

Horizon 7용 TLS 인증서 설정 시나리오

2020년 3월

VMware Horizon 7 7.12



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

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

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

Copyright © 2012-2020 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

Horizon 7용 TLS 인증서 설정 시나리오 4

1 인증 기관에서 TLS 인증서 가져오기 5

이 시나리오가 적용되는지 확인 5

올바른 인증서 유형 선택 6

인증서 서명 요청 생성 및 Microsoft Certreq를 통해 인증서 가져오기 7

CSR 구성 파일 생성 7

CSR 생성 및 CA에서 서명된 인증서 요청 9

CSR 및 해당 개인 키가 Windows 인증서 저장소에 저장되어 있는지 확인 10

Certreq를 사용하여 서명된 인증서 가져오기 11

Horizon 7 서버에 대해 가져온 인증서 설정 12

2 TLS 연결 부하를 중간 서버로 분산 14

TLS 부하 분산 서버의 인증서를 Horizon 7 서버로 가져오기 14

중간 서버에서 TLS 인증서 다운로드 15

중간 서버에서 개인 키 다운로드 16

인증서 파일을 PKCS#12 형식으로 변환 17

Windows 인증서 저장소에 서명된 서버 인증서 가져오기 18

인증서 대화명 수정 19

Windows 인증서 저장소에 루트 및 중간 인증서 가져오기 19

클라이언트가 TLS 부하 분산 서버를 가리키도록 Horizon 7 Server 외부 URL 설정 20

연결 서버 인스턴스의 외부 URL 설정 20

보안 서버의 외부 URL 수정 21

중간 서버의 HTTP 연결 허용 22

Horizon 7용 TLS 인증서 설정 시나리오

"Horizon 7용 TLS 인증서 설정 시나리오"에서는 Horizon 7 서버에서 사용할 수 있도록 TLS 인증서를 설정하는 예를 제공합니다. 첫 번째 시나리오에서는 인증 기관에서 서명된 TLS 인증서를 가져온 후 해당 인증서가 Horizon 7 서버에서 사용할 수 있는 형식인지 확인하는 방법을 보여 줍니다. 두 번째 시나리오는 중간 서버로 TLS 연결 부하를 분산하도록 Horizon 7 서버를 구성하는 방법을 보여 줍니다.

대상

이 정보는 Horizon 7을 설치하려고 하며 Horizon 7 서버에서 사용되는 TLS 인증서를 가져와야 하는 사용자 또는 중간 서버를 사용하여 Horizon 7에 대한 TLS 연결 부하를 분산하는 모든 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영에 익숙하고 경험 많은 Windows 또는 Linux 시스템 관리자를 대상으로 작성되었습니다.

인증 기관에서 TLS 인증서 가져오기

1

VMware에서는 Horizon 연결 서버 인스턴스, 보안 서버 및 View Composer 인스턴스에서 사용할 수 있도록 유효한 인증 기관(CA)에서 서명한 TLS 인증서를 구성하는 것을 권장합니다.

연결 서버, 보안 서버 또는 View Composer 인스턴스를 설치할 때 기본 TLS 인증서가 생성됩니다. 테스트를 위해서는 자체 서명된 기본 인증서를 사용할 수 있지만 가능한 한 빨리 교체하십시오. 기본 인증서는 CA에서 서명되지 않습니다. CA에서 서명하지 않은 인증서를 사용하여 신뢰할 수 없는 사용자가 서버로 가장하여 트래픽을 인터셉트할 수 있습니다.

또한 Horizon 7 환경에서는 vCenter Server와 함께 설치된 기본 인증서를 CA에서 서명한 인증서로 교체해야 합니다. openTLS을 사용하여 vCenter Server에 대해 이 작업을 수행할 수 있습니다. 자세한 내용은 VMware Technical Papers 사이트 <http://www.vmware.com/resources/techresources/>에서 "vCenter Server 인증서 교체"를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 이 시나리오가 적용되는지 확인
- 올바른 인증서 유형 선택
- 인증서 서명 요청 생성 및 Microsoft Certreq를 통해 인증서 가져오기

이 시나리오가 적용되는지 확인

Horizon 7 서버 호스트의 Windows 로컬 컴퓨터 인증서 저장소에 인증서를 가져와 Horizon 7에 대한 인증서를 구성합니다.

인증서를 가져오려면 먼저 CSR(인증서 서명 요청)을 생성하고 CA에서 서명된 유효한 인증서를 가져와야 합니다. 이 시나리오에서 설명하는 예제 절차에 따라 CSR이 생성되지 않는 경우 결과 인증서 및 해당 개인 키를 PKCS#12(이전의 PFX) 형식 파일에서 사용할 수 있어야 합니다.

여러 가지 방법으로 CA에서 TLS 인증서를 가져올 수 있습니다. 이 시나리오에서는 Microsoft certreq 유틸리티를 사용하여 CSR을 생성하고 Horizon 7 서버에서 해당 인증서를 사용할 수 있도록 하는 방법을 보여 줍니다. 필요한 도구에 익숙하며 이러한 도구가 서버에 설치되어 있으면 다른 방법을 사용해도 됩니다.

다음과 같은 문제를 해결하려면 이 시나리오를 사용합니다.

- CA에서 서명한 TLS 인증서가 없고 획득하는 방법을 모르는 경우

■ 서명된 유효한 TLS 인증서가 있지만 PKCS#12(PFX) 형식이 아닌 경우

조직에서 CA가 서명한 TLS 인증서를 제공하면 이러한 인증서를 사용할 수 있습니다. 조직에서는 유효한 내부 CA 또는 타사 상용 CA를 사용할 수 있습니다. 인증서가 PKCS#12 형식이 아니면 변환해야 합니다.

인증서 파일을 PKCS#12 형식으로 변환의 내용을 참조하십시오.

서명된 인증서가 적절한 형식인 경우 Windows 인증서 저장소로 가져오고 해당 인증서를 사용하도록 Horizon 7 서버를 구성할 수 있습니다. [Horizon 7 서버에 대해 가져온 인증서 설정](#)의 내용을 참조하십시오.

올바른 인증서 유형 선택

Horizon 7에서 다양한 유형의 TLS 인증서를 사용할 수 있습니다. 배포에 적합한 인증서 유형을 선택하는 것이 중요합니다. 인증서를 사용할 수 있는 서버의 수에 따라 인증서 유형의 비용이 다릅니다.

선택한 유형이 무엇이든 인증서에 FQDN(정규화된 도메인 이름)을 사용하여 VMware 보안 권장 사항에 따릅니다. 내부 도메인에서의 통신에도 단순한 서버 이름이나 IP 주소를 사용하지 마십시오.

단일 서버 이름 인증서

특정 서버의 대상 이름이 있는 인증서를 생성할 수 있습니다. 예: dept.company.com.

예를 들어 이러한 유형의 인증서는 하나의 연결 서버 인스턴스에만 인증서가 필요한 경우에 유용합니다.

CA에 인증서 서명 요청을 제출할 때 인증서와 연결되는 서버 이름을 제공합니다. Horizon 7 서버에서 인증서에 연결된 이름과 일치하도록 제공된 서버 이름을 확인할 수 있어야 합니다.

제목 대체 이름

SAN(제목 대체 이름)은 인증서를 발급할 때 추가할 수 있는 특성입니다. 이 특성을 사용하여 인증서에서 두 개 이상의 서버를 유효성 검사할 수 있도록 대상 이름(URL)을 추가할 수 있습니다.

예를 들어 dept.company.com 호스트 이름을 갖는 서버에 대해 인증서가 발급될 수 있습니다. 보안 서버를 통해 Horizon 7에 연결하는 외부 사용자가 해당 인증서를 사용하도록 하려고 합니다. 이 인증서가 발급되기 전에 SAN dept.int.company.com을 인증서에 추가하여 터널링이 사용되도록 설정될 때 해당 인증서가 로드 밸런서 뒤에 있는 연결 서버 인스턴스 또는 보안 서버에서 사용되도록 허용할 수 있습니다.

와일드카드 인증서

와일드카드 인증서는 여러 서비스에서 사용할 수 있도록 생성됩니다. 예: *.company.com.

여러 서버에 인증서가 필요한 경우에는 와일드카드 인증서가 유용합니다. Horizon 7 외에도 환경에 있는 다른 애플리케이션에 TLS 인증서가 필요한 경우에는 해당 서버에도 와일드카드 인증서를 사용할 수 있습니다. 그러나 다른 서비스에서 공유되는 와일드카드 인증서를 사용하는 경우 이러한 다른 서비스의 보안도 VMware Horizon 제품 보안에 영향을 미칩니다.

참고 와일드카드 인증서는 단일 도메인 수준에만 사용할 수 있습니다. 예를 들어, 대상 이름이 *.company.com인 와일드카드 인증서는 하위 도메인 dept.company.com에서 사용할 수 있지만 dept.it.company.com에서는 사용할 수 없습니다.

인증서 서명 요청 생성 및 Microsoft Certreq를 통해 인증서 가져오기

인증서를 Horizon 7 서버에서 사용할 수 있게 하려면 구성 파일을 생성하고, 구성 파일에서 CSR(인증서 서명 요청)을 생성하고, CA로 서명 요청을 보내야 합니다. CA에서 인증서를 반환하는 경우 서명된 인증서를 Horizon 7 서버 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다. 여기에서 이전에 생성한 개인 키에 연결됩니다.

CSR은 인증서 자체가 생성되는 방식에 따라 여러 방법으로 생성될 수 있습니다.

Microsoft certreq 유틸리티는 Windows Server 2008 R2에서 사용할 수 있으며 CSR을 생성하고 서명된 인증서를 가져오는 데 사용할 수 있습니다. 타사 CA로 요청을 보내려는 경우 certreq를 사용하는 것이 Horizon 7에 대한 인증서를 가져오는 가장 빠르고 간단한 방법입니다.

절차

1 CSR 구성 파일 생성

Microsoft certreq 유틸리티는 구성 파일을 사용하여 CSR을 생성합니다. 요청을 생성하려면 먼저 구성 파일을 생성해야 합니다. 파일을 생성하고 인증서를 사용하는 Horizon 7 서버를 호스팅하는 Windows Server 컴퓨터에서 CSR을 생성합니다.

2 CSR 생성 및 CA에서 서명된 인증서 요청

완료된 구성 파일을 사용하여 certreq 유틸리티를 통해 CSR을 생성할 수 있습니다. 서명된 인증서를 반환하는 타사 CA로 요청을 전송합니다.

3 CSR 및 해당 개인 키가 Windows 인증서 저장소에 저장되어 있는지 확인

certreq 유틸리티를 사용하여 CSR을 생성하는 경우 이 유틸리티는 관련된 개인 키도 생성합니다. 이 유틸리티는 CSR을 생성한 컴퓨터의 Windows 로컬 컴퓨터 인증서 저장소에 CSR 및 개인 키를 저장합니다. MMC(Microsoft Management Console) 인증서 스냅인을 사용하여 CSR 및 개인 키가 제대로 저장되어 있는지 확인할 수 있습니다.

4 Certreq를 사용하여 서명된 인증서 가져오기

CA에서 서명된 인증서가 있는 경우 인증서를 Horizon 7 서버 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 가져올 수 있습니다.

5 Horizon 7 서버에 대해 가져온 인증서 설정

서버 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져온 후에 Horizon 7 서버가 해당 인증서를 사용하도록 허용하려면 추가 단계를 수행해야 합니다.

CSR 구성 파일 생성

Microsoft certreq 유틸리티는 구성 파일을 사용하여 CSR을 생성합니다. 요청을 생성하려면 먼저 구성 파일을 생성해야 합니다. 파일을 생성하고 인증서를 사용하는 Horizon 7 서버를 호스팅하는 Windows Server 컴퓨터에서 CSR을 생성합니다.

사전 요구 사항

구성 파일에 입력해야 하는 정보를 수집합니다. 대상 이름을 완성하려면 Horizon 7 서버의 FQDN과 조직 구성 단위, 조직, 구/군/시, 시/도 및 국가를 알고 있어야 합니다.

절차

- 1 텍스트 편집기를 열고 다음 텍스트를 시작 태그 및 끝 태그를 포함하여 파일에 붙여넣습니다.

```
;----- 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

;-----
```

이 텍스트를 복사한 후 붙여 넣을 때 추가 CR/LF 문자가 Subject = 줄에 추가될 경우 해당 CR/LF 문자를 삭제하십시오.

- 2 Subject 특성을 Horizon 7 서버 및 배포에 대한 적절한 값으로 업데이트합니다.

예: CN=dept.company.com

VMware 보안 권장 사항을 준수하기 위해 클라이언트 디바이스가 호스트에 연결하는 데 사용하는 FQDN(정규화된 도메인 이름)을 사용하십시오. 내부 도메인에서의 통신에도 단순한 서버 이름이나 IP 주소를 사용하지 마십시오.

일부 CA는 state 특성에 대해 약어를 사용하도록 허용하지 않습니다.

3 (선택 사항) KeyLength 특성을 업데이트합니다.

다른 KeyLength 크기가 명시적으로 필요하지 않으면 기본값 2048이 적절합니다. 많은 수의 CA에서 최소값 2048을 요구합니다. 키 크기가 클수록 더 안전하지만 성능에 더 많은 영향을 미칩니다.

컴퓨터가 계속해서 더 강력해지고 더 강력한 암호를 해독할 수 있게 되면서 NIST(National Institute of Standards and Technology)에서는 1024의 키 크기를 권장하지 않지만 1024의 KeyLength도 여전히 지원됩니다.

중요 1024 미만의 KeyLength 값은 생성하지 마십시오. Windows용 Horizon Client는 1024 미만의 KeyLength로 생성된 Horizon 7서버의 인증서 유효성을 검사하지 않으며 Horizon Client 디바이스는 Horizon 7에 연결되지 않습니다. 연결 서버에서 수행하는 인증서 유효성 검사도 실패하므로 영향을 받는 Horizon 7 서버가 Horizon Administrator 대시보드에 빨간색으로 나타납니다.

4 파일을 request.inf로 저장합니다.

다음에 수행할 작업

구성 파일에서 CSR을 생성합니다.

CSR 생성 및 CA에서 서명된 인증서 요청

완료된 구성 파일을 사용하여 certreq 유틸리티를 통해 CSR을 생성할 수 있습니다. 서명된 인증서를 반환하는 타사 CA로 요청을 전송합니다.

사전 요구 사항

- CSR 구성 파일을 완료했는지 확인합니다. [CSR 구성 파일 생성](#)의 내용을 참조하십시오.
- CSR 구성 파일이 있는 컴퓨터에서 이 절차에 설명된 certreq 작업을 수행합니다.

절차

1 시작 메뉴에서 **명령 프롬프트**를 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택하여 명령 프롬프트를 엽니다.

2 Request.inf 파일을 저장한 디렉토리로 이동합니다.

예: `cd c:\certificates`

3 CSR 파일을 생성합니다.

예: `certreq -new request.inf certreq.txt`

4 CSR 파일의 콘텐츠를 사용하여 CA의 등록 프로세스에 따라 CA에 인증서 요청을 제출합니다.

- a CA에 요청을 제출하면 CA에서는 인증서를 설치할 서버의 유형을 선택하라는 메시지를 표시합니다. Horizon 7에서는 Microsoft 인증서 MMC를 사용하여 인증서를 관리하므로 Microsoft, Microsoft IIS 7 또는 이와 유사한 서버 유형에 대한 인증서를 선택합니다. CA는 Horizon 7에서 사용하기 위한 형식으로 인증서를 생성해야 합니다.
- b 단일 서버 이름 인증서를 요청하는 경우 Horizon Client 디바이스가 이 Horizon 7 서버에 대한 IP 주소로 확인할 수 있는 이름을 사용합니다. 컴퓨터가 Horizon 7 서버에 연결하는 데 사용하는 이름은 인증서와 연결된 이름과 일치해야 합니다.

참고 CA에서는 CSR 파일(예: certreq.txt)의 콘텐츠를 복사한 후 웹 양식으로 붙여 넣도록 요구할 수 있습니다. 텍스트 편집기를 사용하여 CSR 파일의 콘텐츠를 복사할 수 있습니다. 시작 및 끝 태그를 포함해야 합니다. 예:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID2jCCAsICAQAwazEWMBQGA1UEBhMNVW5pdGVkIFN0YXRlc2ELMAkGA1UECawC
Q0ExEjAQBgNVBACMCVBhBg8gQWx0bzEKMAgGA1UECgwBTzELMAkGA1UECwwCT1Ux
FzAVBgNVBAMDM15LmNvbXBhbnkuY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
. . .
. . .
L9nPYX76jeu5rwQfXLivSCea6nZiIOZYw8Dbn8dgwAqpJdzBbrwuM1TuSnx6bAK8
S52Tv0Gxw58jUTtxFV+Roz8TE8wZDFB51jx+FmLs
-----END NEW CERTIFICATE REQUEST-----
```

CA에서는 귀사에 대해 몇 가지 검사를 수행한 후 CSR의 정보를 기준으로 서버 인증서를 생성하고, 해당 개인 키로 서명한 후 인증서를 귀하에게 보냅니다.

또한 CA는 루트 CA 인증서를 보내며 해당되는 경우 중간 CA 인증서도 보냅니다.

5 인증서 텍스트 파일의 이름을 cert.cer로 바꿉니다.

파일이 인증서 요청이 생성된 Horizon 7 서버에 있는지 확인합니다.

6 루트 CA 및 중간 CA 인증서 파일의 이름을 root.cer 및 intermediate.cer로 바꿉니다.

파일이 인증서 요청이 생성된 Horizon 7 서버에 있는지 확인합니다.

참고 certreq 유틸리티를 사용하여 Windows 로컬 컴퓨터 인증서 저장소에 이러한 인증서를 가져올 경우에는 인증서가 PKCS#12(PFX) 형식일 필요는 없습니다. 인증서 가져오기 마법사를 사용하여 Windows 인증서 저장소에 인증서를 가져올 경우에는 PKCS#12(PFX) 형식이 요구됩니다.

다음에 수행할 작업

CSR 파일 및 해당 개인 키가 Windows 로컬 컴퓨터 인증서 저장소에 저장되었는지 확인합니다.

CSR 및 해당 개인 키가 Windows 인증서 저장소에 저장되어 있는지 확인

certreq 유틸리티를 사용하여 CSR을 생성하는 경우 이 유틸리티는 관련된 개인 키도 생성합니다. 이 유틸리티는 CSR을 생성한 컴퓨터의 Windows 로컬 컴퓨터 인증서 저장소에 CSR 및 개인 키를 저장합니다.

MMC(Microsoft Management Console) 인증서 스냅인을 사용하여 CSR 및 개인 키가 제대로 저장되어 있는지 확인할 수 있습니다.

Horizon 7 서버에서 인증서를 제대로 가져오고 사용할 수 있도록 하려면 나중에 개인 키를 서명된 인증서에 가입해야 합니다.

사전 요구 사항

- **certreq** 유틸리티를 사용하여 CSR을 생성하고 CA에서 서명된 인증서를 요청했는지 확인합니다. [CSR 생성 및 CA에서 서명된 인증서 요청](#)의 내용을 참조하십시오.
- MMC(Microsoft Management Console)에 인증서 스냅인을 추가하는 절차를 숙지합니다. "Horizon 7 설치" 문서의 "Horizon 7 Server를 위한 TLS 인증서 구성" 장에서 "MMC에 인증서 스냅인 추가"를 참조하십시오.

절차

- 1 Windows Server 컴퓨터에서 MMC에 인증서 스냅인을 추가합니다.
- 2 Windows Server 컴퓨터의 MMC 창에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **인증서 등록 요청** 폴더를 선택합니다.
- 3 **인증서 등록 요청** 폴더를 확장하고 **인증서** 폴더를 선택합니다.
- 4 인증서 항목이 **인증서** 폴더에 표시되는지 확인합니다.
발급 대상 및 **발급자** 필드에는 CSR을 생성하는 데 사용된 `request.inf` 파일의 **subject:CN** 필드에 입력한 도메인 이름이 표시되어야 합니다.
- 5 다음 단계 중 하나를 수행하여 인증서에 개인 키가 포함되어 있는지 확인합니다.
 - 인증서 아이콘에 노란색 키가 나타나는지 확인합니다.
 - 인증서를 두 번 클릭하고 인증서 정보 대화 상자에 사용자가 이 인증서와 일치하는 개인 키를 갖고 있습니다. 라는 문구가 표시되는지 확인합니다.

다음에 수행할 작업

Windows 로컬 컴퓨터 인증서 저장소로 인증서를 가져옵니다.

Certreq를 사용하여 서명된 인증서 가져오기

CA에서 서명된 인증서가 있는 경우 인증서를 Horizon 7 서버 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 가져올 수 있습니다.

certreq 유틸리티를 사용하여 CSR을 생성한 경우 인증서 개인 키가 CSR을 생성한 서버에 대해 로컬입니다. 제대로 작동하려면 인증서가 개인 키와 결합되어야 합니다. 이 절차에 나오는 **certreq** 명령을 사용하여 인증서 및 개인 키가 제대로 결합되어 있는지와 Windows 인증서 저장소로 가져왔는지 확인합니다.

다른 방법을 사용하여 CA에서 서명된 인증서를 가져오는 경우 MMC(Microsoft Management Console) 스냅인의 인증서 가져오기 마법사를 사용하여 인증서를 Windows 인증서 저장소로 가져올 수 있습니다. 이 방법은 "Horizon 7 설치" 문서의 "Horizon 7 Server를 위한 TLS 인증서 구성"에 설명되어 있습니다.

사전 요구 사항

- CA에서 서명된 인증서를 받았는지 확인합니다. [CSR 생성 및 CA에서 서명된 인증서 요청](#)의 내용을 참조하십시오.
- CSR을 생성하고 서명된 인증서를 저장한 컴퓨터에서 이 절차에 설명된 **certreq** 작업을 수행합니다.

절차

1 시작 메뉴에서 **명령 프롬프트**를 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택하여 명령 프롬프트를 엽니다.

2 **cert.cer**과 같은 서명된 인증서 파일을 저장한 디렉토리로 이동합니다.

예: **cd c:\certificates**

3 **certreq -accept** 명령을 실행하여 서명된 인증서를 가져옵니다.

예: **certreq -accept cert.cer**

결과

인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져옵니다.

다음에 수행할 작업

가져온 인증서를 Horizon 7 서버에서 사용할 수 있게 구성합니다. [Horizon 7 서버에 대해 가져온 인증서 설정](#)의 내용을 참조하십시오.

Horizon 7 서버에 대해 가져온 인증서 설정

서버 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져온 후에 Horizon 7 서버가 해당 인증서를 사용하도록 허용하려면 추가 단계를 수행해야 합니다.

절차

1 서버 인증서를 성공적으로 가져왔는지 확인합니다.

2 인증서 표시 이름을 **vdm**으로 변경합니다.

vdm은 소문자여야 합니다. 표시 이름이 **vdm**인 다른 인증서의 이름을 바꾸거나 해당 인증서에서 표시 이름을 제거해야 합니다.

View Composer에서 사용하는 인증서의 표시 이름을 수정할 필요가 없습니다.

3 Windows 인증서 저장소에 루트 CA 인증서 및 중간 CA 인증서를 설치합니다.

4 연결 서버 서비스, 보안 서버 서비스 또는 View Composer 서비스가 새 인증서를 사용해서 시작되도록 하려면 이러한 서비스를 다시 시작합니다.

5 HTML Access를 사용하는 경우 VMware View Blast Secure Gateway 서비스를 다시 시작합니다.

6 View Composer Server에서 인증서를 설정하는 경우 또 다른 단계를 수행해야 할 수 있습니다.

- View Composer를 설치한 후 새 인증서를 설정하는 경우 **SviConfig ReplaceCertificate** 유틸리티를 실행하여 View Composer가 사용하는 포트에 바인딩되는 인증서를 대체해야 합니다.
- View Composer를 설치하기 전에 새 인증서를 설정하는 경우 **SviConfig ReplaceCertificate** 유틸리티를 실행할 필요가 없습니다. View Composer 설치 관리자를 실행하는 경우, 자체 서명된 기본 인증서 대신 CA에서 서명한 새 인증서를 선택할 수 있습니다.

자세한 내용은 "Horizon 7 설치" 문서에서 "View Composer가 사용하는 포트에 새 TLS 인증서 바인딩"을 참조하십시오.

결과

이 절차의 작업을 수행하려면 다음 항목을 참조하십시오.

- [인증서 대화명 수정](#)
- [Windows 인증서 저장소에 루트 및 중간 인증서 가져오기](#)

자세한 내용은 "Horizon 7 설치" 문서에서 "새로운 TLS 인증서를 사용하도록 연결 서버, 보안 서버 또는 View Composer 구성"을 참조하십시오.

참고 이미 **certreq** 유틸리티를 사용하여 서버 인증서를 가져왔으므로 "Horizon 7 설치" 항목 "Windows 인증서 저장소에 서명된 서버 인증서 가져오기"가 여기에는 나열되지 않습니다. 서버 인증서를 다시 가져올 때는 MMC 스냅인의 인증서 가져오기 마법사를 사용하지 않도록 합니다.

하지만 인증서 가져오기 마법사를 사용하여 루트 CA 인증서 및 중간 CA 인증서를 Windows 인증서 저장소로 가져올 수 있습니다.

TLS 연결 부하를 중간 서버로 분산

2

Horizon 7 서버와 Horizon Client 디바이스 간의 중간 서버가 로드 밸런싱 및 TLS 연결 부하 분산 같은 작업을 수행하도록 설정할 수 있습니다. Horizon Client 디바이스는 HTTPS를 통해 중간 서버에 연결되며 중간 서버는 외부에 연결되는 연결 서버 인스턴스 또는 보안 서버로 연결을 전달합니다.

TLS 연결 부하를 중간 서버로 분산하려면 다음 몇 가지 주요 작업을 완료해야 합니다.

- 중간 서버에서 사용되는 TLS 인증서를 외부 연결 Horizon 7 서버로 가져옵니다.
- 외부 연결 Horizon 7 서버의 외부 URL이 클라이언트가 중간 서버에 연결하는 데 사용할 수 있는 URL과 일치하도록 설정합니다.
- 중간 서버와 Horizon 7 서버 간의 HTTP 연결을 허용합니다.

본 장은 다음 항목을 포함합니다.

- TLS 부하 분산 서버의 인증서를 Horizon 7 서버로 가져오기
- 클라이언트가 TLS 부하 분산 서버를 가리키도록 Horizon 7 Server 외부 URL 설정
- 중간 서버의 HTTP 연결 허용

TLS 부하 분산 서버의 인증서를 Horizon 7 서버로 가져오기

TLS 연결 부하를 중간 서버로 분산하는 경우에는 중간 서버에 연결하는 연결 서버 인스턴스 또는 보안 서버로 중간 서버의 인증서를 가져와야 합니다. 부하 분산 중간 서버와 해당 중간 서버에 연결하는 부하가 분산된 각 Horizon 7 서버에는 동일한 TLS 서버 인증서가 있어야 합니다.

보안 서버를 배포하는 경우에는 중간 서버와 해당 중간 서버에 연결하는 보안 서버에 동일한 TLS 인증서가 있어야 합니다. 보안 서버에 연결되고 중간 서버에 직접 연결하지 않는 연결 서버 인스턴스에는 동일한 TLS 인증서를 설치하지 않아도 됩니다.

보안 서버를 배포하지 않는 경우나 보안 서버와 외부에 연결되는 연결 서버 인스턴스가 혼합되어 있는 네트워크 환경을 사용하는 경우에는 중간 서버와 해당 중간 서버에 연결하는 모든 연결 서버 인스턴스에 동일한 TLS 인증서가 있어야 합니다.

중간 서버의 인증서가 연결 서버 인스턴스나 보안 서버에 설치되어 있지 않으면 클라이언트가 Horizon 7에 대한 연결의 유효성을 검사할 수 없습니다. 이 경우에는 Horizon 7 서버에서 전송한 인증서 지문이 Horizon Client가 연결하는 중간 서버의 인증서와 일치하지 않습니다.

로드 밸런싱과 TLS 부하 분산을 혼동하지 마십시오. 위의 요건은 몇몇 유형의 로드 밸런서를 포함해 TLS 부하 분산을 제공하도록 구성된 디바이스에 적용됩니다. 그러나 순수 로드 밸런싱에는 디바이스 간 인증서 복사가 필요하지 않습니다.

중요 다음 항목에서 설명하는 시나리오에서는 타사 구성 요소와 VMware 구성 요소 간에 TLS 인증서를 공유하는 한 가지 방법에 대해 설명합니다. 이 방법은 모든 사용자에게 적합한 방법이 아니며, 작업을 수행하는 여러 가지 방법 중 한 가지일 뿐입니다.

절차

1 중간 서버에서 TLS 인증서 다운로드

외부 연결 Horizon 7 서버로 가져올 수 있도록 중간 서버에 설치된 CA 서명 TLS 인증서를 다운로드해야 합니다.

2 중간 서버에서 개인 키 다운로드

중간 서버에서 TLS 인증서와 연결된 개인 키를 다운로드해야 합니다. 개인 키는 인증서와 함께 Horizon 7 서버로 가져와야 합니다.

3 인증서 파일을 PKCS#12 형식으로 변환

인증서 및 해당 개인 키를 PEM 또는 다른 형식으로 가져온 경우 Horizon 7 서버의 Windows 인증서 저장소에 인증서를 가져오려면 먼저 PKCS#12(PFX) 형식으로 변환해야 합니다. Windows 인증서 저장소에서 인증서 가져오기 마법사를 사용하는 경우 PKCS#12(PFX) 형식이 필요합니다.

4 Windows 인증서 저장소에 서명된 서버 인증서 가져오기

TLS 서버 인증서를 연결 서버 인스턴스 또는 보안 서버 서비스가 설치된 Windows Server 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다.

5 인증서 대화명 수정

TLS 인증서를 인식하고 사용하도록 연결 서버 인스턴스 또는 보안 서버를 구성하려면 인증서 대화명을 vdm으로 수정해야 합니다.

6 Windows 인증서 저장소에 루트 및 중간 인증서 가져오기

인증서 체인의 루트 인증서 및 모든 중간 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다.

중간 서버에서 TLS 인증서 다운로드

외부 연결 Horizon 7 서버로 가져올 수 있도록 중간 서버에 설치된 CA 서명 TLS 인증서를 다운로드해야 합니다.

절차

1 중간 서버에 연결하고 HTTPS 요청을 전송하는 클라이언트에 제공된 TLS 인증서를 찾습니다.

2 Horizon 7에 사용되는 TLS 인증서를 찾아서 다운로드합니다.

예제: F5 BIG-IP LTM 시스템에서 TLS 인증서 다운로드

이 예에서는 F5 BIG-IP LTM(Local Traffic Manager)을 중간 서버로 사용합니다. 이 예는 자체 중간 서버에서 인증서를 다운로드하는 방법에 대한 일반적인 이해를 돕기 위해 제공됩니다.

중요 이러한 단계는 F5 BIG-IP LTM에만 해당되며 새로운 릴리스 또는 기타 F5 제품에는 적용되지 않을 수 있습니다. 해당 단계는 다른 벤더의 중간 서버에 적용되지 않습니다.

시작하기 전에 F5 BIG-IP LTM 시스템이 Horizon 7에 배포되었는지 확인합니다. <http://www.f5.com/pdf/deployment-guides/f5-vmware-view-dg.pdf>에 있는 F5 배포 가이드 "VMware View에서 BIG-IP LTM 시스템 배포"에서 작업을 완료했는지 확인하십시오.

- 1 F5 BIG-IP LTM 구성 유틸리티에 연결합니다.
- 2 탐색 창의 [기본] 탭에서 **로컬 트래픽**을 확장하고 **SSL 인증서**를 클릭합니다.
이 유틸리티는 시스템에 설치된 인증서 목록을 표시합니다.
- 3 [이름] 열에서 Horizon 7에 사용되는 인증서의 이름을 클릭합니다.
- 4 화면 하단의 **내보내기**를 클릭합니다.
이 유틸리티는 **인증서 텍스트** 상자에 기존 TLS 인증서를 표시합니다.
- 5 **인증서 파일** 설정에서 **file_name 다운로드**를 클릭합니다.
TLS 인증서가 CRT 파일로 다운로드됩니다.

중간 서버에서 개인 키 다운로드

중간 서버에서 TLS 인증서와 연결된 개인 키를 다운로드해야 합니다. 개인 키는 인증서와 함께 Horizon 7 서버로 가져와야 합니다.

절차

- 1 중간 서버에 연결하고 HTTPS 요청을 전송하는 클라이언트에 제공된 TLS 인증서를 찾습니다.
- 2 Horizon 7에 사용되는 인증서를 찾고 해당 개인 키를 다운로드합니다.

예제: F5 BIG-IP LTM 시스템에서 개인 키 다운로드

이 예에서는 F5 BIG-IP LTM(Local Traffic Manager)을 중간 서버로 사용합니다. 이 예는 자체 중간 서버에서 개인 키를 다운로드하는 방법에 대한 일반적인 이해를 돕기 위해 제공됩니다.

중요 이러한 단계는 F5 BIG-IP LTM에만 해당되며 새로운 릴리스 또는 기타 F5 제품에는 적용되지 않을 수 있습니다. 해당 단계는 다른 벤더의 중간 서버에 적용되지 않습니다.

시작하기 전에 F5 BIG-IP LTM 구성 유틸리티에 연결되어 있는지 확인합니다.

- 1 탐색 창의 [기본] 탭에서 **로컬 트래픽**을 확장하고 **SSL 인증서**를 클릭합니다.
이 유틸리티는 시스템에 설치된 인증서 목록을 표시합니다.
- 2 [이름] 열에서 Horizon 7에 사용되는 인증서의 이름을 클릭합니다.

3 메뉴 표시줄에서 **키**를 클릭합니다.

4 화면 하단의 **내보내기**를 클릭합니다.

이 유틸리티는 **키 텍스트** 상자에 기존의 개인 키를 표시합니다.

5 키 파일 설정에서 **file_name 다운로드**를 클릭합니다.

개인 키가 **KEY** 파일로 다운로드됩니다.

인증서 파일을 PKCS#12 형식으로 변환

인증서 및 해당 개인 키를 PEM 또는 다른 형식으로 가져온 경우 Horizon 7 서버의 Windows 인증서 저장소로 인증서를 가져오려면 먼저 PKCS#12(PFX) 형식으로 변환해야 합니다. Windows 인증서 저장소에서 인증서 가져오기 마법사를 사용하는 경우 PKCS#12(PFX) 형식이 필요합니다.

다음 방법 중 하나로 인증서 파일을 가져올 수 있습니다.

- CA에서 인증서 Keystore 파일을 가져옵니다.
- Horizon 7 배포 시 설정된 중간 서버에서 인증서 및 개인 키를 다운로드합니다.
- 조직에서 인증서 파일을 제공합니다.

인증서 파일은 다양한 형식으로 제공됩니다. 예를 들어, PEM 형식은 Linux 환경에서 자주 사용됩니다. 다음 확장명의 인증서 파일, 키 파일 및 CSR 파일이 포함될 수 있습니다.

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

CRT 파일은 CA에 의해 반환된 SSL 인증서를 포함합니다. CSR 파일은 원본 인증서 서명 요청 파일이며 필요하지 않습니다. 키 파일은 개인 키를 포함합니다.

사전 요구 사항

- 시스템에 OpenSSL이 설치되어 있는지 확인합니다. openssl은 <http://www.openssl.org>에서 다운로드할 수 있습니다.
- 또한 CA에 의해 반환된 SSL 인증서의 루트 인증서를 시스템에서 사용할 수 있는지 확인합니다.

절차

1 CRT 및 키 파일을 OpenSSL 설치 디렉토리로 복사합니다.

예: `cd c:\OpenSSL-Win32\bin`

2 Windows 명령 프롬프트를 열고, 필요한 경우 OpenSSL 설치 디렉토리로 이동합니다.

3 인증서 파일 및 개인 키에서 PKCS#12(PFX) Keystore 파일을 생성합니다.

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

이 예에서 CACert.crt는 인증 기관에 의해 반환된 루트 인증서의 이름입니다.

또한 Windows 인증서 저장소는 PFX 확장명으로 생성된 Keystore를 수락합니다. 예: `-out server.pfx`

- 4 PKCS#12 (PFX) 파일을 보호하기 위한 내보내기 암호를 입력합니다.

Windows 인증서 저장소에 서명된 서버 인증서 가져오기

TLS 서버 인증서를 연결 서버 인스턴스 또는 보안 서버 서비스가 설치된 Windows Server 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다.

이 시나리오에서는 PKCS#12(PFX) 형식의 인증서 파일을 사용합니다.

인증서 파일 형식에 따라 keystore 파일에 포함된 전체 인증서 체인을 Windows 로컬 컴퓨터 인증서 저장소로 가져올 수 있습니다. 예를 들어, 서버 인증서, 중간 인증서 및 루트 인증서를 가져올 수 있습니다.

다른 유형의 인증서 파일의 경우 서버 인증서만 Windows 로컬 컴퓨터 인증서 저장소로 가져옵니다. 이 경우 별도의 단계를 거쳐 인증서 체인에 있는 루트 인증서와 중간 인증서를 가져와야 합니다.

인증서에 대한 자세한 내용은 Microsoft 온라인 도움말의 MMC에 인증서 스냅인 추가를 참조하십시오.

사전 요구 사항

TLS 서버 인증서가 PKCS@12(PFX) 형식인지 확인하십시오. 인증서 파일을 PKCS#12 형식으로 변환의 내용을 참조하십시오.

절차

- 1 Windows Server 호스트의 MMC 창에서 인증서(로컬 컴퓨터) 노드를 확장하고 개인 폴더를 선택합니다.
- 2 [작업] 창에서 추가 작업 > 모든 작업 > 가져오기로 이동합니다.
- 3 인증서 가져오기 마법사에서 다음을 클릭하고 인증서가 저장된 위치를 찾습니다.
- 4 인증서 파일을 선택하고 열기를 클릭합니다.
인증서 파일 유형을 표시하려면 파일 이름 드롭다운 메뉴에서 해당 파일 형식을 선택하십시오.
- 5 인증서 파일에 포함된 개인 키 암호를 입력합니다.
- 6 이 키를 내보낼 수 있도록 표시를 선택합니다.
- 7 확장 속성 모두 포함을 선택합니다.
- 8 다음, 마침을 차례로 클릭합니다.
새 인증서가 인증서(로컬 컴퓨터) > 개인 > 인증서 폴더에 나타납니다.
- 9 새 인증서에 개인 키가 포함되어 있는지 확인합니다.
 - a 인증서(로컬 컴퓨터) > 개인 > 인증서 폴더에서 새 인증서를 두 번 클릭합니다.
 - b [인증서 정보] 대화상자의 [일반] 탭에 사용자가 이 인증서와 일치하는 개인 키를 갖고 있습니다. 라는 문구가 표시되는지 확인합니다.

다음에 수행할 작업

인증서 대화명을 **vdm**으로 수정합니다.

인증서 대화명 수정

TLS 인증서를 인식하고 사용하도록 연결 서버 인스턴스 또는 보안 서버를 구성하려면 인증서 대화명을 **vdm**으로 수정해야 합니다.

사전 요구 사항

Windows 인증서 저장소의 **인증서(로컬 컴퓨터) > 개인 > 인증서** 폴더로 서버 인증서를 가져왔는지 확인합니다. [Windows 인증서 저장소에 서명된 서버 인증서 가져오기](#)의 내용을 참조하십시오.

절차

- 1 Windows Server 호스트의 MMC 창에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **개인 > 인증서** 폴더를 선택합니다.
- 2 Horizon 7 서버 호스트에 발급된 인증서를 마우스 오른쪽 단추로 클릭하고 **속성**을 클릭합니다.
- 3 일반 탭에서 **대화명** 텍스트를 삭제하고 **vdm**을 입력합니다.
- 4 **적용**과 **확인**을 차례로 클릭합니다.
- 5 **개인 > 인증서** 폴더에 대화명이 **vdm**인 다른 서버 인증서가 있는지 확인합니다.
 - a 다른 서버 인증서를 찾아 마우스 오른쪽 단추로 클릭하고 **속성**을 클릭합니다.
 - b 인증서의 대화명이 **vdm**일 경우 이름을 삭제하고 **적용**, **확인**을 차례로 클릭합니다.

다음에 수행할 작업

Windows 로컬 컴퓨터 인증서 저장소로 루트 인증서와 중간 인증서를 가져옵니다.

체인의 모든 인증서를 가져온 후 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작하여 변경 사항을 적용해야 합니다.

Windows 인증서 저장소에 루트 및 중간 인증서 가져오기

인증서 체인의 루트 인증서 및 모든 중간 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다.

중간 서버에서 가져온 TLS 서버 인증서가 연결 서버 호스트에서 알려져 있고 신뢰하는 루트 CA에서 서명된 것이며 인증서 체인에 중간 인증서가 없는 경우 이 작업을 건너뛸 수 있습니다. 일반적으로 사용되는 인증 기관은 호스트에서 신뢰할 가능성이 높습니다.

절차

- 1 Windows Server 호스트의 MMC 콘솔에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더로 이동합니다.
 - 루트 인증서가 이 폴더에 있고 인증서 체인에 중간 인증서가 없는 경우 7단계를 건너뛰십시오.

- 루트 인증서가 이 폴더에 있고 인증서 체인에 중간 인증서가 있는 경우 6단계로 건너뛰십시오.
 - 루트 인증서가 이 폴더에 없는 경우 2단계를 진행하십시오.
- 2 신뢰할 수 있는 루트 인증 기관 > 인증서 폴더를 마우스 오른쪽 버튼으로 클릭하고 모든 작업 > 가져오기를 클릭합니다.
 - 3 인증서 가져오기 마법사에서 다음을 클릭하고 루트 CA 인증서가 저장된 위치를 찾습니다.
 - 4 루트 CA 인증서 파일을 선택하고 열기를 클릭합니다.
 - 5 다음, 다음, 마침을 차례로 클릭합니다.
 - 6 중간 CA가 서버 인증서를 서명한 경우 인증서 체인의 모든 중간 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져오십시오.
 - a 인증서(로컬 컴퓨터) > 중간 인증 기관 > 인증서 폴더로 이동합니다.
 - b 가져와야 할 각 중간 인증서에 대해 3~6단계를 반복합니다.
 - 7 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.
 - 8 HTML Access를 사용하는 경우 VMware View Blast Secure Gateway 서비스를 다시 시작합니다.

클라이언트가 TLS 부하 분산 서버를 가리키도록 Horizon 7 Server 외부 URL 설정

TLS의 부하가 중간 서버로 분산되고 Horizon Client 디바이스가 보안 터널을 사용하여 Horizon 7에 연결하는 경우, 보안 터널 외부 URL을 클라이언트가 중간 서버에 액세스하는 데 사용할 수 있는 주소로 설정해야 합니다.

중간 서버에 연결하는 연결 서버 인스턴스 또는 보안 서버의 외부 URL 설정을 구성합니다.

보안 서버를 배포하는 경우, 외부 URL은 보안 서버에만 필요하고 보안 서버와 연결되는 연결 서버 인스턴스에는 필요하지 않습니다.

보안 서버를 배포하지 않는 경우나 보안 서버와 외부에 연결되는 연결 서버 인스턴스가 혼합되어 있는 네트워크 환경을 사용하는 경우에는 중간 서버에 연결하는 모든 연결 서버 인스턴스에 외부 URL이 필요합니다.

참고 PCoIP 보안 게이트웨이(PSG) 또는 Blast 보안 게이트웨이를 사용하는 TLS 연결의 부하를 분산할 수 없습니다. PCoIP 외부 URL과 Blast 보안 게이트웨이 외부 URL은 클라이언트가 PSG 및 Blast 보안 게이트웨이를 호스팅하는 컴퓨터에 연결할 수 있도록 허용해야 합니다. 중간 서버와 Horizon 7 Server 사이에 TLS 연결을 요구할 계획이 아니라면 PCoIP 외부 URL과 Blast 외부 URL이 중간 서버를 가리키도록 재설정하지 마십시오.

연결 서버 인스턴스의 외부 URL 설정

Horizon Administrator를 사용하여 연결 서버 인스턴스의 외부 URL을 구성합니다.

사전 요구 사항

- 보안 터널 연결이 연결 서버 인스턴스에서 사용하도록 설정되었는지 확인하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 클릭합니다.
- 2 연결 서버 탭에서 연결 서버 인스턴스를 선택하고 **편집**을 클릭합니다.
- 3 **외부 URL** 텍스트 상자에 보안 터널 외부 URL을 입력합니다.

URL에는 프로토콜, 클라이언트가 확인 가능한 호스트 이름 및 포트 번호가 포함되어야 합니다.

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

참고 연결 서버 인스턴스에 액세스해야 하는데 호스트 이름을 확인할 수 없을 경우 IP 주소를 사용할 수 있습니다. 그러나 연결할 호스트가 연결 서버 인스턴스에 대해 구성된 TLS 인증서와 일치하지 않으면 액세스가 차단되거나 액세스 시 보안이 약화됩니다.

- 4 이 대화상자의 모든 주소가 클라이언트 시스템이 이 연결 서버 인스턴스에 도달하도록 허용하는지 확인합니다.
- 5 **확인**을 클릭합니다.

보안 서버의 외부 URL 수정

Horizon Administrator를 사용하여 보안 서버의 외부 URL을 수정합니다.

사전 요구 사항

- 보안 터널 연결이 이 보안 서버와 연결된 연결 서버 인스턴스에서 사용하도록 설정되어 있는지 확인하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 보안 서버 탭에서 보안 서버를 선택하고 **편집**을 클릭합니다.
- 3 **외부 URL** 텍스트 상자에 보안 터널 외부 URL을 입력합니다.

URL에는 프로토콜, 클라이언트가 확인 가능한 보안 서버 호스트 이름 및 포트 번호가 포함되어야 합니다.

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

참고 호스트 이름을 확인할 수 없을 때 보안 서버에 액세스해야 할 경우 IP 주소를 사용할 수 있습니다. 그러나 연결할 호스트가 보안 서버에 대해 구성된 TLS 인증서와 일치하지 않으면 액세스가 차단되거나 액세스 시 보안이 약화됩니다.

- 4 이 대화 상자의 모든 주소가 클라이언트 시스템이 이 보안 서버 호스트에 도달하도록 허용하는지 확인합니다.

5 변경 사항을 저장하려면 **확인**을 클릭합니다.

결과

Horizon Administrator는 보안 서버에 업데이트된 외부 URL을 보냅니다. 변경 내용이 적용되도록 보안 서버 서비스를 다시 시작할 필요가 없습니다.

중간 서버의 HTTP 연결 허용

TLS의 부하가 중간 서버로 분산되는 경우 클라이언트 쪽 중간 디바이스의 HTTP 연결을 허용하도록 연결 서버 인스턴스나 보안 서버를 구성할 수 있습니다. 중간 디바이스는 Horizon Client 연결에 대해 HTTPS를 허용해야 합니다.

Horizon 7 서버와 중간 디바이스 사이에 HTTP 연결을 허용하려면 HTTP 연결이 허용되는 각 연결 서버와 보안 서버에서 **locked.properties** 파일을 구성해야 합니다.

Horizon 7 서버와 중간 디바이스 사이에 HTTP 연결을 허용하더라도 Horizon 7에서 TLS를 사용하지 않도록 설정할 수는 없습니다. Horizon 7 서버에서는 HTTP 연결뿐 아니라 HTTPS 연결도 계속해서 수락합니다.

참고 Horizon 클라이언트에서 스마트 카드 인증을 사용하는 경우, 연결 서버나 보안 서버에 대해 직접 HTTPS 연결을 설정해야 합니다. 스마트 카드 인증을 사용하면 TLS 부하 분산 기능이 지원되지 않습니다.

절차

- 1** 연결 서버 또는 보안 서버 호스트의 TLS/SSL 게이트웨이 구성 폴더에 **locked.properties** 파일을 생성 또는 편집합니다.

예: `install_directory\VMware\VMware View\Server\SSlgateway\conf\locked.properties`
- 2** Horizon 7 서버의 프로토콜을 구성하려면 **serverProtocol** 속성을 추가하고 **http**로 설정합니다.

http 값은 소문자로 입력해야 합니다.
- 3** (선택 사항) Horizon 7 서버에 기본값이 아닌 HTTP 수신 포트와 네트워크 인터페이스를 구성하는 속성을 추가합니다.
 - HTTP 수신 포트 80에서 변경하려면 **serverPortNonTLS**를 중간 디바이스가 연결할 수 있도록 구성한 다른 포트 번호로 설정합니다.
 - Horizon 7 서버에 네트워크 인터페이스가 2개 이상 있는 경우에 서버가 하나의 인터페이스에서만 HTTP 연결을 수신하도록 하려면 해당 네트워크 인터페이스의 IP 주소를 **serverHostNonTLS**에 설정합니다.
- 4** **locked.properties** 파일을 저장합니다.
- 5** 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

예제: **locked.properties** 파일

이 파일을 사용하면 Horizon 7 서버에 TLS가 아닌 HTTP 연결을 사용할 수 있습니다. Horizon 7 서버의 클라이언트 쪽 네트워크 인터페이스의 IP 주소는 10.20.30.40입니다. 서버는 기본 포트 80을 사용하여 HTTP 연결을 수신합니다. **http** 값은 소문자로 입력해야 합니다.

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