为 Horizon 7 设置 TLS 证书的方案

2019 年 12 月

VMware Horizon 7 7.11

vmware®

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

如果您对本文档有任何意见或建议，请将反馈信息发送至：

docfeedback@vmware.com

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

威睿信息技术（中国）有限公司
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

为 Horizon 7 设置 TLS 证书的方案

《为 Horizon 7 设置 TLS 证书的方案》提供了一些示例来说明如何设置 TLS 证书以供 Horizon 7 服务器使用。第一个方案演示如何从证书颁发机构获取签名 TLS 证书，并确保证书具有可供 Horizon 7 Server 使用的格式。第二个方案说明了如何配置 Horizon 7 Server 来将 TLS 连接负载分流到中间服务器。

目标读者

本信息面向希望安装 Horizon 7，并需要获取 Horizon 7 Server 所用 TLS 证书的用户，或使用中间服务器将 TLS 连接负载分流到 Horizon 7 的用户。本文档中的信息专门为已熟练掌握虚拟机技术和数据中心操作、并具有丰富经验的 Windows 或 Linux 系统管理员编写。

从证书颁发机构获取 TLS 证书

1

VMware 强烈建议配置由有效证书颁发机构 (Certificate Authority, CA) 签名的 TLS 证书，以供 Horizon 连接服务器实例、安全服务器和 View Composer 实例使用。

在安装连接服务器实例、安全服务器或 View Composer 实例时，会生成默认的 TLS 证书。尽管默认的自签名证书可以用于测试目的，但还是应尽快更换它们。默认证书未由 CA 签名。如果使用未经 CA 签发的证书，不受信任的第三方将有可能伪装成您的服务器并截获流量。

在 Horizon 7 环境中，还应将随 vCenter Server 一起安装的默认证书替换为经由 CA 签名的证书。您可以使用 openTLS 为 vCenter Server 执行此任务。有关详细信息，请参阅 VMware 技术白皮书站点上的“替换 vCenter Server 证书”，其网址为 http://www.vmware.com/resources/techresources/。

本章讨论了以下主题：

确定本方案对您是否适用

可以通过将证书导入到 Horizon 7 Server 主机上的 Windows 本地计算机证书存储区中，来为 Horizon 7 配置证书。

您必须先生成证书签名请求 (Certificate Signing Request, CSR) 并从 CA 获取有效的签名证书，然后才能导入证书。如果未根据本方案介绍的示例过程生成 CSR，则您获取的证书及其私钥必须以 PKCS#12（以前称为 PFX）格式文件提供。

可通过多种方法从 CA 获取 TLS 证书。本方案演示如何使用 Microsoft `certreq` 实用程序生成 CSR 并将证书提供给 Horizon 7 Server 使用。如果您很熟悉所需的工具并且您的服务器上安装有这些工具，则可以使用其他方法。

使用本方案可解决以下问题：

- 您没有由 CA 签名的 TLS 证书，而且您也不知道如何获取它们
- 您拥有有效的签名 TLS 证书，但它们的格式不是 PKCS#12 (PFX)

如果您的组织提供了由 CA 签名的 TLS 证书，则您可以使用这些证书。您的组织可以使用有效的内部 CA 或第三方商业 CA。如果证书的格式不是 PKCS#12，则必须进行转换。请参阅将证书文件转换为 PKCS#12 格式。

如果您具有格式正确的签名证书，则可以将其导入 Windows 证书存储区，并将 Horizon 7 Server 配置为使用该证书。请参阅为 Horizon 7 Server 设置导入的证书。

选择正确的证书类型

您可以将不同类型的 TLS 证书用于 Horizon 7。为您的部署选择正确的证书类型是至关重要的。不同的证书类型具有不同的成本，具体取决于可以使用它们的服务器数。

请使用证书的完全限定域名 (Fully Qualified Domain Name, FQDN) 以遵循 VMware 安全建议，而无论选择哪种类型。不要使用简单的服务器名称或 IP 地址，即使内部域中的通信也是如此。

单服务器名称证书

您可以为特定服务器生成具有使用者名称的证书。例如：`dept.company.com`。

比如在只有一个连接服务器实例需要证书的情况下，这种类型的证书将会非常有用。

在将证书签名请求提交到 CA 时，您可以提供与证书关联的服务器名称。请确保 Horizon 7 Server 可以解析提供的服务器名称，以使其与证书的关联名称相匹配。

使用者备用名称

使用者备用名称 (Subject Alternative Name, SAN) 是一个在颁发证书时可添加到证书中的属性。可以使用该属性将使用者名称 (URL) 添加到证书中，以便它可以验证多个服务器。

例如，可为主机名为 `dept.company.com` 的服务器颁发证书。打算让通过安全服务器连接到 Horizon 7 的外部用户来使用该证书。在签发证书之前，您可以将 SAN `dept-int.company.com` 添加到证书，以便在启用了隧道的情况下，允许证书在负载平衡器背后的连接服务器实例或安全服务器上使用。

通配证书

可以生成一个通配证书，以便将其用于多个服务。例如：`*.company.com`。

如果多个服务器需要使用证书，则通配证书是非常有用的。除了 Horizon 7 以外，如果环境中的其他应用程序需要使用 TLS 证书，您也可以在这些服务器中使用通配证书。不过，如果使用与其他服务共享的通配证书，则 VMware Horizon 产品的安全性还取决于这些其他服务的安全性。

注　您只能在单个域级别使用通配证书。例如，可以将具有主体名称 `*.company.com` 的通配证书用于子域 `dept.company.com`，但不能用于 `dept.it.company.com`。

使用 Microsoft Certreq 生成证书签名请求和获取证书

要将证书提供给 Horizon 7 Server 使用，您必须创建配置文件，从配置文件生成证书签名请求 (CSR)，并将签名请求发送给 CA。当 CA 返回证书时，您必须将签名证书导入 Horizon 7 Server 主机上的 Windows 本地计算机证书存储区，在该位置证书将与以前生成的私钥结合。

CSR 可以通过多种方法生成，具体取决于证书本身的生成方式。

在 Windows Server 2008 R2 上提供了 Microsoft `certreq` 实用程序，可使用该实用程序生成 CSR 和导入签名证书。如果您要将请求发送给第三方 CA，使用 `certreq` 为 Horizon 7 获取证书是最快速、最简单的方法。

步骤

1 创建 CSR 配置文件。

Microsoft `certreq` 实用程序使用配置文件生成 CSR。您必须先创建配置文件，然后才能生成请求。可在托管将使用该证书的 Horizon 7 Server 的 Windows Server 计算机上创建配置文件并生成 CSR。

2 生成 CSR 并从 CA 请求签名证书

利用已完成的配置文件，您可以通过运行 `certreq` 实用程序生成 CSR。将请求发送给第三方 CA，该 CA 将返回签名证书。

3 确认 CSR 及其私钥存储在 Windows 证书存储区中

如果您使用 `certreq` 实用程序生成 CSR，该实用程序还会生成一个关联的私钥。该实用程序将 CSR 及私钥存储在生成该 CSR 时所在计算机的 Windows 本地计算机证书存储区中。您可以通过 Microsoft 管理控制台 (MMC) 证书管理单元来确认 CSR 及私钥已正确存储。

4 使用 Certreq 导入签名证书

如果您有 CA 签名的证书，可以将证书导入 Horizon 7 Server 主机上的 Windows 本地计算机证书存储区。

5 为 Horizon 7 Server 设置导入的证书

将服务器证书导入到 Windows 本地计算机证书存储区后，您必须执行其他步骤以允许 Horizon 7 Server 使用该证书。

创建 CSR 配置文件。

Microsoft `certreq` 实用程序使用配置文件生成 CSR。您必须先创建配置文件，然后才能生成请求。可在托管将使用该证书的 Horizon 7 Server 的 Windows Server 计算机上创建配置文件并生成 CSR。

前提条件

收集填写配置文件所需的信息。您必须知道 Horizon 7 Server 的 FQDN、组织单位、组织、城市、州和国家/地区，才能填写主体名称。

步骤

1 打开文本编辑器，将以下文本（包括开始标记和结束标记）粘贴到文件中。

```
;----------------- 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 7 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

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

如果复制和粘贴文本时在 `Subject =` 行中添加了额外的换行 (CR/LF) 符，请将换行符删除。

2 使用您的 Horizon 7 Server 和部署的相应值更新 `Subject` 属性。

例如：`CN=dept.company.com`

为了遵循 VMware 安全建议，请使用客户端设备在连接主机时使用的完全限定域名 (FQDN)。不要使用简单的服务器名称或 IP 地址，即使内部域中的通信也是如此。

某些 CA 不允许为 state 属性使用缩写形式。

3 （可选） 更新 `Keylength` 属性。

除非您确实需要一个不同的 `KeyLength` 大小，否则默认值 2048 就已足够。许多 CA 要求最小值为 2048。较大的密钥大小会更安全，但对性能的影响会比较大。

虽然也支持值为 1024 的 `KeyLength`，但是国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 不建议使用此大小的密钥，因为计算机越来越强大，很可能能够破解更强大的加密。

重要事项 请勿生成小于 1024 的 `KeyLength` 值。适用于 Windows 的 Horizon Client 将不对 Horizon 7 Server 上生成的、`KeyLength` 值小于 1024 的证书进行验证，Horizon Client 设备将无法连接到 Horizon 7。连接服务器执行的证书验证也会失败，进而导致受影响的 Horizon 7 Server 在 Horizon Administrator 仪表板中显示为红色。

4 将文件另存为 `request.inf`。

后续步骤

从配置文件生成 CSR。

生成 CSR 并从 CA 请求签名证书

利用已完成的配置文件，您可以通过运行 `certreq` 实用程序生成 CSR。将请求发送给第三方 CA，该 CA 将返回签名证书。

前提条件

- 确认您已完成 CSR 配置文件。请参阅创建 CSR 配置文件。。
- 在 CSR 配置文件所在的计算机上执行此过程中所述的 `certreq` 操作。

步骤

1 在**开始**菜单中右键单击**命令提示符**并选择**以管理员身份运行**以打开命令提示符。

2 导航到保存 `request.inf` 文件的目录。

例如：**`cd c:\certificates`**

3 生成 CSR 文件。

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

4 按照 CA 的注册流程，使用 CSR 文件的内容将证书请求提交给 CA。

a 当您将请求提交给 CA 时，CA 会提示您选择将安装该证书的服务器类型。由于 Horizon 7 使用 Microsoft 证书 MMC 管理证书，请选择适用于 Microsoft、Microsoft IIS 7 或类似类型服务器的证书。CA 应会生成一个格式符合 Horizon 7 使用需要的证书。

b 如果您请求单服务器名称证书，请使用 Horizon Client 设备可解析为此 Horizon 7 Server 的 IP 地址的名称。计算机用来连接 Horizon 7 Server 的名称应该与证书的关联名称相一致。

注 CA 可能会要求您将 CSR 文件（例如 `certreq.txt`）的内容复制并粘贴到 Web 表单中。您可以使用文本编辑器复制 CSR 文件的内容。请确保复制内容包括开始标记和结束标记。例如：

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

在对您的公司进行核查后，CA 会根据 CSR 中的信息创建服务器证书，使用私钥对其进行签名，然后将证书发送给您。

CA 还会向您发送一个根 CA 证书和一个中间 CA 证书（如果适用）。

5 将证书文本文件重命名为 `cert.cer`。

请确保该文件位于生成证书请求的 Horizon 7 Server 上。

6 将根 CA 证书文件和中间 CA 证书文件分别重命名为 `root.cer` 和 `intermediate.cer`。

请确保这些文件位于生成证书请求的 Horizon 7 Server 上。

注 当您使用 `certreq` 实用程序将证书导入 Windows 本地计算机证书存储区时，这些证书无需采用 PKCS#12 (PFX) 格式。如果使用证书导入向导将证书导入到 Windows 证书存储区，则需要使用 PKCS#12 (PFX) 格式。

后续步骤

确认 CSR 文件及其私钥存储在 Windows 本地计算机证书存储区中。

确认 CSR 及其私钥存储在 Windows 证书存储区中

如果您使用 `certreq` 实用程序生成 CSR，该实用程序还会生成一个关联的私钥。该实用程序将 CSR 及私钥存储在生成该 CSR 时所在计算机的 Windows 本地计算机证书存储区中。您可以通过 Microsoft 管理控制台 (MMC) 证书管理单元来确认 CSR 及私钥已正确存储。

私钥以后必须随签名证书一起使用，以确保 Horizon 7 Server 能够正确导入和使用证书。

前提条件

- 确认已使用 `certreq` 实用程序生成 CSR，并且已从 CA 请求签名证书。请参阅生成 CSR 并从 CA 请求签名证书。
- 熟悉将证书管理单元添加到 Microsoft 管理控制台 (MMC) 的过程。请参阅《Horizon 7 安装指南》文档中“为 Horizon 7 Server 配置 TLS 证书”一章的“将证书管理单元添加至 MMC”。

步骤

1 在 Windows Server 计算机上，将证书管理单元添加到 MMC。

2 在 Windows Server 计算机的 MMC 窗口中，展开**证书 (本地计算机)** 节点并选择**证书注册申请**文件夹。

3 展开**证书注册申请**文件夹并选择**证书**文件夹。

4 确认证书项显示在**证书**文件夹中。

颁发给和**颁发者**字段必须显示在用于生成 CSR 的 `request.inf` 文件的 **`subject:CN`** 字段中输入的域名。

5 通过以下步骤之一确认证书含有私钥：

- 确认证书图标上显示有黄色钥匙图案。
- 双击证书，确认在“证书信息”对话框中显示有以下声明：您有一个与该证书对应的私钥。

后续步骤

将证书导入 Windows 本地计算机证书存储区。

使用 Certreq 导入签名证书

如果您有 CA 签名的证书，可以将证书导入 Horizon 7 Server 主机上的 Windows 本地计算机证书存储区。

如果您使用 `certreq` 实用程序生成 CSR，则证书私钥位于生成 CSR 的服务器本地。要使证书能够正常使用，必须与私钥结合使用。使用此过程中所示的 `certreq` 命令，可确保证书和私钥正常组合并导入 Windows 证书存储区。

如果您使用其他方法从 CA 获取签名的证书，则可以使用 Microsoft 管理控制台 (MMC) 管理单元中的证书导入向导，将证书导入 Windows 证书存储区。《Horizon 7 安装指南》文档中的“为 Horizon 7 Server 配置 TLS 证书”部分介绍了此方法。

前提条件

- 确认您已从 CA 收到签名证书。请参阅生成 CSR 并从 CA 请求签名证书。
- 在生成 CSR 并存储签名证书的计算机上，执行此过程中所述的 `certreq` 操作。

步骤

1. 在**开始**菜单中右键单击**命令提示符**并选择**以管理员身份运行**以打开命令提示符。
2. 导航到保存签名证书文件（如 `cert.cer`）的目录。

   例如：`cd c:\certificates`
3. 通过运行 `certreq –accept` 命令导入签名的证书。

   例如：`certreq –accept cert.cer`

该证书将导入到 Windows 本地计算机证书存储区。

后续步骤

将导入的证书配置为可由 Horizon 7 Server 使用。请参阅为 Horizon 7 Server 设置导入的证书。

为 Horizon 7 Server 设置导入的证书

将服务器证书导入到 Windows 本地计算机证书存储区后，您必须执行其他步骤以允许 Horizon 7 Server 使用该证书。

步骤

1. 确认服务器证书已成功导入。
2. 将证书的友好名称更改为 **vdm**。

   vdm 必须为小写。具有友好名称 **vdm** 的其他任何证书都必须重新命名，否则必须从这些证书移除友好名称。

   您无需修改 View Composer 所用证书的友好名称。

3 在 Windows 证书存储区中安装根 CA 证书和中间 CA 证书。

4 重新启动连接服务器服务、安全服务器服务或 View Composer 服务，以让该服务开始使用新证书。

5 如果您使用 HTML Access，请重新启动 VMware View Blast 安全网关服务。

6 如果在 View Composer Server 上设置证书，您可能需要执行其他步骤。

   - 如果在安装 View Composer 之后设置新的证书，则必须运行 `SviConfig ReplaceCertificate` 实用程序以替换绑定至 View Composer 所用端口的证书。
   - 如果在安装 View Composer 之前设置新证书，则不必运行 `SviConfig ReplaceCertificate` 实用程序。运行 View Composer 安装程序时，您可以选择用 CA 签名的新证书取代默认的自签名证书。

   有关更多信息，请参阅《Horizon 7 安装指南》文档中的“将新 TLS 证书绑定至 View Composer 使用的端口”。

要在此过程中执行这些任务，请参阅以下主题：

- 修改证书的友好名称
- 将根证书和中间证书导入 Windows 证书存储区

有关更多信息，请参阅《Horizon 7 安装指南》文档中的“配置连接服务器、安全服务器或 View Composer 以使用新 TLS 证书”。

注 此处并未列出《Horizon 7 安装指南》中的主题“将签名的服务器证书导入到 Windows 证书存储区”，因为您已经使用 `certreq` 实用程序导入了服务器证书。您不应使用 MMC 管理单元中的“证书导入”向导再次导入此服务器证书。

但是，您可以使用“证书导入”向导将根 CA 证书和中间 CA 证书导入到 Windows 证书存储区中。

将 TLS 连接负载分流到中间服务器

2

您可以在 Horizon 7 Server 和 Horizon Client 设备之间设置中间服务器，以执行负载平衡和负载分流 TLS 连接之类的任务。Horizon Client 设备通过 HTTPS 连接到中间服务器，然后中间服务器将连接传递到对外的连接服务器实例或安全服务器。

要将 TLS 连接负载分流到中间服务器，您必须完成以下几个关键任务：

- 将中间服务器使用的 TLS 证书导入到对外的 Horizon 7 Server。
- 在对外的 Horizon 7 Server 上，将外部 URL 设置为与客户端可用来连接到中间服务器的 URL 相匹配。
- 允许中间服务器和 Horizon 7 Server 之间的 HTTP 连接。

本章讨论了以下主题：

将 TLS 负载分流服务器的证书导入到 Horizon 7 Server

如果将 TLS 连接负载分流到中间服务器，您必须将中间服务器的证书导入到连接服务器实例或连接到中间服务器的安全服务器中。同一个 TLS 服务器证书必须同时位于正在进行负载分流的中间服务器和连接到中间服务器并且已被负载分流的 Horizon 7 Server 中。

如果您部署安全服务器，则中间服务器和连接到该中间服务器的安全服务器必须拥有相同的 TLS 证书。您不必在已与安全服务器配对但未直接连接到中间服务器的连接服务器实例上安装相同的 TLS 证书。

如果您未部署安全服务器，或者如果您的混合网络环境包含一些安全服务器和一些面向外部的连接服务器实例，则中间服务器和连接到该中间服务器的任何连接服务器实例都必须拥有相同的 TLS 证书。

如果中间服务器的证书未安装在连接服务器实例或安全服务器上，则客户端无法验证其与 Horizon 7 的连接。在这种情况下，Horizon 7 server 发送的证书指纹与 Horizon Client 连接的中间服务器上的证书不一致。

不要混淆负载平衡与 TLS 负载分流。前者适用于任何被配置为提供 TLS 负载分流功能的设备，包括某些类型的负载平衡程序。但是，单纯的负载平衡不要求在设备之间复制证书。

重要事项 以下主题中介绍的方案展示了在第三方组件与 VMware 组件之间共享 TLS 证书的一种方法。此方法可能并非适合所有人，这也不是执行该任务的唯一方法。

步骤

1 从中间服务器下载 TLS 证书

必须先下载在中间服务器上安装的 CA 签名的 TLS 证书，然后才能将其导入到对外的 Horizon 7 Server。

2 从中间服务器下载私钥

必须下载与中间服务器上的 TLS 证书关联的私钥。私钥必须随证书一起导入到 Horizon 7 Server 上。

3 将证书文件转换为 PKCS#12 格式

如果您获取的证书及其私钥采用的是 PEM 格式或其他格式，则必须先将其转换为 PKCS#12 (PFX) 格式，然后才能将该证书导入到 Horizon 7 Server 上的 Windows 证书存储区中。如果您使用 Windows 证书存储区中的“证书导入”向导，则需要使用 PKCS#12 (PFX) 格式。

4 将签名的服务器证书导入到 Windows 证书存储区

您必须将 TLS 服务器证书导入到安装了连接服务器实例或安全服务器服务的 Windows Server 主机上的 Windows 本地计算机证书存储区中。

5 修改证书的友好名称

要将连接服务器实例或安全服务器配置为识别并使用 TLS 证书，必须将证书的友好名称修改为 `vdm`。

6 将根证书和中间证书导入 Windows 证书存储区

您必须将根证书和证书链中的任何中间证书导入 Windows 本地计算机证书存储区。

从中间服务器下载 TLS 证书

必须先下载在中间服务器上安装的 CA 签名的 TLS 证书，然后才能将其导入到对外的 Horizon 7 Server。

步骤

1 连接到中间服务器，并找到向发送 HTTPS 请求的客户端提供的 TLS 证书。

2 找到并下载用于 Horizon 7 的 TLS 证书。

示例： 从 F5 BIG-IP LTM 系统下载 TLS 证书

此示例使用 F5 BIG-IP 本地流量管理器 (Local Traffic Manager, LTM) 作为中间服务器。该示例旨在让您大致了解如何从您自己的中间服务器下载证书。

重要事项 这些步骤是特定于 F5 BIG-IP LTM 的操作，可能不适用于新版本或其他 F5 产品。这些步骤不适用于其他供应商的中间服务器。

在开始之前，请确定已在 Horizon 7 中部署 F5 BIG-IP LTM 系统。确认您已完成 F5 部署指南《在 VMware View 中部署 BIG-IP LTM 系统》（网址为 http://www.f5.com/pdf/deployment-guides/f5-vmware-view-dg.pdf）中的任务。

1 连接 F5 BIG-IP LTM 配置实用程序。

2 在导航窗格的“主页”选项卡上，展开**本地流量**，然后单击 **SSL 证书**。

该实用程序会显示系统中已安装证书的列表。

3 在“名称”列中，单击用于 Horizon 7 的证书的名称。

4 在屏幕底部，单击**导出**。

该实用程序会在**证书文本**框中显示现有的 TLS 证书。

5 从**证书文件**设置中，单击**下载 *file_name***。

将以 CRT 文件形式下载 TLS 证书。

从中间服务器下载私钥

必须下载与中间服务器上的 TLS 证书关联的私钥。私钥必须随证书一起导入到 Horizon 7 Server 上。

步骤

1 连接到中间服务器，并找到向发送 HTTPS 请求的客户端提供的 TLS 证书。

2 找到用于 Horizon 7 的证书并下载其私钥。

示例： 从 F5 BIG-IP LTM 系统下载私钥

此示例使用 F5 BIG-IP 本地流量管理器 (LTM) 作为中间服务器。该示例旨在让您大致了解如何从您自己的中间服务器下载私钥。

重要事项 这些步骤是特定于 F5 BIG-IP LTM 的操作，可能不适用于新版本或其他 F5 产品。这些步骤不适用于其他供应商的中间服务器。

在开始之前，请确定已连接到 F5 BIG-IP LTM 配置实用程序。

1 在导航窗格的“主页”选项卡上，展开**本地流量**，然后单击 **SSL 证书**。

该实用程序会显示系统中已安装证书的列表。

2 在“名称”列中，单击用于 Horizon 7 的证书的名称。

3 在菜单栏中，单击**密钥**。

4 在屏幕底部，单击**导出**。

该实用程序会在**密钥文本**框中显示现有的私钥。

5 从“密钥文件”设置中，单击**下载 *file_name***。

将以 KEY 文件形式下载私钥。

将证书文件转换为 PKCS#12 格式

如果您获取的证书及其私钥采用的是 PEM 格式或其他格式，则必须先将其转换为 PKCS#12 (PFX) 格式，然后才能将该证书导入到 Horizon 7 Server 上的 Windows 证书存储区中。如果您使用 Windows 证书存储区中的“证书导入”向导，则需要使用 PKCS#12 (PFX) 格式。

您可以通过以下方法之一获取证书文件：

- 从 CA 获取证书密钥库文件。
- 从在 Horizon 7 部署中设置的中间服务器下载证书及其私钥。
- 您的组织为您提供证书文件。

证书文件有多种格式：例如，在 Linux 环境中通常使用 PEM 格式。您的文件可能包括具有以下扩展名的证书文件、密钥文件和 CSR 文件：

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

CRT 文件包含由 CA 返回的 SSL 证书。CSR 文件是原始的证书签名请求文件，不需要此文件。KEY 文件包含私钥。

前提条件

- 确认已在系统中安装 OpenSSL。可以从 `http://www.openssl.org` 下载 `openssl`。
- 确认系统中也有 CA 返回的 SSL 证书的根证书。

步骤

1 将 CRT 文件和 KEY 文件复制到 OpenSSL 安装目录。

例如：`cd c:\OpenSSL-Win32\bin`

2 打开 Windows 命令提示符，如果需要，请导航到 OpenSSL 安装目录。

3 从证书文件和私钥生成 PKCS#12 (PFX) 密钥库文件。

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

在此示例中，`CACert.crt` 是证书颁发机构所返回根证书的名称。

Windows 证书存储区还接受使用 PFX 扩展名生成的密钥库。例如：`-out server.pfx`

4 键入导出密码以保护 PKCS#12 (PFX) 文件。

将签名的服务器证书导入到 Windows 证书存储区

您必须将 TLS 服务器证书导入到安装了连接服务器实例或安全服务器服务的 Windows Server 主机上的 Windows 本地计算机证书存储区中。

该方案使用 PKCS#12 (PFX) 格式的证书文件。

根据您的证书文件格式，密钥存储文件中的整个证书链可能都会被导入到 Windows 本地计算机证书存储区。例如，可能会导入服务器证书、中间证书和根证书。

对于其他类型的证书文件，只有服务器证书会被导入到 Windows 本地计算机证书存储区。这种情况下，您必须单独导入证书链中的根证书和全部中间证书。

有关证书的更多信息，请参考 MMC 证书插件中提供的 Microsoft 联机帮助。

前提条件

确认 TLS 服务器证书采用的是 PKCS@12 (PFX) 格式。请参阅将证书文件转换为 PKCS#12 格式。

步骤

1 在 Windows Server 主机上的 MMC 窗口中，展开**证书 (本地计算机)** 节点并选择**个人**文件夹。

2 在“操作”窗格中，转到**更多操作 > 所有任务 > 导入**。

3 在**证书导入**向导中，单击**下一步**并浏览至存储证书的位置。

4 选择证书文件并单击**打开**。

要显示您的证书文件类型，可以从**文件名**下拉菜单中选择其文件格式。

5 键入证书文件中所含私钥的密码。

6 选择**将此密钥标记为可导出**。

7 选择**包含所有已扩展属性**。

8 单击**下一步**，然后单击**完成**。

新证书会显示在**证书 (本地计算机) > 个人 > 证书**文件夹中。

9 确认新证书包含私钥。

a 在**证书 (本地计算机) > 个人 > 证书**文件夹中，双击新证书。

b 在“证书信息”对话框的“常规”选项卡中，确认显示有以下语句：您有一个与该证书对应的私钥 (You have a private key that corresponds to this certificate)。

后续步骤

将证书的友好名称修改为 **vdm**。

修改证书的友好名称

要将连接服务器实例或安全服务器配置为识别并使用 TLS 证书，必须将证书的友好名称修改为 vdm。

前提条件

确认已将服务器证书导入到 Windows 证书存储区的**证书 (本地计算机) > 个人 > 证书**文件夹中。请参阅将签名的服务器证书导入到 Windows 证书存储区。

步骤

1 在 Windows Server 主机上的 MMC 窗口中，展开**证书 (本地计算机)** 节点并选择**个人 > 证书**文件夹。

2 右键单击颁发给 Horizon 7 Server 主机的证书，然后单击**属性**。

3 在“常规”选项卡上，删除**友好名称**文本并键入 **vdm**。

4 单击**应用**，然后单击**确定**。

5 确认**个人 > 证书**文件夹中没有其他服务器证书采用友好名称 **vdm**。

   a 查找任何其他服务器证书，右键单击证书，然后单击**属性**。

   b 如果证书的友好名称为 **vdm**，请删除该名称，单击**应用**，然后单击**确定**。

后续步骤

将根证书和中间证书导入到 Windows 本地计算机证书存储区中。

导入证书链中的所有证书后，必须重新启动连接服务器服务或安全服务器服务以使所做的更改生效。

将根证书和中间证书导入 Windows 证书存储区

您必须将根证书和证书链中的任何中间证书导入 Windows 本地计算机证书存储区。

如果您从中间服务器导入的 TLS 服务器证书由连接服务器主机信任的已知根 CA 签发，且您的证书链中没有中间证书，则可以跳过此任务。常用的证书颁发机构都可能受主机信任。

步骤

1 在 Windows Server 主机上的 MMC 控制台中，展开**证书 (本地计算机)** 节点并转到**受信任的根证书颁发机构 > 证书**文件夹。

   - 如果您的根证书位于此文件夹，且证书链中没有中间证书，则跳至步骤 7。
   - 如果您的根证书位于此文件夹，且证书链中有中间证书，则跳至步骤 6。
   - 如果您的根证书不在此文件夹，则执行步骤 2。

2 右键单击**受信任的根证书颁发机构 > 证书**文件夹，然后单击**所有任务 > 导入**。

3 在**证书导入**向导中，单击**下一步**并浏览至存储根 CA 证书的位置。

4 选择根 CA 证书文件并单击**打开**。

5 连续单击**下一步**，然后单击**完成**。

6 如果您的服务器证书由中间 CA 签发，请将证书链中的所有中间证书导入 Windows 本地计算机证书存储区。

   a 转到**证书 (本地计算机) > 中间证书颁发机构 > 证书**文件夹。

   b 针对每个必须导入的中间证书重复执行步骤 3 到步骤 6。

7 重新启动连接服务器服务或安全服务器服务，使所做的更改生效。

8 如果您使用 HTML Access，请重新启动 VMware View Blast 安全网关服务。

将 Horizon 7 Server 外部 URL 设置为将客户端指向 TLS 负载分流服务器

如果 TLS 负载分流到中间服务器，并且 Horizon Client 设备使用安全加密链路连接 Horizon 7，则必须将安全加密链路外部 URL 设置为客户端可以用来访问中间服务器的地址。

在连接到中间服务器的连接服务器实例或安全服务器上配置外部 URL 设置。

如果部署安全服务器，则安全服务器需要外部 URL，但与安全服务器配对的连接服务器不需要。

如果未部署安全服务器，或者使用包含部分安全服务器和部分对外的连接服务器实例的混合网络环境，则连接到中间服务器的任何连接服务器实例都需要使用外部 URL。

注　无法对来自 PCoIP 安全网关 (PCoIP Secure Gateway, PSG) 或 Blast 安全网关的 TLS 连接进行负载分流。PCoIP 外部 URL 和 Blast 安全网关外部 URL 必须允许客户端连接到托管 PSG 和 Blast 安全网关的计算机。除非规划为在中间服务器与 Horizon 7 Server 之间需要使用 TLS 连接，否则不要将 PCoIP 外部 URL 和 Blast 外部 URL 重置为指向中间服务器。

设置连接服务器实例的外部 URL

您可以使用 Horizon Administrator 配置连接服务器实例的外部 URL。

前提条件

- 确认在连接服务器实例上启用了安全加密链路连接。

步骤

1. 在 Horizon Administrator 中，单击 **View 配置 > 服务器**。
2. 在“连接服务器”选项卡中，选择连接服务器实例，然后单击**编辑**。
3. 在**外部 URL** 文本框中键入安全加密链路的外部 URL。

   URL 必须包含协议、客户端可解析的主机名和端口号。

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

   注　当主机名不可解析时，如果您需要访问连接服务器实例，则可以使用 IP 地址。但是，您连接的主机将与为连接服务器实例配置的 TLS 证书不匹配，从而导致访问被阻止或访问的安全性降低。
4. 确认此对话框中的所有地址都允许客户端系统访问此连接服务器实例。
5. 单击**确定**。

修改安全服务器的外部 URL

您可以使用 Horizon Administrator 修改安全服务器的外部 URL。

前提条件

- 确认与此安全服务器配对的连接服务器实例上已启用安全加密链路连接。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。

2 在“安全服务器”选项卡中，选择安全服务器并单击**编辑**。

3 在**外部 URL** 文本框中键入安全加密链路的外部 URL。

URL 必须包含协议、客户端可解析的安全服务器主机名和端口号。

例如：`https://myserver.example.com:443`

注 如果您需要在主机名不可解析时访问安全服务器，可以使用 IP 地址。但您连接的主机将与为安全服务器实例配置的 TLS 证书不匹配，导致访问被阻止或访问的安全性降低。

4 确认此对话框中的所有地址都允许客户端系统连接此安全服务器主机。

5 单击**确定**保存更改。

Horizon Administrator 会将更新的外部 URL 发送到安全服务器。您无需重新启动安全服务器，所做的更改即可生效。

允许源自中间服务器的 HTTP 连接

TLS 负载分流到中间服务器后，您可以将连接服务器实例或安全服务器配置为允许源自面向客户端的中间设备的 HTTP 连接。中间设备必须接受 HTTPS 作为 Horizon Client 连接。

要允许在 Horizon 7 Server 与中间设备之间建立 HTTP 连接，必须在允许 HTTP 连接的每个连接服务器实例和安全服务器上配置 `locked.properties` 文件。

即使允许在 Horizon 7 Server 与中间设备之间建立 HTTP 连接，也不能在 Horizon 7 中禁用 TLS。Horizon 7 Server 继续接受 HTTPS 连接以及 HTTP 连接。

注 如果您的 Horizon Client 使用智能卡身份验证，这些客户端必须直接与连接服务器或安全服务器建立 HTTPS 连接。智能卡身份验证不支持 TLS 负载分流。

步骤

1 在连接服务器或安全服务器主机的 TLS/SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

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

2 要配置 Horizon 7 server 的协议，请添加 `serverProtocol` 属性并将其设置为 `http`。

值 `http` 必须以小写键入。

3 （可选） 添加属性以在 Horizon 7 server 上配置非默认 HTTP 侦听端口和网络接口。

- 要将 HTTP 侦听端口从 80 更改为其他端口，请将 `serverPortNonTLS` 设置为中间设备已配置连接的另一个端口号。

- 如果 Horizon 7 Server 具有多个网络接口，而您希望该服务器只侦听一个接口上的 HTTP 连接，请将 `serverHostNonTLS` 设置为该网络接口的 IP 地址。

4 保存 `locked.properties` 文件。

5 重新启动连接服务器服务或安全服务器服务，使所做的更改生效。

示例： locked.properties 文件

此文件允许与 Horizon 7 Server 建立非 TLS HTTP 连接。Horizon 7 Server 面向客户端的网络接口的 IP 地址为 10.20.30.40。此服务器使用默认端口 80 来侦听 HTTP 连接。值 `http` 必须为小写。

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