

# Scénarios de configuration des certificats TLS pour Horizon 7

Modifié le 29 mai 2018  
VMware Horizon 7 7.5



vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

<https://docs.vmware.com/fr/>

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware, Inc.**  
100-101 Quartier Boieldieu  
92042 Paris La Défense  
France  
[www.vmware.com/fr](http://www.vmware.com/fr)

Copyright © 2012–2018 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

# Table des matières

Scénarios de configuration des certificats TLS pour Horizon 7 4

## 1 Obtention de certificats TLS à partir d'une autorité de certification 5

Déterminer si ce scénario vous concerne 5

Sélection du type de certificat correct 6

Génération d'une demande de signature de certificat et obtention d'un certificat avec Microsoft  
Certreq 7

## 2 Déchargement de connexions TLS sur des serveurs intermédiaires 16

Importer des certificats des serveurs de déchargement TLS vers des serveurs Horizon 7 16

Définir des URL externes d' Horizon 7 Server pour pointer les clients vers des serveurs de  
déchargement TLS 23

Autoriser les connexions HTTP à partir des serveurs intermédiaires 25

# Scénarios de configuration des certificats TLS pour Horizon 7

*Scénarios de configuration des certificats TLS pour Horizon 7* fournit des exemples de configuration de certificats TLS pour une utilisation par les serveurs Horizon 7. Le premier scénario vous indique comment obtenir des certificats TLS signés auprès d'une autorité de certification et vous assurer que les certificats sont dans un format qui peut être utilisé par les serveurs Horizon 7. Le second scénario vous indique comment configurer les serveurs Horizon 7 pour décharger des connexions TLS vers un serveur intermédiaire.

## Public cible

Ces informations sont conçues pour toute personne qui souhaite installer Horizon 7 et qui doit obtenir des certificats TLS utilisés par les serveurs Horizon 7, ou pour toute personne qui utilise des serveurs intermédiaires pour décharger des connexions TLS vers Horizon 7. Les informations sont destinées aux administrateurs Windows ou Linux expérimentés qui connaissent bien le fonctionnement des datacenters et de la technologie des machines virtuelles.

# Obtention de certificats TLS à partir d'une autorité de certification

1

VMware vous recommande vivement de configurer des certificats TLS signés par une autorité de certification valide pour les instances du Serveur de connexion Horizon, les serveurs de sécurité et les instances de View Composer.

Les certificats TLS par défaut sont générés lorsque vous installez des instances du Serveur de connexion, du serveur de sécurité ou de View Composer. Bien que vous puissiez utiliser les certificats auto-signés par défaut à des fins de test, remplacez-les dès que possible. Les certificats par défaut ne sont pas signés par une autorité de certification. L'utilisation de certificats non signés par une autorité de certification peut permettre à des parties non approuvées d'intercepter le trafic en se faisant passer pour votre serveur.

Dans un environnement Horizon 7, vous devez également remplacer le certificat par défaut qui est installé avec vCenter Server par un certificat signé par une autorité de certification. Vous pouvez utiliser openTLS pour effectuer cette tâche pour vCenter Server. Pour plus d'informations, reportez-vous à la section « Replacing vCenter Server Certificates » (Remplacer les certificats vCenter Server) sur le site Documents techniques VMware à l'adresse <http://www.vmware.com/resources/techresources/>.

Ce chapitre aborde les rubriques suivantes :

- [Déterminer si ce scénario vous concerne](#)
- [Sélection du type de certificat correct](#)
- [Génération d'une demande de signature de certificat et obtention d'un certificat avec Microsoft Certreq](#)

## Déterminer si ce scénario vous concerne

Vous configurez des certificats pour Horizon 7 en les important dans le magasin de certificats Windows de l'ordinateur local sur l'hôte du serveur Horizon 7.

Avant de pouvoir importer un certificat, vous devez générer une demande de signature de certificat (ou CSR, pour Certificate Signing Request) et obtenir un certificat valide et signé d'une autorité de certification. Si la CSR n'est pas générée conformément à l'exemple de procédure présenté dans ce scénario, le certificat qui en résulte et sa clé privée doivent être disponibles dans un fichier au format PKCS#12 (anciennement intitulé PFX).

Vous pouvez obtenir des certificats TLS à partir d'une autorité de certification de plusieurs manières. Ce scénario vous indique comment utiliser l'utilitaire Microsoft certreq pour générer une CSR et la rendre un certificat disponible pour un serveur Horizon 7. Vous pouvez utiliser une autre méthode si vous maîtrisez les outils requis et s'ils sont installés sur votre serveur.

Utilisez ce scénario pour résoudre les problèmes suivants :

- Vous ne disposez pas des certificats TLS qui sont signés par une autorité de certification, et vous ne savez pas comment les obtenir
- Vous disposez de certificats TLS signés valides, mais ils ne sont pas au format PKCS#12 (PFX)

Si votre entreprise vous fournit des certificats TLS signés par une autorité de certification, vous pouvez les utiliser. Votre organisation peut utiliser une autorité de certification interne valide ou une autorité de certification tierce, commerciale. Si vos certificats ne sont pas au format PKCS#12, vous devez les convertir. Reportez-vous à la section [Convertir un fichier de certificat au format PKCS#12](#).

Lorsque vous avez un certificat signé au bon format, vous pouvez l'importer dans le magasin de certificats Windows et configurer un serveur Horizon 7 pour pouvoir l'utiliser. Reportez-vous à la section [Configurer un certificat importé pour un serveur Horizon 7](#).

## Sélection du type de certificat correct

Horizon 7 vous permet d'utiliser de nombreux types de certificats TLS. Il est important de choisir le type de certificat adapté à votre déploiement. Les types de certificat ont des coûts différents, en fonction du nombre de serveurs sur lesquels ils peuvent être utilisés.

Suivez les recommandations de sécurité de VMware en utilisant des noms de domaine complets (FQDN) pour vos certificats, quel que soit le type que vous sélectionnez. N'utilisez pas un nom de serveur simple ou une adresse IP, même pour les communications effectuées à l'intérieur de votre domaine interne.

## Certificat de nom de serveur unique

Vous pouvez générer un certificat avec un nom d'objet pour un serveur spécifique. Par exemple : `dept.company.com`.

Ce type de certificat est utile si, par exemple, une seule instance du Serveur de connexion a besoin d'un certificat.

Lorsque vous soumettez une demande de signature de certificat à une autorité de certification, vous fournissez le nom de serveur qui sera associé au certificat. Vérifiez que le serveur Horizon 7 peut résoudre le nom de serveur que vous fournissez pour qu'il corresponde au nom associé au certificat.

## Autres noms de l'objet

Un autre nom de l'objet (SAN) est un attribut pouvant être ajouté à un certificat lors de son émission. Vous utilisez cet attribut pour ajouter des noms d'objet (URL) à un certificat pour qu'il puisse valider plusieurs serveurs.

Par exemple, un certificat peut être émis pour un serveur dont le nom d'hôte est `dept.company.com`. Ce certificat est prévu pour être utilisé par des utilisateurs externes qui se connectent à Horizon 7 via un serveur de sécurité. Avant l'émission du certificat, vous pouvez ajouter le SAN `dept-int.company.com` au certificat pour permettre l'utilisation de ce dernier sur des instances du Serveur de connexion ou sur des serveurs de sécurité, après un équilibrage de charge lorsque le tunneling est activé.

## Certificat de caractère générique

Un certificat de caractère générique est généré pour pouvoir être utilisé pour plusieurs services. Par exemple : `*.company.com`.

Un certificat de caractère générique est utile si plusieurs serveurs ont besoin d'un certificat. Si, en plus d'Horizon 7, d'autres applications de votre environnement ont besoin de certificats TLS, vous pouvez également utiliser un certificat de caractère générique pour ces serveurs. Toutefois, si vous utilisez un certificat de caractère générique partagé avec d'autres services, la sécurité du produit VMware Horizon dépend également de la sécurité de ces autres services.

---

**Remarque** Vous ne pouvez utiliser un certificat de caractère générique que sur un seul niveau de domaine. Par exemple, un certificat de caractère générique avec le nom d'objet `*.company.com` peut être utilisé pour le sous-domaine `dept.company.com`, mais pas pour le sous-domaine `dept.it.company.com`.

---

## Génération d'une demande de signature de certificat et obtention d'un certificat avec Microsoft Certreq

Pour mettre un certificat à la disposition d'un serveur Horizon 7, vous devez créer un fichier de configuration, générer une demande de signature de certificat (CSR) à partir du fichier de configuration et envoyer la demande de signature à une autorité de certification. Lorsque l'autorité de certification renvoie le certificat, vous devez importer le certificat signé dans le magasin de certificats de l'ordinateur local Windows sur l'hôte du serveur Horizon 7, où il rejoint la clé privée précédemment générée.

Une CSR peut être générée de différentes manières, selon la manière dont sera généré le certificat.

L'utilitaire Microsoft `certreq` est disponible sur Windows Server 2008 R2 et peut être utilisé pour générer une CSR et importer un certificat signé. Si vous prévoyez d'envoyer une demande à une autorité de certification tierce, l'utilisation de `certreq` constitue le moyen le plus rapide et le plus simple d'obtenir un certificat pour Horizon 7.

### 1 Créer un fichier de configuration CSR

L'utilitaire Microsoft `certreq` utilise un fichier de configuration pour générer une demande de signature de certificat (CSR). Vous devez créer un fichier de configuration pour pouvoir générer la demande. Créez le fichier, puis générez la CSR sur l'ordinateur Windows Server qui héberge le serveur Horizon 7 qui utilisera le certificat.

**2 Générer une CSR et demander un certificat signé auprès d'une autorité de certification**

En utilisant le fichier de configuration terminé, vous pouvez générer une demande de signature de certificat (CSR) en exécutant l'utilitaire `certreq`. Vous envoyez la demande à une autorité de certification tierce, qui renvoie un certificat signé.

**3 Vérifier que la CSR et sa clé privée sont stockées dans le magasin de certificats Windows**

Si vous utilisez l'utilitaire `certreq` pour générer une demande de signature de certificat (CSR), l'utilitaire génère également une clé privée associée. L'utilitaire stocke la CSR et sa clé privée dans le magasin de certificats d'ordinateur Windows local sur l'ordinateur sur lequel vous avez généré la CSR. Vous pouvez vérifier que la CSR et sa clé privée sont correctement stockées en utilisant le composant logiciel enfichable Certificats de Microsoft Management Console (MMC).

**4 Importer un certificat signé à l'aide de `certreq`**

Lorsque vous disposez d'un certificat signé par une autorité de certification, vous pouvez l'importer dans le magasin de certificats de l'ordinateur local Windows sur l'hôte du serveur Horizon 7.

**5 Configurer un certificat importé pour un serveur Horizon 7**

Après avoir importé un certificat de serveur dans le magasin de certificats de votre ordinateur local Windows, vous devez suivre d'autres étapes pour autoriser un serveur Horizon 7 à utiliser le certificat.

## Créer un fichier de configuration CSR

L'utilitaire Microsoft `certreq` utilise un fichier de configuration pour générer une demande de signature de certificat (CSR). Vous devez créer un fichier de configuration pour pouvoir générer la demande. Créez le fichier, puis générez la CSR sur l'ordinateur Windows Server qui héberge le serveur Horizon 7 qui utilisera le certificat.

**Prérequis**

Collectez les informations dont vous avez besoin pour remplir le fichier de configuration. Vous devez connaître le nom de domaine complet (FQDN) du serveur Horizon 7, ainsi que l'unité d'organisation, l'organisation, la ville, l'État et le pays pour terminer le nom du sujet.

**Procédure**

- 1 Ouvrez un éditeur de texte et collez le texte suivant, y compris les balises de début et de fin, dans le fichier.

```
;----- 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

;-----

```

Si un caractère de retour chariot/saut de ligne supplémentaire est ajouté à la ligne `Subject =` lorsque vous copiez et collez le texte, supprimez-le.

- 2 Mettez à jour les attributs de `Subject` avec les valeurs appropriées pour votre serveur Horizon 7 et le déploiement.

Par exemple : `CN=dept.company.com`

Pour vous conformer aux recommandations de sécurité VMware, utilisez le nom de domaine complet que les périphériques clients utilisent pour se connecter à l'hôte. N'utilisez pas un nom de serveur simple ou une adresse IP, même pour les communications effectuées à l'intérieur de votre domaine interne.

Certaines autorités de certification ne permettent pas d'utiliser des abréviations pour l'attribut d'état.

- 3 (Facultatif) Mettez à jour l'attribut `KeyLength`.

La valeur par défaut, 2 048, convient, sauf si vous avez besoin d'une autre taille pour l'attribut `KeyLength`. Plusieurs autorités de certification nécessitent une valeur minimale de 2 048. Les clés de grande taille sont plus sécurisées, mais dégradent plus les performances.

Un attribut KeyLength de 1 024 est également pris en charge, bien que le National Institute of Standards and Technology (NIST) déconseille les clés de cette taille, car les ordinateurs gagnent en puissance et peuvent parvenir à déchiffrer un chiffrement renforcé.

---

**Important** Ne générez pas une valeur inférieure à 1 024 pour l'attribut KeyLength. Horizon Client pour Windows ne validera pas un certificat généré avec un attribut KeyLength inférieur à 1 024 sur un serveur Horizon 7. Les périphériques Horizon Client ne pourront donc pas se connecter à Horizon 7. Les validations de certificats exécutées par le Serveur de connexion échoueront également ; les serveurs Horizon 7 affectés s'afficheront alors en rouge dans le tableau de bord d'Horizon Administrator.

---

4 Enregistrez le fichier sous la forme `request.inf`.

#### Suivant

Générez une CSR à partir du fichier de configuration.

## Générer une CSR et demander un certificat signé auprès d'une autorité de certification

En utilisant le fichier de configuration terminé, vous pouvez générer une demande de signature de certificat (CSR) en exécutant l'utilitaire `certreq`. Vous envoyez la demande à une autorité de certification tierce, qui renvoie un certificat signé.

#### Prérequis

- Vérifiez que vous avez terminé un fichier de configuration de CSR. Reportez-vous à la section [Créer un fichier de configuration CSR](#).
- Exécutez l'opération `certreq` décrite dans cette procédure sur l'ordinateur où se trouve le fichier de configuration de CSR.

#### Procédure

- 1 Ouvrez une invite de commande en cliquant avec le bouton droit sur **Invite de commande** dans le menu **Démarrer**, puis en sélectionnant **Exécuter en tant qu'administrateur**.
- 2 Accédez au répertoire dans lequel vous avez enregistré le fichier `request.inf`.

Par exemple : `cd c:\certificates`

- 3 Générez le fichier CSR.

Par exemple : `certreq -new request.inf certreq.txt`

- 4 Utilisez le contenu du fichier CSR pour soumettre une demande de certificat à l'autorité de certification conformément au processus d'inscription de l'autorité de certification.
  - a Lorsque vous soumettez la demande à une autorité de certification, celle-ci vous invite à sélectionner le type de serveur sur lequel vous allez installer le certificat. Comme Horizon 7 utilise Microsoft Management Console (MMC) Certificats pour gérer les certificats, sélectionnez un certificat pour un type de serveur de Microsoft, Microsoft IIS 7 ou similaire. L'autorité de certification doit générer un certificat au format requis pour fonctionner avec Horizon 7.
  - b Si vous demandez un certificat à nom de serveur unique, utilisez un nom que les périphériques Horizon Client peuvent résoudre en une adresse IP pour ce serveur Horizon 7. Nom que les ordinateurs utilisent pour se connecter au serveur Horizon 7 doit correspondre au nom associé au certificat.

**Remarque** L'autorité de certification peut exiger que vous copiez et colliez le contenu du fichier CSR (par exemple certreq.txt) dans un formulaire Web. À l'aide d'un éditeur de texte, vous pouvez copier le contenu du fichier CSR. Veillez à inclure les balises de début et de fin. Par exemple :

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID2jCCAsICAQAwazEWMBQGA1UEBhMNVW5pdGVkIFN0YXRlc2ELMAkGA1UECAwC
Q0ExEjAQBgNVBACMCVBhbG8gQWx0bzEKMAgGA1UECgwBTzELMAkGA1UECwwCT1Ux
FzAVBgNVBAMMDm15LmNvbXBhbnkuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
. . .
. . .
L9nPYX76jeu5rwQfXLivSCea6nZiIOZYw8Dbn8dgaAqpJdzBbrwuM1TuSnx6bAK8
S52Tv0Gxw58jUTtxFV+Roz8TE8wZDFB51jx+FmLs
-----END NEW CERTIFICATE REQUEST-----
```

Après avoir effectué quelques vérifications sur votre société, l'autorité de certification crée un certificat de serveur en fonction des informations de la CSR, signe avec sa clé privée et vous envoie le certificat.

L'autorité de certification vous envoie également un certificat d'autorité de certification racine et, le cas échéant, un certificat d'autorité de certification intermédiaire.

- 5 Renommez le fichier texte du certificat en cert.cer.

Vérifiez que le fichier se trouve sur le serveur Horizon 7 sur lequel la demande de certificat a été générée.

- 6 Renommez les fichiers des autorités de certification racine et intermédiaire en `root.cer` et `intermediate.cer`.

Vérifiez que les fichiers sont situés sur le serveur Horizon 7 sur lequel la demande de certificat a été générée.

---

**Remarque** Ces certificats ne doivent pas obligatoirement être au format PKCS#12 (PFX) lorsque vous utilisez l'utilitaire `certreq` pour importer les certificats dans le magasin de certificats de l'ordinateur local Windows. Le format PKCS#12 (PFX) est requis lorsque vous utilisez l'assistant Importation de certificat pour importer des certificats dans le magasin de certificats Windows.

---

### Suivant

Vérifiez que le fichier CSR et sa clé privée ont été stockés dans le magasin de certificats de l'ordinateur local Windows.

## Vérifier que la CSR et sa clé privée sont stockées dans le magasin de certificats Windows

Si vous utilisez l'utilitaire `certreq` pour générer une demande de signature de certificat (CSR), l'utilitaire génère également une clé privée associée. L'utilitaire stocke la CSR et sa clé privée dans le magasin de certificats d'ordinateur Windows local sur l'ordinateur sur lequel vous avez généré la CSR. Vous pouvez vérifier que la CSR et sa clé privée sont correctement stockées en utilisant le composant logiciel enfichable Certificats de Microsoft Management Console (MMC).

La clé privée doit être jointe ultérieurement avec le certificat signé pour permettre l'importation correcte du certificat et son utilisation par un serveur Horizon 7.

### Prérequis

- Vérifiez que vous avez généré une CSR en utilisant l'utilitaire `certreq` et que vous avez demandé un certificat signé par une autorité de certification. Reportez-vous à la section [Générer une CSR et demander un certificat signé auprès d'une autorité de certification](#).
- Vous devez vous familiariser avec la procédure d'ajout d'un composant logiciel enfichable Certificats dans Microsoft Management Console (MMC). Reportez-vous à la section « Ajouter le composant logiciel enfichable Certificat à MMC », dans le chapitre « Configuration des certificats TLS pour les serveurs Horizon 7 » du document *Installation d'Horizon 7*.

### Procédure

- 1 Sur l'ordinateur Windows Server, ajoutez le composant logiciel enfichable Certificats à MMC.
- 2 Dans la fenêtre MMC sur l'ordinateur Windows Server, développez le nœud **Certificats (ordinateur local)**, puis sélectionnez le dossier **Demande d'inscription de certificats**.
- 3 Développez le dossier **Demande d'inscription de certificats**, puis sélectionnez le dossier **Certificats**.

#### 4 Vérifiez que l'entrée du certificat s'affiche dans le dossier **Certificats**.

Les champs **Délivré à** et **Délivré par** doivent afficher le nom de domaine que vous avez entré dans le champ **Nom commun de l'objet** du fichier `request.inf` qui a été utilisé pour générer la CSR.

#### 5 Vérifiez que le certificat contient une clé privée en effectuant l'une des étapes suivantes :

- Vérifiez qu'une clé jaune apparaît sur l'icône du certificat.
- Double-cliquez sur le certificat et vérifiez que l'instruction suivante s'affiche dans la boîte de dialogue Informations sur le certificat : Vous avez une clé privée qui correspond à ce certificat.

### Suivant

Importez le certificat dans le magasin de certificats de l'ordinateur local Windows.

## Importer un certificat signé à l'aide de certreq

Lorsque vous disposez d'un certificat signé par une autorité de certification, vous pouvez l'importer dans le magasin de certificats de l'ordinateur local Windows sur l'hôte du serveur Horizon 7.

Si vous avez utilisé l'utilitaire `certreq` pour générer une CSR, la clé privée du certificat est locale pour le serveur sur lequel vous avez généré la CSR. Pour fonctionner correctement, le certificat doit être combiné avec la clé privée. Utilisez la commande `certreq` indiquée dans cette procédure pour vous assurer que le certificat et la clé privée sont correctement combinés et importés dans le magasin de certificats Windows.

Si vous utilisez une autre méthode pour obtenir un certificat signé par une autorité de certification, vous pouvez utiliser l'assistant Importation de certificat dans le composant logiciel enfichable Microsoft Management Console (MMC) pour importer un certificat dans le magasin de certificats Windows. Cette méthode est décrite dans « Configuration des certificats TLS pour les serveurs Horizon 7 » du document *Installation d'Horizon 7*.

### Prérequis

- Vérifiez que vous avez reçu un certificat signé par une autorité de certification. Reportez-vous à la section [Générer une CSR et demander un certificat signé auprès d'une autorité de certification](#).
- Effectuez l'opération `certreq` décrite dans cette procédure sur l'ordinateur sur lequel vous avez généré une demande de signature de certificat (CSR) et stocké le certificat signé.

### Procédure

- 1 Ouvrez une invite de commande en cliquant avec le bouton droit sur **Invite de commande** dans le menu **Démarrer**, puis en sélectionnant **Exécuter en tant qu'administrateur**.
- 2 Accédez au répertoire dans lequel vous avez enregistré le fichier de certificat signé, tel que `cert.cer`.

Par exemple : `cd c:\certificates`

- 3 Importez le certificat signé en exécutant la commande `certreq -accept`.

Par exemple : `certreq -accept cert.cer`

Le certificat est importé dans le magasin de certificats de l'ordinateur local Windows.

#### Suivant

Configurez le certificat importé devant être utilisé par un serveur Horizon 7. Reportez-vous à la section [Configurer un certificat importé pour un serveur Horizon 7](#).

## Configurer un certificat importé pour un serveur Horizon 7

Après avoir importé un certificat de serveur dans le magasin de certificats de votre ordinateur local Windows, vous devez suivre d'autres étapes pour autoriser un serveur Horizon 7 à utiliser le certificat.

#### Procédure

- 1 Vérifiez que le certificat du serveur a été correctement importé.
- 2 Remplacez le nom convivial du certificat en le renommant **vdm**.  
  
**vdm** doit être en minuscules. Tous les autres certificats avec le nom convivial **vdm** doivent être renommés, ou vous devez supprimer le nom convivial de ces certificats.  
  
Vous n'avez pas besoin de modifier le nom convivial des certificats qui sont utilisés par View Composer.
- 3 Installez le certificat d'autorité de certification racine et le certificat d'autorité de certification intermédiaire dans le magasin de certificats Windows.
- 4 Redémarrez le service du Serveur de connexion, du serveur de sécurité ou de View Composer, pour qu'il puisse commencer à utiliser les nouveaux certificats.
- 5 Si vous utilisez HTML Access, redémarrez le service VMware View Blast Secure Gateway.
- 6 Si vous configurez un certificat sur une instance de View Composer Server, vous devrez peut-être effectuer une autre étape.
  - Si vous configurez un nouveau certificat après l'installation de View Composer, vous devez exécuter l'utilitaire `SviConfig ReplaceCertificate` pour remplacer le certificat lié au port utilisé par View Composer.
  - Si vous configurez le nouveau certificat avant d'installer View Composer, vous n'avez pas besoin d'exécuter l'utilitaire `SviConfig ReplaceCertificate`. Lorsque vous exécutez le programme d'installation de View Composer, vous pouvez sélectionner le nouveau certificat signé par une autorité de certification au lieu du certificat auto-signé par défaut.

Pour plus d'informations, reportez-vous à la section « Lier un nouveau certificat TLS au port utilisé par View Composer » du document *Installation d'Horizon 7*.

Pour effectuer les tâches de cette procédure, consultez les rubriques suivantes :

- [Modifier le nom convivial du certificat](#)

- [Importer des certificats racine et intermédiaire dans le magasin de certificats Windows](#)

Pour plus d'informations, consultez la section « Configurer le Serveur de connexion, le serveur de sécurité ou View Composer pour utiliser un nouveau certificat TLS » du document *Installation d'Horizon 7*.

---

**Remarque** La rubrique « Importer un certificat de serveur signé dans un magasin de certificats Windows » du document *Installation d'Horizon 7* n'est pas répertoriée ici, car vous avez déjà importé le certificat du serveur en utilisant l'utilitaire `certreq`. Vous ne devez pas utiliser l'assistant Importation de certificat dans le composant logiciel enfichable MMC pour réimporter le certificat de serveur.

Cependant, vous pouvez utiliser l'assistant Importation de certificat pour importer le certificat d'autorité de certification racine et le certificat d'autorité de certification intermédiaire dans le magasin de certificats Windows.

---

# Déchargement de connexions TLS sur des serveurs intermédiaires

## 2

Vous pouvez configurer des serveurs intermédiaires entre vos serveurs Horizon 7 et vos périphériques Horizon Client afin d'effectuer des tâches telles que l'équilibrage de charge et le déchargement de connexions TLS. Les périphériques Horizon Client se connectent via HTTPS aux serveurs intermédiaires, qui transmettent les connexions aux instances externes du Serveur de connexion ou aux serveurs de sécurité.

Pour décharger des connexions TLS sur un serveur intermédiaire, vous devez effectuer quelques tâches clés :

- Importer le certificat TLS utilisé par le serveur intermédiaire vers vos serveurs Horizon 7 externes.
- Définir les URL externes sur vos serveurs Horizon 7 externes qui correspondent à l'URL que les clients peuvent utiliser pour se connecter au serveur intermédiaire.
- Autoriser les connexions HTTP entre le serveur intermédiaire et les serveurs Horizon 7.

Ce chapitre aborde les rubriques suivantes :

- [Importer des certificats des serveurs de déchargement TLS vers des serveurs Horizon 7](#)
- [Définir des URL externes d'Horizon 7 Server pour pointer les clients vers des serveurs de déchargement TLS](#)
- [Autoriser les connexions HTTP à partir des serveurs intermédiaires](#)

## Importer des certificats des serveurs de déchargement TLS vers des serveurs Horizon 7

Si vous déchargez des connexions TLS vers un serveur intermédiaire, vous devez importer le certificat du serveur intermédiaire vers les instances du Serveur de connexion ou les serveurs de sécurité qui se connectent au serveur intermédiaire. Le même certificat de serveur TLS doit résider sur le serveur intermédiaire de déchargement et sur chaque serveur Horizon 7 déchargé qui se connecte au serveur intermédiaire.

Si vous déployez des serveurs de sécurité, le serveur intermédiaire et les serveurs de sécurité qui s'y connectent doivent avoir le même certificat TLS. Vous n'avez pas à installer le même certificat TLS sur les instances du Serveur de connexion qui sont couplées aux serveurs de sécurité et ne se connectent pas directement au serveur intermédiaire.



Si vous ne déployez pas de serveurs de sécurité ou si vous avez un environnement réseau mélangé avec des serveurs de sécurité et des instances du Serveur de connexion frontales externes, le serveur intermédiaire et les instances du Serveur de connexion qui s'y connectent doivent avoir le même certificat TLS.

Si le certificat du serveur intermédiaire n'est pas installé sur l'instance du Serveur de connexion ou sur le serveur de sécurité, les clients ne peuvent pas valider leurs connexions à Horizon 7. Dans ce cas, l'empreinte numérique du certificat envoyée par le serveur Horizon 7 Server ne correspond pas au certificat sur le serveur intermédiaire auquel Horizon Client se connecte.

Ne confondez pas équilibrage de charge et déchargement TLS. L'exigence précédente s'applique à tout périphérique configuré pour fournir le déchargement TLS, y compris certains types d'équilibrages de charge. Toutefois, l'équilibrage de charge pur ne requiert pas la copie de certificats entre périphériques.

---

**Important** Le scénario décrit dans les rubriques suivantes présente une approche de partage des certificats TLS entre composants tiers et composants VMware. Cette approche n'est peut-être pas adaptée à chacun et n'est pas la seule permettant d'effectuer cette tâche.

---

#### 1 Télécharger un certificat TLS à partir du serveur intermédiaire

Vous devez télécharger le certificat TLS signé par une autorité de certification qui est installé sur le serveur intermédiaire afin qu'il puisse être importé dans les serveurs Horizon 7 externes.

#### 2 Téléchargement d'une clé privée à partir du serveur intermédiaire

Vous devez télécharger la clé privée associée au certificat TLS sur le serveur intermédiaire. La clé privée doit être importée avec le certificat dans les serveurs Horizon 7.

#### 3 Convertir un fichier de certificat au format PKCS#12

Si vous avez obtenu un certificat et sa clé privée au format PEM ou dans un autre format, vous devez le reconvertir au format PKCS#12 (PFX) avant de pouvoir l'importer dans un magasin de certificats Windows sur un serveur Horizon 7. Le format PKCS#12 (PFX) est requis si vous utilisez l'assistant Importation de certificat dans le magasin de certificats Windows.

#### 4 Importer un certificat de serveur signé dans un magasin de certificats Windows

Vous devez importer le certificat de serveur TLS dans le magasin de certificats de l'ordinateur local Windows sur l'hôte Windows Server sur lequel l'instance du Serveur de connexion ou le service du serveur de sécurité est installé.

#### 5 Modifier le nom convivial du certificat

Pour configurer une instance du Serveur de connexion ou un serveur de sécurité pour qu'ils reconnaissent et utilisent un certificat TLS, vous devez remplacer le nom convivial du certificat par vdm.

#### 6 Importer des certificats racine et intermédiaire dans le magasin de certificats Windows

Vous devez importer le certificat racine et les certificats intermédiaires dans la chaîne de certificats dans le magasin de certificats de l'ordinateur local Windows.

## Télécharger un certificat TLS à partir du serveur intermédiaire

Vous devez télécharger le certificat TLS signé par une autorité de certification qui est installé sur le serveur intermédiaire afin qu'il puisse être importé dans les serveurs Horizon 7 externes.

### Procédure

- 1 Connectez-vous au serveur intermédiaire et recherchez les certificats TLS présentés aux clients qui envoient des demandes HTTPS.
- 2 Recherchez et téléchargez le certificat TLS utilisé pour Horizon 7.

### Exemple : Téléchargement d'un certificat TLS à partir d'un système LTM F5 BIG-IP

Cet exemple utilise le gestionnaire du trafic local (LTM, Local Traffic Manager) F5 BIG-IP comme serveur intermédiaire. Cet exemple a pour but de vous donner une idée générale sur la manière dont vous pouvez télécharger un certificat à partir de votre propre serveur intermédiaire.

---

**Important** Ces étapes sont spécifiques au LTM F5 BIG-IP et ne peuvent pas s'appliquer aux nouvelles versions ou autres produits F5. Ces étapes ne s'appliquent pas aux serveurs intermédiaires d'autres fournisseurs.

---

Avant de commencer, vérifiez que le système LTM F5 BIG-IP est déployé avec Horizon 7. Vérifiez que vous avez terminé les tâches dans le guide de déploiement de F5, *Déploiement du système LTM BIG-IP avec VMware View*, disponible à l'adresse :

<http://www.f5.com/pdf/deployment-guides/f5-vmware-view-dg.pdf>.

- 1 Connectez-vous à l'utilitaire de configuration du LTM F5 BIG-IP.
- 2 Sous l'onglet Principal du volet de navigation, développez **Trafic local**, puis cliquez sur **Certificats SSL**.

L'utilitaire affiche la liste des certificats installés sur le système.

- 3 Dans la colonne Nom, cliquez sur le nom du certificat utilisé pour Horizon 7.
- 4 En bas de l'écran, cliquez sur **Exporter**.

L'utilitaire affiche le certificat TLS existant dans la zone **Texte du certificat**.

- 5 À partir du paramètre **Fichier de certificat**, cliquez sur **Téléchargernom\_fichier**.

Le certificat TLS est téléchargé en tant que fichier CRT.

## Téléchargement d'une clé privée à partir du serveur intermédiaire

Vous devez télécharger la clé privée associée au certificat TLS sur le serveur intermédiaire. La clé privée doit être importée avec le certificat dans les serveurs Horizon 7.

## Procédure

- 1 Connectez-vous au serveur intermédiaire et recherchez les certificats TLS présentés aux clients qui envoient des demandes HTTPS.
- 2 Recherchez le certificat utilisé pour Horizon 7 et téléchargez sa clé privée.

## Exemple : Télécharger une clé privée à partir d'un système F5 BIG-IP LTM

Cet exemple utilise le gestionnaire du trafic local (LTM, Local Traffic Manager) F5 BIG-IP comme serveur intermédiaire. L'exemple est conçu pour vous donner une idée générale de la manière dont vous pouvez télécharger une clé privée à partir de votre propre serveur intermédiaire.

---

**Important** Ces étapes sont spécifiques au LTM F5 BIG-IP et ne peuvent pas s'appliquer aux nouvelles versions ou autres produits F5. Ces étapes ne s'appliquent pas aux serveurs intermédiaires d'autres fournisseurs.

---

Avant de commencer, vérifiez que vous êtes connecté à l'utilitaire de configuration F5 BIG-IP LTM.

- 1 Sous l'onglet Principal du volet de navigation, développez **Trafic local**, puis cliquez sur **Certificats SSL**.

L'utilitaire affiche une liste de certificats installés sur le système.

- 2 Dans la colonne Nom, cliquez sur le nom du certificat utilisé pour Horizon 7.
- 3 Dans la barre de menus, cliquez sur **Clé**.
- 4 En bas de l'écran, cliquez sur **Exporter**.

L'utilitaire affiche la clé privée existante dans la zone **Texte de la clé**.

- 5 Dans le paramètre du fichier de clé, cliquez sur **Télécharger nom\_fichier..**

La clé privée est téléchargée en tant que fichier de clé.

## Convertir un fichier de certificat au format PKCS#12

Si vous avez obtenu un certificat et sa clé privée au format PEM ou dans un autre format, vous devez le reconverter au format PKCS#12 (PFX) avant de pouvoir l'importer dans un magasin de certificats Windows sur un serveur Horizon 7. Le format PKCS#12 (PFX) est requis si vous utilisez l'assistant Importation de certificat dans le magasin de certificats Windows.

Vous pouvez obtenir des fichiers de certificat de l'une des manières suivantes :

- Vous obtenez un fichier de magasin de clés de certificat à partir d'une autorité de certification.
- Vous téléchargez un certificat et sa clé privée à partir d'un serveur intermédiaire configuré dans votre déploiement Horizon 7.
- Votre entreprise vous fournit des fichiers de certificat.

Les fichiers de certificat se présentent sous divers formats. Par exemple, le format PEM est souvent utilisé dans un environnement Linux. Vos fichiers peuvent avoir un fichier de certificat, un fichier de clé et un fichier CSR avec les extensions suivantes :

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

Le fichier CRT contient le certificat SSL qui a été renvoyé par l'autorité de certification. Le fichier CSR est le fichier de demande de signature de certificat d'origine et n'est pas nécessaire. Le fichier KEY contient la clé privée.

### Prérequis

- Vérifiez qu'OpenSSL est installé sur le système. Vous pouvez télécharger openssl à l'adresse <http://www.openssl.org>.
- Vérifiez que le certificat racine du certificat SSL qui a été renvoyé par l'autorité de certification est également disponible sur le système.

### Procédure

- 1 Copiez les fichiers CRT et KEY dans le répertoire d'installation d'OpenSSL.  
Par exemple : `cd c:\OpenSSL-Win32\bin`
- 2 Ouvrez une invite de commande Windows et, si nécessaire, accédez au répertoire d'installation d'OpenSSL.
- 3 Générez un fichier de magasin de clés PKCS#12 (PFX) à partir du fichier de certificat et de votre clé privée.  
Par exemple : `openssl pkcs12 -export -out server.p12 -inkey server.key -in server.crt -certfile CACert.crt`  
Dans cet exemple, CACert.crt est le nom du certificat racine renvoyé par l'autorité de certification.  
Le magasin de certificats Windows accepte également un magasin de clés généré avec une extension PFX. Par exemple : `-out server.pfx`
- 4 Tapez un mot de passe d'exportation pour protéger le fichier PKCS#12 (PFX).

## Importer un certificat de serveur signé dans un magasin de certificats Windows

Vous devez importer le certificat de serveur TLS dans le magasin de certificats de l'ordinateur local Windows sur l'hôte Windows Server sur lequel l'instance du Serveur de connexion ou le service du serveur de sécurité est installé.

Ce scénario utilise un fichier de certificat au format PKCS#12 (PFX).

En fonction du format de votre fichier de certificat, la chaîne de certificats complète contenue dans le fichier de magasin de clés peut être importée dans le magasin de certificats de l'ordinateur local Windows. Par exemple, le certificat de serveur, le certificat intermédiaire et le certificat racine peuvent être importés.

Pour les autres types de fichiers de certificat, seul le certificat de serveur est importé dans le magasin de certificats de l'ordinateur local Windows. Dans ce cas, vous devez effectuer des étapes séparées pour importer le certificat racine et des certificats intermédiaires dans la chaîne de certificats.

Pour plus d'informations sur les certificats, consultez l'aide en ligne de Microsoft disponible avec le composant logiciel Certificat dans MMC.

### Prérequis

Vérifiez que le certificat du serveur TLS est au format PKCS#12 (PFX). Reportez-vous à la section [Convertir un fichier de certificat au format PKCS#12](#).

### Procédure

- 1 Dans la fenêtre MMC sur l'hôte Windows Server, développez le nœud **Certificats (ordinateur local)** et le dossier **Personnel**.
- 2 Dans le volet Actions, allez dans **Plus d'actions > Toutes les tâches > Importer**.
- 3 Dans l'assistant **Importation de certificat**, cliquez sur **Suivant** et accédez à l'emplacement de stockage du certificat.
- 4 Sélectionnez le fichier du certificat et cliquez sur **Ouvrir**.  
  
Pour afficher votre type de fichier de certificat, vous pouvez sélectionner son format de fichier dans le menu déroulant **Nom de fichier**.
- 5 Tapez le mot de passe de la clé privée incluse dans le fichier de certificat.
- 6 Sélectionnez **Marquer cette clé comme exportable**.
- 7 Sélectionnez **Inclure toutes les propriétés étendues**.
- 8 Cliquez sur **Suivant** et sur **Terminer**.

Le nouveau certificat s'affiche dans le dossier **Certificats (ordinateur local) > Personnel > Certificats**.

- 9 Vérifiez que le nouveau certificat contient une clé privée.
  - a Dans le dossier **Certificats (ordinateur local) > Personnel > Certificats**, double-cliquez sur le nouveau certificat.
  - b Dans l'onglet Général de la boîte de dialogue Informations sur le certificat, vérifiez que la déclaration suivante apparaît : Vous avez une clé privée qui correspond à ce certificat.

### Suivant

Modifiez le nom convivial du certificat en le renommant **vdm**.

## Modifier le nom convivial du certificat

Pour configurer une instance du Serveur de connexion ou un serveur de sécurité pour qu'ils reconnaissent et utilisent un certificat TLS, vous devez remplacer le nom convivial du certificat par **vdm**.

### Prérequis

Vérifiez que le certificat du serveur est importé dans le dossier **Certificats (ordinateur local) > Personnel > Certificats** dans le magasin de certificats Windows. Reportez-vous à la section [Importer un certificat de serveur signé dans un magasin de certificats Windows](#).

### Procédure

- 1 Dans la fenêtre MMC sur l'hôte Windows Server, développez le nœud **Certificats (ordinateur local)** et sélectionnez le dossier **Personnel > Certificats**.
- 2 Cliquez avec le bouton droit sur le certificat qui est émis sur l'hôte du serveur Horizon 7, puis cliquez sur **Propriétés**.
- 3 Dans l'onglet Général, supprimez le texte **Nom convivial** et entrez **vdm**.
- 4 Cliquez sur **Appliquer** puis sur **OK**.
- 5 Vérifiez qu'aucun autre certificat de serveur dans le dossier **Personnel > Certificats** ne porte le nom convivial **vdm**.
  - a Localisez tout autre certificat de serveur, cliquez avec le bouton droit sur le certificat, puis cliquez sur **Propriétés**.
  - b Si le certificat porte le nom convivial **vdm**, supprimez le nom, cliquez sur **Appliquer**, puis sur **OK**.

### Suivant

Importez le certificat racine et les certificats intermédiaires dans le magasin de certificats de l'ordinateur local Windows.

Une fois que tous les certificats de la chaîne ont été importés, vous devez redémarrer le service du Serveur de connexion ou du serveur de sécurité pour que vos modifications prennent effet.

## Importer des certificats racine et intermédiaire dans le magasin de certificats Windows

Vous devez importer le certificat racine et les certificats intermédiaires dans la chaîne de certificats dans le magasin de certificats de l'ordinateur local Windows.

Si le certificat du serveur TLS que vous avez importé à partir du serveur intermédiaire est signé par une autorité de certification racine connue et approuvée par l'hôte du Serveur de connexion, et que vos chaînes de certification ne contiennent pas de certificats intermédiaires, vous pouvez ignorer cette étape. Les autorités de certification couramment utilisées sont susceptibles d'être approuvées par l'hôte.

## Procédure

- 1 Dans la console de gestion Microsoft (MMC) sur l'hôte Windows Server, développez le nœud **Certificats (Ordinateur local)**, puis accédez au dossier **Autorités de certification racines de confiance > Certificats**.
  - Si votre certificat racine se trouve dans ce dossier, et qu'il n'y a pas de certificat intermédiaire dans votre chaîne de certificats, passez à l'étape 7.
  - Si votre certificat racine se trouve dans ce dossier, et qu'il y a des certificats intermédiaires dans votre chaîne de certificats, passez à l'étape 6.
  - Si votre certificat racine ne se trouve pas dans ce dossier, passez à l'étape 2.
- 2 Cliquez avec le bouton droit sur le dossier **Autorités de certification racines de confiance > Certificats** et cliquez sur **Toutes les tâches > Importer**.
- 3 Dans l'assistant **Importation de certificat**, cliquez sur **Suivant** et allez à l'emplacement de stockage du certificat de l'autorité de certification racine.
- 4 Sélectionnez le fichier du certificat de l'autorité de certification racine et cliquez sur **Ouvrir**.
- 5 Cliquez sur **Suivant**, **Suivant** et **Terminer**.
- 6 Si votre certificat de serveur a été signé par une autorité de certification intermédiaire, importez tous les certificats intermédiaires se trouvant dans la chaîne de certificats dans le magasin de certificats de l'ordinateur local Windows.
  - a Allez dans le dossier **Certificats (Ordinateur local) > Autorités de certification intermédiaires > Certificats**.
  - b Répétez les étapes 3 à 6 pour chaque certificat intermédiaire devant être importé.
- 7 Redémarrez le service Serveur de connexion ou le service du serveur de sécurité pour que vos modifications prennent effet.
- 8 Si vous utilisez HTML Access, redémarrez le service VMware View Blast Secure Gateway.

## Définir des URL externes d' Horizon 7 Server pour pointer les clients vers des serveurs de téléchargement TLS

Si TLS est téléchargé vers un serveur intermédiaire et que des périphériques Horizon Client utilisent le tunnel sécurisé pour se connecter à Horizon 7, vous devez définir l'URL externe du tunnel sécurisé sur une adresse que les clients peuvent utiliser pour accéder au serveur intermédiaire.

Vous configurez les paramètres d'URL externe sur l'instance du Serveur de connexion ou sur le serveur de sécurité qui se connecte au serveur intermédiaire.

Si vous déployez des serveurs de sécurité, des URL externes sont requises pour les serveurs de sécurité, mais pas pour les instances du Serveur de connexion qui sont couplées avec les serveurs de sécurité.

Si vous ne déployez pas de serveurs de sécurité ou si vous disposez d'un environnement réseau mixte comportant des serveurs de sécurité et des instances du Serveur de connexion externes, des URL externes sont requises pour les instances du Serveur de connexion qui se connectent au serveur intermédiaire.

---

**Remarque** Vous ne pouvez pas télécharger des connexions TLS à partir d'un composant PCoIP Secure Gateway (PSG) ou Blast Secure Gateway. L'URL externe de PCoIP et l'URL externe de Blast Secure Gateway doivent permettre aux clients de se connecter à l'ordinateur qui héberge PSG et Blast Secure Gateway. Ne réinitialisez pas l'URL externe de PCoIP et l'URL externe de Blast pour pointer vers le serveur intermédiaire sauf si vous prévoyez d'exiger des connexions TLS entre le serveur intermédiaire et Horizon 7 Server.

---

## Définir les URL externes d'une instance du Serveur de connexion

Vous utilisez Horizon Administrator pour configurer les URL externes d'une instance du Serveur de connexion.

### Prérequis

- Vérifiez que les connexions par tunnel sécurisé sont activées sur l'instance du Serveur de connexion.

### Procédure

- 1 Dans Horizon Administrator, cliquez sur **Configuration de View > Serveurs**.
- 2 Dans l'onglet Serveurs de connexion, sélectionnez une instance du Serveur de connexion et cliquez sur **Modifier**.
- 3 Saisissez l'URL externe du tunnel sécurisé dans la zone de texte **URL externe**.

L'URL doit contenir le protocole, le nom d'hôte résolvable par le client et le numéro de port.

Par exemple : **https://myserver.example.com:443**

---

**Remarque** Vous pouvez utiliser l'adresse IP si vous avez accès à une instance du Serveur de connexion lorsque le nom de l'hôte ne peut être résolu. Toutefois, dans ce cas, l'hôte que vous contactez ne correspond pas au certificat TLS configuré pour l'instance du Serveur de connexion, ce qui bloque l'accès ou autorise l'accès avec une sécurité limitée.

---

- 4 Vérifiez que toutes les adresses de cette boîte de dialogue permettent aux systèmes clients d'atteindre cette instance du Serveur de connexion.
- 5 Cliquez sur **OK**.

## Modifier les URL externes d'un serveur de sécurité

Vous utilisez Horizon Administrator pour modifier les URL externes d'un serveur de sécurité.



## Prérequis

- Vérifiez que les connexions par tunnel sécurisé sont activées sur l'instance du Serveur de connexion qui est couplée avec ce serveur de sécurité.

## Procédure

- 1 Dans Horizon Administrator, sélectionnez **Configuration de View > Serveurs**.
- 2 Sélectionnez l'onglet Serveurs de sécurité, sélectionnez le serveur de sécurité et cliquez sur **Modifier**.
- 3 Saisissez l'URL externe du tunnel sécurisé dans la zone de texte **URL externe**.

L'URL doit contenir le protocole, le nom d'hôte de serveur de sécurité résolvable par le client et le numéro de port.

Par exemple : `https://myserver.example.com:443`

---

**Remarque** Vous pouvez utiliser l'adresse IP si vous devez accéder à un serveur de sécurité lorsque le nom d'hôte n'est pas résolvable. Toutefois, l'hôte que vous contactez ne correspondra pas au certificat TLS configuré pour le serveur de sécurité, ce qui se traduit par un accès bloqué ou un accès avec une sécurité réduite.

---

- 4 Vérifiez que toutes les adresses de cette boîte de dialogue permettent aux systèmes clients d'atteindre cet hôte du serveur de sécurité.
- 5 Cliquez sur **OK** pour enregistrer vos modifications.

Horizon Administrator envoie l'URL externe mise à jour au serveur de sécurité. Vous n'avez pas à redémarrer le service du serveur de sécurité pour que les modifications prennent effet.

## Autoriser les connexions HTTP à partir des serveurs intermédiaires

Quand le certificat TLS est déchargé vers un serveur intermédiaire, vous pouvez configurer les instances du Serveur de connexion ou les serveurs de sécurité pour autoriser les connexions HTTP à partir des périphériques intermédiaires clients. Les périphériques intermédiaires doivent accepter HTTPS pour les connexions d'Horizon Client.

Pour autoriser les connexions HTTP entre les serveurs Horizon 7 et les périphériques intermédiaires, vous devez configurer le fichier `locked.properties` sur chaque instance du Serveur de connexion et le serveur de sécurité sur lequel les connexions HTTP sont autorisées.

Même lorsque les connexions HTTP entre les serveurs Horizon 7 et les périphériques intermédiaires sont autorisées, vous ne pouvez pas désactiver le protocole TLS dans Horizon 7. Les serveurs Horizon 7 continuent d'accepter les connexions HTTPS, ainsi que les connexions HTTP.

---

**Remarque** Si vos clients Horizon utilisent l'authentification par carte à puce, ils doivent établir des connexions HTTPS directement avec le Serveur de connexion ou le serveur de sécurité. Le déchargement TLS n'est pas pris en charge avec l'authentification par carte à puce.

---

### Procédure

- 1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle TLS/SSL sur l'hôte du Serveur de connexion ou du serveur de sécurité.

Par exemple : `install_directory\VMware\VMware View\Server\SSLgateway\conf\locked.properties`

- 2 Pour configurer le protocole du serveur Horizon 7, ajoutez la propriété `serverProtocol` et définissez-la sur `http`.

La valeur `http` doit être tapée en minuscules.

- 3 (Facultatif) Ajoutez des propriétés pour configurer un port d'écoute HTTP qui n'est pas par défaut et une interface réseau sur le serveur Horizon 7.

- Pour modifier le port d'écoute HTTP 80, définissez `serverPortNonTLS` sur un autre numéro de port sur lequel le périphérique intermédiaire est configuré pour se connecter.
- Si le serveur Horizon 7 dispose de plus d'une interface réseau et que vous prévoyez que le serveur écoute les connexions HTTP sur une seule interface, définissez `serverHostNonTLS` sur l'adresse IP de cette interface réseau.

- 4 Enregistrez le fichier `locked.properties`.

- 5 Redémarrez le service Serveur de connexion ou le service du serveur de sécurité pour que vos modifications prennent effet.

## Exemple : fichier `locked.properties`

Ce fichier autorise les connexions HTTP non-TLS à un serveur Horizon 7. L'adresse IP de l'interface réseau client du serveur Horizon 7 est 10.20.30.40. Le serveur utilise le port 80 par défaut pour écouter les connexions HTTP. La valeur `http` doit être en minuscules.

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