

Szenarien zum Einrichten von TLS-Zertifikaten für Horizon 7

Geändert am 14. März 2019
VMware Horizon 7 7.8



vmware®

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Die VMware-Website enthält auch die neuesten Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Inhalt

Szenarien zum Einrichten von TLS-Zertifikaten für Horizon 7 4

1 Beziehen von TLS-Zertifikaten von einer Zertifizierungsstelle 5

Ermitteln, ob dieses Szenario für Sie gültig ist 5

Auswählen des korrekten Zertifikattyps 6

Generieren einer Zertifikatsignieranforderung und Beziehen eines Zertifikats mit Microsoft Certreq 7

2 Verschieben von TLS-Verbindungen auf Zwischenserver 16

Importieren von TLS-Zertifikaten verschiebender Server auf Horizon 7 -Servern 16

Einstellen externer URLs von Horizon 7 Server, sodass sie Clients auf verschiebende TLS-Server
verweisen 23

Zulassen der HTTP-Verbindungen von Zwischenservern 25

Szenarien zum Einrichten von TLS-Zertifikaten für Horizon 7

Szenarien zum Einrichten von TLS-Zertifikaten für Horizon 7 bietet Beispiele zum Einrichten von TLS-Zertifikaten für die Verwendung von Horizon 7-Servern. Im ersten Szenario wird gezeigt, wie Sie signierte TLS-Zertifikate von einer Zertifizierungsstelle beziehen und sicherstellen, dass die Zertifikate in einem Format vorliegen, das von Horizon 7-Servern verwendet werden kann. Im zweiten Szenario wird gezeigt, wie Sie Horizon 7 Server für das Verschieben von TLS-Verbindungen auf einen Zwischenserver konfigurieren.

Zielgruppe

Diese Informationen sind für Personen gedacht, die Horizon 7 installieren und TLS-Zertifikate beziehen möchten, die von Horizon 7 Servern verwendet werden, bzw. für Personen, die mit Zwischenservern TLS-Verbindungen zu Horizon 7 verschieben. Die bereitgestellten Informationen sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb von Rechenzentren vertraut sind.

Beziehen von TLS-Zertifikaten von einer Zertifizierungsstelle

1

VMware empfiehlt ausdrücklich die Konfiguration von TLS-Zertifikaten, die von einer gültigen Zertifizierungsstelle (Certificate Authority, CA) für die Verwendung von Horizon-Verbindungsserver-Instanzen, Sicherheitsservern und View Composer-Instanzen signiert wurden.

Standard-TLS-Zertifikate werden generiert, wenn Sie den Verbindungsserver, den Sicherheitsserver oder View Composer-Instanzen installieren. Sie können zwar die standardmäßigen selbstsignierten Zertifikate für Testzwecke verwenden, sollten Sie aber so bald wie möglich ersetzen. Die Standardzertifikate sind nicht von einer Zertifizierungsstelle signiert. Die Verwendung von Zertifikaten, die nicht von einer Zertifizierungsstelle signiert wurden, kann von nicht vertrauenswürdigen Parteien dazu ausgenutzt werden, sich als Ihr Server auszugeben und Daten abzufangen.

In einer Horizon 7-Umgebung sollten Sie auch das Standardzertifikat ersetzen, das mit vCenter Server mit einem Zertifikat installiert wird, das von einer Zertifizierungsstelle signiert wurde. Sie können diese Aufgabe für vCenter Server mit openTLS ausführen. Ausführliche Informationen dazu finden Sie unter „Replacing vCenter Server Certificates“ (Ersetzen von vCenter Server-Zertifikaten) auf der VMware Technical Papers-Website unter <http://www.vmware.com/resources/techresources/>.

Dieses Kapitel enthält die folgenden Themen:

- [Ermitteln, ob dieses Szenario für Sie gültig ist](#)
- [Auswählen des korrekten Zertifikattyps](#)
- [Generieren einer Zertifikatsignieranforderung und Beziehen eines Zertifikats mit Microsoft Certreq](#)

Ermitteln, ob dieses Szenario für Sie gültig ist

Konfigurieren Sie Zertifikate für Horizon 7 durch Importieren der Zertifikate in den Zertifikatspeicher des lokalen Windows-Computers auf dem Horizon 7-Serverhost.

Bevor Sie ein Zertifikat importieren können, müssen Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und von einer Zertifizierungsstelle ein gültiges signiertes Zertifikat beziehen. Wenn die Zertifikatsignieranforderung nicht gemäß der in diesem Szenario beispielhaft beschriebenen Vorgehensweise generiert wurde, müssen das generierte Zertifikat und dessen privater Schlüssel in einer PKCS #12-Formatdatei (früher PFX) verfügbar sein.

Es gibt viele Möglichkeiten zum Beziehen von TLS-Zertifikaten von einer Zertifizierungsstelle. Dieses Szenario zeigt, wie Sie das Dienstprogramm Microsoft certreq zum Generieren einer Zertifikatsignieranforderung und zur Bereitstellung eines Zertifikats für einen Horizon 7-Server verwenden. Sie können auch eine andere Methode verwenden, wenn Sie mit den erforderlichen Tools vertraut und diese auf dem Server installiert sind.

Dieses löst folgende Probleme:

- Sie verfügen nicht über TLS-Zertifikate, die von einer Zertifizierungsstelle signiert wurden, und Sie wissen nicht, wie Sie diese beziehen können.
- Sie verfügen über gültige signierte TLS-Zertifikate, aber nicht im Format PKCS #12 (PFX).

Wenn Ihre Organisation von einer Zertifizierungsstelle signierte TLS-Zertifikate für Sie bereitstellt, können Sie diese verwenden. Ihre Organisation kann eine gültige interne Zertifizierungsstelle oder eine kommerzielle Zertifizierungsstelle eines Drittanbieters verwenden. Wenn Ihre Zertifikate nicht im Format PKCS #12 vorliegen, müssen Sie diese konvertieren. Siehe [Konvertieren einer Zertifikatdatei in das Format PKCS#12](#).

Wenn Sie über ein signiertes Zertifikat im richtigen Format verfügen, können Sie dieses in den Windows-Zertifikatspeicher importieren und einen Horizon 7-Server für dessen Verwendung konfigurieren. Siehe [Einrichten eines importierten Zertifikats für einen Horizon 7 Server](#).

Auswählen des korrekten Zertifikattyps

Sie können für Horizon 7 verschiedene Typen von TLS-Zertifikaten verwenden. Die Auswahl des korrekten Zertifikattyps ist entscheidend für Ihre Bereitstellung. Die Kosten der verschiedenen Zertifikattypen sind unterschiedlich, je nach der Anzahl der Server, auf denen diese verwendet werden können.

Folgen Sie den VMware-Sicherheitsempfehlungen und verwenden Sie vollqualifizierte Domännennamen (FQDN) für Ihre Zertifikate, unabhängig vom ausgewählten Typ. Verwenden Sie selbst für die Kommunikation innerhalb Ihrer internen Domäne keinen einfachen Servernamen bzw. keine einfache IP-Adresse.

Namenszertifikat für Einzelserver

Sie können ein Zertifikat mit einem Antragstellernamen für einen bestimmten Server generieren. Beispiel: dept.company.com.

Dieser Zertifikattyp ist beispielsweise hilfreich, wenn nur für eine Verbindungsserver-Instanz ein Zertifikat benötigt wird.

Wenn Sie eine Zertifikatsignieranforderung an eine Zertifizierungsstelle übermitteln, geben Sie den Servernamen an, der mit dem Zertifikat verknüpft ist. Stellen Sie sicher, dass der Horizon 7 Server den bereitgestellten Servernamen auflösen kann und dass dieser mit dem Namen identisch ist, der dem Zertifikat zugeordnet wurde.

Alternative Antragstellernamen

Ein alternativer Antragstellername (Subject Alternative Name, SAN) ist ein Attribut, das einem Zertifikat bei der Ausstellung hinzugefügt werden kann. Mit diesem Attribut können Sie einem Zertifikat Antragstellernamen (URLs) hinzufügen, damit es mehr als einen Server validieren kann.

So kann beispielsweise ein Zertifikat für einen Server mit dem Hostnamen `dept.company.com` ausgestellt werden. Sie benötigen das Zertifikat für externe Benutzer, die damit über einen Sicherheitsserver eine Verbindung mit Horizon 7 herstellen sollen. Bevor das Zertifikat ausgestellt wird, können Sie dem Zertifikat den SAN `dept-int.company.com` hinzufügen, damit das Zertifikat auf Verbindungsserver-Instanzen oder Sicherheitsservern hinter einem Lastausgleichsdienst verwendet werden kann, wenn die Tunnel-Funktionen aktiviert sind.

Platzhalterzertifikat

Ein Platzhalterzertifikat wird für Verwendung für mehrere Dienste generiert. Beispiel: `*.company.com`.

Ein Platzhalterzertifikat ist sinnvoll, wenn für viele Server ein Zertifikat nötig ist. Wenn andere Anwendungen in Ihrer Umgebung zusätzlich zu Horizon 7 TLS-Zertifikate benötigen, können Sie ein Platzhalterzertifikat auch für diese Server verwenden. Wenn Sie allerdings ein Platzhalterzertifikat benutzen, das mit anderen Diensten gemeinsam verwendet wird, richtet sich die Sicherheit des VMware Horizon-Produkts auch nach der Sicherheit der anderen Dienste.

Hinweis Ein Platzhalterzertifikat lässt sich nur auf einer Ebene einer Domäne verwenden. Beispielsweise kann ein Platzhalterzertifikat mit dem Antragstellernamen `*.company.com` für die Unterdomäne `dept.company.com`, aber nicht für `dept.it.company.com` eingesetzt werden.

Generieren einer Zertifikatsignieranforderung und Beziehen eines Zertifikats mit Microsoft Certreq

Um ein Zertifikat für einen Horizon 7 Server verfügbar zu machen, müssen Sie eine Konfigurationsdatei erstellen, eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) aus der Konfigurationsdatei generieren und die Signieranforderung an eine Zertifizierungsstelle senden. Wenn die Zertifizierungsstelle das Zertifikat zurückgibt, müssen Sie das signierte Zertifikat in den Zertifikatspeicher des lokalen Windows-Computers auf dem Horizon 7 Server-Host importieren, auf dem der zuvor generierte private Schlüssel angewendet wird.

Eine Zertifikatsignieranforderung (CSR) kann auf verschiedene Weise generiert werden, je nachdem, wie das Zertifikat selbst generiert wird.

Das Microsoft-Dienstprogramm `Certreq` steht auf Windows Server 2008 R2 zur Verfügung und kann zum Generieren einer CSR und zum Importieren eines signierten Zertifikats verwendet werden. Wenn Sie eine Anforderung an eine Drittanbieter-Zertifizierungsstelle senden möchten, bietet `Certreq` die schnellste und einfachste Möglichkeit, ein Zertifikat für Horizon 7 zu erwerben.

1 Erstellen einer CSR-Konfigurationsdatei

Das Microsoft-Dienstprogramm Certreq verwendet eine Konfigurationsdatei zum Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR). Sie müssen eine Konfigurationsdatei erstellen, bevor Sie die Anforderung generieren können. Erstellen Sie die Datei und generieren Sie die CSR auf dem Windows Server-Computer, der den Horizon 7 Server hostet, der das Zertifikat verwenden soll.

2 Generieren einer Zertifikatsignieranforderung und Anfordern eines signierten Zertifikats von einer Zertifizierungsstelle

Unter Verwendung der erstellten Konfigurationsdatei können Sie mit dem Dienstprogramm Certreq eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren. Sie senden dabei die Anforderung an eine Drittanbieter-Zertifizierungsstelle, die ein signiertes Zertifikat zurückgibt.

3 Sicherstellen, dass die Zertifikatsignieranforderung und ihr privater Schlüssel im Windows-Zertifikatsspeicher gespeichert sind

Wenn Sie mit dem Dienstprogramm Certreq eine Zertifikatsignieranforderung erstellen, wird dabei auch ein damit verknüpfter privater Schlüssel generiert. Das Dienstprogramm speichert die Zertifikatsignieranforderung und den privaten Schlüssel im Zertifikatsspeicher des lokalen Windows-Computers, auf dem Sie die Zertifikatsignieranforderung erstellt haben. Sie können mithilfe des Zertifikat-Snap-In in der Microsoft Management Console (MMC) überprüfen, ob die Zertifikatsignieranforderung und der private Schlüssel ordnungsgemäß gespeichert wurden.

4 Importieren eines signierten Zertifikats mit Certreq

Wenn Sie über ein signiertes Zertifikat von einer Zertifizierungsstelle verfügen, können Sie das Zertifikat in den Zertifikatsspeicher des lokalen Windows-Computers auf dem Horizon 7 Server-Host importieren.

5 Einrichten eines importierten Zertifikats für einen Horizon 7 Server

Nachdem Sie ein Serverzertifikat in den Zertifikatsspeicher des lokalen Windows-Computers importiert haben, müssen Sie weitere Schritte durchführen, damit ein Horizon 7 Server dieses Zertifikat verwenden kann.

Erstellen einer CSR-Konfigurationsdatei

Das Microsoft-Dienstprogramm Certreq verwendet eine Konfigurationsdatei zum Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR). Sie müssen eine Konfigurationsdatei erstellen, bevor Sie die Anforderung generieren können. Erstellen Sie die Datei und generieren Sie die CSR auf dem Windows Server-Computer, der den Horizon 7 Server hostet, der das Zertifikat verwenden soll.

Voraussetzungen

Holen Sie die Informationen ein, die Sie für die Konfigurationsdatei benötigen. Sie müssen den vollqualifizierten Domännennamen (FQDN) des Horizon 7 Server und die Organisationseinheit, die Organisation, den Ort, das Bundesland und das Land zur Vervollständigung des Antragstellernamens kennen.

Verfahren

- 1 Öffnen Sie einen Texteditor und fügen Sie den folgenden Text, einschließlich der Anfangs- und End-Tags, in die Datei ein.

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

[Version]

Signature="$Windows NT$"

[NewRequest]

Subject = "CN=View Server-FQDN, OU=Organisationseinheit, O=Organisation, L=Stadt, S=Bundesland, C=Land"
; 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

;-----
```

Wenn beim Kopieren und Einfügen des Textes ein zusätzliches CR/LF-Zeichen (manueller Zeilenumbruch) in der Zeile `Subject =` hinzugefügt wird, löschen Sie es.

- 2 Aktualisieren Sie die Subject-Attribute durch die entsprechenden Werte für Ihren Horizon 7 Server und Ihre Bereitstellung.

Beispiel: `CN=dept.company.com`

Verwenden Sie zur Einhaltung der VMware-Sicherheitsempfehlungen den vollqualifizierten Domänennamen (FQDN), mit dem Clientgeräte eine Verbindung mit dem Host herstellen. Verwenden Sie selbst für die Kommunikation innerhalb Ihrer internen Domäne keinen einfachen Servernamen bzw. keine einfache IP-Adresse.

Einige Zertifizierungsstellen lassen die Verwendung von Abkürzungen für das Statusattribut nicht zu.

- 3 (Optional) Aktualisieren Sie das Attribut `KeyLength`.

Der Standardwert 2048 ist geeignet, wenn Sie nicht ausdrücklich eine andere `KeyLength`-Größe benötigen. Viele Zertifizierungsstellen erfordern den Mindestwert 2048. Größere Schlüssel sind sicherer, jedoch haben sie eine größere Auswirkung auf die Leistung.

Ein `KeyLength`-Wert von 1024 wird auch unterstützt, obwohl das „National Institute of Standards and Technology“ (NIST) Schlüssel dieser Größe nicht empfiehlt. Computer werden immer leistungsstärker, sodass die Wahrscheinlichkeit steigt, dass auch stärkere Verschlüsselungen in Zukunft entschlüsselt werden können.

Wichtig Generieren Sie keine `KeyLength`-Werte unter 1024. Horizon Client für Windows validiert keine Zertifikate auf einem Horizon 7 Server, die mit einem `KeyLength`-Wert unter 1024 generiert wurden. Die Verbindung der Horizon Client-Geräte mit Horizon 7 wird dann fehlschlagen. Auch vom Verbindungsserver durchgeführte Zertifikatüberprüfungen schlagen fehl, sodass die betreffenden Horizon 7-Server im Horizon Administrator-Dashboard in rot angezeigt werden.

- 4 Speichern Sie die Datei als `request.inf`.

Nächste Schritte

Generieren Sie eine Zertifikatsignieranforderung aus der Konfigurationsdatei.

Generieren einer Zertifikatsignieranforderung und Anfordern eines signierten Zertifikats von einer Zertifizierungsstelle

Unter Verwendung der erstellten Konfigurationsdatei können Sie mit dem Dienstprogramm `Certreq` eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren. Sie senden dabei die Anforderung an eine Drittanbieter-Zertifizierungsstelle, die ein signiertes Zertifikat zurückgibt.

Voraussetzungen

- Stellen Sie sicher, dass die Erstellung einer CSR-Konfigurationsdatei abgeschlossen ist. Siehe [Erstellen einer CSR-Konfigurationsdatei](#).
- Führen Sie auf dem Computer mit der CSR-Konfigurationsdatei den in dieser Vorgehensweise beschriebenen `Certreq`-Vorgang durch.

Verfahren

- 1 Öffnen Sie eine Eingabeaufforderung, indem Sie mit der rechten Maustaste auf **Eingabeaufforderung** im **Startmenü** klicken, und wählen Sie **Als Administrator ausführen** aus.
- 2 Wechseln Sie zu dem Verzeichnis, in dem die Datei `request.inf` gespeichert ist.
Beispiel: `cd c:\certificates`
- 3 Generieren Sie die CSR-Datei.
Beispiel: `certreq -new request.inf certreq.txt`
- 4 Verwenden Sie den Inhalt der CSR-Datei, um eine Zertifikatanforderung an die Zertifizierungsstelle in Übereinstimmung mit dem dafür vorgesehenen Registrierungsverfahren zu senden.
 - a Wenn Sie die Anforderung an eine Zertifizierungsstelle übermitteln, werden Sie von der Zertifizierungsstelle aufgefordert, den Typ des Servers auszuwählen, auf dem Sie das Zertifikat installieren möchten. Da Horizon 7 für die Verwaltung von Zertifikaten das Zertifikate-MMC von Microsoft verwendet, wählen Sie ein Zertifikat für einen Server vom Typ Microsoft, Microsoft IIS 7 oder etwas Vergleichbares aus. Von der Zertifizierungsstelle wird ein Zertifikat in dem Format benötigt, das für die Arbeit mit Horizon 7 erforderlich ist.
 - b Wenn Sie ein Namenszertifikat für einen einzelnen Server anfordern, müssen Sie einen Namen verwenden, den Horizon Client-Geräte in eine IP-Adresse für diesen Horizon 7 Server auflösen können. Der Name, den Computer für die Herstellung einer Verbindung mit dem Horizon 7 Server verwenden, muss mit dem dem Zertifikat zugeordneten Namen übereinstimmen.

Hinweis Die Zertifizierungsstelle verlangt möglicherweise das Kopieren und Einfügen des Inhalts der CSR-Datei (z. B. `certreq.txt`) in ein Webformular. Den Inhalt der CSR-Datei können Sie mit einem Texteditor kopieren. Achten Sie darauf, dass die öffnenden und schließenden Tags enthalten sind. Beispiel:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID2jCCAsICAQAwazEWMBOGA1UEBhMNW5pdGVkIFN0YXRlc2ELMAkGA1UECAwC
Q0ExEjAQBgNVBACMCVBhbG8gQWx0bzEKMAgGA1UECgwBTzELMAkGA1UECwwCT1Ux
FzAVBgNVBAMMDm15LmNvbXBhbnkuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
. . .
. . .
L9nPYX76jeu5rwQFXLivSCea6nZiIOZYw8Dbn8dgaAqJdzBbrwuM1TuSnx6bAK8
S52Tv0GxW58jUTtxFV+Roz8TE8wZDFB51jx+FmLs
-----END NEW CERTIFICATE REQUEST-----
```

Nach einigen Überprüfungen in Ihrem Unternehmen erstellt die Zertifizierungsstelle ein Serverzertifikat auf der Grundlage der Informationen in der CSR-Datei, signiert diese mit dem privaten Schlüssel und sendet Ihnen das Zertifikat.

Die Zertifizierungsstelle sendet Ihnen auch ein Stammzertifizierungsstellenzertifikat und, wenn erforderlich, ein Zwischenzertifizierungsstellenzertifikat.

5 Benennen Sie die Textdatei des Zertifikats in `cert.cer` um.

Stellen Sie sicher, dass sich die Datei auf dem Horizon 7 Server befindet, auf dem die Zertifikatanforderung generiert wurde.

6 Benennen Sie die Dateien des Stammzertifizierungsstellen- und Zwischenzertifizierungsstellenzertifikats in `root.cer` und `intermediate.cer` um.

Stellen Sie sicher, dass sich die Dateien auf dem Horizon 7 Server befinden, auf dem die Zertifikatanforderung generiert wurde.

Hinweis Diese Zertifikate müssen nicht im Format PKCS #12 (PFX) vorliegen, wenn Sie die Zertifikate mit dem Dienstprogramm `Certreq` in den Zertifikatspeicher des lokalen Windows-Computers importieren. Das Format PKCS #12 (PFX) ist erforderlich, wenn Sie Zertifikate mit dem Assistenten „Zertifikat importieren“ in den Windows-Zertifikatspeicher importieren.

Nächste Schritte

Stellen Sie sicher, dass die CSR-Datei und deren privater Schlüssel im Zertifikatspeicher des lokalen Windows-Computers gespeichert wurden.

Sicherstellen, dass die Zertifikatsignieranforderung und ihr privater Schlüssel im Windows-Zertifikatspeicher gespeichert sind

Wenn Sie mit dem Dienstprogramm `Certreq` eine Zertifikatsignieranforderung erstellen, wird dabei auch ein damit verknüpfter privater Schlüssel generiert. Das Dienstprogramm speichert die Zertifikatsignieranforderung und den privaten Schlüssel im Zertifikatspeicher des lokalen Windows-Computers, auf dem Sie die Zertifikatsignieranforderung erstellt haben. Sie können mithilfe des Zertifikat-Snap-In in der Microsoft Management Console (MMC) überprüfen, ob die Zertifikatsignieranforderung und der private Schlüssel ordnungsgemäß gespeichert wurden.

Der private Schlüssel muss später mit dem signierten Zertifikat verknüpft werden, damit das Zertifikat ordnungsgemäß importiert und von einem Horizon 7 Server verwendet werden kann.

Voraussetzungen

- Überprüfen Sie, ob eine Zertifikatsignieranforderung mithilfe des Dienstprogramms `Certreq` erstellt und ein signiertes Zertifikat von einer Zertifizierungsstelle angefordert wurde. Siehe [Generieren einer Zertifikatsignieranforderung und Anfordern eines signierten Zertifikats von einer Zertifizierungsstelle](#).
- Machen Sie sich mit der Vorgehensweise für das Hinzufügen eines Zertifikat-Snap-In zur Microsoft Management Console (MMC) vertraut. Erläuterungen dazu erhalten Sie unter „Hinzufügen des Zertifikat-Snap-In zur MMC“ im Kapitel „Konfigurieren von TLS-Zertifikaten für Horizon 7 Server“ im Dokument *Horizon 7-Installation*.

Verfahren

- 1 Fügen Sie auf dem Windows Server-Computer das Zertifikat-Snap-In zu MMC hinzu.

- 2 Erweitern Sie im MMC-Fenster auf dem Windows Server-Computer den Knoten **Zertifikate (Lokaler Computer)** und wählen Sie den Ordner **Certificate Enrollment Request** (Zertifikatregistrierungsanforderung) aus.
- 3 Erweitern Sie den Ordner **Certificate Enrollment Request** (Zertifikatregistrierungsanforderung) und wählen Sie den Ordner **Zertifikate** aus.
- 4 Stellen Sie sicher, dass der Zertifikateintrag im Ordner **Zertifikate** enthalten ist.

Die Felder **Herausgegeben für** und **Herausgegeben von** müssen den Domännennamen enthalten, den Sie im Feld **subject:CN** der Datei `request.inf` eingegeben haben, mit der Sie die Zertifikatsignieranforderung erstellt haben.

- 5 Stellen Sie sicher, dass das Zertifikat einen privaten Schlüssel enthält, indem Sie einen dieser Schritte ausführen:
 - Stellen Sie sicher, dass ein gelber Schlüssel auf dem Symbol Zertifikat erscheint.
 - Doppelklicken Sie auf das Zertifikat und überprüfen Sie, ob die folgende Aussage im Dialogfeld „Zertifikatsinformationen“ enthalten ist: *Sie besitzen einen privaten Schlüssel für dieses Zertifikat.*

Nächste Schritte

Importieren Sie das Zertifikat in den Zertifikatspeicher des lokalen Windows-Computers.

Importieren eines signierten Zertifikats mit Certreq

Wenn Sie über ein signiertes Zertifikat von einer Zertifizierungsstelle verfügen, können Sie das Zertifikat in den Zertifikatspeicher des lokalen Windows-Computers auf dem Horizon 7 Server-Host importieren.

Wenn Sie das Dienstprogramm `Certreq` zum Generieren einer Zertifikatsignieranforderung verwendet haben, befindet sich der private Schlüssel des Zertifikats lokal auf dem Server, auf dem Sie die Zertifikatsignieranforderung generiert haben. Für ein ordnungsgemäßes Funktionieren muss das Zertifikat mit dem privaten Schlüssel kombiniert werden. Stellen Sie mit dem Befehl `certreq`, wie in dieser Vorgehensweise gezeigt, sicher, dass das Zertifikat und der private Schlüssel ordnungsgemäß kombiniert und in den Windows-Zertifikatspeicher importiert wurden.

Wenn Sie eine andere Methode zum Bezug eines signierten Zertifikats von einer Zertifizierungsstelle verwenden, können Sie mit dem Zertifikatimport-Assistenten des Snap-In „Microsoft Management Console“ (MMC) ein Zertifikat in den Windows-Zertifikatspeicher importieren. Diese Methode wird unter „Konfigurieren von TLS-Zertifikaten für Horizon 7 Server“ im Dokument *Horizon 7-Installation* beschrieben.

Voraussetzungen

- Stellen Sie sicher, dass Sie ein signiertes Zertifikat von einer Zertifizierungsstelle erhalten haben. Siehe [Generieren einer Zertifikatsignieranforderung und Anfordern eines signierten Zertifikats von einer Zertifizierungsstelle](#).
- Führen Sie den `Certreq`-Vorgang, wie in dieser Vorgehensweise beschrieben, auf dem Computer aus, auf dem Sie eine Zertifikatsignieranforderung generiert und das signierte Zertifikat gespeichert haben.

Verfahren

- 1 Öffnen Sie eine Eingabeaufforderung, indem Sie mit der rechten Maustaste auf **Eingabeaufforderung** im **Startmenü** klicken, und wählen Sie **Als Administrator ausführen** aus.
- 2 Wechseln Sie zu dem Verzeichnis, in dem die Datei des signierten Zertifikats (z. B. `cert.cer`) gespeichert ist.

Beispiel: `cd c:\certificates`

- 3 Importieren Sie das signierte Zertifikat durch Ausführung des Befehls `certreq -accept`.

Beispiel: `certreq -accept cert.cer`

Das Zertifikat wird in den Zertifikatspeicher des lokalen Windows-Computers importiert.

Nächste Schritte

Konfigurieren Sie das importierte Zertifikat, damit es von einem Horizon 7 Server verwendet werden kann. Siehe [Einrichten eines importierten Zertifikats für einen Horizon 7 Server](#).

Einrichten eines importierten Zertifikats für einen Horizon 7 Server

Nachdem Sie ein Serverzertifikat in den Zertifikatspeicher des lokalen Windows-Computers importiert haben, müssen Sie weitere Schritte durchführen, damit ein Horizon 7 Server dieses Zertifikat verwenden kann.

Verfahren

- 1 Stellen Sie sicher, dass das Serverzertifikat erfolgreich importiert wurde.
- 2 Ändern Sie den Anzeigenamen des Zertifikats in **vdm**.

vdm muss in Kleinbuchstaben geschrieben sein. Alle anderen Zertifikate mit den Anzeigenamen **vdm** müssen umbenannt werden, oder Sie müssen den Anzeigenamen von diesen Zertifikaten entfernen.

Sie müssen den Anzeigenamen von Zertifikaten, die von View Composer verwendet werden, nicht ändern.
- 3 Installieren Sie das Stammzertifizierungsstellenzertifikat und das Zwischenzertifizierungsstellenzertifikat im Windows-Zertifikatspeicher.
- 4 Starten Sie den Verbindungsserver-Dienst, den Sicherheitsserverdienst oder den View Composer-Dienst neu, damit der Dienst die neuen Zertifikate verwenden kann.
- 5 Wenn Sie HTML Access verwenden, starten Sie den VMware View Blast Secure Gateway-Dienst neu.

6 Wenn Sie ein Zertifikat auf einem View Composer Server einrichten, müssen Sie möglicherweise einen weiteren Schritt durchführen.

- Wenn Sie nach der Installation von View Composer das neue Zertifikat einrichten, müssen Sie das Dienstprogramm `SviConfig ReplaceCertificate` ausführen, um das Zertifikat, das an den von View Composer verwendeten Port gebunden ist, zu ersetzen.
- Wenn Sie das neue Zertifikat einrichten, bevor Sie View Composer installieren, müssen Sie das Dienstprogramm `SviConfig ReplaceCertificate` nicht ausführen. Wenn Sie das View Composer-Installationsprogramm ausführen, können Sie statt des selbstsignierten Standardzertifikats das neue Zertifikat auswählen, das von einer Zertifizierungsstelle signiert wurde.

Weitere Informationen finden Sie unter „Bindung eines neuen TLS-Zertifikats an den von View Composer verwendeten Port“ im Dokument *Horizon 7-Installation*.

Weitere Informationen zum Durchführen der Aufgaben in dieser Vorgehensweise finden Sie in den folgenden Themen:

- [Ändern des Anzeigenamens eines Zertifikats](#)
- [Importieren der Stamm- und Zwischenzertifikate in einen Windows-Zertifikatspeicher](#)

Zusätzliche Erläuterungen erhalten Sie unter „Konfigurieren des Verbindungsservers, Sicherheitsservers oder von View Composer für die Verwendung eines neuen TLS-Zertifikats“ im Dokument *Horizon 7-Installation*.

Hinweis Das *Horizon 7-Installation*-Thema „Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher“ ist hier nicht aufgeführt, da Sie das Serverzertifikat mithilfe des Dienstprogramms `Certreq` bereits importiert haben. Verwenden Sie nicht den Assistenten „Zertifikat importieren“ des MMC-Snap-In zum erneuten Importieren des Serverzertifikats.

Sie können jedoch mit dem Assistenten „Zertifikat importieren“ das Stammzertifizierungsstellenzertifikat und das Zwischenzertifizierungsstellenzertifikat in den Windows-Zertifikatspeicher importieren.

Verschieben von TLS-Verbindungen auf Zwischenserver

2

Sie können Zwischenserver zwischen Ihren Horizon 7 Servern und Horizon Client-Geräten für Aufgaben wie z. B. den Lastausgleich und das Verschieben von TLS-Verbindungen einrichten. Horizon Client-Geräte stellen über HTTPS Verbindungen mit den Zwischenservern her, die diese Verbindungen an externe Verbindungsserver-Instanzen oder Sicherheitsserver übergeben.

Um die TLS-Verbindungen auf einen Zwischenserver zu verschieben, müssen Sie einige wichtige Aufgaben durchführen:

- Importieren des TLS-Zertifikats, das von dem Zwischenserver für Ihre externen Horizon 7 Server verwendet wird.
- Festlegen der externen URLs auf Ihren externen Horizon 7-Servern, um eine Übereinstimmung mit den URLs herzustellen, mit denen Clients eine Verbindung mit dem Zwischenserver herstellen können.
- Lassen Sie HTTP-Verbindungen zwischen dem Zwischenserver und den Horizon 7-Servern zu.

Dieses Kapitel enthält die folgenden Themen:

- [Importieren von TLS-Zertifikaten verschiebender Server auf Horizon 7-Servern](#)
- [Einstellen externer URLs von Horizon 7 Server, sodass sie Clients auf verschiebende TLS-Server verweisen](#)
- [Zulassen der HTTP-Verbindungen von Zwischenservern](#)

Importieren von TLS-Zertifikaten verschiebender Server auf Horizon 7 -Servern

Wenn Sie TLS-Verbindungen auf einen Zwischenserver verschieben, müssen Sie das Zertifikat des Zwischenservers auf die Verbindungsserver-Instanzen oder Sicherheitsserver importieren, die eine Verbindung zum Zwischenserver herstellen. Sowohl auf dem verschiebenden Zwischenserver als auch auf jedem verschobenen Horizon 7-Server, der eine Verbindung zum Zwischenserver herstellt, muss sich dasselbe TLS-Serverzertifikat befinden.

Wenn Sie Sicherheitsserver bereitstellen, muss sich sowohl auf dem Zwischenserver als auch auf den Sicherheitsservern, die eine Verbindung zum Zwischenserver herstellen, dasselbe TLS-Zertifikat befinden. Es ist nicht erforderlich, dasselbe TLS-Zertifikat auf Verbindungsserver-Instanzen zu installieren, die an die Sicherheitsserver gekoppelt sind und keine direkte Verbindung zum Zwischenserver herstellen.

Wenn Ihre Bereitstellung keine Sicherheitsserver enthält oder wenn es sich um eine gemischte Netzwerkkumgebung mit Sicherheitsservern und Verbindungsserver-Instanzen mit externen Verbindungen handelt, muss sich sowohl auf dem Zwischenserver als auch auf den Verbindungsserver-Instanzen, die eine Verbindung zum Zwischenserver herstellen, dasselbe TLS-Zertifikat befinden.

Wenn das Zertifikat des Zwischenservers nicht auf der Verbindungsserver-Instanz oder dem Sicherheitsserver installiert ist, können Clients ihre Verbindungen zu Horizon 7 nicht validieren. Unter diesen Umständen entspricht der vom Horizon 7-Server gesendete Zertifikatfingerabdruck nicht dem Zertifikat auf dem Zwischenserver, mit dem sich Horizon Client verbindet.

Verwechseln Sie nicht Lastausgleich mit TLS-Verschieben. Das zuvor genannte Erfordernis gilt für alle Geräte, die konfiguriert wurden, TLS-Verschiebungen zu leisten, einschließlich einiger Lastausgleichstypen. Ein reiner Lastenausgleich erfordert jedoch nicht das Kopieren von Zertifikaten zwischen Geräten.

Wichtig Das in den folgenden Themen beschriebene Szenario zeigt einen Ansatz für die gemeinsame Nutzung von TLS-Zertifikaten durch Komponenten von Drittanbietern und VMware-Komponenten. Dieser Ansatz ist möglicherweise nicht für alle Fälle geeignet und ist auch nicht die einzige Möglichkeit, wie diese Aufgabe ausgeführt werden kann.

1 [Herunterladen eines TLS-Zertifikats vom Zwischenserver](#)

Sie müssen das auf dem Zwischenserver installierte TLS-Zertifikat, das von der Zertifizierungsstelle signiert ist, herunterladen, damit es in externe Horizon 7 Server importiert werden kann.

2 [Herunterladen eines privaten Schlüssels vom Zwischenserver](#)

Sie müssen den privaten Schlüssel herunterladen, der dem TLS-Zertifikat auf dem Zwischenserver zugeordnet ist. Der private Schlüssel muss mit dem Zertifikat in den Horizon 7 Server importiert werden.

3 [Konvertieren einer Zertifikatdatei in das Format PKCS#12](#)

Wenn Sie ein Zertifikat und dessen privaten Schlüssel in PEM-Format oder in einem anderen Format erhalten, müssen Sie es in das Format PKCS#12 (PFX) konvertieren, bevor Sie das Zertifikat in einen Windows-Zertifikatspeicher auf einem Horizon 7 Server importieren können. Das Format PKCS#12 (PFX) ist erforderlich, wenn Sie den Assistenten „Zertifikat importieren“ im Windows-Zertifikatspeicher verwenden.

4 [Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher](#)

Sie müssen das TLS-Serverzertifikat in den Zertifikatspeicher des lokalen Windows-Computers auf dem Windows Server-Host importieren, auf dem die Verbindungsserver-Instanz oder der Sicherheitsserver-Dienst installiert ist.

5 [Ändern des Anzeigenamens eines Zertifikats](#)

Um die Verbindungsserver-Instanz oder den Sicherheitsserver für die Erkennung und Verwendung eines TLS-Zertifikats zu konfigurieren, müssen Sie den Anzeigenamen des Zertifikats in vdm ändern.

6 [Importieren der Stamm- und Zwischenzertifikate in einen Windows-Zertifikatspeicher](#)

Sie müssen das Stammzertifikat und alle Zwischenzertifikate in der Zertifikatkette in den Zertifikatspeicher des lokalen Windows-Computers importieren.

Herunterladen eines TLS-Zertifikats vom Zwischenserver

Sie müssen das auf dem Zwischenserver installierte TLS-Zertifikat, das von der Zertifizierungsstelle signiert ist, herunterladen, damit es in externe Horizon 7 Server importiert werden kann.

Verfahren

- 1 Stellen Sie die Verbindung mit dem Zwischenserver her und suchen Sie die TLS-Zertifikate für Clients, die HTTPS-Anfragen senden.
- 2 Suchen Sie das TLS-Zertifikat, das für Horizon 7 verwendet wird, und laden Sie es herunter.

Beispiel: Herunterladen eines TLS-Zertifikats von einem F5 BIG-IP LTM-System

Dieses Beispiel verwendet den F5 BIG-IP-Local Traffic Manager (LTM) als Zwischenserver. Das Beispiel soll einen allgemeinen Überblick geben, wie Sie ein Zertifikat von Ihrem eigenen Zwischenserver herunterladen können.

Wichtig Diese Schritte beziehen sich auf F5 BIG-IP LTM und können nicht für neuere Versionen oder andere F5-Produkte angewendet werden. Die dargestellten Schritte gelten auch nicht für Zwischenserver anderer Anbieter.

Bevor Sie beginnen, müssen Sie sicherstellen, dass das System F5 BIG-IP LTM mit Horizon 7 bereitgestellt ist. Stellen Sie sicher, dass Sie die Aufgaben im F5-Bereitstellungshandbuch, *Bereitstellung des BIG-IP LTM-Systems mit VMware View* durchgeführt haben (siehe <http://www.f5.com/pdf/deployment-guides/f5-vmware-view-dg.pdf>).

- 1 Stellen Sie eine Verbindung mit dem Konfigurationsdienstprogramm F5 BIG-IP LTM her.
- 2 Klicken Sie auf die Registerkarte „Übersicht“ im Navigationsbereich, erweitern Sie **Lokaler Datenverkehr** und klicken Sie auf **SSL-Zertifikate**.

Das Dienstprogramm stellt eine Liste der Zertifikate dar, die auf dem System installiert sind.

- 3 Klicken Sie in der Spalte „Name“ auf den Namen des Zertifikats, das für Horizon 7 verwendet wird.
- 4 Klicken Sie am unteren Bildschirmrand auf **Exportieren**.

Das Dienstprogramm zeigt das vorhandene TLS-Zertifikat im Feld **Zertifikatstext** an.

- 5 Klicken Sie in der Einstellung **Zertifikatdatei** auf **Herunterladen Dateiname**.

Das TLS-Zertifikat wird als CRT-Datei heruntergeladen.

Herunterladen eines privaten Schlüssels vom Zwischenserver

Sie müssen den privaten Schlüssel herunterladen, der dem TLS-Zertifikat auf dem Zwischenserver zugeordnet ist. Der private Schlüssel muss mit dem Zertifikat in den Horizon 7 Server importiert werden.

Verfahren

- 1 Stellen Sie die Verbindung mit dem Zwischenserver her und suchen Sie die TLS-Zertifikate für Clients, die HTTPS-Anfragen senden.
- 2 Suchen Sie das Zertifikat, das für Horizon 7 verwendet wird, und laden Sie dessen privaten Schlüssel herunter.

Beispiel: Herunterladen eines privaten Schlüssels von einem F5 BIG-IP LTM-System

Dieses Beispiel verwendet den F5 BIG-IP-Local Traffic Manager (LTM) als Zwischenserver. Das Beispiel soll einen allgemeinen Überblick geben, wie Sie einen privaten Schlüssel von Ihrem eigenen Zwischenserver herunterladen können.

Wichtig Diese Schritte beziehen sich auf F5 BIG-IP LTM und können nicht für neuere Versionen oder andere F5-Produkte angewendet werden. Die dargestellten Schritte gelten auch nicht für Zwischenserver anderer Anbieter.

Bevor Sie beginnen, müssen Sie sicherstellen, dass Sie mit dem Konfigurationsdienstprogramm F5 BIG-IP LTM verbunden sind.

- 1 Klicken Sie auf die Registerkarte „Übersicht“ im Navigationsbereich, erweitern Sie **Lokaler Datenverkehr** und klicken Sie auf **SSL-Zertifikate**.

Das Dienstprogramm stellt eine Liste der Zertifikate dar, die auf dem System installiert sind.

- 2 Klicken Sie in der Spalte „Name“ auf den Namen des Zertifikats, das für Horizon 7 verwendet wird.

- 3 Klicken Sie in der Menüleiste auf **Schlüssel**.

- 4 Klicken Sie am unteren Bildschirmrand auf **Exportieren**.

Das Dienstprogramm zeigt den vorhandenen privaten Schlüssel im Feld **Schlüsseltext** an.

- 5 Klicken Sie in der Einstellung für die Schlüsseldatei auf **HerunterladenDateiname**.

Der private Schlüssel wird als KEY-Datei heruntergeladen.

Konvertieren einer Zertifikatdatei in das Format PKCS#12

Wenn Sie ein Zertifikat und dessen privaten Schlüssel in PEM-Format oder in einem anderen Format erhalten, müssen Sie es in das Format PKCS#12 (PFX) konvertieren, bevor Sie das Zertifikat in einen Windows-Zertifikatspeicher auf einem Horizon 7 Server importieren können. Das Format PKCS#12 (PFX) ist erforderlich, wenn Sie den Assistenten „Zertifikat importieren“ im Windows-Zertifikatspeicher verwenden.

Sie können Zertifikatdateien mit einer der folgenden Methoden abrufen:

- Sie erhalten von einer Zertifizierungsstelle eine Zertifikat-Keystore-Datei.
- Sie laden ein Zertifikat und dessen privaten Schlüssel von einem Zwischenserver herunter, der in Ihrer Horizon 7-Bereitstellung eingerichtet ist.

- Ihre Organisation stellt Ihnen die Zertifikatdateien zur Verfügung.

Zertifikatdateien können in verschiedenen Formaten vorliegen. Das PEM-Format wird z. B. häufig in einer Linux-Umgebung verwendet. Ihre Dateien enthalten möglicherweise eine Zertifikatdatei, eine Schlüssel-datei und eine CSR-Datei mit den folgenden Erweiterungen:

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

Die CRT-Datei enthält das SSL-Zertifikat, das von der Zertifizierungsstelle zurückgegeben wurde. Die CSR-Datei ist die ursprüngliche Zertifikatsignieranforderungsdatei. Sie ist nicht erforderlich. Die KEY-Datei enthält den privaten Schlüssel.

Voraussetzungen

- Stellen Sie sicher, dass OpenSSL auf dem System installiert ist. Sie können `openssl` über <http://www.openssl.org> herunterladen.
- Stellen Sie sicher, dass das Stammzertifikat des SSL-Zertifikats, das von der Zertifizierungsstelle zurückgegeben wurde, auch auf dem System verfügbar ist.

Verfahren

- 1 Kopieren Sie die CRT- und KEY-Dateien in das OpenSSL-Installationsverzeichnis.

Beispiel: `cd c:\OpenSSL-Win32\bin`

- 2 Öffnen Sie eine Windows-Eingabeaufforderung und wechseln Sie bei Bedarf in das Installationsverzeichnis von OpenSSL.

- 3 Generieren Sie eine PKCS#12 (PFX)-Keystore-Datei aus der Zertifikatdatei und Ihrem privaten Schlüssel.

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

In diesem Beispiel ist `CACert.crt` der Name des Stammzertifikats, das von der Zertifizierungsstelle zurückgegeben wurde.

Der Windows-Zertifikatspeicher akzeptiert auch eine Keystore-Datei, die mit der Erweiterung PFX generiert wurde. Beispiel: `-out server.pfx`

- 4 Geben Sie ein Exportkennwort ein, um die PKCS#12 (PFX)-Datei zu schützen.

Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher

Sie müssen das TLS-Serverzertifikat in den Zertifikatspeicher des lokalen Windows-Computers auf dem Windows Server-Host importieren, auf dem die Verbindungsserver-Instanz oder der Sicherheitsserver-Dienst installiert ist.

Bei diesem Szenario wird eine Zertifikatdatei im Format PKCS#12 (PFX) verwendet.

Je nach Format Ihrer Zertifikatdateien wird möglicherweise die gesamte Zertifikatkette, die sich in der Schlüsselspeicherdatei befindet, in den Zertifikatspeicher des lokalen Windows-Computers importiert. Beispielsweise können das Serverzertifikat, Zwischenzertifikat und Stammzertifikat importiert werden.

Bei anderen Arten von Zertifikatdateien wird nur das Serverzertifikat in den Zertifikatspeicher des lokalen Windows-Computers importiert. In diesem Fall müssen Sie separate Schritte ausführen, um das Stammzertifikat und ggf. alle Zwischenzertifikate in der Zertifikatkette zu importieren.

Weitere Informationen zu Zertifikaten finden Sie in der Microsoft-Onlinehilfe für das MMC-Snap-In „Zertifikate“.

Voraussetzungen

Stellen Sie sicher, dass das TLS-Serverzertifikat das Format PKCS#12 (PFX) aufweist. Siehe [Konvertieren einer Zertifikatdatei in das Format PKCS#12](#).

Verfahren

- 1 Erweitern Sie im MMC-Fenster auf dem Windows Server-Host den Knoten **Zertifikate (Lokaler Computer)** und wählen Sie den Ordner **Persönlich**.
- 2 Wechseln Sie im Bereich „Aktionen“ zu **Weitere Aktionen > Alle Aufgaben > Importieren**.
- 3 Klicken Sie im **Zertifikatimport-Assistenten** auf **Weiter** und navigieren Sie zum Speicherort des Zertifikats.
- 4 Wählen Sie die Zertifikatdatei und klicken Sie auf **Öffnen**.

Um den Typ Ihrer Zertifikatdatei anzuzeigen, können Sie ihr Dateiformat im Dropdown-Menü **Dateiname** auswählen.

- 5 Geben Sie das Kennwort für den privaten Schlüssel in der Zertifikatdatei ein.
- 6 Wählen Sie **Schlüssel als exportierbar markieren**.
- 7 Aktivieren Sie **Alle erweiterten Eigenschaften mit einbeziehen**.
- 8 Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.

Das neue Zertifikat wird im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** angezeigt.

- 9 Überprüfen Sie, ob das neue Zertifikat einen privaten Schlüssel enthält.
 - a Doppelklicken Sie im Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** auf das neue Zertifikat.
 - b Prüfen Sie, ob die folgende Meldung im Dialogfeld „Zertifikatinformationen“ auf der Registerkarte „Allgemein“ angezeigt wird: Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

Nächste Schritte

Ändern Sie den Anzeigenamen des Zertifikats auf **vdm**.

Ändern des Anzeigenamens eines Zertifikats

Um die Verbindungsserver-Instanz oder den Sicherheitsserver für die Erkennung und Verwendung eines TLS-Zertifikats zu konfigurieren, müssen Sie den Anzeigenamen des Zertifikats in vdm ändern.

Voraussetzungen

Prüfen Sie, ob das Serverzertifikat in den Ordner **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** im Windows-Zertifikatspeicher importiert wurde. Siehe [Importieren eines signierten Serverzertifikats in einen Windows-Zertifikatspeicher](#).

Verfahren

- 1 Erweitern Sie im MMC-Fenster auf dem Windows Server-Host den Knoten **Zertifikate (Lokaler Computer)** und wählen Sie den Ordner **Persönlich > Zertifikate** aus.
- 2 Klicken Sie mit der rechten Maustaste auf das Zertifikat, das für den Horizon 7-Serverhost ausgestellt wurde, und klicken Sie auf **Eigenschaften**.
- 3 Löschen Sie auf der Registerkarte „Allgemein“ den Text **Anzeigename** und geben Sie **vdm** ein.
- 4 Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
- 5 Stellen Sie sicher, dass keine anderen Serverzertifikate im Ordner **Persönlich > Zertifikate** den Anzeigenamen **vdm** haben.
 - a Suchen Sie die anderen Serverzertifikate, klicken Sie mit der rechten Maustaste auf das Zertifikat und klicken Sie auf **Eigenschaften**.
 - b Wenn das Zertifikat den Anzeigenamen **vdm** hat, löschen Sie den Namen und klicken Sie auf **Anwenden** und danach auf **OK**.

Nächste Schritte

Importieren Sie das Stammzertifikat und die Zwischenzertifikate in den Zertifikatspeicher des lokalen Windows-Computers.

Nach dem Import aller Zertifikate aus der Kette müssen Sie den Verbindungsserver-Dienst oder den Sicherheitsserver-Dienst neu starten, damit die Änderungen wirksam werden.

Importieren der Stamm- und Zwischenzertifikate in einen Windows-Zertifikatspeicher

Sie müssen das Stammzertifikat und alle Zwischenzertifikate in der Zertifikatkette in den Zertifikatspeicher des lokalen Windows-Computers importieren.

Wenn das vom Zwischenserver importierte TLS-Serverzertifikat von einer bekannten und vom Verbindungsserver-Host als vertrauenswürdig eingestuften Zertifizierungsstelle importiert wurde, und Ihre Zertifikatketten keine Zwischenzertifikate enthalten, können Sie diese Aufgabe überspringen. Häufig verwendete Zertifizierungsstellen vertraut der Host im Allgemeinen.

Verfahren

- 1 Erweitern Sie an der MMC-Konsole auf dem Windows Server-Host den Knoten **Zertifikate (Lokaler Computer)** und wechseln Sie zum Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
 - Wenn Ihr Stammzertifikat sich in diesem Ordner befindet und Ihre Zertifikatkette keine Zwischenzertifikate enthält, fahren Sie mit Schritt 7 fort.
 - Wenn Ihr Stammzertifikat sich in diesem Ordner befindet und Ihre Zertifikatkette Zwischenzertifikate enthält, fahren Sie mit Schritt 6 fort.
 - Wenn Ihr Stammzertifikat sich nicht in diesem Ordner befindet, fahren Sie mit Schritt 2 fort.
- 2 Klicken Sie mit der rechten Maustaste auf den Ordner **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** und klicken Sie auf **Alle Aufgaben > Importieren**.
- 3 Klicken Sie im **Zertifikatsimport-Assistenten** auf **Weiter** und navigieren Sie zum Speicherort des Stamm-Zertifizierungsstellenzertifikats.
- 4 Wählen Sie die Datei mit dem Stamm-Zertifizierungsstellenzertifikat aus und klicken Sie auf **Öffnen**.
- 5 Klicken Sie auf **Weiter**, klicken Sie auf **Weiter** und klicken Sie auf **Fertig stellen**.
- 6 Wenn Ihr Serverzertifikat von einer Zwischenzertifizierungsstelle signiert wurde, importieren Sie alle Zwischenzertifikate in der Zertifikatskette in den Zertifikatspeicher des lokalen Windows-Computers.
 - a Navigieren Sie zum Ordner **Zertifikate (Lokaler Computer) > Zwischenzertifizierungsstellen > Zertifikate**.
 - b Wiederholen Sie die Schritte 3 bis 6 für jedes zu importierende Zwischenzertifikat.
- 7 Starten Sie den Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.
- 8 Wenn Sie HTML Access verwenden, starten Sie den VMware View Blast Secure Gateway-Dienst neu.

Einstellen externer URLs von Horizon 7 Server, sodass sie Clients auf verschiebende TLS-Server verweisen

Wenn TLS auf einen Zwischenserver verschoben wird und Horizon Client-Geräte den sicheren Tunnel nutzen, um sich mit Horizon 7 zu verbinden, müssen Sie die externe URL des sicheren Tunnels auf eine Adresse einstellen, die Clients verwenden können, um auf den Zwischenserver zuzugreifen.

Sie konfigurieren die externen URL-Einstellungen auf der Verbindungsserver-Instanz oder dem Sicherheitsserver, der eine Verbindung zum Zwischenserver herstellt.

Wenn Sie Sicherheitsserver bereitstellen, sind externe URLs für die Sicherheitsserver erforderlich, nicht jedoch für die Verbindungsserver-Instanzen, die mit den Sicherheitsservern gekoppelt werden.

Wenn Sie keine Sicherheitsserver bereitstellen oder über eine heterogene Netzwerkumgebung mit einigen Sicherheitsservern und einigen externen, vorgelagerten Verbindungsserver-Instanzen verfügen, sind externe URLs für alle Verbindungsserver-Instanzen notwendig, die eine Verbindung mit dem Zwischenserver herstellen.

Hinweis Sie können TLS-Verbindungen nicht über ein PCoIP Secure Gateway (PSG) oder Blast Secure Gateway auslagern. Die externe PCoIP-URL und die externe Blast Secure Gateway-URL müssen Clients ermöglichen, eine Verbindung zum Computer herzustellen, der das PSG und Blast Secure Gateway hostet. Setzen Sie die externe PCoIP-URL und die externe Blast-URL nicht zurück, um auf den Zwischenserver zu zeigen – es sei denn, um TLS-Verbindungen zwischen dem Zwischenserver und dem Horizon 7 Server herzustellen.

Festlegen der externen URLs für eine Verbindungsserver-Instanz

Sie können mit Horizon Administrator die externen URLs für eine Verbindungsserver-Instanz konfigurieren.

Voraussetzungen

- Stellen Sie sicher, dass die sicheren Tunnelverbindungen für die Verbindungsserver-Instanz aktiviert sind.

Verfahren

- 1 Klicken Sie in Horizon Administrator auf **View-Konfiguration > Server**.
- 2 Wählen Sie auf der Registerkarte „Verbindungsserver“ die Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 3 Geben Sie im Textfeld **Externe URL** die externe URL des sicheren Tunnels ein.

Die URL muss das Protokoll, den durch Clients auflösbaren Hostnamen und die Portnummer enthalten.

Beispiel: **https://myserver.example.com:443**

Hinweis Um auf eine Verbindungsserver-Instanz zuzugreifen, deren Hostname nicht aufgelöst werden kann, können Sie die IP-Adresse verwenden. Der Host, den Sie kontaktieren, passt jedoch nicht zu dem TLS-Zertifikat, das für die Verbindungsserver-Instanz konfiguriert ist. Dies führt dazu, dass der Zugriff blockiert wird oder weniger sicher ist.

- 4 Stellen Sie sicher, dass Clientsysteme mit allen Adressen in diesem Dialogfeld eine Verbindung mit dieser Verbindungsserver-Instanz herstellen können.
- 5 Klicken Sie auf **OK**.

Ändern der externen URLs für einen Sicherheitsserver

Mit Horizon Administrator können Sie die externen URLs für einen Sicherheitsserver ändern.

Voraussetzungen

- Stellen Sie sicher, dass die sicheren Tunnelverbindungen auf der mit diesem Sicherheitsserver kombinierten Verbindungsserver-Instanz aktiviert sind.

Verfahren

- 1 Wählen Sie in Horizon Administrator **View-Konfiguration > Server** aus.
- 2 Wählen Sie die Registerkarte „Sicherheitsserver“ aus, wählen Sie den Sicherheitsserver aus und klicken Sie auf **Bearbeiten**.
- 3 Geben Sie im Textfeld **Externe URL** die externe URL des sicheren Tunnels ein.

Die URL muss das Protokoll, den durch den Client auflösbaren Hostnamen des Sicherheitsservers sowie die Portnummer enthalten.

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

Hinweis Um auf einen Sicherheitsserver zuzugreifen, dessen Hostname nicht aufgelöst werden kann, können Sie die IP-Adresse verwenden. Der Host, mit dem Sie Verbindung aufnehmen, entspricht jedoch nicht dem für den Sicherheitsserver konfigurierten TLS-Zertifikat. Aus diesem Grund wird der Zugriff blockiert oder die Sicherheit des Zugriffs reduziert.

- 4 Stellen Sie sicher, dass Clientsysteme mit allen Adressen in diesem Dialogfeld eine Verbindung mit diesem Sicherheitsserverhost herstellen können.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Horizon Administrator sendet die aktualisierte externe URL an den Sicherheitsserver. Es ist kein Neustart des Sicherheitsserverdienstes erforderlich, damit die Änderungen wirksam werden.

Zulassen der HTTP-Verbindungen von Zwischenservern

Wenn TLS auf einen Zwischenserver verschoben wird, können Sie Verbindungsserver-Instanzen oder Sicherheitsserver so konfigurieren, dass HTTP-Verbindungen von Zwischengeräten mit Client-Verbindung zugelassen werden. Die Zwischengeräte müssen HTTPS für Horizon Client-Verbindungen akzeptieren.

Um HTTP-Verbindungen zwischen Horizon 7-Servern und Zwischengeräten zuzulassen, müssen Sie die Datei `locked.properties` auf jeder Verbindungsserver-Instanz und jedem Sicherheitsserver konfigurieren, auf denen HTTP-Verbindungen zugelassen sind.

Auch wenn HTTP-Verbindungen zwischen Horizon 7-Servern und Zwischengeräten zugelassen sind, können Sie TLS in Horizon 7 nicht deaktivieren. Die Horizon 7-Server nehmen weiterhin sowohl HTTPS- als auch HTTP-Verbindungen an.

Hinweis Wenn Ihre Horizon-Clients die Smartcard-Authentifizierung verwenden, müssen die Clients direkte HTTPS-Verbindungen zum Verbindungsserver bzw. zum Sicherheitsserver herstellen. Die Smartcard-Authentifizierung unterstützt das Verschieben von TLS nicht.

Verfahren

- 1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im TLS/SSL-Gatewaykonfigurationsordner auf dem Verbindungsserver- oder Sicherheitsserver-Host.

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

- 2 Um das Horizon 7-Serverprotokoll zu konfigurieren, fügen Sie die Eigenschaft `serverProtocol` hinzu, und legen Sie dafür den Wert `http` fest.

Der Wert `http` muss in Kleinbuchstaben eingegeben werden.

- 3 (Optional) Fügen Sie Eigenschaften hinzu, um einen nicht-standardmäßigen HTTP-Überwachungsport und eine Netzwerkschnittstelle auf dem Horizon 7-Server zu konfigurieren.
 - Um den HTTP-Überwachungsport von 80 zu ändern, legen Sie für `serverPortNonTLS` eine andere Portnummer fest, zu der das Zwischengerät per Konfiguration eine Verbindung herstellen soll.
 - Wenn der Horizon 7-Server über mehr als eine Netzwerkschnittstelle verfügt, der Server aber HTTP-Verbindungen nur an einer Schnittstelle überwachen soll, geben Sie für `serverHostNonTLS` die IP-Adresse dieser Netzwerkschnittstelle an.

- 4 Speichern Sie die Datei `locked.properties`.

- 5 Starten Sie den Verbindungsserver- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Beispiel: `locked.properties`, Datei

Diese Datei lässt Nicht-TLS-HTTP-Verbindungen zu einem Horizon 7-Server zu. Die IP-Adresse der Netzwerkschnittstelle mit Client-Verbindung des Horizon 7-Servers lautet 10.20.30.40. Der Server überwacht HTTP-Verbindungen an Standardport 80. Der Wert `http` muss in Kleinbuchstaben eingegeben werden.

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