用於設定 Horizon 之 TLS 憑證的案例

VMware Horizon 2006

您可以在 VMware 網站上找到最新的技術文件，網址如下：

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

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

Copyright © 2020 VMware, Inc. 保留所有權利。 版權與商標資訊。

目錄

用於設定 Horizon 之 TLS 憑證的案例

《用於設定 Horizon 之 TLS 憑證的案例》提供設定 TLS 憑證供 Horizon Server 使用的範例。第一個案例說明如何從憑證授權機構取得簽署的 TLS 憑證，並確定這些憑證採用可供 Horizon Server 使用的格式。第二個案例說明如何設定 Horizon Server，以便將 TLS 連線卸載至中繼伺服器。

主要對象

這項資訊適用於想要安裝 Horizon 且需要取得 TLS 憑證以供 Horizon Server 使用的任何人員，或是使用中繼伺服器將 TLS 連線卸載至 Horizon 的任何人員。這些資訊是針對熟悉虛擬機器技術及資料中心作業的資深 Windows 或 Linux 系統管理員所撰寫。

從憑證授權機構取得 TLS 憑證

1

VMware 強烈建議您設定由有效憑證授權機構 (CA) 簽署的 TLS 憑證，以供 Horizon 連線伺服器執行個體使用。

當您安裝連線伺服器時，將會產生預設的 TLS 憑證。儘管您可以使用預設的自我簽署憑證進行測試，但應盡快將其取代。預設憑證並非由 CA 簽署。使用未經 CA 簽署的憑證可能會讓不受信任者偽裝成您的伺服器來攔截流量。

在 Horizon 環境中，請將隨 vCenter Server 安裝的預設憑證取代為 CA 簽署的憑證。您可以使用 openTLS 針對 vCenter Server 執行此工作。如需詳細資料，請參閱 VMware Technical Papers 網站上的「取代 vCenter Server 憑證」，網址為：http://www.vmware.com/resources/techresources/。

本章節討論下列主題：

- 判斷您是否適用此案例
- 選取正確的憑證類型
- 使用 Microsoft Certreq 產生憑證簽署要求並取得憑證

判斷您是否適用此案例

您可以將憑證匯入至 Horizon Server 主機上的 Windows 本機電腦憑證存放區，藉以設定 Horizon 的憑證。

您必須先產生憑證簽署要求 (CSR)，並從 CA 取得有效的已簽署憑證才能匯入憑證。若未根據此案例中說明的範例程序產生 CSR，則產生的憑證及其私密金鑰必須可在 PKCS#12 (先前稱為 PFX) 格式的檔案中使用。

您可以使用多種方式從 CA 取得 TLS 憑證。此案例說明如何使用 Microsoft `certreq` 公用程式來產生 CSR，並使憑證可供 Horizon Server 使用。如果您熟悉必要的工具，且伺服器上已安裝這些工具，則可以使用其他方法。

使用此案例可解決下列問題：

- 您沒有由 CA 簽署的 TLS 憑證，且不知道如何取得
- 您具有已簽署的有效 TLS 憑證，但並非為 PKCS#12 (PFX) 格式

如果您的組織為您提供由 CA 簽署的 TLS 憑證，您可以使用這些憑證。您的組織可以使用有效的內部 CA 或第三方商業 CA。如果您的憑證並非採用 PKCS#12 格式，則必須進行轉換。請參閱將憑證檔案轉換為 PKCS#12 格式。

如果您已擁有適當格式的已簽署憑證，則可以將其匯入 Windows 憑證存放區中，並設定 Horizon Server 使用該憑證。請參閱為 Horizon Server 設定匯入的憑證。

選取正確的憑證類型

您可將多種類型的 TLS 憑證用於 Horizon。為您的部署選取正確的憑證類型十分重要。憑證類型不同，其成本也不同，端視其可使用在的伺服器數目而定。

無論您選取何種憑證類型，請務必遵循 VMware 的安全建議：針對憑證使用完整網域名稱 (FQDN)。請勿使用簡單伺服器名稱或 IP 位址，即使針對內部網域內的通訊。

單一伺服器名稱憑證

您可針對特定伺服器，產生具有主體名稱的憑證。例如：`dept.company.com`。

舉例來說，如果只有一個連線伺服器執行個體需要憑證，這種類型的憑證就很有用。

當您提交憑證簽署要求至 CA 時，需提供與憑證相關聯的伺服器名稱。請確定 Horizon Server 可解析您提供的伺服器名稱，使其符合憑證關聯的名稱。

主體別名

主體別名 (SAN) 是在核發憑證時可以新增至憑證的屬性。使用此屬性新增主體名稱 (URL) 至憑證，讓憑證可以驗證多個伺服器。

例如，憑證可能會核發給具有主機名稱 `dept.company.com` 的伺服器。您想要讓透過連線伺服器連線至 Horizon 的外部使用者使用憑證。核發憑證之前，您可以將 SAN `dept-int.company.com` 新增至憑證，讓憑證在通道啟用的情況下，能夠在負載平衡器後方的連線伺服器執行個體上使用。

萬用字元憑證

產生萬用字元憑證以用於多個服務。例如：`*.company.com`。

如果有多個伺服器需要憑證，萬用字元就很有用。如果除了 Horizon 以外，您環境中還有其他應用程式需要 TLS 憑證，您也可以為這些伺服器使用萬用字元憑證。不過，如果使用與其他服務共用的萬用字元憑證，則 VMware Horizon 產品的安全性也會取決於上述其他服務的安全性。

備註 萬用字元憑證只能用於單一網域層級。例如，具有主體名稱 `*.company.com` 的萬用字元憑證可以用於子網域 `dept.company.com`，但不能用於 `dept.it.company.com`。

使用 Microsoft Certreq 產生憑證簽署要求並取得憑證

要讓憑證可供 Horizon Server 使用，您必須建立組態檔、從組態檔產生憑證簽署要求 (CSR)，並將簽署要求傳送至 CA。當 CA 傳回憑證時，您必須將簽署的憑證匯入至 Horizon Server 主機上的 Windows 本機電腦憑證存放區，使其與先前產生的私密金鑰連結。

CSR 可透過多種方式產生，這取決於憑證本身的產生方式。

程序

1 建立 CSR 組態檔

Microsoft `certreq` 公用程式會使用組態檔來產生 CSR。您必須先建立組態檔，才能產生要求。請建立組態檔，然後在主控將使用憑證之 Horizon Server 的 Windows Server 電腦上產生 CSR。

2 產生 CSR 並向 CA 要求簽署的憑證

使用已完成的組態檔，您可以藉由執行 `certreq` 公用程式來產生 CSR。您可以將要求傳送至第三方 CA 以傳回簽署的憑證。

3 確認 CSR 及其私密金鑰皆儲存在 Windows 憑證存放區中

如果您使用 `certreq` 公用程式來產生 CSR，該公用程式也會產生相關聯的私密金鑰。公用程式會在您產生 CSR 的電腦上，將 CSR 和私密金鑰儲存在 Windows 本機電腦憑證存放區中。您可以使用 Microsoft Management Console (MMC) 憑證嵌入式管理單元，確認 CSR 和私密金鑰皆已正確儲存。

4 使用 Certreq 匯入簽署的憑證

如果您具有來自 CA 的已簽署憑證，您可以將該憑證匯入至 Horizon Server 主機上的 Windows 本機電腦憑證存放區中。

5 為 Horizon Server 設定匯入的憑證

將伺服器憑證匯入至 Windows 本機電腦憑證存放區之後，您必須採取額外的步驟讓 Horizon Server 能夠使用該憑證。

建立 CSR 組態檔

Microsoft `certreq` 公用程式會使用組態檔來產生 CSR。您必須先建立組態檔，才能產生要求。請建立組態檔，然後在主控將使用憑證之 Horizon Server 的 Windows Server 電腦上產生 CSR。

必要條件

收集您填妥組態檔所需的資訊。您必須知道 Horizon Server 的 FQDN，以及組織單位、組織、城市、州和國家/地區才能完成主體名稱。

程序

1 開啟文字編輯器，並將下列包括開始和結束標記的文字貼到檔案中。

```
;----------------- request.inf -----------------

[Version]

Signature="$Windows NT$"

[NewRequest]

Subject = "CN=View_Server_FQDN, OU=Organizational_Unit, O=Organization, L=City, S=State,
C=Country"
```

```
; Replace View_Server_FQDN with the FQDN of the Horizon server.
; Replace the remaining Subject attributes.
KeySpec = 1
KeyLength = 2048
; KeyLength is usually chosen from 2048, 3072, or 4096. A KeyLength
; of 1024 is also supported, but it is not recommended.
HashAlgorithm = SHA256
; Algorithms earlier than SHA-2 are insufficiently secure and are not recommended.
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication

;-----------------------------------------------
```

如果您在複製並貼上文字時，將額外的 CR/LF 字元新增至 `Subject =` 行中，請刪除 CR/LF 字元。

2 使用 Horizon Server 和部署的適當值來更新 `Subject` 屬性。

例如：`CN=dept.company.com`

若要符合 VMware 安全性建議，請使用用戶端裝置用於連線至主機的完整網域名稱 (FQDN)。請勿使用簡單伺服器名稱或 IP 位址，即使針對內部網域內的通訊。

某些 CA 不允許您對州屬性使用縮寫。

3 (選擇性) 更新 `Keylength` 屬性。

除非您明確需要不同的 `KeyLength` 大小，否則預設值 2048 即足夠使用。許多 CA 皆需要至少 2048 的值。較大的金鑰大小更為安全，但對於效能影響較大。

1024 的 `KeyLength` 也受支援，但美國國家標準技術研究所 (NIST) 建議不要使用此大小的金鑰，因為隨著電腦的效能日益強大，更強的加密也可能遭到破解。

重要 請勿產生低於 1024 的 `KeyLength` 值。Windows 版 Horizon Client 不會驗證 Horizon Server 上以低於 1024 之 `KeyLength` 產生的憑證，且 Horizon Client 裝置將無法連線至 Horizon。連線伺服器執行的憑證驗證也會失敗，導致受影響的 Horizon Server 在 Horizon Console 儀表板中顯示為紅色。

4 將檔案儲存為 `request.inf`。

後續步驟

從組態檔產生 CSR。

產生 CSR 並向 CA 要求簽署的憑證

使用已完成的組態檔，您可以藉由執行 `certreq` 公用程式來產生 CSR。您可以將要求傳送至第三方 CA 以傳回簽署的憑證。

必要條件

- 確認您已完成 CSR 組態檔。請參閱建立 CSR 組態檔。
- 在 CSR 組態檔所在的電腦上，執行此程序中說明的 `certreq` 作業。

程序

1 在**開始**功能表中的**命令提示字元**上按一下滑鼠右鍵，並選取**以系統管理員身分執行**，以開啟命令提示字元。

2 導覽至您儲存 `request.inf` 檔案的目錄。

例如：**`cd c:\certificates`**

3 產生 CSR 檔案。

例如：**`certreq –new request.inf certreq.txt`**

4 使用 CSR 檔案的內容以根據 CA 註冊程序將憑證要求提交至 CA。

a 當您將要求提交至 CA 時，CA 會提示您選取將安裝憑證的伺服器類型。由於 Horizon 會使用 Microsoft 憑證 MMC 來管理憑證，因此，請選取 Microsoft、Microsoft IIS 7 或類似伺服器類型的憑證。CA 應該會以搭配使用 Horizon 所需的格式來產生憑證。

b 如果您要求單一伺服器名稱憑證，請使用 Horizon Client 裝置可以針對此 Horizon Server 解析 IP 位址的名稱。電腦用來連線至 Horizon Server 的名稱，應符合與憑證相關聯的名稱。

備註 CA 可能會要求您將 CSR 檔案 (例如 `certreq.txt`) 的內容複製並貼上至 Web 表單中。您可以使用文字編輯器複製 CSR 檔案的內容。請確定包含開始和結束標記。例如：

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID2jCCAsICAQAwazEWMBQGA1UEBhMNVW5pdGVkIFN0YXRlczELMAkGA1UECAwC
Q0ExEjAQBgNVBAcMCVBhbG8gQWx0bzEKMAgGA1UECgwBTzELMAkGA1UECwwCT1Ux
FzAVBgNVBAMMDm15LmNvbXBhbnkuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
. . .
. . .
L9nPYX76jeu5rwQfXLivSCea6nZiIOZYw8Dbn8dgwAqpJdzBbrwuM1TuSnx6bAK8
S52Tv0GxW58jUTtxFV+Roz8TE8wZDFB51jx+FmLs
-----END NEW CERTIFICATE REQUEST-----
```

CA 對您的公司進行某些檢查後，即會根據 CSR 中的資訊建立伺服器憑證、使用其私密金鑰進行簽署，以及將憑證傳送給您。

CA 也會將根 CA 憑證和中繼 CA 憑證 (如果適用) 傳送給您。

5 將憑證文字檔重新命名為 `cert.cer`。

請確定該檔案位於產生憑證要求的 Horizon Server 上。

6 將根 CA 和中繼 CA 憑證檔案重新命名為 `root.cer` 和 `intermediate.cer`。

請確定這些檔案位於產生憑證要求的 Horizon Server 上。

備註 當您使用 `certreq` 公用程式將憑證匯入至 Windows 本機電腦憑證存放區時，這些憑證不一定要採用 PKCS#12 (PFX) 格式。如果您使用「憑證匯入」精靈將憑證匯入 Windows 憑證存放區中，則需要使用 PKCS#12 (PFX) 格式。

後續步驟

確認 CSR 檔案及其私密金鑰儲存在 Windows 本機電腦憑證存放區中。

確認 CSR 及其私密金鑰皆儲存在 Windows 憑證存放區中

如果您使用 `certreq` 公用程式來產生 CSR，該公用程式也會產生相關聯的私密金鑰。公用程式會在您產生 CSR 的電腦上，將 CSR 和私密金鑰儲存在 Windows 本機電腦憑證存放區中。您可以使用 Microsoft Management Console (MMC) 憑證嵌入式管理單元，確認 CSR 和私密金鑰皆已正確儲存。

後續必須將私密金鑰與簽署的憑證連結，Horizon Server 才能正確匯入並使用憑證。

必要條件

- 確認您已使用 `certreq` 公用程式產生 CSR，且已從 CA 要求簽署的憑證。請參閱產生 CSR 並向 CA 要求簽署的憑證。
- 熟悉將憑證嵌入式管理單元新增至 Microsoft Management Console (MMC) 的程序。請參閱《Horizon 安裝》文件之〈設定 Horizon Server 的 TLS 憑證〉一章中的「將憑證嵌入式管理單元新增至 MMC 中」。

程序

1 在 Windows Server 電腦上，將憑證嵌入式管理單元新增到 MMC 中。

2 在 Windows Server 電腦的 MMC 視窗中，展開**憑證 (本機電腦)** 節點，然後選取**憑證註冊要求**資料夾。

3 展開**憑證註冊要求**資料夾，然後選取**憑證**資料夾。

4 確認憑證項目顯示在**憑證**資料夾中。

核發給和**核發者**欄位必須顯示用來產生 CSR 之 `request.inf` 檔案的 **`subject:CN`** 欄位中所輸入的網域名稱。

5 採取下列其中一個步驟，確認憑證包含私密金鑰：

- 確認憑證圖示上出現一個黃色金鑰。
- 按兩下憑證，並確認 [憑證資訊] 對話方塊中顯示下列陳述：這個憑證有一個對應的私密金鑰。

後續步驟

將憑證匯入 Windows 本機電腦憑證存放區中。

使用 Certreq 匯入簽署的憑證

如果您具有來自 CA 的已簽署憑證，您可以將該憑證匯入至 Horizon Server 主機上的 Windows 本機電腦憑證存放區中。

如果您已使用 `certreq` 公用程式產生 CSR，則憑證私密金鑰會位於您產生 CSR 的本機伺服器位置。若要正確運作，憑證必須與私密金鑰結合。請使用此程序中顯示的 `certreq` 命令，確保憑證和私密金鑰正確結合且已匯入 Windows 憑證存放區中。

如果您使用其他方法取得來自 CA 的簽署憑證，您可以使用 Microsoft Management Console (MMC) 嵌入式管理單元中的「憑證匯入」精靈，將憑證匯入 Windows 憑證存放區中。此方法的相關說明請參閱《Horizon 安裝》文件中的〈設定 Horizon Server 的 TLS 憑證〉。

必要條件

- 確認您已收到來自 CA 的簽署憑證。請參閱產生 CSR 並向 CA 要求簽署的憑證。
- 在您產生 CSR 及儲存已簽署憑證的電腦上，執行此程序中說明的 `certreq` 作業。

程序

1. 在**開始**功能表中的**命令提示字元**上按一下滑鼠右鍵，並選取**以系統管理員身分執行**，以開啟命令提示字元。
2. 導覽至用來儲存已簽署憑證檔案 (例如 `cert.cer`) 的目錄。

   例如：**`cd c:\certificates`**
3. 執行 `certreq –accept` 命令以匯入簽署的憑證。

   例如：**`certreq –accept cert.cer`**

結果

憑證會匯入 Windows 本機電腦憑證存放區中。

後續步驟

設定要由 Horizon Server 使用的已匯入憑證。請參閱為 Horizon Server 設定匯入的憑證。

為 Horizon Server 設定匯入的憑證

將伺服器憑證匯入至 Windows 本機電腦憑證存放區之後，您必須採取額外的步驟讓 Horizon Server 能夠使用該憑證。

程序

1. 確認伺服器憑證已成功匯入。
2. 將憑證的易記名稱變更為 **`vdm`**。

   `vdm` 必須為小寫。任何具有易記名稱 **`vdm`** 的其他憑證皆必須重新命名，或者，您必須從那些憑證中移除易記名稱。
3. 將根 CA 憑證和中繼 CA 憑證安裝在 Windows 憑證存放區中。

4 重新啟動連線伺服器服務，讓服務能夠開始使用新的憑證。

5 如果您使用 HTML Access，請重新啟動 Blast 安全閘道服務。

結果

若要執行此程序中的工作，請參閱下列主題：

- 修改憑證易記名稱
- 將根憑證和中繼憑證匯入 Windows 憑證存放區中

如需詳細資訊，請參閱《Horizon 安裝》文件中的〈設定連線伺服器以使用新的 TLS 憑證〉。

備註 此處並未列出《Horizon 安裝》主題〈將簽署的伺服器憑證匯入 Windows 憑證存放區〉，因為您已使用 `certreq` 公用程式匯入伺服器憑證。您不應使用 MMC 嵌入式管理單元中的「憑證匯入」精靈再次匯入伺服器憑證。

不過，您可以使用「憑證匯入」精靈將根 CA 憑證和中繼 CA 憑證匯入至 Windows 憑證存放區。

將 TLS 連線卸載至中繼伺服器

2

您可以在 Horizon Server 與 Horizon Client 裝置之間設定中繼伺服器，以執行負載平衡和卸載 TLS 連線等工作。Horizon Client 裝置會透過 HTTPS 連線至中繼伺服器，這會將連線傳遞至面向外部的連線伺服器執行個體。

若要將 TLS 連線卸載至中繼伺服器，您必須完成幾項重要工作：

- 將中繼伺服器所使用的 TLS 憑證匯入至面向外部的 Horizon Server。
- 在面向外部的 Horizon Server 上設定外部 URL，使其符合可讓用戶端用來連線至中繼伺服器的 URL。
- 允許中繼伺服器與 Horizon Server 之間的 HTTP 連線。

本章節討論下列主題：

將 TLS 卸載伺服器的憑證匯入 Horizon Server

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

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

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

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

重要 下列主題中所述的案例，說明了在第三方元件與 VMware 元件之間共用 TLS 憑證的方法。此方法可能並非適合所有人，而且也不是執行此工作的唯一方式。

程序

1 從中繼伺服器下載 TLS 憑證

   您必須下載安裝在中繼伺服器上的 CA 簽署 TLS 憑證，使其能夠匯入面向外部的 Horizon Server 中。

2 從中繼伺服器下載私密金鑰

   您必須在中繼伺服器上下載與 TLS 憑證相關聯的私密金鑰。私密金鑰必須連同憑證匯入 Horizon Server 中。

3 將憑證檔案轉換為 PKCS#12 格式

   如果您已取得 PEM 或其他格式的憑證及其私密金鑰，您必須將其轉換為 PKCS#12 (PFX) 格式，才能將憑證匯入至 Horizon Server 上的 Windows 憑證存放區。如果您在 Windows 憑證存放區中使用「憑證匯入」精靈，則需要使用 PKCS#12 (PFX) 格式。

4 將簽署的伺服器憑證匯入 Windows 憑證存放區

   您必須將 TLS 伺服器憑證匯入至連線伺服器安裝所在 Windows Server 主機上的 Windows 本機電腦憑證存放區中。

5 修改憑證易記名稱

   若要設定連線伺服器執行個體，使其可辨識並使用 TLS 憑證，您必須將憑證易記名稱修改為 `vdm`。

6 將根憑證和中繼憑證匯入 Windows 憑證存放區中

   您必須將根憑證和憑證鏈結中的任何中繼憑證匯入 Windows 本機電腦憑證存放區中。

從中繼伺服器下載 TLS 憑證

您必須下載安裝在中繼伺服器上的 CA 簽署 TLS 憑證，使其能夠匯入面向外部的 Horizon Server 中。

程序

1 連線至中繼伺服器，然後尋找為傳送 HTTPS 要求之用戶端所提供的 TLS 憑證。

2 尋找並下載用於 Horizon 的 TLS 憑證。

範例： 從 F5 BIG-IP LTM 系統下載 TLS 憑證

此範例會使用 F5 BIG-IP Local Traffic Manager (LTM) 作為中繼伺服器。此範例旨在為您提供如何從您自己的中繼伺服器下載憑證的一般概念。

重要 這些是專屬於 F5 BIG-IP LTM 的步驟，可能不適用於新版本或其他 F5 產品。這些步驟不適用於其他廠商的中繼伺服器。

開始之前，請確認已使用 Horizon 部署 F5 BIG-IP LTM 系統。請確認您已完成 F5 部署指南《使用 VMware View 部署 BIG-IP LTM 系統》(位於 http://www.f5.com/pdf/deployment-guides/f5-vmware-view-dg.pdf 上) 中的工作。

1 連線至 F5 BIG-IP LTM 組態公用程式。

2 在導覽窗格的 [主要] 索引標籤上展開**本機流量**，然後按一下 **SSL 憑證**。

公用程式會顯示系統上安裝的憑證清單。

3 在 [名稱] 資料行中，按一下用於 Horizon 的憑證名稱。

4 在畫面底部，按一下**匯出**。

公用程式會在**憑證文字**方塊中顯示現有的 TLS 憑證。

5 在**憑證檔案**設定中，按一下**下載 *file_name***。

TLS 憑證會以 CRT 檔案的形式下載。

從中繼伺服器下載私密金鑰

您必須在中繼伺服器上下載與 TLS 憑證相關聯的私密金鑰。私密金鑰必須連同憑證匯入 Horizon Server 中。

程序

1 連線至中繼伺服器，然後尋找為傳送 HTTPS 要求之用戶端所提供的 TLS 憑證。

2 尋找用於 Horizon 的憑證，並下載其私密金鑰。

範例： 從 F5 BIG-IP LTM 系統下載私密金鑰

此範例會使用 F5 BIG-IP Local Traffic Manager (LTM) 作為中繼伺服器。此範例旨在為您提供如何從您自己的中繼伺服器下載私密金鑰的一般概念。

重要 這些是專屬於 F5 BIG-IP LTM 的步驟，可能不適用於新版本或其他 F5 產品。這些步驟不適用於其他廠商的中繼伺服器。

開始之前，請確認您已連線至 F5 BIG-IP LTM 組態公用程式。

1 在導覽窗格的 [主要] 索引標籤上展開**本機流量**，然後按一下 **SSL 憑證**。

公用程式會顯示系統上安裝的憑證清單。

2 在 [名稱] 資料行中，按一下用於 Horizon 的憑證名稱。

3 在功能表列上，按一下**金鑰**。

4 在畫面底部，按一下**匯出**。

公用程式會在**金鑰文字**方塊中顯示現有的私密金鑰。

5 在 [金鑰檔案] 設定中，按一下**下載 *file_name***。

私密金鑰會以 KEY 檔案的形式下載。

將憑證檔案轉換為 PKCS#12 格式

如果您已取得 PEM 或其他格式的憑證及其私密金鑰，您必須將其轉換為 PKCS#12 (PFX) 格式，才能將憑證匯入至 Horizon Server 上的 Windows 憑證存放區。如果您在 Windows 憑證存放區中使用「憑證匯入」精靈，則需要使用 PKCS#12 (PFX) 格式。

您可以透過下列其中一種方式取得憑證檔案：

- 您可以從 CA 取得憑證金鑰儲存區檔案。
- 您可以從 Horizon 部署中設定的中繼伺服器下載憑證及其私密金鑰。
- 您的組織會為您提供憑證檔案。

憑證檔案具有各種的格式。例如，PEM 格式通常用於 Linux 環境中。您的檔案可能具有包含下列副檔名的憑證檔案、金鑰檔案和 CSR 檔案：

```
server.crt
server.csr
server.key
```

CRT 檔案包含 CA 所傳回的 SSL 憑證。CSR 檔案是不需要的原始憑證簽署要求檔案。KEY 檔案包含私密金鑰。

必要條件

- 確認系統已安裝 OpenSSL。您可以從 `http://www.openssl.org` 下載 `openssl`。
- 確認 CA 傳回之 SSL 憑證的根憑證也可以在系統上使用。

程序

1. 將 CRT 和 KEY 檔案複製到 OpenSSL 安裝目錄。

   例如：`cd c:\OpenSSL-Win32\bin`

2. 開啟 Windows 命令提示字元，然後視需要導覽至 OpenSSL 安裝目錄。
3. 從憑證檔案和您的私密金鑰產生 PKCS#12 (PFX) 金鑰儲存區檔案。

   例如：`openssl pkcs12 -export -out server.p12 -inkey server.key -in server.crt -certfile CACert.crt`

   在此範例中，`CACert.crt` 是憑證授權機構所傳回之根憑證的名稱。

   Windows 憑證存放區也接受以 PFX 副檔名產生的金鑰儲存區。例如：`-out server.pfx`

4. 輸入匯出密碼以保護 PKCS#12 (PFX) 檔案。

將簽署的伺服器憑證匯入 Windows 憑證存放區

您必須將 TLS 伺服器憑證匯入至連線伺服器安裝所在 Windows Server 主機上的 Windows 本機電腦憑證存放區中。

此案例使用了 PKCS#12 (PFX) 格式的憑證檔案。

根據您的憑證檔案格式而定，包含在 keystore 檔案中的整個憑證鏈結可能會匯入至 Windows 本機電腦憑證存放區。例如，可能會匯入伺服器憑證、中繼憑證和根憑證。

對於其他類型的憑證檔案，只會將伺服器憑證匯入至 Windows 本機電腦憑證存放區。在此情況下，您必須採取額外的步驟，以匯入憑證鏈結中的根憑證和任何中繼憑證。

如需憑證的詳細資訊，請參閱 MMC 的憑證嵌入式管理單元中提供的 Microsoft 線上說明。

必要條件

確認 TLS 伺服器憑證是否為 PKCS@12 (PFX) 格式。請參閱將憑證檔案轉換為 PKCS#12 格式。

程序

1 在 Windows Server 主機的 MMC 視窗中，展開**憑證 (本機電腦)** 節點，並選取**個人**資料夾。

2 在 [動作] 窗格中，移至**更多動作 > 所有工作 > 匯入**。

3 在**憑證匯入**精靈中，按**下一步**並瀏覽至儲存憑證所在的位置。

4 選取憑證檔案，然後按一下**開啟**。

若要顯示憑證檔案類型，可以從**檔案名稱**下拉式功能表選取其檔案格式。

5 為包含在憑證檔案中的私密金鑰輸入密碼。

6 選取**將這個金鑰設成可匯出**。

7 選取**包含所有延伸內容**。

8 按**下一步**，然後再按一下**完成**。

新憑證會出現在**憑證 (本機電腦) > 個人 > 憑證**資料夾中。

9 確認新憑證包含私密金鑰。

a 在**憑證 (本機電腦) > 個人 > 憑證**資料夾中，按兩下新憑證。

b 在 [憑證資訊] 對話方塊的 [一般] 索引標籤中，確認顯示下列描述：這個憑證有一個對應的私密金鑰。

後續步驟

將憑證易記名稱修改為 **vdm**。

修改憑證易記名稱

若要設定連線伺服器執行個體，使其可辨識並使用 TLS 憑證，您必須將憑證易記名稱修改為 vdm。

必要條件

確認伺服器憑證已匯入 Windows 憑證存放區的**憑證 (本機電腦) > 個人 > 憑證**資料夾中。請參閱將簽署的伺服器憑證匯入 Windows 憑證存放區。

程序

1 在 Windows Server 主機的 MMC 視窗中，展開**憑證 (本機電腦)** 節點，並選取**個人 > 憑證**資料夾。

2 以滑鼠右鍵按一下核發給 VMware Horizon Server 主機的憑證，然後按一下**內容**。

3 在「一般」索引標籤上，刪除**易記名稱**文字並輸入 **vdm**。

4 按一下**套用**，然後再按一下**確定**。

5 確認在**個人 > 憑證**資料夾中沒有其他伺服器憑證的易記名稱為 **vdm**。

   a 找到任何其他伺服器憑證，在憑證上按一下滑鼠右鍵，然後按一下**內容**。

   b 如果該憑證具有易記名稱 **vdm**，則將其刪除，按一下**套用**，然後按一下**確定**。

後續步驟

將根憑證和中繼憑證匯入至 Windows 本機電腦憑證存放區。

匯入鏈結中的所有憑證後，您必須重新啟動連線伺服器服務，才能讓變更生效。

將根憑證和中繼憑證匯入 Windows 憑證存放區中

您必須將根憑證和憑證鏈結中的任何中繼憑證匯入 Windows 本機電腦憑證存放區中。

如果您從中繼伺服器匯入的 TLS 伺服器憑證是由連線伺服器主機已知且信任的根 CA 所簽署，且您的憑證鏈結中沒有中繼憑證，則可略過此工作。主機可能會信任常用的憑證授權機構。

程序

1 在 Windows Server 主機的 MMC 主控台中，展開**憑證 (本機電腦)** 節點，然後移至**受信任的根憑證授權單位 > 憑證**資料夾。

   - 如果您的根憑證位於此資料夾中，而且憑證鏈結中沒有任何中繼憑證，請跳至步驟 7。
   - 如果您的根憑證位於此資料夾中，且憑證鏈結中有中繼憑證，請跳至步驟 6。
   - 如果您的根憑證不在此資料夾中，請繼續進行步驟 2。

2 以滑鼠右鍵按一下**信任的根憑證授權機構 > 憑證**資料夾，然後按一下**所有工作 > 匯入**。

3 在**憑證匯入**精靈中，按**下一步**並瀏覽至儲存根 CA 憑證所在的位置。

4 選取根 CA 憑證檔案，然後按一下**開啟**。

5 依序按**下一步**、**下一步**，然後按一下**完成**。

6 如果您的伺服器憑證是由中繼 CA 所簽署，請將憑證鏈結中的所有中繼憑證匯入至 Windows 本機電腦憑證存放區。

   a 移至**憑證 (本機電腦) > 中繼憑證授權機構 > 憑證**資料夾。

   b 針對必須匯入的每個中繼憑證重複步驟 3 到 6。

7 重新啟動連線伺服器服務來讓您的變更生效。

8 如果您使用 HTML Access，請重新啟動 Blast 安全閘道服務。

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

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

您可以在連線至中繼伺服器的連線伺服器執行個體上設定外部 URL 設定。

如果您的網路環境混合了某些中繼伺服器與某些面向外部的連線伺服器執行個體，則連線至中繼伺服器的任何連線伺服器執行個體均需要外部 URL。

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

設定連線伺服器執行個體的外部 URL

您可以使用 Horizon Console 設定連線伺服器執行個體的外部 URL。

必要條件

- 確認已在連線伺服器執行個體上啟用安全通道連線。

程序

1. 在 Horizon Console 中，按一下**設定 > 伺服器**。
2. 依序選取**連線伺服器**和連線伺服器執行個體，然後按一下**編輯**。
3. 在**外部 URL** 文字方塊中輸入安全通道外部 URL。

   URL 必須包含通訊協定、用戶端可解析的主機名稱與連接埠號碼。

   例如：`https://myserver.example.com:443`

   備註 主機名稱無法解析時，如果您必須存取連線伺服器執行個體，則可以使用 IP 位址。不過，您聯繫的主機將不符合為連線伺服器執行個體設定的 TLS 憑證，因而導致存取遭封鎖，或只能在安全性降低的情況下存取。
4. 確認此對話方塊中的所有位址皆允許用戶端系統連接此連線伺服器執行個體。
5. 按一下**確定**。

允許來自中繼伺服器的 HTTP 連線

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

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

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

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

程序

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

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

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

必須以小寫輸入值 `http`。

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

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

4 儲存 `locked.properties` 檔案。

5 重新啟動連線伺服器服務來讓您的變更生效。

範例： locked.properties 檔案

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

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