Horizon 7 の TLS 証明書設定のシナリオ

変更：2019 年 3 月 14 日

VMware Horizon 7 7.8

vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。
https://docs.vmware.com/jp/
VMware の Web サイトでは、最新の製品アップデートを提供しています。
本書に関するご意見、ご要望をお寄せください。フィードバック送信先：
docfeedback@vmware.com

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

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

内容

Horizon 7 の TLS 証明書設定のシナリオ

『Horizon 7 の TLS 証明書設定のシナリオ』に、Horizon 7 サーバが使用する TLS 証明書の設定例が記載されています。最初のシナリオは、認証局から署名付き TLS 証明書を取得し、その証明書が Horizon 7 Server で使用できる形式であることを確認する方法を示したものです。2 番目のシナリオは、TLS 接続を中間サーバにオフロードするように Horizon 7 Server を構成する方法を示します。

対象読者

この情報は、Horizon 7 をインストールしようとし、Horizon 7 Server が使用する TLS 証明書を取得する必要があるすべての方、または Horizon 7 への TLS 接続をオフロードするために中間サーバを使用するすべての方を対象としています。本書に記載されている情報は、仮想マシンのテクノロジーとデータセンターの操作に精通した、経験豊富な Windows または Linux システム管理者向けに書かれています。

認証局からの TLS 証明書の取得

1

VMware では、Horizon 接続サーバ インスタンス、セキュリティ サーバ、および View Composer サービス インスタンスが使用するために、有効な認証局 (CA) が署名した TLS 証明書を構成することを強く推奨しています。

接続サーバ インスタンス、セキュリティ サーバ、または View Composer インスタンスをインストールするときに、デフォルトの TLS 証明書が生成されます。デフォルトの自己署名証明書をテスト用に使用できますが、できるだけ早くこれらを置き換えます。デフォルト証明書は、認証局 (CA) によって署名されていません。CA によって署名されていない証明書を使用すると、信頼されていないパーティがユーザーのサーバになりすましてトラフィックを傍受できる可能性があります。

また、Horizon 7 環境では、vCenter Server でインストールされたデフォルト証明書は、認証局 (CA) によって署名された証明書に置き換える必要があります。**openTLS** を使用して、vCenter Server 用にこのタスクを実行できます。詳細については、VMware のテクニカル ペーパー サイト (http://www.vmware.com/resources/techresources/) の「Replacing vCenter Server Certificates」を参照してください。

この章には、次のトピックが含まれています。

- このシナリオが適用対象かどうかの確認
- 正しい証明書タイプの選択
- Microsoft Certreq を使用した証明書署名要求の生成および証明書の取得

このシナリオが適用対象かどうかの確認

Horizon 7 Server ホスト上の Windows ローカル コンピュータ証明書ストアに証明書をインポートすることで、Horizon 7 の証明書を構成します。

証明書をインポートする前には、証明書署名要求 (CSR) を生成し、有効な署名付き証明書を CA から取得する必要があります。CSR がこのシナリオで説明するサンプル手順に従って生成されない場合は、最終的な証明書とプライベート キーが PKCS#12（以前の PFX）形式のファイルで使用できることが必要です。

TLS 証明書を CA から取得する方法は多数あります。このシナリオでは、Microsoft **certreq** ユーティリティを使用して CSR を生成し、Horizon 7 Server で証明書を使用できるようにする方法を示します。必要なツールに慣れていて、これらのツールがサーバにインストールされている場合には、別の方法で行うこともできます。

このシナリオは、次の問題を解決するために使用します。

- CA によって署名された TLS 証明書がなく、証明書の取得方法がわからない

- 署名付きの有効な TLS 証明書はあるが、PKCS#12 (PFX) 形式ではない

組織が CA によって署名された TLS 証明書を提供している場合には、これらの証明書を使用できます。組織は、有効な内部 CA か、サードパーティ製の商用 CA を使用できます。証明書が PKCS#12 形式でない場合は、その証明書を変換する必要があります。「証明書ファイルの PKCS#12 形式への変換」を参照してください。

正しい形式の署名付き証明書がある場合は、その証明書を Windows 証明書ストアにインポートして、それを使用できるように Horizon 7 Server を構成できます。「Horizon 7 Server のためのインポートされた証明書の設定」を参照してください。

正しい証明書タイプの選択

Horizon 7 では、異なるタイプの TLS 証明書を使用できます。導入するのに適したタイプの証明書を選択することが重要です。各タイプの証明書は、証明書を使用できるサーバの数に応じてコストが異なります。

どのタイプの証明書を選択した場合でも、証明書の完全修飾ドメイン名 (FQDN) を使用し、VMware のセキュリティに関する推奨事項に従ってください。内部ドメインの範囲内の通信にも、シンプルなサーバ名や IP アドレスは使用しないでください。

単一サーバ名証明書

特定のサーバのサブジェクト名を含む証明書を生成できます。たとえば `dept.company.com` のようにします。

このタイプの証明書が役立つのは、たとえば、証明書を必要とする接続サーバ インスタンスが 1 つのみの場合です。

証明書署名要求を CA に送信するときは、証明書に関連付けられたサーバ名を指定します。ユーザーが指定したサーバ名を Horizon 7 Server が解決でき、証明書に関連付けられた名前とそのサーバ名が一致することを確認します。

サブジェクトの別名

サブジェクトの別名 (SAN) は、発行する証明書に追加できる属性です。この属性は、証明書にサブジェクト名 (URL) を追加して、複数のサーバを検証できるようにするために使用します。

たとえば、証明書はホスト名が `dept.company.com` のサーバに対して発行されるとします。この証明書は、セキュリティ サーバを介して Horizon 7 に接続する外部ユーザーに使用されることを意図しています。この証明書が発行される前に、SAN `dept-int.company.com` を証明書に追加し、トンネルが有効にされるときに、ロード バランサの背後の接続サーバ インスタンスまたはセキュリティ サーバでこの証明書が使用されることを許可できます。

ワイルドカード証明書

ワイルドカード証明書は、複数のサービスで使用できるようにするために生成されます。たとえば `*.company.com` のような証明書です。

ワイルドカードは、多数のサーバが証明書を必要とする場合に便利です。Horizon 7 の他に、環境内の他のアプリケーションが TLS 証明書を必要とする場合は、それらのサーバに対してもワイルドカード証明書を使用できます。ただし、他のサービスと共有されるワイルドカード証明書を使用する場合、VMware Horizon 製品のセキュリティは、それらのサービスのセキュリティにも依存します。

注: ワイルドカード証明書は、単一レベルのドメインでのみ使用できます。たとえば、`*.company.com` というサブジェクト名を含むワイルドカード証明書は、サブドメイン `dept.company.com` では使用できますが、`dept.it.company.com` では使用できません。

Microsoft Certreq を使用した証明書署名要求の生成および証明書の取得

Horizon 7 Server で証明書を使用できるようにするには、構成ファイルを作成し、その構成ファイルから証明書署名要求 (CSR) を生成し、CA に署名要求を送信する必要があります。CA から証明書が返されたら、署名付き証明書を、Horizon 7 Server ホスト上の Windows ローカル コンピュータ証明書ストアにインポートする必要があります。ここで、以前に生成されたプライベート キーが結合されます。

CSR は、証明書自体の生成方法に応じていくつかの方法で生成されます。

Windows Server 2008 R2 では、Microsoft **certreq** ユーティリティを使用して CSR を生成し、署名付き証明書をインポートできます。サードパーティの CA に要求を送信する場合は、**certreq** を使用して Horizon 7 の証明書を取得する方法が最も早く、簡単です。

1 CSR 構成ファイルの作成

Microsoft の **certreq** ユーティリティは、構成ファイルを使用して CSR を生成します。要求を生成する前に、構成ファイルを作成する必要があります。証明書を使用する Horizon 7 サーバをホストする Windows Server コンピュータで、ファイルを作成し、CSR を生成します。

2 CSR の生成および CA からの署名付き証明書の要求

完成した構成ファイルを使用すると、**certreq** ユーティリティを実行して CSR を生成できます。サードパーティの CA に要求を送信すると、署名付き証明書が返されます。

3 証明書署名要求 (CSR) およびプライベート キーが Windows 証明書ストアに保存されていることの確認

証明書署名要求 (CSR) の生成に **certreq** ユーティリティを使用する場合、このユーティリティは関連するプライベート キーも生成します。このユーティリティは、証明書署名要求 (CSR) を生成したコンピュータの Windows ローカル コンピュータの証明書ストアに、証明書署名要求 (CSR) およびプライベート キーを保存します。証明書署名要求 (CSR) およびプライベート キーが適切に保存されていることは、Microsoft Management Console (MMC) 証明書スナップインを使用して確認できます。

4 certreq を使用した署名付き証明書のインポート

CA による署名付き証明書がある場合は、Horizon 7 Server ホスト上の Windows ローカル コンピュータ証明書ストアにその証明書をインポートできます。

5 Horizon 7 Server のためのインポートされた証明書の設定

サーバ証明書を Windows ローカル コンピュータの証明書ストアにインポートしたら、Horizon 7 Server がその証明書を使用することを許可するための追加の手順を実施する必要があります。

CSR 構成ファイルの作成

Microsoft の **certreq** ユーティリティは、構成ファイルを使用して CSR を生成します。要求を生成する前に、構成ファイルを作成する必要があります。証明書を使用する Horizon 7 サーバをホストする Windows Server コンピュータで、ファイルを作成し、CSR を生成します。

前提条件

構成ファイルの設定に必要な情報を収集します。サブジェクト名を完成させるため、Horizon 7 サーバの FQDN と、組織単位、組織、市区町村、都道府県、および国を把握しておく必要があります。

手順

1 テキスト エディタを開いて次のテキスト（開始タグと終了タグを含む）をファイルに貼り付けます。

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

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

テキストをコピーして貼り付けるときに `Subject =` 行に余分な改行文字が追加された場合は、それらの改行文字を削除します。

2 `Subject` 属性を Horizon 7 サーバと導入環境に適切な値に変更します。

例：`CN=dept.company.com`

VMware セキュリティ推奨事項に準拠するために、クライアント デバイスがホストへの接続に使用する完全修飾ドメイン名（FQDN）を使用します。内部ドメインの範囲内の通信にも、シンプルなサーバ名や IP アドレスは使用しないでください。

一部の認証局 (CA) は、state 属性での略語の使用を許可しません。

3 (オプション) `Keylength` 属性を更新します。

`KeyLength` に特定のサイズを指定する必要がない限り、デフォルト値の 2048 が適正です。多くの認証局で必要とされる最小値は 2048 です。キー サイズは大きい方が安全ですが、これを増やすとパフォーマンスに大きく影響します。

`KeyLength` には 1024 も使用できますが、National Institute of Standards and Technology (NIST) はこのサイズを推奨していません。コンピュータの性能が高まるにつれ、強固な暗号が解読されるおそれが出て来るためです。

重要: 1024 未満の `KeyLength` 値は生成しないでください。Horizon Client for Windows は、1024 未満の `KeyLength` で生成された Horizon 7 Server 上の証明書は検証しません。この場合、Horizon Client デバイスは Horizon 7 への接続に失敗します。接続サーバによって実行される証明書検証も失敗し、影響を受ける Horizon 7 Server が Horizon Administrator のダッシュボードで赤色に表示されます。

---

4 ファイルを `request.inf` として保存します。

次のステップ

構成ファイルから CSR を生成します。

CSR の生成および CA からの署名付き証明書の要求

完成した構成ファイルを使用すると、`certreq` ユーティリティを実行して CSR を生成できます。サードパーティの CA に要求を送信すると、署名付き証明書が返されます。

前提条件

- CSR 構成ファイルが完成したことを確認します。「CSR 構成ファイルの作成」を参照してください。
- この手順で説明する `certreq` 操作を、コンピュータ上の CSR 構成ファイルがある場所で実行します。

手順

1 [スタート] メニューの [コマンド プロンプト] を右クリックし、[管理者として実行] を選択してコマンド プロンプトを開きます。

2 `request.inf` ファイルを保存したディレクトリに移動します。

例：**`cd c:\certificates`**

3 CSR ファイルを生成します。

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

4 CSR ファイルの内容を使用して、証明書要求を CA の登録プロセスに従って CA に送信します。

a CA に要求を送信する際は、証明書のインストール先サーバのタイプを選択するように促すプロンプトが CA によって表示されます。Horizon 7 は Microsoft Certificates MMC を使用して証明書を管理するため、Microsoft、Microsoft IIS 7、または同様のサーバ タイプの証明書を選択してください。CA によって生成される証明書は、Horizon 7 で動作する形式であることが必要です。

b 単一サーバ名の証明書を要求する場合は、Horizon Client デバイスがこの Horizon 7 Server の IP アドレスに解決できる名前を使用します。コンピュータが Horizon 7 Server への接続に使用する名前は、証明書に関連付けられた名前と一致する必要があります。

注: CA は、CSR ファイル（`certreq.txt` など）の内容をコピーして Web フォームに貼り付けることを求める場合があります。テキスト エディタを使用すると、CSR ファイルのコンテンツをコピーできます。開始タグと終了タグを忘れずに含めてください。例：

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

CA は、会社に対するいくつかのチェックを実施した後、CSR の情報に基づいてサーバ証明書を作成し、プライベート キーを使用して署名し、証明書を送信します。

CA は、ルート CA 証明書も送信するほか、該当する場合は中間 CA 証明書も送信します。

5 証明書テキスト ファイルの名前を `cert.cer` に変更します。

証明書要求が生成された Horizon 7 Server にファイルが配置されていることを確認します。

6 ルート CA 証明書ファイルと中間 CA 証明書ファイルの名前を **root.cer** と **intermediate.cer** にそれぞれ変更します。

証明書要求が生成された Horizon 7 Server にファイルが配置されていることを確認します。

注: **certreq** ユーティリティを使用して証明書を Windows ローカル コンピュータ証明書ストアにインポートした場合、これらの証明書は PKCS#12 (PFX) 形式でなくてもかまいません。PKCS#12 (PFX) 形式は、証明書のインポート ウィザードを使用して Windows 証明書ストアに証明書をインポートするときに必要です。

次のステップ

CSR ファイルとそのプライベート キーが Windows ローカル コンピュータ証明書ストアに保存されていたことを確認します。

証明書署名要求 (CSR) およびプライベート キーが Windows 証明書ストアに保存されていることの確認

証明書署名要求 (CSR) の生成に **certreq** ユーティリティを使用する場合、このユーティリティは関連するプライベート キーも生成します。このユーティリティは、証明書署名要求 (CSR) を生成したコンピュータの Windows ローカル コンピュータの証明書ストアに、証明書署名要求 (CSR) およびプライベート キーを保存します。証明書署名要求 (CSR) およびプライベート キーが適切に保存されていることは、Microsoft Management Console (MMC) 証明書スナップインを使用して確認できます。

証明書が適切にインポートされ、Horizon 7 サーバによって使用されるようにするには、後でプライベート キーを署名付き証明書と結合する必要があります。

前提条件

- **certreq** ユーティリティを使用して証明書署名要求 (CSR) を生成し、認証局 (CA) からの署名付き証明書を要求したことを確認します。「CSR の生成および CA からの署名付き証明書の要求」を参照してください。
- Microsoft Management Console (MMC) に証明書スナップインを追加するための手順について理解しておきます。『Horizon 7 のインストール』ドキュメントの「Horizon 7 Server の TLS 証明書の構成」の章の「MMC への証明書スナップインの追加」を参照してください。

手順

1 Windows Server コンピュータで、証明書スナップインを MMC に追加します。

2 Windows Server コンピュータの MMC ウィンドウで、[証明書（ローカル コンピュータ）] ノードを展開して [Certificate Enrollment Request] フォルダを選択します。

3 [Certificate Enrollment Request] フォルダを展開し、[証明書] フォルダを選択します。

4 証明書エントリが [証明書] フォルダに表示されることを確認します。

証明書署名要求 (CSR) の生成に使用した **request.inf** ファイルの **subject:CN** フィールドに入力したドメイン名が、[発行先] フィールドおよび [発行者] フィールドに表示されるはずです。

5 次のいずれかの手順を実行して、証明書にプライベート キーが含まれていることを確認します。

- 黄色のキーが証明書アイコンに表示されることを確認します。
- 証明書をダブルクリックし、[証明書情報] ダイアログ ボックスに次の文が表示されることを確認します。**この証明書に対応するプライベート キーがあります。**

次のステップ

証明書を Windows ローカル コンピュータ証明書ストアにインポートします。

certreq を使用した署名付き証明書のインポート

CA による署名付き証明書がある場合は、Horizon 7 Server ホスト上の Windows ローカル コンピュータ証明書ストアにその証明書をインポートできます。

certreq ユーティリティを使用して CSR を生成した場合、証明書プライベート キーは、CSR を生成したサーバに対してローカルです。正しい動作を実現するには、証明書にプライベート キーを結合する必要があります。この手順に示す **certreq** コマンドを使用して、証明書とプライベート キーを適切に結合し、Windows 証明書ストアにインポートしてください。

別の方法で署名付き証明書を CA から取得する場合は、Microsoft Management Console (MMC) スナップインの証明書のインポート ウィザードを使用して、証明書を Windows 証明書ストアにインポートします。この方法は、『Horizon 7 のインストール』ドキュメントの「Horizon 7 Server 用の TLS 証明書の構成」で説明されています。

前提条件

- CA から署名付き証明書を受信したことを確認します。「CSR の生成および CA からの署名付き証明書の要求」を参照してください。
- この手順で説明する **certreq** 操作を、CSR を生成し、署名付き証明書を保存したコンピュータ上で実行します。

手順

1 [スタート] メニューの [コマンド プロンプト] を右クリックし、[管理者として実行] を選択してコマンド プロンプトを開きます。

2 **cert.cer** などの署名付き証明書ファイルを保存したディレクトリに移動します。

例：**cd c:\certificates**

3 **certreq –accept** コマンドを実行して、署名付き証明書をインポートします。

例：**certreq –accept cert.cer**

証明書が Windows ローカル コンピュータ証明書ストアにインポートされます。

次のステップ

インポートされた証明書を Horizon 7 Server で使用できるように構成します。「Horizon 7 Server のためのインポートされた証明書の設定」を参照してください。

Horizon 7 Server のためのインポートされた証明書の設定

サーバ証明書を Windows ローカル コンピュータの証明書ストアにインポートしたら、Horizon 7 Server がその証明書を使用することを許可するための追加の手順を実施する必要があります。

手順

1 サーバ証明書が正常にインポートされたことを確認します。

2 証明書のフレンドリ名を **vdm** に変更します。

vdm は小文字である必要があります。フレンドリ名として **vdm** が付いたその他の証明書がある場合、それらの名前を変更するか、それらの証明書からフレンドリ名を削除する必要があります。

View Composer が使用している証明書のフレンドリ名を変更する必要はありません。

3 ルート CA 証明書と中間 CA 証明書を Windows 証明書ストアにインストールします。

4 サービスが新しい証明書の使用を開始できるように、接続サーバ サービス、セキュリティ サーバ サービス、または View Composer サービスを再起動します。

5 HTML Access を使用する場合は、VMware View Blast Secure Gateway サービスを再起動します。

6 View Composer Server 上で証明書を設定中の場合、別の手順を実行する必要がある可能性があります。

- View Composer をインストールした後に新しい証明書を設定する場合、View Composer が使用するポートにバインドされた証明書と置き換えるために **SviConfig ReplaceCertificate** ユーティリティを実行する必要があります。
- View Composer をインストールする前に新しい証明書を設定する場合、**SviConfig ReplaceCertificate** ユーティリティを実行する必要はありません。View Composer インストーラの実行時、デフォルトの自己署名証明書の代わりに、認証局 (CA) によって署名された新しい証明書を選択できます。

詳細については、『Horizon 7 のインストール』ドキュメントの「View Composer が使用するポートに新規 TLS 証明書をバインドする」を参照してください。

この手順の中のタスクを実行するには、次のトピックを参照してください。

- 「証明書のわかりやすい名前を変更する」
- 「Windows 証明書ストアへのルート証明書と中間証明書のインポート」

詳細については、『Horizon 7 のインストール』ドキュメントの「新しい TLS 証明書を使用するように接続サーバに、セキュリティ サーバ、または View Composer を構成する」を参照してください。

注: 『Horizon 7 のインストール』の「署名付きサーバ証明書を Windows Certificate Store にインポートする」は、**certreq** ユーティリティを使用してサーバ証明書をすでにインストールしたため、ここには記載されていません。サーバ証明書を再度インポートするためには、MMC スナップインの証明書のインポート ウィザードは使用しないでください。

ただし、ルート CA 証明書と中間 CA 証明書を Windows 証明書ストアにインストールするためには、証明書のインポート ウィザードを使用できます。

TLS 接続の中間サーバへのオフロード 2

ロード バランシングや TLS 接続のオフロードなどのタスクを実行するために、Horizon 7 Server と Horizon Client デバイスとの間の中間サーバを設定できます。Horizon Client デバイスは、HTTPS を介して接続される中間サーバに接続します。このサーバによって、外部に接している接続サーバ インスタンスまたはセキュリティ サーバにこの接続が渡されます。

TLS 接続を中間サーバにオフロードするには、次のいくつかの主なタスクを実行する必要があります。

- 中間サーバが使用する TLS 証明書を、外部に接している Horizon 7 Server にインポートします。
- 外部に接している Horizon 7 Server 上で、クライアントが中間サーバへの接続に使用できる URL と一致するように外部 URL を設定します。
- 中間サーバと Horizon 7 Server との間の HTTP 接続を許可します。

この章には、次のトピックが含まれています。

TLS オフロード サーバの証明書を Horizon 7 サーバにインポートする

TLS 接続を中間サーバにオフロードする場合、中間サーバの証明書を接続サーバ インスタンスまたは中間サーバに接続するセキュリティ サーバにインポートする必要があります。同じ TLS サーバ証明書が、オフロードする中間サーバと、中間サーバに接続する、オフロードされる各 Horizon 7 Server の両方に存在している必要があります。

セキュリティ サーバを展開する場合、中間サーバおよびそれに接続するセキュリティ サーバに、同じ TLS 証明書が必要です。同じ TLS 証明書を、セキュリティ サーバとペアリングされて中間サーバに直接接続していない接続サーバ インスタンスにインストールする必要はありません。

セキュリティ サーバを展開しない場合、またはいくつかのセキュリティ サーバおよび外部に接続している接続サーバ インスタンスを含む混在ネットワーク環境の場合、中間サーバおよびそれに接続する接続サーバ インスタンスに同じ TLS 証明書が必要です。

中間サーバの証明書が接続サーバ インスタンスまたはセキュリティ サーバにインストールされていないと、クライアントは Horizon 7 への接続を検証できません。この場合、Horizon 7 Server によって送信された証明書のサムプリントが、Horizon Client が接続している中間サーバの証明書と一致しません。

ロード バランシングを TLS オフロードと混同しないようにしてください。この前提条件は、一部のタイプの負荷分散を含む、TLS オフロードを提供するように構成されたすべてのデバイスに適用されます。ただし、純粋な負荷分散には、デバイス間の証明書のコピーは必要ありません。

重要: 次のトピックに記載されているシナリオで、サードパーティ製コンポーネントと VMware コンポーネント間で TLS 証明書を共有する 1 つのアプローチを示します。誰にでも適している方法でも、タスクを実行する唯一の方法でもありません。

1 中間サーバからの TLS 証明書のダウンロード

   中間サーバにインストールされている CA 署名付き TLS 証明書をダウンロードして、外部に接している Horizon 7 Server にインポートできるようにする必要があります。

2 中間サーバからのプライベート キーのダウンロード

   中間サーバにある、TLS 証明書と関連付けられたプライベート キーをダウンロードする必要があります。プライベート キーは、証明書とともに Horizon 7 Server にインポートする必要があります。

3 証明書ファイルの PKCS#12 形式への変換

   証明書とそのプライベート キーを PEM または他の形式で取得した場合は、Horizon 7 Server で証明書を Windows 証明書ストアにインポートする前に、それを PKCS#12 (PFX) 形式に変換する必要があります。PKCS#12 (PFX) 形式は、Windows 証明書ストアで証明書のインポート ウィザードを使用する際に必要です。

4 署名付きサーバ証明書を Windows 証明書ストアにインポートする

   TLS サーバ証明書を、接続サーバ インスタンスまたはセキュリティ サーバ サービスがインストールされている Windows Server ホスト上の Windows ローカル コンピュータの証明書ストアにインポートする必要があります。

5 証明書のわかりやすい名前を変更する

   TLS 証明書を認識して使用するように、接続サーバ インスタンスまたはセキュリティ サーバを構成するには、証明書のフレンドリ名を `vdm` に変更する必要があります。

6 Windows 証明書ストアへのルート証明書と中間証明書のインポート

   証明書チェーンのルート証明書と中間証明書は Windows ローカル コンピュータ証明書ストアにインポートする必要があります。

中間サーバからの TLS 証明書のダウンロード

中間サーバにインストールされている CA 署名付き TLS 証明書をダウンロードして、外部に接している Horizon 7 Server にインポートできるようにする必要があります。

手順

1 中間サーバに接続し、HTTPS 要求を送信するクライアントに提示する TLS 証明書を検索します。

2 Horizon 7 に使用されている TLS 証明書を検索してダウンロードします。

例：F5 BIG-IP LTM システムからの TLS 証明書のダウンロード

この例では、中間サーバとして F5 BIG-IP Local Traffic Manager (LTM) を使用しています。この例は、独自の中間サーバから証明書をダウンロードする方法についての一般的な概念を示すことを目的としています。

重要: ここに示す手順は F5 BIG-IP LTM 固有のもので、新しいリリースやその他の F5 製品には当てはまらない場合があります。これらの手順は、他のベンダーの中間サーバには当てはまりません。

開始前に、F5 BIG-IP LTM システムが Horizon 7 とともに展開されていることを確認します。F5 導入ガイド、『Deploying F5 with VMware View and Horizon View』(http://www.f5.com/pdf/deployment-guides/f5-vmware-view-dg.pdf) に記載されているタスクを完了していることを確認します。

1 F5 BIG-IP LTM 構成ユーティリティに接続します。

2 ナビゲーション ペインの [メイン] タブで、[ローカル トラフィック] を展開し、[SSL 証明書] をクリックします。

システムにインストールされている証明書の一覧が表示されます。

3 [名前] 列で、Horizon 7 に使用されている証明書の名前をクリックします。

4 画面の一番下で、[エクスポート] をクリックします。

既存の TLS 証明書が [証明書テキスト] ボックスに表示されます。

5 [証明書ファイル] 設定から [<file_name> のダウンロード] をクリックします。

TLS 証明書が CRT ファイルとしてダウンロードされます。

中間サーバからのプライベート キーのダウンロード

中間サーバにある、TLS 証明書と関連付けられたプライベート キーをダウンロードする必要があります。プライベート キーは、証明書とともに Horizon 7 Server にインポートする必要があります。

手順

1 中間サーバに接続し、HTTPS 要求を送信するクライアントに提示する TLS 証明書を検索します。

2 Horizon 7 に使用される証明書を検索し、プライベート キーをダウンロードします。

例：F5 BIG-IP LTM システムからのプライベート キーのダウンロード

この例では、中間サーバとして F5 BIG-IP Local Traffic Manager (LTM) を使用しています。この例は、独自の中間サーバからプライベート キーをダウンロードする方法についての一般的な概念を示すことを目的としています。

重要: ここに示す手順は F5 BIG-IP LTM 固有のもので、新しいリリースやその他の F5 製品には当てはまらない場合があります。これらの手順は、他のベンダーの中間サーバには当てはまりません。

開始前に、F5 BIG-IP LTM 構成ユーティリティに接続していることを確認します。

1 ナビゲーション ペインの [メイン] タブで、[ローカル トラフィック] を展開し、[SSL 証明書] をクリックします。

システムにインストールされている証明書の一覧が表示されます。

2 [名前] 列で、Horizon 7 に使用されている証明書の名前をクリックします。

3 メニュー バーで、[キー] をクリックします。

4 画面の一番下で、[エクスポート] をクリックします。

既存のプライベート キーが [キー テキスト] ボックスに表示されます。

5 [キー ファイル] 設定から [<file_name> のダウンロード] をクリックします。

プライベート キーが KEY ファイルとしてダウンロードされます。

証明書ファイルの PKCS#12 形式への変換

証明書とそのプライベート キーを PEM または他の形式で取得した場合は、Horizon 7 Server で証明書を Windows 証明書ストアにインポートする前に、それを PKCS#12 (PFX) 形式に変換する必要があります。PKCS#12 (PFX) 形式は、Windows 証明書ストアで証明書のインポート ウィザードを使用する際に必要です。

証明書ファイルは、次のいずれかの方法で取得できます。

- 認証局から証明書キーストア ファイルを取得する。
- Horizon 7 のデプロイ環境に設定されている中間サーバから証明書とプライベート キーをダウンロードする。
- 組織から証明書ファイルを受け取る。

証明書ファイルはさまざまな形式で提供されます。たとえば、PEM 形式は通常 Linux 環境で使用されます。ファイルには、次の拡張子の付いた証明書ファイル、キー ファイル、および CSR ファイルが含まれる場合があります。

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

CRT ファイルには、認証局から返された SSL 証明書が含まれています。CSR ファイルは、元の証明書署名要求ファイルであり、必要ではありません。KEY ファイルにはプライベート キーが含まれています。

前提条件

- システムに OpenSSL がインストールされていることを確認します。`openssl` は `http://www.openssl.org` からダウンロードできます。
- 認証局 (CA) から返された SSL 証明書のルート証明書もシステムで使用できることを確認します。

手順

1 CRT ファイルと KEY ファイルを OpenSSL のインストール ディレクトリにコピーします。

例：`cd c:\OpenSSL-Win32\bin`

2 Windows コマンド プロンプトを開き、必要に応じて OpenSSL のインストール ディレクトリに移動します。

3 証明書ファイルとプライベート キーから PKCS#12 (PFX) キーストア ファイルを生成します。

例：`openssl pkcs12 –export –out server.p12 –inkey server.key –in server.crt –certfile CACert.crt`

この例の `CACert.crt` は、認証局から返されたルート証明書の名前です。

Windows 証明書ストアも、拡張子 PFX を使用して生成されたキーストアを受け付けます。例：`–out server.pfx`

4 PKCS#12 (PFX) ファイルを保護するため、エクスポート パスワードを入力します。

署名付きサーバ証明書を Windows 証明書ストアにインポートする

TLS サーバ証明書を、接続サーバ インスタンスまたはセキュリティ サーバ サービスがインストールされている Windows Server ホスト上の Windows ローカル コンピュータの証明書ストアにインポートする必要があります。

このシナリオは、PKCS#12 (PFX) 形式の証明書ファイルを使用します。

証明書のファイル形式によって、キーストア ファイルに含まれる証明書チェーン全体が Windows ローカル コンピュータの証明書ストアにインポートされる場合があります。たとえば、サーバ証明書、中間証明書、ルート証明書がインポートされる場合があります。

その他のタイプの証明書ファイルについては、サーバ証明書のみが Windows ローカル コンピュータの証明書ストアにインポートされます。この場合、別の手順を行い、ルート証明書と証明書チェーン内の中間証明書をインポートする必要があります。

証明書の詳細については、MMC に対する証明書のスナップインで利用できる Microsoft オンライン ヘルプを参照してください。

前提条件

TLS サーバ証明書が PKCS@12 (PFX) 形式であることを確認します。「証明書ファイルの PKCS#12 形式への変換」を参照してください。

手順

1 Windows Server ホストの MMC ウィンドウで、[証明書（ローカル コンピュータ）] ノードを展開して [個人] フォルダを選択します。

2 [操作] ペインで、[追加の操作] - [すべてのタスク] - [インポート] の順に移動します。

3 **[Certificate Import（証明書のインポート）]** ウィザードで、[次へ] をクリックして証明書が格納されている場所を参照します。

4 証明書ファイルを選択して [開く] をクリックします。

証明書ファイルのタイプを表示するには、[ファイル名] ドロップダウン メニューからそのファイル形式を選択できます。

5 証明書ファイルに含まれるプライベート キーのパスワードを入力します。

6 [この鍵をエクスポート可能にマークする] を選択します。

7 [すべての拡張プロパティを含める] を選択します。

8 [次へ] をクリックして [終了] をクリックします。

新しい証明書が [証明書（ローカル コンピュータ）] - [個人] - [証明書] フォルダに表示されます。

9 新しい証明書にプライベート キーが含まれていることを確認します。

a [証明書（ローカル コンピュータ）] - [個人] - [証明書] フォルダで、新しい証明書をダブルクリックします。

b [証明書情報] ダイアログ ボックスの [全般] タブで、「**この証明書に対応するプライベート キーがあります。**」というメッセージが表示されることを確認します。

次のステップ

証明書のわかりやすい名前を **vdm** に変更します。

証明書のわかりやすい名前を変更する

TLS 証明書を認識して使用するように、接続サーバ インスタンスまたはセキュリティ サーバを構成するには、証明書のフレンドリ名を **vdm** に変更する必要があります。

前提条件

サーバ証明書が Windows 証明書ストアの[証明書（ローカル コンピュータ）] - [個人] - [証明書] フォルダにインポートされていることを確認します。「署名付きサーバ証明書を Windows 証明書ストアにインポートする」を参照してください。

手順

1 Windows Server ホストの MMC ウィンドウで、[証明書（ローカル コンピュータ）] ノードを展開して [個人] - [証明書] フォルダを選択します。

2 Horizon 7 サーバ ホストに発行される証明書を右クリックし、[プロパティ] をクリックします。

3 [全般] タブで、[わかりやすい名前] のテキストを削除し、**vdm** と入力します。

4 [適用]、[OK] の順にクリックします。

5 [個人] - [証明書] フォルダのその他のサーバ証明書で、フレンドリ名が **vdm** になっていないことを確認します。

a その他のサーバ証明書がある場合はそれを見つけて証明書を右クリックし、[個人] をクリックします。

b 証明書のわかりやすい名前が **vdm** である場合は、その名前を削除し、[適用] をクリックして、[OK] をクリックします。

次のステップ

ルート証明書と中間証明書を Windows ローカル コンピュータの証明書ストアにインポートします。

チェーン内のすべての証明書をインポートした後で、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動して変更を反映する必要があります。

Windows 証明書ストアへのルート証明書と中間証明書のインポート

証明書チェーンのルート証明書と中間証明書は Windows ローカル コンピュータ証明書ストアにインポートする必要があります。

中間サーバからインポートした TLS サーバ証明書が、接続サーバ ホストから信頼されている既知のルート CA によって署名されていて、証明書チェーン内に中間証明書がない場合、このタスクをスキップできます。一般的に使用されている証明機関は、ホストから信頼される可能性が高くなります。

手順

1 Windows Server ホストの MMC コンソールで、[証明書（ローカル コンピュータ）] ノードを展開して、[信頼されたルート証明機関] - [証明書] フォルダに移動します。

- ルート証明書がこのフォルダにあり、証明書チェーン内に中間証明書がない場合は、手順 7 までスキップします。
- ルート証明書がこのフォルダにあり、証明書チェーン内に中間証明書がある場合は、手順 6 までスキップします。
- ルート証明書がこのフォルダになければ、手順 2 に進みます。

2 [信頼されたルート証明機関] - [証明書] フォルダを右クリックし、[すべてのタスク] - [インポート] をクリックします。

3 **[証明書のインポート]** ウィザードで、[次へ]をクリックしてルート CA 証明書が保存されている場所を参照します。

4 ルート CA 証明書ファイルを選択し、[開く] をクリックします。

5 [次へ] をクリックし、[次へ] をクリックし、そして [終了] をクリックします。

6 サーバ証明書が中間 CA によって署名されていた場合、証明書チェーンのすべての中間証明書を Windows ローカル コンピュータ証明書ストアにインポートします。

a [証明書（ローカル コンピュータ）] - [中間証明機関] - [証明書] フォルダに移動します。

b インポートする必要がある各中間証明書で手順 3 から 6 を繰り返します。

7 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

8 HTML Access を使用する場合は、VMware View Blast Secure Gateway サービスを再起動します。

クライアントを TLS オフロード サーバにポイントするように Horizon 7 Server の外部 URL を設定する

TLS が中間サーバにオフロードされ、Horizon Client デバイスがセキュアなトンネルを使用して Horizon 7 に接続する場合は、セキュアなトンネルの外部 URL を、クライアントが中間サーバへのアクセスに使用できるアドレスに設定するようにします。

中間サーバに接続する接続サーバ インスタンスまたはセキュリティ サーバの外部 URL 設定を構成します。

セキュリティ サーバを展開する場合、それらのセキュリティ サーバに外部 URL が必要ですが、セキュリティ サーバとペアになる接続サーバ インスタンスには外部 URL は必要ありません。

セキュリティ サーバを展開しない場合や、セキュリティ サーバや外部向けの接続サーバ インスタンスがいくつか集まった混合ネットワーク環境を利用している場合には、中間サーバに接続する接続サーバ インスタンスに外部 URL が必要です。

注: PCoIP Secure Gateway (PSG) または Blast Secure Gateway から TLS 接続をオフロードすることはできません。PCoIP 外部 URL と Blast Secure Gateway 外部 URL は、PSG と Blast Secure Gateway をホストするコンピュータへの接続をクライアントに許可する必要があります。中間サーバと Horizon 7 Server 間に TLS 接続を要求する予定がない限り、中間サーバをポイントするように PCoIP 外部 URL と Blast 外部 URL をリセットすることは避けてください。

接続サーバ インスタンスの外部 URL を設定する

接続サーバ インスタンスの外部 URL を設定するには、Horizon Administrator を使用します。

前提条件

- 安全なトンネル接続が接続サーバ インスタンス上で有効になっていることを確認します。

手順

1. Horizon Administrator で、[View 構成] - [サーバ] の順にクリックします。
2. [接続サーバ] タブで、接続サーバ インスタンスを選択して [編集] をクリックします。
3. [外部 URL] テキスト ボックスに安全なトンネルの外部 URL を入力します。

   URL には、プロトコル、クライアントで解決可能なホスト名、およびポート番号が含まれている必要があります。

   例：**`https://myserver.example.com:443`**

   注: ホスト名が解決できないときに接続サーバ インスタンスにアクセスする必要がある場合は、IP アドレスを使用できます。ただし、通信するホストは、接続サーバ インスタンスに対して構成された TLS 証明書に一致しないため、アクセスがブロックされたりアクセスのセキュリティが低下したりします。
4. このダイアログのすべてのアドレスによって、クライアント システムがこの接続サーバ インスタンスに到達できることを確認します。
5. [OK] をクリックします。

セキュリティ サーバの外部 URL を変更する

セキュリティ サーバの外部 URL を変更するには、Horizon Administrator を使用します。

前提条件

- 安全なトンネル接続が、このセキュリティ サーバとペアになっている接続サーバ インスタンス上で有効になっていることを確認します。

手順

1. Horizon Administrator で、[View 構成] - [サーバ] を選択します。
2. [セキュリティ サーバ] タブを選択し、セキュリティ サーバを選択して、[編集] をクリックします。

3 [外部 URL] テキスト ボックスに安全なトンネルの外部 URL を入力します。

URL には、プロトコル、クライアントで解決可能なセキュリティ サーバのホスト名およびポート番号が含まれている必要があります。

例：`https://myserver.example.com:443`

注: ホスト名が解決できないときにセキュリティ サーバにアクセスする必要がある場合は、IP アドレスを使用できます。ただし、通信するホストは、セキュリティ サーバ用に構成されている TLS 証明書に対応していないため、アクセスがブロックされたりアクセスのセキュリティが低下したりします。

4 このダイアログのすべてのアドレスでクライアント システムがこのセキュリティ サーバ ホストに到達できることを確認します。

5 [OK] をクリックして変更を保存します。

Horizon Administrator が、更新された外部 URL をセキュリティ サーバに送信します。変更を有効にするためにセキュリティ サーバ サービスを再起動する必要はありません。

中間サーバからの HTTP 接続を許可する

TLS が中間サーバにオフロードされる場合、接続サーバ インスタンスまたはセキュリティ サーバが、クライアントが接続する中間デバイスからの HTTP 接続を許可するように構成できます。中間デバイスは Horizon Client 接続の HTTPS を受け入れる必要があります。

Horizon 7 Server と中間デバイスとの HTTP 接続を許可するには、HTTP 接続が許可される各接続サーバ インスタンスおよびセキュリティ サーバに `locked.properties` ファイルを構成する必要があります。

Horizon 7 Server サーバと中間デバイスとの間の HTTP 接続が許可されたとしても、Horizon 7 での TLS を無効にすることはできません。Horizon 7 サーバは HTTP 接続と同様に HTTPS 接続を引き続き受け入れます。

注: Horizon クライアントがスマート カード認証を使用する場合、クライアントは接続サーバまたはセキュリティ サーバに対し直接 HTTPS 接続を行う必要があります。TLS オフロードはスマート カード認証ではサポートされていません。

手順

1 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例： `<install_directory>\VMware\VMware View\Server\SSLgateway\conf\locked.properties`

2 Horizon 7 Server のプロトコルを構成するには、`ServerProtocol` プロパティを追加して、`http` に設定します。

値 `http` は小文字で入力する必要があります。

3 (オプション) プロパティを追加して、デフォルト以外の HTTP リスニング ポートおよびネットワーク インターフェイスを Horizon 7 Server に構成します。

   - HTTP リスニング ポートを 80 から変更するには、`serverPortNonTLS` を、中間デバイスの接続先に構成されている別のポート番号に設定します。
   - Horizon 7 Server に複数のネットワーク インターフェイスがあり、サーバに 1 つのインターフェイスのみで HTTP 接続をリスンさせる場合、`serverHostNonTLS` をそのネットワーク インターフェイスの IP アドレスに設定します。

4 `locked.properties` ファイルを保存します。

5 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

例：locked.properties ファイル

このファイルにより Horizon 7 Server への非 TLS HTTP 接続が許可されます。Horizon 7 Server のクライアント側のネットワーク インターフェイスの IP アドレスは 10.20.30.40 です。サーバは、デフォルトのポート 80 を使用して、HTTP 接続を待機します。その値 `http` は小文字である必要があります。

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