在 DMZ 中部署 VMware Identity Manager

VMware Identity Manager 2.9.1
VMware Identity Manager 2.8

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/

VMware 網站還提供了最新的產品更新。

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

在 DMZ 中部署 VMware Identity Manager

*《在 DMZ 中部署 VMware Identity Manager》*提供如何在 DMZ (而非內部網路) 中部署 VMware Identity Manager 的相關資訊。如需在內部網路中部署 VMware Identity Manager 的相關資訊，請參閱*《安裝和設定 VMware Identity Manager》*。

主要對象

本資訊是針對熟悉 VMware 技術 (尤其是 vCenter™、ESX™ 和 vSphere®)、網路功能概念、Active Directory 和資料庫的資深 Windows 和 Linux 系統管理員所撰寫。SUSE Linux 11 是 VMware Identity Manager 和 VMware Identity Manager Connector 虛擬應用裝置的基礎作業系統。

若要您想要實作這些功能，熟悉 RSA 調適性驗證、RSA SecurID 和 RADIUS 等其他技術也會有所幫助。

VMware Technical Publications Glossary

VMware 技術出版品將為您提供可能不熟悉的術語詞彙。如需 VMware 技術說明文件中所用術語的定義，請前往 http://www.vmware.com/support/pubs。

1 部署模型

有兩個主要類型的部署模型可用來在 DMZ 中部署 VMware Identity Manager，一個可與 VMware AirWatch® 部署整合，一個不需要 AirWatch 而會使用 VMware Identity Manager Connector。

如果您需要在其中一個模型中不受支援的功能，您也可以結合部署模型。

- 使用 AirWatch Cloud Connector 的部署模型

  如果您有現有的 AirWatch 部署，您可以將其與 VMware Identity Manager 快速整合。在此模型中，使用者和群組會從您的企業目錄進行同步，而使用者驗證會由 AirWatch 進行處理。您需要在 DMZ 中部署 VMware Identity Manager。

  請注意，在此模型中不支援將 VMware Identity Manager 與 Horizon 7 之類的資源和 Citrix 發佈的資源整合。僅支援與 Web 應用程式和原生行動應用程式進行整合。

  請參閱"使用 AirWatch Cloud Connector 的內部部署模型," 第 8 頁。

- 在僅限輸出連線模式中使用 VMware Identity ManagerConnector 的部署模型

  在不需要 AirWatch 部署的情況下，您可以將 VMware Identity Manager 伺服器虛擬應用裝置安裝在 DMZ 中，並將 VMware Identity Manager Connector 虛擬應用裝置安裝在企業網路中。連接器會連接伺服器與內部部署服務，例如 Active Directory。連接器會以僅限輸出連線模式安裝，且不需要開啟輸入防火牆連接埠 443。在此模型中，使用者和群組會從您的企業目錄進行同步，而使用者驗證會由 VMware Identity ManagerConnector 進行處理。

  請參閱"在僅限輸出連線模式中使用 VMware Identity Manager Connector 的內部部署模型," 第 10 頁。

  - 將 Kerberos 驗證支援新增至您的 VMware Identity ManagerConnector 部署

    您可以將內部使用者的 Kerberos 驗證 (需要輸入連線模式) 新增至您根據僅限輸出連線模式連接器的部署。

    請參閱"將 Kerberos 驗證支援新增至您的部署," 第 12 頁。

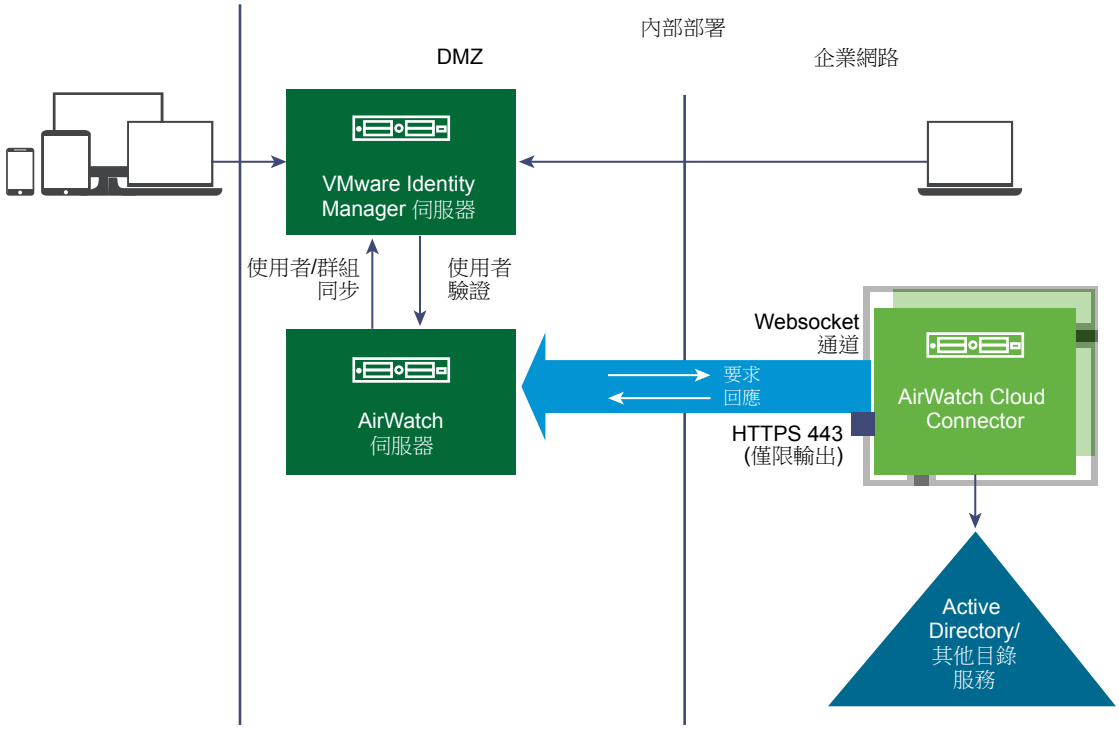
本章節討論下列主題:

使用 AirWatch Cloud Connector 的內部部署模型

如果您有現有的 AirWatch 部署，您可以將其與 VMware Identity Manager 整合。您需要在 DMZ 中部署 VMware Identity Manager 虛擬應用裝置。在此模型中，使用者和群組會從您的企業目錄進行同步，而使用者驗證會由 AirWatch 進行處理。

請注意，在此模型中不支援將 VMware Identity Manager 與 Horizon 7 等資源或 Citrix 發佈的資源整合。僅支援與 Web 應用程式和原生行動應用程式進行整合。

圖 1-1 使用 AirWatch Cloud Connector 的部署



必要條件

您必須具有下列元件：

- 一個 AirWatch 伺服器部署
- 一個部署於內部、並且與您的企業目錄整合的 AirWatch Cloud Connector 執行個體

連接埠需求

VMware Identity Manager 伺服器需要下列連接埠：

- 輸入 443 (HTTPS)
- 輸入 88 (TCP/UDP) - 僅限 iOS
- 輸入 5262 (TCP/UDP) - 僅限 Android

如需 AirWatch 部署需求，請參閱 AirWatch 說明文件。

支援的驗證方法

此部署模型支援下列驗證方法。以下是可透過 VMware Identity Manager 內建身分識別提供者來使用的方法。

- 密碼 (AirWatch Connector)
- 行動 SSO (iOS 版)
- 行動 SSO (Android 版)
- 裝置符合性 (與 AirWatch)
- 憑證 (雲端部署)
- VMware Verify

支援的目錄整合

您可以整合您的企業目錄與 AirWatch。請參閱 AirWatch 說明文件，以瞭解支援的目錄類型。

支援的資源

在此部署模型中，您可以將下列類型的資源與 VMware Identity Manager 整合：

- Web 應用程式
- 原生行動應用程式

在此部署模型中，您無法將下列資源與 VMware Identity Manager 整合：

- Horizon 7、Horizon 6 或 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
- Horizon Air - 雲端主控應用程式和桌面平台

其他資訊

- 第 2 章, “在 DMZ 中部署 VMware Identity Manager,” 第 13 頁
- 《*VMware Identity Manager 管理指南*》中的整合 AirWatch 與 VMware Identity Manager
- AirWatch 說明文件

在僅限輸出連線模式中使用 VMware Identity Manager Connector 的內部部署模型

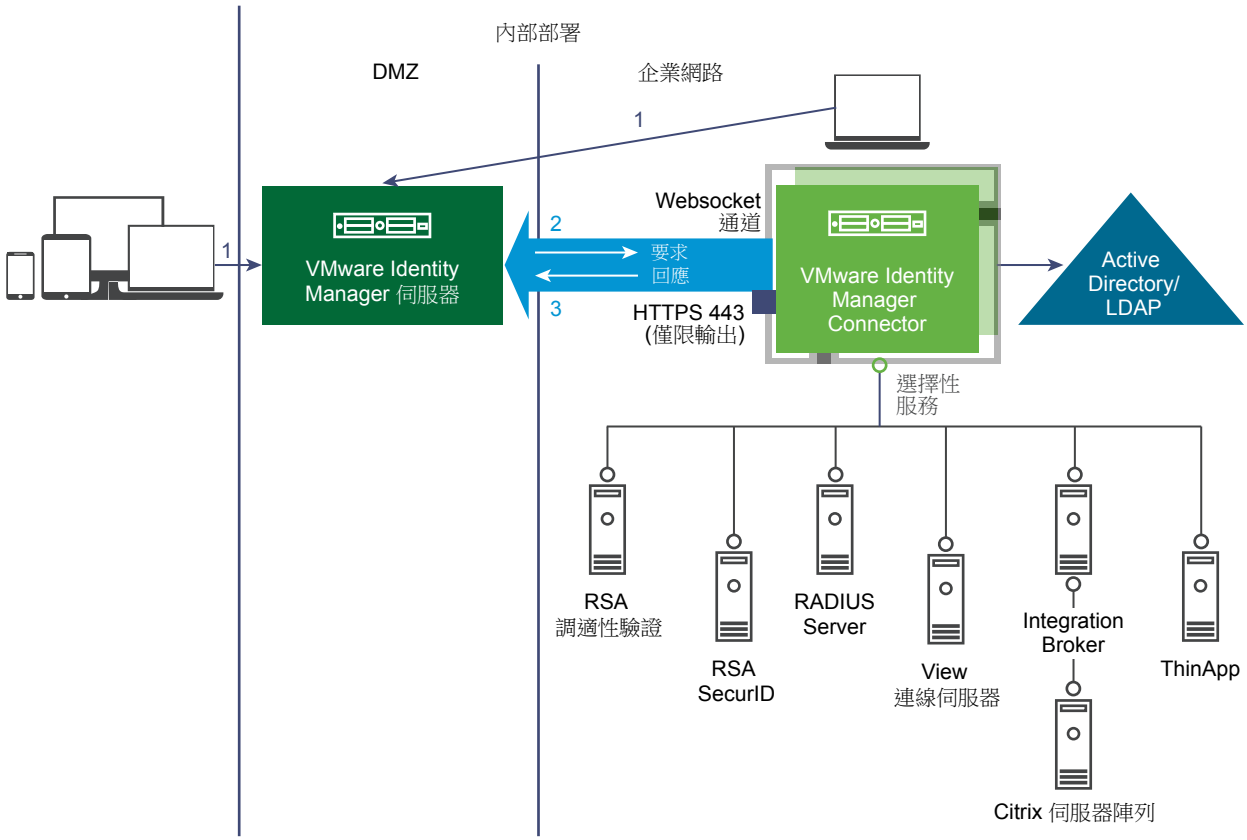
在此模型中，您需要在 DMZ 中安裝 VMware Identity Manager 虛擬應用裝置。您也需要在企業網路中使用僅限輸出連線模式來安裝獨立 VMware Identity ManagerConnector 虛擬應用裝置。此模型不包含任何 AirWatch 元件。

使用者和群組會從您的企業目錄進行同步，而使用者驗證會由獨立 VMware Identity ManagerConnector 進行處理。連接器也可將資源 (例如 Horizon 7 桌面平台和應用程式) 同步至 VMware Identity Manager 服務。

備註 有些驗證方法不需要連接器，而是由服務直接管理。

重要事項 請使用獨立連接器 (而非與 VMware Identity Manager 應用裝置整合的連接器) 進行使用者和群組的同步以及使用者驗證。

圖 1-2 在輸出模式中使用 VMware Identity Manager Connector



連接埠需求

VMware Identity Manager 伺服器需要下列連接埠：

- 輸入 443 (HTTPS)
- 輸入 88 (TCP/UDP) - 僅限 iOS
- 輸入 5262 (TCP/UDP) - 僅限 Android

VMware Identity ManagerConnector 會以僅限輸出連線模式安裝，且不需要開啟輸入連接埠 443。連接器會透過 Websocket 型通訊通道與 VMware Identity Manager 服務通訊。

如需所使用連接埠的完整清單，請參閱第 2 章, “在 DMZ 中部署 VMware Identity Manager,” 第 13 頁和第 3 章, “在企業網路中部署 VMware Identity ManagerConnector,” 第 15 頁。

支援的驗證方法

此部署模型支援所有的驗證方法。其中有部分驗證方法不需要連接器，而會透過內建身分識別提供者直接由服務進行管理。

- 密碼 - 使用連接器
- RSA 調適性驗證 - 使用連接器
- RSA SecurID - 使用連接器
- RADIUS - 使用連接器
- 憑證 (雲端部署) - 透過內建身分識別提供者
- VMware Verify - 透過內建身分識別提供者
- 行動 SSO (iOS) - 透過內建身分識別提供者
- 行動 SSO (Android) - 透過內建身分識別提供者
- 透過第三方身分識別提供者的輸入 SAML

備註 如需使用 Kerberos 的相關資訊，請參閱“將 Kerberos 驗證支援新增至您的部署,” 第 12 頁。

備註 此部署模型不支援透過連接器的憑證驗證。您可以使用「憑證 (雲端部署)」驗證方法。

支援的目錄整合

在此部署模型中，您可以將下列類型的企業目錄與 VMware Identity Manager 服務整合：

- Active Directory over LDAP
- Active Directory, 整合式 Windows 驗證
- LDAP 目錄

  如果您計劃要整合 LDAP 目錄，請參閱《*安裝和設定 VMware Identity Manager*》中的〈與 LDAP 目錄整合〉的相關限制。

或者，您可以使用下列方法在 VMware Identity Manager 服務中建立使用者：

- 直接在 VMware Identity Manager 服務中建立本機使用者。
- 使用 Just-in-Time 佈建，在登入時使用第三方身分識別提供者所傳送的 SAML 判斷提示動態地在 VMware Identity Manager 服務中建立使用者。

支援的資源

在此部署模型中，您可以將下列類型的資源與 VMware Identity Manager 服務整合：

- Web 應用程式
- Horizon 7、Horizon 6 或 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
- Horizon Air - 雲端主控的應用程式和桌面平台 (技術預覽)

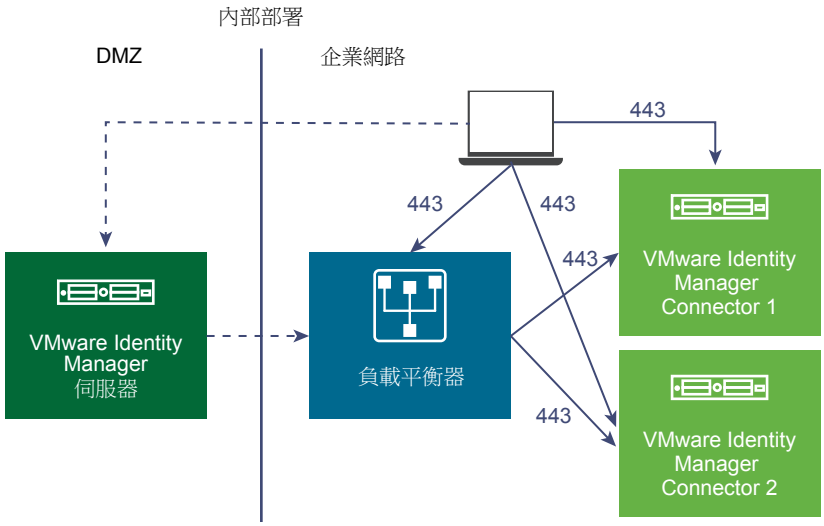
其他資訊

- 第 2 章, “在 DMZ 中部署 VMware Identity Manager,” 第 13 頁和第 3 章, “在企業網路中部署 VMware Identity ManagerConnector,” 第 15 頁
- 目錄
  - *《安裝和設定 VMware Identity Manager》*中的〈與您的企業目錄整合〉
  - *《安裝和設定 VMware Identity Manager》*中的〈使用本機目錄〉
  - *《VMware Identity Manager 管理》*中的〈Just-in Time 使用者佈建〉
- *《VMware Identity Manager 管理》*中的〈在 VMware Identity Manager 中設定使用者驗證〉
- *《在 VMware Identity Manager 中設定資源》*

將 Kerberos 驗證支援新增至您的部署

您可以將內部使用者的 Kerberos 驗證 (需要輸入連線模式) 新增至以 VMware Identity Manager 僅限輸出連線模式連接器為基礎的部署。您可以設定相同的連接器，以便對來自內部網路的使用者使用 Kerberos 驗證，而對來自外部的使用者使用另一個驗證方法。若要這麼做，請根據網路範圍定義驗證原則。

圖 1-3 新增 Kerberos 驗證



請注意，設定 Kerberos 驗證的高可用性須執行不同的程序。

如需詳細資訊，請參閱 “將 Kerberos 驗證支援新增至您的 VMware Identity Manager Connector 部署,” 第 25 頁。

在 DMZ 中部署 VMware Identity Manager

2

如果您不想在企業網路中部署 VMware Identity Manager 虛擬應用裝置，則可以將其部署在 DMZ 中。在 DMZ 中部署 VMware Identity Manager 應用裝置時，您也需要在企業網路中使用僅限輸出連線模式來部署獨立 VMware Identity Manager Connector。

系統和網路組態需求

除了此處列出的差異以外，在 DMZ 中部署 VMware Identity Manager 的網路組態需求皆與在企業網路中部署 VMware Identity Manager 的需求相似，相關說明請參閱《*安裝和設定 VMware Identity Manager*》中的系統和網路組態需求與準備部署 VMware Identity Manager。

- 您無須對企業網路中的任何應用裝置開啟輸入防火牆連接埠。

  VMware Identity Manager 虛擬應用裝置會部署在 DMZ 中。VMware Identity Manager Connector 會使用僅限輸出連線模式部署在企業網路中，並且透過 Websocket 型通訊通道與服務通訊。

- 您不需要部署反向 Proxy 或負載平衡器，即可啟用對 VMware Identity Manager 的外部存取。
- 僅在為 VMware Identity Manager 虛擬應用裝置設定高可用性和備援時才需要負載平衡器。
- 使用的連接埠如下。您的部署可能僅需要其中一個子集。

連接埠	來源	目標	說明
443	負載平衡器	VMware Identity Manager 虛擬應用裝置	HTTPS
443	VMware Identity Manager 虛擬應用裝置	VMware Identity Manager 虛擬應用裝置	HTTPS
443	瀏覽器	VMware Identity Manager 虛擬應用裝置	HTTPS
88	瀏覽器	VMware Identity Manager 虛擬應用裝置	TCP/UDP 僅限 iOS
5262	瀏覽器	VMware Identity Manager 虛擬應用裝置	TCP/UDP 僅限 Android
443	VMware Identity Manager 虛擬應用裝置	vapp-updates.vmware.com	存取 VMware 升級伺服器
8443	瀏覽器	VMware Identity Manager 虛擬應用裝置	管理員連接埠 HTTPS

連接埠	來源	目標	說明
25	VMware Identity Manager 虛擬應用裝置	SMTP 伺服器	轉送輸出郵件的 TCP 連接埠
53	VMware Identity Manager 虛擬應用裝置	DNS 伺服器	TCP/UDP 每個虛擬應用裝置都必須可透過連接埠 53 存取 DNS 伺服器，並在連接埠 22 上允許傳入 SSH 流量。
TCP：9300-9400 UDP：54328	VMware Identity Manager 虛擬應用裝置	VMware Identity Manager 虛擬應用裝置	稽核需求
5432	VMware Identity Manager 虛擬應用裝置	資料庫	PostgreSQL 預設連接埠是 5432。Oracle 預設連接埠是 1521。
443	VMware Identity Manager 虛擬應用裝置	AirWatch REST API	HTTPS 適用於裝置符合性檢查，以及 ACC 密碼驗證方法 (如有使用)。

部署 VMware Identity Manager 應用裝置

如需部署及設定 VMware Identity Manager 虛擬應用裝置的相關資訊，請參閱《*安裝和設定 VMware Identity Manager*》中的部署 VMware Identity Manager 和管理應用裝置系統組態設定。

設定容錯移轉和備援

如需為 VMware Identity Manager 虛擬應用裝置設定容錯移轉和備援的相關資訊，請參閱《*安裝和設定 VMware Identity Manager*》中的下列章節：

- 在單一資料中心設定容錯移轉和備援
- 在次要資料中心部署 VMware Identity Manager 以進行容錯移轉和備援

備註 〈使用負載平衡器或反向 Proxy 來啟用 VMware Identity Manager 的外部存取〉一節中的說明不適用於將 VMware Identity Manager 部署在 DMZ 中的情況。

在企業網路中部署 VMware Identity Manager Connector

3

當您在 DMZ 中部署 VMware Identity Manager 虛擬應用裝置時，必須也在企業網路中使用僅限輸出連線模式來部署獨立 VMware Identity Manager Connector 應用裝置。

連接器可將 VMware Identity Manager 服務連線至企業網路內的其他元件，例如 Active Directory 和 Horizon 7。

連接器可透過通訊通道使用僅限輸出連線模式與服務通訊。

備註 如果您已部署 AirWatch 且使用 AirWatch Cloud Connector，則不需要 VMware Identity ManagerConnector，除非您需要 VMware Identity Manager Connector 所支援的使用案例。請參閱"使用 AirWatch Cloud Connector 的內部部署模型," 第 8 頁。

系統和網路組態需求

請參閱"系統和網路組態需求," 第 16 頁。

部署和設定 VMware Identity Manager Connector

如需使用僅限輸出連線模式來部署和設定 VMware Identity ManagerConnector 的相關資訊，請參閱下列主題。

- "部署 VMware Identity Manager Connector," 第 16 頁
- "設定 VMware Identity ManagerConnector 的高可用性," 第 22 頁
- "將 Kerberos 驗證支援新增至您的 VMware Identity Manager Connector 部署," 第 25 頁

容錯移轉和備援

如需針對容錯移轉和備援設定連接器的相關資訊，請參閱下列主題。

- "設定 VMware Identity ManagerConnector 的高可用性," 第 22 頁
- "將 Kerberos 驗證支援新增至您的 VMware Identity Manager Connector 部署," 第 25 頁

本章節討論下列主題:

- "部署 VMware Identity Manager Connector," 第 16 頁
- "設定 VMware Identity ManagerConnector 的高可用性," 第 22 頁
- "將 Kerberos 驗證支援新增至您的 VMware Identity Manager Connector 部署," 第 25 頁

部署 VMware Identity Manager Connector

若要部署 VMware Identity Manager Connector，您必須在 vCenter Server 中安裝連接器虛擬應用裝置，接著開啟其電源，然後使用您在 VMware Identity Manager 管理主控台中產生的啟動碼加以啟動。您也可以設定應用裝置設定，例如設定密碼。

在您安裝並設定連接器後，您可以移至 VMware Identity Manager 管理主控台，設定對您企業目錄的連線、啟用連接器的驗證配接器，以及啟用連接器的輸出模式。

系統和網路組態需求

在決定硬體、資源和網路需求時，請考量您整體的部署，包括您預計要整合的資源。

支援的 vSphere 和 ESX 版本

您可以在 vCenter Server 中安裝虛擬應用裝置。支援下列 vSphere 和 ESX 伺服器版本：

- 5.0 U2 及更新版本
- 5.1 及更新版本
- 5.5 及更新版本
- 6.0 及更新版本

您需要 VMware vSphere® Client™ 或 VMware vSphere® Web Client 才能部署 OVA 檔案，以及從遠端存取已部署的虛擬應用裝置。vSphere Client 可從 my.vmware.com 上的 vSphere 產品下載頁面取得。

VMware Identity Manager Connector 虛擬應用裝置需求

請確定您的伺服器和分配給每個伺服器的資源符合數量上的需求。

使用者數量	最多 1,000	1,000-10,000	10,000-25,000	25,000-50,000	50,000-100,1000
連接器伺服器數量	1 個伺服器	2 個負載平衡的伺服器	2 個負載平衡的伺服器	2 個負載平衡的伺服器	2 個負載平衡的伺服器
CPU (每一伺服器)	2 個 CPU	4 個 CPU	4 個 CPU	4 個 CPU	4 個 CPU
RAM (每一伺服器)	6 GB	6 GB	8 GB	16 GB	16 GB
磁碟空間 (每一伺服器)	60 GB	60 GB	60 GB	60 GB	60 GB

網路組態需求

元件	最低需求
DNS 記錄和靜態 IP 位址	連接器的需求與 VMware Identity Manager 虛擬應用裝置的需求相同。請參閱《*安裝和設定 VMware Identity Manager*》中的〈建立 DNS 記錄和 IP 位址〉。
防火牆連接埠	請確定從連接器執行個體到您的 VMware Identity Manager URL 之間，已開啟輸出防火牆連接埠 443。

連接埠需求

以下說明連接器伺服器組態中使用的連接埠。您的部署可能只包含其中一個子集。

連接埠	來源	目標	說明
443	連接器虛擬應用裝置	VMware Identity Manager 服務	HTTPS
443	連接器虛擬應用裝置	vapp-updates.vmware.com	存取升級伺服器
8443	瀏覽器	連接器虛擬應用裝置	管理員連接埠 HTTPS
389, 636, 3268, 3269	連接器虛擬應用裝置	Active Directory	顯示預設值。可以設定這些連接埠。
445	Connector-va	VMware ThinApp 存放庫	存取 ThinApp 存放庫
5500	連接器虛擬應用裝置	RSA SecurID 系統	顯示預設值。此連接埠可供設定
53	連接器虛擬應用裝置	DNS 伺服器	TCP/UDP 每個虛擬應用裝置必須可以透過連接埠 53 存取 DNS 伺服器，並在連接埠 22 上允許傳入 SSH 流量
88, 464, 135	連接器虛擬應用裝置	網域控制站	TCP/UDP
389, 443	連接器虛擬應用裝置	View 連線伺服器	存取 View 連線伺服器執行個體以進行 Horizon/View 整合

目錄需求

您可以整合企業目錄與 VMware Identity Manager，並將使用者和群組從企業目錄同步至服務。您可以整合下列類型的目錄。

- 由單一 Active Directory 網域、單一 Active Directory 樹系中的多個網域，或多個 Active Directory 樹系中的多個網域組成的 Active Directory 環境。

  VMware Identity Manager 支援 Windows 2008、2008 R2、2012 和 2012 R2 (具有網域功能層級) 上的 Active Directory，以及 Windows 2003 及更新版本 (具有樹系功能層級) 的 Active Directory。

- LDAP 目錄

您的目錄必須可供連接器虛擬應用裝置存取。

備註 您也可以在 VMware Identity Manager 服務中建立本機目錄。

部署檢查清單

連接器的需求類似於 VMware Identity Manager 虛擬應用裝置的需求。請參閱《*安裝和設定 VMware Identity Manager*》中的〈部署檢查清單〉。

產生連接器的啟動碼

在安裝 VMware Identity Manager Connector 之前，請登入 VMware Identity Manager 管理主控台，並產生連接器的啟動碼。此啟動碼會用來建立服務與連接器之間的通訊。

程序

1 登入管理主控台。

2 按一下**身分識別與存取管理**索引標籤。

3 按一下**設定**。

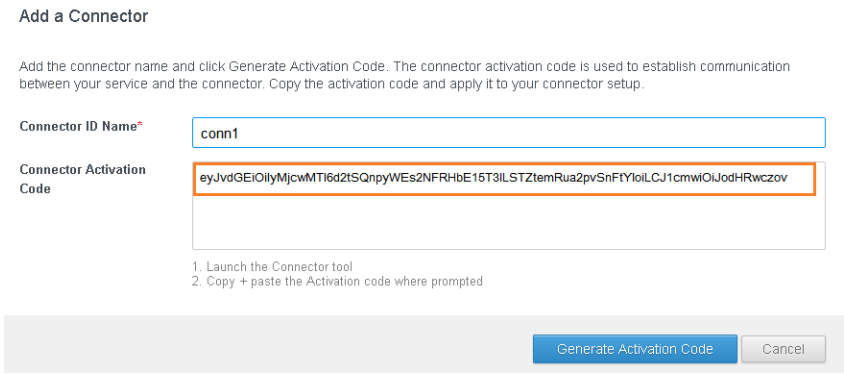
4 在 [連接器] 頁面上，按一下**新增連接器**。

5 輸入連接器的名稱。

6 按一下**產生啟動碼**。

啟動碼會顯示在頁面上。

7 複製啟動碼，並加以儲存。



您在後續部署連接器時將需要此啟動碼。

您現在可以安裝連接器虛擬應用裝置。

安裝及設定連接器虛擬應用裝置

若要部署連接器，您必須使用 vSphere Client 或 vSphere Web Client 在 vCenter Server 中安裝連接器虛擬應用裝置，接著開啟其電源，然後使用您在 VMware Identity Manager 管理主控台中產生的啟動碼加以啟動。

先決條件

- 從 my.vmware.com 上的 VMware Identity Manager 產品頁面下載連接器 OVA 檔案。
- 確定您擁有 vSphere Client 或 vSphere Web Client。
- 如果您使用 vSphere Web Client，請使用 Firefox 或 Chrome 瀏覽器。請勿使用 Internet Explorer 來部署 OVA 檔案。
- 識別用於應用裝置的 DNS 記錄和主機名稱。

程序

1 在 vSphere Client 或 vSphere Web Client 中，選取**檔案 > 部署 OVF 範本**。

2 遵循精靈的指示來部署範本。

頁面	說明
來源	瀏覽至 OVA 套件位置，或輸入特定 URL。
OVA 範本詳細資料	確認您選取正確的版本。
授權	閱讀使用者授權合約，然後按一下**接受**。
名稱和位置	輸入虛擬應用裝置的名稱。此名稱在詳細目錄資料夾中必須是唯一的，且最多可包含 80 個字元。名稱須區分大小寫。 選取虛擬應用裝置的位置。
主機/叢集	選取要執行已部署範本的主機或叢集。
資源集區	選取資源集區。
儲存區	選取虛擬機器檔案的儲存位置。
磁碟格式	選取檔案的磁碟格式。對於生產環境，請選取**完整佈建**格式。若要進行評估和測試，請使用**精簡佈建**格式。

頁面	說明
網路對應	將環境中的網路對應到 OVF 範本中的網路。
內容	a 在**時區設定**欄位中，選取正確的時區。 b [客戶經驗改進計劃] 核取方塊依預設已選取。VMware 會收集關於部署的匿名資料，以便改進對使用者需求的回應。如果您不想讓資料被收集，請取消選取此核取方塊。 c 在 [主機名稱] 文字方塊中，輸入要使用的主機名稱。如果此處空白，則會使用反向 DNS 來查閱主機名稱。 d 若要設定連接器的靜態 IP 位址，請輸入以下各項的位址：預設閘道、DNS、IP 位址及網路遮罩。 **重要事項** 如果這四個位址欄位中有任何欄位保留空白 (包括 [主機名稱])，系統便會使用 DHCP。 若要設定 DHCP，請將位址欄位保留空白。
即將完成	檢閱選取項目，然後按一下**完成**。

部署可能需要幾分鐘的時間，視您的網路速度而定。您可以在進度對話方塊中檢視進度。

3 當部署完成時，請選取連接器應用裝置，並以滑鼠右鍵按一下，然後選取**電源 > 電源開啟**。

連接器應用裝置隨即會進行初始化。您可以移至**主控台**索引標籤，以檢視詳細資料。當虛擬應用裝置初始化完成時，主控台畫面會顯示連接器版本，以及登入連接器安裝精靈的 URL。

4 若要執行安裝精靈，請將瀏覽器指向 [主控台] 索引標籤中顯示的連接器 URL。

5 在 [歡迎] 頁面上，按一下**繼續**。

6 為以下 連接器 虛擬應用裝置管理員帳戶建立強式密碼。

強式密碼的長度至少要有八個字元，並且包含大寫和小寫字元，以及至少一個數字或特殊字元。

選項	說明
應用裝置管理員	建立應用裝置管理員密碼。使用者名稱為 **admin** 且不得變更。您可以使用此帳戶和密碼來登入連接器服務，以管理憑證、應用裝置密碼及 syslog 組態。 **重要事項** **Admin** 使用者密碼的長度至少必須為 6 個字元。
根帳戶	用來安裝 連接器 應用裝置的預設 VMware 根密碼。建立新的根密碼。
sshuser 帳戶	建立用於遠端存取連接器應用裝置的密碼。

7 按一下**繼續**。

8 將啟動碼貼到 [啟動連接器] 頁面，然後按一下**繼續**。

系統會驗證啟動碼，隨後建立 VMware Identity Manager 服務與連接器執行個體之間的通訊。

連接器設定完成。

下一個

按一下 [設定完成] 頁面中的連結以移至管理主控台。然後，設定目錄連線。

設定目錄

部署連接器虛擬應用裝置後，請在 VMware Identity Manager 管理主控台中設定目錄。您可以從企業目錄將使用者和群組同步至 VMware Identity Manager 服務。

VMware Identity Manager 支援整合下列類型的目錄。

- Active Directory over LDAP
- Active Directory, 整合式 Windows 驗證

- LDAP 目錄

如需詳細資訊，請參閱與您的企業目錄整合。

備註 您也可以在 VMware Identity Manager 服務中建立本機目錄。請參閱使用本機目錄。

程序

1 按一下 [設定完成] 頁面上的連結 (此頁面會在您啟動連接器之後顯示)。

身分識別與存取管理 > 目錄索引標籤隨即顯示。

2 按一下**新增目錄**，然後選取您要新增的目錄類型。

3 依照精靈的指示輸入目錄組態資訊，接著選取要同步的群組和使用者，然後將使用者同步至 VMware Identity Manager 服務。

如需如何設定目錄的相關資訊，請參閱與您的企業目錄整合。

下一個

按一下**使用者和群組**索引標籤，並確認使用者已同步。

在連接器上啟用驗證配接器

輸出模式中的連接器有數個可用的驗證配接器，包括 PasswordIdpAdapter、RSAAIdpAdapter、SecurIDAdapter 和 RadiusAuthAdapter。設定並啟用您要使用的配接器。

程序

1 在 VMware Identity Manager 管理主控台中，按一下**身分識別與存取管理**索引標籤。

2 按一下**設定**，然後按一下**連接器**索引標籤。

您已部署的連接器隨即列出。

3 按一下 **Worker** 資料行中的連結。

4 按一下**驗證配接器**索引標籤。

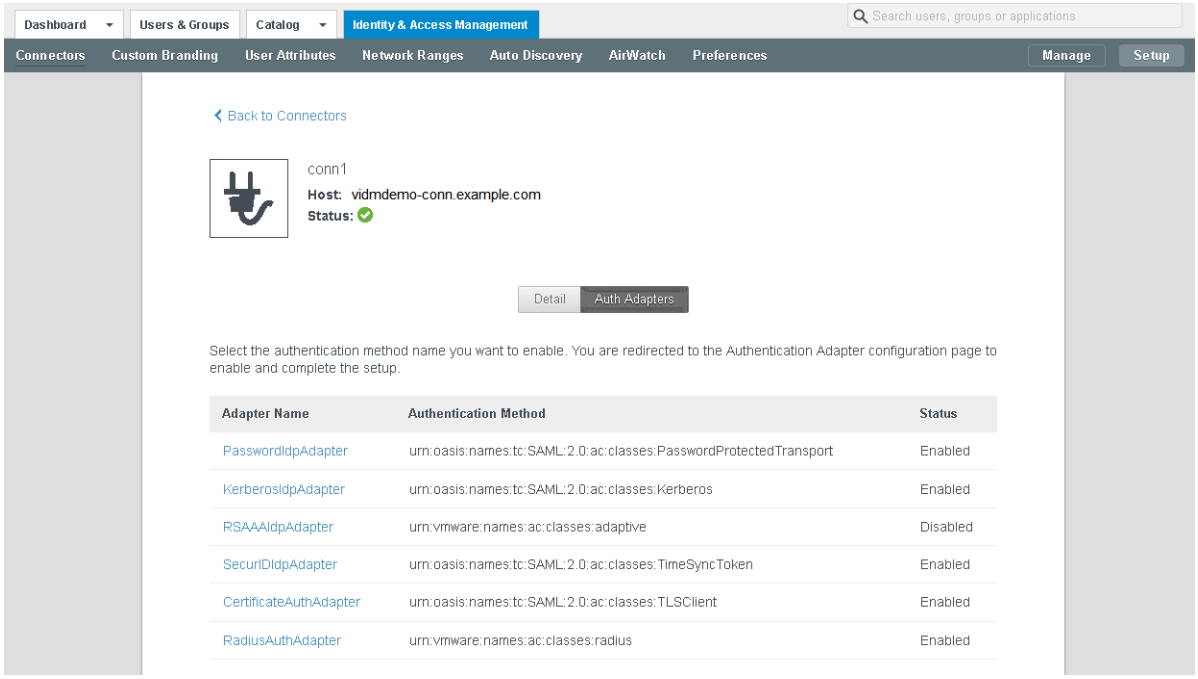
該連接器所有可用的驗證配接器皆會列出。

如果您已設定目錄，則 PasswordIdpAdapter 即已使用您在建立目錄時指定的組態資訊進行設定及啟用。

5 按一下每個驗證配接器的連結，並輸入組態資訊，以設定並啟用您要使用的配接器。您至少必須啟用一個驗證配接器。

如需設定特定驗證配接器的相關資訊，請參閱*《VMware Identity Manager 管理指南》*。

例如：



啟用連接器的輸出模式

若要啟用連接器的僅限輸出連線模式，請建立連接器與內建身分識別提供者的關聯。

內建身分識別提供者依預設會在 VMware Identity Manager 服務中啟用，並提供額外的內建驗證方法，例如 VMware Verify。如需內建身分識別提供者的相關資訊，請參閱*《VMware Identity Manager 管理指南》*。

備註 連接器可同時在輸出和一般模式中使用。即使您啟用輸出模式，仍可以使用驗證方法和原則為內部使用者設定 Kerberos 驗證。

程序

1 在管理主控台的**身分識別與存取管理**索引標籤中，按一下**管理**。

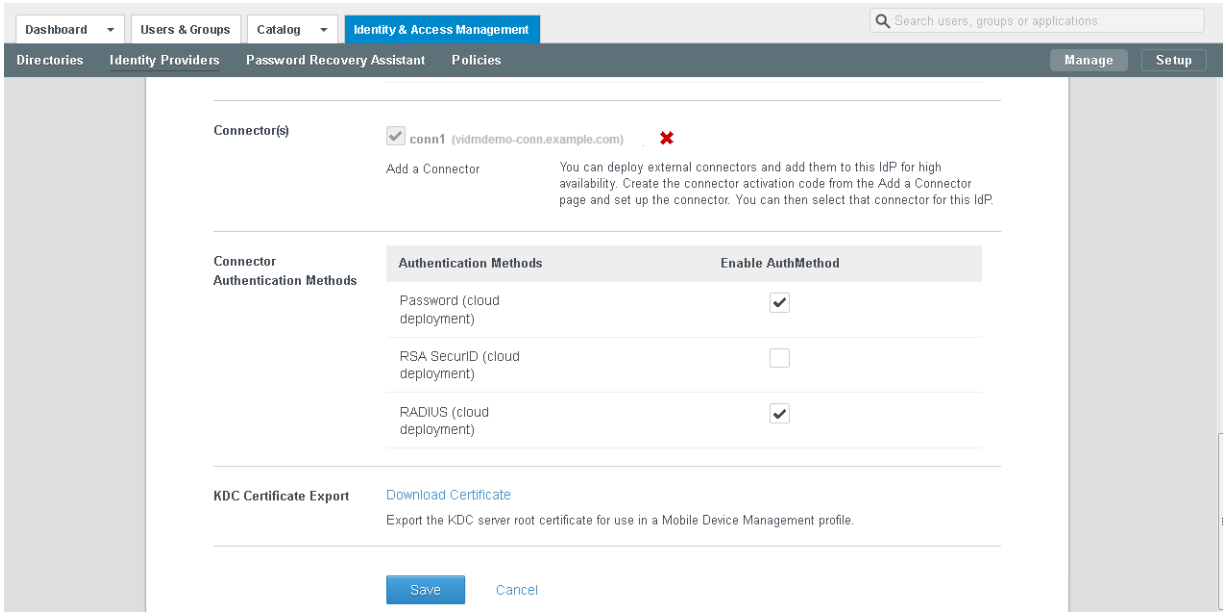
2 按一下**身分識別提供者**索引標籤。

3 按一下**內建**連結。

4 輸入下列資訊。

選項	說明
使用者	選取將使用內建身分識別提供者的目錄或網域。
網路	選取將使用內建身分識別提供者的網路範圍。
連接器	選取您所設定的連接器。 **備註** 隨後，當您新增高可用性所需的其他連接器時，請加以選取並將其新增至此處，以建立這些連接器與內建身分識別提供者的關聯。VMware Identity Manager 會自動將流量分配給所有與內建身分識別提供者相關聯的連接器。不需要負載平衡器。
連接器驗證方法	您為連接器啟用的部署方法皆會列出。請選取您要使用的驗證方法。 在您建立目錄時自動設定並啟用的 PasswordIdpAdapter，會在此頁面上顯示為**密碼 (雲端部署)**，這表示它會用於輸出模式中的連接器。

例如：



5 按一下**儲存**，以儲存內建身分識別提供者組態。

6 編輯原則，以使用您已啟用的驗證方法。

a 在**身分識別與存取管理**索引標籤中，按一下**管理**。

b 按一下**原則**索引標籤，然後按一下您要編輯的原則。

c 在**原則規則**下方，針對您要編輯的規則，按一下**驗證方法**資料行中的連結。

d 在 [編輯原則規則] 頁面中，選取要用於此規則的驗證方法。

e 按一下**確定**。

f 按一下**儲存**。

如需關於設定原則的詳細資訊，請參閱《*VMware Identity Manager 管理指南*》。

此時，連接器的輸出模式已啟用。當使用者使用您在 [內建身分識別提供者] 頁面中為連接器啟用的其中一個驗證方法登入時，將不需要透過 HTTP 重新導向至連接器。

設定 VMware Identity Manager Connector 的高可用性

您可以在叢集中新增多個連接器虛擬應用裝置，以設定高可用性和容錯移轉所需的 VMware Identity ManagerConnector。如果某個虛擬應用裝置基於任何原因而無法使用，仍將有其他連接器可供使用。

若要建立叢集，您必須安裝新的連接器虛擬應用裝置，然後以設定第一個連接器的相同方式來設定這些應用裝置。

接著，您可以將所有連接器執行個體與內建身分識別提供者建立關聯。VMware Identity Manager 服務會自動將流量分配給所有與內建身分識別提供者相關聯的連接器。不需要負載平衡器。如果其中一個連接器因網路問題而無法使用，則服務不會將流量導向至該處。當連線功能恢復時，服務會繼續將流量傳送至該連接器。

在您設定連接器叢集後，您在連接器上啟用的驗證方法會具有高可用性。如果有其中一個連接器執行個體無法使用，則驗證仍可執行。然而對於目錄同步來說，當連接器執行個體失敗時，您需要手動將其他連接器執行個體選取為同步連接器。目錄同步一次只能在一個連接器上啟用。

備註 本節內容不適用於 Kerberos 驗證的高可用性。請參閱"將 Kerberos 驗證支援新增至您的 VMware Identity Manager Connector 部署," 第 25 頁。

安裝其他連接器執行個體

在安裝並設定第一個連接器執行個體後，您可以新增其他連接器以達到高可用性。安裝新的連接器虛擬應用裝置，然後以設定第一個連接器執行個體的相同方式設定這些應用裝置。

先決條件

您已依照"部署 VMware Identity Manager Connector," 第 16 頁中的說明，安裝並設定第一個連接器執行個體。

程序

1 依照下列指示，安裝並設定新的連接器執行個體。

- "產生連接器的啟動碼," 第 17 頁
- "安裝及設定連接器虛擬應用裝置," 第 18 頁

2 將新的連接器與第一個連接器執行個體的 `WorkspaceIDP` 建立關聯。

a 在管理主控台內，依序選取**身分識別與存取管理**和**身分識別提供者**索引標籤。

b 在 [身分識別提供者] 頁面中尋找第一個連接器執行個體的 `WorkspaceIDP`，然後按一下連結。

c 在**連接器**欄位中，選取新的連接器。

d 輸入繫結 DN 密碼，然後按一下**新增連接器**。

e 按一下**儲存**。

3 如果您已在第一個連接器執行個體中加入 Active Directory 網域，則也必須在新的連接器執行個體中加入該網域。

a 在**身分識別與存取管理**索引標籤中，按一下**設定**。

[連接器] 頁面中會列出新的連接器執行個體。

b 按一下新連接器旁的**加入網域**，並指定網域資訊。

備註 針對類型為「整合式 Windows 驗證 (IWA)」的目錄，您必須執行下列動作。

a 將新的連接器執行個體加入至原始連接器執行個體中的 IWA 目錄所加入的網域。

1 選取**身分識別與存取管理**索引標籤，然後按一下**設定**。

[連接器] 頁面中會列出新的連接器執行個體。

2 按一下**加入網域**，並指定網域資訊。

b 儲存 IWA 目錄組態。

1 選取**身分識別與存取管理**索引標籤。

2 在 [目錄] 頁面中，按一下 IWA 目錄連結。

3 按一下**儲存**以儲存目錄組態。

---

4 在新的連接器上設定並啟用驗證配接器。

重要事項 您的叢集中所有連接器的驗證配接器必須以相同的方式進行設定。所有連接器上皆必須啟用相同的驗證方法。

---

a 在**身分識別與存取管理**索引標籤中按一下**設定**，然後按一下**連接器**索引標籤。

b 按一下新連接器之 **Worker** 資料行中的連結。

c 按一下**驗證配接器**索引標籤。

該連接器所有可用的驗證配接器皆會列出。

由於您已將新的連接器與第一個連接器的相關目錄建立關聯，因此 PasswordIdpAdapter 已設定並啟用。

d 使用與第一個連接器相同的方式，設定並啟用其他驗證配接器。請確定組態資訊是相同的。

如需設定驗證配接器的相關資訊，請參閱《*VMware Identity Manager 管理指南*》。

下一個

"將新的連接器新增至內建身分識別提供者," 第 24 頁

將新的連接器新增至內建身分識別提供者

在部署並設定新的連接器執行個體後，請將其新增至內建身分識別提供者，並啟用在第一個連接器上所啟用的相同驗證方法。VMware Identity Manager 會自動將流量分配給所有與內建身分識別提供者相關聯的連接器。

程序

1 在管理主控台的**身分識別與存取管理**索引標籤中，按一下**管理**。

2 按一下**身分識別提供者**索引標籤。

3 按一下**內建**連結。

4 在**連接器**欄位中，從下拉式清單中選取新的連接器，然後按一下**新增連接器**。

5 在**連接器驗證方法**區段中，啟用您為第一個連接器選取的相同驗證方法。

系統會自動設定並啟用「密碼 (雲端部署)」驗證方法。您必須啟用其他驗證方法。

重要事項 您的叢集中所有連接器的驗證配接器必須以相同的方式進行設定。所有連接器上皆必須啟用相同的驗證方法。

如需設定特定驗證配接器的相關資訊，請參閱《*VMware Identity Manager 管理指南*》。

6 按一下**儲存**，以儲存內建身分識別提供者組態。

失敗時在其他連接器上啟用目錄同步

在一個連接器執行個體失敗時，驗證會自動由另一個連接器執行個體進行處理。不過，針對目錄同步，您必須在 VMware Identity Manager 服務中修改目錄設定，才能使用另一個連接器執行個體，而非原始連接器執行個體。目錄同步一次只能在一個連接器上啟用。

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，然後按一下**目錄**。

3 按一下與原始連接器執行個體相關聯的目錄。

Tip 您可以在**設定 > 連接器**頁面上檢視此資訊。

4 在目錄頁面的**目錄同步與驗證**區段中的**同步連接器**下拉式清單中，選取另一個連接器執行個體。

5 在**繫結 DN 密碼**文字方塊中，輸入您的 Active Directory 繫結帳戶密碼。

6 按一下**儲存**。

將 Kerberos 驗證支援新增至您的 VMware Identity Manager Connector 部署

您可以將內部使用者的 Kerberos 驗證 (需要輸入連線模式) 新增至您根據僅限輸出連線模式連接器的部署。您可以設定相同的連接器，以便對來自內部網路的使用者使用 Kerberos 驗證，而對來自外部的使用者使用另一個驗證方法。若要這麼做，請根據網路範圍定義驗證原則。

備註 若要設定 Kerberos 驗證的高可用性，則必須具備負載平衡器。

設定並啟用 Kerberos 驗證配接器

在 VMware Identity Manager Connector 上設定並啟用 KerberosIdpAdapter。如果您已部署高可用性所需的叢集，請在叢集中的所有連接器上設定並啟用配接器。

重要事項 您的叢集中所有連接器的驗證配接器必須以相同的方式進行設定。所有連接器上皆必須設定相同的驗證方法。

如需關於設定 Kerberos 驗證的詳細資訊，請參閱*《VMware Identity Manager 管理指南》*。

先決條件

連接器必須加入 Active Directory 網域。

程序

1 在 VMware Identity Manager 管理主控台中，按一下**身分識別與存取管理**索引標籤。

2 按一下**設定**，然後按一下**連接器**索引標籤。

您已部署的所有連接器皆會列出。

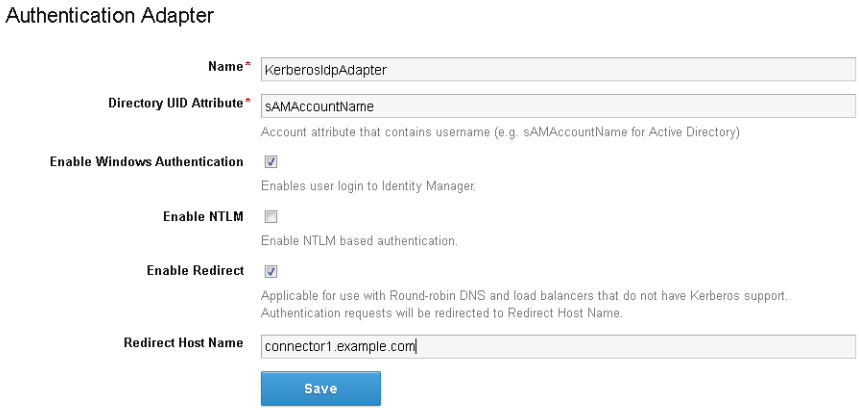
3 按一下其中一個連接器之 **Worker** 資料行中的連結。

4 按一下**驗證配接器**索引標籤。

5 按一下 KerberosIdpAdapter 連結，然後設定並啟用配接器。

選項	說明
名稱	配接器的預設名稱為 KerberosIdpAdapter。您可以變更此名稱。
目錄 UID 屬性	包含使用者名稱的帳戶屬性。
啟用 Windows 驗證	選取此選項。
啟用 NTLM	除非您的 Active Directory 基礎結構依存於 NTLM 驗證，否則您不需要選取此選項。
啟用重新導向	如果您在一個叢集中有多個連接器，而且您想要使用負載平衡器來設定 Kerberos 高可用性，請選取此選項，並指定**重新導向主機名稱**的值。 如果您的部署只有一個連接器，則不需要使用**啟用重新導向**和**重新導向主機名稱**選項。
重新導向主機名稱	如果選取**啟用重新導向**選項，則必須提供值。輸入連接器本身的主機名稱。例如，如果連接器的主機名稱為 connector1.example.com，請在文字方塊中輸入 **`connector1.example.com`**。

例如：



如需關於設定 KerberosIdPAdapter 的詳細資訊，請參閱《*VMware Identity Manager 管理指南*》。

6 如果您已部署叢集，請在叢集中的所有連接器上設定 KerberosIdPAdapter。

確定在所有連接器上設定相同的配接器。

下一個

視需要設定 Kerberos 驗證的高可用性。若沒有負載平衡器，則 Kerberos 驗證將不具有高可用性。

設定 Kerberos 驗證的高可用性

若要設定 Kerberos 驗證的高可用性，請在您位於防火牆內的內部網路中安裝負載平衡器，並為其新增連接器應用裝置。

您也必須在負載平衡器上進行某些設定、建立負載平衡器與連接器之間的 SSL 信任，以及將連接器驗證 URL 變更為使用負載平衡器主機名稱。

設定負載平衡器設定

您必須設定負載平衡器上的特定設定，例如啟用 X-Forwarded-For 標頭、正確地設定負載平衡器逾時，以及啟用黏性工作階段。

請設定下列設定。

- X-Forwarded-For 標頭

  您必須在負載平衡器上啟用 X-Forwarded-For 標頭。這會決定驗證方法。如需詳細資訊，請參閱您的負載平衡器廠商所提供的文件。

- 負載平衡器逾時

  若要讓 連接器 正常運作，您可能必須從預設值提高負載平衡器要求逾時。此值以分鐘為單位設定，如果逾時設定太低，您可能會看見下列錯誤。

  ```
  502 錯誤：服務目前無法使用
  ```

- 啟用黏性工作階段

  如果您的部署有多個連接器應用裝置，則您必須在負載平衡器上啟用黏性工作階段設定。負載平衡器隨後會將使用者的工作階段繫結至特定的連接器執行個體。

將 VMware Identity Manager Connector 根憑證套用至負載平衡器

在進行 VMware Identity Manager 連接器 虛擬應用裝置的負載平衡器設定時，您必須在負載平衡器與連接器之間建立 SSL 信任。必須將連接器根憑證複製到負載平衡器。

連接器 憑證可以從連接器應用裝置管理頁面 (https://*myconnector*) 下載。*mycompany*:8443/cfg/ssl。

如果 連接器 網域名稱指向負載平衡器，則只能將 SSL 憑證套用至負載平衡器。

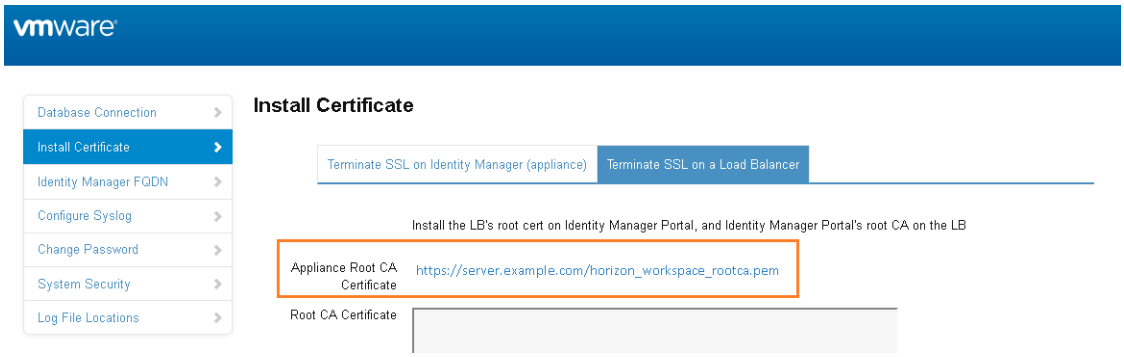
由於負載平衡器會與連接器虛擬應用裝置通訊，因此您必須將連接器根 CA 憑證複製到負載平衡器作為受信任的根憑證。

程序

1 以管理員使用者身分登入 連接器 應用裝置管理頁面，網址 https://*myconnector.mycompany*:8443/cfg/ssl。

2 選取**安裝憑證**。

3 選取**終止負載平衡器上的 SSL** 索引標籤，然後在**應用裝置根 CA 憑證**欄位中，按一下連結 `https://hostname/horizon_workspace_rootca.pem`。



4 複製 -----BEGIN CERTIFICATE----- 與 -----END CERTIFICATE---- 之間的各行內容，並將根憑證貼到每個負載平衡器上的正確位置。請參閱負載平衡器說明文件。

下一個

複製負載平衡器根憑證並貼到 VMware Identity Manager 連接器 應用裝置。

將負載平衡器根憑證套用至 VMware Identity Manager Connector

在進行 VMware Identity Manager 連接器 虛擬應用裝置的負載平衡器設定時，您必須在負載平衡器與連接器之間建立信任。除了將連接器根憑證複製至負載平衡器，您也必須將負載平衡器根憑證複製至連接器。

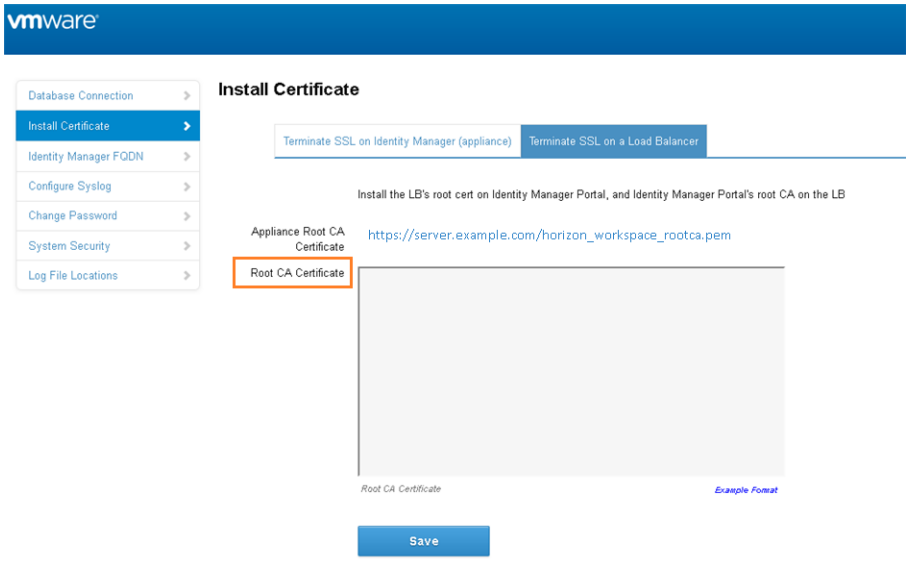
程序

1 取得負載平衡器根憑證。

2 前往 連接器 應用裝置管理頁面，網址 https://*myconnector.mycompany*:8443/cfg/ssl，並以管理員使用者身分登入。

3 在**安裝憑證**頁面中，選取**終止負載平衡器上的 SSL** 索引標籤。

4 將負載平衡器憑證的文字貼上至**根 CA 憑證**欄位。



5 按一下**儲存**。

將連接器 IdP 主機名稱變更為負載平衡器主機名稱

將連接器虛擬應用裝置新增至負載平衡器之後，您必須將每個連接器之 Workspace IdP 上的 IdP 主機名稱變更為負載平衡器主機名稱。

先決條件

您必須在負載平衡器後方設定 連接器 虛擬應用裝置。確認負載平衡器連接埠是 443。請勿使用 8443，因為該連接埠號碼是管理連接埠，它在每個虛擬應用裝置上都是唯一的。

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**身分識別提供者**索引標籤。

4 在 [身分識別提供者] 頁面中，按一下您 連接器 執行個體的 Workspace IdP 連結。

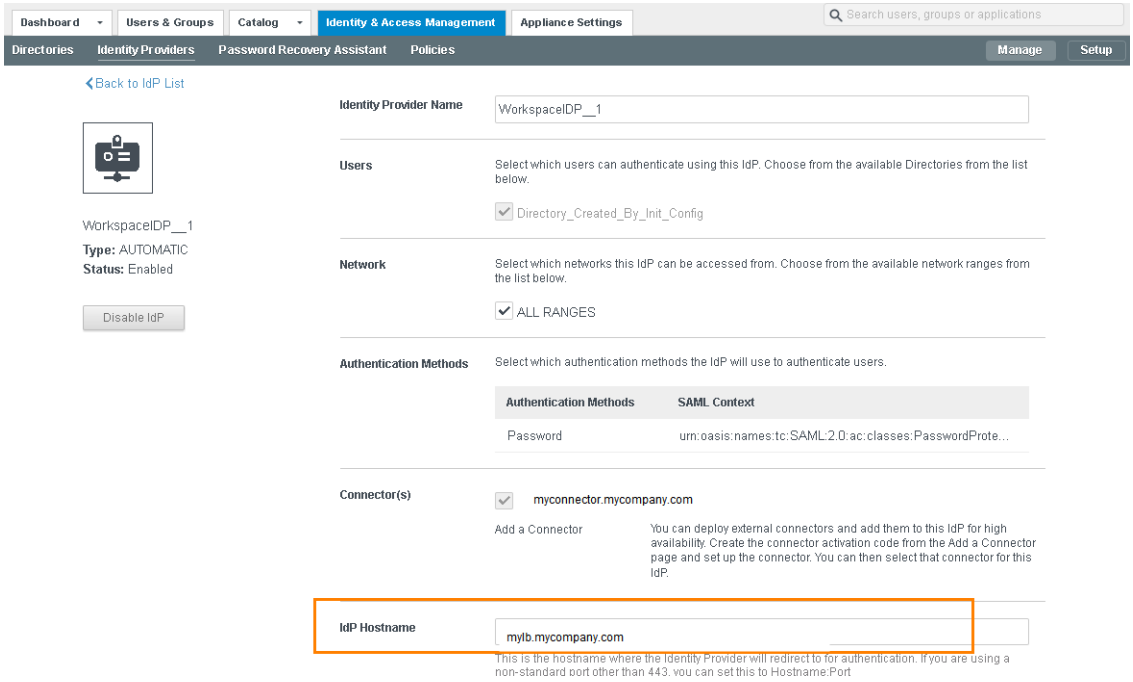
5 在 **IdP 主機名稱**文字方塊中，將主機名稱從連接器主機名稱變更為負載平衡器主機名稱。

例如，如果您的連接器主機名稱為 `myconnector`，而您的負載平衡器主機名稱為 `mylb`，請變更 URL

`myconnector.mycompany.com:`*`port`*

變更為下列：

`mylb.mycompany.com:`*`port`*



索引