功能

您必須在要與 VMware Identity Manager 整合的 Citrix XML Broker 伺服器上啟用 Citrix PowerShell 遠端功能。Citrix PowerShell 遠端功能可啟用 Integration Broker 與 Citrix 伺服器陣列之間的連線。

備註 您僅需要在將於 VMware Identity Manager 中設定的 XML Broker 上啟用 Citrix PowerShell 遠端功能，而不需要在伺服器陣列中的所有伺服器上設定。

先決條件

- 如果您未安裝 Winrm，請從 Microsoft 網站下載和安裝 Winrm。
- 確認 Citrix XML Broker 具有有效的 SSL 憑證。此外，按一下**內容**，並確認憑證的 [伺服器驗證] 已啟用。

程序

1. 以管理員模式開啟 PowerShell。
2. 啟用 Citrix PowerShell 遠端功能。
   a. 輸入 `Get-Service winrm` 命令來確認已在伺服器上安裝 Winrm。
   b. 輸入 `Enable-PSRemoting` 命令。

      此命令會在伺服器上啟用 PowerShell 遠端功能。
   c. 根據 Citrix 伺服器版本來安裝 Citrix PowerShell SDK 5.0 或 6.0。
   d. 從命令提示字元啟用 `winrm` HTTPS 接聽程式。
      1. 在伺服器上建立憑證。
      2. 記錄憑證的憑證指紋。
      3. 驗證已設定憑證的憑證指紋。

```
winrm quickconfig -transport:https
```

e 確認已建立接聽程式。

```
winrm e winrm/config/listener
```

此伺服器以就緒並可供使用。

f 建立接聽程式之後，前往 Integration Broker 伺服器來確認已正確安裝 PowerShell 遠端功能。

```
winrm identify –r:https://XENAPP_HOSTNAME:5986 –u:USERNAME
```

輸出：

IdentifyResponse

ProtocolVersion=http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd

ProductVendor=Microsoft Corporation

ProductVersion=OS: 6.0.6002 SP: 2.0 Stack: 2.0

確認 Citrix 伺服器陣列的連線

部署 Integration Broker 並設定 PowerShell 遠端功能後，請確認 Citrix 伺服器陣列的連線。

程序

1 在瀏覽器中，針對您的 Citrix 伺服器陣列版本輸入適當的 URL。

- Citrix XenApp 或 XenDesktop 伺服器陣列 7.x

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=*XenAppServerHostname*&xenappversion=Version7*x*

- Citrix 伺服器陣列 6.5

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=*XenAppServerHostname*&xenappversion=Version65*orLater*

- Citrix 伺服器陣列 5.0 或 6.0

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=*XenAppServerHostname*&xenappversion=Legacy

2 檢閱輸出。

如果 Integration Broker 已正確設定，則頁面會顯示如下所示的 Citrix 伺服器陣列資訊：

```
"[{\"FarmName\":\"test data\",\"ServerVersion\":\"
6.0.6410\",\"AdministratorType\":\"Full\",\"SessionCount\":\"2\",\"MachineName\"
:\"test data\"}]”
```

如果網頁並未顯示伺服器陣列資訊，請在 `%programdata%/VMware/HorizonIntegrationBroker` 檢閱 Integration Broker 伺服器上的記錄。

下載 Citrix Web Interface SDK 5.4

Citrix Web Interface SDK 可用來從 Citrix Delivery Controller 或 XML Broker 產生 ICA 檔案，並使用該檔案進行驗證以啟動 Citrix 發佈的應用程式和桌面平台。

備註 如果您打算使用 Citrix StoreFront ReST API 與 Citrix 伺服器陣列通訊以產生 ICA 檔案，則不需要安裝 Citrix Web Interface SDK。

程序

1. 從 Citrix 網站下載 Citrix Web Interface SDK 5.4 (WISDK zip 檔案)。
2. 解壓縮 `wisdk.zip` 檔案。
3. 將 `WI5_4_0_SDK/zipfiles/sdkdemo/wisdk` 目錄中的內容複製到 Integration Broker 的預設 bin 目錄 `c:\inetpub\wwwroot\IB\bin`。
4. 重新啟動 IIS。
   a. 以管理員身分開啟 [命令提示字元] 視窗。
   b. 輸入 `iisreset`。

在 VMware Identity Manager 中設定 Citrix 伺服器陣列

若要在 VMware Identity Manager 中設定 Citrix 發佈的資源，您必須在 VMware Identity Manager 管理主控台中輸入 Integration Broker 與 Citrix 伺服器陣列資訊，並排程 VMware Identity Manager 與 Citrix 伺服器陣列之間的同步化頻率。

在 VMware Identity Manager 中設定 Citrix 發佈的資源之前，請確定您符合所有的必要條件。

此外也請遵循下列關於 Citrix 伺服器陣列設定的準則。

- 同步傳遞群組

  傳遞群組在 Citrix 中的 [傳遞類型] 設定可決定 VMware Identity Manager 同步傳遞群組的方式。

  VMware Identity Manager 只有在傳遞群組的 [傳遞類型] 設定為 DesktopsAndApps 或 DesktopsOnly 時，才會同步傳遞群組。如果傳遞群組的 [傳遞類型] 設定為 AppsOnly，則其應用程式仍會同步，但傳遞群組本身將不會同步，且不會顯示在 VMware Identity Manager 目錄中。

  請視情況設定您的傳遞群組。

- 在 XenDesktop 和 XenApp 7.9 中，如果您使用 [有限可見度群組] 選項來限制使用者，請確定 [有限可見度群組] 中包含使用者或群組。如果其中未包含任何使用者或群組，則同步至 VMware Identity Manager 的作業將無法正常運作。
- 確定一個站台中所有 Citrix 發佈的應用程式和桌面平台皆包含有效的使用者。若您刪除使用者或群組，請確保也從 Citrix 發佈的資源中移除該使用者或群組。
- 確定使用者和群組已指派給正確的傳遞群組。

  如果您選取了限制使用者的設定，請確保其中包含使用者和群組。

先決條件

- 設定 VMware Identity Manager。如需相關資訊，請參閱《*安裝和設定 VMware Identity Manager*》以及《*VMware Identity Manager 管理*》。
- 確定具有 Citrix 權利的使用者和群組已使用目錄同步從您的企業目錄同步至 VMware Identity Manager。

  確定 VMware Identity Manager 目錄中已將 **distinguishedName** 標示為必要屬性。沒有這個屬性，Citrix 發佈的資源將無法同步。您必須先設定必要屬性才能建立目錄。如果您已建立目錄但 **distinguishedName** 不是必要屬性，請刪除該目錄、在**身分識別與存取管理 > 設定 > 使用者屬性**頁面中將 **distinguishedName** 設為必要屬性，然後建立新目錄。
- 部署 Integration Broker，並確定您已符合 Citrix 整合的必要條件中所述的所有必要條件。
- 若要分散大型企業部署中的負載，請將兩個以上 Integration Broker 執行個體專用於同步作業，並將兩個以上 Integration Broker 執行個體專用於 SSO 用途。

  如果您將多個 Integration Broker 執行個體用於同步或 SSO 用途，請在這些 Integration Broker 執行個體前方放置負載平衡器，並記下負載平衡器的主機名稱或 IP 位址，以便在此工作期間使用。
- 如果您想要使用 [使用 StoreFront] 選項 (VMware Identity manager 2.9.1 和更新版本中所提供)，請確定您符合下列需求。
  - 安裝 Integration Broker 2.9.1 或更新版本。
  - 確定使用的 XenApp 或 XenDesktop 版本支援 StoreFront。
  - 確定 Integration Broker 可與 StoreFront 伺服器通訊。

    當您啟用 StoreFront ReST API 時，Integration Broker 會與 StoreFront 伺服器通訊以產生 ICA 檔案。
  - 在 Citrix StoreFront 儲存區中將 [HTTP 基本驗證] 啟用為驗證方法。此需求僅適用於內部存取。

    警告　若您並未啟用 [HTTP 基本驗證]，則驗證將會失敗。
- 檢閱您 Citrix XenApp 或 XenDesktop 版本的 Citrix 說明文件。

程序

1. 登入 VMware Identity Manager 管理主控台。
2. 選取**目錄**索引標籤。
3. 按一下**管理桌面平台應用程式**，然後從下拉式功能表中選取 **Citrix 發佈的應用程式**。
4. 在 [已發佈的應用程式 - Citrix] 頁面中，選取**啟動 Citrix 型應用程式**核取方塊。
5. 輸入同步 Integration Broker 或負載平衡器的主機名稱和連接埠號碼。

   如果您在用於同步的多個 Integration Broker 執行個體前面設定了負載平衡器，請輸入負載平衡器的主機名稱或 IP 位址以及連接埠名稱。

   如果您透過 SSL 連線至 Integration Broker，請選取**使用 SSL**。

6 輸入 SSO Integration Broker 資訊。

- 如果要讓同步和單一登入使用相同的 Integration Broker 執行個體，請按一下**使用與同步 Integration Broker 相同的項目**按鈕。
- 如果您設定了專用的同步和 SSO Integration Broker 執行個體，請輸入下列資訊。
  a 輸入 SSO Integration Broker 或負載平衡器的主機名稱和連接埠號碼。

  如果您在專用於提供 SSO 的多個 Integration Broker 執行個體前面設定了負載平衡器，請輸入負載平衡器的主機名稱或 IP 位址以及連接埠號碼。

  b 如果您透過 SSL 連線至 Integration Broker，請選取**使用 SSL**。

7 輸入 Citrix 伺服器陣列詳細資料。

若要新增多個伺服器陣列，請按一下 **+新增伺服器陣列**。

選項	說明
版本	選取 Citrix 伺服器陣列版本：5.0、6.0、6.5 或 7.x。
使用 StoreFront	如果您要使用 Citrix StoreFront ReST API 來啟動 XenApp 資源，請選取此選項。選取此選項時，Integration Broker 會使用 Citrix StoreFront ReST API 與 StoreFront 伺服器通訊，並擷取 ICA 檔案。若未選取此選項，則 Integration Broker 會使用 Citrix Web Interface SDK 與 Citrix 元件通訊，並擷取 ICA 檔案。 **備註** 如果您在初始設定和同步化之後選取或取消選取此選項，請按一下**儲存**，然後按一下**立即同步**再次進行同步以使變更生效。
StoreFront URL	以下列格式輸入 StoreFront 伺服器 URL： *transportType*://*storefrontServerFQDN*/Citrix/*storename*Web 例如：http://xen76.example.com/Citrix/mystoreWeb **備註** 這是 Store Web Receiver 網站 URL。 **重要事項** 此外，請在 [網路範圍] 設定之 XenApp 區段的**用戶端存取 URL 主機**欄位中輸入此 URL。
伺服器名稱	您環境中指派的伺服器名稱。
伺服器 (容錯移轉順序)	依容錯移轉順序組織 Citrix XML 代理 (伺服器)。VMware Identity Manager 在 SSO 和發生容錯移轉狀況時會遵守此順序。 **備註** XML 代理必須已啟用 PowerShell 遠端功能。
傳輸類型	Citrix 伺服器組態中使用的傳輸類型：HTTP、HTTPS 或 SSL RELAY。 **備註** 傳輸類型和連接埠必須符合 Citrix 伺服器組態。
連接埠號碼	Citrix 伺服器組態中使用的連接埠設定 **備註** 傳輸類型和連接埠必須符合 Citrix 伺服器組態。

8 在**部署類型**下拉式清單中，選取讓使用者能夠在 Workspace ONE 中使用 Citrix 發佈的資源的方法。

- **使用者啟動** -VMware Identity Manager 會將 Citrix 資源新增至 [目錄] 頁面。若要使用資源，使用者必須將資源從 [目錄] 頁面移至 [書籤] 頁面。
- **自動** - VMware Identity Manager 會將資源直接新增至 [書籤] 頁面，以供使用者立即使用。

您在此處選取的部署類型，即為對您的 Citrix 整合中所有資源的所有使用者權利進行套用的全域設定。您可以在應用程式或桌面平台的 [權利] 頁面上，針對不同的資源修改個別使用者或群組的部署類型。

建議您將全域部署類型設為**使用者啟動**。接著，您可以針對各個資源修改特定使用者或群組的設定。

如需關於設定部署類型的詳細資訊，請參閱設定 Citrix 權利的部署類型。

9 如果要將類別從 Citrix 伺服器陣列同步至 VMware Identity Manager，請選取**從伺服器陣列同步類別**。

10 選取**不要同步重複的應用程式**可防止從多個伺服器同步重複的應用程式。在多個資料中心部署 VMware Identity Manager 時，系統會在多個資料中心中設定相同的資源。選取此選項可防止 VMware Identity Manager 目錄中出現重複的桌面平台或應用程式。

11 在**選擇頻率**欄位中，選取要自動從 Citrix 伺服器陣列同步資源和權利的頻率。如果您不想設定自動同步排程，請選取**手動**。

12 按一下**立即排程**，將 Citrix 發佈的資源同步化至 VMware Identity Manager。

有時候在同步 Integration Broker 和 SSL 時，由於一些環境因素會使同步化變慢，例如網路速度和流量。如果 Citrix 部署規模很大，例如超過 300 個應用程式，也可能使同步化變慢。

備註 VMware Identity Manager 不支援 Citrix 產品中的匿名使用者群組功能。

13 按一下**儲存**。

隨即會顯示一個對話方塊，列出即將同步的應用程式、傳遞群組 (桌面平台) 和權利的數目。您可以按一下連結來檢視詳細資料。按一下對話方塊中的**儲存並繼續**。

Citrix 發佈的資源和對應的權利就會與 VMware Identity Manager 同步。

下一個

如果您選取 [使用 StoreFront] 選項，請編輯網路範圍設定，並在 XenApp 區段的**用戶端存取 URL 主機**欄位中，輸入您在 **StoreFront URL** 欄位中所輸入的相同 URL。

在 VMware Identity Manager 中設定 Citrix 資源啟動

在設定 [Citrix 發佈的應用程式] 頁面之後，請設定資源啟動的網路 IP 範圍。您可以指定使用者來自於特定網路範圍的應用程式或桌面平台啟動流量 (ICA 流量) 要透過 NetScaler 或直接連線路由傳送至 XenApp 伺服器。如此一來，您可以滿足使用者從外部和內部存取部署中之 Citrix 資源的需求。

當使用者從 Workspace ONE 入口網站啟動應用程式或桌面平台時，如果其 IP 位址落在針對 NetScaler 設定的網路範圍內，則系統會透過 NetScaler 將 ICA 流量路由到 XenApp 伺服器。如果 IP 位址落在直接連線範圍內，系統會將 ICA 流量直接路由到 XenApp 伺服器。

設定內部網路的資源啟動

您可以設定使用者的應用程式或桌面平台啟動流量 (ICA 流量) 應直接傳送至 XenApp 伺服器的網路範圍。此方式通常用來提供對 Citrix 發佈之資源的內部存取。

當使用者從 Workspace ONE 入口網站啟動應用程式或桌面平台時，如果其 IP 位址落在直接連線範圍內，則系統會直接將 ICA 流量路由到 XenApp 伺服器。

備註 若要設定外部網路的資源啟動，請參閱設定使用 NetScaler 從外部網路進行的資源啟動。

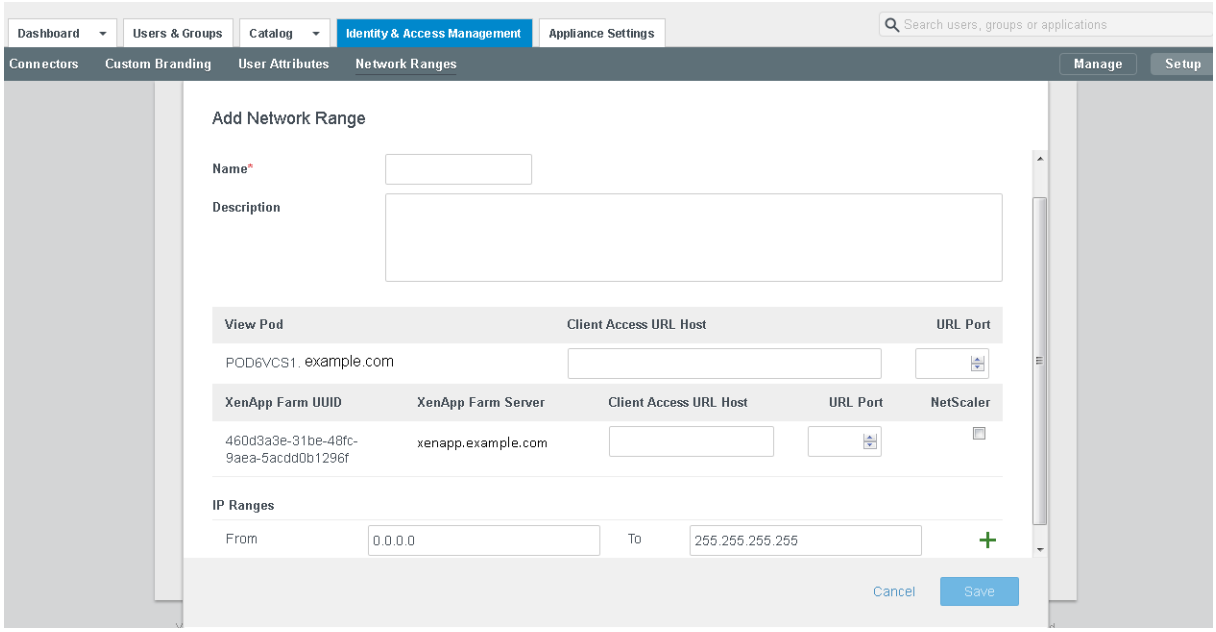
程序

1 登入 VMware Identity Manager 管理主控台。

2 按一下**身分識別與存取管理**索引標籤。

3 按一下**設定**，接著選取**網路範圍**索引標籤。

4 選取現有的網路範圍，或按一下**新增網路範圍**來建立新範圍。



5 如果您要建立新網路範圍，請提供網路範圍的名稱和說明。

6 在頁面的 [XenApp] 區段中輸入以下資訊。

   a 在**用戶端存取 URL 主機**欄位中輸入 XenApp 伺服器主機名稱。例如：**xenapphost.example.com**

   備註 如果您在 [已發佈的應用程式 - Citrix] 頁面中為伺服器陣列選取**使用 StoreFront** 核取方塊，請輸入您在 **StoreFront URL** 欄位中所輸入的相同 URL。

   b 在 **URL 連接埠** 欄位中輸入連接埠。例如：**443**

   c 取消選取 **NetScaler** 核取方塊以直接連線。

7 在 **IP 範圍**欄位中，指定要套用選項的 IP 範圍。

8 按一下**儲存**。

設定使用 NetScaler 從外部網路進行的資源啟動

VMware Identity Manager 支援包含 NetScaler 的 Citrix 部署。NetScaler 應用裝置通常用來提供對 XenApp 或 XenDesktop 應用程式或桌面平台的外部存取。

如果您的 Citrix 部署包含 NetScaler 應用裝置，您可以為 VMware Identity Manager 設定適當的設定，使得在使用者啟動 Citrix 資源時，流量會透過 NetScaler 路由到 XenApp 伺服器。

在 VMware Identity Manager 中，您需要為每個 XenApp 伺服器陣列指定 Secure Ticket Authority (STA) 伺服器。STA 伺服器可用來在應用程式啟動程序進行時產生及驗證 STA 票證。

您也可以針對指定啟動流量要透過 NetScaler 路由到 XenApp 伺服器還是直接路由到 XenApp 伺服器的用戶端網路 IP 範圍，設定其相關原則。這個做法可讓您符合外部和內部存取需求。

備註 若要使用 NetScaler 功能，您必須使用 Integration Broker 2.4 或更新版本。您可以從 My VMware 下載 Integration Broker。不支援升級。請先解除安裝舊版本，然後再安裝新版本。

在 VMware Identity Manager 中進行 NetScaler 設定

若要進行 VMware Identity Manager 的 NetScaler 設定，您必須為 Citrix 部署中的每個 XenApp Farm 指定 Secure Ticket Authority (STA) 伺服器。STA 伺服器可用來在應用程式或桌面平台啟動程序進行時產生及驗證 STA 票證。

當使用者啟動應用程式或桌面平台時，VMware Identity Manager 會從 STA 伺服器取得票證。它會將票證和其他資訊一併提供給 NetScaler，而 NetScaler 則會在建立連往 XenApp Farm 的安全連線之前，向 STA 伺服器驗證票證。

先決條件

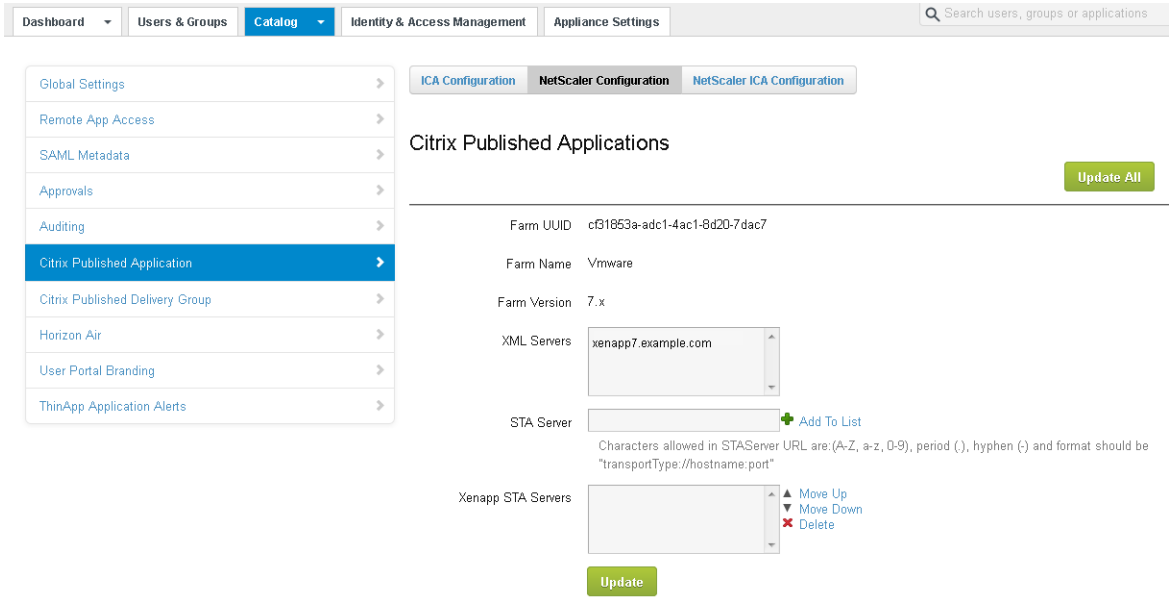
您已整合 Citrix 發佈的資源與 VMware Identity Manager，並已完成**目錄 > 管理桌面平台應用程式 > Citrix 發佈的應用程式**頁面中的組態。

程序

1 在 VMware Identity Manager 管理主控台內，按一下**目錄**索引標籤上的箭頭，接著選取**設定**。

2 從左側窗格選取 **Citrix 發佈的應用程式**。

3 選取 **NetScaler 組態**索引標籤。



4 **伺服器陣列 UUID**、**伺服器陣列名稱**、**伺服器陣列版本**和 **XML 伺服器**欄位會預先填入，且您無法修改其中的值。

5 指定一或多部 STA 伺服器。

a 在 **STA 伺服器**欄位中，依照下列格式輸入 STA 伺服器 URL。

transporttype`://`*server*`:`*port*

例如：**`http://staserver.example.com:80`**

URL 只允許英數字元、句號 (.) 及連字號 (-)。

b 按一下**新增至清單**。

伺服器隨即會出現在 **XenApp STA 伺服器**清單中。

c (選用) 視需要輸入其他 STA 伺服器。例如，為了進行容錯移轉，您可以指定第二部 STA 伺服器。

d 如果您新增多部 STA 伺服器，請在 **XenApp STA 伺服器**欄位中按一下**上移**或**下移**來選取順序。

6 按一下**更新**。

7 如果您的部署中有多部 XenApp 伺服器陣列，請為每個伺服器陣列指定一部 STA 伺服器。

下一個

針對特定網路 IP 範圍設定原則，指定透過 NetScaler 將啟動流量路由傳送至 XenApp 伺服器。

設定 NetScaler 的網路範圍

您可以設定使用者的應用程式或桌面平台啟動流量 (ICA 流量) 應透過 NetScaler 路由傳送至 XenApp 伺服器的網路範圍。此方式通常用來提供對 Citrix 發佈之資源的外部存取。

當使用者從 Workspace ONE 入口網站啟動應用程式或桌面平台時，如果其 IP 位址落在針對 NetScaler 設定的範圍內，則系統會透過 NetScaler 將 ICA 流量路由到 XenApp 伺服器。

備註 若要設定內部網路的資源啟動，請參閱設定內部網路的資源啟動。

先決條件

已在**目錄 > 設定 > Citrix 發佈的應用程式 > NetScaler 組態**索引標籤中進行 VMware Identity Manager 的 Netscaler 設定。

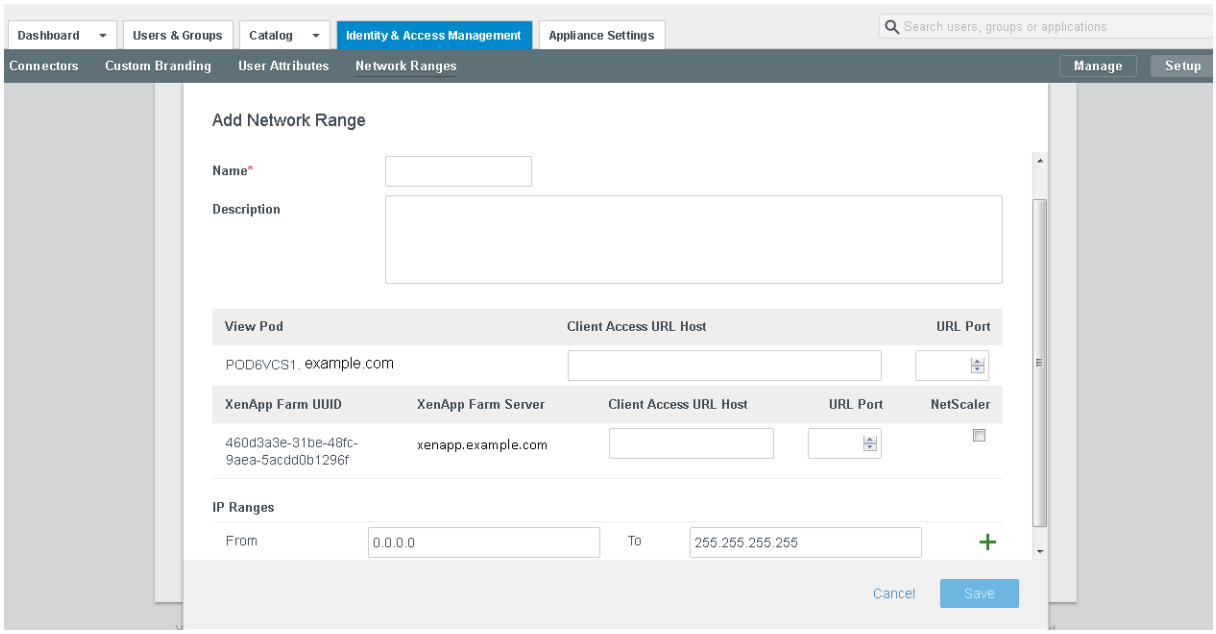
程序

1 登入 VMware Identity Manager 管理主控台。

2 按一下**身分識別與存取管理**索引標籤。

3 按一下**設定**，然後按一下**網路範圍**索引標籤。

4 選取現有的網路範圍，或按一下**新增網路範圍**來建立新範圍。



5 如果您要建立新網路範圍，請提供網路範圍的名稱和說明。

6 在頁面的 [XenApp] 區段中輸入以下資訊。

a 在**用戶端存取 URL 主機**欄位中，輸入 NetScaler 主機名稱。例如：**`netscalerhost.example.com`**

備註 如果您在 [已發佈的應用程式 - Citrix] 頁面中為伺服器陣列選取**使用 StoreFront** 核取方塊，請輸入您在 **StoreFront URL** 欄位中所輸入的相同 URL。

b 在 [URL 連接埠] 欄位中輸入連接埠。例如：**443**

c 選取 **NetScaler** 核取方塊。

7 在 **IP 範圍**欄位中，指定要套用選項的 IP 範圍。

8 按一下**儲存**。

設定 VMware Identity Manager 設定以用於 Citrix 整合

您可以在 VMware Identity Manager 中進行數個設定以用於 Citrix 整合。

設定 Citrix 權利的部署類型

您可以為 Citrix 發行的資源設定部署類型，以決定如何讓使用者能夠使用這些資源。將部署類型設為 [使用者啟動] 之後，系統會將資源新增至 [目錄] 頁面。若要使用資源，使用者必須將資源從 [目錄] 頁面移至 [書籤] 頁面。將部署類型設為 [自動] 之後，系統會將資源直接新增至 [書籤] 頁面，以立即供使用者使用。

您可以設定不同層級的部署類型。

- 全域層級

  全域設定會套用至您的部署中所有 Citrix 發行資源的所有使用者權利。您可以在第一次整合 Citrix 發佈的資源與 VMware Identity Manager 時，使用 [已發佈的應用程式 - Citrix] 頁面指定全域部署類型。在初始整合之後，您可以從相同的頁面修改全域設定。請注意，如果您在初始整合後變更了全域設定，新的設定將僅會套用至同步的新權利。若要修改現有的權利，您可以變更個別資源層級的設定。

  備註 建議您將全域部署類型設為 [使用者啟動]。在一般情況下，您會先將全域設定設為 [使用者啟動]，再將其修改為針對特定使用者和群組權利進行啟用。

- 使用者或群組權利層級

  您也可以針對特定的使用者和群組，在個別的應用程式或桌面平台層級上設定部署類型。此設定會覆寫全域設定。此設定在後續同步期間將不會變更。

在同步期間，系統不會變更現有權利的部署類型。對於同步中的新權利，系統會套用全域設定。

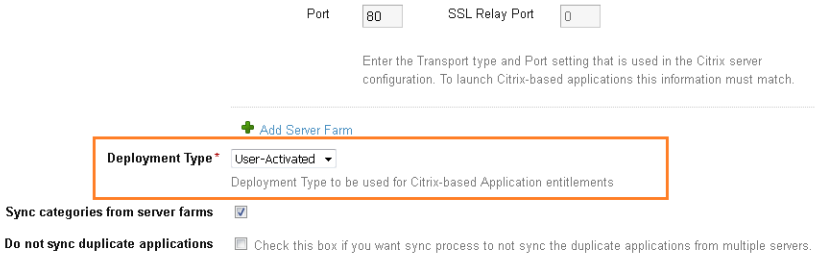
備註 當資源啟動後，也就是資源顯示在使用者的 [書籤] 頁面後，它將持續顯示在 [書籤] 頁面中，除非使用者加以刪除。對部署類型所做的任何變更，皆不會將該資源從 [書籤] 頁面中移除。

程序

1 若要設定全域層級的部署類型，請執行下列步驟。

a 按一下**目錄**索引標籤，然後選取**管理桌面平台應用程式 > Citrix 發佈的應用程式**。

b 在**部署類型**欄位中，選取**使用者啟動**或**自動**。



備註 建議您將全域部署類型設為 [使用者啟動]。

c 按一下**儲存**。

這些設定將從下次同步時開始套用至所有新的權利。

2 若要為特定的使用者或群組權利設定部署類型，請執行下列步驟。

a 按一下**目錄**索引標籤。

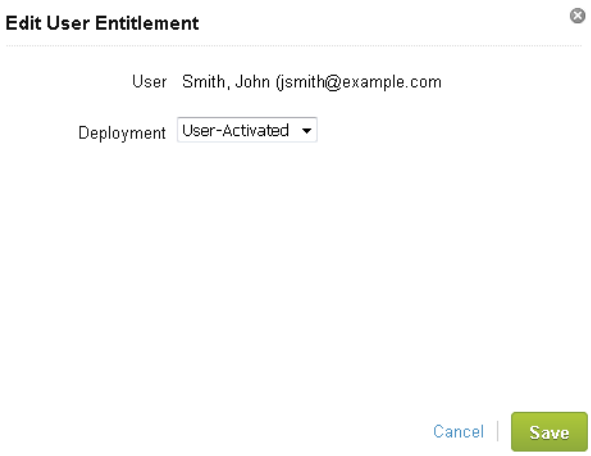
b 按一下要編輯權利的應用程式或桌面平台。

c 按一下**權利**，以顯示應用程式的 [權利] 頁面。

您可以在**部署**資料行中檢視使用者和群組權利目前的部署設定。

d 在您要編輯的權利旁，按一下**編輯**。

e 在 [編輯使用者權利] 對話方塊中，選取權利的部署類型。



f 按一下**儲存**。

設定使用者或群組權利層級的部署類型時，將具有高於全域部署類型設定的優先順序，且在同步期間將不會遭到修改。

管理 Citrix 發行的資源的類別

您可使用 VMware Identity Manager 管理主控台和您的 Citrix 部署來管理 Citrix 發行的資源類別。

在 Citrix 部署中，可透過編輯資源內容中的**用戶端應用程式資料夾**文字方塊，提供類別名稱給 Citrix 發行的應用程式或桌面平台。將 Citrix 部署與 VMware Identity Manager 整合時，Citrix 發行的應用程式和桌面平台的現有類別名稱也會一同移轉至 VMware Identity Manager。

整合之後，您可在 Citrix 部署中繼續建立類別。如果啟用 [已發佈的應用程式 - Citrix] 頁面上的**從伺服器陣列同步類別**核取方塊，新類別會在下次同步時移轉至 VMware Identity Manager。請參閱 在 VMware Identity Manager 中設定 Citrix 伺服器陣列。

您也可以直接在 VMware Identity Manager 中建立類別。如需使用資源類別的相關資訊，請參閱 *《VMware Identity Manager 管理指南》*。

在管理主控台中，依序按一下**類別**索引標籤和**任何應用程式類型**，接著為應用程式選取 **Citrix 發行的應用程式**或為桌面平台選取 **Citrix 發行的傳遞群組**，即可建立和檢視所有 Citrix 發行的資源的類別。按一下資源名稱並選取**詳細資料**，即可檢視和編輯特定 Citrix 發行的資源的類別。

如果在 VMware Identity Manager 中建立類別，該類別不會出現在 Citrix 部署中。

如果在 Citrix 部署中建立類別，該類別會在下次同步時出現在 VMware Identity Manager 中。如果在 Citrix 部署中更新類別名稱，更新後的類別名稱會出現在 VMware Identity Manager 中，同時保留原始的類別名稱。如果想從 VMware Identity Manager 移除原始的類別名稱，您必須以手動方式移除。

為 Citrix 發佈的資源設定傳遞設定 (ICA 內容)

您可以在 VMware Identity Manager 管理主控台中，為 Citrix 發佈的應用程式和桌面平台編輯傳遞設定。桌面平台是指傳遞群組。

您可以為可從您的 VMware Identity Manager 部署中使用的所有 Citrix 發佈應用程式和 Citrix 發佈桌面平台全域編輯傳遞設定，或針對特定的 Citrix 發佈資源個別進行編輯。

您可以藉由編輯獨立運算架構 (ICA) 內容來設定傳遞設定。ICA 是 Citrix 專屬通訊協定。可用的 ICA 內容有很多種，分別控制安全性、顯示和壓縮等領域。如需設定 ICA 內容的詳細資訊，請參閱 Citrix 文件。

VMware Identity Manager 包含預設全域設定，用以定義已設定的 Citrix 部署如何將 Citrix 發佈的資源傳遞給使用者。您可以編輯預設 VMware Identity Manager 設定，以及新增設定。

您也可以為個別資源指定傳遞設定。個別資源的設定具有高於全域設定的優先順序。當您為特定資源的傳遞提供 ICA 內容時，請列出 Citrix 部署以您預期的方式傳遞資源所需的所有內容。當個別資源的傳遞設定存在於 VMware Identity Manager 時，VMware Identity Manager 將只會套用這些設定，而忽略所有的全域資源傳遞設定。

為所有 Citrix 發佈的資源編輯資源傳遞設定

您可以為 VMware Identity Manager 部署中由 Citrix 發佈的應用程式和桌面平台編輯全域傳遞設定。

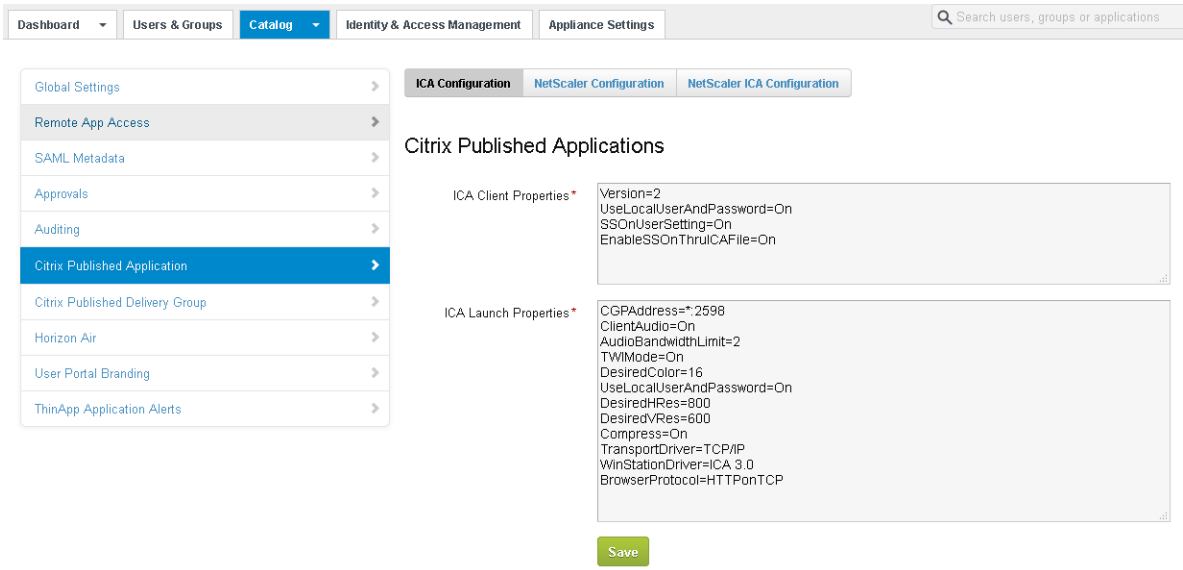
在您編輯之前，這些全域設定的 ICA 內容欄位都會以預設值填入。

重要事項 指定於 **Citrix 發佈的應用程式 > ICA 組態**或 **Citrix 發佈的傳遞群組 > ICA 組態**索引標籤中的 ICA 內容，會套用至經由直接連線傳輸的啟動流量。若想了解經由 Netscaler 路由的啟動流量，請參閱 編輯 NetScaler 的 ICA 內容。

程序

1. 登入 管理主控台。
2. 按一下**目錄**索引標籤上的箭號，然後選取**設定**。
3. 選取 **Citrix 發佈的應用程式**以編輯應用程式的 ICA 設定，或選取 **Citrix 發佈的傳遞群組**以編輯桌面平台的 ICA 設定。

   例如：



4 在 **ICA 組態**索引標籤中，根據 Citrix 準則編輯 ICA 內容。

ICA 用戶端內容和 **ICA 啟動內容**欄位必須一起使用。兩個欄位必須都有值，或都是空的。

5 按一下**儲存**。

除非個別資源有其本身的資源傳遞設定，否則您的 Citrix 部署在將 Citrix 發佈的資源 (透過 VMware Identity Manager 而可供使用) 傳遞給使用者時，將會套用全域 ICA 內容。

為單一 Citrix 發佈的資源編輯傳遞設定

您可以為 VMware Identity Manager 部署中由 Citrix 發佈的個別應用程式和桌面平台編輯傳遞設定 (ICA 內容)。

依預設，個別應用程式的 ICA 內容文字方塊會是空的。

當您編輯個別 Citrix 發佈資源的 ICA 內容時，這些設定的優先順序會高於全域設定。如需全域設定的相關資訊，請參閱為所有 Citrix 發佈的資源編輯資源傳遞設定。

重要事項 在個別應用程式或桌面平台上設定的 ICA 內容，不會套用至透過 Netscaler 路由的 ICA 流量。只有位於 **Netscaler ICA 內容**頁面上，從**目錄 > 設定 > Citrix 發佈的應用程式**索引標籤和**目錄 > 設定 > Citrix 發佈的傳遞群組**索引標籤存取的全域設定，才會套用至透過 Netscaler 路由的 ICA 流量。如需詳細資訊，請參閱 編輯 NetScaler 的 ICA 內容。

程序

1 登入管理主控台。

2 按一下**目錄**索引標籤。

3 按一下**任何應用程式類型 > Citrix 發佈的應用程式**以編輯應用程式的設定，或按一下**任何應用程式類型 > Citrix 發佈的傳遞群組**以編輯桌面平台的設定。

4 按一下要編輯之 Citrix 發佈資源的名稱。

5 按一下**組態**。

6 檢視從您的 Citrix 部署傳送之資源的相關資訊。

此頁面會提供資源的幾項詳細資料，例如資源名稱、資源識別碼、伺服器名稱等等。此外，此頁面也會顯示資源啟用情形的相關資訊。如果未選取**啟用**核取方塊，則會在您的 Citrix 部署中停用該資源，並且對使用者隱藏該資源。

7 在 ICA 內容文字方塊中，根據 Citrix 準則新增內容或編輯現有內容。

備註 **ICA 用戶端內容**和 **ICA 啟動內容**文字方塊必須都有值，或者都是空的。

8 按一下**儲存**。

編輯 NetScaler 的 ICA 內容

您可以藉由編輯 ICA 內容，為 Citrix 發佈的資源設定傳遞設定。針對透過 NetScaler 路由傳送的 ICA 流量，您必須在 **Citrix 發佈的應用程式 > NetScaler ICA 組態**或 **Citrix 發佈的傳遞群組 > NetScaler ICA 組態**索引標籤中編輯 ICA 內容。針對應用程式，請使用 **Citrix 發佈的應用程式 > NetScaler ICA 組態**。針對桌面平台，請使用 **Citrix 發佈的傳遞群組 > NetScaler ICA 組態**。

對個別 Citrix 資源設定的應用程式傳遞設定，將不會套用至透過 NetScaler 路由的 ICA 流量。

備註 若要為透過直接連線 (而非 NetScaler) 傳輸的 ICA 流量編輯 ICA 內容，請參閱為所有 Citrix 發佈的資源編輯資源傳遞設定。

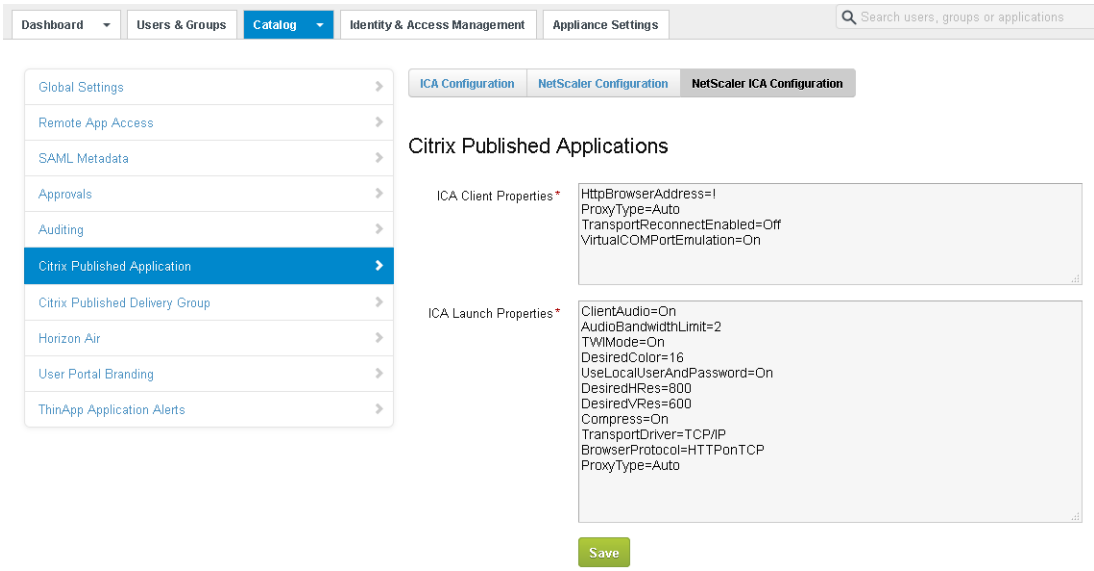
程序

1 登入管理主控台。

2 按一下**目錄**索引標籤上的箭頭，然後選取**設定**。

3 選取 **Citrix 發佈的應用程式** (適用於應用程式) 或 **Citrix 發佈的傳遞群組** (適用於桌面平台)，然後選取 **NetScaler ICA 內容**索引標籤。

內容欄位會以預設設定填入。



4 編輯 ICA 用戶端內容或啟動內容。

您可以變更內容的值，或新增內容。如需 ICA 內容的相關資訊，請參閱 Citrix 文件。

備註 **ICA 用戶端內容**和 **ICA 啟動內容**欄位必須一起使用。兩個欄位必須都有值，或都是空的。

5 按一下**儲存**。

設定特定應用程式和桌面平台的存取原則

預設存取原則集會套用至您的目錄中的所有應用程式和桌面平台。您也可以設定個別應用程式或桌面平台集區的存取原則，這將會覆寫預設存取原則。

您可以從 [原則] 頁面將存取原則套用至一或多個應用程式和桌面平台，或從 [應用程式組態] 頁面中選取特定應用程式的存取原則。

如需存取原則的詳細資訊，請參閱《*VMware Identity Manager 管理指南*》。

程序

1 若要從 [原則] 頁面將存取原則套用至應用程式和桌面平台，請遵循下列步驟。

   a 導覽至 [身分識別與存取管理] > [管理] > [原則] 頁面。

   b 按一下原則加以編輯，或按一下**新增原則**以建立新原則。

   c 在原則頁面中，編輯或定義原則。

   d 在**套用到**區段中，選取要套用原則的應用程式。

   e 按一下**儲存**。

2 若要從 [應用程式組態] 頁面中選取特定應用程式的存取原則，請遵循下列步驟。

   a 按一下**目錄**索引標籤。

   b 按一下應用程式。

   c 按一下左窗格中的**存取原則**。

   d 選取應用程式的存取原則，然後按一下**儲存**。

檢視 Citrix 發佈的資源的使用者和群組權利

您可以查看 VMware Identity Manager 使用者和群組獲授權的 Citrix 發佈的應用程式和桌面平台。桌面平台在 VMware Identity Manager 管理主控台中稱為傳遞群組。

重要事項 您無法使用 VMware Identity Manager 來對您的 Citrix 部署進行變更。如果 Citrix 管理員進行任何變更，例如授權新使用者使用 Citrix 發佈的資源，或新增伺服器陣列，您必須強制進行同步來將變更填入至 VMware Identity Manager。

先決條件

確認 VMware Identity Manager 已與您的 Citrix 部署整合。請參閱第 7 章提供存取 Citrix 發佈的資源。

從您的 Citrix 部署同步資訊 (包括權利) 至 VMware Identity Manager。您可以使用下列步驟強制進行同步：

1 登入 VMware Identity Manager 管理主控台。

2 選取**目錄**索引標籤。

3 按一下**管理桌面平台應用程式**，然後從下拉式功能表選取 **Citrix 發佈的應用程式**。

4 在 [已發佈的應用程式 - Citrix] 頁面上，按一下**立即同步**。

程序

1 登入 VMware Identity Manager 管理主控台。

2 檢視 Citrix 發佈的資源的使用者和群組權利。

Citrix 發佈的資源包含 Citrix 發佈的應用程式和 Citrix 發佈的桌面平台，也稱為傳遞群組。

選項	動作
檢視獲授權使用特定 Citrix 發佈的資源的使用者和群組。	a 按一下**目錄**索引標籤。 b 按一下**任何應用程式類型**並選取 **Citrix 發佈的應用程式**以檢視應用程式，或選取 **Citrix 發佈的傳遞群組**以檢視桌面平台。 c 按一下您想要列出其權利的 Citrix 發佈的資源名稱。 依預設會選取**權利**索引標籤。群組權利和使用者權利會列於不同的表格中。
檢視特定使用者或群組的 Citrix 發佈的資源權利清單。	a 按一下**使用者和群組**索引標籤。 b 按一下**使用者**索引標籤或**群組**索引標籤。 c 按一下個別使用者或群組的名稱。 d 按一下**應用程式**索引標籤。 獲授權之 Citrix 發佈的資源會列在 [Citrix 發佈的應用程式] 和 [Citrix 發佈的傳遞群組] 表格中。

在不同的瀏覽器中啟動 Citrix 發佈的資源

當使用者從 Workspace ONE 入口網站啟動 Citrix 發佈的桌面平台或應用程式時，會下載 ICA 檔案並傳遞給 Citrix Receiver。Citrix Receiver 是原生作業系統應用程式，可啟動 Citrix 發佈的桌面平台或應用程式。啟動經驗在不同的平台和瀏覽器上會有所不同。

啟動程序

視平台和瀏覽器而定，桌面平台或應用程式的啟動方式也會不同。在某些情況下，應用程式或桌面平台會直接啟動。在其他情況下，使用者必須先建立 .ica 檔案類型與 Citrix Receiver 的關聯，應用程式或桌面平台才能直接啟動。而在少數情況下，使用者需要按一下已下載的 ICA 檔案，以便啟動應用程式或桌面平台。請參閱表格，了解詳細資訊。

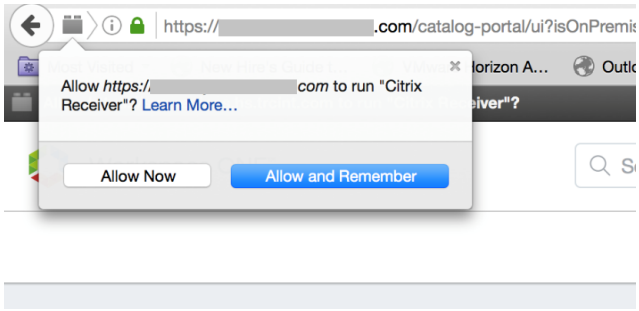
平台	瀏覽器	應用程式或桌面平台的啟動方式	需要採取的動作
Windows	Firefox	直接啟動應用程式或桌面平台	無
	Chrome	直接啟動應用程式或桌面平台。 **備註** 使用 Citrix 4.5 Receiver 和 XenDesktop 時，傳遞群組啟動具有一些已知問題。	無
	Internet Explorer	下載具有 .ica 副檔名的 ICA 檔案。建立檔案類型與 Citrix Receiver 的關聯後，應用程式或桌面平台會自動啟動。	在瀏覽器中，建立 .ica 檔案類型與 Citrix Receiver 的關聯。
	Edge	直接啟動應用程式或桌面平台。 **備註** 使用 Citrix 4.5 Receiver 和 XenDesktop 時，傳遞群組啟動具有一些已知問題。	無
Mac	Safari、Firefox	直接啟動應用程式或桌面平台	無

平台	瀏覽器	應用程式或桌面平台的啟動方式	需要採取的動作
	Chrome	直接啟動應用程式或桌面平台	無
Windows Surface	Chrome	下載具有 .ica 副檔名的 ICA 檔案。建立檔案類型與 Citrix Receiver 的關聯後，應用程式或桌面平台會自動啟動。	在瀏覽器中，建立 .ica 檔案類型與 Citrix Receiver 的關聯。
Android	Chrome	下載 ICA 檔案	按一下 ICA 檔案，啟動桌面平台或應用程式。
iOS	Safari	下載 ICA 檔案	按一下 ICA 檔案，啟動桌面平台或應用程式。
	Chrome	無法下載 ICA 檔案	不支援此案例。

在 Firefox 上允許 Citrix Receiver 外掛程式

在 Firefox 上，當使用者啟動 Citrix 發佈的應用程式時，系統會提示他們允許 Citrix Receiver 外掛程式。

允許 `https://IdentityManagerHostname 執行 Citrix Receiver?`



使用者必須按一下**現在允許**或**允許並記住**才能啟動應用程式。

升級對於 Citrix 發佈之資源整合的影響

在 VMware Identity Manager 升級或 Citrix 產品升級之後不需要進一步的設定，即可維護 VMware Identity Manager 與 Citrix 發佈的資源之間的整合。

若要升級 Integration Broker，您必須先將舊版本解除安裝，再安裝新版本。

若要重新安裝 Citrix Receiver，請參閱 Citrix 說明文件。

疑難排解 VMware Identity Manager 資源組態

8

您可以疑難排解您或使用者在設定 VMware Identity Manager 資源後遇到的問題。

本章節討論下列主題:

疑難排解 ThinApp 整合

使用這項資訊以疑難排解 VMware Identity Manager 中的 ThinApp 組態。

無法從使用者入口網站啟動 ThinApp 套件

當使用者嘗試從使用者入口網站啟動 ThinApp 套件，可能會出現一個瀏覽器訊息，提示使用者下載並安裝 VMware Identity Manager 桌面平台應用程式 (即使該應用程式已安裝並正在執行中)。

問題

安裝 VMware Identity Manager 桌面平台應用程式後，當使用者在該 Windows 系統上的瀏覽器中開啟使用者入口網站、登入並嘗試啟動 ThinApp 套件時，可能會出現一個訊息，指出必須在系統上安裝 VMware Identity Manager 桌面平台應用程式，並阻止 ThinApp 套件啟動。即使 Windows 系統上正在執行 VMware Identity Manager 桌面平台應用程式程序，仍會出現這個訊息。VMware Identity Manager 桌面平台應用程式可能會報告所有檔案都是最新的。

原因

此問題的發生有多個原因。

原因	說明
VMware Identity Manager 桌面平台瀏覽器外掛程式未正確安裝，或是針對使用者嘗試用來啟動 ThinApp 套件的瀏覽器，其瀏覽器視窗中未啟動此瀏覽器外掛程式。	由於必須安裝 VMware Identity Manager 桌面平台應用程式才能在 Windows 系統上執行 ThinApp 套件，因此在從使用者入口網站啟動 ThinApp 套件前，使用者入口網站會先使用一個瀏覽器外掛程式來確認是否已安裝此應用程式。當使用者按一下使用者入口網站中的 ThinApp 套件圖示，VMware Identity Manager 桌面平台瀏覽器外掛程式就會檢查應用程式是否已安裝，然後才啟動套件。如果未在瀏覽器中安裝並啟用瀏覽器外掛程式就無法執行驗證，接著會出現訊息，且不會啟動套件。 如果在 VMware Identity Manager 桌面平台安裝程序期間開啟了瀏覽器視窗，可能無法正確安裝該瀏覽器的瀏覽器外掛程式。如果使用者在瀏覽器的附加元件或外掛程式頁面中停用外掛程式，瀏覽器外掛程式就會變成停用。
針對使用者嘗試用來啟動 ThinApp 套件的瀏覽器，用來從該瀏覽器啟動 ThinApp 套件的自訂通訊協定處理常式已停用。	在 Workspace ONE 入口網站中，ThinApp 套件會以使用 `horizon://` 通訊協定的連結來表示。安裝 VMware Identity Manager 桌面平台應用程式時，安裝程式會登錄該 `horizon://` 通訊協定的通訊協定處理常式。通訊協定處理常式是一個名為 HorizonThinAppLauncher.exe 的可執行檔，並由登錄項目 `HKEY_CLASSES_ROOT\horizon\shell\open\command` 登錄為處理常式。當使用者嘗試從 Workspace ONE 入口網站中的圖示啟動 ThinApp 套件時，此 HorizonThinAppLauncher.exe 應用程式就會啟動。 如果使用者已停用瀏覽器中所有通訊協定處理常式的使用，或是停用 `horizon://` 通訊協定之處理常式的使用，ThinApp 套件就無法透過 Workspace ONE 入口網站中的圖示啟動。有些瀏覽器會在通訊協定處理常式啟動時顯示警告，並提供讓使用者選取以執行通訊協定處理常式的選項。使用者可能停用 `horizon://` 通訊協定處理常式之使用的其中一個狀況，就是當使用者第一次按下某個 ThinApp 套件圖示時，出現瀏覽器警告對話方塊要求執行通訊協定處理常式的權限，此時使用者選取**否**或類似選項因而阻止啟動，同時也選取了阻止所有此類連結啟動的**記住我的選擇**或類似選項。由於未授與執行通訊協定處理常式的權限且系統已記住此選擇，因此無法從 Workspace ONE 入口網站啟動任何 ThinApp 套件。

解決方案

1 確認使用者已使用該使用者的 VMware Identity Manager 使用者帳戶登入 VMware Identity Manager 桌面平台應用程式。

使用者可使用 Windows 系統匣中的 VMware Identity Manager 圖示來登入用戶端。

2 如果在系統上安裝應用程式後不久出現此問題，請關閉所有開啟的瀏覽器視窗、重新開啟瀏覽器、登入使用者入口網站，接著嘗試啟動 ThinApp 套件。

3 如果在關閉開啟的瀏覽器視窗並重新開啟瀏覽器後仍出現此問題，請確認瀏覽器外掛程式顯示在瀏覽器的外掛程式清單中並且在作用中。

瀏覽器	說明

Internet Explorer	對於 Internet Explorer，登錄的是 COM 伺服器而非瀏覽器外掛程式或附加元件。若要測試是否已安裝 COM 伺服器，請使用下列內容建立測試 HTML 檔案，並在 Internet Explorer 中開啟該檔案。由結果可得知是否已安裝 COM 伺服器。
	`<html>`
	`<script type="text/vbscript">`
	`On Error Resume Next`
	
	`dim objName`
	`objName = "HorizonAgentFinder.HorizonFinder"`
	`dim obj`
	`Set obj = CreateObject(objName)`
	
	`document.write(objName & " is ")`
	`if IsEmpty(obj) then`
	`document.write("not installed")`
	`else`
	`document.write("installed")`
	`end if`
	`</script>`
	`</html>`

Firefox	按一下**工具 > 附加元件**，開啟 Firefox 的 [附加元件管理員]。在 [外掛程式] 頁面上，確認 VMware Horizon Agent Finder 瀏覽器外掛程式已列出並設定為一律允許執行。
Chrome	開啟 [設定] 頁面並按一下**顯示進階設定 > 內容設定**，開啟 Chrome 的內容設定。按一下**管理個別外掛程式**，顯示外掛程式清單。確認 VMware Horizon Agent Finder 瀏覽器外掛程式已列出並設定為一律啟用。
Windows 版 Safari	按一下**輔助說明 > 已安裝的外掛程式**，開啟 Safari 的已安裝外掛程式清單。確認 VMware Horizon Agent Finder 瀏覽器外掛程式已列出。確認已為 Safari 啟用該外掛程式。

4 確認登錄項目 `HKEY_CLASSES_ROOT\horizon\shell\open\command` 存在，且具有指向所需通訊協定處理常式 (名為 HorizonThinAppLauncher.exe) 位置之路徑的值，此處即為 VMware Identity Manager 桌面平台應用程式在 Windows 系統上的安裝位置。

如果登錄項目不存在，或不具指向 VMware Identity Manager 桌面平台應用程式安裝位置的值，請解除安裝應用程式再重新安裝。

5 如果登錄項目存在，且具有指向 HorizonThinAppLauncher.exe 可執行檔之位置的值，請確認可執行檔存在於該位置，且未遭到移動或刪除。

如果登錄項目不存在，或不具指向 VMware Identity Manager 桌面平台應用程式安裝位置的值，請解除安裝應用程式再重新安裝。

6 如果登錄項目存在，且具有指向 HorizonThinAppLauncher.exe 可執行檔之位置的值，請確認登錄項目 `HKEY_CLASSES_ROOT\horizon` 的 (預設值) 值具有 URL:horizon Protocol 的 [資料] 值，且 `HKEY_CLASSES_ROOT\horizon` 項目的 URL Protocol 值存在。

如果 `HKEY_CLASSES_ROOT\horizon` 登錄項目之 (預設值) 值的 [資料] 值不是設定為 URL:horizon Protocol，請更新 [資料] 值以將其設定為 URL:horizon Protocol。如果 `HKEY_CLASSES_ROOT\horizon` 項目的 URL Protocol 值不存在，您可使用值名稱 URL Protocol 和無值資料來建立此值。

7 確定使用者是否已停用瀏覽器的 horizon:// 通訊協定，或是瀏覽器中的所有通訊協定處理常式都已停用，若是，請依據貴組織需求，啟用瀏覽器的通訊協定處理常式。

在大部分情況下，瀏覽器會依賴登錄中的設定來取得該 Windows 系統可用之通訊協定處理常式的相關資訊。對於某些瀏覽器，當使用者按下與通訊協定處理常式相關聯的連結時，會出現對話方塊提示，詢問使用者類似 `Do you want to allow this website to open a program on your computer?` 或 `This link needs to be opened with an application` 之類的問題，或需要啟動外部應用程式以處理連結的類似陳述。通常此對話方塊會提供選項，讓使用者選擇不啟動外部應用程式以及記住所有該類型連結的選擇。將啟動與通訊協定處理常式相關聯之應用程式的能力重新啟用的步驟，通常視瀏覽器類型而異。請參閱使用者瀏覽器類型的說明文件，了解如何啟用該瀏覽器類型的通訊協定處理常式。

疑難排解 Horizon 整合

使用這項資訊以疑難排解 VMware Identity Manager 中的 Horizon 7、Horizon 6 或 View 組態。

無法同步化 View 資源

Horizon 7、Horizon 6 或 View 資源同步化至 VMware Identity Manager 的作業不成功，或十分緩慢。

問題

您無法同步 Horizon 7、Horizon 6 或 View 資源與 VMware Identity Manager。同步化的速度十分緩慢，或程序不成功並且顯示如下的錯誤。

因 `View` 連線伺服器有問題而無法完成 `View` 同步：無法對 `View` 代理進行驗證，目錄有問題

因 `View` 連線伺服器有問題而無法完成 `View` 同步：無法對網繭中的任何代理查詢集區和權利資訊。請檢查 `View` 網繭的連線

原因

如果 `/etc/krb5.conf` 檔案未包含正確的網域資訊，就會發生此問題。

解決方案

如需解決此問題的相關資訊，請參閱知識庫文章 2091744。高階工作包括下列項目。

1 編輯 `domain_krb.properties` 檔案，以新增 View 和 VMware Identity Manager 所使用的網域。

2 編輯 `krb5.conf` 檔案，並以 `domain_krb.properties` 檔案中使用的相同「網域-主機」值更新 `realms` 區段。

重要事項 如果您設定了多個 VMware Identity Manager 應用裝置以組成叢集，則在您將複製的應用裝置加入至網域後，您必須再次使用網域資訊來更新 `krb5.conf` 檔案。

使用者無法啟動 View 應用程式或桌面平台

使用者無法從 VMware Identity Manager 使用者入口網站啟動 Horizon 7、Horizon 6 或 View 應用程式。

問題

使用者無法從 VMware Identity Manager 使用者入口網站啟動 Horizon 7、Horizon 6 或 View 應用程式，且使用者介面中顯示下列錯誤：

```
啟動資源時發生錯誤。請聯絡您的 IT 管理員。
```

原因

如果 View 連線伺服器執行個體上的 SAML 中繼資料在上次同步後已到期，即可能發生此錯誤。

解決方案

1. 在管理主控台中，按一下**目錄**索引標籤。
2. 按一下**管理桌面平台應用程式 > View 應用程式**。
3. 在 [View 集區] 頁面的**網繭和同步**索引標籤中，按一下**立即同步**，將 View 資源再次同步至 VMware Identity Manager。

疑難排解 Citrix 發佈之資源整合

使用這項資訊以疑難排解 VMware Identity Manager 中 Citrix 發佈的資源組態。

存取 Citrix 發行的資源的使用者收到加密錯誤

VMware Identity Manager 中的 XenApp ICA 內容必須包含與伺服器陣列中 XenApp 伺服器上所設定相同加密層級的加密內容集，否則使用者會無法存取其 Citrix 發行的應用程式或桌面平台。

問題

當使用者從 VMware Identity Manager 連線至 Citrix 發行的資源時，系統會顯示下列錯誤訊息。

```
您沒有適當的加密層級可存取此工作階段
```

原因

VMware Identity Manager 未設定加密層級。如果 XenApp 伺服器上的加密層級設定為高於 Citrix-Receiver 中使用的預設設定，使用者會看見此錯誤。

```
您必須在 Workspace 中設定更高的加密層級。
```

解決方案

1. 登入管理主控台。
2. 按一下**目錄**索引標籤上的箭頭，然後選取**設定**。
3. 選取 **Citrix 發行的應用程式**。

4 同時在 **ICA 組態**和 **Netscaler ICA 組態**索引標籤中進行下列變更。

a 編輯 **ICA 用戶端內容**文字方塊。若要將加密層級設定為 128，請輸入

EncryptionLevelSession=EncRC5-128。

b 編輯 **ICA 啟動內容**文字方塊。若要將加密層級設定為 128，請輸入

[EncRC5-128]

DriverNameWin16=pdc128w.dll

DriverNameWin32=pdc128n.dll。

Citrix 發行的資源在 VMware Identity Manager 無法使用

Integration Broker 與 PowerShell SDK 之間的通訊問題，可能會使得 Citrix 發行的應用程式和桌面平台不會出現在 VMware Identity Manager 目錄中。

問題

整合 Citrix 與 VMware Identity Manager 之後，Citrix 發行的資源未出現在 VMware Identity Manager 目錄中。

原因

Integration Broker 設定可能會出現組態問題，使得無法正確與 PowerShell SDK 通訊。

解決方案

您可以在瀏覽器中指定 URL 以疑難排解存在 Integration Broker 組態問題的位置。此疑難排解方法可以幫助您識別問題是否為下列區域中的組態問題。

- Citrix 伺服器陣列
- Citrix 發佈的資源
- 資源權利

如果網頁未顯示預期的輸出，則它會顯示錯誤，並將資訊新增至 Integration Broker 記錄。檢閱 Integration Broker 記錄以繼續疑難排解程序。

程序

1 使用瀏覽器查看 Citrix 伺服器陣列資訊。

a 在瀏覽器中，輸入如下的其中一個 URL，將預留位置取代為適當資訊。

- Citrix Server Farm 7.x

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=*XenAppServerHostname*&xenappversion=Version7x

- Citrix Server Farm 6.5

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=*XenAppServerHostname*&xenappversion=Version65orLater

- Citrix Server Farm 5.5 或 6.0

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=*XenAppServerHostname*&xenappversion=Legacy

b 檢閱網頁的內容，並且如果必要，請檢閱 Integration Broker 記錄。

如果已正確設定 Integration Broker，頁面會顯示如下所示的 Citrix 伺服器陣列資訊。

"[{\"FarmName\":\"test data\",\"ServerVersion\":\"6.0.6410\",\"AdministratorType\":\"Full\",\"SessionCount\":\"2\",\"MachineName\":\"test data\"}]"

如果網頁未顯示伺服器陣列資訊，記錄資訊會傳送至 Integration Broker。若要進一步疑難排解問題，請在 `%programdata%/VMware/HorizonIntegrationBroker` 檢閱 Integration Broker 主機上的記錄。

2 使用瀏覽器列出伺服器陣列中所有由 Citrix 發行的資源。

a 在瀏覽器中，輸入如下的其中一個 URL，將預留位置取代為適當資訊。

- Citrix Server Farm 7.x

  若要列出所有的應用程式：

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/applications?computerName=*XenAppServerHostname*&xenappversion=Version7x

  若要列出所有的傳遞群組：

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/deliveryGroups?computerName=*XenAppServerHostname*&xenappversion=Version7x

- Citrix Server Farm 6.5

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/applications?computerName=*XenAppServerHostname*&xenappversion=Version65orLater

- Citrix Server Farm 5.5 或 6.0

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/applications?computerName=*XenAppServerHostname*&xenappversion=Legacy

b 檢閱網頁的內容，並且如果必要，請檢閱 Integration Broker 記錄。

如果已正確設定 Integration Broker，頁面會顯示 Citrix 伺服器陣列中所有資源的清單。

如果網頁未顯示資源的清單，記錄資訊會傳送至 Integration Broker。若要進一步疑難排解問題，請在 `%programdata%/VMware/HorizonIntegrationBroker` 檢閱 Integration Broker 主機上的記錄。

3 使用瀏覽器檢查單一 Citrix 發行資源的權利。

a 在瀏覽器中，輸入如下的其中一個 URL，將預留位置取代為適當資訊。

將 *ApplicationName* 預留位置以您指定的應用程式名稱取代。

- Citrix Server Farm 7.x

  若要檢查應用程式：

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?computerName=*XenAppServerHostname*&xenappversion=Version7x&appName=*ApplicationName*

  若要檢查傳遞群組：

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/deliveryGroup/entitlements?computerName=*XenAppServerHostname*&xenappversion=Version7x&deliveryGroupName=*deliveryGroupName*

- Citrix Server Farm 6.5

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?computerName=*XenAppServerHostname*&xenappversion=Version65orLater&appName=*ApplicationName*

- Citrix Server Farm 5.5 或 6.0

  https://*IBhostname*/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?computerName=*XenAppServerHostname*&xenappversion=Legacy&appName=*ApplicationName*

b 檢閱網頁的內容，並且如果必要，請檢閱 Integration Broker 記錄。

如果已正確設定 Integration Broker，頁面將會列出您所指定應用程式或傳遞群組的所有權利清單。

如果網頁未顯示權利的清單，記錄資訊會傳送至 Integration Broker。若要進一步疑難排解問題，請在 `%programdata%/VMware/HorizonIntegrationBroker` 檢閱 Integration Broker 主機上的記錄。

使用者啟動 Citrix 發行的資源時，瀏覽器顯示 500 內部伺服器錯誤

Citrix 伺服器陣列與 VMware Identity Manager 組態之間的不相符可能會造成 Citrix 發行的資源啟動失敗。

問題

Citrix 發行的資源啟動失敗，因為瀏覽器顯示 500 內部伺服器錯誤。

原因

在 管理主控台 中提供的 Citrix 伺服器陣列資訊不符合 Citrix 伺服器組態時，即會發生 500 錯誤。

解決方案

1 記下與您 VMware Identity Manager 部署整合的每個伺服器陣列的傳輸類型、連接埠號碼和 SSL 轉接埠號碼的設定。

2 登入 VMware Identity Manager 管理主控台。

3 選取**目錄**索引標籤。

4 按一下**管理桌面平台應用程式**，然後選取 **Citrix 發行的應用程式**。

5 在**伺服器陣列**區段中，變更每個伺服器陣列的**傳輸類型**、**連接埠**和 **SSL 轉接埠**設定，以符合您的 Citrix 伺服器組態中的設定。

記憶體問題導致 Integration Broker 無法設定正確組態

將 VMware Identity Manager 與 Citrix 伺服器陣列 6.0 版和更早版本整合時，如果分配給 PowerShell SDK 的記憶體不足將會導致錯誤。

問題

發出 `Invoke-Command` 命令來確認 PowerShell 遠端功能時，出現與記憶體不足相關的錯誤。系統指示您在 GUID-A51BFD94-9975-41C7-A9E5-ADB854ADAA6E#GUID-A51BFD94-9975-41C7-A9E5-ADB854ADAA6E 期間發出 `Invoke-Command` 命令。

原因

在執行 PowerShell 遠端功能的 Windows 系統上，對於 Citrix 發行的資源數量來說，分配給 PowerShell SDK 的記憶體可能不足。

解決方案

您可以提高分配給 PowerShell SDK 的記憶體。

程序

1 出現此錯誤時，請發出命令以提高分配的記憶體。例如，

```
winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="1024"}'
```

2 重新發出 `Invoke-Command` 命令並完成工作。

啟動 XenApp 7.x 桌面平台時發生資源無法使用錯誤

使用者無法啟動 XenApp 7.x 桌面平台。出現資源無法使用錯誤。

問題

從 XenApp 7.x 傳遞群組啟動桌面平台時，使用者看見資源無法使用錯誤。

原因

使用 Citrix Machine Creation 伺服器建立的機器目錄依預設會將電源管理切換至「開啟」。這會導致機器在登出後即關閉。

解決方案

1 為 Citrix XenApp 7.x 伺服器中的傳遞群組關閉電源管理選項。

2 將 Citrix 發佈的資源再次重新同步至 VMware Identity Manager 服務。

在 Windows 7 上無法從 Citrix XenDesktop 伺服器陣列啟動桌面平台

在 Windows 7 上，如果為 Integration Broker 啟用了 SSL，使用者無法從 Citrix XenDesktop 伺服器陣列啟動桌面平台。

問題

如果為 Integration Broker 啟用了 SSL，當使用者在 Windows 7 上啟動桌面平台時，有時桌面平台會無法啟動，並顯示下列錯誤：「*desktop* 的連線失敗，狀態 1030」。過去已觀察到此問題會間歇性地出現在 Firefox 上，但其他瀏覽器也可能發生此問題。

解決方案

如需此問題的詳細資訊，請參閱 Citrix 知識中心文章：對 Windows 7 映像的 1030 錯誤進行疑難排解。

XML 連接埠設定不正確時，Citrix 發佈的資源即無法啟動

如果 XML 連接埠在 VMware Identity Manager 中的設定不正確，則從 Citrix 7.x 或 6.x 伺服器陣列啟動 Citrix 發佈的資源將會失敗。

問題

如果 XML 連接埠在 VMware Identity Manager 中的設定不正確，則從 Citrix 7.x 或 6.x 伺服器陣列啟動 Citrix 發佈的資源將會失敗。

解決方案

確定 XML 連接埠已正確設定。

在 XenApp 6.x 或更早版本的環境中，要求 Citrix 管理員執行 `CTXXMLS.EXE` 以確認連接埠，或在 XenApp 管理伺服器上瀏覽至登錄內的下列位置：

```
HKLM/SYSTEM/CurrentControlSet/Services/CtxHttp | TcpPort=
```

確認連接埠號碼。依預設連接埠會設為 80，但通常會變更為 8080 或 88。請確認**目錄 > 管理桌面平台應用程式 > Citrix 發佈的應用程式**頁面的 VMware Identity Manager Citrix 組態中已設定正確的連接埠。

針對 XenDesktop 7.x，請參閱 https://support.citrix.com/article/CTX127945 以取得確認 XML 連接埠的相關資訊。

如果有限可見度群組並未包含任何使用者或群組，則 Citrix 資源同步便會失敗

如果已選取 [有限可見度群組] 設定，但其中並未包含任何 AD 使用者或群組，則 Citrix 資源同步便會失敗。

問題

在 XenDesktop 與 XenApp 7.9 和更新版本中，如果已選取 [有限可見度群組] 設定，但其中並未包含任何使用者或群組，則同步至 VMware Identity Manager 的作業便會失敗。

原因

若已設定，則 [有限可見度群組] 必須包含使用者或群組。

解決方案

1 透過執行下列 PowerShell 命令以找出應用程式的實際名稱：

```
asnp citrix*
Get-brokerapplication -browsername nameOfCitrixPublishedResource
```

在顯示的應用程式詳細資料中，找出應用程式的名稱。

2 在 Citrix Studio 中找出具有該名稱的應用程式、編輯 [有限可見度] 內容，然後將使用者和群組新增至清單。

如果站台中已發佈的應用程式或桌面平台並未包含有效的使用者，則會發生同步問題

如果 Citrix 發佈的應用程式或桌面平台並未包含有效使用者，則同步至 VMware Identity Manager 的作業即無法正常運作。

問題

站台中所有 Citrix 發佈的應用程式和桌面平台皆必須包含有效的使用者。如果刪除了某個使用者或群組，但該使用者或群組並未從 Citrix 發佈的資源中移除，則 Citrix 應用程式或桌面平台會顯示孤立的 SID。這會使同步至 VMware Identity Manager 的作業無法正常運作。

您可以使用下列 API 來檢查此問題：

```
http://CitrixBrokerFQDN:80/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?computerName=IBFQDN&xenappversion=VersionNumber&appName=applicationName
```

產生的檔案會包含空的資源。範例輸出：

```
"[{\"IncludedUsers\":\"DomainName\\\\USERNAME:User
$S-1-5-21-1097426297-1557994628-1672037986-53944:Group\"}]"
```

原因

站台中某些已發佈的應用程式或桌面平台並未包含有效的使用者。

解決方案

確定站台中所有 Citrix 發佈的應用程式和桌面平台皆包含有效的使用者。

Citrix 權利未顯示在 VMware Identity Manager 中

Citrix 權利未顯示在 VMware Identity Manager 中。

問題

應用程式或傳遞群組的權利已設定於 Citrix 伺服器上，但並未顯示在 VMware Identity Manager 中。

原因

有權使用應用程式或傳遞群組的使用者和群組可能並未同步至 VMware Identity Manager。

解決方案

請確保使用者和群組已同步至 VMware Identity Manager。

1 登入 Citrix 管理主控台，並找出沒有任何權利的應用程式。

2 記下有權在 Citrix 管理主控台中啟動應用程式的 Active Directory 使用者和群組。

3 登入 VMware Identity Manager 管理主控台、按一下**使用者和群組**索引標籤，並確認使用者和群組顯示在清單中。

您也可以使用頁面右上方的搜尋方塊。

4 如果使用者和群組已顯示，請從**目錄 > 管理桌面平台應用程式 > Citrix 發佈的應用程式**頁面再次同步 Citrix 資源。

備註 在您同步 Citrix 資源之前，使用者和群組必須存在於 VMware Identity Manager 中。如果不存在，則同步將會執行，但權利將不會更新。

5 如果使用者和群組不存在於 VMware Identity Manager 中，請執行下列動作。

a 檢查使用者和群組於 Active Directory 中的所在位置 (使用「Active Directory 使用者和電腦嵌入式管理單元」)。

b 在 VMware Identity Manager 管理主控台中，在目錄的**同步設定**頁面中更新使用者和群組的 AD 同步 DNS。

c 當使用者和群組顯示在 VMware Identity Manager 管理主控台中時，請再次同步 Citrix 資源。

同步完成後，權利即會顯示在 VMware Identity Manager 中。

在同步期間因未設定應用程式集區身分識別而發生例外狀況

在將 Citrix 資源同步至 VMware Identity Manager 期間，由於 Integration Broker 設定中出現一般錯誤，即為錯誤的應用程式集區設定了 [身分識別] 設定而發生例外狀況。

問題

在同步期間，Integration Broker 記錄中發生下列例外狀況。

```
IntegrationBrokerLogger Error 1002 2017-04-04 19:10:38,936 (16)
HznXenIntegrationBroker.ApplicationException.ServiceErrorHandler – 連線至遠端伺服器失敗，並出現下列錯誤訊息：用戶端無法連線至要求中指定的目的地。請確認目的地上的服務正在執行，並接受要求。請參閱在目的地上執行之 WS-Management 服務 (通常為 IIS 或 WinRM) 的記錄和說明文
```

件。如果目的地執行的是 WinRM 服務，請在目的地上執行下列命令，以分析及設定 WinRM 服務：「winrm quickconfig」。如需詳細資訊，請參閱位於 System.Management.Automation.Runspaces.AsyncResult.EndInvoke() 的 about_Remote_Troubleshooting 說明主題

原因

如果未正確設定 [身分識別] 設定，或為錯誤的應用程式集區進行此設定，即會發生此錯誤。

解決方案

請在連結至 Integration Broker 的應用程式集區中設定 [身分識別] 設定。這可能與預設應用程式集區不同。

若要確認正確的應用程式集區：

1 在 [IIS 管理員] 中，按一下左窗格中的**應用程式集區**。

2 在應用程式集區上按一下滑鼠右鍵，然後選取**檢視應用程式**。

3 確認 Integration Broker 顯示在應用程式清單中。

若要設定應用程式集區的 [身分識別] 設定，請遵循設定 IIS 管理員設定中的指示。

在 Citrix 資源啟動期間未建立 ICA 檔案

在 Citrix 資源啟動期間未建立 ICA 檔案，且發生例外狀況。

問題

當使用者嘗試啟動 Citrix 資源時，系統未建立 ICA 檔案，且 Integration Broker 記錄中顯示如下的例外狀況。

```
IntegrationBrokerLogger Information 1004 2017-05-02 11:50:42,093 (8)
HznXenIntegrationBroker.API.RestServiceImpl - Get ICA file contents for
AppNameCitrix.MPS.App.XA65Test.Airwatch Notepad Test, Farm Name: XA65Test, Server
Name: serverName, Username: user1 IntegrationBrokerLogger Error 1002 2017-05-02
11:50:42,093 (8) HznXenIntegrationBroker.ApplicationException.ServiceErrorHandler -
WebPNBuilder implementation class WebPNImpl!
com.citrix.wing.webpnimpl.WebPNBuilderImpl not found at
com.citrix.wing.webpn.WebPNBuilder.getInstance() at
HznXenIntegrationBroker.XenAppSDK.Impl.XenAppSDKClient.CreateUserContext(UserPrincip
al userPrincipal, String appName, Configuration configuration) at
HznXenIntegrationBroker.XenAppSDK.Impl.XenAppSDKClient.GenerateICAFileCommon(UserPri
ncipal userPrincipal, String appName, Configuration configuration) at
HznXenIntegrationBroker.XenAppSDK.Impl.XenAppSDKClient.GenerateICAFile(UserPrincipal
userPrincipal, String farmName, String serverName, String serverPort, String
appName, XMLServiceTransportProtocol xmlserviceTransportProtocol, Int32
sslRelayPort)
```

解決方案

在 Integration Broker 伺服器中重新安裝 Microsoft Visual J# 2.0。

重新啟動 Integration Broker

如果 Integration Broker 無法回應，請在 Windows Server 上重新啟動 IIS。

問題

Integration Broker 無法回應，且需要重新啟動。

解決方案

1 以管理員身分開啟 [命令提示字元] 視窗。

2 輸入 `iisreset`。