

Horizon 7 설치

2019년 12월

VMware Horizon 7 7.11



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 © 2011-2019 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

Horizon 7 설치 7

1 서버 구성 요소의 시스템 요구 사항 8

Horizon 연결 서버 요구 사항 8

Horizon 연결 서버의 하드웨어 요구 사항 8

Horizon 연결 서버 지원 운영 체제 9

Horizon 연결 서버 가상화 소프트웨어 요구 사항 9

복제된 Horizon 연결 서버 인스턴스의 네트워크 요구 사항 10

Horizon Administrator 요구 사항 10

View Composer 요구 사항 11

View Composer 지원 운영 체제 11

독립 실행형 View Composer의 하드웨어 요구 사항 12

View Composer 및 이벤트 데이터베이스의 데이터베이스 요구 사항 12

2 게스트 운영 체제의 시스템 요구 사항 14

Horizon Agent에 대해 지원되는 운영 체제 14

독립 실행형 Horizon Persona Management 지원 운영 체제 15

원격 디스플레이 프로토콜 및 소프트웨어 지원 15

PCoIP 16

Microsoft RDP 18

VMware Blast Extreme 18

3 IPv6 환경에 Horizon 7 설치 23

IPv6 환경에서 Horizon 7 설정 23

IPv6 환경에서 지원되는 vSphere 데이터베이스 및 Active Directory 버전 24

IPv6 환경에서 Horizon 7 서버를 지원하는 운영 체제 24

IPv6 환경에서 데스크톱 및 RDS 호스트에 지원되는 Windows 운영 체제 24

IPv6 환경에서 지원되는 클라이언트 25

IPv6 환경에서 지원되는 원격 프로토콜 25

IPv6 환경에서 지원되는 인증 유형 26

IPv6 환경에서 지원되는 기타 기능 26

4 FIPS 모드에서 Horizon 7 설치 29

FIPS 모드의 Horizon 7 설정 개요 29

FIPS 모드의 시스템 요구 사항 30

5 Active Directory 준비 32

도메인 및 신뢰 관계 구성 33

신뢰 관계 및 도메인 필터링	34
원격 데스크톱의 OU 생성	34
키오스크 모드 클라이언트 계정을 위한 OU 및 그룹 생성	34
사용자 그룹 생성	35
vCenter Server의 사용자 계정 생성	35
독립 실행형 View Composer Server의 사용자 계정 생성	35
View Composer AD 작업을 위한 사용자 계정 생성	35
인스턴트 클론 작업을 위한 사용자 계정 만들기	36
제한된 그룹 정책 구성	37
Horizon 7 그룹 정책 관리 템플릿 파일 사용	38
스마트 카드 인증을 위한 Active Directory 준비	39
스마트 카드 사용자의 UPN 추가	39
신뢰할 수 있는 루트 인증 기관에 루트 인증서 추가	40
중간 인증 기관에 중간 인증서 추가	41
Enterprise NTAAuth 저장소에 루트 인증서 추가	41
SSL/TLS에서 취약한 암호 사용 안 함	42

6 View Composer 설치 43

View Composer 데이터베이스 준비	43
View Composer용 SQL Server 데이터베이스 생성	44
View Composer용 Oracle 데이터베이스 생성	48
View Composer를 위한 SSL 인증서 구성	52
View Composer 서비스 설치	52
View Composer에서 vCenter의 TLSv1.0 및 ESXi 연결 사용	54
View Composer를 위한 인프라 구축	55
View Composer를 위한 vSphere 환경 구성	56
View Composer의 추가 모범 사례	56

7 Horizon 연결 서버 설치 57

Horizon 연결 서버 소프트웨어 설치	57
Horizon 연결 서버의 설치 전제 조건	58
새 구성을 사용하여 Horizon 연결 서버 설치	59
Horizon 연결 서버 자동 설치	62
Horizon 연결 서버 표준 설치의 자동 설치 속성	64
연결 서버의 vCenter 연결에서 TLSv1.0 사용	65
Horizon 연결 서버의 복제된 인스턴스 설치	66
Horizon 연결 서버의 복제된 인스턴스 자동 설치	69
Horizon 연결 서버의 복제된 인스턴스 자동 설치 속성	72
보안 서버 연결 암호 구성	73
보안 서버 설치	73
보안 서버 자동 설치	77

보안 서버 자동 설치 속성	79
보안 서버에 대한 IPsec 규칙 제거	81
VPN보다 나은 Unified Access Gateway 장치의 이점	82
Horizon 연결 서버의 방화벽 규칙	83
IPsec을 지원하도록 백엔드 방화벽 구성	84
백업 구성을 사용하여 Horizon 연결 서버 재설치	85
Microsoft Windows Installer 명령줄 옵션	86
MSI 명령줄 옵션을 사용하여 Horizon 7 구성 요소 자동 제거	88

8 Horizon 7 서버를 위한 TLS 인증서 구성 91

Horizon 7 서버를 위한 TLS 인증서 이해	91
TLS 인증서 설정 작업 개요	93
CA에서 서명된 TLS 인증서 가져오기	94
Windows 도메인 또는 Enterprise CA를 통해 서명된 인증서 가져오기	95
새로운 TLS 인증서를 사용하도록 Horizon 연결 서버, 보안 서버 또는 View Composer 구성	96
MMC에 인증서 스냅인 추가	97
Windows 인증서 저장소에 서명된 서버 인증서 가져오기	98
인증서 대화명 수정	99
Windows 인증서 저장소에 루트 인증서 및 중간 인증서 가져오기	100
View Composer가 사용하는 포트에 새 TLS 인증서 바인딩	101
루트 및 중간 인증서를 신뢰하도록 클라이언트 끝점 구성	102
루트 및 중간 인증서를 신뢰하도록 Mac용 Horizon Client 구성	103
루트 및 중간 인증서를 신뢰하도록 iOS용 Horizon Client 구성	104
서버 인증서에 대한 인증서 해지 검사 구성	104
새 TLS 인증서를 사용하도록 PCoIP 보안 게이트웨이 구성	105
서버 이름이 PSG 인증서 주체 이름과 일치하는지 확인	106
Windows 인증서 저장소에 PSG 인증서 구성	107
Windows 레지스트리에서 PSG 인증서 대화명 설정	108
PSG에 대한 연결에 CA 서명 인증서를 강제로 사용하도록 설정	109
vCenter Server 또는 View Composer 인증서를 신뢰하도록 Horizon Administrator 설정	110
CA에서 서명한 TLS 인증서 사용 시 장점	110
Horizon 연결 서버 및 보안 서버의 인증서 문제 해결	110

9 처음으로 Horizon 7 구성 112

vCenter Server, View Composer 및 인스턴트 클론에 대한 사용자 계정 구성	112
vCenter Server 사용자 및 View Composer 사용자 사용처	113
Horizon 7 및 View Composer를 위한 vCenter Server 사용자 구성	113
vCenter Server 사용자에게 필요한 권한	115
vCenter Server 사용자에게 필요한 View Composer 및 인스턴트 클론 권한	116
처음으로 Horizon 연결 서버 구성	118
Horizon Administrator 및 Horizon 연결 서버	118

Horizon Administrator에 로그인	119
제품 라이선스 키 설치	120
Horizon 7에 vCenter Server 인스턴스 추가	120
View Composer 설정 구성	122
View Composer 도메인 구성	123
인스턴트 클론 도메인 관리자 추가	124
vSphere가 연결된 클론 가상 시스템의 디스크 공간을 회수할 수 있도록 허용	125
vCenter Server의 View Storage Accelerator 구성	126
vCenter Server 및 View Composer의 동시 작업 수 제한	128
동시 전원 작업 수를 설정하여 원격 데스크톱 로그인 스톱 지원	129
기본 TLS 인증서의 지문 허용	130
Horizon Client 연결 구성	131
PCoIP 보안 게이트웨이 및 보안 터널 연결 구성	132
Blast 보안 게이트웨이 구성	133
보안 게이트웨이 및 터널 연결용 외부 URL 구성	135
연결 서버 인스턴스의 외부 URL 설정	136
보안 서버의 외부 URL 수정	137
Horizon 연결 서버가 주소 정보를 반환할 때 DNS 이름을 기본 설정으로 사용	138
로드 밸런서를 통한 HTML Access 허용	139
게이트웨이를 통한 HTML Access 허용	139
Horizon 7 서비스의 기본 포트 교체	140
Horizon 연결 서버 인스턴스 및 보안 서버의 기본 HTTP 포트 또는 NIC 교체	140
Horizon 연결 서버 인스턴스 및 보안 서버의 PCoIP 보안 게이트웨이의 기본 포트 또는 NIC 교체	141
연결 서버 인스턴스 및 보안 서버에서 PCoIP 보안 게이트웨이의 기본 제어 포트 교체	143
View Composer의 기본 포트 교체	143
연결 서버에 대한 HTTP 리디렉션 포트 번호 변경	144
연결 서버에 대한 클라이언트 연결에 HTTP 리디렉션 사용 안 함	145
연결 서버에서 Horizon 7 성능 카운터에 대한 원격 액세스 사용	145
Windows Server 설정을 크기 조정하여 배포 지원	146
Horizon 연결 서버의 메모리 크기 조정	146
시스템 페이지 파일 설정 구성	146

10 이벤트 보고 구성 148

Horizon 7 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가	148
이벤트 보고용 SQL Server 데이터베이스 준비	149
이벤트 데이터베이스 구성	150
Syslog 서버의 이벤트 로깅 구성	151

Horizon 7 설치

“Horizon 7 설치”에서는 VMware Horizon[®] 7 서버 및 클라이언트 구성 요소를 설치하는 방법을 설명합니다.

대상

이 정보는 VMware Horizon 7을 설치하려는 모든 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영에 익숙하고 경험 많은 Windows 또는 Linux 시스템 관리자를 대상으로 작성되었습니다.

서버 구성 요소의 시스템 요구 사항

1

Horizon 7 서버 구성 요소를 실행하는 호스트는 특정 하드웨어 및 소프트웨어 요구 사항을 충족해야 합니다.

본 장은 다음 항목을 포함합니다.

- [Horizon 연결 서버 요구 사항](#)
- [Horizon Administrator 요구 사항](#)
- [View Composer 요구 사항](#)

Horizon 연결 서버 요구 사항

Horizon 연결 서버는 들어오는 사용자 요청을 인증한 다음 적절한 원격 데스크톱 및 애플리케이션으로 전달하여 클라이언트 연결의 브로커 역할을 합니다. Horizon 연결 서버에는 특정 하드웨어, 운영 체제, 설치 및 지원하는 소프트웨어 요구 사항이 있습니다.

- [Horizon 연결 서버의 하드웨어 요구 사항](#)
표준, 복제본, 보안 서버 및 등록 서버 설치를 포함한 모든 Horizon 연결 서버 설치 유형을 특정 하드웨어 요구 사항을 충족하는 전용 물리적 시스템 또는 가상 시스템에 설치해야 합니다.
- [Horizon 연결 서버 지원 운영 체제](#)
지원되는 Windows Server 운영 체제에 Horizon 연결 서버를 설치해야 합니다.
- [Horizon 연결 서버 가상화 소프트웨어 요구 사항](#)
Horizon 연결 서버에는 특정한 VMware 가상화 소프트웨어 버전이 필요합니다.
- [복제된 Horizon 연결 서버 인스턴스의 네트워크 요구 사항](#)
복제된 Horizon 연결 서버 인스턴스를 설치할 경우 일반적으로 동일한 물리적 위치에서 인스턴스를 구성하고 고성능 LAN을 통해 연결해야 합니다. 그렇지 않으면 지연 문제로 인해 Horizon 연결 서버 인스턴스의 View LDAP 구성이 일관되지 않게 됩니다. 구성이 오래된 Horizon 연결 서버 인스턴스에 연결하는 경우 사용자의 액세스가 거부될 수 있습니다.

Horizon 연결 서버의 하드웨어 요구 사항

표준, 복제본, 보안 서버 및 등록 서버 설치를 포함한 모든 Horizon 연결 서버 설치 유형을 특정한 하드웨어 요구 사항을 충족하는 전용 물리적 시스템 또는 가상 시스템에 설치해야 합니다.

표 1-1. Horizon 연결 서버 하드웨어 요구 사항

하드웨어 구성 요소	필수	권장
프로세서	Pentium IV 2.0GHz 프로세서 이상	CPU 4개
네트워크 어댑터	100Mbps NIC	1Gbps NIC
메모리 Windows Server 2008 R2 64비트	4GB RAM 이상	원격 데스크톱을 50대 이상 배포하는 경우 10GB RAM 이상
메모리 Windows Server 2012 R2 64비트	4GB RAM 이상	원격 데스크톱을 50대 이상 배포하는 경우 10GB RAM 이상

이러한 요구 사항은 고가용성 또는 외부 액세스를 위해 설치하는 복제본 및 보안 서버 Horizon 연결 서버 인스턴스에도 적용됩니다.

중요 Horizon 연결 서버를 호스팅하는 물리적 시스템이나 가상 시스템에는 변경되지 않는 IP 주소가 있어야 합니다. IPv4 환경에서 정적 IP 주소를 구성합니다. IPv6 환경에서 시스템은 변경되지 않는 IP 주소를 자동으로 가져옵니다.

Horizon 연결 서버 지원 운영 체제

지원되는 Windows Server 운영 체제에 Horizon 연결 서버를 설치해야 합니다.

다음 운영 체제는 표준, 복제본 및 보안 서버 설치를 포함한 모든 Horizon 연결 서버 설치 유형을 지원합니다.

표 1-2. Horizon 연결 서버의 운영 체제 지원

운영 체제	버전	버전
Windows Server 2008 R2 SP1	64비트	Standard Enterprise 데이터 센터
Windows Server 2012 R2	64비트	Standard 데이터 센터
Windows Server 2016	64비트	Standard 데이터 센터
Windows Server 2019	64비트	Standard 데이터 센터

참고 서비스 팩이 포함되지 않은 Windows Server 2008 R2는 더 이상 지원되지 않습니다.

Horizon 연결 서버 가상화 소프트웨어 요구 사항

Horizon 연결 서버에는 특정한 VMware 가상화 소프트웨어 버전이 필요합니다.

vSphere를 사용할 경우 지원되는 버전의 vSphere ESX/ESXi 호스트와 vCenter Server를 사용해야 합니다.

어떤 Horizon 버전이 어떤 vCenter Server 및 ESXi 버전과 호환되는지에 대한 자세한 내용은 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php의 "VMware 제품 상호 운용성 매트릭스"를 참조하십시오.

복제된 Horizon 연결 서버 인스턴스의 네트워크 요구 사항

복제된 Horizon 연결 서버 인스턴스를 설치할 경우 일반적으로 동일한 물리적 위치에서 인스턴스를 구성하고 고성능 LAN을 통해 연결해야 합니다. 그렇지 않으면 지연 문제로 인해 Horizon 연결 서버 인스턴스의 View LDAP 구성이 일관되지 않게 됩니다. 구성이 오래된 Horizon 연결 서버 인스턴스에 연결하는 경우 사용자의 액세스가 거부될 수 있습니다.

중요 Horizon 배포가 여러 데이터 센터에 걸쳐 이루어져야 하는 경우 복제된 연결 서버 인스턴스 그룹을 WAN, MAN(Metropolitan Area Network) 또는 LAN이 아닌 기타 네트워크에서 사용하려면 Cloud Pod 아키텍처 기능을 사용해야 합니다. 자세한 내용은 "Horizon 7에서 Cloud Pod 아키텍처 관리" 문서를 참조하십시오.

Horizon Administrator 요구 사항

관리자는 Horizon Administrator를 사용하여 Horizon Connection Server를 구성하고, 원격 데스크톱 및 애플리케이션을 배포 및 관리하며, 사용자 인증을 제어하고, 시스템 이벤트를 초기화 및 관찰하고, 분석 작업을 수행합니다. Horizon Administrator를 실행하는 클라이언트 시스템은 특정 요구 사항을 충족해야 합니다.

Horizon Administrator는 View 연결 서버를 설치할 때 설치된 웹 기반 애플리케이션입니다. Horizon Administrator에 액세스하여 다음 웹 브라우저와 함께 사용할 수 있습니다.

- Internet Explorer 9(권장하지 않음)
- Internet Explorer 10
- Internet Explorer 11
- Firefox(최신 지원 버전)
- Chrome(최신 지원 버전)
- Safari 6 이상 릴리스
- Microsoft Edge(Windows 10)

웹 브라우저에서 Horizon Administrator를 사용할 경우, Adobe Flash Player 10.1 이상을 설치해야 합니다. Adobe Flash Player가 설치될 수 있도록 클라이언트 시스템이 인터넷에 액세스할 수 있어야 합니다.

Horizon Administrator를 실행하는 컴퓨터가 연결 서버를 호스팅하는 서버의 루트 및 중간 인증서를 신뢰해야 합니다. 지원되는 브라우저에 잘 알려진 모든 인증 기관(CA)의 인증서가 이미 있습니다. 잘 알려지지 않은 CA에서 인증서를 가져오는 경우 [루트 및 중간 인증서를 신뢰하도록 클라이언트 끝점 구성](#)의 지침에 따라야 합니다.

텍스트를 올바르게 표시하려면 Horizon Administrator에 Microsoft 특정 글꼴이 필요합니다. 웹 브라우저가 Linux, UNIX 또는 Mac과 같은 비 Windows 운영 체제에서 실행될 경우 Microsoft 특정 글꼴이 컴퓨터에 설치되어 있어야 합니다.

현재 Microsoft 웹 사이트에서는 Microsoft 글꼴을 배포하지 않지만 독립 웹 사이트에서 다운로드할 수 있습니다.

View Composer 요구 사항

View Composer를 사용하여 중앙화된 단일 기본 이미지에서 여러 연결된 클론 데스크톱을 배포할 수 있습니다. View Composer에는 특정 설치 및 스토리지 요구 사항이 있습니다.

■ View Composer 지원 운영 체제

View Composer는 64비트 운영 체제를 지원하며, 여기에는 특정 요구 사항 및 제한 사항이 적용됩니다. View Composer를 vCenter Server와 동일한 물리적 또는 가상 시스템이나 별도의 서버에 설치할 수 있습니다.

■ 독립 실행형 View Composer의 하드웨어 요구 사항

View Composer를 vCenter Server에 사용되는 시스템과 다른 물리적 또는 가상 시스템에 설치하는 경우 특정 하드웨어 요구 사항을 충족하는 전용 시스템을 사용해야 합니다.

■ View Composer 및 이벤트 데이터베이스의 데이터베이스 요구 사항

데이터를 저장하려면 View Composer에 SQL 데이터베이스가 필요합니다. View Composer 데이터베이스는 View Composer Server 호스트에 있거나 View Composer Server 호스트에서 사용할 수 있어야 합니다. 선택적으로, Horizon Connection Server에서 Horizon 이벤트에 대한 정보를 기록하도록 이벤트 데이터베이스를 설정할 수도 있습니다.

View Composer 지원 운영 체제

View Composer는 64비트 운영 체제를 지원하며, 여기에는 특정 요구 사항 및 제한 사항이 적용됩니다. View Composer를 vCenter Server와 동일한 물리적 또는 가상 시스템이나 별도의 서버에 설치할 수 있습니다.

표 1-3. View Composer에 대한 운영 체제 지원

운영 체제	버전	버전
Windows Server 2008 R2 SP1	64비트	Standard Enterprise 데이터 센터
Windows Server 2012 R2	64비트	Standard 데이터 센터

표 1-3. View Composer에 대한 운영 체제 지원 (계속)

운영 체제	버전	버전
Windows Server 2016	64비트	Standard 데이터 센터
Windows Server 2019	64비트	Standard 데이터 센터

참고 서비스 팩이 포함되지 않은 Windows Server 2008 R2는 더 이상 지원되지 않습니다.

View Composer를 vCenter Server와 다른 물리적 또는 가상 시스템에 설치하려는 경우 **독립 실행형 View Composer의 하드웨어 요구 사항**을 참조하십시오.

Windows Server 2016 또는 Windows Server 2019 가상 시스템의 View Composer 설치 문제 해결에 대한 자세한 내용은 VMware 기술 자료 문서 <https://kb.vmware.com/s/article/59633>를 참조하십시오.

독립 실행형 View Composer의 하드웨어 요구 사항

View Composer를 vCenter Server에 사용되는 시스템과 다른 물리적 또는 가상 시스템에 설치하는 경우 특정 하드웨어 요구 사항을 충족하는 전용 시스템을 사용해야 합니다.

독립 실행형 View Composer 설치하는 별개의 Windows Server 시스템에 설치된 vCenter Server 또는 Linux 기반 vCenter Server Appliance에서 작동합니다. 각 View Composer 서비스와 vCenter Server 인스턴스가 일대일로 매핑되도록 하는 것이 좋습니다.

표 1-4. View Composer 하드웨어 요구 사항

하드웨어 구성 요소	필수	권장
프로세서	2대의 CPU가 포함된 1.4GHz 이상의 Intel 64 또는 AMD 64 프로세서	2GHz 이상 및 4대의 CPU
네트워킹	10/100Mbps NIC(네트워크 인터페이스 카드) 1개 이상	1Gbps NIC
메모리	4GB RAM 이상	원격 데스크톱을 50대 이상 배포하는 경우 8GB RAM 이상
디스크 공간	40GB	60GB

중요 View Composer를 호스팅하는 물리적 시스템이나 가상 시스템에는 변경되지 않는 IP 주소가 있어야 합니다. IPv4 환경에서 정적 IP 주소를 구성합니다. IPv6 환경에서 시스템은 변경되지 않는 IP 주소를 자동으로 가져옵니다.

View Composer 및 이벤트 데이터베이스의 데이터베이스 요구 사항

데이터를 저장하려면 View Composer에 SQL 데이터베이스가 필요합니다. View Composer 데이터베이스는 View Composer Server 호스트에 있거나 View Composer Server 호스트에서 사용할 수

있어야 합니다. 선택적으로, Horizon Connection Server에서 Horizon 이벤트에 대한 정보를 기록하도록 이벤트 데이터베이스를 설정할 수도 있습니다.

vCenter Server의 데이터베이스 서버 인스턴스가 이미 있고 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php의 VMware 제품 상호 운용성 매트릭스에 나열된 버전일 경우 View Composer가 이 기존 인스턴스를 사용할 수 있습니다. 데이터베이스 서버 인스턴스가 아직 없을 경우 설치해야 합니다.

View Composer는 vCenter Server에서 지원하는 데이터베이스 서버의 하위 집합을 지원합니다. View Composer에서 지원하지 않는 데이터베이스 서버와 함께 vCenter Server를 이미 사용하고 있는 경우 vCenter Server용으로 해당 데이터베이스 서버를 계속 사용하고 View Composer용으로 별도의 데이터베이스 서버를 설치합니다.

중요 vCenter Server와 동일한 SQL Server 인스턴스에 View Composer 데이터베이스를 생성하는 경우 vCenter Server 데이터베이스를 덮어쓰지 마십시오.

지원되는 데이터베이스에 대한 가장 최신 정보는 VMware 제품 상호 운용성 매트릭스(http://www.vmware.com/resources/compatibility/sim/interop_matrix.php)를 참조하십시오. **솔루션/데이터베이스 상호 운용성**의 경우 제품과 버전을 선택한 후 데이터베이스 추가 단계에서 지원되는 모든 데이터베이스 목록을 보려면 **임의**를 선택하고 **추가**를 클릭합니다.

게스트 운영 체제의 시스템 요구 사항

2

Horizon Agent 또는 Horizon Persona Management를 실행하는 시스템은 특정 하드웨어 및 소프트웨어 요구 사항을 충족해야 합니다.

본 장은 다음 항목을 포함합니다.

- Horizon Agent에 대해 지원되는 운영 체제
- 독립 실행형 Horizon Persona Management 지원 운영 체제
- 원격 디스플레이 프로토콜 및 소프트웨어 지원

Horizon Agent에 대해 지원되는 운영 체제

Horizon Agent 구성 요소(이전 릴리스에서는 View Agent)는 세션 관리, Single Sign-On, 디바이스 리디렉션 및 기타 기능을 지원합니다. Horizon Agent를 모든 가상 시스템, 물리적 시스템 및 RDS 호스트에 설치해야 합니다.

지원되는 게스트 운영 체제의 유형 및 버전은 Windows 버전에 따라 다릅니다. 지원되는 Windows 10 운영 체제 목록에 대한 업데이트를 보려면 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2149393>를 참조하십시오. Windows 10 이외의 Windows 운영 체제의 경우 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2150295>를 참조하십시오.

Horizon Agent가 설치된 Windows 운영 체제에서 지원되는 특정 원격 환경 기능 목록을 보려면 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2150305>를 참조하십시오.

Horizon Agent에서 Horizon Persona Management 설정 옵션을 사용하려면 Windows 10, Windows 8, Windows 8.1, Windows 7, Windows Server 2012 R2, Windows Server 2008 R2 또는 Windows Server 2016 가상 시스템에 Horizon Agent를 설치해야 합니다. 이 옵션은 물리적 컴퓨터 또는 RDS 호스트에서는 작동하지 않습니다.

물리적 컴퓨터에 Horizon Persona Management 독립 실행형 버전을 설치할 수 있습니다. **독립 실행형 Horizon Persona Management 지원 운영 체제**의 내용을 참조하십시오.

참고 VMware Blast 디스플레이 프로토콜을 사용하려면 단일 세션 가상 시스템이나 RDS 호스트에 Horizon Agent를 설치해야 합니다. RDS 호스트는 물리적 시스템 또는 가상 시스템일 수 있습니다. Windows 10 RS4의 엔터프라이즈 버전 및 이후 빌드를 제외하고 VMware Blast 디스플레이 프로토콜은 단일 사용자 물리적 컴퓨터에서 작동하지 않습니다.

보안 강화를 위해서는 암호 제품군을 구성하여 알려진 취약성을 제거하는 것이 좋습니다. View Composer 또는 Horizon Agent를 실행하는 Windows 시스템의 암호 제품군에 도메인 정책을 설정하는 방법에 대한 지침은 [SSL/TLS에서 취약한 암호 사용 안 함](#)을 참조하십시오.

독립 실행형 Horizon Persona Management 지원 운영 체제

독립 실행형 Horizon Persona Management 소프트웨어는 Horizon Agent가 설치되지 않은 독립 실행형 물리적 컴퓨터 및 가상 시스템을 위한 개인 설정 관리를 제공합니다. 사용자가 로그인하면 사용자의 프로파일이 원격 프로필 저장소에서 독립 실행형 시스템에 동적으로 다운로드됩니다.

참고 Horizon 데스크톱의 Horizon Persona Management를 구성하려면 **Persona Management** 설정 옵션을 사용하여 Horizon Agent를 설치하십시오. 독립 실행형 Persona Management 소프트웨어는 비 Horizon 시스템만을 대상으로 합니다.

독립 실행형 Horizon Persona Management 소프트웨어에 지원되는 운영 체제 목록을 보려면 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2150295>를 참조하십시오.

독립 실행형 Persona Management 소프트웨어는 Microsoft 원격 데스크톱 서비스에서 지원되지 않습니다.

원격 디스플레이 프로토콜 및 소프트웨어 지원

원격 디스플레이 프로토콜 및 소프트웨어는 원격 데스크톱 및 애플리케이션에 대한 액세스를 제공합니다. 사용되는 원격 디스플레이 프로토콜은 클라이언트 디바이스 유형, 원격 데스크톱 또는 원격 애플리케이션에 연결하는지 여부 및 관리자가 데스크톱 또는 애플리케이션 풀을 구성하는 방식에 따라 달라집니다.

■ PCoIP

PCoIP(PC over IP)는 LAN 또는 WAN의 많은 사용자에게 애플리케이션, 이미지, 오디오 및 비디오 콘텐츠를 포함한 전체 원격 데스크톱 환경 또는 게시된 애플리케이션의 제공을 위해 최적화된 데스크톱 환경을 제공합니다. PCoIP는 지연 증가 또는 대역폭 감소를 보완하여 네트워크 상태와 상관없이 최종 사용자가 효율적으로 유지할 수 있도록 합니다.

■ Microsoft RDP

원격 데스크톱 프로토콜은 가정용 컴퓨터에서 회사 컴퓨터에 액세스할 때 많이 사용하는 다채널 프로토콜과 동일합니다. Microsoft Remote Desktop Connection(RDC)은 RDP를 사용하여 데이터를 전송합니다.

■ VMware Blast Extreme

모바일 클라우드용으로 최적화된 VMware Blast Extreme은 H.264를 지원하는 클라이언트 디바이스를 가장 폭넓게 지원합니다. VMware Blast는 디스플레이 프로토콜 중에서 가장 CPU 소비가 적기 때문에 모바일 디바이스에서 배터리 수명이 더 깁니다. VMware Blast Extreme은 지연 시간 증가나 대역폭 감소를 보완할 수 있으며 TCP 및 UDP 네트워크 전송을 모두 활용할 수 있습니다.

PCoIP

PCoIP(PC over IP)는 LAN 또는 WAN의 많은 사용자에게 애플리케이션, 이미지, 오디오 및 비디오 콘텐츠를 포함한 전체 원격 데스크톱 환경 또는 게시된 애플리케이션의 제공을 위해 최적화된 데스크톱 환경을 제공합니다. PCoIP는 지연 증가 또는 대역폭 감소를 보완하여 네트워크 상태와 상관없이 최종 사용자가 효율적으로 유지할 수 있도록 합니다.

PCoIP 디스플레이 프로토콜은 RDS 호스트의 공유 세션 데스크톱, Teradici 호스트 카드가 있는 물리적 시스템 또는 가상 시스템을 사용하는 원격 데스크톱 및 게시된 애플리케이션에 사용할 수 있습니다.

PCoIP 기능

PCoIP의 키 기능에는 다음 내용이 포함됩니다.

- 회사 방화벽 외부 사용자는 회사의 VPN(Virtual Private Network)에 이 프로토콜을 사용하거나 회사 DMZ에서 보안 서버 또는 Access Point 장치에 대한 암호화된 보안 연결을 구성할 수 있습니다.
 - AES(Advanced Encryption Standard) 128비트 암호화가 지원되며 기본적으로 사용됩니다. 하지만 암호화 키 암호를 AES-256으로 변경할 수 있습니다.
 - [Horizon Agent에 대해 지원되는 운영 체제](#)에 나열된 Horizon Agent 운영 체제 버전이 있는 Windows 데스크톱으로의 연결이 지원됩니다.
 - 모든 유형의 클라이언트 디바이스에서 연결할 수 있습니다.
 - LAN 및 WAN에서 대역폭 사용을 줄이는 최적화 제어가 제공됩니다.
 - 32비트 색상이 가상 디스플레이를 위해 지원됩니다.
 - ClearType 글꼴이 지원됩니다.
 - LAN 및 WAN의 동적 오디오 품질 조정이 포함된 오디오 리디렉션이 지원됩니다.
 - 일부 클라이언트 유형에서 웹캠 및 마이크를 사용할 수 있도록 실시간 오디오-비디오가 지원됩니다.
 - 클라이언트 운영 체제와 원격 데스크톱 또는 게시된 애플리케이션 간의 텍스트와 이미지(일부 클라이언트) 복사 및 붙여넣기가 지원됩니다. 다른 클라이언트 유형에서는 일반 텍스트 복사 및 붙여넣기만 지원됩니다. 시스템 사이에서 폴더 및 파일과 같은 시스템 개체를 복사하고 붙여 넣을 수 없습니다.
 - 일부 클라이언트 유형에서 다중 모니터가 지원됩니다. 일부 클라이언트에서는 디스플레이당 해상도가 최대 2560 x 1600인 모니터를 최대 4개까지 사용하거나, Aero를 사용하지 않는 Windows 7 원격 데스크톱의 경우 해상도가 최대 4K(3840 x 2160)인 모니터를 최대 3개까지 사용할 수 있습니다. 피벗 디스플레이 및 자동 맞춤도 지원됩니다.
- 3D 기능을 사용하도록 설정된 경우에는 최대 1920 x 1200 해상도를 사용하는 최대 2대의 모니터나 해상도가 4K(3840 x 2160)인 모니터 한 대가 지원됩니다.
- 일부 클라이언트 유형에서 USB 리디렉션이 지원됩니다.
 - MMR 리디렉션은 일부 Windows 클라이언트 운영 체제와 일부 원격 데스크톱 운영 체제(Horizon Agent 설치)에서 지원됩니다.

특정 PCoIP 기능을 지원하는 데스크톱 운영 체제 유형에 대한 내용은 “Horizon 7 아키텍처 계획” 문서를 참조하십시오.

특정 PCoIP 기능을 지원하는 클라이언트 디바이스에 대한 자세한 내용은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>에 나와 있습니다.

권장된 게스트 운영 체제 설정

고화질 또는 전체 화면 모드로 재생하거나 720p 이상 형식 비디오를 재생하려면 1GB RAM 이상 및 이중 CPU를 사용하는 것이 좋습니다. CAD 애플리케이션 같은 그래픽 위주의 애플리케이션에 vDGA(Virtual Dedicated Graphics Acceleration)를 사용하려면 4GB의 RAM이 필요합니다.

비디오 품질 요구 사항

480p 형식 비디오

원격 데스크톱에 단일 가상 CPU가 있는 경우 기본 해상도에서 480p 이하로 비디오를 재생할 수 있습니다. 고화질 Flash 또는 전체 화면 모드로 비디오를 재생하려는 경우 데스크톱에 이중 가상 CPU가 필요합니다. 이중 가상 CPU 데스크톱을 사용하더라도 최소 360p 형식 비디오를 전체 화면 모드로 재생하면 특히 Windows 클라이언트에서 비디오가 오디오보다 늦게 재생될 수 있습니다.

720p 형식 비디오

원격 데스크톱에 이중 가상 CPU가 있는 경우 기본 해상도에서 720p로 비디오를 재생할 수 있습니다. 고화질 또는 전체 화면 모드로 720p에서 비디오를 재생할 경우 성능이 영향을 받을 수 있습니다.

1080p 형식 비디오

원격 데스크톱에 이중 가상 CPU가 있는 경우 미디어 플레이어의 창 크기를 더 작게 조정해야 할 수도 있지만 1080p 형식 비디오를 재생할 수 있습니다.

3D 렌더링

소프트웨어 또는 하드웨어 가속 그래픽을 사용하도록 원격 데스크톱을 구성할 수 있습니다. 소프트웨어 가속 그래픽 기능을 사용하면 물리적 GPU(그래픽 처리 장치)가 없어도 DirectX 9 및 OpenGL 2.1 애플리케이션을 실행할 수 있습니다. 하드웨어 가속 그래픽 기능을 사용하면 가상 시스템이 vSphere 호스트의 물리적 GPU(그래픽 처리 장치)를 공유하거나 물리적 GPU를 단일 가상 시스템 데스크톱 전용으로 사용할 수 있습니다.

3D 애플리케이션의 경우 최대 2대의 모니터가 지원되며 최대 화면 해상도는 1920 x 1200입니다. 원격 데스크톱의 게스트 운영 체제는 Windows 7 이상이어야 합니다.

클라이언트 시스템의 하드웨어 요구 사항

프로세서 및 메모리 요구 사항에 대한 자세한 내용은 특정 유형의 데스크톱 또는 모바일 클라이언트 디바이스에 대한 “VMware Horizon Client 사용” 문서를 참조하십시오. 자세한 사항은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>의 내용을 참조하십시오.

Microsoft RDP

원격 데스크톱 프로토콜은 가정용 컴퓨터에서 회사 컴퓨터에 액세스할 때 많이 사용하는 다채널 프로토콜과 동일합니다. Microsoft Remote Desktop Connection(RDC)은 RDP를 사용하여 데이터를 전송합니다.

Microsoft RDP는 RDS 호스트의 가상 시스템, 물리적 시스템 또는 공유 세션 데스크톱을 사용하는 원격 데스크톱용으로 지원되는 디스플레이 프로토콜입니다. (게시된 애플리케이션에서는 PCoIP 디스플레이 프로토콜과 VMware Blast 디스플레이 프로토콜만 지원됩니다.) Microsoft RDP는 다음과 같은 기능을 제공합니다.

- RDP 7은 최대 16대의 다중 모니터 지원이 가능합니다.
- 로컬 시스템과 원격 데스크톱 간에 폴더 및 파일과 같은 시스템 개체와 텍스트를 복사하고 붙여 넣을 수 있습니다.
- 32비트 색상이 가상 디스플레이를 위해 지원됩니다.
- RDP는 128비트 암호화를 지원합니다.
- 회사 방화벽 외부 사용자는 회사의 VPN(Virtual Private Network)에 이 프로토콜을 사용하거나 회사 DMZ에서 View 보안 서버에 대한 암호화된 보안 연결을 구성할 수 있습니다.

TLSv1.1 및 TLSv1.2 연결을 Windows 7 및 Windows Server 2008 R2에 지원하려면 Microsoft 핫픽스 KB3080079를 적용해야 합니다.

클라이언트 시스템의 하드웨어 요구 사항

프로세서 및 메모리 요구 사항에 대한 자세한 내용은 특정 유형의 클라이언트 시스템에 대한 “VMware Horizon Client 사용” 문서를 참조하십시오. 자세한 사항은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>의 내용을 참조하십시오.

참고 모바일 클라이언트 3.x 디바이스에서는 PCoIP 디스플레이 프로토콜만 사용합니다. 모바일 클라이언트 4.x 클라이언트에서는 PCoIP 디스플레이 프로토콜 또는 VMware Blast 디스플레이 프로토콜만 사용합니다.

VMware Blast Extreme

모바일 클라우드용으로 최적화된 VMware Blast Extreme은 H.264를 지원하는 클라이언트 디바이스를 가장 폭넓게 지원합니다. VMware Blast는 디스플레이 프로토콜 중에서 가장 CPU 소비가 적기 때문에 모바일 디바이스에서 배터리 수명이 더 길다. VMware Blast Extreme은 지연 시간 증가나 대역폭 감소를 보완할 수 있으며 TCP 및 UDP 네트워크 전송을 모두 활용할 수 있습니다.

VMware Blast 디스플레이 프로토콜은 RDS 호스트의 가상 시스템이나 공유 세션 데스크톱을 사용하는 원격 데스크톱 및 게시된 애플리케이션에 사용할 수 있습니다. RDS 호스트는 물리적 시스템 또는 가상 시스템일 수 있습니다. Windows 10 RS4의 엔터프라이즈 버전 및 이후 빌드를 제외하고 VMware Blast 디스플레이 프로토콜은 단일 사용자 물리적 컴퓨터에서 작동하지 않습니다.

참고 영화 및 TV 애플리케이션은 Windows 10 RS4에서 실행하는 물리적 컴퓨터에서 지원되지 않습니다.

VMware Blast Extreme 기능

VMware Blast Extreme의 주요 기능에는 다음 내용이 포함됩니다.

- 회사 방화벽 외부 사용자는 회사의 VPN(Virtual Private Network)에 이 프로토콜을 사용하거나 회사 DMZ에서 보안 서버 또는 Access Point 장치에 대한 암호화된 보안 연결을 구성할 수 있습니다.
- AES(Advanced Encryption Standard) 128비트 암호화가 지원되며 기본적으로 사용됩니다. 하지만 암호화 키 암호를 AES-256으로 변경할 수 있습니다.
- [Horizon Agent에 대해 지원되는 운영 체제](#)에 나열된 Horizon Agent 운영 체제 버전이 있는 Windows 데스크톱으로의 연결이 지원됩니다.
- 모든 유형의 클라이언트 디바이스에서 연결할 수 있습니다.
- LAN 및 WAN에서 대역폭 사용을 줄이는 최적화 제어가 제공됩니다.
- Windows 에이전트의 PerfMon을 사용하여 표시되는 성능 카운터는 다음에 대해 일정한 속도로 업데이트되는 시스템의 현재 상태도 정확히 반영합니다.
 - Blast 세션
 - 이미징
 - 오디오
 - CDR
 - USB: Windows 에이전트에서 PerfMon을 사용하여 표시되는 USB 카운터는 USB 트래픽이 VVC(VMware 가상 채널)를 사용하도록 구성된 경우에 유효합니다.
 - 비즈니스용 Skype: 제어 트래픽에 대한 카운터만 제공됩니다.
 - 클립보드
 - RTAV
 - 직렬 포트 및 스캐너 리디렉션 기능
 - 가상 인쇄
 - HTML5 MMR
 - Windows Media MMR: 성능 카운터는 VVC(VMware 가상 채널)를 사용하도록 이 기능을 구성한 경우에만 나타납니다.
- Windows 클라이언트의 일시적 네트워크 손실 동안 네트워크 연속성이 유지됩니다.
- 32비트 색상이 가상 디스플레이를 위해 지원됩니다.
- ClearType 글꼴이 지원됩니다.
- LAN 및 WAN의 동적 오디오 품질 조정이 포함된 오디오 리디렉션이 지원됩니다.
- 일부 클라이언트 유형에서 웹캠 및 마이크를 사용할 수 있도록 실시간 오디오-비디오가 지원됩니다.

- 클라이언트 운영 체제와 원격 데스크톱 또는 게시된 애플리케이션 간의 텍스트와 이미지(일부 클라이언트) 복사 및 붙여넣기가 지원됩니다. 다른 클라이언트 유형에서는 일반 텍스트 복사 및 붙여넣기만 지원됩니다. 시스템 사이에서 폴더 및 파일과 같은 시스템 개체를 복사하고 붙여 넣을 수 없습니다.
- 일부 클라이언트 유형에서 다중 모니터가 지원됩니다. 일부 클라이언트에서는 디스플레이당 해상도가 최대 2560 x 1600인 모니터를 최대 4대까지 사용하거나, Aero를 사용하지 않도록 설정된 Windows 7 원격 데스크톱의 경우 해상도가 최대 4K(3840 x 2160)인 모니터를 최대 3대까지 사용할 수 있습니다. 피벗 디스플레이 및 자동 맞춤도 지원됩니다.

3D 기능을 사용하도록 설정된 경우에는 최대 1920 x 1200 해상도를 사용하는 최대 2대의 모니터나 해상도가 4K(3840 x 2160)인 모니터 1대가 지원됩니다.

- 일부 클라이언트 유형에서 USB 리디렉션이 지원됩니다.
- MMR 리디렉션은 일부 Windows 클라이언트 운영 체제와 일부 원격 데스크톱 운영 체제(Horizon Agent 설치)에서 지원됩니다.
- NVIDIA 그래픽 카드를 사용하면 모니터가 연결되지 않은 물리적 시스템에 연결할 수 있습니다. 최고의 성능을 위해 H.264 인코딩을 지원하는 그래픽 카드를 사용하십시오.

추가 분리형 GPU와 내장된 GPU가 있는 경우 운영 체제에서는 내장된 GPU를 기본값으로 설정할 수 있습니다. 이 문제를 해결하기 위해 디바이스 관리자에서 디바이스를 사용하지 않도록 설정하거나 제거할 수 있습니다. 문제가 지속되는 경우 내장된 GPU에 대해 WDDM 그래픽 드라이버를 설치하거나 시스템 BIOS에서 내장된 GPU를 사용하지 않도록 설정할 수 있습니다. 내장된 GPU를 사용하지 않도록 설정하는 방법은 시스템 설명서를 참조하십시오.

경고 내장된 GPU를 사용하지 않도록 설정하면 향후 BIOS 설정 또는 NT 부팅 로더에 대한 콘솔 액세스와 같은 기능에 대한 액세스를 잃게 될 수 있습니다.

- Blast 코덱은 좀 더 선명한 이미지와 글꼴을 전달하여 데스크톱 사용에서 적응형 및 H.264 인코더의 기능을 개선하며 동작 감지, 동작 벡터 및 예측된 인터 매크로 블록이 있는 비디오 코덱처럼 작동합니다. 이 코덱은 다음 환경에서 지원되며 기본적으로 사용하지 않도록 설정됩니다.
 - Windows 및 Linux 에이전트. 이 코덱을 사용하도록 설정하려면:
 - Windows 에이전트에서 레지스트리 키를 설정합니다. HKLM\SOFTWARE\VMware, Inc.\VMware Blast\WConfig\EncoderBlastCodecEnabled = 1
 - Linux 에이전트의 `Wetc\Wvmware\Wconfig` 아래에서 `RemoteDisplay.allowBlastCodec=TRUE`를 설정합니다.
- Windows, Linux 및 MacOS 클라이언트 설정에서 H.264를 사용하지 않도록 설정합니다. 이 기능은 모바일 클라이언트 및 웹 클라이언트에서 지원되지 않습니다.
- 동적 인코더 스위치를 사용하면 비디오 최적화 인코더(H.264 4:2:0 또는 H.264 4:4:4)와 텍스트 최적화 인코더(Blast 코덱 또는 적응형) 간을 전환할 수 있습니다. 이 스위치를 사용하면 대역폭 사용량이 감소하는 선명한 텍스트 및 비디오를 유지할 수 있습니다. 이 기능을 사용하려면 인코더 스위치를 사용하도록 설정합니다.
 - Windows 에이전트에서 레지스트리 키를 설정합니다. HKLM\SOFTWARE\VMware, Inc.\VMware Blast\WConfig\EncoderSwitchEnabled = 1

- Linux 에이전트의 `WetcWvmwareWconfig` 아래에서 `RemoteDisplay.allowSwitchEncoder=TRUE`를 설정합니다.
- 기본적으로 사용하지 않도록 설정되는 Blast 코덱을 사용하도록 설정합니다. Blast 코덱을 사용하지 않도록 설정하면 스위치 인코더는 텍스트 최적화 인코딩을 위해 적응형을 사용합니다.
- Windows, Linux 및 MacOS 클라이언트 설정에서 H.264를 사용하도록 설정합니다. 이 기능은 모바일 클라이언트 및 웹 클라이언트에서 지원되지 않습니다.

참고 인코더 스위치는 소프트웨어 H.264를 사용하며 하드웨어 가속 그래픽을 지원하지 않습니다.

특정 VMware Blast Extreme 기능을 지원하는 클라이언트 디바이스에 대한 자세한 내용은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>에 나와 있습니다.

Wake-on-LAN

Wake-on-LAN은 Windows 10 RS4의 엔터프라이즈 에디션 이상을 갖춘 물리적 시스템에서 지원됩니다. 이 기능을 통해 사용자는 Horizon Connection Server을(를) 사용하여 연결할 때 물리적 시스템을 잠금 해제할 수 있습니다. Wake-on-LAN 기능에는 다음과 같은 사전 요구 사항이 있습니다.

- Wake-on-LAN(WoL)은 IPv4 환경에서만 지원됩니다.
- Wake-on-LAN은 네트워크 카드 설정뿐 아니라 BIOS 설정에서 사용하도록 설정하면 물리적 시스템을 구성하여 Wake-on-LAN 패킷을 받도록 잠금 해제해야 합니다.
- 대상 포트 9는 연결 서버에서 WoL 패킷에 대해 사용됩니다.
- WoL 패킷은 IP 전달 브로드캐스트 패킷으로서 Horizon Connection Server에서 전송하는 경우 Horizon Agent에 연결할 수 있어야 합니다. 이러한 시나리오에서 Wake-on-LAN 기능:
 - 물리적 시스템에 있는 연결 서버 및 Horizon Agent은(는) LAN 환경에서 동일한 서브넷에 있습니다.
 - 연결 서버와 Horizon Agent간의 모든 라우터는 구성됩니다. 이를 통해 잠금 해제하려는 물리적 시스템의 대상 서브넷에 대해 IP 전달 브로드캐스트 패킷을 허용합니다.

참고 Wake-on-LAN 기능은 물리적 Windows 10 에이전트의 부동 할당 풀을 지원하지 않습니다. 특정 사용자에게 권한이 부여된 전용 할당 풀로만 WoL 패킷이 전송됩니다.

권장된 게스트 운영 체제 설정

고화질 또는 전체 화면 모드로 재생하거나 720p 이상 형식 비디오를 재생하려면 1GB RAM 이상 및 이중 CPU를 사용하는 것이 좋습니다. CAD 애플리케이션 같은 그래픽 위주의 애플리케이션에 vDGA(Virtual Dedicated Graphics Acceleration)를 사용하려면 4GB의 RAM이 필요합니다.

비디오 품질 요구 사항

480p 형식 비디오

원격 데스크톱에 단일 가상 CPU가 있는 경우 기본 해상도에서 480p 이하로 비디오를 재생할 수 있습니다. 고화질 Flash 또는 전체 화면 모드로 비디오를 재생하려는 경우 데스크톱에 이중 가상 CPU가 필요합니다. 이

중 가상 CPU 데스크톱을 사용하더라도 최소 360p 형식 비디오를 전체 화면 모드로 재생하면 특히 Windows 클라이언트에서 비디오가 오디오보다 늦게 재생될 수 있습니다.

720p 형식 비디오

원격 데스크톱에 이중 가상 CPU가 있는 경우 기본 해상도에서 720p로 비디오를 재생할 수 있습니다. 고화질 또는 전체 화면 모드로 720p에서 비디오를 재생할 경우 성능이 영향을 받을 수 있습니다.

1080p 형식 비디오

원격 데스크톱에 이중 가상 CPU가 있는 경우 미디어 플레이어의 창 크기를 더 작게 조정해야 할 수도 있지만 1080p 형식 비디오를 재생할 수 있습니다.

3D 렌더링

소프트웨어 또는 하드웨어 가속 그래픽을 사용하도록 원격 데스크톱을 구성할 수 있습니다. 소프트웨어 가속 그래픽 기능을 사용하면 물리적 GPU(그래픽 처리 장치)가 없어도 DirectX 9 및 OpenGL 2.1 애플리케이션을 실행할 수 있습니다. 하드웨어 가속 그래픽 기능을 사용하면 가상 시스템이 vSphere 호스트의 물리적 GPU(그래픽 처리 장치)를 공유하거나 물리적 GPU를 단일 가상 데스크톱 전용으로 사용할 수 있습니다.

3D 애플리케이션의 경우 최대 2대의 모니터가 지원되며 최대 화면 해상도는 1,920 x 1,200입니다. 원격 데스크톱의 게스트 운영 체제는 Windows 7 이상이어야 합니다.

클라이언트 시스템의 하드웨어 요구 사항

특정 유형의 데스크톱 또는 모바일 클라이언트 디바이스에 대한 프로세서 및 메모리 요구 사항에 대한 내용은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>에 나와 있습니다.

IPv6 환경에 Horizon 7 설치

3

Horizon 7는 IPv4의 대체로 IPv6을 지원합니다. 사용하는 환경은 IPv6 전용 또는 IPv4 전용 환경이어야 합니다. Horizon 7는 IPv6과 IPv4가 혼재된 환경을 지원하지 않습니다.

IPv4 환경에서 지원되는 Horizon 7 기능 중 일부는 IPv6 환경에서 지원되지 않습니다. Horizon 7는 IPv4 환경에서 IPv6 환경으로의 업그레이드를 지원하지 않습니다. 또한 Horizon 7는 IPv4 환경과 IPv6 환경 사이의 마이그레이션을 지원하지 않습니다.

중요 Horizon 7를 IPv6 환경에서 실행하려면 모든 Horizon 7 구성 요소의 설치 시 IPv6을 지정해야 합니다.

본 장은 다음 항목을 포함합니다.

- [IPv6 환경에서 Horizon 7 설정](#)
- [IPv6 환경에서 지원되는 vSphere 데이터베이스 및 Active Directory 버전](#)
- [IPv6 환경에서 Horizon 7 서버를 지원하는 운영 체제](#)
- [IPv6 환경에서 데스크톱 및 RDS 호스트에 지원되는 Windows 운영 체제](#)
- [IPv6 환경에서 지원되는 클라이언트](#)
- [IPv6 환경에서 지원되는 원격 프로토콜](#)
- [IPv6 환경에서 지원되는 인증 유형](#)
- [IPv6 환경에서 지원되는 기타 기능](#)

IPv6 환경에서 Horizon 7 설정

IPv6 환경에서 Horizon 7를 실행하려면 특정 관리 작업을 수행할 때 IPv6에만 해당하는 요구 사항과 선택 사항을 알고 있어야 합니다.

Horizon 7를 설치하려면 먼저 작업 중인 IPv6 환경이 있어야 합니다. 다음과 같은 Horizon 7 관리 작업에는 IPv6에만 해당하는 옵션이 있습니다.

- Horizon 연결 서버 설치. [새 구성을 사용하여 Horizon 연결 서버 설치](#)의 내용을 참조하십시오.
- View 복제 서버 설치. [Horizon 연결 서버의 복제된 인스턴스 설치](#)의 내용을 참조하십시오.
- View 보안 서버 설치. [보안 서버 설치](#)의 내용을 참조하십시오.

- PCoIP 외부 URL 구성. [보안 게이트웨이 및 터널 연결용 외부 URL 구성](#)의 내용을 참조하십시오.
- PCoIP 외부 URL 설정. [연결 서버 인스턴스의 외부 URL 설정](#)의 내용을 참조하십시오.
- PCoIP 외부 URL 수정. [연결 서버 인스턴스의 외부 URL 설정](#)의 내용을 참조하십시오.
- Horizon Agent 설치. "데스크톱 및 애플리케이션 풀 설정" 문서에서 Horizon Agent 설치 항목을 참조하십시오.
- Horizon Client 설치. [IPv6 환경에서 지원되는 클라이언트](#)의 내용을 참조하십시오.

참고 Horizon 7에서는 그 어떤 관리 작업에도 IPv6 주소를 입력할 필요가 없습니다. FQDN(정규화된 도메인 이름)과 IPv6 주소 중에서 선택하여 지정할 수 있는 경우에는 잠재적인 오류를 방지하기 위해 FQDN을 지정하는 것이 좋습니다.

IPv6 환경에서 지원되는 vSphere 데이터베이스 및 Active Directory 버전

IPv6 환경에서 Horizon 7는 특정 vSphere, 데이터베이스 서버 및 Active Directory 버전을 지원합니다.

SQL Server 2012 이상 및 Oracle 11g 이상 데이터베이스는 IPv6 환경에서 지원됩니다. IPv6 환경에서 지원되는 데이터베이스, vSphere 버전 및 Active Directory 버전에 대한 최신 정보는 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php에서 VMware 제품 상호운용성 매트릭스를 참조하십시오.

IPv6 환경에서 Horizon 7 서버를 지원하는 운영 체제

IPv6 환경에서는 Horizon 7 서버를 특정 Windows Server 운영 체제에 설치해야 합니다.

Horizon 7 서버에는 연결 서버 인스턴스, 복제 서버, 보안 서버 및 Horizon 7 Composer 인스턴스가 포함됩니다.

운영 체제	버전
Windows Server 2016	Standard, Enterprise
Windows Server 2008 R2 SP1	Standard, Enterprise
Windows Server 2012 R2	Standard

IPv6 환경에서 데스크톱 및 RDS 호스트에 지원되는 Windows 운영 체제

IPv6 환경에서 Horizon 7는 데스크톱 시스템 및 RDS 호스트에 대해 특정 Windows 운영 체제를 지원합니다. RDS 호스트는 세션 기반의 데스크톱과 애플리케이션을 사용자에게 제공합니다.

지원되는 게스트 운영 체제의 유형 및 버전은 Windows 버전에 따라 다릅니다. 지원되는 Windows 10 운영 체제 목록 업데이트를 보려면 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2149393>을 참조하십시오. Windows 10 이외의 Windows 운영 체제의 경우 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2150295>를 참조하십시오.

Horizon Agent가 설치된 Windows 운영 체제에서 지원되는 특정 원격 환경 기능 목록을 보려면 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2150305>를 참조하십시오.

IPv6 환경에서 지원되는 클라이언트

IPv6 환경에서 Horizon 7는 특정 데스크톱 운영 체제에서 실행되는 클라이언트를 지원합니다.

표 3-1. 지원되는 Windows 운영 체제

운영 체제	버전	버전
Windows 7 및 Windows 7 SP1	32비트 또는 64비트	Home, Enterprise, Professional 및 Ultimate
Windows 8 및 Windows 8.1	32비트 또는 64비트	Pro, Enterprise 및 Industry Embedded
Windows 10	32비트 또는 64비트	Home, Pro, Pro for Workstations, Enterprise 및 IoT Enterprise

iOS 디바이스의 경우 iOS용 Horizon Client 4.1 이상에서 iOS 9.2 이상이 지원됩니다.

macOS 디바이스의 경우 Mac용 Horizon Client 4.9 이상이 필요합니다.

Android 디바이스의 경우 Android용 Horizon Client 4.9 이상이 필요합니다.

Chromebook 디바이스의 경우 Android용 Horizon Client 5.1 이상이 필요합니다.

지원되지 않는 클라이언트는 다음과 같습니다.

- Linux용 Horizon Client, Chrome용 Horizon Client, Chrome OS용 Horizon Client, Windows 10 UWP용 Horizon Client, Windows 스토어용 Horizon Client.
- PCoIP 제로 클라이언트

IPv6 환경에서 지원되는 원격 프로토콜

IPv6 환경에서 Horizon 7는 특정 원격 프로토콜을 지원합니다.

다음 원격 프로토콜이 지원됩니다.

- RDP
- 보안 터널을 사용하는 RDP
- PCoIP
- PCoIP 보안 게이트웨이를 통한 PCoIP
- VMware Blast

- Blast 보안 게이트웨이를 통한 VMware Blast
- BEAT(Blast Extreme Adaptive Transport)

IPv6 환경에서 지원되는 인증 유형

IPv6 환경에서 Horizon 7는 특정 인증 유형을 지원합니다.

다음 인증 유형이 지원됩니다.

- Active Directory를 사용하는 암호 인증
- 스마트 카드
- Single Sign-On

다음 인증 유형은 지원되지 않습니다.

- SecurID
- RADIUS
- SAML

IPv6 환경에서 지원되는 기타 기능

IPv6 환경에서 Horizon 7는 이전 항목에서 다루지 않은 특정 기능을 지원합니다.

지원되는 기능은 다음과 같습니다.

- 애플리케이션 풀
- 오디오 출력
- 전체 가상 시스템, 인스턴스 클론 또는 Horizon 7 Composer 연결된 클론의 자동화된 데스크톱 풀
- BEAT(Blast Extreme Adaptive Transport)
- CEIP(고객 환경 향상 프로그램)
- 디스크 공간 회수
- 이벤트
- VMware Horizon 성능 추적기
- HTML5 멀티미디어 리디렉션
- 인스턴트 클론 데스크톱 풀
- LDAP 백업
- vCenter Server를 통해 관리되지 않는 vCenter Server 가상 시스템, 물리적 컴퓨터 및 가상 시스템을 포함한 수동 데스크톱 풀
- 기본 NFS 스냅샷(VAAI)

- 개인 설정 관리
- 실시간 오디오-비디오(RTAV)
- RDS 데스크톱 풀
- RDS 호스트 3D
- 역할 기반 관리
- 세션 공동 작업
- 현재 사용자로 로그인 기능을 포함한 Single Sign-On
- 시스템 상태 대시보드
- ThinApp
- Unity Touch
- USB 리디렉션
- Horizon 7 Composer Agent
- Horizon 7 Storage Accelerator
- Horizon 7 Composer 데이터베이스 백업
- 가상 인쇄
- VMware 오디오
- VMware 비디오
- 비즈니스용 Skype에 대한 VMware Virtualization Pack(Windows만 해당)

지원되지 않는 기능은 다음과 같습니다.

- 클라이언트 드라이브 리디렉션
- 클라이언트 IP 투명성(64비트만)
- Cloud Pod 아키텍처
- 디바이스 브리지
- 파일 연결
- 플래시 URL 리디렉션
- HTML Access
- Log Insight
- Lync
- RDSH 인스턴트 클론 풀을 포함하는 PCoIP
- 스캐너 리디렉션
- 직렬 포트 리디렉션

- Syslog
- Teradici TERA 호스트 카드
- TSMRR
- URL 리디렉션
- vSAN
- 가상 볼륨
- vRealize Operations Desktop Agent

FIPS 모드에서 Horizon 7 설치

4

Horizon 7에서 FIPS(Federal Information Processing Standard) 140-2 준수 알고리즘을 사용하여 암호화 작업을 수행할 수 있습니다. Horizon 7을 FIPS 모드에서 설치하면 이러한 알고리즘을 사용하도록 설정할 수 있습니다.

모든 Horizon 7 기능이 FIPS 모드에서 지원되는 것은 아닙니다. 또한 Horizon 7은 비 FIPS 설치에서 FIPS 설치로 업그레이드하는 것을 지원하지 않습니다.

참고 Horizon 7이 FIPS 모드에서 실행되도록 하려면 모든 Horizon 7 구성 요소를 설치할 때 FIPS를 사용하도록 설정해야 합니다.

본 장은 다음 항목을 포함합니다.

- FIPS 모드의 Horizon 7 설정 개요
- FIPS 모드의 시스템 요구 사항

FIPS 모드의 Horizon 7 설정 개요

Horizon 7을 FIPS 모드에서 설정하려면 먼저 Windows 환경에서 FIPS 모드를 사용하도록 설정해야 합니다. 그런 다음 FIPS 모드에서 모든 Horizon 7 구성 요소를 설치합니다.

Horizon 7을 FIPS 모드에서 설치하는 옵션은 Windows 환경에서 FIPS 모드를 사용하도록 설정된 경우에만 사용할 수 있습니다. Windows에서 FIPS 모드를 활성화하는 방법에 대한 자세한 내용은 <https://support.microsoft.com/en-us/kb/811833>을 참조하십시오.

참고 Horizon Administrator에서는 Horizon 7이 FIPS 모드에서 실행되는지 여부를 표시하지 않습니다.

Horizon 7을 FIPS 모드에서 설치하려면 다음 관리 작업을 수행하십시오.

- 연결 서버를 설치할 때 FIPS 모드 옵션을 선택합니다. [새 구성을 사용하여 Horizon 연결 서버 설치](#)를 참조하십시오.
- 복제 서버를 설치할 때 FIPS 모드 옵션을 선택합니다. [Horizon 연결 서버의 복제된 인스턴스 설치](#)를 참조하십시오.

- 보안 서버를 설치하기 전에 Horizon Administrator에서 전역 설정 **보안 서버 연결용 IPSec 사용**을 선택 취소하고 수동으로 IPsec를 구성합니다. <http://kb.vmware.com/kb/2000175>을 참조하십시오.
- 보안 서버를 설치할 때 FIPS 모드 옵션을 선택합니다. **보안 서버 설치**를 참조하십시오.
- Windows 시스템이 FIPS 작업에 대해 구성되고 Horizon 7이 연결 서버와 IPSec 보안 서버 간에 통신이 수행되도록 구성되면 보안 서버를 설치하지 못합니다. IPv4 환경에서는 IP 주소와 포트 번호 4172를 사용하여 PCoIP 외부 URL을 지정합니다. IPv6 환경에서는 IP 주소 또는 정규화된 도메인 이름과 함께 포트 번호 4172를 지정할 수 있습니다. 두 경우 모두 프로토콜 이름은 포함하지 않습니다.

IPv4 환경의 예: 10.20.30.40:4172

클라이언트는 이 URL을 사용하여 보안 서버에 액세스할 수 있어야 합니다.

- View Composer 및 Horizon Agent 시스템에서 취약한 암호를 사용하지 않도록 설정합니다. **SSL/TLS에서 취약한 암호 사용 안 함**를 참조하십시오.
- View Composer를 설치할 때 FIPS 모드 옵션을 선택합니다. **장 6 View Composer 설치**를 참조하십시오.
- Horizon Agent를 설치할 때 FIPS 모드 옵션을 선택합니다. "Horizon 7에서 가상 데스크톱 설정" 또는 "Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정" 문서에서 Horizon Agent 설치 항목을 참조하십시오.
- Windows 클라이언트의 경우 클라이언트 운영 체제에서 FIPS 모드를 사용하도록 설정하고 Windows용 Horizon Client를 설치할 때 FIPS 모드 옵션을 선택합니다. "Windows용 VMware Horizon Client 설치 및 설정 가이드" 문서를 참조하십시오.
- Linux 클라이언트의 경우 클라이언트 운영 체제에서 FIPS 모드를 사용하도록 설정합니다. "Linux용 VMware Horizon Client 설치 및 설정 가이드" 문서를 참조하십시오.

FIPS 모드의 시스템 요구 사항

FIPS 모드를 지원하려면 Horizon 7 배포가 다음 요구 사항을 충족해야 합니다.

vSphere

- vCenter Server 6.0 이상
- ESXi 6.0 이상

원격 데스크톱

- FIPS 인증서가 있는 모든 Windows 플랫폼입니다. 자세한 내용은 Microsoft TechNet 웹 사이트에서 "FIPS 140 유효성 검사"를 참조하십시오.
- View Agent 6.2 이상 또는 Horizon Agent 7.0 이상, Windows 플랫폼 전용

Horizon Client

- FIPS 인증서가 있는 모든 Windows 플랫폼입니다. 자세한 내용은 Microsoft TechNet 웹 사이트에서 "FIPS 140 유효성 검사"를 참조하십시오.

암호화 프로토콜

- Windows용 Horizon Client 3.5 이상
- TLSv1.2

Active Directory 준비

5

Horizon 7는 사용자의 기존 Microsoft Active Directory 인프라를 통해 사용자를 인증하고 관리합니다. 특정 작업을 수행하여 Horizon 7과 함께 사용할 Active Directory를 준비해야 합니다.

Horizon 7는 다음 AD DS(Active Directory 도메인 서비스) 도메인 기능 수준을 지원합니다.

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

본 장은 다음 항목을 포함합니다.

- 도메인 및 신뢰 관계 구성
- 원격 데스크톱의 OU 생성
- 키오스크 모드 클라이언트 계정을 위한 OU 및 그룹 생성
- 사용자 그룹 생성
- vCenter Server의 사용자 계정 생성
- 독립 실행형 View Composer Server의 사용자 계정 생성
- View Composer AD 작업을 위한 사용자 계정 생성
- 인스턴트 클론 작업을 위한 사용자 계정 만들기
- 제한된 그룹 정책 구성
- Horizon 7 그룹 정책 관리 템플릿 파일 사용
- 스마트 카드 인증을 위한 Active Directory 준비
- SSL/TLS에서 취약한 암호 사용 안 함

도메인 및 신뢰 관계 구성

각 연결 서버 호스트를 Active Directory 도메인에 가입시켜야 합니다. 호스트를 도메인 컨트롤러로 사용하면 안 됩니다.

또한 Active Directory는 단일 사용자 시스템 및 RDS 호스트를 비롯한 Horizon Agent 시스템과, Horizon 7 배포의 사용자 및 그룹을 관리합니다. 사용자 및 그룹에 원격 데스크톱 및 애플리케이션에 대한 권한을 부여하고 Horizon Administrator에서 관리자가 될 사용자 및 그룹을 선택할 수 있습니다.

다음 Active Directory 도메인에 Horizon Agent 시스템, View Composer 서버 및 사용자와 그룹을 배치할 수 있습니다.

- 연결 서버 도메인
- 연결 서버 도메인과 양방향 신뢰 관계가 있는 다른 도메인
- 연결 서버 도메인과 단방향 외부 또는 영역 신뢰 관계에 있지만 이 연결 서버 도메인이 포함되어 있지 않은 다른 포리스트에 있는 도메인
- 연결 서버 도메인과 단방향 또는 양방향 전이적 포리스트 신뢰 관계에 있지만 이 연결 서버 도메인이 포함되어 있지 않은 다른 포리스트에 있는 도메인

사용자는 Active Directory를 사용하여 연결 서버 도메인 및 신뢰 계약이 존재하는 모든 추가 사용자 도메인에 대해 인증됩니다.

사용자 및 그룹이 신뢰할 수 있는 단방향 도메인에 있는 경우 Horizon Administrator에서 관리자 사용자에게 대한 보조 자격 증명을 제공해야 합니다. 관리자는 이러한 사용자에게 신뢰할 수 있는 단방향 도메인에 대한 액세스 권한을 제공하려면 보조 자격 증명에 있어야 합니다. 신뢰할 수 있는 단방향 도메인은 외부 도메인이거나 전이적 포리스트 신뢰 관계에 있는 도메인일 수 있습니다.

보조 자격 증명은 최종 사용자의 데스크톱 또는 애플리케이션 세션이 아니라 Horizon Administrator 세션에만 필요합니다. 관리자 사용자만 보조 자격 증명에 필요합니다.

vdmadmin -T 명령을 사용하여 보조 자격 증명을 제공할 수 있습니다.

- 개별 관리자에 대해 보조 자격 증명을 구성합니다.
- 포리스트 신뢰의 경우 포리스트 루트 도메인에 대해 보조 자격 증명을 구성할 수 있습니다. 그러면 연결 서버는 포리스트 신뢰 관계에 있는 하위 도메인을 열거할 수 있습니다.

자세한 내용은 "Horizon 7 관리" 문서의 "-T 옵션을 사용하여 관리자에게 보조 자격 증명 제공"을 참조하십시오.

신뢰할 수 있는 단방향 도메인에서는 스마트 카드 및 사용자의 SAML 인증이 지원되지 않습니다.

Horizon 7 버전 7.10부터 Windows용 Horizon Client의 [현재 사용자로 로그인] 기능이 신뢰할 수 있는 단방향 도메인에서 지원됩니다.

참고 보안 서버는 Active Directory를 포함한 어떤 인증 저장소에도 액세스하지 않으므로 Active Directory 도메인에 있지 않아도 됩니다.

신뢰 관계 및 도메인 필터링

액세스할 수 있는 도메인을 결정하기 위해 연결 서버 인스턴스는 도메인부터 시작하여 신뢰 관계를 탐색합니다.

규모가 작고 서로 잘 연결되어 있는 도메인 집합의 경우 연결 서버는 신속하게 도메인 전체 목록을 확인할 수 있지만 도메인 수가 증가하거나 도메인 간의 연결성이 떨어질수록 확인하는 데 더 많은 시간이 걸립니다. 목록에는 사용자가 원격 데스크톱 및 애플리케이션에 연결할 때 사용자에게 제공하기 원하지 않는 도메인이 포함될 수도 있습니다.

vdmadmin 명령을 사용해 도메인 필터링을 구성함으로써 연결 서버 인스턴스에서 검색하고 사용자에게 표시하는 도메인을 제한할 수 있습니다. 자세한 내용은 "Horizon 7 관리" 문서를 참조하십시오.

포리스트 신뢰가 이름 접미사 제외를 사용하여 구성된 경우 구성된 예외가 포리스트 하위 도메인 목록을 필터링하는 데 사용됩니다. vdmadmin 명령으로 지정된 필터링 외에 이름 접미사 제외 필터링이 적용됩니다.

원격 데스크톱의 OU 생성

원격 데스크톱에 대해 특별히 OU(조직 단위)를 생성해야 합니다. OU는 사용자, 그룹, 컴퓨터 또는 OU를 포함하고 있는 Active Directory의 하위 분류 단위입니다.

데스크톱과 동일한 도메인에 있는 다른 Windows 서버 또는 워크스테이션에 그룹 정책 설정을 적용하지 않으려면 Horizon 7 그룹 정책의 GPO를 생성하고 원격 데스크톱을 포함하고 있는 OU에 연결하면 됩니다. 서버 운영자 또는 개인 사용자 등과 같은 종속 그룹에 OU 제어 권한을 위임할 수 있습니다.

View Composer를 사용하는 경우 연결된 클론 데스크톱에 대해 원격 데스크톱의 OU를 기반으로 하는 개별 Active Directory 컨테이너를 생성해야 합니다. Active Directory에서 OU 관리자 권한을 가지고 있는 관리자는 도메인 관리자 권한 없이 연결된 클론 데스크톱을 프로비저닝할 수 있습니다.

Active Directory의 관리자 자격 증명을 변경하면 View Composer의 자격 증명 정보도 업데이트해야 합니다.

키오스크 모드 클라이언트 계정을 위한 OU 및 그룹 생성

키오스크 모드의 클라이언트는 잠금 PC 또는 쉘 클라이언트이며, 클라이언트 소프트웨어를 실행해 연결 서버 인스턴스에 연결하고 원격 데스크톱 세션을 시작합니다. 키오스크 모드에서 클라이언트를 구성하면 키오스크 모드 클라이언트 계정을 위해 Active Directory에서 전용 OU 및 그룹을 생성해야 합니다.

키오스크 모드 클라이언트 계정의 전용 OU 및 그룹을 생성하면 허가 받지 않은 침입으로부터 클라이언트 시스템을 보호하고, 클라이언트 구성과 관리를 간소화할 수 있습니다.

자세한 내용은 "Horizon 7 관리" 문서를 참조하십시오.

사용자 그룹 생성

Active Directory에서 서로 다른 사용자 유형에 대해 그룹을 생성해야 합니다. 예를 들어 최종 사용자에 대해 Horizon 7 Users라는 그룹을 생성하고 원격 데스크톱 및 애플리케이션을 관리할 사용자에게 대해 Horizon 7 Administrator라는 또 다른 그룹을 생성할 수 있습니다.

vCenter Server의 사용자 계정 생성

vCenter Server에서 사용하기 위해 Active Directory에 사용자 계정을 생성해야 합니다. Horizon Administrator에서 vCenter Server 인스턴스를 추가할 때 이 사용자 계정을 지정합니다.

vCenter Server에서 특정 작업을 수행할 수 있도록 사용자 계정 권한을 부여해야 합니다. 적절한 권한이 있는 vCenter Server 역할을 생성한 후 해당 역할을 vCenter Server 사용자에게 할당할 수 있습니다. View Composer와 함께 또는 View Composer 없이 Horizon 7을 사용하는지에 따라 vCenter Server 역할에 추가하는 권한 목록이 다릅니다. 이러한 권한 구성에 대한 자세한 내용은 [vCenter Server, View Composer 및 인스턴트 클론에 대한 사용자 계정 구성](#)에 나와 있습니다.

View Composer를 vCenter Server와 동일한 시스템에 설치하는 경우 vCenter Server 사용자를 vCenter Server 시스템의 로컬 관리자 그룹에 추가해야 합니다. 이러한 요구 사항에 따라 Horizon 7가 View Composer 서비스에 인증할 수 있습니다.

View Composer를 vCenter Server와 다른 시스템에 설치하는 경우 vCenter Server 사용자를 vCenter Server 시스템의 로컬 관리자 그룹에 만들지 않아도 됩니다. 그러나 View Composer 시스템의 로컬 관리자여야 하는 독립 실행형 View Composer Server 사용자 계정을 생성해야 합니다.

독립 실행형 View Composer Server의 사용자 계정 생성

View Composer를 vCenter Server와 다른 시스템에 설치하는 경우 Horizon 7가 독립 실행형 시스템의 View Composer 서비스에 인증하는 데 사용할 수 있는 Active Directory의 도메인 사용자 계정을 생성해야 합니다.

사용자 계정은 연결 서버 호스트와 같은 도메인 또는 신뢰할 수 있는 도메인에 있어야 합니다. 사용자 계정을 독립 실행형 View Composer 시스템의 로컬 관리자 그룹에 추가해야 합니다.

Horizon Administrator에서 View Composer 설정을 구성하고 **독립 실행형 View Composer Server**를 선택할 때 이 사용자 계정을 지정합니다. [View Composer 설정 구성](#)을 참조하십시오.

View Composer AD 작업을 위한 사용자 계정 생성

View Composer를 사용하는 경우 View Composer가 Active Directory에서 특정 작업을 수행하도록 허용하는 Active Directory의 사용자 계정을 생성해야 합니다. View Composer에서는 연결된 클론 가상 시스템을 Active Directory 도메인에 가입시키기 위해 이 계정을 필요로 합니다.

보안 상의 이유로 View Composer에서 사용할 사용자 계정을 별도로 생성해야 합니다. 별도 계정을 생성해 다른 용도로 정의된 추가 권한을 가지고 있지 않도록 보장할 수 있습니다. 특정 Active Directory 컨테이너에서 컴퓨터 개체를 생성 또는 제거하는데 필요한 최소 권한을 계정에 부여할 수 있습니다. 예를 들어 View Composer 계정에는 도메인 관리자 권한이 필요하지 않습니다.

절차

1 Active Directory에서 연결 서버 호스트와 동일한 도메인 또는 신뢰할 수 있는 도메인에서 사용자 계정을 생성하십시오.

2 연결된 클론 컴퓨터 계정을 생성하거나 연결된 클론 컴퓨터 계정을 이동한 Active Directory 컨테이너 계정에 **컴퓨터 개체 생성**, **컴퓨터 개체 삭제** 및 **모든 속성 쓰기** 사용 권한을 추가하십시오.

다음 목록은 기본으로 할당된 사용 권한을 포함해 사용자 계정에 필요한 모든 사용 권한을 보여줍니다.

- 목록 내용
- 모든 속성 읽기
- 모든 속성 쓰기
- 사용 권한 읽기
- 암호 재설정
- 컴퓨터 개체 생성
- 컴퓨터 개체 삭제

참고 데스크톱 풀에 대해 **기존 컴퓨터 계정의 재사용 허용** 설정을 선택하는 경우 보다 적은 사용 권한이 필요합니다. 다음과 같은 사용 권한이 사용자 계정에 할당되어 있는지 확인하십시오.

- 목록 내용
- 모든 속성 읽기
- 사용 권한 읽기
- 암호 재설정

3 Active Directory 컨테이너 및 컨테이너의 모든 하위 개체에 사용자 계정의 사용 권한을 적용했는지 확인하십시오.

다음에 수행할 작업

vCenter Server 추가 마법사에서 View Composer 도메인을 구성하거나 연결된 클론 데스크톱 풀을 구성 및 배포할 때 Horizon Administrator에서 계정을 지정하십시오.

인스턴트 클론 작업을 위한 사용자 계정 만들기

인스턴트 클론을 배포하기 전에 Active Directory에서 특정 작업을 수행할 수 있는 사용 권한이 있는 사용자 계정을 생성해야 합니다.

인스턴트 클론 데스크톱 풀을 배포하기 전에 인스턴트 클론 도메인 관리자를 추가할 때 이 계정을 선택합니다. 자세한 내용은 “Horizon 7에서 가상 데스크톱 설정” 문서에서 “인스턴트 클론 도메인 관리자 추가”를 참조하십시오.

절차

- 1 Active Directory에서 연결 서버와 동일한 도메인 또는 신뢰할 수 있는 도메인에서 사용자 계정을 생성합니다.
- 2 인스턴트 클론 컴퓨터 계정에 대한 컨테이너의 계정에 **컴퓨터 개체 생성**, **컴퓨터 개체 삭제** 및 **모든 속성 쓰기** 사용 권한을 추가합니다.

다음 목록은 기본으로 할당된 사용 권한을 포함해 사용자 계정에 필요한 사용 권한을 보여줍니다.

- 목록 내용
- 모든 속성 읽기
- 모든 속성 쓰기
- 사용 권한 읽기
- 암호 재설정
- 컴퓨터 개체 생성
- 컴퓨터 개체 삭제

올바른 컨테이너 및 컨테이너의 모든 하위 개체에 사용 권한을 적용했는지 확인합니다.

제한된 그룹 정책 구성

원격 데스크톱의 로컬 원격 데스크톱 사용자 그룹에 속해 있는 사용자만 원격 데스크톱에 연결할 수 있습니다. 도메인에 가입되어 있는 모든 원격 데스크톱의 로컬 원격 데스크톱 사용자 그룹에 Active Directory의 제한된 그룹 정책을 사용해 사용자 또는 그룹을 추가할 수 있습니다.

제한된 그룹 정책은 도메인에 있는 컴퓨터의 로컬 그룹 구성원 자격을 제한된 그룹 정책에 정의된 구성원 자격 목록 설정과 일치하도록 설정합니다. 원격 데스크톱 사용자 그룹의 구성원은 도메인에 가입된 모든 원격 데스크톱의 로컬 원격 데스크톱 사용자 그룹에 항상 추가됩니다. 새 사용자를 추가할 때는 원격 데스크톱 사용자 그룹에만 추가해야 합니다.

이러한 단계는 Horizon 7 가상 데스크톱 또는 게시된 데스크톱 및 애플리케이션이 가입된 도메인의 Active Directory 서버에 적용됩니다.

사전 요구 사항

Active Directory의 도메인에 원격 데스크톱 사용자 그룹을 생성합니다. 예를 들어 “Horizon Users” 라는 그룹을 생성합니다.

절차

- 1 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동하십시오.

AD 버전	탐색 경로
Windows 2003	<ol style="list-style-type: none"> a 시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터를 선택합니다. b 도메인을 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다. c 그룹 정책 탭에서 열기를 클릭하여 그룹 정책 관리 플러그인을 엽니다. d 기본 도메인 정책을 마우스 오른쪽 단추로 클릭하고 편집을 클릭합니다.
Windows 2008	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2012 R2	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2016	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.

- 2 컴퓨터 구성 섹션을 확장하고 **Windows Settings\Security Settings**를 여십시오.
- 3 마우스 오른쪽 단추로 **제한된 그룹**을 클릭하고 **그룹 추가**를 선택한 다음 원격 데스크톱 사용자 그룹을 추가하십시오.
- 4 그룹을 마우스 오른쪽 버튼으로 클릭하고 새 원격 데스크톱 사용자 그룹을 그룹 멤버 자격 목록에 추가합니다.

예를 들어 원격 데스크톱 사용자에 “Horizon Users”를 추가합니다.

- 5 변경 사항을 저장하려면 **확인**을 클릭합니다.

Horizon 7 그룹 정책 관리 템플릿 파일 사용

Horizon 7에는 여러 구성 요소 특정 그룹 정책 관리(ADMX) 템플릿 파일이 있습니다.

Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip에 있습니다. 여기서 x.x.x는 버전이고 yyyyyy는 빌드 번호입니다. <https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 파일을 다운로드할 수 있습니다. Desktop & End-User Computing에서 ZIP 파일이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

이러한 파일의 정책 설정을 Active Directory의 새 GPO 또는 기존 GPO에 추가한 다음 해당 GPO를 데스크톱이 포함된 OU에 연결하여 원격 데스크톱을 최적화하고 보호할 수 있습니다.

Horizon 7 그룹 정책 설정 사용에 관한 정보는 “Horizon 7 관리” 및 “Horizon 7에서 원격 데스크톱 기능 구성” 문서를 참조하십시오.

스마트 카드 인증을 위한 Active Directory 준비

스마트 카드 인증을 구현할 때 Active Directory에서 특정 작업을 수행해야 할 수 있습니다.

■ 스마트 카드 사용자의 UPN 추가

스마트 카드 로그인에서 UPN(사용자 계정 이름)을 사용하기 때문에 스마트 카드를 사용해 Horizon 7에서 인증을 받는 사용자 및 관리자의 Active Directory 계정에 UPN이 올바르게 구성되어 있어야 합니다.

■ 신뢰할 수 있는 루트 인증 기관에 루트 인증서 추가

인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 신뢰할 수 있는 루트 인증 기관 그룹 정책에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA로 사용하면 이 절차를 수행할 필요가 없습니다.

■ 중간 인증 기관에 중간 인증서 추가

중간 인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 중간 인증 기관 그룹 정책에 중간 인증서를 추가해야 합니다.

■ Enterprise NTAAuth 저장소에 루트 인증서 추가

CA를 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 Enterprise NTAAuth 저장소에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA로 사용하면 이 절차를 수행할 필요가 없습니다.

스마트 카드 사용자의 UPN 추가

스마트 카드 로그인에서 UPN(사용자 계정 이름)을 사용하기 때문에 스마트 카드를 사용해 Horizon 7에서 인증을 받는 사용자 및 관리자의 Active Directory 계정에 UPN이 올바르게 구성되어 있어야 합니다.

스마트 카드 사용자가 위치한 도메인이 루트 인증서를 발급한 도메인과 다르면 사용자의 UPN을 신뢰할 수 있는 CA의 루트 인증서에 포함된 SAN(주체 대체 이름)으로 설정해야 합니다. 스마트 카드 사용자의 현재 도메인에 있는 서버에서 루트 인증서를 발급한 경우 사용자의 UPN을 수정할 필요가 없습니다.

참고 같은 도메인에서 인증서를 발급한 경우에도 기본 Active Directory 계정에 대한 UPN을 설정해야 할 수 있습니다. 관리자를 포함해 기본 계정에는 UPN이 기본적으로 설정되지 않습니다.

사전 요구 사항

- 인증서 속성을 확인해 신뢰할 수 있는 CA의 루트 인증서에 포함된 SAN을 가져오십시오.
- Active Directory 서버에 ADSI 편집 유틸리티가 없으면 Microsoft 웹 사이트에서 적절한 Windows 지원 도구를 다운로드하여 설치하십시오.

절차

- 1 Active Directory 서버에서 ADSI 편집 유틸리티를 시작하십시오.
- 2 왼쪽 창에서 사용자가 위치한 도메인을 확장하고 CN=Users를 두 번 클릭합니다.

- 3 오른쪽 창에서 마우스 오른쪽 단추로 사용자를 클릭한 다음 **속성**을 클릭합니다.
- 4 userPrincipalName 특성을 두 번 클릭하고 신뢰할 수 있는 CA 인증서의 SAN 값을 입력하십시오.
- 5 특성 설정을 저장하려면 **확인**을 클릭합니다.

신뢰할 수 있는 루트 인증 기관에 루트 인증서 추가

인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 신뢰할 수 있는 루트 인증 기관 그룹 정책에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA로 사용하면 이 절차를 수행할 필요가 없습니다.

절차

- 1 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동하십시오.

AD 버전	탐색 경로
Windows 2003	<ol style="list-style-type: none"> a 시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터를 선택합니다. b 도메인을 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다. c 그룹 정책 탭에서 열기를 클릭하여 그룹 정책 관리 플러그인을 엽니다. d 기본 도메인 정책을 마우스 오른쪽 단추로 클릭하고 편집을 클릭합니다.
Windows 2008	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2012 R2	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2016	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.

- 2 컴퓨터 구성 섹션을 확장하고 **Windows 설정\보안 설정\공개 키**를 여십시오.
- 3 **신뢰할 수 있는 루트 인증 기관**을 마우스 오른쪽 버튼으로 클릭하고 **가져오기**를 선택합니다.
- 4 마법사에 표시된 메시지에 따라 루트 인증서(예: rootCA.cer)를 가져오고 **확인**을 클릭합니다.
- 5 그룹 정책 창을 닫습니다.

이제 도메인의 모든 시스템에서 신뢰할 수 있는 루트 저장소의 루트 인증서 복사본을 가지고 있습니다.

다음에 수행할 작업

중간 인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 중간 인증 기관 그룹 정책에 중간 인증서를 추가하십시오. [중간 인증 기관에 중간 인증서 추가](#)의 내용을 참조하십시오.

중간 인증 기관에 중간 인증서 추가

중간 인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 중간 인증 기관 그룹 정책에 중간 인증서를 추가해야 합니다.

절차

- 1 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동하십시오.

AD 버전	탐색 경로
Windows 2003	<ol style="list-style-type: none"> a 시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터를 선택합니다. b 도메인을 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다. c 그룹 정책 탭에서 열기를 클릭하여 그룹 정책 관리 플러그인을 엽니다. d 기본 도메인 정책을 마우스 오른쪽 단추로 클릭하고 편집을 클릭합니다.
Windows 2008	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2012 R2	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2016	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.

- 2 컴퓨터 구성 섹션을 확장하고 Windows 설정\보안 설정\공개 키에 대한 정책을 엽니다.
- 3 중간 인증 기관을 마우스 오른쪽 버튼으로 클릭하고 가져오기를 선택합니다.
- 4 마법사에 표시된 메시지에 따라 중간 인증서(예: intermediateCA.cer)를 가져오고 확인을 클릭합니다.
- 5 그룹 정책 창을 닫습니다.

이제 도메인의 모든 시스템에서 중간 인증 기관 저장소의 중간 인증서 복사본을 가지고 있습니다.

Enterprise NTAUTH 저장소에 루트 인증서 추가

CA를 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 Enterprise NTAUTH 저장소에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA로 사용하면 이 절차를 수행할 필요가 없습니다.

절차

- ◆ Enterprise NTAUTH 저장소에 인증서를 게시하려면 Active Directory 서버에서 `certutil` 명령을 사용하십시오.

예: `certutil -dspublish -f path_to_root_CA_cert NTAUTHCA`

이제 해당 CA에서 이러한 유형의 인증서를 신뢰하고 발급할 수 있습니다.

SSL/TLS에서 취약한 암호 사용 안 함

도메인 정책 GPO(그룹 정책 개체)를 구성하면 View Agent 또는 Horizon Agent를 실행하는 View Composer 및 Windows 기반 시스템에서 SSL/TLS 프로토콜을 사용하여 통신할 때 취약한 암호를 사용하지 않도록 함으로써 보안을 강화할 수 있습니다.

절차

- 1 Active Directory 서버에서, **시작 > 관리 도구 > 그룹 정책 관리**를 선택하고 GPO를 마우스 오른쪽 버튼으로 클릭한 다음 **편집**을 선택하여 GPO를 편집합니다.
- 2 그룹 정책 관리 편집기에서 **컴퓨터 구성 > 정책 > 관리 템플릿 > 네트워크 > SSL 구성 설정**으로 이동합니다.
- 3 **SSL Cipher Suite Order**를 두 번 클릭합니다.
- 4 SSL Cipher Suite Order 창에서 **사용**을 클릭합니다.
- 5 옵션 창에서 SSL Cipher Suite 텍스트 상자의 내용 전체를 다음 암호 목록으로 교체합니다.

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

암호 제품군은 읽기 쉽도록 별도의 행에 나열됩니다. 목록을 텍스트 상자에 붙여 넣을 때, 암호 제품군은 쉼표 뒤에 공백을 사용하지 않고 한 행에 넣어야 합니다.

- 6 그룹 정책 관리 편집기를 종료합니다.
- 7 View Composer 및 View Agent 또는 Horizon Agent 시스템을 다시 시작하여 새로운 그룹 정책을 적용합니다.

View Composer 설치

6

View Composer를 사용하려면 View Composer 데이터베이스를 생성하고 View Composer 서비스를 설치하고 View 인프라를 최적화하여 View Composer를 지원합니다. vCenter Server와 동일한 호스트 또는 별도 호스트에 View Composer 서비스를 설치할 수 있습니다.

View Composer는 선택 기능입니다. 연결된 클론 데스크톱 풀을 배포하려면 View Composer를 설치합니다.

View Composer 기능을 설치하고 사용하려면 라이선스가 있어야 합니다.

참고 View Composer를 설치하기 전에 Active Directory가 준비되었는지 확인합니다.

참고 vCenter Server 6.5가 설치된 동일한 시스템에 View Composer를 설치하는 경우 vCenter Server에서 View Composer가 다르게 작동할 수 있습니다. 자세한 내용은 다음 VMware 기술 자료 문서(<https://kb.vmware.com/s/article/2150066>)를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- View Composer 데이터베이스 준비
- View Composer를 위한 SSL 인증서 구성
- View Composer 서비스 설치
- View Composer에서 vCenter의 TLSv1.0 및 ESXi 연결 사용
- View Composer를 위한 인프라 구축

View Composer 데이터베이스 준비

데이터베이스 및 데이터 소스 이름(DSN)을 생성하여 View Composer 데이터를 저장해야 합니다.

View Composer 서비스에는 데이터베이스가 포함되지 않습니다. 네트워크 환경에 데이터베이스 인스턴스가 없으면 설치해야 합니다. 데이터베이스 인스턴스를 설치한 후 View Composer 데이터베이스를 인스턴스에 추가합니다.

View Composer 데이터베이스를 vCenter Server 데이터베이스가 지정된 인스턴스에 추가할 수 있습니다. 데이터베이스를 로컬로, 또는 네트워크 연결된 Linux, UNIX 또는 Windows Server 컴퓨터에서 원격으로 구성할 수 있습니다.

View Composer 데이터베이스는 View Composer에서 사용하는 연결 및 구성 요소에 대한 정보를 저장합니다.

- vCenter Server 연결
- Active Directory 연결
- View Composer에서 배포한 연결된 클론 데스크톱
- View Composer에서 생성된 복제본

View Composer 서비스의 각 인스턴스에는 고유의 View Composer 데이터베이스가 있어야 합니다. 여러 View Composer 서비스는 View Composer 데이터베이스를 공유할 수 없습니다.

지원되는 데이터베이스 버전 목록은 [View Composer 및 이벤트 데이터베이스의 데이터베이스 요구 사항](#)을 참조하십시오.

View Composer 데이터베이스를 설치된 데이터베이스 인스턴스에 추가하려면 이러한 절차 중 하나를 선택합니다.

■ View Composer용 SQL Server 데이터베이스 생성

View Composer는 연결된 클론 데스크톱 정보를 SQL Server 데이터베이스에 저장할 수 있습니다. SQL Server에 View Composer 데이터베이스를 추가하고 ODBC 데이터 소스를 구성하여 이를 생성합니다.

■ View Composer용 Oracle 데이터베이스 생성

View Composer는 연결된 클론 데스크톱 정보를 Oracle 12c 또는 11g 데이터베이스에 저장할 수 있습니다. 기존 Oracle 인스턴스에 View Composer 데이터베이스를 추가하고 ODBC 데이터 소스를 구성하여 생성합니다. Oracle 데이터베이스 구성 도우미를 사용하거나 SQL 문을 실행해 새 View Composer 데이터베이스를 추가할 수 있습니다.

View Composer용 SQL Server 데이터베이스 생성

View Composer는 연결된 클론 데스크톱 정보를 SQL Server 데이터베이스에 저장할 수 있습니다. SQL Server에 View Composer 데이터베이스를 추가하고 ODBC 데이터 소스를 구성하여 이를 생성합니다.

절차

1 SQL Server에 View Composer 데이터베이스 추가

기존 Microsoft SQL Server 인스턴스에 새 View Composer 데이터베이스를 추가해 View Composer의 연결된 클론 데이터를 저장할 수 있습니다.

2 (선택 사항) 수동으로 데이터베이스 역할을 생성하여 SQL Server 데이터베이스 사용 권한 설정

이 권장되는 방법을 사용하여 View Composer 데이터베이스 관리자는 Microsoft SQL Server 데이터베이스 역할을 통해 부여될 View Composer 관리자에 대한 권한을 설정할 수 있습니다.

3 SQL Server에 ODBC 데이터 소스 추가

SQL Server에 View Composer 데이터베이스를 추가한 후에 View Composer 서비스에서 이 데이터 소스를 볼 수 있도록 새 데이터베이스에 대한 ODBC 연결을 구성해야 합니다.

SQL Server에 View Composer 데이터베이스 추가

기존 Microsoft SQL Server 인스턴스에 새 View Composer 데이터베이스를 추가해 View Composer의 연결된 클론 데이터를 저장할 수 있습니다.

데이터베이스가 로컬에 있는 경우, View Composer가 설치될 시스템에서 통합 Windows 인증 보안 모델을 사용할 수 있습니다. 데이터베이스가 원격 시스템에 있으면 이 인증 방법을 사용할 수 없습니다.

사전 요구 사항

- View Composer를 설치하려는 컴퓨터 또는 네트워크 환경에 지원되는 SQL Server 버전이 설치되어 있는지 확인하십시오. 자세한 내용은 [View Composer 및 이벤트 데이터베이스의 데이터베이스 요구 사항](#)에 나와 있습니다.
- SQL Server Management Studio를 사용하여 데이터베이스를 생성하고 관리하는지 확인하십시오. 또는 다음 웹 사이트에서 다운로드 및 설치할 수 있는 SQL Server Management Studio Express를 사용할 수 있습니다.

<http://www.microsoft.com/en-us/download/details.aspx?id=7593>

절차

- 1 View Composer 컴퓨터에서 **시작 > 모든 프로그램 > Microsoft SQL Server 2014, Microsoft SQL Server 2012 또는 Microsoft SQL Server 2008**을 선택하십시오.
- 2 **SQL Server Management Studio**를 선택하고 SQL Server 인스턴스에 연결하십시오.
- 3 개체 탐색기 패널에서 마우스 오른쪽 단추로 데이터베이스 항목을 클릭하고 **새 데이터베이스**를 선택하십시오.

데이터베이스 및 로그 파일에 대한 Initial size 및 Autogrowth 매개변수에 기본값을 사용할 수 있습니다.

- 4 새 데이터베이스 대화 상자의 데이터베이스 이름 텍스트 상자에 이름을 입력하십시오.

예: **ViewComposer**

- 5 **확인**을 클릭합니다.

SQL Server Management Studio에서 개체 탐색기 패널의 데이터베이스 항목에 데이터베이스를 추가합니다.

- 6 Microsoft SQL Server Management Studio를 종료하십시오.

다음에 수행할 작업

필요한 경우 [수동으로 데이터베이스 역할을 생성하여 SQL Server 데이터베이스 사용 권한 설정](#)의 지침을 따르십시오.

[SQL Server에 ODBC 데이터 소스 추가](#)의 지침을 따르십시오.

수동으로 데이터베이스 역할을 생성하여 SQL Server 데이터베이스 사용 권한 설정

이 권장되는 방법을 사용하여 View Composer 데이터베이스 관리자는 Microsoft SQL Server 데이터베이스 역할을 통해 부여될 View Composer 관리자에 대한 권한을 설정할 수 있습니다.

이 방법을 사용하면 View Composer를 설치 및 업그레이드하는 View Composer 관리자에 대해 **db_owner** 역할을 설정할 필요가 없기 때문에 VMware에서는 이 방법을 권장합니다.

이 절차에서 데이터베이스 로그인 이름, 사용자 이름 및 데이터베이스 역할에 대한 고유한 이름을 제공할 수 있습니다. 사용자 **[vcmpuser]** 및 데이터베이스 역할, **VCMP_ADMIN_ROLE** 및 **VCMP_USER_ROLE**은 예제 이름입니다. View Composer 데이터베이스를 생성할 때 **dbo** 스키마가 생성됩니다. **dbo** 스키마 이름을 사용해야 합니다.

사전 요구 사항

- View Composer 데이터베이스가 생성되었는지 확인하십시오. [SQL Server에 View Composer 데이터베이스 추가](#)의 내용을 참조하십시오.

절차

- 1 sysadmin(SA) 계정 또는 **sysadmin** 권한이 있는 사용자 계정으로 Microsoft SQL Server Management Studio 세션에 로그인합니다.
- 2 적절한 SQL Server 데이터베이스 사용 권한이 부여될 사용자를 생성합니다.

```
use ViewComposer
go
CREATE LOGIN [vcmpuser] WITH PASSWORD=N'vcmpuser!0', DEFAULT_DATABASE=ViewComposer,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
use MSDB
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
```

- 3 View Composer 데이터베이스에서 데이터베이스 역할 **VCMP_ADMIN_ROLE**을 생성합니다.
- 4 View Composer 데이터베이스에서 **VCMP_ADMIN_ROLE**에 권한을 부여합니다.
 - a **dbo** 스키마의 스키마 사용 권한 **ALTER**, **REFERENCES** 및 **INSERT**를 부여합니다.
 - b 사용 권한 **CREATE TABLE**, **CREATE VIEW** 및 **CREATE PROCEDURES**를 부여합니다.
- 5 View Composer 데이터베이스에서 **VCMP_USER_ROLE**을 생성합니다.
- 6 View Composer 데이터베이스에서 **VCMP_USER_ROLE**에 **dbo** 스키마의 스키마 사용 권한 **SELECT**, **INSERT**, **DELETE**, **UPDATE** 및 **EXECUTE**를 부여합니다.
- 7 **[vcmpuser]** 사용자에게 **VCMP_USER_ROLE**을 부여합니다.
- 8 **[vcmpuser]** 사용자에게 **VCMP_ADMIN_ROLE**을 부여합니다.

- 9 MSDB 데이터베이스에서 데이터베이스 역할 **VCMP_ADMIN_ROLE**을 생성합니다.
- 10 MSDB에서 **VCMP_ADMIN_ROLE**에 권한을 부여합니다.
 - a MSDB 테이블 syscategories, sysjobsteps 및 sysjobs에서 **[vcmpuser]** 사용자에게 **SELECT** 사용 권한을 부여합니다.
 - b MSDB 저장 프로시저 sp_add_job, sp_delete_job, sp_add_jobstep, sp_update_job, sp_add_jobserver, sp_add_jobschedule 및 sp_add_category에서 **VCMP_ADMIN_ROLE** 역할에 **EXECUTE** 사용 권한을 부여합니다.
- 11 MSDB 데이터베이스에서 **[vcmpuser]** 사용자에게 **VCMP_ADMIN_ROLE**을 부여합니다.
- 12 SQL Server 로그인 **vcmpuser**를 사용하여 ODBC 시스템 DSN을 생성합니다.
지침은 [SQL Server에 ODBC 데이터 소스 추가](#)에 나와 있습니다.
- 13 View Composer를 설치합니다.
지침은 [View Composer 서비스 설치](#)에 나와 있습니다.
- 14 MSDB 데이터베이스에서 **[vcmpuser]** 사용자의 **VCMP_ADMIN_ROLE**을 해지합니다.
역할을 해지한 후 비활성 상태로 두거나 제거하여 보안을 강화할 수 있습니다.

SQL Server에 ODBC 데이터 소스 추가

SQL Server에 View Composer 데이터베이스를 추가한 후에 View Composer 서비스에서 이 데이터 소스를 볼 수 있도록 새 데이터베이스에 대한 ODBC 연결을 구성해야 합니다.

View Composer에 대해 ODBC DSN을 구성하는 경우, 기본적 데이터베이스 연결의 보안 수준을 해당 환경에 적합하게 지정하십시오. 데이터베이스 연결의 보안 지정에 대한 내용은 SQL Server 설명서를 참조하십시오.

기본 데이터베이스 연결에 SSL 암호화가 사용되는 경우 신뢰할 수 있는 CA에서 서명한 SSL 인증서로 데이터베이스 서버를 구성하는 것이 좋습니다. 자체 서명된 인증서를 사용하는 경우, 데이터베이스 연결이 외부 공격에 민감할 수 있습니다.

사전 요구 사항

[SQL Server에 View Composer 데이터베이스 추가](#)에 설명된 단계를 완료하십시오.

절차

- 1 View Composer가 설치되는 컴퓨터에서 **시작 > 관리 도구 > 데이터 소스(ODBC)**를 선택하십시오.
- 2 **시스템 DSN** 탭을 선택하십시오.
- 3 **추가**를 클릭하고 목록에서 **SQL Native Client**를 선택하십시오.
- 4 **마침**을 클릭합니다.
- 5 **SQL Server 설치에 새 데이터 원본 만들기** 마법사에서 View Composer 데이터베이스 이름과 설명을 입력하십시오.

예: **ViewComposer**

- 6 서버 텍스트 상자에 SQL Server 데이터베이스 이름을 입력하십시오.

host_name\server_name 형식을 사용하십시오. *host_name*은 컴퓨터 이름, *server_name*은 SQL Server 인스턴스입니다.

예: VCHOST1WVIM_SQLEXP

- 7 다음을 클릭하십시오.

- 8 추가 구성 옵션의 기본 설정을 얻기 위해 SQL Server에 연결 확인란을 선택했는지 확인하고 인증 옵션을 선택하십시오.

옵션	설명
Windows 통합 인증	SQL Server의 로컬 인스턴스를 사용하는 경우 이 옵션을 선택합니다. 신뢰할 수 있는 인증이라고도 합니다. 로컬 컴퓨터에서 SQL Server를 실행하는 경우에만 Windows 통합 인증을 지원합니다.
SQL Server 인증	SQL Server의 원격 인스턴스를 사용하는 경우 이 옵션을 선택합니다. 원격 SQL Server에서는 Windows NT 인증을 지원하지 않습니다. SQL Server 데이터베이스 사용 권한을 수동으로 설정한 후 사용자에게 할당한 경우 해당 사용자로 인증하십시오. 예를 들어 vcmpuser 사용자로 인증합니다. 아닌 경우 sysadmin(SA) 또는 sysadmin 권한이 있는 사용자 계정으로 인증하십시오.

- 9 다음을 클릭하십시오.

- 10 기본 데이터베이스를 다음으로 변경: 확인란을 선택하고 목록에서 View Composer 데이터베이스 이름을 선택하십시오.

예: ViewComposer

- 11 SSL이 활성화된 상태로 SQL Server 연결이 구성된 경우 Microsoft SQL Server DSN 구성 페이지로 이동한 다음 데이터에 강력한 암호 사용을 선택합니다.

- 12 Microsoft ODBC 데이터 원본 관리자 마법사를 종료하고 닫으십시오.

다음에 수행할 작업

새 View Composer 서비스를 설치합니다. [View Composer 서비스 설치](#)의 내용을 참조하십시오.

View Composer용 Oracle 데이터베이스 생성

View Composer는 연결된 클론 데스크톱 정보를 Oracle 12c 또는 11g 데이터베이스에 저장할 수 있습니다. 기존 Oracle 인스턴스에 View Composer 데이터베이스를 추가하고 ODBC 데이터 소스를 구성하여 생성합니다. Oracle 데이터베이스 구성 도우미를 사용하거나 SQL 문을 실행해 새 View Composer 데이터베이스를 추가할 수 있습니다.

■ Oracle 12c 또는 11g에 View Composer 데이터베이스 추가

Oracle 데이터베이스 구성 도우미를 사용해 기존 Oracle 12c 또는 11g 인스턴스에 새로운 View Composer 데이터베이스를 추가할 수 있습니다.

■ SQL 문을 사용하여 Oracle 인스턴스에 View Composer 데이터베이스 추가

■ View Composer의 Oracle 데이터베이스 사용자 구성

기본적으로 View Composer 데이터베이스를 실행하는 데이터베이스 사용자는 Oracle 시스템 관리자 사용 권한을 가지고 있습니다. View Composer 데이터베이스를 실행하는 사용자의 보안 사용 권한을 제한하려면 특정 사용 권한을 가진 Oracle 데이터베이스 사용자를 구성해야 합니다.

■ Oracle 12c 또는 11g에 ODBC 데이터 소스 추가

Oracle 12c 또는 11g 인스턴스에 View Composer 데이터베이스를 추가한 후에는 View Composer 서비스에서 이 데이터 소스를 볼 수 있도록 새 데이터베이스에 대한 ODBC 연결을 구성해야 합니다.

Oracle 12c 또는 11g에 View Composer 데이터베이스 추가

Oracle 데이터베이스 구성 도우미를 사용해 기존 Oracle 12c 또는 11g 인스턴스에 새로운 View Composer 데이터베이스를 추가할 수 있습니다.

사전 요구 사항

로컬 또는 원격 컴퓨터에 지원되는 Oracle 12c 또는 11g 버전이 설치되어 있는지 확인하십시오. [View Composer 및 이벤트 데이터베이스의 데이터베이스 요구 사항](#)의 내용을 참조하십시오.

절차

- 1 View Composer 데이터베이스를 추가하는 컴퓨터에서 **데이터베이스 구성 도우미**를 시작합니다.

데이터베이스 버전	조치
Oracle 12c	시작 > 모든 프로그램 > Oracle-OraDb12c_home > 구성 및 마이그레이션 도구 > 데이터베이스 구성 도우미를 선택하십시오.
Oracle 11g	시작 > 모든 프로그램 > Oracle-OraDb11g_home > 구성 및 마이그레이션 도구 > 데이터베이스 구성 도우미를 선택하십시오.

- 2 작업 페이지에서 **데이터베이스 만들기**를 선택하십시오.
- 3 데이터베이스 템플릿 페이지에서 **범용 또는 트랜잭션 처리** 템플릿을 선택하십시오.
- 4 데이터베이스 ID 페이지에서 전역 데이터베이스 이름 및 Oracle SID(시스템 식별자) 접두사를 입력하십시오.

양쪽 항목에 동일한 값을 사용하면 간단하게 작업할 수 있습니다.
- 5 관리 옵션 페이지에서 **다음**을 클릭해 기본 설정을 적용하십시오.
- 6 데이터베이스 자격 증명 페이지에서 **모든 계정에 동일한 관리 암호 사용**을 선택하고 암호를 입력하십시오.
- 7 나머지 구성 페이지에서 **다음**을 클릭해 기본 설정을 적용하십시오.
- 8 생성 옵션 페이지에서 **데이터베이스 생성**을 선택했는지 확인하고 **마침**을 클릭하십시오.
- 9 확인 페이지에서 옵션을 검토하고 **확인**을 클릭하십시오.

구성 도구가 데이터베이스를 생성합니다.
- 10 데이터베이스 생성 완료 페이지에서 **확인**을 클릭하십시오.

다음에 수행할 작업

Oracle 12c 또는 11g에 ODBC 데이터 소스 추가의 지침을 따르십시오.

SQL 문을 사용하여 Oracle 인스턴스에 View Composer 데이터베이스 추가

데이터베이스를 생성할 때 데이터 및 로그 파일의 위치를 사용자 지정할 수 있습니다.

사전 요구 사항

View Composer 데이터베이스에는 특정 테이블 공간 및 권한이 있어야 합니다. SQL문을 사용하여 Oracle 12c 또는 11g 데이터베이스 인스턴스에 View Composer 데이터베이스를 생성할 수도 있습니다.

로컬 또는 원격 컴퓨터에 지원되는 Oracle 12c 또는 11g 버전이 설치되어 있는지 확인하십시오. 자세한 내용은 [View Composer 및 이벤트 데이터베이스의 데이터베이스 요구 사항](#)에 나와 있습니다.

절차

- 1 시스템 계정으로 SQL*Plus 세션에 로그인하십시오.
- 2 다음 SQL문을 실행하여 데이터베이스를 생성합니다.

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

이 예에서, VCMP는 View Composer 데이터베이스의 샘플 이름이고 vcmp01.dbf는 데이터베이스 파일의 이름입니다.

Windows 설치의 경우 vcmp01.dbf 파일에 대한 디렉토리 경로에 Windows 규칙을 사용합니다.

다음에 수행할 작업

특정 보안 권한을 사용하여 View Composer 데이터베이스를 실행할 경우 [View Composer의 Oracle 데이터베이스 사용자 구성](#)의 지침을 따르십시오.

Oracle 12c 또는 11g에 ODBC 데이터 소스 추가의 지침을 따르십시오.

View Composer의 Oracle 데이터베이스 사용자 구성

기본적으로 View Composer 데이터베이스를 실행하는 데이터베이스 사용자는 Oracle 시스템 관리자 사용 권한을 가지고 있습니다. View Composer 데이터베이스를 실행하는 사용자의 보안 사용 권한을 제한하려면 특정 사용 권한을 가진 Oracle 데이터베이스 사용자를 구성해야 합니다.

사전 요구 사항

Oracle 12c 또는 11g 인스턴스에 View Composer 데이터베이스가 생성되었는지 확인하십시오.

절차

- 1 시스템 계정으로 SQL*Plus 세션에 로그인하십시오.

- 2 올바른 사용 권한을 가진 View Composer 데이터베이스 사용자를 생성하려면 다음 SQL 명령을 실행하십시오.

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
grant connect to VCMPADMIN;
grant resource to VCMPADMIN;
grant create view to VCMPADMIN;
grant create sequence to VCMPADMIN;
grant create table to VCMPADMIN;
grant create materialized view to VCMPADMIN;
grant execute on dbms_lock to VCMPADMIN;
grant execute on dbms_job to VCMPADMIN;
grant unlimited tablespace to VCMPADMIN;
```

이 예에서 사용자 이름은 VCMPADMIN이고 View Composer 데이터베이스 이름은 VCMP입니다.

기본적으로 resource 역할은 create procedure, create table 및 create sequence 권한을 가지고 있습니다. resource 역할에 이런 권한이 없으면 View Composer 데이터베이스 사용자에게 명시적으로 이들 권한을 부여하십시오.

Oracle 12c 또는 11g에 ODBC 데이터 소스 추가

Oracle 12c 또는 11g 인스턴스에 View Composer 데이터베이스를 추가한 후에는 View Composer 서비스에서 이 데이터 소스를 볼 수 있도록 새 데이터베이스에 대한 ODBC 연결을 구성해야 합니다.

View Composer에 대해 ODBC DSN을 구성하는 경우, 기본적 데이터베이스 연결의 보안 수준을 해당 환경에 적합하게 지정하십시오. 데이터베이스 연결의 보안 지정에 대한 내용은 Oracle 데이터베이스 설명서를 참조하십시오.

기본 데이터베이스 연결에 SSL 암호화가 사용되는 경우 신뢰할 수 있는 CA에서 서명한 SSL 인증서로 데이터베이스 서버를 구성하는 것이 좋습니다. 자체 서명된 인증서를 사용하는 경우, 데이터베이스 연결이 외부 공격에 민감할 수 있습니다.

사전 요구 사항

Oracle 12c 또는 11g에 View Composer 데이터베이스 추가 또는 SQL 문을 사용하여 Oracle 인스턴스에 View Composer 데이터베이스 추가.

절차

- 1 View Composer 데이터베이스 컴퓨터에서 **시작 > 관리 도구 > 데이터 소스(ODBC)**를 선택하십시오.
- 2 **Microsoft ODBC 데이터 원본 관리자** 마법사에서 **시스템 DSN** 탭을 선택하십시오.
- 3 **추가**를 클릭하고 목록에서 적절한 Oracle 드라이버를 선택하십시오.

예: OraDb11g_home

- 4 **마침**을 클릭합니다.

- 5 Oracle ODBC 드라이버 구성 대화 상자에서 View Composer와 함께 사용할 DSN, 데이터 소스 설명, 데이터베이스에 연결할 사용자 ID를 입력하십시오.

특정 보안 사용 권한을 가진 Oracle 데이터베이스 사용자 ID를 구성한 경우 해당 사용자 ID를 지정하십시오.

참고 View Composer 서비스를 설치할 때 DSN을 사용합니다.

- 6 드롭다운 메뉴에서 전역 데이터베이스 이름을 선택하여 **TNS 서비스 이름**을 지정하십시오.

Oracle 데이터베이스 구성 도우미가 전역 데이터베이스 이름을 지정합니다.

- 7 데이터 소스를 확인하려면 **연결 테스트**를 클릭하고 **확인**을 클릭하십시오.

다음에 수행할 작업

새 View Composer 서비스를 설치합니다. [View Composer 서비스 설치](#)의 내용을 참조하십시오.

View Composer를 위한 SSL 인증서 구성

기본적으로 View Composer에 자체 서명 인증서가 설치되어 있습니다. 기본 인증서를 테스트용으로 사용할 수 있지만 운영 용도로 사용하려면 기본 인증서를 인증 기관(CA)에서 서명한 인증서로 대체해야 합니다.

View Composer를 설치하기 전 또는 후에 인증서를 구성할 수 있습니다. View 5.1 이상 릴리스에서는 View Composer가 있거나 설치될 Windows Server 컴퓨터의 Windows 로컬 컴퓨터 인증서 저장소로 가져와서 인증서를 구성합니다.

- View Composer를 설치하기 전에 CA 서명 인증서를 가져오려면 View Composer 설치 도중 서명된 인증서를 선택할 수 있습니다. 이 방법을 사용하면 설치 후에 기본 인증서를 수동으로 교체할 필요가 없습니다.
- View Composer를 설치한 후 기존 인증서 또는 기본 자체 서명 인증서를 새 인증서와 교체하려는 경우, 새 인증서를 가져온 다음 SviConfig ReplaceCertificate 유틸리티를 실행하여 새 인증서를 View Composer에서 사용하는 포트에 바인딩해야 합니다.

SSL 인증서 구성 및 SviConfig ReplaceCertificate 유틸리티 사용에 대한 자세한 내용은 [장 8 Horizon 7 서버를 위한 TLS 인증서 구성](#)을 참조하십시오.

동일한 Windows Server 컴퓨터에 vCenter Server 및 View Composer를 설치하는 경우, 동일한 SSL 인증서를 사용할 수 있지만 각 구성 요소의 인증서를 별도로 구성해야 합니다.

View Composer 서비스 설치

View Composer를 사용하려면 View Composer 서비스를 설치해야 합니다. Horizon 7는 View Composer를 사용해 vCenter Server에 연결된 클론 데스크톱을 생성하고 배포합니다.

vCenter Server가 설치된 Windows Server 컴퓨터 또는 개별 Windows Server 컴퓨터에 View Composer 서비스를 설치할 수 있습니다. 독립 실행형 View Composer 설치하는 Windows Server 컴퓨터에 설치된 vCenter Server와 Linux 기반 vCenter Server Appliance에서 작동합니다.

View Composer 소프트웨어는 복제 서버, 보안 서버, 연결 서버, Horizon Agent 또는 Horizon Client를 포함하여 기타 모든 Horizon 7 소프트웨어 구성 요소가 포함된 동일한 가상 또는 물리적 시스템에 공존할 수 없습니다.

보안을 강화하기 위해서는 암호 제품군을 구성하여 알려진 취약성을 제거하는 것이 좋습니다. View Composer 또는 Horizon Agent를 실행하는 Windows 시스템의 암호 제품군에 도메인 정책을 설정하는 방법에 대한 지침은 [SSL/TLS에서 취약한 암호 사용 안 함](#)을 참조하십시오.

사전 요구 사항

- [View Composer 요구 사항](#)의 View Composer 요구 사항에 따라 설치했는지 확인하십시오.
- View Composer를 설치하려는 시스템에 연결 서버, 보안 서버, Horizon Agent 또는 Horizon Client를 포함한 기타 모든 Horizon 7 구성 요소가 설치되어 있지 않은지 확인하십시오.
- View Composer를 설치 및 사용할 수 있는 라이선스를 가지고 있는지 확인하십시오.
- ODBC 데이터 원본 관리자 마법사에서 제공한 DSN, 도메인 관리자 사용자 이름, 암호를 가지고 있는지 확인하십시오. View Composer 서비스를 설치할 때 해당 정보를 입력합니다.
- 설치 도중 View Composer에 대해 CA에서 서명한 SSL 인증서를 구성하려면 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져왔는지 확인하십시오. [장 8 Horizon 7 서버를 위한 TLS 인증서 구성](#)을 참조하십시오.
- View Composer 컴퓨터에서 실행되는 애플리케이션이 Microsoft Secure Channel(Schannel) 보안 패키지를 통해 제공된 SSL 버전 2(SSLv2)가 필요한 Windows SSL 라이브러리를 사용하지 않는지 확인하십시오. View Composer 설치 관리자는 Microsoft Schannel에서 SSLv2를 사용하지 않습니다. Java SSL을 사용하는 Tomcat 또는 OpenSSL을 사용하는 Apache와 같은 애플리케이션은 이 제약 조건의 영향을 받지 않습니다.
- View Composer 설치 관리자를 실행하려면 시스템에서 관리자 권한을 가진 사용자여야 합니다.

절차

- 1 <http://www.vmware.com/products/>의 VMware 제품 페이지에서 View Composer 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드합니다.

설치 관리자 파일 이름은 VMware-viewcomposer-y.y.y-xxxxxx.exe입니다. 여기서 xxxxxx는 빌드 번호이고 y.y.y는 버전 번호입니다. 해당 설치 관리자 파일로 64비트 Windows Server 운영 체제에 View Composer 서비스를 설치할 수 있습니다.

- 2 View Composer 설치 프로그램을 시작하려면 설치 관리자 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.
- 3 VMware 사용 약관에 동의하십시오.
- 4 대상 폴더를 허용 또는 변경하십시오.

- 5 Microsoft 또는 Oracle **ODBC 데이터 원본 관리자** 마법사에 제공된 View Composer 데이터베이스의 DSN을 입력하십시오.

예: **VMware View Composer**

참고 View Composer 데이터베이스의 DSN을 구성하지 않은 경우 지금 이름을 구성하려면 **ODBC DSN 설치**를 클릭하십시오.

- 6 **ODBC 데이터 원본 관리자** 마법사에 제공된 도메인 관리자 사용자 이름과 암호를 입력하십시오.
특정 보안 사용 권한을 가진 Oracle 데이터베이스 사용자를 구성한 경우 해당 사용자 이름을 지정하십시오.
- 7 포트 번호를 입력하거나 기본값을 허용하십시오.
View 연결 서버는 해당 포트를 사용해 View Composer 서비스와 통신합니다.
- 8 SSL 인증서를 지정하십시오.

옵션	조치
기본 SSL 인증서 생성	View Composer 서비스에 대한 기본 SSL 인증서를 생성하려면 이 라디오 단추를 선택합니다. 설치 후에 기본 인증서를 CA에서 서명한 SSL 인증서로 바꿀 수 있습니다.
기존 SSL 인증서 사용	View Composer 서비스에 대해 사용할 서명된 SSL 인증서를 설치한 경우 이 라디오 단추를 선택합니다. 목록에서 SSL 인증서를 선택합니다.

- 9 View Composer 서비스 설치를 완료하려면 **설치**와 **마침**을 클릭하십시오.

VMware Horizon View Composer 서비스가 시작됩니다.

View Composer는 Windows Server 운영 체제에서 제공하는 암호화 암호 제품군을 사용합니다. 조직의 지침에 따라 Windows Server 시스템의 암호 제품군을 관리해야 합니다. 조직에서 지침을 제공하지 않는 경우에는 View Composer Server에서 취약한 암호화 암호 제품군을 사용하지 않도록 설정하여 Horizon 7 환경의 보안을 강화하는 것이 좋습니다. 암호화 암호 제품군 관리에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

다음에 수행할 작업

이전 버전의 vCenter Server를 사용하는 경우에는 [View Composer에서 vCenter의 TLSv1.0 및 ESXi 연결 사용](#)을 참조하십시오.

수동으로 SQL Server 데이터베이스 사용 권한을 설정하고 사용자에게 할당한 경우 해당 사용자의 데이터베이스 관리자 역할을 해지할 수 있습니다. 자세한 내용은 [수동으로 데이터베이스 역할을 생성하여 SQL Server 데이터베이스 사용 권한 설정](#)의 절차에 있는 마지막 단계를 참조하십시오.

View Composer에서 vCenter의 TLSv1.0 및 ESXi 연결 사용

Horizon 7 이상 구성 요소에서는 TLSv1.0 보안 프로토콜이 기본적으로 사용 안 함으로 설정됩니다. 배포에 TLSv1.0만 지원하는 이전 버전의 vCenter Server가 포함되어 있는 경우에는 View

Composer 연결 서버 7.0 이상 릴리스를 설치 또는 업그레이드한 후에 View Composer 연결 서버에 대해 TLSv1.0 연결을 사용하도록 설정해야 할 수도 있습니다.

vCenter Server 5.0, 5.1, 5.5의 일부 초기 유지 보수 릴리스에서는 Horizon 7 이상 릴리스에서 더 이상 기본적으로 사용하도록 설정되지 않는 TLSv1.0만 지원합니다. vCenter Server를 TLSv1.1 또는 TLSv1.2를 지원하는 버전으로 업그레이드할 수 없는 경우에는 View Composer 연결에 대해 TLSv1.0을 사용하도록 설정할 수 있습니다.

ESXi 호스트가 ESXi 6.0 U1b 이상을 실행하지 않고 업그레이드도 할 수 없는 경우에는 View Composer에서 ESXi 호스트로의 TLSv1.0 연결도 사용하도록 설정해야 할 수 있습니다.

사전 요구 사항

- View Composer 7.0 이상 릴리스가 설치되어 있는지 확인합니다.
- View Composer 시스템에 관리자로 로그인하여 Windows 레지스트리 편집기를 사용할 수 있는지 확인합니다.

절차

- 1 View Composer를 호스팅하는 시스템에서 Windows 레지스트리 편집기(regedit.exe)를 엽니다.
- 2 HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHannel\Protocols\TLS_1.0\Client로 이동합니다.

이 키가 아직 없는 경우에는 이 키를 만듭니다.

- 3 **Enabled** 값이 있으면 삭제합니다.
- 4 **DWORD** 값 **DisabledByDefault**를 만들거나 편집하여 **0**으로 설정합니다.
- 5 VMware Horizon View Composer 서비스가 다시 시작됩니다.
View Composer에서 vCenter로의 TLSv1.0 연결이 이제 사용되도록 설정됩니다.
- 6 View Composer 시스템의 Windows 레지스트리에서 HKLM\SOFTWARE\VMware, Inc.\VMware View Composer로 이동합니다.
- 7 문자열 값 **EnableTLS1.0**을 만들거나 편집하여 **1**로 설정합니다.
- 8 View Composer 호스트가 64비트 시스템인 경우에는 HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware View Composer로 이동합니다.
- 9 문자열 값 **EnableTLS1.0**을 만들거나 편집하여 **1**로 설정합니다.
- 10 VMware Horizon View Composer 서비스가 다시 시작됩니다.

View Composer에서 ESXi 호스트로의 TLSv1.0 연결이 이제 사용하도록 설정됩니다.

View Composer를 위한 인프라 구축

vSphere, vCenter Server, Active Directory 및 인프라의 다른 구성 요소에 있는 기능을 사용해 View Composer 성능, 가용성, 신뢰성을 최적화할 수 있습니다.

View Composer를 위한 vSphere 환경 구성

View Composer를 지원하려면 특정 모범 사례에 따라 vCenter Server, ESXi 및 기타 vSphere 구성 요소를 설치하고 구성해야 합니다.

이러한 모범 사례를 통해 vSphere 환경에서 View Composer가 더욱 효율적으로 작동할 수 있습니다.

- 연결된 클론 가상 시스템의 경로 및 폴더 정보를 생성한 후에는 vCenter Server에서 해당 정보를 변경하지 마십시오. 대신 Horizon Administrator를 사용해 폴더 정보를 변경하십시오.
vCenter Server에서 이 정보를 변경할 경우 Horizon 7가 vCenter Server에서 가상 시스템을 찾을 수 없습니다.
- ESXi 호스트에서 실행되는 연결된 클론 가상 시스템에 구성되어 있는 총 가상 NIC 수를 지원하기에 충분한 포트가 구성되었는지 ESXi 호스트의 vSwitch 설정을 확인하십시오.
- 연결된 클론 데스크톱을 리소스 풀에 배포할 때 vSphere 환경에 필요한 데스크톱 수를 호스팅하기에 충분한 CPU와 메모리가 준비되어 있는지 확인하십시오. 리소스 풀의 CPU와 메모리 사용량을 모니터링하려면 vSphere Client를 사용하십시오.
- vSphere 5.1 이상에서는 VMFS5 이상의 데이터스토어 또는 NFS 데이터스토어에 복제 디스크가 저장된 경우 View Composer 연결된 클론에 사용되는 클러스터가 9대 이상의 ESXi 호스트를 포함할 수 있습니다. 복제본을 VMFS5 이전의 VMFS 버전에 저장할 경우, 클러스터는 최대 8개의 호스트만을 가질 수 있습니다.
- vSphere DRS를 사용하십시오. DRS는 호스트에서 연결된 클론 가상 시스템을 효율적으로 분산시킵니다.

참고 연결된 클론 데스크톱은 Storage vMotion을 지원하지 않습니다.

View Composer의 추가 모범 사례

View Composer가 효율적으로 작동하는지 확인하려면 DNS(Dynamic Name Service)가 제대로 작동하는지 확인하고 바이러스 백신 소프트웨어 검사를 여러 차례로 나눠 실시합니다.

DNS 확인 작업을 올바르게 수행하면 DNS 오류로 인해 간혹 발생하는 문제를 해결할 수 있습니다. View Composer 서비스는 동적 이름 확인을 통해 다른 컴퓨터와 통신합니다. DNS 작업을 테스트하려면 Active Directory 및 View 연결 서버 컴퓨터를 이름으로 Ping합니다.

바이러스 백신 소프트웨어 실행 시간을 분산하면 연결된 클론 데스크톱 성능에 영향을 미치지 않습니다. 모든 연결된 클론에서 바이러스 백신 소프트웨어를 동시에 실행하면 스토리지 하위 시스템에서 초당 I/O 작업(IOPS)이 과도하게 발생합니다. 이러한 과도한 활동은 연결된 클론 데스크톱 성능에 영향을 미칠 수 있습니다.

Horizon 연결 서버 설치

7

연결 서버를 사용하려면 지원된 컴퓨터에 소프트웨어를 설치하고 필요한 구성 요소를 구성하며 선택적으로 구성 요소를 최적화합니다.

본 장은 다음 항목을 포함합니다.

- Horizon 연결 서버 소프트웨어 설치
- Horizon 연결 서버의 설치 전제 조건
- 새 구성을 사용하여 Horizon 연결 서버 설치
- Horizon 연결 서버의 복제된 인스턴스 설치
- 보안 서버 연결 암호 구성
- 보안 서버 설치
- VPN보다 나은 Unified Access Gateway 장치의 이점
- Horizon 연결 서버의 방화벽 규칙
- 백업 구성을 사용하여 Horizon 연결 서버 재설치
- Microsoft Windows Installer 명령줄 옵션
- MSI 명령줄 옵션을 사용하여 Horizon 7 구성 요소 자동 제거

Horizon 연결 서버 소프트웨어 설치

Horizon 7 배포의 성능, 가용성 및 보안 요구에 따라 연결 서버의 단일 인스턴스, 연결 서버의 복제된 인스턴스 및 보안 서버를 설치할 수 있습니다. 연결 서버 인스턴스를 하나 이상 설치해야 합니다.

연결 서버를 설치할 때 설치 유형을 선택합니다.

표준 설치

새 View LDAP 구성을 사용하여 연결 서버 인스턴스를 생성합니다.

복제 설치

기존 인스턴스에서 복사된 View LDAP 구성을 사용하여 연결 서버 인스턴스를 생성합니다.

보안 서버 설치

인터넷 및 내부 네트워크 사이에 추가 보안 계층을 추가하는 연결 서버 인스턴스를 생성합니다.

등록 서버 설치

True SSO(Single Sign-On) 기능에 필요한 등록 서버를 설치하여, 사용자가 VMware Identity Manager에 로그인하면 Active Directory 자격 증명을 제공하지 않고도 원격 데스크톱이나 애플리케이션에 연결할 수 있도록 합니다. 등록 서버에서는 인증에 사용되는 일시적인 인증서를 요청합니다.

참고 이 기능을 사용하려면 인증 기관도 설정하고 특정 구성을 수행해야 하기 때문에 이 설치 설명서 대신 "Horizon 7 관리" 문서의 "자격 증명을 요구하지 않고 사용자 인증" 장에 등록 서버의 설치 절차를 준비해 두었습니다.

Horizon 연결 서버의 설치 전제 조건

연결 서버를 설치하기 전에 설치 환경이 특정 전제 조건을 충족해야 합니다.

- Horizon 7의 유효한 라이선스 키가 있어야 합니다.
- 연결 서버 호스트를 Active Directory 도메인에 결합시켜야 합니다. 연결 서버는 다음 AD DS(Active Directory 도메인 서비스) 도메인 기능 수준을 지원합니다.
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016

연결 서버 호스트는 도메인 컨트롤러가 될 수 없습니다.

참고 연결 서버에서는 Active Directory에 대해 스키마 또는 구성을 업데이트하지 않고 업데이트가 필요하지도 않습니다.

- Windows Terminal Server 역할이 설치된 시스템에 연결 서버를 설치하지 마십시오. 연결 서버를 설치할 임의의 시스템에서 Windows Terminal Server 역할을 제거해야 합니다.
- 다른 기능 또는 역할을 수행하는 시스템에 연결 서버를 설치하지 마십시오. 예를 들어 동일한 시스템을 사용하여 vCenter Server를 호스팅하지 마십시오.
- 연결 서버를 설치하는 시스템은 고정 IP 주소를 가지고 있어야 합니다. IPv4 환경에서 정적 IP 주소를 구성합니다. IPv6 환경에서 시스템은 변경되지 않는 IP 주소를 자동으로 가져옵니다.
- Horizon 연결 서버 설치 관리자를 실행하려면 시스템에서 관리자 권한을 가진 도메인 사용자 계정을 사용해야 합니다.

- 연결 서버를 설치할 때 Administrator 계정을 인증합니다. 로컬 관리자 그룹, 도메인 사용자 또는 그룹 계정을 지정할 수 있습니다. Horizon 7에서는 복제된 연결 서버 인스턴스를 설치할 수 있는 권한을 포함하여 전체 관리 권한을 이 계정에만 할당합니다. 도메인 사용자 또는 그룹을 지정할 경우, 설치 관리자를 실행하기 전에 Active Directory에 계정을 생성해야 합니다.

새 구성을 사용하여 Horizon 연결 서버 설치

복제된 연결 서버 인스턴스 그룹의 단일 서버 또는 첫 번째 인스턴스로 연결 서버를 설치하려면 표준 설치 옵션을 사용합니다.

표준 설치 옵션을 선택하면 설치 중 새 로컬 View LDAP 구성이 생성됩니다. 설치 중 스키마 정의, Directory Information Tree(DIT) 정의 및 ACL이 로드되고 데이터가 초기화됩니다.

설치 후 Horizon Administrator를 사용하여 대부분의 View LDAP 구성 데이터를 관리합니다. 연결 서버는 일부 View LDAP 항목을 자동으로 관리합니다.

연결 서버 소프트웨어는 복제 서버, 보안 서버, View Composer, Horizon Agent 또는 Horizon Client를 포함하여 기타 모든 Horizon 7 소프트웨어 구성 요소가 포함된 동일한 가상 또는 물리적 시스템에 공존할 수 없습니다.

새 구성을 사용하여 연결 서버를 설치할 경우 고객 환경 향상 프로그램에 참여할 수 있습니다.

VMware는 사용자 요구 사항에 대한 VMware의 응답을 개선하기 위해 배포에 관한 익명 데이터를 수집합니다. 조직을 식별할 수 있는 데이터는 수집하지 않습니다. 설치 도중 이 옵션을 선택 해제하여 참여하지 않도록 선택할 수 있습니다. 설치 후에 참여 의사가 변경될 경우 Horizon Administrator의 제품 라이선싱 및 사용량 페이지를 편집하여 프로그램에 가입하거나 가입을 철회할 수 있습니다. 익명 필드 등 데이터가 수집되는 필드 목록을 확인하려면 "Horizon 7 관리" 문서의 "고객 환경 향상 프로그램에서 수집한 정보"를 참조하십시오.

기본적으로, 연결 서버를 설치할 때 HTML Access 구성 요소가 연결 서버 호스트에 설치됩니다. 이 구성 요소는 Horizon 7 사용자 포털 페이지에서 HTML Access 아이콘과 Horizon Client 아이콘을 표시하도록 구성합니다. 추가 아이콘을 통해 사용자는 자신의 데스크톱에 연결할 때 HTML Access를 선택할 수 있습니다.

HTML Access에 대한 연결 서버 설정 개요는 Horizon Client 설명서 페이지에 있는 "VMware Horizon HTML Access 설치 및 설정 가이드" 문서를 참조하십시오.

사전 요구 사항

- 연결 서버를 설치할 Windows Server 컴퓨터에 관리자 권한을 가진 도메인 사용자로 로그인할 수 있는지 확인합니다.
- [Horizon 연결 서버 요구 사항](#)에 설명된 설치 요구 사항을 충족하는지 확인하십시오.
- 설치 환경을 준비하십시오. [Horizon 연결 서버의 설치 전제 조건](#)의 내용을 참조하십시오.
- Administrator 계정으로 도메인 사용자 또는 그룹을 인증할 경우, Active Directory에 도메인 계정을 생성했는지 확인하십시오.

- 데이터 복구 암호를 준비하십시오. 연결 서버를 백업할 때 View LDAP 구성이 암호화된 LDIF 데이터로 보내집니다. 암호화된 백업 Horizon 7 구성을 복원하려면 데이터 복구 암호를 입력해야 합니다. 암호는 1 ~ 128자 사이여야 합니다. 조직의 모범 사례에 따라 보안 암호를 생성하십시오.

중요 BCDR(비즈니스 연속성 및 재해 복구) 시나리오에서 계속해서 Horizon 7를 작동하고 다운타임을 피하려면 데이터 복구 암호가 필요합니다. 연결 서버를 설치할 때 암호를 포함한 암호 알림을 입력할 수 있습니다.

- 연결 서버 인스턴스의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. [Horizon 연결 서버의 방화벽 규칙](#)의 내용을 참조하십시오.
- 연결 서버 인스턴스와 보안 서버를 연결하려는 경우, 고급 보안이 적용된 Windows 방화벽이 활성 프로파일에 **켜짐**으로 설정되어 있는지 확인하십시오. 모든 프로파일에 대해 이 설정을 **켜짐**으로 설정하는 것이 좋습니다. 기본적으로 IPsec 규칙은 보안 서버 및 연결 서버 간 연결을 통제하며 고급 보안이 적용된 Windows 방화벽이 사용되도록 설정되어야 합니다.
- 네트워크 토폴로지가 보안 서버와 연결 서버 인스턴스 간 백엔드 방화벽을 둔 경우 IPsec를 지원하도록 방화벽을 구성해야 합니다. [IPsec을 지원하도록 백엔드 방화벽 구성](#)의 내용을 참조하십시오.

절차

- 1 VMware 다운로드 사이트(<https://my.vmware.com/web/vmware/downloads>)에서 연결 서버 설치 관리자 파일을 다운로드합니다.

Desktop & End-User Computing에서 연결 서버가 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe입니다. 여기서 xxxxxx는 빌드 번호이며 y.y.y는 버전 번호입니다.

- 2 연결 서버 설치 프로그램을 시작하려면 설치 관리자 파일을 두 번 클릭합니다.
- 3 VMware 사용 약관에 동의하십시오.
- 4 대상 폴더를 수락하거나 변경하십시오.
- 5 **View 표준 서버** 설치 옵션을 선택합니다.

- 6 IP(인터넷 프로토콜) 버전, **IPv4** 또는 **IPv6**을 선택합니다.

동일한 IP 버전으로 모든 Horizon 7 구성 요소를 설치해야 합니다.

- 7 FIPS 모드 사용 여부를 선택합니다.

이 옵션은 Windows에서 FIPS 모드를 사용하도록 설정된 경우에만 사용할 수 있습니다.

- 8 사용자가 웹 브라우저를 통해 자신의 데스크톱에 연결할 수 있도록 하려면 **HTML Access 설치**가 선택되었는지 확인합니다.

IPv4가 선택된 경우 이 설정이 기본적으로 선택됩니다. **IPv6**이 선택된 경우 IPv6 환경에서 HTML Access가 지원되지 않기 때문에 이 설정이 표시되지 않습니다.

- 9 데이터 복구 암호와 암호 알림(선택 사항)을 입력합니다.

10 Windows 방화벽 서비스 구성 방법을 선택합니다.

옵션	조치
자동으로 Windows 방화벽 구성	설치 관리자에서 Windows 방화벽을 구성해 필요한 네트워크 연결을 허용합니다.
Windows 방화벽 구성 안 함	Windows 방화벽 규칙을 수동으로 구성합니다. 조직에서 미리 정의된 자체 규칙을 사용하여 Windows 방화벽을 구성하는 경우에만 이 옵션을 선택하십시오.

11 Horizon Administrator 계정을 인증하십시오.

이 계정의 구성원만 Horizon Administrator에 로그인하고 전체 관리 권한을 실행하고, 복제된 연결 서버 인스턴스 및 기타 Horizon 7 서버를 설치할 수 있습니다.

옵션	설명
로컬 관리자 그룹 인증	로컬 Administrators 그룹의 사용자가 Horizon 7를 관리할 수 있도록 허용합니다.
특정 도메인 사용자 또는 도메인 그룹 인증	지정된 도메인 사용자 또는 그룹이 Horizon 7를 관리할 수 있도록 허용합니다.

12 도메인 Horizon Administrator 계정을 지정했고 도메인 계정에 액세스하지 않고 로컬 관리자 또는 다른 사용자로 설치 관리자를 실행 중인 경우, 인증된 사용자 이름 및 암호를 사용하여 도메인에 로그인할 수 있도록 자격 증명을 제공하십시오.

domain name\user name 또는 UPN 형식을 사용합니다. UPN은 *user@domain.com*의 형식으로 되어 있습니다.

13 고객 환경 개선 프로그램에 참여할지를 선택하십시오.

참여할 경우 조직의 유형, 규모 및 위치를 선택할 수 있습니다(선택 사항).

14 설치 마법사를 완료하여 연결 서버 설치를 마칩니다.

15 Windows Server 컴퓨터에서 새 패치를 확인하고 필요에 따라 Windows 업데이트를 실행합니다.

연결 서버를 설치하기 전에 Windows Server 컴퓨터를 완전히 패치했더라도 설치 시 처음으로 운영 체제 기능을 사용하도록 설정할 수 있습니다. 이제 추가 패치가 필요할 수 있습니다.

Windows Server 컴퓨터에 Horizon 7 서비스가 설치되었습니다.

- VMware Horizon 연결 서버
- VMware Horizon View Framework 구성 요소
- VMware Horizon View Message Bus 구성 요소
- VMware Horizon View Script Host
- VMware Horizon View Security Gateway 구성 요소
- VMware Horizon View PCoIP 보안 게이트웨이

- VMware Horizon View Blast 보안 게이트웨이
- VMware Horizon View 웹 구성 요소
- View LDAP 디렉토리 서비스를 제공하는 VMware VDMDS

이러한 서비스에 대한 자세한 내용은 "Horizon 7 관리" 문서를 참조하십시오.

설치 중에 **HTML Access 설치** 설정을 지정한 경우 HTML Access 구성 요소가 Windows Server 컴퓨터에 설치됩니다. 이 구성 요소는 HTML Access 아이콘을 Horizon 7 사용자 포털 페이지에 구성하고 Windows 방화벽에서 **VMware Horizon View 연결 서버(Blast-In)** 규칙을 사용하도록 설정합니다. 이 방화벽 규칙을 통해 클라이언트 디바이스의 웹 브라우저가 TCP 포트 8443에서 연결 서버에 연결할 수 있습니다.

다음에 수행할 작업

연결 서버를 위한 SSL 서버 인증서를 구성하십시오. [장 8 Horizon 7 서버를 위한 TLS 인증서 구성](#)의 내용을 참조하십시오.

이전 버전의 vCenter Server를 사용하는 경우에는 [연결 서버의 vCenter 연결에서 TLSv1.0 사용](#)을 참조하십시오.

연결 서버에서 초기 구성을 수행합니다. [장 9 처음으로 Horizon 7 구성](#)의 내용을 참조하십시오.

연결 서버 인스턴스 및 보안 서버를 배포할 경우 연결 서버 설치 관리자 파일을 실행하여 각 서버 인스턴스를 설치해야 합니다.

연결 서버를 다시 설치하는 중이며 성능 데이터를 모니터링하도록 데이터 수집기 세트를 구성한 경우 데이터 수집기 세트를 중지하고 다시 시작합니다.

Horizon 연결 서버 자동 설치

Microsoft Windows Installer의 자동 설치(MSI) 기능을 사용하여 여러 Windows 컴퓨터에 연결 서버 표준 설치를 수행할 수 있습니다. 자동 설치 시에는 명령줄을 사용하고 마법사 메시지에 응답할 필요가 없습니다.

자동 설치를 사용하면 대규모 기업에서 Horizon 7 구성 요소를 효과적으로 배포할 수 있습니다.

사전 요구 사항

- 연결 서버를 설치할 Windows Server 컴퓨터에 관리자 권한을 가진 도메인 사용자로 로그인할 수 있는지 확인합니다.
- [Horizon 연결 서버 요구 사항](#)에 설명된 설치 요구 사항을 충족하는지 확인하십시오.
- 설치 환경을 준비하십시오. [Horizon 연결 서버의 설치 전제 조건](#)을 참조하십시오.
- Horizon Administrators 계정으로 도메인 사용자 또는 그룹을 인증할 경우, Active Directory에 도메인 계정을 생성했는지 확인하십시오.
- 연결 서버를 설치 중인 Windows Server 2008 R2 컴퓨터에 로그인하는 데 MIT Kerberos 인증을 사용하는 경우, <http://support.microsoft.com/kb/978116>의 KB 978116에 설명된 Microsoft 핫픽스를 설치하십시오.

- 연결 서버 인스턴스의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. [Horizon 연결 서버의 방화벽 규칙](#)를 참조하십시오.
- 연결 서버 인스턴스와 보안 서버를 연결하려는 경우, 고급 보안이 적용된 Windows 방화벽이 활성 프로파일에 **켜짐**으로 설정되어 있는지 확인하십시오. 모든 프로파일에 대해 이 설정을 **켜짐**으로 설정하는 것이 좋습니다. 기본적으로 IPsec 규칙은 보안 서버 및 연결 서버 간 연결을 통제하며 고급 보안이 적용된 Windows 방화벽이 사용되도록 설정되어야 합니다.
- 네트워크 토폴로지가 보안 서버와 연결 서버 인스턴스 간 백엔드 방화벽을 둔 경우 IPsec를 지원하도록 방화벽을 구성해야 합니다. [IPsec을 지원하도록 백엔드 방화벽 구성](#)를 참조하십시오.
- 연결 서버를 설치할 Windows 컴퓨터에는 MSI 런타임 엔진 버전 2.0 이상이 있어야 합니다. 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.
- MSI 설치 관리자 명령줄 옵션을 숙지하십시오. [Microsoft Windows Installer 명령줄 옵션](#)를 참조하십시오.
- 연결 서버의 표준 설치에 사용할 수 있는 자동 설치 속성을 숙지하십시오. [Horizon 연결 서버 표준 설치의 자동 설치 속성](#)를 참조하십시오.

절차

- 1 VMware 다운로드 사이트(<https://my.vmware.com/web/vmware/downloads>)에서 연결 서버 설치 관리자 파일을 다운로드합니다.

Desktop & End-User Computing에서 연결 서버가 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe입니다. 여기서 xxxxxx는 빌드 번호이며 y.y.y는 버전 번호입니다.

- 2 Windows Server 컴퓨터에서 명령 프롬프트를 엽니다.
- 3 설치 명령을 한 줄에 입력하십시오.

```
예: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1
VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini
VDM_SERVER_RECOVERY_PWD_REMINDER="First car"""
```

중요 자동 설치를 수행할 경우 데이터 복구 암호를 포함한 전체 명령줄이 설치 관리자의 vminst.log 파일에 기록됩니다. 설치가 완료되면 이 로그 파일을 삭제하거나 Horizon Administrator를 사용하여 데이터 복구 암호를 변경하십시오.

- 4 Windows Server 컴퓨터에서 새 패치를 확인하고 필요에 따라 Windows 업데이트를 실행합니다.

연결 서버를 설치하기 전에 Windows Server 컴퓨터를 완전히 패치했더라도 설치 시 처음으로 운영 체제 기능을 사용하도록 설정할 수 있습니다. 이제 추가 패치가 필요할 수 있습니다.

Windows Server 컴퓨터에 Horizon 7 서비스가 설치되었습니다.

- VMware Horizon 연결 서버
- VMware Horizon View Framework 구성 요소

- VMware Horizon View Message Bus 구성 요소
- VMware Horizon View Script Host
- VMware Horizon View Security Gateway 구성 요소
- VMware Horizon View PCoIP 보안 게이트웨이
- VMware Horizon View Blast 보안 게이트웨이
- VMware Horizon View 웹 구성 요소
- View LDAP 디렉토리 서비스를 제공하는 VMware VDMDS

설치 중에 **HTML Access 설치** 설정을 지정한 경우 HTML Access 구성 요소가 Windows Server 컴퓨터에 설치됩니다. 이 구성 요소는 HTML Access 아이콘을 Horizon 7 사용자 포털 페이지에 구성하고 Windows 방화벽에서 **VMware Horizon View 연결 서버(Blast-In)** 규칙을 사용하도록 설정합니다. 이 방화벽 규칙을 통해 클라이언트 디바이스의 웹 브라우저가 TCP 포트 8443에서 연결 서버에 연결할 수 있습니다.

이러한 서비스에 대한 자세한 내용은 "Horizon 7 관리" 문서를 참조하십시오.

다음에 수행할 작업

연결 서버를 위한 SSL 서버 인증서를 구성하십시오. [장 8 Horizon 7 서버를 위한 TLS 인증서 구성](#)를 참조하십시오.

이전 버전의 vCenter Server를 사용하는 경우에는 [연결 서버의 vCenter 연결에서 TLSv1.0 사용](#)을 참조하십시오.

처음으로 Horizon 7을 구성할 경우 연결 서버의 초기 구성을 수행하십시오. [장 9 처음으로 Horizon 7 구성](#)를 참조하십시오.

Horizon 연결 서버 표준 설치의 자동 설치 속성

명령줄에서 무인 설치 또는 업그레이드를 수행할 때 특정 연결 서버 속성이 포함될 수 있습니다.

MSI(Microsoft Windows Installer)가 속성 및 값을 해석할 수 있도록 *PROPERTY=value* 형식을 사용해야 합니다. 자동 업그레이드는 동일한 설치 명령을 사용합니다.

표 7-1. 표준 설치에서 연결 서버를 자동 설치하기 위한 MSI 속성

MSI 속성	설명	기본 값
INSTALLDIR	연결 서버 소프트웨어가 설치된 경로 및 폴더입니다. 예: <code>INSTALLDIR="D:\abc\my folder"</code> 해당 경로를 둘러싸고 있는 큰따옴표 두 쌍은 MSI 설치 관리자가 공백을 경로의 유효한 부분으로 해석하도록 합니다.	<code>%ProgramFiles%\VMware View\Server</code>
VDM_SERVER_INSTANCE_TYPE	Horizon Server 설치 유형: <ul style="list-style-type: none"> ■ 1. 표준 설치 ■ 2. 복제 설치 ■ 3. 보안 서버 설치 ■ 5. 등록 서버 설치 예를 들어, 표준 설치를 수행하려면 <code>VDM_SERVER_INSTANCE_TYPE=1</code> 을 정의합니다.	1

표 7-1. 표준 설치에서 연결 서버를 자동 설치하기 위한 MSI 속성 (계속)

MSI 속성	설명	기본 값
FWCHOICE	연결 서버 인스턴스의 방화벽을 구성할지 여부를 결정하는 MSI 속성입니다. 1의 값은 방화벽을 구성합니다. 2의 값은 방화벽을 구성하지 않습니다. 예: FWCHOICE=1	1
VDM_INITIAL_ADMIN_SID	Horizon의 전체 관리 권한으로 인증된 초기 Horizon Administrators 사용자 또는 그룹의 SID입니다. 기본값은 연결 서버 컴퓨터에 있는 로컬 관리자 그룹의 SID입니다. 도메인 사용자 또는 그룹 계정의 SID를 지정할 수 있습니다.	S-1-5-32-544
VDM_SERVER_RECOVERY_PWD	데이터 복구 암호입니다. 데이터 복구 암호가 Horizon LDAP에 설정되어 있지 않은 경우 이 속성이 필수입니다. 암호는 1 ~ 128자 사이여야 합니다. 조직의 모범 사례에 따라 보안 암호를 생성하십시오.	없음
VDM_SERVER_RECOVERY_PWD_REMINDER	데이터 복구 암호 알림입니다. 이 속성은 선택 사항입니다.	없음
VDM_IP_PROTOCOL_USAGE	Horizon 구성 요소가 통신에 사용하는 IP 버전을 지정합니다. 가능한 값은 IPv4 및 IPv6 입니다.	IPv4
VDM_FIPS_ENABLED	FIPS 모드 사용 여부를 지정합니다. 값이 1이면 FIPS 모드를 활성화합니다. 값이 0이면 FIPS 모드를 비활성화합니다. 이 속성을 1로 설정했는데 Windows가 FIPS 모드에 있지 않으면 설치 관리자가 중단됩니다.	0
HTMLACCESS	HTML Access 추가 기능 설치를 제어합니다. HTML Access를 구성하려면 이 속성을 1로 설정하고, HTML Access가 필요 없는 경우에는 이 속성을 생략합니다.	1

연결 서버의 vCenter 연결에서 TLSv1.0 사용

Horizon 7 이상 구성 요소에서는 TLSv1.0 보안 프로토콜이 기본적으로 사용 안 함으로 설정됩니다. 배포에 TLSv1.0만 지원하는 이전 버전의 vCenter Server가 포함되어 있는 경우에는 연결 서버 7.0 이상 릴리스를 설치 또는 업그레이드한 후에 연결 서버 연결에 대해 TLSv1.0을 사용하도록 설정해야 할 수도 있습니다.

vCenter Server 5.1 및 5.5의 일부 초기 유지 보수 릴리스에서는 Horizon 7 이상 릴리스에서 더 이상 기본적으로 사용하도록 설정되지 않는 TLSv1.0만 지원합니다. vCenter Server를 TLSv1.1 또는 TLSv1.2를 지원하는 버전으로 업그레이드할 수 없는 경우에는 연결 서버 연결에 대해 TLSv1.0을 사용하도록 사용하도록 설정할 수 있습니다.

사전 요구 사항

- Horizon 7으로 업그레이드하려는 경우는 업그레이드 전에 이 절차를 수행하여 서비스를 다시 시작할 횟수를 최소화해야 합니다. 업그레이드하는 동안 연결 서버 서비스가 다시 시작되며, 이 절차에 설명된 구성 변경을 적용하려면 다시 시작해야 합니다. 이 절차를 수행하기 전에 업그레이드한 경우에는 서비스를 두 번째로 다시 시작해야 합니다.

- 사용하고 있는 Windows 운영 체제 버전에서 ADSI 편집 유틸리티를 사용하는 방법은 Microsoft TechNet 웹 사이트를 참조하십시오.

절차

- 1 연결 서버 호스트에서 ADSI 편집 유틸리티를 시작하십시오.
- 2 콘솔 트리에서 **연결**을 선택합니다.
- 3 **고유 이름 또는 명명 컨텍스트를 선택하거나 입력합니다** 텍스트 상자에 고유 이름 **DC=vdi, DC=vmware, DC=int**를 입력합니다.
- 4 컴퓨터 창에서 **localhost:389**를 선택하거나 연결 서버 호스트의 FQDN(정규화된 도메인 이름)과 포트 389를 차례로 입력합니다.
예: **localhost:389** 또는 **mycomputer.example.com:389**
- 5 ADSI 편집 트리를 확장하고 **OU=Properties**를 확장한 다음 **OU=Global**을 선택하고 오른쪽 창에서 **CN=Common**을 두 번 클릭합니다.
- 6 속성 대화상자에서 **pae-ClientSSLSecureProtocols** 특성을 편집하여 다음 값을 추가합니다.
WLIST:TLSv1.2,TLSv1.1,TLSv1
행 시작 부분에 백슬래시를 포함해야 합니다.
- 7 **확인**을 클릭합니다.
- 8 새로 설치하는 경우 구성 변경을 적용하려면 각 연결 서버 인스턴스에서 연결 서버 서비스를 다시 시작합니다.
업그레이드를 계획하는 중이면 업그레이드 프로세스에서 자동으로 서비스가 다시 시작되기 때문에 서비스를 다시 시작할 필요가 없습니다.

Horizon 연결 서버의 복제된 인스턴스 설치

기존 연결 서버 인스턴스를 복제한 연결 서버 인스턴스를 1개 이상 추가 설치해 가용성을 향상하고 로드 밸런싱을 제공할 수 있습니다. 복제본을 설치한 다음에는 기존 및 새로 설치된 연결 서버 인스턴스가 동일합니다.

복제된 인스턴스를 설치할 때 Horizon 7이 기존 연결 서버 인스턴스에서 View LDAP 구성 데이터를 복제합니다.

설치 후 동일한 View LDAP 구성 데이터가 복제된 그룹의 모든 연결 서버 인스턴스에서 유지됩니다. 인스턴스 1개에서 내용을 변경하면 다른 인스턴스에 업데이트 정보가 복사됩니다.

복제된 인스턴스가 잘못된 경우 그룹의 다른 인스턴스에서 작업을 계속합니다. 잘못된 인스턴스가 다시 작업을 시작하면 운영을 중단했던 동안 변경된 구성이 업데이트됩니다.

참고 Active Directory와 동일한 복제 기술을 사용하는 View LDAP에서 복제 기능을 제공합니다.

복제 서버 소프트웨어는 보안 서버, 연결 서버, View Composer, Horizon Agent 또는 Horizon Client를 포함하여 기타 모든 Horizon 7 소프트웨어 구성 요소가 포함된 동일한 가상 또는 물리적 시스템에 공존할 수 없습니다.

기본적으로, 연결 서버를 설치할 때 HTML Access 구성 요소가 연결 서버 호스트에 설치됩니다. 이 구성 요소는 Horizon 7 사용자 포털 페이지에서 HTML Access 아이콘과 Horizon Client 아이콘을 표시하도록 구성합니다. 추가 아이콘을 통해 사용자는 자신의 데스크톱에 연결할 때 HTML Access를 선택할 수 있습니다.

HTML Access에 대한 연결 서버 설정 개요는 Horizon Client 설명서 페이지에 있는 "VMware Horizon HTML Access 설치 및 설정 가이드" 문서를 참조하십시오.

사전 요구 사항

- 네트워크에 연결 서버 인스턴스가 1개 이상 설치 및 구성되어 있는지 확인하십시오.
- 복제된 인스턴스를 설치하려면 Administrator 역할을 가진 사용자로 로그인해야 합니다. 연결 서버의 첫 번째 인스턴스를 설치할 때 Administrator 역할이 있는 계정 또는 그룹을 지정합니다. 이 역할은 로컬 관리자 그룹 또는 도메인 사용자 또는 그룹에 할당될 수 있습니다. [새 구성을 사용하여 Horizon 연결 서버 설치](#)를 참조하십시오.
- 기존 연결 서버 인스턴스가 복제된 인스턴스가 아닌 다른 도메인에 있는 경우, 도메인 사용자는 기존 인스턴스가 설치된 Windows Server 컴퓨터에 대해서도 Administrator 권한을 가지고 있어야 합니다.
- 연결 서버를 설치 중인 Windows Server 2008 R2 컴퓨터에 로그인하는 데 MIT Kerberos 인증을 사용하는 경우, <http://support.microsoft.com/kb/978116>의 KB 978116에 설명된 Microsoft 핫픽스를 설치하십시오.
- [Horizon 연결 서버 요구 사항](#)에 설명된 설치 요구 사항을 충족하는지 확인하십시오.
- 복제된 연결 서버 인스턴스가 설치되어 있는 컴퓨터가 고성능 LAN을 통해 연결되어 있는지 확인하십시오. [복제된 Horizon 연결 서버 인스턴스의 네트워크 요구 사항](#)을 참조하십시오.
- 설치 환경을 준비하십시오. [Horizon 연결 서버의 설치 전제 조건](#)을 참조하십시오.
- Horizon 7 5.1 이상인 복제된 연결 서버 인스턴스를 설치하고 복제할 기존 연결 서버 인스턴스가 Horizon 7 5.0.x 이하인 경우 데이터 복구 암호를 준비하십시오. [새 구성을 사용하여 Horizon 연결 서버 설치](#)를 참조하십시오.
- 연결 서버 인스턴스의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. [Horizon 연결 서버의 방화벽 규칙](#)을 참조하십시오.
- 연결 서버 인스턴스와 보안 서버를 연결하려는 경우, 고급 보안이 적용된 Windows 방화벽이 활성 프로파일에 **켜짐**으로 설정되어 있는지 확인하십시오. 모든 프로파일에 대해 이 설정을 **켜짐**으로 설정하는 것이 좋습니다. 기본적으로 IPsec 규칙은 보안 서버 및 연결 서버 간 연결을 통제하며 고급 보안이 적용된 Windows 방화벽이 사용되도록 설정되어야 합니다.
- 네트워크 토폴로지가 보안 서버와 연결 서버 인스턴스 간 백엔드 방화벽을 둔 경우 IPsec를 지원하도록 방화벽을 구성해야 합니다. [IPsec을 지원하도록 백엔드 방화벽 구성](#)을 참조하십시오.

절차

- 1 VMware 다운로드 사이트(<https://my.vmware.com/web/vmware/downloads>)에서 연결 서버 설치 관리자 파일을 다운로드합니다.

Desktop & End-User Computing에서 연결 서버가 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe입니다. 여기서 xxxxxx는 빌드 번호이며 y.y.y는 버전 번호입니다.

- 2 연결 서버 설치 프로그램을 시작하려면 설치 관리자 파일을 두 번 클릭합니다.
- 3 VMware 사용 약관에 동의하십시오.
- 4 대상 폴더를 수락하거나 변경하십시오.
- 5 **View 복제 서버** 설치 옵션을 선택하십시오.

- 6 IP(인터넷 프로토콜) 버전, **IPv4** 또는 **IPv6**을 선택합니다.

동일한 IP 버전으로 모든 Horizon 7 구성 요소를 설치해야 합니다.

- 7 FIPS 모드 사용 여부를 선택합니다.

이 옵션은 Windows에서 FIPS 모드를 사용하도록 설정된 경우에만 사용할 수 있습니다.

- 8 사용자가 HTML Access를 통해 자신의 데스크톱에 연결할 수 있도록 하려면 **HTML Access 설치**가 선택되었는지 확인합니다.

IPv4가 선택된 경우 이 설정이 기본적으로 선택됩니다. **IPv6**이 선택된 경우 IPv6 환경에서 HTML Access가 지원되지 않기 때문에 이 설정이 표시되지 않습니다.

- 9 복제 중인 기존 연결 서버 인스턴스의 호스트 이름 또는 IP 주소를 입력합니다.

- 10 데이터 복구 암호와 암호 알림(선택 사항)을 입력합니다.

복제할 기존 연결 서버 인스턴스가 Horizon 7 5.0.x 이하인 경우에만 데이터 복구 암호를 묻는 메시지가 표시됩니다.

- 11 Windows 방화벽 서비스 구성 방법을 선택합니다.

옵션	조치
자동으로 Windows 방화벽 구성	설치 관리자에서 Windows 방화벽을 구성해 필요한 네트워크 연결을 허용합니다.
Windows 방화벽 구성 안 함	Windows 방화벽 규칙을 수동으로 구성합니다. 조직에서 미리 정의된 자체 규칙을 사용하여 Windows 방화벽을 구성하는 경우에만 이 옵션을 선택하십시오.

- 12 복제된 인스턴스 설치를 종료하려면 설치 마법사를 완료하십시오.

- 13 Windows Server 컴퓨터에서 새 패치를 확인하고 필요에 따라 Windows 업데이트를 실행합니다.

연결 서버를 설치하기 전에 Windows Server 컴퓨터를 완전히 패치했더라도 설치 시 처음으로 운영 체제 기능을 사용하도록 설정할 수 있습니다. 이제 추가 패치가 필요할 수 있습니다.

Windows Server 컴퓨터에 Horizon 7 서비스가 설치되었습니다.

- VMware Horizon 연결 서버
- VMware Horizon View Framework 구성 요소
- VMware Horizon View Message Bus 구성 요소
- VMware Horizon View Script Host
- VMware Horizon View Security Gateway 구성 요소
- VMware Horizon View PCoIP 보안 게이트웨이
- VMware Horizon View Blast 보안 게이트웨이
- VMware Horizon View 웹 구성 요소
- View LDAP 디렉토리 서비스를 제공하는 VMware VDMDS

이러한 서비스에 대한 자세한 내용은 “Horizon 7 관리” 문서를 참조하십시오.

설치 중에 **HTML Access 설치** 설정을 지정한 경우 HTML Access 구성 요소가 Windows Server 컴퓨터에 설치됩니다. 이 구성 요소는 HTML Access 아이콘을 Horizon 7 사용자 포털 페이지에 구성하고 Windows 방화벽에서 **VMware Horizon View 연결 서버(Blast-In)** 규칙을 사용하도록 설정합니다. 이 방화벽 규칙을 통해 클라이언트 디바이스의 웹 브라우저가 TCP 포트 8443에서 연결 서버에 연결할 수 있습니다.

다음에 수행할 작업

연결 서버 인스턴스에 대해 SSL 서버 인증서를 구성합니다. [장 8 Horizon 7 서버를 위한 TLS 인증서 구성](#)을 참조하십시오.

연결 서버의 복제된 인스턴스에서 초기 Horizon 7 구성을 수행할 필요가 없습니다. 복제된 인스턴스는 기존 연결 서버 인스턴스의 구성을 상속합니다.

그러나 이 연결 서버 인스턴스에 대해 클라이언트 연결 설정을 구성해야 할 수 있으며, Windows Server 설정을 조정하여 대규모 배포를 지원하도록 할 수 있습니다. 자세한 내용은 [Horizon Client 연결 구성](#) 및 [Windows Server 설정을 크기 조정하여 배포 지원](#)의 내용을 참조하십시오.

연결 서버를 다시 설치하는 중이며 성능 데이터를 모니터링하도록 데이터 수집기 세트를 구성한 경우 데이터 수집기 세트를 중지하고 다시 시작합니다.

Horizon 연결 서버의 복제된 인스턴스 자동 설치

MSI(Microsoft Windows Installer)의 자동 설치 기능을 사용해 여러 Windows 컴퓨터에 연결 서버의 복제된 인스턴스를 설치할 수 있습니다. 자동 설치 시에는 명령줄을 사용하고 마법사 메시지에 응답할 필요가 없습니다.

자동 설치를 사용하면 대규모 기업에서 Horizon 7 구성 요소를 효과적으로 배포할 수 있습니다.

사전 요구 사항

- 네트워크에 연결 서버 인스턴스가 1개 이상 설치 및 구성되어 있는지 확인하십시오.

- 복제된 인스턴스를 설치하려면 Administrator 계정에 액세스할 수 있는 자격 증명을 가진 사용자 로 로그인해야 합니다. 연결 서버의 첫 번째 인스턴스를 설치할 때 Administrator 계정을 지정합니다. 이 계정은 로컬 관리자 그룹, 도메인 사용자 또는 그룹 계정이 될 수 있습니다. [새 구성을 사용하여 Horizon 연결 서버 설치](#)를 참조하십시오.
- 기존 연결 서버 인스턴스가 복제된 인스턴스가 아닌 다른 도메인에 있는 경우, 도메인 사용자는 기존 인스턴스가 설치된 Windows Server 컴퓨터에 대해서도 Administrator 권한을 가지고 있어야 합니다.
- 연결 서버를 설치 중인 Windows Server 2008 R2 컴퓨터에 로그인하는 데 MIT Kerberos 인증을 사용하는 경우, <http://support.microsoft.com/kb/978116>의 KB 978116에 설명된 Microsoft 핫픽스를 설치하십시오.
- [Horizon 연결 서버 요구 사항](#)에 설명된 설치 요구 사항을 충족하는지 확인하십시오.
- 복제된 연결 서버 인스턴스가 설치되어 있는 컴퓨터가 고성능 LAN을 통해 연결되어 있는지 확인하십시오. [복제된 Horizon 연결 서버 인스턴스의 네트워크 요구 사항](#)을 참조하십시오.
- 설치 환경을 준비하십시오. [Horizon 연결 서버의 설치 전제 조건](#)을 참조하십시오.
- 연결 서버 인스턴스의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. [Horizon 연결 서버의 방화벽 규칙](#)을 참조하십시오.
- 연결 서버 인스턴스와 보안 서버를 연결하려는 경우, 고급 보안이 적용된 Windows 방화벽이 활성 프로파일에 **켜짐**으로 설정되어 있는지 확인하십시오. 모든 프로파일에 대해 이 설정을 **켜짐**으로 설정하는 것이 좋습니다. 기본적으로 IPsec 규칙은 보안 서버 및 연결 서버 간 연결을 통제하며 고급 보안이 적용된 Windows 방화벽이 사용되도록 설정되어야 합니다.
- 네트워크 토폴로지가 보안 서버와 연결 서버 인스턴스 간 백엔드 방화벽을 둔 경우 IPsec를 지원하도록 방화벽을 구성해야 합니다. [IPsec을 지원하도록 백엔드 방화벽 구성](#)을 참조하십시오.
- MSI 설치 관리자 명령줄 옵션을 숙지하십시오. [Microsoft Windows Installer 명령줄 옵션](#)을 참조하십시오.
- 연결 서버의 복제 설치에 사용할 수 있는 자동 설치 속성을 숙지하십시오. [Horizon 연결 서버의 복제된 인스턴스 자동 설치 속성](#)을 참조하십시오.

절차

- 1 VMware 다운로드 사이트(<https://my.vmware.com/web/vmware/downloads>)에서 연결 서버 설치 관리자 파일을 다운로드합니다.

Desktop & End-User Computing에서 연결 서버가 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe입니다. 여기서 xxxxxx는 빌드 번호이며 y.y.y는 버전 번호입니다.

- 2 Windows Server 컴퓨터에서 명령 프롬프트를 엽니다.
- 3 설치 명령을 한 줄에 입력하십시오.

예: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2
ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544"

View 5.1 이상인 복제된 연결 서버 인스턴스를 설치하고 복제할 기존 연결 서버 인스턴스가 View 5.0.x 이하인 경우 데이터 복구 암호를 지정해야만 암호 알림을 추가할 수 있습니다. 예: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2
 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544
 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER="First car""

중요 자동 설치를 수행할 경우 데이터 복구 암호를 포함한 전체 명령줄이 설치 관리자의 vminst.log 파일에 기록됩니다. 설치가 완료되면 이 로그 파일을 삭제하거나 Horizon Administrator를 사용하여 데이터 복구 암호를 변경하십시오.

4 Windows Server 컴퓨터에서 새 패치를 확인하고 필요에 따라 Windows 업데이트를 실행합니다.

연결 서버를 설치하기 전에 Windows Server 컴퓨터를 완전히 패치했더라도 설치 시 처음으로 운영 체제 기능을 사용하도록 설정할 수 있습니다. 이제 추가 패치가 필요할 수 있습니다.

Windows Server 컴퓨터에 Horizon 7 서비스가 설치되었습니다.

- VMware Horizon 연결 서버
- VMware Horizon View Framework 구성 요소
- VMware Horizon View Message Bus 구성 요소
- VMware Horizon View Script Host
- VMware Horizon View Security Gateway 구성 요소
- VMware Horizon View PCoIP 보안 게이트웨이
- VMware Horizon View Blast 보안 게이트웨이
- VMware Horizon View 웹 구성 요소
- View LDAP 디렉토리 서비스를 제공하는 VMware VDMDS

이러한 서비스에 대한 자세한 내용은 "Horizon 7 관리" 문서를 참조하십시오.

설치 중에 **HTML Access 설치** 설정을 지정한 경우 HTML Access 구성 요소가 Windows Server 컴퓨터에 설치됩니다. 이 구성 요소는 HTML Access 아이콘을 Horizon 7 사용자 포털 페이지에 구성하고 Windows 방화벽에서 **VMware Horizon View 연결 서버(Blast-In)** 규칙을 사용하도록 설정합니다. 이 방화벽 규칙을 통해 클라이언트 디바이스의 웹 브라우저가 TCP 포트 8443에서 연결 서버에 연결할 수 있습니다.

다음에 수행할 작업

연결 서버 인스턴스에 대해 SSL 서버 인증서를 구성합니다. [장 8 Horizon 7 서버를 위한 TLS 인증서 구성](#)를 참조하십시오.

연결 서버의 복제된 인스턴스에서 초기 Horizon 7 구성을 수행할 필요가 없습니다. 복제된 인스턴스는 기존 연결 서버 인스턴스의 구성을 상속합니다.

그러나 이 연결 서버 인스턴스에 대해 클라이언트 연결 설정을 구성해야 할 수 있으며, Windows Server 설정을 조정하여 대규모 배포를 지원하도록 할 수 있습니다. 자세한 내용은 [Horizon Client 연결 구성](#) 및 [Windows Server 설정을 크기 조정하여 배포 지원](#)의 내용을 참조하십시오.

Horizon 연결 서버의 복제된 인스턴스 자동 설치 속성

명령줄에서 복제된 Horizon 연결 서버 인스턴스를 자동 설치할 때 특정 속성이 포함될 수 있습니다. MSI(Microsoft Windows Installer)가 속성 및 값을 해석할 수 있도록 *PROPERTY=value* 형식을 사용해야 합니다.

표 7-2. Horizon 연결 서버의 복제된 인스턴스 자동 설치를 위한 MSI 속성

MSI 속성	설명	기본 값
INSTALLDIR	연결 서버 소프트웨어가 설치된 경로 및 폴더입니다. 예: INSTALLDIR="D:\abc\my folder" 해당 경로를 둘러싸고 있는 큰따옴표 두 쌍은 MSI 설치 관리자가 공백을 경로의 유효한 부분으로 해석하도록 합니다. 이 MSI 속성은 선택 사항입니다.	%ProgramFiles%\VMware\VMware View WServer
VDM_SERVER_INSTANCE_TYPE	연결 서버 설치 유형: ■ 1. 표준 설치 ■ 2. 복제 설치 ■ 3. 보안 서버 설치 복제된 인스턴스를 설치하려면 VDM_SERVER_INSTANCE_TYPE=2를 정의하십시오. 이 MSI 속성은 복제본 설치 시 필수입니다.	1
ADAM_PRIMARY_NAME	복제 중인 기존 연결 서버 인스턴스의 호스트 이름이나 IP 주소입니다. 예: ADAM_PRIMARY_NAME=cs1.companydomain.com 이 MSI 속성은 필수입니다.	없음
FWCHOICE	연결 서버 인스턴스의 방화벽을 구성할지 여부를 결정하는 MSI 속성입니다. 1의 값은 방화벽을 구성합니다. 2의 값은 방화벽을 구성하지 않습니다. 예: FWCHOICE=1 이 MSI 속성은 선택 사항입니다.	1
VDM_SERVER_RECOVERY_PWD	데이터 복구 암호입니다. 데이터 복구 암호가 View LDAP에 설정되어 있지 않은 경우 이 속성이 필수입니다. 참고 복제할 표준 연결 서버 인스턴스가 View 5.0 이하이면 데이터 복구 암호가 View LDAP에 설정되지 않습니다. 복제할 연결 서버 인스턴스가 View 5.1 이상이면 이 속성을 입력하지 않아도 됩니다. 암호는 1 ~ 128자 사이여야 합니다. 조직의 모범 사례에 따라 보안 암호를 생성하십시오.	없음
VDM_SERVER_RECOVERY_PWD_REMINDER	데이터 복구 암호 알림입니다. 이 속성은 선택 사항입니다.	없음

표 7-2. Horizon 연결 서버의 복제된 인스턴스 자동 설치를 위한 MSI 속성 (계속)

MSI 속성	설명	기본 값
VDM_IP_PROTOCOL_USAGE	Horizon 7 구성 요소가 통신에 사용하는 IP 버전을 지정합니다. 가능한 값은 IPv4 및 IPv6 입니다.	IPv4
VDM_FIPS_ENABLED	FIPS 모드 사용 여부를 지정합니다. 값이 1이면 FIPS 모드를 활성화합니다. 값이 0이면 FIPS 모드를 비활성화합니다. 이 속성을 1로 설정했는데 Windows가 FIPS 모드에 있지 않으면 설치 관리자가 중단됩니다.	0

보안 서버 연결 암호 구성

보안 서버를 설치하기 전에 보안 서버 연결 암호를 구성해야 합니다. 연결 서버 설치 프로그램을 사용해 보안 서버를 설치하면 설치 도중 이 암호를 묻는 메시지가 표시됩니다.

보안 서버 연결 암호는 보안 서버와 연결 서버 인스턴스를 연결하는 일회성 암호입니다. 연결 서버 설치 프로그램에 암호를 입력하면 해당 암호는 더 이상 사용할 수 없습니다.

참고 이전 버전의 보안 서버와 현재 버전의 연결 서버를 연결할 수 없습니다. 현재 버전의 연결 서버에서 연결 암호를 구성하고 이전 버전의 보안 서버를 설치하려고 하면 연결 암호가 무효화됩니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 [연결 서버] 탭에서 보안 서버와 연결할 연결 서버 인스턴스를 선택합니다.
- 3 **추가 명령** 드롭다운 메뉴에서 **보안 서버 연결 암호 지정**을 선택하십시오.
- 4 연결 암호와 암호 확인 텍스트 상자에 암호를 입력하고 암호 시간 초과 값을 지정하십시오.
지정된 제한 시간 내에 암호를 사용해야 합니다.
- 5 암호를 구성하려면 **확인**을 클릭합니다.

다음에 수행할 작업

보안 서버를 설치합니다. [보안 서버 설치](#) 항목을 참조하십시오.

중요 암호 제한 시간 내에 연결 서버 설치 프로그램에 보안 서버 연결 암호를 입력하지 않으면 암호는 더 이상 유효하지 않으므로 새 암호를 구성해야 합니다.

보안 서버 설치

보안 서버는 인터넷과 내부 네트워크 사이에 보안 계층을 추가하는 연결 서버 인스턴스입니다. 연결 서버 인스턴스에 연결될 수 있도록 보안 서버를 1개 이상 설치할 수 있습니다.

보안 서버 소프트웨어는 복제 서버, 연결 서버, View Composer, Horizon Agent 또는 Horizon Client를 포함하여 기타 모든 Horizon 7 소프트웨어 구성 요소가 포함된 동일한 가상 또는 물리적 시스템에 공존할 수 없습니다.

사전 요구 사항

- 사용할 토폴로지 유형을 지정하십시오. 예를 들어 사용할 로드 밸런싱 솔루션을 지정하십시오. 보안 서버에 연결된 연결 서버 인스턴스를 외부 네트워크 사용자 전용으로 사용할 것인지 결정하십시오. 자세한 내용은 "Horizon 7 아키텍처 계획" 문서를 참조하십시오.

중요 로드 밸런서를 사용하는 경우 변경되지 않는 IP 주소가 있어야 합니다. IPv4 환경에서 정적 IP 주소를 구성합니다. IPv6 환경에서 시스템은 변경되지 않는 IP 주소를 자동으로 가져옵니다.

- [Horizon 연결 서버 요구 사항](#)에 설명된 설치 요구 사항을 충족하는지 확인하십시오.
- 설치 환경을 준비하십시오. [Horizon 연결 서버의 설치 전제 조건](#)의 내용을 참조하십시오.
- 보안 서버에 연결할 연결 서버 인스턴스가 설치 및 구성되어 있으며 해당 보안 서버 버전과 호환되는 연결 서버 버전을 실행 중인지 확인하십시오. "Horizon 7 업그레이드" 문서에서 "Horizon 7 구성 요소 호환성 매트릭스"를 참조하십시오.
- 보안 서버에 연결할 연결 서버 인스턴스에서 보안 서버를 설치할 컴퓨터에 액세스할 수 있는지 확인하십시오.

참고 연결 서버가 Horizon 7 버전 7.5로 업그레이드된 후에 IPsec이 사용되지 않도록 설정된 보안 서버를 다시 설치해야 합니다. 보안 서버의 IP 주소가 변경되면 다시 설치해야 합니다. 보안 서버가 동적 NAT 뒤에 있는 경우 보안 서버 연결이 제대로 작동하지 않습니다.

- 보안 서버 연결 암호를 구성하십시오. [보안 서버 연결 암호 구성](#)의 내용을 참조하십시오.
- 외부 URL 형식을 숙지하십시오. [보안 게이트웨이 및 터널 연결용 외부 URL 구성](#)의 내용을 참조하십시오.
- 고급 보안이 포함된 Windows 방화벽이 활성 프로파일에 **켜짐**으로 설정되어 있는지 확인하십시오. 모든 프로파일에 대해 이 설정을 **켜짐**으로 설정하는 것이 좋습니다. 기본적으로 IPsec 규칙은 보안 서버 및 View 연결 서버 간 연결을 통제하며 고급 보안이 포함된 Windows 방화벽이 사용되도록 설정되어야 합니다.
- 보안 서버의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. [Horizon 연결 서버의 방화벽 규칙](#)의 내용을 참조하십시오.
- 네트워크 토폴로지가 보안 서버와 연결 서버 간 백엔드 방화벽을 둔 경우 IPsec를 지원하도록 방화벽을 구성해야 합니다. [IPsec을 지원하도록 백엔드 방화벽 구성](#)의 내용을 참조하십시오.
- 보안 서버를 업그레이드하거나 다시 설치할 경우 보안 서버의 기존 IPsec 규칙이 제거되었는지 확인하십시오. [보안 서버에 대한 IPsec 규칙 제거](#)의 내용을 참조하십시오.
- Horizon 7을 FIPS 모드에서 설치하는 경우, FIPS 모드에서는 보안 서버를 설치한 후에 IPsec를 수동으로 구성해야 하기 때문에 Horizon Administrator에서 전역 설정 **보안 서버 연결용 IPsec 사용**을 선택 취소해야 합니다.

절차

- 1 VMware 다운로드 사이트(<https://my.vmware.com/web/vmware/downloads>)에서 연결 서버 설치 관리자 파일을 다운로드합니다.

Desktop & End-User Computing에서 연결 서버가 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

설치 관리자 파일 이름은 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`입니다. 여기서 `xxxxxx`는 빌드 번호이며 `y.y.y`는 버전 번호입니다.

- 2 연결 서버 설치 프로그램을 시작하려면 설치 관리자 파일을 두 번 클릭합니다.
- 3 VMware 사용 약관에 동의하십시오.
- 4 대상 폴더를 수락하거나 변경하십시오.
- 5 **View 보안 서버** 설치 옵션을 선택하십시오.

- 6 IP(인터넷 프로토콜) 버전, **IPv4** 또는 **IPv6**을 선택합니다.

동일한 IP 버전으로 모든 Horizon 7 구성 요소를 설치해야 합니다.

- 7 FIPS 모드 사용 여부를 선택합니다.

이 옵션은 Windows에서 FIPS 모드를 사용하도록 설정된 경우에만 사용할 수 있습니다.

- 8 보안 서버에 연결할 연결 서버 인스턴스의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 **서버** 텍스트 상자에 입력합니다.

보안 서버에서 이 연결 서버 인스턴스에 네트워크 트래픽을 전송합니다.

- 9 **암호** 텍스트 상자에 보안 서버 연결 암호를 입력합니다.

암호가 만료된 경우 Horizon Administrator를 사용해 새 암호를 구성하고 설치 프로그램에 새 암호를 입력할 수 있습니다.

- 10 **외부 URL** 텍스트 상자에 보안 서버의 외부 URL을 입력합니다. 이 작업은 사용하는 디스플레이 프로토콜과 관계없이 모든 클라이언트에 필요합니다.

URL에는 프로토콜 식별자(`https`), 클라이언트가 확인 가능한 보안 서버 이름 및 포트 번호(`443`)가 포함되어야 합니다.

예: `https://view.example.com:443`

네트워크 외부의 터널 지원 클라이언트는 URL을 사용하여 보안 서버를 통해 네트워크 내부의 시스템에 연결합니다.

- 11 **PCoIP 외부 URL** 텍스트 상자에 보안 서버 PCoIP 게이트웨이의 외부 URL을 입력합니다. 이 작업은 PCoIP 디스플레이 프로토콜을 사용하여 원격 데스크톱에 연결하는 클라이언트에 필요합니다.

프로토콜 상대 URL에는 보안 서버 IP 주소와 포트 번호(`4172`)가 포함되어야 합니다. IPv4 환경에서는 IPv4 주소를 사용합니다. IPv6 환경에서는 IPv6 주소를 사용합니다.

IPv4 환경의 예: `10.20.30.40:4172`

네트워크 외부의 PColP 지원 클라이언트는 URL을 사용하여 보안 서버를 통해 네트워크 내부의 시스템에 연결합니다.

참고 IPv6 환경에 있는 경우 IPv6 주소를 여기에 입력해야 하지만 설치 후 클라이언트에서 확인할 수 있는 이름으로 교체할 수도 있습니다.

12 Blast 외부 URL 텍스트 상자에 보안 서버 Blast 게이트웨이의 외부 URL을 입력합니다. 이 작업은 Blast 디스플레이 프로토콜 또는 HTML Access를 사용하여 원격 데스크톱에 연결하는 클라이언트에 필요합니다.

URL에는 프로토콜 식별자(https), 클라이언트가 확인 가능한 보안 서버 이름 및 포트 번호(8443)가 포함되어야 합니다.

예: https://myserver.example.com:8443

네트워크 외부의 Blast 지원 및 HTML Access 클라이언트는 URL을 사용하여 보안 서버를 통해 네트워크 내부의 시스템에 연결합니다.

13 Windows 방화벽 서비스 구성 방법을 선택합니다.

옵션	조치
자동으로 Windows 방화벽 구성	설치 관리자에서 Windows 방화벽을 구성해 필요한 네트워크 연결을 허용합니다.
Windows 방화벽 구성 안 함	Windows 방화벽 규칙을 수동으로 구성합니다. 조직에서 미리 정의된 자체 규칙을 사용하여 Windows 방화벽을 구성하는 경우에만 이 옵션을 선택하십시오.

14 보안 서버 설치를 종료하려면 설치 마법사를 완료하십시오.

Windows Server 컴퓨터에 보안 서버 서비스가 설치됩니다.

- VMware Horizon View 보안 서버
- VMware Horizon View Framework 구성 요소
- VMware Horizon View Security Gateway 구성 요소
- VMware Horizon View PColP 보안 게이트웨이
- VMware Blast 보안 게이트웨이

이러한 서비스에 대한 자세한 내용은 "Horizon 7 관리" 문서를 참조하십시오.

Horizon Administrator의 [보안 서버] 창에 보안 서버가 나타납니다.

VMware Horizon View 연결 서버(Blast-In) 규칙은 보안 서버의 Windows 방화벽에서 활성화됩니다. 이 방화벽 규칙을 통해 클라이언트 디바이스의 웹 브라우저가 HTML Access를 사용하여 TCP 포트 8443에서 보안 서버에 연결할 수 있습니다.

참고 설치가 취소되거나 중단될 경우 설치를 다시 시작하기 위해 보안 서버의 IPsec 규칙을 제거해야 할 수 있습니다. 보안 서버를 다시 설치하거나 업그레이드하기 전에 이미 IPsec 규칙을 제거한 경우에도 이 단계를 수행하십시오. IPsec 규칙 제거 관련 지침은 [보안 서버에 대한 IPsec 규칙 제거](#)를 참조하십시오.

다음에 수행할 작업

보안 서버를 위한 SSL 서버 인증서를 구성하십시오. [장 8 Horizon 7 서버를 위한 TLS 인증서 구성](#)의 내용을 참조하십시오.

보안 서버에 대해 클라이언트 연결 설정을 구성해야 할 수 있으며, Windows Server 설정을 조정하여 대규모 배포를 지원하도록 할 수 있습니다. 자세한 내용은 [Horizon Client 연결 구성](#) 및 [Windows Server 설정을 크기 조정하여 배포 지원](#)의 내용을 참조하십시오.

보안 서버를 다시 설치하고 성능 데이터를 모니터링하도록 데이터 수집기 세트를 구성한 경우 데이터 수집기 세트를 중지하고 다시 시작합니다.

보안 서버 자동 설치

MSI(Microsoft Windows Installer)의 자동 설치 기능을 사용해 여러 Windows 컴퓨터에 보안 서버를 설치할 수 있습니다. 자동 설치 시에는 명령줄을 사용하고 마법사 메시지에 응답할 필요가 없습니다.

자동 설치를 사용하면 대규모 기업에서 Horizon 7 구성 요소를 효과적으로 배포할 수 있습니다.

사전 요구 사항

- 사용할 토폴로지 유형을 지정하십시오. 예를 들어 사용할 로드 밸런싱 솔루션을 지정하십시오. 보안 서버에 연결된 연결 서버 인스턴스를 외부 네트워크 사용자 전용으로 사용할 것인지 결정하십시오. 자세한 내용은 "Horizon 7 아키텍처 계획" 문서를 참조하십시오.

중요 로드 밸런서를 사용하는 경우 변경되지 않는 IP 주소가 있어야 합니다. IPv4 환경에서 정적 IP 주소를 구성합니다. IPv6 환경에서 시스템은 변경되지 않는 IP 주소를 자동으로 가져옵니다.

- [Horizon 연결 서버 요구 사항](#)에 설명된 설치 요구 사항을 충족하는지 확인하십시오.
- 설치 환경을 준비하십시오. [Horizon 연결 서버의 설치 전제 조건](#)를 참조하십시오.
- 보안 서버에 연결할 연결 서버 인스턴스가 설치 및 구성되어 있으며 해당 보안 서버 버전과 호환되는 연결 서버 버전을 실행 중인지 확인하십시오. "Horizon 7 업그레이드" 문서에서 "Horizon 7 구성 요소 호환성 매트릭스"를 참조하십시오.
- 보안 서버에 연결할 연결 서버 인스턴스에서 보안 서버를 설치할 컴퓨터에 액세스할 수 있는지 확인하십시오.

참고 연결 서버가 Horizon 7 버전 7.5로 업그레이드된 후에 IPsec이 사용되지 않도록 설정된 보안 서버를 다시 설치해야 합니다. 보안 서버의 IP 주소가 변경되면 다시 설치해야 합니다. 보안 서버가 동적 NAT 뒤에 있는 경우 보안 서버 연결이 제대로 작동하지 않습니다.

- 보안 서버 연결 암호를 구성하십시오. [보안 서버 연결 암호 구성](#)를 참조하십시오.
- 외부 URL 형식을 숙지하십시오. [보안 게이트웨이 및 터널 연결용 외부 URL 구성](#)를 참조하십시오.
- 고급 보안이 포함된 Windows 방화벽이 활성 프로파일에 **켜짐**으로 설정되어 있는지 확인하십시오. 모든 프로파일에 대해 이 설정을 **켜짐**으로 설정하는 것이 좋습니다. 기본적으로 IPsec 규칙은 보안 서버 및 연결 서버 간 연결을 통제하며 고급 보안이 적용된 Windows 방화벽이 사용되도록 설정되어야 합니다.

- 보안 서버의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. [Horizon 연결 서버의 방화벽 규칙](#)을 참조하십시오.
- 네트워크 토폴로지가 보안 서버와 연결 서버 간 백엔드 방화벽을 둔 경우 IPsec를 지원하도록 방화벽을 구성해야 합니다. [IPsec을 지원하도록 백엔드 방화벽 구성](#)을 참조하십시오.
- 보안 서버를 업그레이드하거나 다시 설치할 경우 보안 서버의 기존 IPsec 규칙이 제거되었는지 확인하십시오. [보안 서버에 대한 IPsec 규칙 제거](#)을 참조하십시오.
- MSI 설치 관리자 명령줄 옵션을 숙지하십시오. [Microsoft Windows Installer 명령줄 옵션](#)을 참조하십시오.
- 보안 서버에서 사용할 수 있는 자동 설치 속성을 숙지하십시오. [보안 서버 자동 설치 속성](#)을 참조하십시오.
- Horizon 7을 FIPS 모드에서 설치하는 경우, FIPS 모드에서는 보안 서버를 설치한 후에 IPsec를 수동으로 구성해야 하기 때문에 Horizon Administrator에서 전역 설정 **보안 서버 연결용 IPsec 사용**을 선택 취소해야 합니다.

절차

- 1 VMware 다운로드 사이트(<https://my.vmware.com/web/vmware/downloads>)에서 연결 서버 설치 관리자 파일을 다운로드합니다.

Desktop & End-User Computing에서 연결 서버가 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

설치 관리자 파일 이름은 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`입니다. 여기서 `xxxxxx`는 빌드 번호이며 `y.y.y`는 버전 번호입니다.

- 2 Windows Server 컴퓨터에서 명령 프롬프트를 엽니다.
- 3 설치 명령을 한 줄에 입력하십시오.

```
예: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3
VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443
VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 VDM_SERVER_SS_PCOIP_TCPPORT=4172
VDM_SERVER_SS_PCOIP_UDPPORT=4172 VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443
VDM_SERVER_SS_PWD=secret"
```

Windows Server 컴퓨터에 보안 서버 서비스가 설치됩니다.

- VMware Horizon View 보안 서버
- VMware Horizon View Framework 구성 요소
- VMware Horizon View Security Gateway 구성 요소
- VMware Horizon View PCoIP 보안 게이트웨이
- VMware Blast 보안 게이트웨이

이러한 서비스에 대한 자세한 내용은 "Horizon 7 관리" 문서를 참조하십시오.

Horizon Administrator의 [보안 서버] 창에 보안 서버가 나타납니다.

VMware Horizon View 연결 서버(Blast-In) 규칙은 보안 서버의 Windows 방화벽에서 활성화됩니다. 이 방화벽 규칙을 통해 클라이언트 디바이스의 웹 브라우저가 HTML Access를 사용하여 TCP 포트 8443에서 보안 서버에 연결할 수 있습니다.

참고 설치가 취소되거나 중단될 경우 설치를 다시 시작하기 위해 보안 서버의 IPsec 규칙을 제거해야 할 수 있습니다. 보안 서버를 다시 설치하거나 업그레이드하기 전에 이미 IPsec 규칙을 제거한 경우에도 이 단계를 수행하십시오. IPsec 규칙 제거 관련 지침은 [보안 서버에 대한 IPsec 규칙 제거](#)를 참조하십시오.

다음에 수행할 작업

보안 서버를 위한 SSL 서버 인증서를 구성하십시오. [장 8 Horizon 7 서버를 위한 TLS 인증서 구성](#)를 참조하십시오.

보안 서버에 대해 클라이언트 연결 설정을 구성해야 할 수 있으며, Windows Server 설정을 조정하여 대규모 배포를 지원하도록 할 수 있습니다. 자세한 내용은 [Horizon Client 연결 구성](#) 및 [Windows Server 설정을 크기 조정하여 배포 지원](#)의 내용을 참조하십시오.

보안 서버 자동 설치 속성

명령줄에서 보안 서버를 자동 설치할 때 특정 속성이 포함될 수 있습니다. MSI(Microsoft Windows Installer)가 속성 및 값을 해석할 수 있도록 *PROPERTY=value* 형식을 사용해야 합니다.

표 7-3. 보안 서버 자동 설치를 위한 MSI 속성

MSI 속성	설명	기본 값
INSTALLDIR	연결 서버 소프트웨어가 설치된 경로 및 폴더입니다. 예: INSTALLDIR="D:\abc\my folder" 해당 경로를 둘러싸고 있는 큰따옴표 두 쌍은 MSI 설치 관리자가 공백을 경로의 유효한 부분으로 해석하도록 합니다. 이 MSI 속성은 선택 사항입니다.	%ProgramFiles%\VMware\VMware View WServer
VDM_SERVER_INSTANCE_TYPE	연결 서버 설치 유형: ■ 1. 표준 설치 ■ 2. 복제 설치 ■ 3. 보안 서버 설치 보안 서버를 설치하려면 VDM_SERVER_INSTANCE_TYPE=3을 정의하십시오. 이 MSI 속성은 보안 서버 설치 시 필수입니다.	1
VDM_SERVER_NAME	보안 서버와 연결할 기존 연결 서버 인스턴스의 호스트 이름이나 IP 주소입니다. 예: VDM_SERVER_NAME=cs1.internaldomain.com 이 MSI 속성은 필수입니다.	없음
VDM_SERVER_SS_EXTURL	보안 서버의 외부 URL입니다. URL에는 프로토콜, 외부에서 확인 가능한 보안 서버 이름 및 포트 번호가 포함되어야 합니다. 예: VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443 이 MSI 속성은 필수입니다.	없음

표 7-3. 보안 서버 자동 설치를 위한 MSI 속성 (계속)

MSI 속성	설명	기본 값
VDM_SERVER_SS_PWD	보안 서버 연결 암호입니다. 예: VDM_SERVER_SS_PWD=secret 이 MSI 속성은 필수입니다.	없음
FWCHOICE	연결 서버 인스턴스의 방화벽을 구성할지 여부를 결정하는 MSI 속성입니다. 1의 값은 방화벽을 구성합니다. 2의 값은 방화벽을 구성하지 않습니다. 예: FWCHOICE=1 이 MSI 속성은 선택 사항입니다.	1
VDM_SERVER_SS_PCOIP_IPADDR	PCoIP 보안 게이트웨이 외부 IP 주소입니다. IPv6 환경에서는 이 속성을 PCoIP 보안 게이트웨이의 FQDN으로 설정할 수도 있습니다. 이 속성은 보안 서버가 Windows Server 2008 R2 이상에 설치될 경우에만 지원됩니다. 예: VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 이 속성은 PCoIP Secure Gateway 구성 요소를 사용할 계획인 경우 필수입니다.	없음
VDM_SERVER_SS_PCOIP_TCPPORT	PCoIP 보안 게이트웨이 외부 TCP 포트 번호입니다. 이 속성은 보안 서버가 Windows Server 2008 R2 이상에 설치될 경우에만 지원됩니다. 예: VDM_SERVER_SS_PCOIP_TCPPORT=4172 이 속성은 PCoIP Secure Gateway 구성 요소를 사용할 계획인 경우 필수입니다.	없음
VDM_SERVER_SS_PCOIP_UDPPORT	PCoIP 보안 게이트웨이 외부 UDP 포트 번호입니다. 이 속성은 보안 서버가 Windows Server 2008 R2 이상에 설치될 경우에만 지원됩니다. 예: VDM_SERVER_SS_PCOIP_UDPPORT=4172 이 속성은 PCoIP Secure Gateway 구성 요소를 사용할 계획인 경우 필수입니다.	없음
VDM_SERVER_SS_BSG_EXTURL	Blast 보안 게이트웨이 외부 URL입니다. URL에는 HTTPS 프로토콜, 외부에서 확인 가능한 보안 서버 이름 및 포트 번호가 포함되어야 합니다. 예: VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443 기본 포트 번호는 8443입니다. 사용자가 Horizon 7 데스크톱에 대해 웹 연결을 수행할 수 있도록 하려면 보안 서버에 Blast 보안 게이트웨이를 설치해야 합니다.	없음
VDM_SERVER_SS_FORCE_IPSEC	IPsec가 보안 서버와 연결된 연결 서버 인스턴스 간에 강제로 사용되도록 합니다. 기본적으로 IPsec를 사용하지 않도록 설정한 상태에서 보안 서버를 무인 설치하고 연결 서버 인스턴스에 연결하면 연결이 실패합니다. 기본값 1은 IPsec 연결을 강제합니다. IPsec 없이 연결할 수 있도록 하려면 이 값을 0으로 설정하십시오.	1

표 7-3. 보안 서버 자동 설치를 위한 MSI 속성 (계속)

MSI 속성	설명	기본 값
VDM_IP_PROTOCOL_USA GE	Horizon 7 구성 요소가 통신에 사용하는 IP 버전을 지정합니다. 가능 한 값은 IPv4 및 IPv6 입니다.	IPv4
VDM_FIPS_ENABLED	FIPS 모드 사용 여부를 지정합니다. 값이 1이면 FIPS 모드를 활성화 합니다. 값이 0이면 FIPS 모드를 비활성화합니다. 이 속성을 1로 설정 했는데 Windows가 FIPS 모드에 있지 않으면 설치 관리자가 중단됩 니다.	0

보안 서버에 대한 IPsec 규칙 제거

보안 서버 인스턴스를 업그레이드하거나 재설치하려면 먼저 보안 서버와 연결된 연결 서버 인스턴스 간의 통신을 관리하는 현재 IPsec 규칙을 제거해야 합니다. 이 단계를 수행하지 않으면 업그레이드 또는 재설치가 실패합니다.

기본적으로 보안 서버와 연결된 연결 서버 인스턴스 간의 통신은 IPsec 규칙에 의해 관리됩니다. 보안 서버를 업그레이드하거나 재설치하고 연결 서버 인스턴스와 다시 연결할 경우 새로운 IPsec 규칙 집합을 구성해야 합니다. 업그레이드 또는 재설치 전에 기존 IPsec 규칙을 제거하지 않으면 연결이 실패합니다.

보안 서버를 업그레이드하거나 재설치하고 IPsec를 사용해 보안 서버와 연결 서버 간의 통신을 보호하려는 경우 이 단계를 수행해야 합니다.

IPsec 규칙을 사용하지 않고 초기 보안 서버 연결을 구성할 수 있습니다. 보안 서버를 설치하기 전에 Horizon Administrator를 열고 기본적으로 사용하도록 설정된 전역 설정인 **보안 서버 연결용 IPsec 사용**을 선택 해제하십시오. IPsec 규칙이 적용되지 않을 경우 업그레이드 또는 재설치 전에 IPsec 규칙을 제거하지 않아도 됩니다.

참고 보안 서버를 업그레이드하거나 재설치하기 전에 Horizon Administrator에서 보안 서버를 제거하지 않아도 됩니다. Horizon 7 환경에서 보안 서버를 영구적으로 제거하려는 경우에만 Horizon Administrator에서 보안 서버를 제거하십시오.

5.0.x 이전 릴리스에서는 Horizon Administrator 사용자 인터페이스 내에서 또는 `vdadmin -S` 명령줄 명령을 사용해 보안 서버를 제거할 수 있습니다. View 5.1 이상 릴리스에서는 `vdadmin -S`를 사용해야 합니다. "Horizon 7 관리" 문서의 "-S 옵션을 사용하여 Horizon 연결 서버 인스턴스 또는 보안 서버의 항목 제거"를 참조하십시오.

경고 활성화 보안 서버의 IPsec 규칙을 제거하면 보안 서버를 업그레이드하거나 재설치할 때까지 보안 서버와의 통신이 끊어집니다. 따라서 로드 밸런서를 사용하여 보안 서버 그룹을 관리하는 경우 한 대의 서버에서 이 절차를 수행한 다음 해당 서버를 업그레이드한 후에 다음 서버에 대한 IPsec 규칙을 제거하십시오. 운영에서 서버를 제거한 후 이 방식으로 일대일로 다시 추가하여 최종 사용자의 다운타임을 피할 수 있습니다.

절차

1 Horizon Administrator에서 **View 구성 > 서버**를 클릭합니다.

2 보안 서버 탭에서 보안 서버를 선택하고 **추가 명령 > 업그레이드 또는 재설치 준비**를 클릭합니다.

보안 서버를 설치하기 전에 IPsec 규칙을 사용하지 않도록 설정한 경우 이 설정이 비활성화됩니다. 이 경우 재설치 또는 업그레이드 전에 IPsec 규칙을 제거하지 않아도 됩니다.

3 확인을 클릭합니다.

IPsec 규칙이 제거되고 **업그레이드 또는 재설치 준비** 설정이 비활성화되면 보안 서버를 재설치하거나 업그레이드할 수 있음을 나타냅니다.

다음에 수행할 작업

보안 서버를 업그레이드하거나 재설치합니다.

VPN보다 나은 Unified Access Gateway 장치의 이점

Unified Access Gateway 장치는 회사 방화벽 외부에서 원격 데스크톱 및 애플리케이션으로 안전하게 액세스하기 위한 기본 게이트웨이입니다.

최신 버전의 Unified Access Gateway 설명서를 보려면 <https://docs.vmware.com/kr/Unified-Access-Gateway/index.html>의 "VMware Unified Access Gateway 배포 및 구성" 문서를 참조하십시오.

Unified Access Gateway 장치는 네트워크 DMZ(비무장 지대) 내에 상주하고, 신뢰할 수 있는 네트워크 내의 연결을 위한 프록시 호스트 역할을 하며, 공용 인터넷에서 가상 데스크톱, 애플리케이션 호스트 및 서버를 보호함으로써 추가적인 보안 계층을 제공합니다.

Unified Access Gateway 장치 구성

Unified Access Gateway 및 일반 VPN 솔루션은 강력하게 인증된 사용자에게 대한 트래픽만 내부 네트워크로 전달되도록 한다는 측면에서 서로 유사합니다.

일반 VPN과 비교할 때 Unified Access Gateway의 장점은 다음과 같습니다.

- Access Control Manager. Unified Access Gateway는 액세스 규칙을 자동으로 적용합니다. Unified Access Gateway는 내부적으로 연결하는 데 필요한 사용자의 사용 권한 및 주소 지정을 인식합니다. 대부분의 VPN은 관리자가 모든 사용자 또는 사용자 그룹에 대한 네트워크 연결 규칙을 개별적으로 구성할 수 있도록 하므로 VPN 하나로도 동일한 역할을 합니다. 처음에는 VPN 하나로 충분하지만 나중에는 필요한 규칙을 유지 관리하기 위해 상당한 관리 노력이 필요합니다.
- 사용자 인터페이스. Unified Access Gateway는 직관적인 Horizon Client 사용자 인터페이스를 변경하지 않습니다. Unified Access Gateway를 사용하면 Horizon Client를 실행할 때 인증된 사용자가 View 환경에서 작업하게 되며 데스크톱 및 애플리케이션에 대한 액세스를 제어할 수 있습니다. VPN에서는 사용자가 먼저 VPN 소프트웨어를 설치한 다음, 별도로 인증을 받고 Horizon Client를 시작해야 합니다.
- 성능: Unified Access Gateway는 보안 및 성능을 최대화하도록 디자인되었습니다. Unified Access Gateway를 사용하면 추가 캡슐화 없이도 PCoIP, HTML Access 및 WebSocket 프로토콜 보안이 유지됩니다. VPN은 SSL VPN으로 구현됩니다. 이러한 구현은 보안 요구 사항을 충족하며, TLS(Transport Layer Security)가 설정되면 안전한 것으로 간주됩니다. 하지만 SSL/TLS를 사용한 기본 프로토콜은 TCP만을 기반으로 합니다. 연결 없는 UDP 기반 전송을 할

용하는 최신 비디오 원격 프로토콜을 사용할 경우 TCP 기반 전송이 적용되면 성능상의 이점이 크게 줄어들 수 있습니다. SSL/TLS 대신 DTLS 또는 IPsec으로도 작동할 수 있는 VPN 기술은 Horizon 7 데스크톱 프로토콜에서도 잘 작동할 수 있기 때문에 이러한 특성이 모든 VPN 기술에 해당되는 것은 아닙니다.

Unified Access Gateway를 사용한 Horizon 보안 강화

Unified Access Gateway 장치는 사용자 인증 위에 디바이스 인증 계층을 배치하여 알려진 정상 디바이스에서만 액세스할 수 있도록 하며 Virtual Desktop Infrastructure에 또 다른 보안 계층을 추가함으로써 보안을 향상합니다.

참고 이 기능은 Windows용 Horizon Client에서만 지원됩니다.

- “VMware Unified Access Gateway 배포 및 구성” 문서(<https://docs.vmware.com/kr/Unified-Access-Gateway/index.html>)에서 “Unified Access Gateway 장치에서 인증서 또는 스마트 카드 인증 구성”을 참조하십시오.
- 끝점 규정 준수 검사 기능은 Unified Access Gateway에서 사용할 수 있는 기타 사용자 인증 서비스 외에, Horizon 데스크톱에 액세스하기 위한 추가 보안 계층을 제공합니다. “VMware Unified Access Gateway 배포 및 구성” 문서(<https://docs.vmware.com/kr/Unified-Access-Gateway/index.html>)에서 “Horizon에 대한 끝점 규정 준수 검사”를 참조하십시오.

중요 Unified Access Gateway 장치가 2 요소 인증(RSA SecureID 및 RADIUS)용으로 구성되어 있고, Windows 사용자 이름 일치가 사용 설정되어 있으며, 여러 사용자 도메인이 있는 경우, 사용자가 Windows 사용자 이름 및 암호를 인증에 사용하는 동안 올바른 도메인을 선택할 수 있도록 연결 서버에서 도메인 목록을 전송하도록 설정해야 합니다.

이중 홉 DMZ

인터넷과 내부 네트워크 간에 이중 홉 DMZ가 필요한 경우 내부 DMZ에서 Unified Access Gateway를 갖춘 Web Reverse Proxy로 외부 DMZ에서 Unified Access Gateway 장치를 배포하여 이중 홉 DMZ 구성을 생성할 수 있습니다. 각 DMZ 계층에서 특정 역방향 프록시를 통해 트래픽이 통과하면 DMZ 계층을 건너뛸 수 없습니다. 구성 세부 정보는 “VMware Unified Access Gateway 배포 및 구성” 문서를 참조하십시오.

Horizon 연결 서버의 방화벽 규칙

연결 서버 인스턴스와 보안 서버의 방화벽에서 특정 포트를 열어야 합니다.

연결 서버를 설치할 때 설치 프로그램에서 사용자에게 필요한 Windows 방화벽 규칙을 선택적으로 구성할 수 있습니다. 이러한 규칙은 기본적으로 사용되는 포트를 엽니다. 설치 후에 기본 포트를 변경할 경우 Horizon Client 디바이스가 업데이트된 포트를 통해 Horizon 7에 연결할 수 있도록 수동으로 Windows 방화벽을 구성해야 합니다.

다음 표에는 설치 중 자동으로 열 수 있는 기본 포트가 나와 있습니다. 이러한 포트는 다른 설명이 없는 한 수신용입니다.

표 7-4. Horizon 연결 서버 설치 중 열리는 포트

프로토콜	포트	Horizon 연결 서버 인스턴스 유형
JMS	TCP 4001	표준 및 복제
JMS	TCP 4002	표준 및 복제
JMSIR	TCP 4100	표준 및 복제
JMSIR	TCP 4101	표준 및 복제
AJP13	TCP 8009	표준 및 복제
HTTP	TCP 80	표준, 복제, 보안 서버
HTTPS	TCP 443	표준, 복제, 보안 서버
PCoIP	TCP 4172 수신, UDP 4172 양방향	표준, 복제, 보안 서버
HTTPS	TCP 8443 UDP 8443	표준, 복제 및 보안 서버 Horizon 7에 처음 연결된 후 웹 브라우저 또는 클라이언트 디바이스에서 TCP 포트 8443의 Blast 보안 게이트웨이에 연결합니다. 이러한 두 번째 연결이 이루어지려면 보안 서버 또는 View 연결 서버 인스턴스에서 Blast 보안 게이트웨이를 사용하도록 설정해야 합니다.
HTTPS	TCP 8472	표준 및 복제 Cloud Pod 아키텍처 기능: 포트 간 통신에 사용됩니다.
HTTP	TCP 22389	표준 및 복제 Cloud Pod 아키텍처 기능: 전역 LDAP 복제에 사용됩니다.
HTTPS	TCP 22636	표준 및 복제 Cloud Pod 아키텍처 기능: 보안 전역 LDAP 복제에 사용됩니다.

IPsec을 지원하도록 백엔드 방화벽 구성

해당 네트워크 토폴로지에서 보안 서버와 연결 서버 인스턴스 사이에 백엔드 방화벽이 포함된 경우, IPsec을 지원하도록 방화벽에서 특정 프로토콜 및 포트를 구성해야 합니다. 적합하게 구성하지 않으면 보안 서버와 연결 서버 인스턴스 사이에서 전송되는 데이터가 방화벽을 통과하지 못합니다.

기본적으로, IPsec 규칙은 보안 서버와 연결 서버 인스턴스 사이의 연결을 관리합니다. IPsec을 지원하기 위해 연결 서버 설치 관리자가 Horizon 7 서버가 설치된 Windows Server 호스트에서 Windows 방화벽 규칙을 구성할 수 있습니다. 백엔드 방화벽의 경우, 사용자가 규칙을 직접 구성해야 합니다.

참고 IPsec의 사용이 강력히 권장됩니다. 또 다른 방법으로, Horizon Administrator 전역 설정인 **보안 서버 연결용 IPsec 사용**을 해제할 수 있습니다.

다음 규칙이 양방향 트래픽을 허용해야 합니다. 방화벽에서 인바운드 및 아웃바운드 트래픽에 개별 규칙을 지정해야 할 수도 있습니다.

네트워크 주소 변환(NAT)을 사용하는 방화벽과 NAT를 사용하지 않는 방화벽에 서로 다른 규칙이 적용됩니다.

표 7-5. NAT 이외 방화벽의 IPsec 규칙 지원 요구 사항

소스	프로토콜	포트	대상	참고
보안 서버	ISAKMP	UDP 500	Horizon 연결 서버	보안 서버는 UDP 포트 500을 사용하여 IPsec 보안을 협상합니다.
보안 서버	ESP	N/A	Horizon 연결 서버	ESP 프로토콜은 IPsec 암호화된 트래픽을 캡슐화합니다. 규칙의 일부로 ESP에 대한 포트를 지정할 필요는 없습니다. 필요한 경우, 소스 및 대상 IP 주소를 지정하여 규칙의 범위를 줄일 수 있습니다.

다음 규칙은 NAT를 사용하는 방화벽에 적용됩니다.

표 7-6. NAT 방화벽의 IPsec 규칙 지원 요구 사항

소스	프로토콜	포트	대상	참고
보안 서버	ISAKMP	UDP 500	Horizon 연결 서버	보안 서버는 UDP 포트 500을 사용하여 IPsec 보안 협상을 실행합니다.
보안 서버	NAT-T ISAKMP	UDP 4500	Horizon 연결 서버	보안 서버는 UDP 포트 500을 사용하여 NAT를 탐색하고 IPsec 보안을 조정합니다.

백업 구성을 사용하여 Horizon 연결 서버 재설치

특정한 상황에서 현재 버전의 연결 서버 인스턴스를 다시 설치하고 View LDAP 구성 데이터를 포함하는 백업 LDIF 파일을 가져와 기존 Horizon 7 구성을 복원해야 할 수 있습니다.

예를 들어, 비즈니스 연속성 및 재해 복구(BC/DR) 계획의 일환으로 데이터 센터의 기능이 중지될 경우 즉시 구현할 수 있는 절차를 마련하고자 할 수 있습니다. 그러한 계획의 첫 번째 단계는 View LDAP 구성이 다른 위치에 백업되어 있는지 확인하는 것입니다. 두 번째 단계는 새 위치에 연결 서버를 설치하고 이 절차에 설명된 대로 백업 구성을 가져오는 것입니다.

기존 Horizon 7 구성을 사용해 두 번째 데이터 센터를 설정할 경우에도 이 절차를 사용할 수 있습니다. 또는 Horizon 7 배포에 단일 연결 서버 인스턴스만 포함되어 있고 해당 서버에 문제가 발생한 경우에 이 절차를 사용할 수 있습니다.

복제된 그룹에 여러 개의 연결 서버 인스턴스가 있고 단일 인스턴스가 중단된 경우에는 이 절차를 따를 필요가 없습니다. 연결 서버를 복제된 인스턴스로 다시 설치하면 됩니다. 설치 도중 다른 연결 서버 인스턴스에 대한 연결 정보를 입력하면 Horizon 7이 다른 인스턴스에서 View LDAP 구성을 복원합니다.

사전 요구 사항

- View LDAP 구성이 암호화된 LDIF 파일에 백업되었는지 확인하십시오.
- `vdmimport` 명령을 사용하여 LDIF 백업 파일에서 View LDAP 구성을 복원하는 방법을 숙지하십시오.

“Horizon 7 관리” 문서의 “Horizon 7 구성 데이터 백업 및 복원”을 참조하십시오.

- 새로운 연결 서버 인스턴스 설치 단계를 숙지하십시오. [새 구성을 사용하여 Horizon 연결 서버 설치](#)를 참조하십시오.

절차

- 1 새 구성을 사용하여 연결 서버를 설치합니다.
- 2 암호화된 LDIF 파일의 암호를 해독합니다.

예:

```
vdmimport -d -p mypassword
-f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

- 3 암호화된 LDIF 파일을 가져와 View LDAP 구성을 복원합니다.

예:

```
vdmimport -f MyDecryptedexport.LDF
```

참고 이 단계에서는 아직 Horizon 7 구성에 액세스할 수 없습니다. 클라이언트가 연결 서버에 액세스하거나 해당 데스크톱에 연결할 수 없습니다.

- 4 Windows **프로그램 추가/제거** 유틸리티를 사용하여 컴퓨터에서 연결 서버를 제거합니다.
AD LDS Instance VMwareVDMDS 인스턴스라는 View LDAP 구성은 제거하지 마십시오. **프로그램 추가/제거** 유틸리티를 사용하여 Windows Server 컴퓨터에서 AD LDS Instance VMwareVDMDS 인스턴스가 제거되지 않았는지 확인할 수 있습니다.

- 5 연결 서버를 재설치합니다.

설치 관리자 프롬프트에서 기존 View LDAP 디렉토리를 수락합니다.

다음에 수행할 작업

새로운 구성을 사용하여 연결 서버 인스턴스를 설치한 후 원하는 대로 연결 서버와 Horizon 7 환경을 구성합니다.

Microsoft Windows Installer 명령줄 옵션

Horizon 7 구성 요소를 자동으로 설치하려면 Microsoft Windows Installer(MSI) 명령줄 옵션 및 속성을 사용해야 합니다. Horizon 7 구성 요소 설치 관리자는 MSI 프로그램이며 표준 MSI 기능을 사용합니다.

MSI에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오. MSI 명령줄 옵션은 Microsoft Developer Network(MSDN) Library 웹 사이트를 참조하여 MSI 명령줄 옵션을 검색합니다. MSI 명령줄 사용을 보려면 Horizon 7 구성 요소 컴퓨터에서 명령 프롬프트를 열어 `msiexec /?`를 입력하면 됩니다.

Horizon 7 구성 요소 설치 관리자를 자동으로 실행하려면 임시 디렉토리로 설치 관리자를 추출하고 대화식 설치를 시작하는 부트스트랩 프로그램을 잠시 중단하여 시작합니다.

명령줄에 설치 관리자의 부트스트랩 프로그램을 제어하는 명령줄 옵션을 입력해야 합니다.

표 7-7. Horizon 7 구성 요소의 부트스트랩 프로그램의 명령줄 옵션

옵션	설명
/s	대화식 대화 상자를 디스플레이할 수 없는 부트스트랩 스플래시 화면 및 추출 대화 상자를 해제합니다. 예: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s 자동 설치를 실행하기 위해 /s 옵션이 필요합니다.
/v "MSI_command_line_options"	설치 관리자가 해석할 MSI의 옵션 집합으로 명령줄에 입력할 큰 따옴표로 닫힌 문자열을 전달하도록 지시합니다. 큰 따옴표 사이에 명령줄 항목을 넣어야 합니다. /v 뒤에 그리고 명령줄 끝에 큰 따옴표를 지정합니다. 예: VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v "command_line_options" MSI 설치 관리자가 공백을 포함하는 문자열을 해석하도록 지시하려면 두 세트의 큰 따옴표에 문자열을 지정합니다. 예를 들어 공백을 포함한 설치 경로 이름에 Horizon 7 구성 요소를 설치할 수 있습니다. 예: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v "command_line_options INSTALLDIR=""d:\Wabc\My folder"" 이 예에서 MSI 설치 관리자는 설치 디렉토리 경로에서 전달하며 문자열을 두 개의 명령줄 옵션으로 해석하지 않습니다. 전체 명령줄을 둘러싼 마지막 큰 따옴표에 유의하십시오. 자동 설치를 실행하기 위해 /v "command_line_options" 옵션이 필요합니다.

MSI 설치 관리자 msixexec.exe에 명령줄 옵션 및 MSI 속성 값을 전달하여 나머지 자동 설치를 제어합니다. MSI 설치 관리자에는 Horizon 7 구성 요소의 설치 코드가 포함됩니다. 설치 관리자는 명령줄에 입력하는 값과 옵션을 사용하여 Horizon 7 구성 요소에 특정한 설치 선택 사항 및 설치 옵션을 해석합니다.

표 7-8. MSI 명령줄 옵션 및 MSI 속성

MSI 옵션 또는 속성	설명
/qn	MSI 설치 관리자가 설치 관리자 마법사 페이지를 표시하지 않도록 지시합니다. 예를 들어 Horizon Agent를 자동 설치하고 기본 설정 옵션 및 기능만 사용할 수 있습니다. VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v "/qn" 또는 /qb 옵션을 사용하여 자동화된 비대화식 설치에서 기본 진행률 대화상자를 표시할 수 있습니다. 자동 설치를 실행하기 위해 /qn 또는 /qb 옵션이 필요합니다. 추가 /q 매개 변수에 대한 자세한 내용은 Microsoft 개발자 센터 웹 사이트를 참조하십시오.
INSTALLDIR	Horizon 7 구성 요소의 다른 설치 경로를 지정합니다. INSTALLDIR=path 형식을 사용하여 설치 경로를 지정합니다. 기본 경로에 Horizon 7 구성 요소를 설치할 경우 이 MSI 속성을 무시할 수 있습니다. 이 MSI 속성은 선택 사항입니다.

표 7-8. MSI 명령줄 옵션 및 MSI 속성 (계속)

MSI 옵션 또는 속성	설명
ADDLOCAL	<p>설치할 구성 요소 특정 옵션을 결정합니다.</p> <p>대화식 설치에서 Horizon 7 설치 관리자는 선택하거나 선택 취소할 수 있는 사용자 지정 설치 옵션을 표시합니다. 자동 설치에서는 ADDLOCAL 속성을 사용하여 명령줄에서 옵션을 지정하여 선별적으로 개별 설치 옵션을 설치할 수 있습니다. 명시적으로 지정하지 않는 옵션은 설치되지 않습니다.</p> <p>대화식 설치와 자동 설치 모두에서 Horizon 7 설치 관리자는 특정 기능을 자동으로 설치합니다. ADDLOCAL을 사용하여 선택 사항이 아닌 이러한 기능을 설치할지 여부를 제어할 수 없습니다.</p> <p>대화형 설치를 수행하는 동안 기본적으로 설치되는 옵션과 선택하여 설치하는 옵션을 포함하여 설치가 가능한 사용자 지정 설치 옵션을 NGVC만 제외하고 모두 설치하려면 ADDLOCAL=ALL을 입력합니다. NGVC와 SVIAgent는 상호 배타적입니다.</p> <p>다음 예에서는 Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG 및 게스트 운영 체제에서 지원되는 모든 기능을 설치합니다. VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</p> <p>ADDLOCAL 속성을 사용하지 않는 경우 기본적으로 설치되는 사용자 지정 설치 옵션과 자동으로 설치되는 기능이 설치됩니다. 기본적으로 해제(선택 취소)되어 있는 사용자 지정 설치 옵션은 설치되지 않습니다.</p> <p>다음 예에서는 Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG 및 게스트 운영 체제에서 지원되는 기본 사용자 지정 설치 옵션을 설치합니다. VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn"</p> <p>개별 설치 옵션을 지정하려면 쉼표로 구분된 설치 옵션 이름 목록을 입력합니다. 이름 사이에 공백을 사용하지 마십시오. ADDLOCAL=value,value,value... 형식을 사용하십시오.</p> <p>ADDLOCAL=value,value,value... 속성을 사용할 때는 Core를 포함해야 합니다.</p> <p>다음 예에서는 Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, 인스턴트 클론 에이전트 및 가상 인쇄 기능이 있는 Horizon Agent를 설치합니다.</p> <p>VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC,ThinPrint"</p> <p>이전 예에서는 기본적으로 대화형으로 설치되는 구성 요소라도 다른 구성 요소는 설치하지 않습니다. ADDLOCAL MSI 속성은 선택 사항입니다.</p>
REBOOT	<p>시스템을 재부팅하기 전에 시스템 구성 작업이 완료되게 하는 REBOOT=ReallySuppress 옵션을 사용할 수 있습니다.</p> <p>이 MSI 속성은 선택 사항입니다.</p>
/!v log_file	<p>자세한 출력으로 지정된 로그 파일에 로깅 정보를 작성합니다.</p> <p>예: /!v "%TEMP%\Wvmmsi.log"</p> <p>이 예는 대화식 설치 중 생성된 로그와 유사한 자세한 로그 파일을 생성합니다.</p> <p>이 옵션을 사용하여 설치에 고유하게 적용할 수 있는 사용자 지정 기능을 기록할 수 있습니다. 기록된 정보를 사용하여 나중에 자동 설치 시 설치 기능을 지정할 수 있습니다.</p> <p>/!v 옵션은 선택 사항입니다.</p>

MSI 명령줄 옵션을 사용하여 Horizon 7 구성 요소 자동 제거

Microsoft Windows Installer(MSI) 명령줄 옵션을 사용하여 Horizon 7 구성 요소를 제거할 수 있습니다.

구문

```
msiexec.exe
```



```
/qb
/x
product_code
```

옵션

/qb 옵션은 제거 진행 표시줄을 표시합니다. 제거 진행 표시줄을 표시하지 않으려면 /qb 옵션을 /qn 옵션으로 교체하십시오.

/x 옵션은 Horizon 7 구성 요소를 제거합니다.

product_code 문자열은 MSI 제거 프로그램에 대해 Horizon 7 구성 요소 제품 파일을 식별합니다. 설치 중 생성된 %TEMP%\Wmmsi.log 파일에서 ProductCode를 검색하여 *product_code* 문자열을 찾을 수 있습니다. 이전 버전의 Horizon 7 구성 요소에 적용되는 *product_code* 문자열을 찾으려면 <http://kb.vmware.com/kb/2064845>의 VMware KB(기술 자료) 문서를 참조하십시오.

MSI 명령줄 옵션에 대한 자세한 내용은 [Microsoft Windows Installer 명령줄 옵션](#)에 나와 있습니다.

Horizon Agent 제거 예

32비트 Horizon Agent 버전 7.0.2를 제거하려면 다음 명령을 입력합니다.

```
msiexec.exe /qb /x {B23352D8-AD44-4379-A56E-0E337F9C4036}
```

64비트 Horizon Agent 버전 7.0.2를 제거하려면 다음 명령을 입력합니다.

```
msiexec.exe /qb /x {53D6EE37-6B10-4963-81B1-8E2972A1DA4D}
```

명령에 자세한 로그를 추가합니다.

```
/!v "%TEMP%\Wmmsi_uninstall.log"
```

/! 옵션을 명시적으로 전달하지 않을 경우의 기본 로그 파일은 %TEMP%\WMSI****.log이며, 여기서 ****은 4자리 GUID입니다.

Horizon Agent 제거 프로세스는 일부 레지스트리 키를 유지합니다. 이러한 키는 연결 서버 구성 정보를 유지하여 에이전트가 제거된 후 다시 설치되더라도 원격 데스크톱이 연결 서버와 계속 연결되도록 하는 데 필요합니다. 이러한 레지스트리 키를 제거하면 해당 연결이 끊어집니다.

다음 레지스트리 키가 유지됩니다.

- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CRLs
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CTLs
- HKLM\SOFTWARE\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Policies\VMware, Inc.\vRealize Operations for Horizon*

- HKLM\SOFTWARE\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMwareView*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\WvRealize Operations for Horizon*
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM

Horizon 7 서버를 위한 TLS 인증서 구성



VMware에서는 연결 서버 인스턴스, 보안 서버 및 View Composer 서비스 인스턴스의 인증을 위해 TLS 인증서를 구성하는 것을 권장합니다.

기본 TLS 서버 인증서는 연결 서버 인스턴스, 보안 서버 또는 View Composer 인스턴스를 설치할 때 생성됩니다. 테스트 용도로 기본 인증서를 사용할 수 있습니다.

연결 서버 간 및 Horizon Agent와 연결 서버 인스턴스 간 통신에 사용되는 인증서는 자동 메커니즘을 사용하여 대체되며 수동으로 대체할 수 없습니다. 자세한 내용은 “Horizon 7 보안” 문서를 참조하십시오.

중요 가능한 한 빨리 기본 인증서를 교체합니다. 기본 인증서는 인증 기관(CA)에 의해 서명되지 않습니다. CA에서 서명하지 않은 인증서를 사용하여 신뢰할 수 없는 사용자가 서버로 가장하여 트래픽을 인터셉트할 수 있습니다

본 장은 다음 항목을 포함합니다.

- [Horizon 7 서버를 위한 TLS 인증서 이해](#)
- [TLS 인증서 설정 작업 개요](#)
- [CA에서 서명된 TLS 인증서 가져오기](#)
- [새로운 TLS 인증서를 사용하도록 Horizon 연결 서버, 보안 서버 또는 View Composer 구성](#)
- [루트 및 중간 인증서를 신뢰하도록 클라이언트 끝점 구성](#)
- [서버 인증서에 대한 인증서 해지 검사 구성](#)
- [새 TLS 인증서를 사용하도록 PCoIP 보안 게이트웨이 구성](#)
- [vCenter Server 또는 View Composer 인증서를 신뢰하도록 Horizon Administrator 설정](#)
- [CA에서 서명한 TLS 인증서 사용 시 장점](#)
- [Horizon 연결 서버 및 보안 서버의 인증서 문제 해결](#)

Horizon 7 서버를 위한 TLS 인증서 이해

Horizon 7 서버 및 관련 구성 요소에 대해 TLS 인증서를 구성할 경우 특정 지침을 따라야 합니다.

Horizon 연결 서버 및 보안 서버

클라이언트에서 서버에 연결하기 위해서는 TLS가 필요합니다. 클라이언트 연결의 연결 서버 인스턴스, 보안 서버 및 중간 서버에서 TLS 연결을 종료하려면 TLS 서버 인증서가 필요합니다.

기본적으로 연결 서버 또는 보안 서버를 설치하면 서버를 위한 자체 서명 인증서가 생성됩니다. 그러나 이 설치하는 다음과 같은 경우 기존 인증서를 사용합니다.

- 대화명이 vdm인 유효한 인증서가 Windows 인증서 저장소에 이미 있는 경우
- 이전 릴리스에서 Horizon 7으로 업그레이드하며 유효한 키 저장소 파일이 Windows Server 컴퓨터에 구성된 경우 설치 중에 키 및 인증서가 추출된 후 Windows 인증서 저장소로 가져옵니다.

vCenter Server 및 View Composer

운영 환경에서 vCenter Server와 View Composer를 Horizon 7에 추가하기 전에 vCenter Server와 View Composer가 CA에서 서명한 인증서를 사용하는지 확인하십시오.

vCenter Server의 기본 인증서를 교체하는 방법에 대한 자세한 내용은 VMware Technical Papers 사이트(<http://www.vmware.com/resources/techresources/>)에 있는 "vCenter Server 인증서 교체"를 참조하십시오.

동일한 Windows Server 호스트에 vCenter Server 및 View Composer를 설치하는 경우, 동일한 TLS 인증서를 사용할 수 있지만 각 구성 요소의 인증서를 별도로 구성해야 합니다.

PCoIP 보안 게이트웨이

산업 또는 국가 보안 규정을 준수하려면 PCoIP 보안 게이트웨이(PSG) 서비스에서 생성한 기본 TLS 인증서를 CA에서 서명한 인증서로 바꾸십시오. 특히 준수 테스트를 통과하기 위해 보안 스캐너를 사용해야 하는 배포의 경우 CA 서명 인증서를 사용하도록 PSG 서비스를 구성하는 것이 좋습니다. [새 TLS 인증서를 사용하도록 PCoIP 보안 게이트웨이 구성](#)를 참조하십시오.

Blast 보안 게이트웨이

기본적으로 Blast 보안 게이트웨이(BSG)는 연결 서버 인스턴스 또는 BSG가 실행 중인 보안 서버에 대해 구성된 TLS 인증서를 사용합니다. 서버를 위한 기본 자체 서명 인증서를 CA 서명 인증서로 교체하면 BSG도 CA 서명 인증서를 사용합니다.

SAML 2.0 인증자

VMware Identity Manager는 SAML 2.0 인증자를 사용하여 보안 도메인 전체에 웹 기반 인증 및 권한 부여를 제공합니다. Horizon 7가 VMware Identity Manager에 인증을 위임하도록 하려면 VMware Identity Manager에서 SAML 2.0 인증 세션을 수락하도록 Horizon 7를 구성합니다.

Horizon 7를 지원하도록 VMware Identity Manager가 구성된 경우 VMware Identity Manager 사용자는 Horizon 사용자 포털에서 데스크톱 아이콘을 선택하여 원격 데스크톱에 연결할 수 있습니다.

Horizon Administrator에서 연결 서버 인스턴스에서 사용할 수 있도록 SAML 2.0 인증자를 구성할 수 있습니다.

Horizon Administrator에서 SAML 2.0 인증자를 추가하기 전에 SAML 2.0 인증자가 CA에서 서명한 인증서를 사용하는지 확인하십시오.

추가 지침

CA에서 서명한 TLS 인증서 요청 및 사용에 대한 일반 정보는 [CA에서 서명한 TLS 인증서 사용 시 장](#)점을 참조하십시오.

클라이언트 끝점이 연결 서버 인스턴스 또는 보안 서버에 연결할 때 서버의 TLS 서버 인증서와 신뢰 체인의 모든 중간 인증서가 제공됩니다. 서버 인증서를 신뢰하려면 클라이언트 시스템에 서명 CA의 루트 인증서가 설치되어 있어야 합니다.

연결 서버가 vCenter Server 및 View Composer와 통신할 경우 연결 서버에 이러한 서버의 TLS 서버 인증서와 중간 인증서가 제공됩니다. vCenter Server와 View Composer Server를 신뢰하려면 연결 서버 컴퓨터에 서명 CA의 루트 인증서가 설치되어 있어야 합니다.

마찬가지로 연결 서버에 SAML 2.0 인증자가 구성되어 있는 경우 연결 서버 컴퓨터에 SAML 2.0 서버 인증서의 서명 CA의 루트 인증서가 설치되어 있어야 합니다.

TLS 인증서 설정 작업 개요

Horizon 7 서버의 TLS 서버 인증서를 설정하려면 여러 가지의 개괄적인 작업을 수행해야 합니다.

복제된 연결 서버 인스턴스의 포드에서 포드의 모든 인스턴스에 대해 다음 작업을 수행해야 합니다.

이러한 작업을 수행하는 절차는 이 개요 다음에 이어지는 항목에 설명되어 있습니다.

- 1 CA에서 새로운 서명 TLS 인증서를 가져와야 하는지 확인합니다.

조직에 이미 유효한 TLS 서버 인증서가 있는 경우 해당 인증서를 사용하여 연결 서버, 보안 서버 또는 View Composer에서 제공하는 기본 TLS 서버 인증서를 교체할 수 있습니다. 기존 인증서를 사용하려면 동봉된 개인 키도 필요합니다.

시작 위치	조치
조직에서 유효한 TLS 서버 인증서를 제공했습니다.	자세한 내용은 직접 2단계로 이동하십시오.
TLS 서버 인증서가 없습니다.	CA를 통해 서명된 TLS 서버 인증서를 구하십시오.

- 2 TLS 인증서를 Horizon 7 서버 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 가져옵니다.

- 3 연결 서버 인스턴스와 보안 서버의 경우 인증서 대화명을 **vdm**으로 설정합니다.

대화명 **vdm**을 각 Horizon 7 서버 호스트의 인증서 하나에만 할당합니다.

- 4 연결 서버 컴퓨터에서 Windows Server 호스트가 루트 인증서를 신뢰하지 않는 경우 루트 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져오십시오.

또한 연결 서버 인스턴스가 보안 서버, View Composer 및 vCenter Server 호스트에 대해 구성된 TLS 서버 인증서의 루트 인증서를 신뢰하지 않을 경우에도 이러한 루트 인증서를 가져와야 합니다. 연결 서버 인스턴스에 대해서만 이러한 단계를 수행하십시오. 루트 인증서를 View Composer, vCenter Server 또는 보안 서버 호스트로 가져올 필요가 없습니다.

- 5 서버 인증서를 중간 CA에서 서명한 경우 중간 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져오십시오.

클라이언트 구성을 간소화하기 위해 전체 인증서 체인을 Windows 로컬 컴퓨터 인증서 저장소로 가져옵니다. 중간 인증서가 Horizon 7 서버에서 누락된 경우 Horizon Administrator를 실행하는 클라이언트 및 컴퓨터에 대해 중간 인증서를 구성해야 합니다.

6 View Composer 인스턴스에 대해 다음 단계 중 하나를 수행하십시오.

- View Composer를 설치하기 전에 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져오면 View Composer 설치 도중 인증서를 선택할 수 있습니다.
- View Composer를 설치한 후 기존 인증서 또는 기본 자체 서명 인증서를 새 인증서로 교체하려면 SviConfig ReplaceCertificate 유틸리티를 실행하여 새 인증서를 View Composer에서 사용하는 포트에 바인딩해야 합니다.

7 CA가 잘 알려져 있지 않다면 루트 및 중간 인증서를 신뢰하도록 클라이언트를 구성하십시오.

또한 Horizon Administrator를 실행할 컴퓨터가 루트 및 중간 인증서를 신뢰하는지 확인하십시오.

8 인증서 해지 검사를 재구성할지 결정하십시오.

연결 서버가 Horizon 7 서버, View Composer 및 vCenter Server에 대한 인증서 해지 검사를 수행합니다. CA에서 서명한 대부분의 인증서에는 인증서 해지 정보가 포함되어 있습니다. CA에 이 정보가 포함되어 있지 않은 경우 인증서에 대해 해지 검사를 수행하지 않도록 서버를 구성할 수 있습니다.

SAML 인증자가 연결 서버 인스턴스에서 사용되도록 구성된 경우 연결 서버가 SAML 서버 인증서에 대한 인증서 해지 검사도 수행합니다.

CA에서 서명된 TLS 인증서 가져오기

조직에서 TLS 서버 인증서를 제공하지 않는 경우 CA에서 서명한 새 인증서를 요청해야 합니다.

여러 가지 방법을 사용하여 서명된 새 인증서를 가져올 수 있습니다. 예를 들어, Microsoft certreq 유틸리티를 사용해 인증서 서명 요청(CSR)을 생성하고 CA에 인증서 요청을 제출할 수 있습니다.

certreq를 사용하여 이 작업을 수행하는 방법을 보여 주는 예제는 "Horizon 7용 TLS 인증서 설정 시나리오" 문서를 참조하십시오.

신뢰할 수 없는 루트를 기반으로 한 무료 임시 인증서를 많은 CA에서 테스트 용도로 구할 수 있습니다.

중요 CA에서 서명된 TLS 인증서를 가져올 때 특정 규칙 및 지침을 따라야 합니다.

- 컴퓨터에서 인증서 요청을 생성할 경우 개인 키도 생성되었는지 확인하십시오. TLS 서버 인증서를 구해서 Windows 로컬 컴퓨터 인증서 저장소로 가져오면 인증서와 일치하는 동봉된 개인 키가 있어야 합니다.
- 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.
- Windows Server 2008 Enterprise CA 이상과만 호환되는 인증서 템플릿을 사용하여 서버의 인증서를 생성하지 마십시오.
- 1024 미만의 KeyLength 값을 사용하여 서버의 인증서를 생성하지 마십시오. 클라이언트 끝점은 서버에서 1024 미만의 KeyLength로 생성된 인증서의 유효성을 검사하지 않으므로 클라이언트가 서버에 연결되지 않습니다. 연결 서버에서 수행하는 인증서 유효성 검사도 실패하므로 영향을 받는 서버가 Horizon Administrator 대시보드에 빨간색으로 나타납니다.

인증서 가져오기에 대한 일반 정보는 Microsoft 온라인 도움말의 MMC에 인증서 스냅인 추가를 참조하십시오. 인증서 스냅인이 아직 컴퓨터에 설치되지 않은 경우 [MMC에 인증서 스냅인 추가](#)를 참조하십시오.

Windows 도메인 또는 Enterprise CA를 통해 서명된 인증서 가져오기

Windows 도메인 또는 Enterprise CA에서 서명된 인증서를 가져오려면 Windows 인증서 저장소에 서 Windows 인증서 등록 마법사를 사용합니다.

컴퓨터 간 통신이 내부 도메인 내에서 유지되는 경우 이 인증서 요청 방법이 적절합니다. 예를 들어 Windows 도메인 CA에서 서명된 인증서를 가져오는 방법은 서버 간 통신에 적절할 수 있습니다.

클라이언트가 외부 네트워크에서 Horizon 7 서버에 연결하는 경우 신뢰할 수 있는 타사 CA에서 서명된 TLS 서버 인증서를 요청합니다.

사전 요구 사항

- 클라이언트 디바이스가 호스트에 연결하는 데 사용하는 FQDN(정규화된 도메인 이름)을 결정합니다.
VMware 보안 권장 사항을 준수하기 위해 내부 도메인에서의 통신에도 단순한 서버 이름이나 IP 주소가 아닌 FQDN을 사용합니다.
- 인증서 스냅인이 MMC에 추가되었는지 확인하십시오. [MMC에 인증서 스냅인 추가](#)의 내용을 참조하십시오.
- 컴퓨터 또는 서비스에 발급될 수 있는 인증서를 요청하기에 적절한 자격 증명이 있는지 확인하십시오.

절차

- 1 Windows Server 호스트의 **MMC** 창에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **개인** 폴더를 선택합니다.
- 2 **작업** 메뉴에서 **모든 작업 > 새 인증서 요청**으로 이동하여 **인증서 등록** 마법사를 표시합니다.
- 3 인증서 등록 정책을 선택합니다.
- 4 요청할 인증서 유형을 선택하고 **개인 키를 내보낼 수 있게 설정** 옵션을 선택한 다음 **등록**을 클릭합니다.
- 5 **마침**을 클릭합니다.

새로운 서명된 인증서가 Windows 인증서 저장소의 **개인 > 인증서** 폴더에 추가됩니다.

다음에 수행할 작업

- 서버 인증서 및 인증서 체인을 Windows 인증서 저장소로 가져왔는지 확인합니다.
- 연결 서버 인스턴스 또는 보안 서버의 경우 인증서 대화명을 **vdm**으로 수정합니다. [인증서 대화명 수정](#)의 내용을 참조하십시오.
- View Composer Server의 경우 새 인증서를 View Composer에서 사용하는 포트에 바인딩합니다. [View Composer가 사용하는 포트에 새 TLS 인증서 바인딩](#)을 참조하십시오.

새로운 TLS 인증서를 사용하도록 Horizon 연결 서버, 보안 서버 또는 View Composer 구성

TLS 인증서를 사용하도록 연결 서버 인스턴스, 보안 서버 또는 View Composer 인스턴스를 구성하려면 서버 인증서와 전체 인증서 체인을 연결 서버, 보안 서버 또는 View Composer 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다.

복제된 연결 서버 인스턴스의 포트에서 포트의 모든 인스턴스에 서버 인증서 및 인증서 체인을 가져와야 합니다.

기본적으로 Blast 보안 게이트웨이(BSG)는 연결 서버 인스턴스 또는 BSG가 실행 중인 보안 서버에 대해 구성된 TLS 인증서를 사용합니다. View server를 위한 기본 자체 서명 인증서를 CA 서명 인증서로 교체하면 BSG도 CA 서명 인증서를 사용합니다.

중요 인증서를 사용하도록 연결 서버 인스턴스 또는 보안 서버를 구성하려면 인증서 대화명을 **vdm**으로 변경해야 합니다. 또한 인증서에 동봉된 개인 키가 있어야 합니다.

View Composer를 설치한 후 기존 인증서 또는 기본 자체 서명 인증서를 새 인증서로 교체하려면 SviConfig ReplaceCertificate 유틸리티를 실행하여 새 인증서를 View Composer에서 사용하는 포트에 바인딩해야 합니다.

절차

1 MMC에 인증서 스냅인 추가

Windows 인증서 저장소에 인증서를 추가하려면 먼저 Horizon 7 서버가 설치된 Windows Server 호스트에서 Microsoft Management Console(MMC)에 인증서 스냅인을 추가해야 합니다.

2 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.

3 인증서 대화명 수정

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

4 Windows 인증서 저장소에 루트 인증서 및 중간 인증서 가져오기

연결 서버가 설치된 Windows Server 호스트가 서명된 TLS 서버 인증서의 루트 인증서를 신뢰하지 않을 경우 루트 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다. 또한 연결 서버 호스트가 보안 서버, View Composer 및 vCenter Server 호스트에 대해 구성된 TLS 서버 인증서의 루트 인증서를 신뢰하지 않을 경우에도 이러한 루트 인증서를 가져와야 합니다.

5 View Composer가 사용하는 포트에 새 TLS 인증서 바인딩

View Composer를 설치한 후 새 TLS 인증서를 구성하는 경우, SviConfig ReplaceCertificate 유틸리티를 실행하여 View Composer가 사용하는 포트에 바인딩되는 인증서를 대체해야 합니다. 이 유틸리티는 기존 인증서의 바인딩을 해제하고 새 인증서를 포트에 바인딩합니다.

MMC에 인증서 스냅인 추가

Windows 인증서 저장소에 인증서를 추가하려면 먼저 Horizon 7 서버가 설치된 Windows Server 호스트에서 Microsoft Management Console(MMC)에 인증서 스냅인을 추가해야 합니다.

사전 요구 사항

Horizon 7 서버가 설치된 Windows Server 컴퓨터에서 MMC와 인증서 스냅인을 사용할 수 있는지 확인합니다.

절차

- 1 Windows Server 컴퓨터에서 **시작**을 클릭하고 **mmc.exe**를 입력합니다.
- 2 **MMC** 창에서 **파일 > 스냅인 추가/제거**로 이동합니다.
- 3 **스냅인 추가 또는 제거** 창에서 **인증서**를 선택하고 **추가**를 클릭합니다.
- 4 **인증서 스냅인** 창에서 **컴퓨터 계정**을 선택하고 **다음**을 클릭한 다음 **로컬 컴퓨터**를 선택하고 **마침**을 클릭합니다.
- 5 **스냅인 추가 또는 제거** 창에서 **확인**을 클릭합니다.

다음에 수행할 작업

Windows 인증서 저장소로 TLS 서버 인증서를 가져옵니다.

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.

View Composer 서비스가 설치된 Windows Server 호스트에 대해서도 이 작업을 수행해야 합니다.

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.

참고 TLS 연결 부하를 중간 서버로 분산시키려면 동일한 TLS 서버 인증서를 중간 서버와 부하가 분산된 Horizon 7 서버로 가져와야 합니다. 자세한 내용은 "Horizon 7 관리" 문서의 "TLS 연결 부하를 중간 서버로 분산"을 참조하십시오.

사전 요구 사항

인증서 스냅인이 MMC에 추가되었는지 확인하십시오. [MMC에 인증서 스냅인 추가](#)의 내용을 참조하십시오.

절차

- 1 Windows Server 호스트의 MMC 창에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **개인** 폴더를 선택합니다.
- 2 [작업] 창에서 **추가 작업 > 모든 작업 > 가져오기**로 이동합니다.
- 3 **인증서 가져오기** 마법사에서 **다음**을 클릭하고 인증서가 저장된 위치를 찾습니다.
- 4 인증서 파일을 선택하고 **열기**를 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.

View Composer에서 사용하는 TLS 인증서의 대화명을 수정할 필요가 없습니다.

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 인증서 및 중간 인증서 가져오기

연결 서버가 설치된 Windows Server 호스트가 서명된 TLS 서버 인증서의 루트 인증서를 신뢰하지 않을 경우 루트 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다. 또한 연결 서버 호스트가 보안 서버, View Composer 및 vCenter Server 호스트에 대해 구성된 TLS 서버 인증서의 루트 인증서를 신뢰하지 않을 경우에도 이러한 루트 인증서를 가져와야 합니다.

연결 서버, 보안 서버, View Composer 및 vCenter Server 인증서가 알려져 있고 연결 서버 호스트에서 신뢰하는 CA에서 서명되고 인증서 체인에 중간 인증서가 없는 경우 이 작업을 건너뛸 수 있습니다. 일반적으로 사용되는 인증 기관은 호스트에서 신뢰할 가능성이 높습니다.

신뢰할 수 없는 루트 인증서를 포드의 모든 복제된 연결 서버 인스턴스로 가져와야 합니다.

참고 루트 인증서를 View Composer, vCenter Server 또는 보안 서버 호스트로 가져올 필요가 없습니다.

중간 CA가 서버 인증서를 서명된 경우에도 인증서 체인의 각 중간 인증서를 가져와야 합니다. 클라이언트 구성을 간소화하기 위해 전체 중간 체인을 연결 서버 호스트뿐 아니라 보안 서버, View Composer 및 vCenter Server 호스트로도 가져옵니다. 중간 인증서가 연결 서버 또는 보안 서버 호스트에서 누락된 경우 Horizon Administrator를 실행하는 클라이언트 및 컴퓨터에 대해 중간 인증서를 구성해야 합니다. 중간 인증서가 View Composer 또는 vCenter Server 호스트에서 누락된 경우 각 연결 서버 인스턴스에 대해 구성해야 합니다.

전체 인증서 체인을 Windows 로컬 컴퓨터 인증서 저장소로 가져왔는지 이미 확인했다면 이 작업을 건너뛸 수 있습니다.

참고 SAML 인증자가 연결 서버 인스턴스에서 사용되도록 구성된 경우 동일한 지침이 SAML 2.0 인증자에 적용됩니다. 연결 서버 호스트가 SAML 인증자에 대해 구성된 루트 인증서를 신뢰하지 않거나 SAML 서버 인증서를 중간 CA에서 서명한 경우 인증서 체인을 Windows 로컬 컴퓨터 인증서 저장소로 가져왔는지 확인해야 합니다.

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 없는 경우 2단계를 진행하십시오.
- 2 **신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **모든 작업 > 가져오기**를 클릭합니다.
- 3 **인증서 가져오기** 마법사에서 **다음**을 클릭하고 루트 CA 인증서가 저장된 위치를 찾습니다.
- 4 루트 CA 인증서 파일을 선택하고 **열기**를 클릭합니다.
- 5 **다음, 다음, 마침**을 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, 보안 서버 서비스, View Composer 서비스 또는 vCenter Server 서비스를 다시 시작하십시오.

View Composer가 사용하는 포트에 새 TLS 인증서 바인딩

View Composer를 설치한 후 새 TLS 인증서를 구성하는 경우, SviConfig ReplaceCertificate 유틸리티를 실행하여 View Composer가 사용하는 포트에 바인딩되는 인증서를 대체해야 합니다. 이 유틸리티는 기존 인증서의 바인딩을 해제하고 새 인증서를 포트에 바인딩합니다.

View Composer를 설치하기 전에 Windows Server 컴퓨터에 새 인증서를 설치하는 경우, SviConfig ReplaceCertificate 유틸리티를 실행할 필요가 없습니다. View Composer 설치 관리자를 실행하는 경우, 자체 서명된 기본 인증서 대신 CA에서 서명한 인증서를 선택할 수 있습니다. 설치 과정에서 선택된 인증서가 View Composer에서 사용하는 포트에 바인딩됩니다.

기존 인증서 또는 자체 서명된 기본 인증서를 새 인증서로 대체하려는 경우, SviConfig ReplaceCertificate 유틸리티를 사용해야 합니다.

사전 요구 사항

View Composer가 설치된 Windows Server 컴퓨터의 Windows 로컬 컴퓨터 인증서 저장소로 새 인증서를 가져왔는지 확인합니다.

절차

- 1 View Composer 서비스를 중지합니다.
- 2 View Composer가 설치된 Windows Server 호스트에서 명령 프롬프트를 엽니다.
- 3 SviConfig 실행 파일로 이동합니다.

파일은 View Composer 애플리케이션으로 찾을 수 있습니다. 기본 경로는 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe입니다.

- 4 SviConfig ReplaceCertificate 명령을 입력합니다.

예:

```
sviconfig -operation=ReplaceCertificate
         -delete=false
```

여기서 `-delete`는 대체되는 인증서에 적용되는 필수 매개 변수입니다. Windows 로컬 컴퓨터 인증서 저장소에서 이전 인증서를 삭제하려면 `-delete=true`를 지정하거나 Windows 인증서 저장소에 이전 인증서를 유지하려면 `-delete=false`를 지정해야 합니다.

유틸리티가 Windows 로컬 컴퓨터 인증서 저장소에서 사용할 수 있는 TLS 인증서 번호 목록을 표시합니다.

5 인증서를 선택하려면 인증서 번호를 입력하고 Enter를 누릅니다.

6 변경 내용을 적용하려면 View Composer 서비스를 다시 시작하십시오.

예제: SviConfig ReplaceCertificate

다음 예제는 View Composer 포트에 바인딩된 인증서를 대체합니다.

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

루트 및 중간 인증서를 신뢰하도록 클라이언트 끝점 구성

Horizon 7 서버 인증서가 해당 클라이언트 컴퓨터 및 Horizon Administrator에 액세스하는 클라이언트 컴퓨터에서 신뢰하지 않는 CA에 의해 서명된 경우, 루트 및 중간 인증서를 신뢰하도록 도메인의 모든 Windows 클라이언트 시스템을 구성할 수 있습니다. 이렇게 하려면 루트 인증서의 공용 키를 Active Directory의 신뢰할 수 있는 루트 인증 기관 그룹 정책에 추가하고 루트 인증서를 Enterprise NTAUTH 저장소에 추가해야 합니다.

예를 들어, 조직에서 내부 인증서 서비스를 사용할 경우 이러한 단계를 적용해야 할 수도 있습니다.

Windows 도메인 컨트롤러가 루트 CA 역할을 하거나 잘 알려진 CA에서 인증서를 서명할 경우 이러한 단계를 수행할 필요가 없습니다. 잘 알려진 CA의 경우, 운영 체제 공급 업체는 클라이언트 시스템에 루트 인증서를 미리 설치합니다.

잘 알려지지 않은 중간 CA에서 서버 인증서를 서명할 경우, 중간 인증서를 Active Directory의 중간 인증 기관 그룹 정책에 추가해야 합니다.

Windows가 아닌 다른 운영 체제를 사용하는 클라이언트 디바이스의 경우 다음 지침을 참조해 사용자가 설치할 수 있는 루트 및 중간 인증서를 배포하십시오.

- Mac용 Horizon Client는 [루트 및 중간 인증서를 신뢰하도록 Mac용 Horizon Client 구성](#)을 참조하십시오.
- iOS용 Horizon Client는 [루트 및 중간 인증서를 신뢰하도록 iOS용 Horizon Client 구성](#)을 참조하십시오.
- Android용 Horizon Client는 "Android 3.0 사용자 가이드"와 같은 Google 웹 사이트 설명서를 참조하십시오.
- Linux용 Horizon Client는 Ubuntu 설명서를 참조하십시오.

사전 요구 사항

서버 인증서가 1024 이상의 KeyLength 값으로 생성되었는지 확인합니다. 클라이언트 끝점은 서버에서 1024 미만의 KeyLength로 생성된 인증서의 유효성을 검사하지 않으므로 클라이언트가 서버에 연결되지 않습니다.

절차

- 1 Enterprise NTAAuth 저장소에 인증서를 게시하려면 Active Directory 서버에서 `certutil` 명령을 사용하십시오.

예: `certutil -dspublish -f path_to_root_CA_cert NTAAuthCA`

- 2 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동하십시오.

AD 버전	탐색 경로
Windows 2003	<ol style="list-style-type: none"> a 시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터를 선택합니다. b 도메인을 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다. c 그룹 정책 탭에서 열기를 클릭하여 그룹 정책 관리 플러그인을 엽니다. d 기본 도메인 정책을 마우스 오른쪽 단추로 클릭하고 편집을 클릭합니다.
Windows 2008	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2012 R2	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2016	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.

- 3 컴퓨터 구성 섹션을 확장하고 **Windows 설정 > 보안 설정 > 공개 키 정책**으로 이동합니다.

- 4 인증서를 가져 오십시오.

옵션	설명
루트 인증서	<ol style="list-style-type: none"> a 신뢰할 수 있는 루트 인증 기관을 마우스 오른쪽 버튼으로 클릭하고 가져오기를 선택합니다. b 마법사에 표시된 메시지에 따라 루트 인증서(예: rootCA.cer)를 가져오고 확인을 클릭합니다.
중간 인증서	<ol style="list-style-type: none"> a 중간 인증 기관을 마우스 오른쪽 버튼으로 클릭하고 가져오기를 선택합니다. b 마법사에 표시된 메시지에 따라 중간 인증서(예: intermediateCA.cer)를 가져오고 확인을 클릭합니다.

- 5 **그룹 정책** 창을 닫으십시오.

이제 도메인의 모든 시스템의 신뢰할 수 있는 루트 인증서 저장소 및 중간 인증서 저장소에 인증서 정보가 있으므로 루트 및 중간 인증서를 신뢰할 수 있습니다.

루트 및 중간 인증서를 신뢰하도록 Mac용 Horizon Client 구성

Mac용 Horizon Client를 실행하는 컴퓨터에서 신뢰하지 않는 CA가 서버 인증서를 서명한 경우 루트 및 중간 인증서를 신뢰하도록 이러한 컴퓨터를 구성할 수 있습니다. 신뢰 체인의 루트 인증서 및 모든 중간 인증서를 클라이언트 컴퓨터에 배포해야 합니다.

절차

1 루트 인증서와 중간 인증서를 Mac용 Horizon Client를 실행하는 컴퓨터에 제공합니다.

2 Mac 컴퓨터에서 루트 인증서를 엽니다.

인증서에는 다음 메시지가 표시됩니다. 현재 이후로 컴퓨터에서 *CA 이름*에서 서명한 인증서를 신뢰하도록 설정하시겠습니까?

3 **항상 신뢰**를 클릭합니다.

4 사용자 암호를 입력합니다.

5 신뢰 체인의 모든 중간 인증서에 대해 2 ~ 4단계를 반복합니다.

루트 및 중간 인증서를 신뢰하도록 iOS용 Horizon Client 구성

iOS용 Horizon Client를 실행하는 iPad 및 iPhone에서 신뢰하지 않는 CA가 서버 인증서를 서명한 경우 루트 및 중간 인증서를 신뢰하도록 해당 디바이스를 구성할 수 있습니다. 신뢰 체인의 루트 인증서 및 모든 중간 인증서를 해당 디바이스에 배포해야 합니다.

절차

1 루트 인증서 및 중간 인증서를 e-메일 첨부 파일로 iPad에 전송합니다.

2 루트 인증서의 e-메일 첨부 파일을 열고 **설치**를 선택합니다.

인증서에서 다음과 같은 내용의 메시지를 표시합니다.

확인할 수 없는 프로파일입니다. 인증서 이름의 신뢰성을 확인할 수 없습니다. 이 프로파일을 설치하면 iPad의 설정이 변경됩니다. 루트 인증서입니다. 인증서 인증서 이름을 설치하면 iPad의 신뢰할 수 있는 인증서 목록에 추가됩니다.

3 다시 한 번 **설치**를 선택합니다.

4 신뢰 체인의 모든 중간 인증서에 대해 2단계와 3단계를 반복합니다.

서버 인증서에 대한 인증서 해지 검사 구성

각 연결 서버 인스턴스가 자체 인증서와 연결된 보안 서버의 인증서에 대한 인증서 해지 검사를 수행합니다. 또한 각 인스턴스가 vCenter 및 View Composer Server의 인증서에 대한 연결을 구성할 때마다 해당 인증서를 검사합니다. 기본적으로 루트 인증서를 제외한 체인의 모든 인증서가 검사됩니다. 그러나 이 기본 동작을 변경할 수 있습니다.

SAML 2.0 인증자가 연결 서버 인스턴스에서 사용되도록 구성된 경우 연결 서버가 SAML 2.0 서버 인증서에 대한 인증서 해지 검사도 수행합니다.

Horizon 7는 CRL(인증서 해지 목록) 및 OCSP(온라인 인증서 상태 프로토콜)와 같은 다양한 방법을 사용하여 인증서 해지 검사를 지원합니다. CRL은 인증서를 발행한 CA에서 게시한 해지된 인증서 목록입니다. OCSP는 X.509 인증서의 해지 상태를 얻는 데 사용되는 인증서 유효성 검사 프로토콜입니다.

해지된 인증서 목록인 CRL은 종종 인증서에서 지정되는 인증서 배포 지점(DP)에서 다운로드됩니다. 서버가 인증서에 지정된 CRL DP URL에 정기적으로 연결하여 목록을 다운로드하고 서버 인증서가 해지되었는지 확인합니다. OCSP를 사용해 서버가 OCSP 응답자에 요청을 보내 인증서의 해지 상태를 확인합니다.

타사 인증 기관(CA)에서 서버 인증서를 가져온 경우 인증서에 해지 상태를 확인할 수 있는 수단이 하나 이상 포함되어 있습니다(예: OCSP 응답자의 CRL DP URL 또는 URL). 자체 CA가 있고 인증서를 생성하되 인증서에 해지 정보를 포함하지 않을 경우 인증서 해지 검사에 실패합니다. 그러한 인증서의 해지 정보에는 CRL을 호스팅하는 서버의 웹 기반 CRL DP에 대한 URL 등이 포함될 수 있습니다.

자체 CA가 있지만 인증서에 인증서 해지 정보를 포함하지 않거나 포함할 수 없는 경우 인증서에 대해 해지 검사를 수행하지 않거나 체인의 특정 인증서만 검사하도록 선택할 수 있습니다. 서버에서 Windows 레지스트리 편집기를 사용하여 HKLM\Software\VMware, Inc.\VMware VDMW\Security 아래에서 문자열(REG_SZ) 값 **CertificateRevocationCheckType**을 생성하고 이 값을 다음 데이터 값 중 하나로 설정할 수 있습니다.

값 설명

- 1 인증서 해지 검사를 수행하지 않습니다.
- 2 서버 인증서만 검사합니다. 체인의 다른 인증서를 검사하지 않습니다.
- 3 체인의 모든 인증서를 검사합니다.
- 4 (기본) 루트 인증서를 제외한 모든 인증서를 검사합니다.

이 레지스트리 값이 설정되지 않았거나 설정된 값이 올바르지 않은 경우(즉, 이 값이 1, 2, 3 또는 4가 아닌 경우) 루트 인증서를 제외한 모든 인증서가 검사됩니다. 해지 검사를 수행할 각 서버에서 이 레지스트리 값을 설정합니다. 이 값을 설정한 후 시스템을 새로 시작할 필요가 없습니다.

참고 조직에서 인터넷 액세스를 위해 프록시 설정을 사용할 경우 프록시 설정을 사용해 보안 클라이언트 연결에 사용되는 보안 서버 또는 연결 서버 인스턴스에 대해 인증서 해지 검사를 수행할 수 있도록 연결 서버 컴퓨터를 구성해야 할 수 있습니다. 연결 서버 인스턴스가 인터넷에 액세스할 수 없는 경우 인증서 해지 검사에 실패할 수 있으며 연결 서버 인스턴스 또는 연결된 보안 서버가 Horizon Administrator 대시보드에 빨간색으로 표시될 수 있습니다. 이 문제를 해결하려면 "Horizon 7 관리" 문서의 "보안 서버 인증서 해지 검사 문제 해결"을 참조하십시오.

새 TLS 인증서를 사용하도록 PCoIP 보안 게이트웨이 구성

산업 또는 국가 보안 규정을 준수하려면 PCoIP 보안 게이트웨이(PSG) 서비스에서 생성한 기본 TLS 인증서를 CA에서 서명한 인증서로 바꾸십시오.

Horizon 7에서 PSG 서비스는 시작 시 기본 자체 서명 TLS 인증서를 생성합니다. PSG 서비스는 PSG에 연결된 Horizon Client 2.0(또는 Windows용 Horizon Client 5.2) 이상 릴리스를 실행하는 클라이언트에 자체 서명 인증서를 제공합니다.

또한 PSG는 PSG에 연결된 이전 클라이언트 또는 이전 릴리스를 실행하는 클라이언트에 제공되는 기본 레거시 TLS 인증서를 제공합니다.

기본 인증서는 클라이언트 끝점에서 PSG로의 보안 연결을 제공하므로 Horizon Administrator에서 추가로 구성할 필요가 없습니다. 그러나 특히 준수 테스트를 통과하기 위해 보안 스캐너를 사용해야 하는 배포의 경우 CA 서명 인증서를 사용하도록 PSG 서비스를 구성하는 것이 좋습니다.

반드시 필요하지는 않지만 기본 PSG 인증서를 CA 서명 인증서로 교체하기 전에 서버를 위한 새 CA 서명 TLS 인증서를 구성하는 것이 좋습니다. 이후 절차에서는 PSG가 실행 중인 서버의 Windows 인증서 저장소에 CA 서명 인증서를 이미 가져왔다고 가정합니다.

참고 준수 테스트를 위해 보안 스캐너를 사용하는 경우 서버와 동일한 인증서를 사용하고 PSG 포트 전에 View 포트를 스캔하도록 PSG를 설정하여 시작할 수 있습니다. View 포트 스캔 도중 발생하는 신뢰 또는 유효성 검사 문제로 인해 PSG 포트 및 인증서 테스트가 무효화되지 않도록 이러한 문제를 해결할 수 있습니다. 그런 다음 PSG를 위한 고유한 인증서를 구성하고 다시 스캔을 수행할 수 있습니다.

절차

1 서버 이름이 PSG 인증서 주체 이름과 일치하는지 확인

연결 서버 인스턴스 또는 보안 서버가 설치된 경우 설치 관리자가 컴퓨터의 FQDN을 포함하는 값으로 레지스트리 설정을 만듭니다. 이 값이 보안 스캐너가 PSG 포트에 도달하기 위해 사용하는 URL의 서버 이름 부분과 일치하는지 확인해야 합니다. 서버 이름도 PSG에 사용하려는 TLS 인증서의 주체 이름 또는 주체 대체 이름(SAN)과 일치해야 합니다.

2 Windows 인증서 저장소에 PSG 인증서 구성

기본 PSG 인증서를 CA 서명 인증서로 교체하려면 PSG가 실행 중인 보안 서버 컴퓨터 또는 연결 서버의 Windows 로컬 컴퓨터 인증서 저장소에 인증서와 해당 개인 키를 구성해야 합니다.

3 Windows 레지스트리에서 PSG 인증서 대화명 설정

PSG는 서버 이름과 인증서 대화명을 통해 사용할 TLS 인증서를 식별합니다. 연결 서버 또는 PSG가 실행 중인 보안 서버 컴퓨터의 Windows 레지스트리에서 대화명 값을 설정해야 합니다.

4 (선택 사항) PSG에 대한 연결에 CA 서명 인증서를 강제로 사용하도록 설정

PSG에 대한 모든 클라이언트 연결에 기본 레거시 인증서 대신 PSG를 위한 CA 서명 인증서를 사용하도록 할 수 있습니다. PSG를 위한 CA 서명 인증서를 구성할 경우에는 이 절차가 필요하지 않습니다. Horizon 7 배포에 CA 서명 인증서를 강제로 사용하도록 하는 것이 적절한 경우에만 이러한 단계를 수행하십시오.

서버 이름이 PSG 인증서 주체 이름과 일치하는지 확인

연결 서버 인스턴스 또는 보안 서버가 설치된 경우 설치 관리자가 컴퓨터의 FQDN을 포함하는 값으로 레지스트리 설정을 만듭니다. 이 값이 보안 스캐너가 PSG 포트에 도달하기 위해 사용하는 URL의 서버 이름 부분과 일치하는지 확인해야 합니다. 서버 이름도 PSG에 사용하려는 TLS 인증서의 주체 이름 또는 주체 대체 이름(SAN)과 일치해야 합니다.

예를 들어, 스캐너가 URL `https://view.customer.com:4172`로 PSG에 연결하려면 레지스트리 설정에 `view.customer.com` 값이 포함되어 있어야 합니다. 설치 도중 설정된 연결 서버 또는 보안 서버 컴퓨터의 FQDN이 이 외부 서버 이름과 동일하지 않을 수도 있습니다.

절차

- 1 연결 서버 또는 PColP 보안 게이트웨이가 실행 중인 보안 서버 호스트에서 Windows 레지스트리 편집기를 시작합니다.
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway\SSLCertPsgSni 레지스트리 설정으로 이동합니다.
- 3 SSLCertPsgSni 설정의 값이 스캐너가 PSG에 연결하는 데 사용할 URL의 서버 이름과 일치하고 PSG에 설치하려는 TLS 인증서의 주체 이름 또는 주체 대체 이름과 일치하는지 확인합니다.
이 값이 일치하지 않으면 올바른 값으로 바꾸십시오.
- 4 변경 내용을 적용하려면 VMware Horizon View PColP 보안 게이트웨이 서비스를 다시 시작합니다.

다음에 수행할 작업

CA 서명 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져오고 인증서 대화명을 구성하십시오.

Windows 인증서 저장소에 PSG 인증서 구성

기본 PSG 인증서를 CA 서명 인증서로 교체하려면 PSG가 실행 중인 보안 서버 컴퓨터 또는 연결 서버의 Windows 로컬 컴퓨터 인증서 저장소에 인증서와 해당 개인 키를 구성해야 합니다.

PSG가 고유 인증서를 사용하도록 하려면 내보낼 수 있는 개인 키와 함께 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져오고 해당 대화명을 설정해야 합니다.

PSG가 서버와 동일한 인증서를 사용하도록 하려면 이 절차를 수행하지 않아도 됩니다. 그러나 Windows 레지스트리에서 서버 인증서 주체 이름과 일치하도록 서버 이름을 설정한 다음 대화명을 **vdm**으로 설정해야 합니다.

사전 요구 사항

- 키 길이가 최소한 1,024비트 이상인지 확인하십시오.
- TLS 인증서가 유효한지 확인하십시오. 서버 컴퓨터의 현재 시간이 인증서 시작 날짜와 종료 날짜 사이여야 합니다.
- 인증서 주체 이름 또는 주체 대체 이름이 Windows 레지스트리의 SSLCertPsgSni 설정과 일치하는지 확인하십시오. [서버 이름이 PSG 인증서 주체 이름과 일치하는지 확인](#)의 내용을 참조하십시오.
- 인증서 스냅인이 MMC에 추가되었는지 확인하십시오. [MMC에 인증서 스냅인 추가](#)의 내용을 참조하십시오.
- 인증서를 Windows 인증서 저장소로 가져오는 방법을 숙지하십시오. [Windows 인증서 저장소에 서명된 서버 인증서 가져오기](#)의 내용을 참조하십시오.
- 인증서 대화명을 편집하는 방법을 숙지하십시오. [인증서 대화명 수정](#)의 내용을 참조하십시오.

절차

- 1 Windows Server 호스트의 MMC 창에서 **인증서(로컬 컴퓨터) > 개인** 폴더를 선택합니다.

2 추가 작업 > 모든 작업 > 가져오기를 선택하여 PSG에 발급된 TLS 인증서를 가져옵니다.

인증서 가져오기 마법사에서 다음 설정을 선택합니다.

a **이 키를 내보낼 수 있도록 표시**

b **확장 가능한 모든 속성 포함**

마법사를 종료하여 **Personal** 폴더로 인증서 가져오기를 마칩니다.

3 다음 단계 중 하나를 수행하여 새 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.

4 새 인증서를 마우스 오른쪽 단추로 클릭하고 **속성**을 클릭합니다.

5 일반 탭에서 **대화명** 텍스트를 삭제하고 선택한 대화명을 입력합니다.

다음 절차에서 설명된 것처럼 Windows 레지스트리의 SSLCertWinCertFriendlyName 설정에 지정된 것과 정확히 같은 이름을 입력해야 합니다.

6 적용과 확인을 차례로 클릭합니다.

PSG가 PCoIP를 통해 서버에 연결하는 클라이언트 디바이스에 CA 서명 인증서를 제공합니다.

참고 이 절차는 레거시 클라이언트 디바이스에는 영향을 주지 않습니다. PSG는 PCoIP를 통해 이 서버에 연결하는 레거시 클라이언트 디바이스에는 계속해서 기본 레거시 인증서를 제공합니다.

다음에 수행할 작업

Windows 레지스트리에서 인증서 대화명을 구성합니다.

Windows 레지스트리에서 PSG 인증서 대화명 설정

PSG는 서버 이름과 인증서 대화명을 통해 사용할 TLS 인증서를 식별합니다. 연결 서버 또는 PSG가 실행 중인 보안 서버 컴퓨터의 Windows 레지스트리에서 대화명 값을 설정해야 합니다.

인증서 대화명 **vdm**은 모든 연결 서버 인스턴스와 보안 서버에서 사용됩니다. 반면, PSG 인증서를 위한 고유한 인증서 대화명을 구성할 수 있습니다. PSG가 사용자가 Windows 인증서 저장소에 설정할 대화명과 일치하는 이름을 찾을 수 있도록 Windows 레지스트리 설정을 구성해야 합니다.

PSG는 PSG가 실행 중인 서버와 동일한 TLS 인증서를 사용할 수 있습니다. 서버와 동일한 인증서를 사용하도록 PSG를 구성하는 경우 대화명이 **vdm**이어야 합니다.

레지스트리와 Windows 인증서 저장소의 대화명 값은 대/소문자를 구분합니다.

사전 요구 사항

- Window 레지스트리에 PSG 포트에 도달하는 데 사용되며 PSG 인증서 주체 이름 또는 주체 대체 이름과 일치하는 올바른 주체 이름이 있는지 확인하십시오. **서버 이름이 PSG 인증서 주체 이름과 일치하는지 확인**의 내용을 참조하십시오.

- 인증서 대화명이 Windows 로컬 컴퓨터 인증서 저장소에 구성되었는지 확인하십시오. [Windows 인증서 저장소에 PSG 인증서 구성](#)의 내용을 참조하십시오.

절차

- 1 연결 서버 또는 PColP 보안 게이트웨이가 실행 중인 보안 서버 컴퓨터에서 Windows 레지스트리 편집기를 시작합니다.
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway 레지스트리 키로 이동합니다.
- 3 이 레지스트리 키에 새 문자열(REG_SZ) 값 SSLCertWinCertFriendlyName을 추가합니다.
- 4 SSLCertWinCertFriendlyName 값을 수정하고 PSG에서 사용할 인증서 대화명을 입력합니다.
예: **pcoip**
서버와 동일한 인증서를 사용하는 경우 값이 **vdm**이어야 합니다.
- 5 변경 내용을 적용하려면 VMware Horizon View PColP 보안 게이트웨이 서비스를 다시 시작합니다.

다음에 수행할 작업

클라이언트 디바이스가 계속 PSG에 연결하는지 확인하십시오.

준수 테스트를 위해 보안 스캐너를 사용할 경우 PSG 포트를 스캔하십시오.

PSG에 대한 연결에 CA 서명 인증서를 강제로 사용하도록 설정

PSG에 대한 모든 클라이언트 연결에 기본 레거시 인증서 대신 PSG를 위한 CA 서명 인증서를 사용하도록 할 수 있습니다. PSG를 위한 CA 서명 인증서를 구성할 경우에는 이 절차가 필요하지 않습니다. Horizon 7 배포에 CA 서명 인증서를 강제로 사용하도록 하는 것이 적절한 경우에만 이러한 단계를 수행하십시오.

경우에 따라 PSG가 보안 스캐너에 CA 서명 인증서 대신 기본 레거시 인증서를 제공하여 PSG 포트에 대한 준수 테스트가 무효화될 수 있습니다. 이 문제를 해결하려면 연결을 시도하는 디바이스에 기본 레거시 인증서를 제공하지 않도록 PSG를 구성하십시오.

중요 이 절차를 수행하면 모든 레거시 클라이언트가 PColP를 통해 이 서버에 연결하지 못하게 됩니다.

사전 요구 사항

썬 클라이언트를 포함해 이 서버에 연결하는 모든 클라이언트 디바이스가 Windows용 Horizon Client 5.2 또는 Horizon Client 2.0 이상 릴리스를 실행하는지 확인합니다. 레거시 클라이언트를 업그레이드해야 합니다.

절차

- 1 연결 서버 또는 PColP 보안 게이트웨이가 실행 중인 보안 서버 컴퓨터에서 Windows 레지스트리 편집기를 시작합니다.
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway 레지스트리 키로 이동합니다.

- 3 이 레지스트리 키에 새 문자열(REG_SZ) 값 SSLCertPresentLegacyCertificate를 추가합니다.
- 4 SSLCertPresentLegacyCertificate 값을 0으로 설정합니다.
- 5 변경 내용을 적용하려면 VMware Horizon View PCoIP 보안 게이트웨이 서비스를 다시 시작합니다.

vCenter Server 또는 View Composer 인증서를 신뢰하도록 Horizon Administrator 설정

Horizon Administrator 대시보드에서 신뢰할 수 없는 vCenter Server 또는 View Composer 인증서를 신뢰하도록 Horizon 7을 구성할 수 있습니다.

CA에서 서명한 TLS 인증서를 사용하도록 vCenter Server와 View Composer를 구성하는 것이 좋습니다. 또는 vCenter Server 또는 View Composer의 기본 인증서 지문을 허용할 수 있습니다.

마찬가지로 CA에서 서명한 TLS 인증서를 사용하도록 SAML 2.0 인증자를 구성하는 것이 좋습니다. 또는 Horizon Administrator 대시보드에서 기본 인증서의 지문을 허용하여 신뢰할 수 없는 SAML 2.0 서버 인증서를 신뢰하도록 Horizon 7을 구성할 수 있습니다.

CA에서 서명한 TLS 인증서 사용 시 장점

CA는 인증서와 작성자의 ID를 보증하는 신뢰할 수 있는 엔티티입니다. 신뢰할 수 있는 CA에서 인증서에 서명한 경우, 사용자에게 인증서 확인을 묻는 메시지가 더 이상 표시되지 않으며, 추가 구성 없이 웹 클라이언트 디바이스에 연결할 수 있습니다.

www.mycorp.com과 같은 웹 도메인에 특정한 TLS 서버 인증서를 요청하거나 *.mycorp.com과 같이 도메인 전반에 사용할 수 있는 와일드카드 TLS 서버 인증서를 요청할 수 있습니다. 여러 서버 또는 여러 하위 도메인에 인증서를 설치할 경우, 관리를 간소화하기 위해 와일드카드 인증서를 요청할 수 있습니다.

일반적으로 도메인 특정 인증서는 보안 설치에서 사용되며, CA는 대개 와일드카드 인증서보다 도메인 특정 인증서에 대해 손실에 대비한 더 높은 수준의 보호를 보장합니다. 다른 서비스에서 공유되는 와일드카드 인증서를 사용하는 경우 이러한 다른 서비스의 보안도 Horizon 7 제품 보안에 영향을 미칩니다. 와일드카드 인증서를 사용할 때는 개인 키를 서버 간에 전송할 수 있는지 확인해야 합니다.

기본 인증서를 자신의 인증서와 교체할 경우 클라이언트는 인증서를 사용하여 서버를 인증합니다. 인증서가 CA에서 서명되지 않은 경우 CA의 인증서는 기본적으로 브라우저에 내장되어 있거나 클라이언트가 액세스할 수 있는 신뢰된 데이터베이스에 있습니다. 클라이언트가 인증서에 동의한 후 인증서에 포함된 공용 키로 암호화된 비밀 키를 사용하여 응답합니다. 비밀 키는 클라이언트 및 서버 사이의 트래픽을 암호화하기 위해 사용됩니다.

Horizon 연결 서버 및 보안 서버의 인증서 문제 해결

Horizon 7 Server에 인증서 문제가 있을 경우 Horizon Administrator에 연결하지 못하거나 서버에 대해 빨간색 상태 표시기가 표시될 수 있습니다.

문제

문제가 있는 연결 서버 인스턴스에서 Horizon Administrator에 연결할 수 없습니다. 동일한 포드의 다른 연결 서버 인스턴스에서 Horizon Administrator에 연결하면 문제가 발생한 연결 서버 인스턴스의 대시보드 상태 표시기가 빨간색으로 나타납니다.

다른 연결 서버 인스턴스에서 빨간색 상태 표시기를 클릭하면 SSL 인증서: 유효하지 않음 및 상태: (비어 있음)이 표시되며 유효한 인증서를 찾을 수 없음을 나타냅니다. Horizon 7 로그 파일에 keystore의 인증서 검증 안 함과 같은 오류 텍스트를 표시하는 오류 유형의 로그 항목이 포함됩니다.

Horizon 7 로그 데이터는 연결 서버 인스턴스의 C:\ProgramData\VMware\WDM\logs\Wlog-*.txt에 있습니다.

원인

다음과 같은 이유로 인증서가 Horizon 7 Server에 설치되지 않았을 수 있습니다.

- 인증서가 Windows 로컬 컴퓨터 인증서 저장소의 개인 폴더에 없습니다.
- 인증서 저장소에 해당 인증서에 대한 개인 키가 없습니다.
- 인증서에 **vdm**이라는 대화명이 없습니다.
- Windows Server 2008 이상 서버의 경우 v3 인증서 템플릿에서 인증서가 생성됩니다. Horizon 7가 개인 키를 검색할 수 없지만 인증서 스냅인을 통해 Windows 인증서 저장소를 살펴보면 저장소에 개인 키가 있는 것으로 표시됩니다.

해결책

- ◆ Windows 로컬 컴퓨터 인증서 저장소의 개인 폴더로 인증서를 가져왔는지 확인합니다.
[Windows 인증서 저장소에 서명된 서버 인증서 가져오기](#)를 참조하십시오.
- ◆ 인증서에 개인 키가 포함되어 있는지 확인합니다.
[Windows 인증서 저장소에 서명된 서버 인증서 가져오기](#)를 참조하십시오.
- ◆ 인증서에 **vdm**이라는 대화명이 있는지 확인합니다.
[인증서 대화명 수정](#)를 참조하십시오.
- ◆ 인증서가 v3 인증서 템플릿에서 생성된 경우 v3 템플릿을 사용하지 않는 CA로부터 서명된 올바른 인증서를 가져옵니다.
[CA에서 서명된 TLS 인증서 가져오기](#)를 참조하십시오.

처음으로 Horizon 7 구성

9

Horizon 7 서버 소프트웨어를 설치하고 서버에 대해 SSL 인증서를 구성한 후에는 몇 가지 추가 단계를 수행하여 Horizon 7 환경을 설정해야 합니다.

vCenter Server 및 View Composer 사용자 계정을 구성하고, Horizon 7 라이선스 키를 설치하고, vCenter Server와 View Composer를 Horizon 7 환경에 추가하고, PCoIP 보안 게이트웨이와 보안 채널을 구성하고, 필요한 경우 Horizon 7 환경을 지원하도록 Windows Server 설정의 크기를 조정합니다.

본 장은 다음 항목을 포함합니다.

- [vCenter Server, View Composer 및 인스턴트 클론에 대한 사용자 계정 구성](#)
- [처음으로 Horizon 연결 서버 구성](#)
- [Horizon Client 연결 구성](#)
- [Horizon 7 서비스의 기본 포트 교체](#)
- [Windows Server 설정을 크기 조정하여 배포 지원](#)

vCenter Server, View Composer 및 인스턴트 클론에 대한 사용자 계정 구성

vCenter Server를 Horizon 7와 함께 사용하려면 적절한 vCenter Server 권한이 있는 사용자 계정을 구성해야 합니다. 적절한 권한이 있는 vCenter Server 역할을 생성한 후 해당 역할을 vCenter Server 사용자 계정에 할당할 수 있습니다.

View Composer를 vCenter Server와 다른 시스템에 설치하는 경우 Horizon 7가 독립 실행형 시스템의 View Composer 서비스에 인증하는 데 사용할 수 있는 Active Directory의 사용자 계정도 생성해야 합니다.

View Composer를 사용하는 경우 View Composer가 Active Directory에서 특정 작업을 수행하도록 허용하는 Active Directory의 세 번째 사용자 계정을 생성해야 합니다. View Composer에서는 연결된 클론 가상 시스템을 Active Directory 도메인에 가입시키기 위해 이 계정을 필요로 합니다. [View Composer AD 작업을 위한 사용자 계정 생성](#)를 참조하십시오.

인스턴트 클론을 사용하는 경우 연결 서버가 Active Directory에서 특정 작업을 수행하도록 허용하는 Active Directory의 사용자 계정을 생성해야 합니다. 연결 서버에서는 인스턴트 클론 가상 시스템을 Active Directory 도메인에 가입시키기 위해 이 계정을 필요로 합니다. [인스턴트 클론 작업을 위한 사용자 계정 만들기](#)를 참조하십시오.

요약하자면 Horizon 7을 처음 구성할 때 Horizon Administrator에서 이러한 사용자 계정을 제공해야 합니다.

- vCenter Server 사용자는 Horizon 7과 View Composer가 vCenter Server에서 작업을 수행하도록 허용합니다.
- 독립 실행형 View Composer Server 사용자는 Horizon 7가 독립 실행형 시스템의 View Composer 서비스에 인증하도록 허용합니다.

View Composer를 vCenter Server와 동일한 시스템에 설치하는 경우 vCenter Server 사용자가 앞의 기능을 둘 다 수행하며 독립 실행형 View Composer Server 사용자를 사용하지 않습니다.

- AD 작업에 대한 View Composer 사용자는 View Composer가 Active Directory에서 특정 작업을 수행하도록 허용합니다.
- AD 작업에 대한 인스턴트 클론 사용자는 연결 서버가 Active Directory에서 특정 작업을 수행하도록 허용합니다.

vCenter Server 사용자 및 View Composer 사용자 사용자

이러한 사용자 계정을 생성하여 구성한 다음 Horizon Administrator의 사용자 이름을 지정합니다.

- vCenter Server를 Horizon 7에 추가할 때 vCenter Server 사용자를 지정합니다.
- View Composer 설정을 구성하고 **독립 실행형 View Composer Server**를 선택할 때 독립 실행형 View Composer Server 사용자를 지정합니다.
- View Composer 도메인을 구성할 때 AD 작업을 위한 View Composer 사용자를 지정합니다.
- 연결된 클론 풀을 생성할 때 AD 작업을 위한 View Composer 사용자를 지정합니다.

Horizon 7 및 View Composer를 위한 vCenter Server 사용자 구성

Horizon 7가 vCenter Server에서 작업을 수행하도록 허용하는 사용자 계정을 구성하려면 해당 사용자에게 적절한 권한을 가진 vCenter Server 역할을 할당해야 합니다.

View Composer와 함께 또는 View Composer 없이 Horizon 7를 사용하는지 여부에 따라 vCenter Server 역할에 추가해야 하는 권한 목록이 다릅니다. View Composer 서비스는 vCenter Server에서 기본 권한과 함께 권한을 필요로 하는 작업을 수행합니다.

View Composer를 vCenter Server와 동일한 시스템에 설치하는 경우 vCenter Server 사용자를 vCenter Server 시스템의 로컬 시스템 관리자로 만들어야 합니다. 이러한 요구 사항에 따라 Horizon 7가 View Composer 서비스에 인증할 수 있습니다.

View Composer를 vCenter Server와 다른 시스템에 설치하는 경우 vCenter Server 사용자를 vCenter Server 시스템의 로컬 관리자로 만들지 않아도 됩니다. 그러나 View Composer 시스템의 로컬 관리자여야 하는 독립 실행형 View Composer Server 사용자 계정을 생성해야 합니다.

사전 요구 사항

- Active Directory에서 연결 서버 도메인 또는 신뢰할 수 있는 도메인에 사용자를 생성하십시오. [vCenter Server의 사용자 계정 생성](#)를 참조하십시오.
- 해당 사용자 계정에 필요한 vCenter Server 권한을 숙지하십시오. [vCenter Server 사용자에게 필요한 권한](#)를 참조하십시오.
- View Composer를 사용하는 경우, 필요한 추가 권한을 숙지하십시오. [vCenter Server 사용자에게 필요한 View Composer 및 인스턴트 클론 권한](#)를 참조하십시오.

절차

- 1 vCenter Server에서 사용자에게 대해 필요한 권한을 가진 역할을 준비하십시오.

- vCenter Server의 미리 정의된 관리자 역할을 사용할 수 있습니다. 이 역할을 사용하면 vCenter Server에서 모든 작업을 수행할 수 있습니다.
- View Composer를 사용하는 경우 vCenter Server 작업을 수행하기 위해 연결 서버 및 View Composer에 필요한 최소 권한을 가진 제한된 역할을 생성할 수 있습니다.

vSphere Client에서 **홈 > 역할 > 역할 추가**를 클릭하고 **View Composer Administrator**와 같은 역할 이름을 입력한 다음 역할에 대한 권한을 선택하십시오.

이 역할은 연결 서버 및 View Composer가 vCenter Server에서 작업하는 데 필요한 모든 권한을 가지고 있어야 합니다.

- View Composer 없이 Horizon 7을 사용하는 경우 vCenter Server 작업을 수행하기 위해 연결 서버에 필요한 최소 권한을 가진 더욱 제한된 역할을 생성할 수 있습니다.

vSphere Client에서 **홈 > 역할 > 역할 추가**를 클릭하고 **View Manager Administrator**와 같은 역할 이름을 입력한 다음 역할에 대한 권한을 선택하십시오.

- 인스턴트 클론을 사용하는 경우 vCenter Server 작업을 수행하기 위해 연결 서버에 필요한 최소 권한을 가진 제한된 역할을 생성할 수 있습니다.

vSphere Client에서 **홈 > 역할 > 역할 추가**를 클릭하고 **View Manager 인스턴트 클론 관리자**와 같은 역할 이름을 입력한 다음 역할에 대한 권한을 선택하십시오. 인스턴트 클론 권한에 대해서는 [vCenter Server 사용자에게 필요한 View Composer 및 인스턴트 클론 권한](#)을 참조하십시오.

- 2 vSphere Client의 인벤토리 최상위 수준에서 마우스 오른쪽 단추로 vCenter Server를 클릭하고 **사용 권한 추가**를 클릭한 다음 vCenter Server 사용자를 추가하십시오.

참고 vCenter Server 수준의 vCenter Server 사용자를 정의해야 합니다.

- 3 드롭다운 메뉴에서 관리자 역할 또는 생성한 View Composer나 View Manager 역할을 선택한 다음 vCenter Server 사용자에게 할당합니다.
- 4 View Composer를 vCenter Server와 동일한 시스템에 설치하는 경우 vCenter Server 사용자 계정을 vCenter Server 시스템의 로컬 시스템 관리자 그룹의 멤버로 추가합니다.

View Composer를 vCenter Server와 다른 시스템에 설치하는 경우에는 이 단계가 필요하지 않습니다.

다음에 수행할 작업

Horizon Administrator에서 Horizon 7에 vCenter Server를 추가할 때 vCenter Server 사용자를 지정합니다. [Horizon 7에 vCenter Server 인스턴스 추가](#)를 참조하십시오.

vCenter Server 사용자에게 필요한 권한

vCenter Server 사용자는 Horizon 7가 vCenter Server에서 작업을 수행할 수 있도록 충분한 vCenter Server 권한을 가지고 있어야 합니다. 필요한 권한을 사용하여 vCenter Server 사용자의 View Manager 역할을 생성합니다.

표 9-1. View Manager 역할에 필요한 권한

권한 그룹	사용하도록 설정할 권한
폴더	폴더 생성 폴더 삭제
데이터스토어	공간 할당
가상 시스템	구성에서 <ul style="list-style-type: none"> ■ 디바이스 추가 또는 제거 ■ 고급 ■ 디바이스 설정 수정 상호 작용에서 <ul style="list-style-type: none"> ■ 전원 끄기 ■ 전원 켜기 ■ 재설정 ■ 일시 중단 ■ 지우기 또는 축소 작업 수행 인벤토리에서 <ul style="list-style-type: none"> ■ 새로 만들기 ■ 기존 항목에서 생성 ■ 제거 프로비저닝에서 <ul style="list-style-type: none"> ■ 사용자 지정 ■ 템플릿 배포 ■ 사용자 지정 규격 읽기 ■ 템플릿 복제 ■ 가상 시스템 복제
리소스	리소스 풀에 가상 시스템 할당
전역	vCenter Server로 작동 View Storage Accelerator를 사용하지 않는 경우에도 vCenter Server 사용자는 이 권한이 필요합니다.

표 9-1. View Manager 역할에 필요한 권한 (계속)

권한 그룹	사용하도록 설정할 권한
호스트	View Storage Accelerator를 구현하여 ESXi 호스트 캐싱을 수행할 수 있도록 하려면 다음 호스트 권한이 필요합니다. View Storage Accelerator를 사용하지 않을 경우에는 vCenter Server 사용자에게 이 권한이 필요하지 않습니다. 구성에서 ■ 고급 설정
프로파일 기반 스토리지 (vSAN 데이터스토어 또는 가상 볼륨을 사용하는 경우)	(모두)

vCenter Server 사용자에게 필요한 View Composer 및 인스턴트 클론 권한

View Composer 또는 인스턴트 클론을 지원하려면 vCenter Server 사용자에게 Horizon 7을 지원하는 데 필요한 것 이외의 권한이 있어야 합니다.

View Composer 및 인스턴트 클론 권한은 View Manager, View Composer 및 인스턴트 클론에 필요한 권한의 상위 집합을 나타냅니다.

표 9-2. View Composer 및 인스턴트 클론 권한

vCenter Server의 권한 그룹	사용하도록 설정할 권한
폴더	폴더 생성 폴더 삭제
데이터스토어	공간 할당 데이터스토어 찾아보기 하위 수준 파일 작업
호스트	인벤토리에서 ■ 클러스터 수정

표 9-2. View Composer 및 인스턴트 클론 권한 (계속)

vCenter Server의 권한 그룹	사용하도록 설정할 권한
가상 시스템	구성 (모두) 상호 작용에서 ■ 전원 끄기 ■ 전원 켜기 ■ 재설정 ■ 일시 중단 ■ 지우기 또는 축소 작업 수행 ■ 디바이스 연결 인벤토리 (모두) 스냅샷 관리 (모두) 프로비저닝: ■ 사용자 지정 ■ 템플릿 배포 ■ 사용자 지정 규격 읽기 ■ 템플릿 복제 ■ 가상 시스템 복제 ■ 디스크 액세스 허용
리소스	리소스 풀에 가상 시스템 할당 다음 권한은 View Composer 재조정 작업을 수행하는 데 필요합니다. 전원이 꺼진 가상 시스템 마이그레이션
전역	메서드 사용 메서드 사용 안 함 시스템 태그 사용자 지정 특성 관리 사용자 지정 특성 설정 View Storage Accelerator를 구현하여 ESXi 호스트 캐싱을 수행할 수 있도록 하려면 다음 권한이 필요합니다. View Storage Accelerator를 사용하지 않는 경우에도 vCenter Server 사용자는 이 권한이 필요합니다. vCenter Server로 작동
네트워크	(모두)
프로파일 기반 스토리지	(vSAN 데이터스토어 또는 가상 볼륨을 사용하는 경우 - 모두)

표 9-2. View Composer 및 인스턴트 클론 권한 (계속)

vCenter Server의 권한 그룹	사용하도록 설정할 권한
스토리지 보기	보기
암호화 작업	<p>다음 권한은 vTPM(신뢰할 수 있는 플랫폼 모듈) 디바이스에서 인스턴트 클론 VM을 사용하는 경우에 필요합니다.</p> <ul style="list-style-type: none"> ■ 클론 ■ 암호 해독 ■ 직접 액세스 ■ 암호화 ■ KMS 관리 ■ 마이그레이션 ■ 호스트 등록

처음으로 Horizon 연결 서버 구성

연결 서버를 설치한 후에는 제품 라이선스를 설치하고 vCenter Server와 View Composer 서비스를 Horizon 7에 추가해야 합니다. 또한 ESXi 호스트가 연결된 클론 가상 시스템의 디스크 공간을 회수하도록 허용하고 가상 시스템 디스크 데이터를 캐시하도록 ESXi 호스트를 구성할 수 있습니다.

보안 서버를 설치하면 보안 서버가 Horizon 7에 추가되어 Horizon Administrator에 자동으로 나타납니다.

Horizon Administrator 및 Horizon 연결 서버

Horizon Administrator는 Horizon 7에 대한 웹 기반 관리 인터페이스를 제공합니다.

Horizon 연결 서버에는 복제 서버 또는 보안 서버로 작동하는 여러 인스턴스가 포함될 수 있습니다. Horizon 7 배포에 따라 각 연결 서버의 인스턴스가 있는 Horizon Administrator 인터페이스를 사용할 수 있습니다.

다음의 모범 사례를 활용하여 연결 서버에서 Horizon Administrator를 사용하십시오.

- 연결 서버의 호스트 이름 및 IP 주소를 사용하여 Horizon Administrator에 로그인합니다. Horizon Administrator 인터페이스를 사용하여 연결 서버와 모든 관련 보안 서버 또는 복제 서버를 관리합니다.
- 포드 환경에서는 모든 관리자가 동일한 연결 서버의 호스트 이름 및 IP 주소를 사용하여 Horizon Administrator에 로그인하는지 확인합니다. Horizon Administrator 웹 페이지에 액세스할 때는 로드 밸런서의 호스트 이름 및 IP 주소를 사용하지 마십시오.
- 사용 중인 연결 서버의 CPA 포드 또는 클러스터 이름을 식별하려면 Horizon Administrator 헤더 및 웹 브라우저 탭에서 이름을 볼 수 있습니다.

참고 보안 서버 대신 Unified Access Gateway 장치를 사용하는 경우에는 Unified Access Gateway REST API를 사용하여 Unified Access Gateway 장치를 관리해야 합니다. Unified Access Gateway의 이전 버전 이름은 Access Point입니다. 자세한 내용은 "Unified Access Gateway 배포 및 구성"의 내용을 참조하십시오.

Horizon Administrator에 로그인

초기 구성 작업을 수행하려면 Horizon Administrator에 로그인해야 합니다.

사전 요구 사항

Horizon Administrator에서 지원하는 웹 브라우저를 사용하는지 확인하십시오. [Horizon Administrator 요구 사항](#) 항목을 참조하십시오.

절차

- 1 웹 브라우저를 열고 다음 URL을 입력하십시오. *server*는 연결 서버 인스턴스의 호스트 이름입니다.

https://*server*/admin

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.

Horizon Administrator에 대한 액세스는 연결 서버 컴퓨터에 구성된 인증서의 유형에 따라 다릅니다. 연결 서버 호스트에서 웹 브라우저를 여는 경우 **https://localhost** 대신 **https://127.0.0.1**을 사용하여 연결합니다. 이렇게 하면 localhost 확인에서 잠재적인 DNS 공격이 방지되므로 보안이 강화됩니다.

옵션	설명
Horizon 연결 서버에 대해 CA에서 서명한 인증서를 구성했습니다.	처음 연결하면 웹 브라우저에서 VMware Horizon 7 시작 페이지를 표시합니다.
Horizon 연결 서버에서 제공되는 기본 자체 서명 인증서가 구성됩니다.	처음 연결할 때 신뢰할 수 있는 인증서 기관에서 해당 주소와 연결된 보안 인증서를 발행하지 않았다는 내용의 경고 페이지가 웹 브라우저에 나타날 수 있습니다. 현재 TLS 인증서를 계속 사용하려면 무시 를 클릭합니다.

- 2 Horizon Administrator 아래에서 **시작**을 클릭합니다.

- 3 관리자 역할을 가진 계정을 사용하여 로그인합니다.

복제된 그룹에 독립 실행형 연결 서버 인스턴스 또는 첫 번째 연결 서버 인스턴스를 설치할 때 관리자 역할에 대한 초기 할당을 작성합니다. 기본적으로 연결 서버를 설치하는 데 사용하는 계정이 선택되지만 이 계정을 Administrators 로컬 그룹 또는 도메인 전역 그룹으로 변경할 수 있습니다.

Administrators 로컬 그룹을 선택한 경우 직접 또는 전역 그룹 구성원을 통해 이 그룹에 추가된 모든 도메인 사용자를 사용할 수 있습니다. 이 그룹에 추가된 로컬 사용자는 사용할 수 없습니다.

Horizon Administrator에 로그인한 후 **View 구성 > 관리자**를 통해 Administrators 역할을 가진 사용자 및 그룹의 목록을 변경할 수 있습니다.

제품 라이선스 키 설치

연결 서버를 사용하기 전에 제품 라이선스 키를 입력해야 합니다.

참고 Horizon 7 구독 라이선스가 있는 경우 제품 라이선스 키가 필요하지 않습니다. 구독 라이선스에 대한 자세한 내용은 [#unique_128](#)을 참조하십시오.

처음 로그인하면 Horizon Administrator에 제품 라이선싱 및 사용량 페이지가 나타납니다.

라이선스 키를 설치한 다음 로그인할 때 Horizon Administrator에 대시보드 페이지가 나타납니다.

복제된 연결 서버 인스턴스 또는 보안 서버를 설치할 때는 라이선스 키를 구성하지 않아도 됩니다. 복제된 인스턴스 및 보안 서버는 View LDAP 구성에 저장된 일반 라이선스 키를 사용합니다.

참고 연결 서버를 사용하려면 유효한 라이선스 키가 필요합니다. 제품 라이선스 키는 25자 키입니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 제품 라이선싱 및 사용량**을 선택합니다.
- 2 **라이선싱** 패널에서 **라이선스 편집**을 클릭합니다.
- 3 라이선스 일련 번호를 입력하고 **확인**을 클릭합니다.
- 4 라이선스 만료 날짜를 확인하십시오.
- 5 제품 라이선스에서 사용 권한을 부여하는 VMware Horizon 7을 기준으로 데스크톱 라이선스, 애플리케이션 원격 라이선스 및 View Composer 라이선스가 사용되도록 설정되었는지 또는 사용되지 않도록 설정되었는지 확인합니다.

VMware Horizon 7의 일부 특징과 기능은 버전에 따라 제공되지 않을 수 있습니다. 버전별 기능 세트 비교는 <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>를 참조하십시오.

Horizon 7에 vCenter Server 인스턴스 추가

Horizon 7 배포에서 vCenter Server 인스턴스에 연결하도록 Horizon 7을 구성해야 합니다. vCenter Server는 Horizon 7이 데스크톱 풀에서 사용하는 가상 시스템을 생성하고 관리합니다.

Linked Mode 그룹에서 vCenter Server 인스턴스를 실행하려면 각 vCenter Server 인스턴스를 Horizon 7에 따로 추가해야 합니다.

Horizon 7는 보안 채널(SSL)을 사용해 vCenter Server 인스턴스에 연결합니다.

사전 요구 사항

- 연결 서버 제품 라이선스 키를 설치하십시오.
- vCenter Server 사용자가 vCenter Server에서 Horizon 7를 지원하는 데 필요한 작업을 수행할 수 있는 사용 권한을 가지도록 준비하십시오. View Composer를 사용하려면 사용자에게 추가 권한을 부여해야 합니다.

[Horizon 7 및 View Composer를 위한 vCenter Server 사용자 구성](#)의 내용을 참조하십시오.

- TLS/SSL 서버 인증서가 vCenter Server 호스트에 설치되어 있는지 확인하십시오. 운영 환경에는 신뢰할 수 있는 인증 기관(CA)에서 서명한 유효한 인증서를 설치하십시오.

테스트 환경에서는 vCenter Server에 설치된 기본 인증서를 사용할 수 있지만 vCenter Server를 Horizon 7에 추가할 때 인증서 지문을 허용해야 합니다.

- 복제된 그룹의 모든 연결 서버 인스턴스가 vCenter Server 호스트에 설치된 서버 인증서의 루트 CA 인증서를 신뢰하는지 확인하십시오. 루트 CA 인증서가 연결 서버 호스트의 Windows 로컬 컴퓨터 인증서 저장소에 위치한 **신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더에 있는지 확인하십시오. 없는 경우 루트 CA 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져오십시오.

자세한 내용은 [Windows 인증서 저장소에 루트 인증서 및 중간 인증서 가져오기](#)를 참조하십시오.

- vCenter Server 인스턴스에 ESXi 호스트가 포함되어 있는지 확인하십시오. vCenter Server 인스턴스에 호스트가 구성되어 있지 않은 경우 인스턴스를 Horizon 7에 추가할 수 없습니다.
- vSphere 5.5 이후 릴리스로 업그레이드하는 경우 vCenter Server 사용자로 사용하는 도메인 관리자 계정에 vCenter Server 로컬 사용자가 vCenter Server로 로그인할 사용 권한이 명시적으로 할당되어 있는지 확인하십시오.
- Horizon 7을 FIPS 모드에서 사용하려는 경우에는 vCenter Server 6.0 이상 및 ESXi 6.0 이상 호스트가 있는지 확인하십시오.

자세한 내용은 [장 4 FIPS 모드에서 Horizon 7 설치](#)의 내용을 참조하십시오.

- vCenter Server와 View Composer의 최대 작업 수 제한을 결정하는 설정을 숙지하십시오. 자세한 내용은 [vCenter Server 및 View Composer의 동시 작업 수 제한 및 동시 전원 작업 수를 설정하여 원격 데스크톱 로그인 스톱 지원](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **vCenter Server** 탭에서 **추가**를 클릭합니다.
- 3 vCenter Server 설정 **서버 주소** 텍스트 상자에 vCenter Server 인스턴스의 FQDN(정규화된 도메인 이름)을 입력합니다.

FQDN에는 호스트 이름과 도메인 이름이 포함되어 있습니다. 예를 들어 FQDN

*myserverhost.companydomain.com*에서 *myserverhost*는 호스트 이름이고 *companydomain.com*은 도메인입니다.

참고 DNS 이름 또는 URL을 사용해 서버를 입력하면 Horizon 7에서 DNS 조회를 통해 이전에 관리자가 IP 주소를 사용하여 Horizon 7에 이 서버를 추가했는지 여부를 확인하지 않습니다. DNS 이름과 IP 주소를 모두 사용해 vCenter Server를 추가하면 충돌이 발생합니다.

- 4 vCenter Server 사용자 이름을 입력하십시오.
예: `domainWuser` 또는 `user@domain.com`
- 5 vCenter Server 사용자 암호를 입력하십시오.
- 6 (선택 사항) 이 vCenter Server 인스턴스에 대한 설명을 입력하십시오.

7 TCP 포트 번호를 입력하십시오.

기본 포트는 443입니다.

8 고급 설정에서 vCenter Server 및 View Composer 작업의 동시 작업 수 제한을 설정합니다.

9 다음을 클릭하여 View Composer 설정 페이지를 표시합니다.

다음에 수행할 작업

View Composer 설정을 구성합니다.

- vCenter Server 인스턴스가 서명된 SSL 인증서로 구성되고 연결 서버가 루트 인증서를 신뢰하면 vCenter Server 추가 마법사에 View Composer 설정 페이지가 표시됩니다.
- vCenter Server 인스턴스가 기본 인증서로 구성된 경우 먼저 기존 인증서의 지문을 허용할지 결정해야 합니다. [기본 TLS 인증서의 지문 허용](#)의 내용을 참조하십시오.

Horizon 7가 여러 vCenter Server 인스턴스를 사용하는 경우 이 절차를 반복해 다른 vCenter Server 인스턴스를 추가하십시오.

View Composer 설정 구성

View Composer를 사용하려면 연결 서버가 View Composer 서비스에 연결할 수 있도록 설정을 구성해야 합니다. View Composer는 자체 독립 실행형 시스템 또는 vCenter Server와 동일한 시스템에 설치할 수 있습니다.

각 View Composer 서비스와 vCenter Server 인스턴스가 일대일로 매핑되도록 하는 것이 좋습니다.

사전 요구 사항

- vCenter Server에 연결하도록 연결 서버를 구성했는지 확인하십시오. 그러려면 vCenter Server 추가 마법사의 vCenter Server 정보 페이지를 작성해야 합니다. [Horizon 7에 vCenter Server 인스턴스 추가](#)를 참조하십시오.
- 이 View Composer 서비스가 아직 다른 vCenter Server 인스턴스에 연결하도록 구성되어 있지 않은지 확인하십시오.
- 독립 실행형 시스템에 View Composer를 설치한 경우 독립 실행형 View Composer Server 사용자 계정을 생성했는지 확인하십시오. 이 도메인 사용자 계정은 View Composer 시스템의 로컬 관리자 그룹의 멤버여야 합니다.

절차

- 1 Horizon Administrator에서 vCenter Server 추가 마법사의 vCenter Server 정보 페이지를 작성하십시오.
 - a **View 구성 > 서버**를 클릭합니다.
 - b vCenter Servers 탭에서 **추가**를 클릭하고 vCenter Server 설정을 입력합니다.

- 2 View Composer를 사용하지 않으려면 View Composer 설정 페이지에서 **View Composer 사용 안 함**을 선택하십시오.

View Composer 사용 안 함을 선택하면 다른 View Composer 설정이 비활성화됩니다. 다음을 클릭하면 vCenter Server 추가 마법사에 스토리지 설정 페이지가 표시됩니다. View Composer 도메인 페이지는 표시되지 않습니다.

- 3 View Composer를 사용할 경우 View Composer 시스템의 위치를 선택하십시오.

옵션	설명
View Composer가 vCenter Server와 동일한 시스템에 설치되었습니다.	<p>a vCenter Server와 함께 설치된 View Composer를 선택합니다.</p> <p>b vCenter Server에 View Composer 서비스를 설치할 때 지정한 포트와 포트 번호가 동일한지 확인합니다. 기본 포트 번호는 18443입니다.</p>
View Composer가 별도의 시스템에 설치되었습니다.	<p>a 독립 실행형 View Composer Server를 선택합니다.</p> <p>b View Composer Server 주소 텍스트 상자에서 View Composer 시스템의 FQDN(정규화된 도메인 이름)을 입력합니다.</p> <p>c View Composer 서비스에 인증할 수 있는 도메인 사용자 계정의 이름을 입력합니다.</p> <p>계정은 독립 실행형 View Composer 시스템의 로컬 관리자 그룹의 멤버여야 합니다.</p> <p>예: domain.com\user 또는 user@domain.com</p> <p>d 이 도메인 사용자 계정의 암호를 입력합니다.</p> <p>e View Composer 서비스를 설치할 때 지정한 포트와 포트 번호가 동일한지 확인합니다. 기본 포트 번호는 18443입니다.</p>

- 4 다음을 클릭하여 View Composer 도메인 페이지를 표시합니다.

다음에 수행할 작업

View Composer 도메인을 구성합니다.

- View Composer 인스턴스가 서명된 SSL 인증서로 구성되고 연결 서버가 루트 인증서를 신뢰하면 vCenter Server 추가 마법사에 View Composer 도메인 페이지가 표시됩니다.
- View Composer 인스턴스가 기본 인증서로 구성된 경우 먼저 기존 인증서의 지문을 허용할지 결정해야 합니다. [기본 TLS 인증서의 지문 허용](#)을 참조하십시오.

View Composer 도메인 구성

View Composer가 연결된 클론 데스크톱을 배포할 Active Directory 도메인을 구성해야 합니다.

View Composer에 대해 여러 도메인을 구성할 수 있습니다. 먼저 vCenter Server와 View Composer 설정을 View에 추가한 후 Horizon Administrator에서 vCenter Server 인스턴스를 편집하여 추가 View Composer 도메인을 추가할 수 있습니다.

사전 요구 사항

- Active Directory 관리자가 AD 작업에 대한 View Composer 사용자를 생성해야 합니다. 이 도메인 사용자는 연결된 클론이 포함된 Active Directory 도메인에서 가상 시스템을 추가 및 제거할 수 있는 사용 권한이 있어야 합니다. 이 사용자에게 필요한 사용 권한에 대한 자세한 내용은 [View Composer AD 작업을 위한 사용자 계정 생성](#)을 참조하십시오.
- Horizon Administrator에서 vCenter Server 추가 마법사의 vCenter Server 정보 및 View Composer 설정 페이지를 완료했는지 확인합니다.

절차

- 1 View Composer 도메인 페이지에서 **추가**를 클릭하여 AD 작업 계정 정보에 대한 View Composer 사용자를 추가하십시오.
- 2 Active Directory 도메인의 도메인 이름을 입력하십시오.
예: **domain.com**
- 3 View Composer 사용자의 도메인 이름을 포함한 도메인 사용자 이름을 입력하십시오.
예: **domain.com\Wadmin**
- 4 계정 암호를 입력하십시오.
- 5 **확인**을 클릭합니다.
- 6 연결된 클론 풀을 배포한 다른 Active Directory 도메인에 권한을 가진 도메인 사용자 계정을 추가하려면 앞의 단계를 반복하십시오.
- 7 **다음**을 클릭하여 스토리지 설정 페이지를 표시합니다.

다음에 수행할 작업

가상 시스템 디스크 공간 재사용을 사용하도록 설정하고 Horizon 7에 대해 View Storage Accelerator를 구성합니다.

인스턴트 클론 도메인 관리자 추가

인스턴트 클론 데스크톱 풀을 생성하려면 먼저 Horizon 7에 인스턴트 클론 도메인 관리자를 추가해야 합니다.

인스턴트 클론 도메인 관리자는 특정 Active Directory 도메인 권한을 가지고 있어야 합니다. "Horizon 7 설치" 문서에서 "vCenter Server 사용자에게 필요한 View Composer 및 인스턴트 클론 권한"을 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 인스턴트 클론 도메인 관리자**를 선택합니다.
- 2 **추가**를 클릭합니다.
- 3 인스턴트 클론 도메인 관리자의 로그인 이름 및 암호를 입력합니다.

vSphere가 연결된 클론 가상 시스템의 디스크 공간을 회수할 수 있도록 허용

vSphere 5.1 이상에서는 Horizon 7의 디스크 공간 회수 기능을 사용하도록 설정할 수 있습니다.

vSphere 5.1에서 시작하면 Horizon 7이 ESXi 호스트에서 연결된 클론의 사용되지 않은 디스크 공간을 재사용하여 연결된 클론에 필요한 총 스토리지 공간을 줄일 수 있는 효율적인 디스크 형식으로 연결된 클론 가상 시스템을 생성합니다.

사용자가 연결된 클론 데스크톱과 상호 작용하므로 클론의 OS 디스크가 확장되어 결국 거의 전체 클론 데스크톱과 비슷한 양의 디스크 공간을 사용할 수 있습니다. 디스크 공간 재사용을 사용하면 연결된 클론을 새로 고치거나 재구성할 필요 없이 OS 디스크의 크기를 줄일 수 있습니다. 가상 시스템의 전원이 켜져 있고 사용자가 원격 데스크톱과 상호 작용하고 있는 동안 공간을 재사용할 수 있습니다.

디스크 공간 재사용은 로그오프 시 새로 고침과 같은 스토리지 절약 전략을 활용할 수 없는 배포에 특히 유용합니다. 예를 들어, 전용 원격 데스크톱에 사용자 애플리케이션을 설치하는 지식 작업자는 원격 데스크톱을 새로 고치거나 재구성할 경우 개인 애플리케이션을 잃을 수 있습니다. 디스크 공간 재사용 기능을 사용하면 Horizon 7가 처음 프로비저닝될 때 시작하는 줄어든 크기에 가깝게 연결된 클론을 유지할 수 있습니다.

이 기능에는 공간 효율적인 디스크 형식 및 공간 재사용 작업의 두 가지 구성 요소가 있습니다.

vSphere 5.1 이상의 환경에서 상위 가상 시스템의 가상 하드웨어 버전이 9 이상인 경우 Horizon 7가 공간 재사용 작업의 설정 여부에 관계없이 공간 효율적인 OS 디스크 형식의 연결된 클론을 생성합니다.

공간 회수 작업을 사용하도록 설정하려면 Horizon Administrator를 사용해 vCenter Server에 대해 공간 재사용을 사용하도록 설정하고 개별 데스크톱 풀의 VM 디스크 공간을 회수해야 합니다. vCenter Server의 공간 재사용 설정은 vCenter Server 인스턴스에 의해 관리되는 모든 데스크톱 풀에서 이 기능을 사용하지 않도록 설정할 수 있는 옵션을 제공합니다. vCenter Server에 대해 이 기능을 사용하지 않도록 설정하면 데스크톱 풀 수준에서 설정이 재정의됩니다.

공간 재사용 기능에 다음과 같은 지점이 적용됩니다.

- 연결된 클론의 공간 효율적인 OS 디스크에서만 작동합니다.
- View Composer 영구 디스크에는 영향을 주지 않습니다.
- vSphere 5.1 이상과 가상 하드웨어 버전 9 이상인 가상 시스템에서만 작동합니다.
- 전체 클론 데스크톱에서는 작동하지 않습니다.
- SCSI 컨트롤러가 있는 가상 시스템에서 작동합니다. IDE 컨트롤러는 지원되지 않습니다.

VCAI(View Composer 어레이 통합)는 공간 효율적인 디스크를 사용하는 가상 시스템이 포함된 풀에서는 지원되지 않습니다. VCAI는 VAAI(vStorage API for Array Integration) 기본 NFS 스냅샷 기술을 사용해 가상 시스템을 복제합니다.

사전 요구 사항

- vCenter Server 및 ESXi 호스트(클러스터의 모든 ESXi 호스트 포함) 버전이 ESXi 5.1 다운로드 패치 ESXi510-201212001 이상이 적용된 5.1인지 확인합니다.

절차

- 1 Horizon Administrator에서 스토리지 설정 페이지 앞에 나오는 vCenter Server 추가 마법사 페이지를 완료합니다.
 - a **View 구성 > 서버**를 선택합니다.
 - b **vCenter Server** 탭에서 **추가**를 클릭합니다.
 - c vCenter Server 정보, View Composer 설정 및 View Composer 도메인 페이지를 완료합니다.

- 2 스토리지 설정 페이지에서 **공간 재사용을 사용하도록 설정**이 선택되었는지 확인합니다.

Horizon 7 5.2 이상을 새로 설치할 경우 공간 재사용이 기본적으로 선택됩니다. Horizon 7 5.1 또는 이전 릴리스에서 Horizon 7 5.2 이상으로 업그레이드할 경우 **공간 재사용을 사용하도록 설정**을 선택해야 합니다.

다음에 수행할 작업

스토리지 설정 페이지에서 View Storage Accelerator를 구성합니다.

Horizon 7에서 디스크 공간 재사용 구성을 완료하려면 데스크톱 풀에 대해 공간 재사용을 설정하십시오.

vCenter Server의 View Storage Accelerator 구성

vSphere 5.1 이상 버전의 경우, ESXi 호스트를 구성하여 가상 시스템 디스크 데이터를 캐시할 수 있습니다. View Storage Accelerator라는 이 기능은 ESXi 호스트의 CBRC(Content Based Read Cache) 기능을 사용합니다. View Storage Accelerator는 여러 가상 시스템이 한꺼번에 시작하거나 바이러스 백신 스캔을 실행할 때 발생할 수 있는 I/O 스톱 중 Horizon 7 성능을 향상시킵니다. 이 기능은 관리자 또는 사용자가 애플리케이션이나 데이터를 자주 로드하는 경우에도 유용합니다. 스토리지 시스템에서 전체 OS 또는 애플리케이션을 반복해서 읽는 대신, 호스트는 캐시에서 공통 데이터 블록을 읽을 수 있습니다.

부트 스톱 중 IOPS 수가 감소하면 View Storage Accelerator가 스토리지 어레이의 요구를 줄여 주고, 따라서 Horizon 7 배포를 지원하는 스토리지 I/O 대역폭을 덜 사용하게 됩니다.

이 절차에 설명된 대로 Horizon Administrator의 vCenter Server 마법사에서 View Storage Accelerator 설정을 선택하여 ESXi 호스트에서 캐싱을 사용하도록 설정합니다.

View Storage Accelerator가 개별 데스크톱 풀에 대해서도 구성되어 있는지 확인하십시오. 데스크톱 풀에서 작동하도록 하려면 View Storage Accelerator가 vCenter Server와 개별 데스크톱 풀에 사용하도록 설정되어 있어야 합니다.

View Storage Accelerator는 기본적으로 데스크톱 풀에 대해 사용하도록 설정되어 있습니다. 이 기능은 풀을 생성하거나 편집할 때 사용하거나 사용하지 않도록 설정할 수 있습니다. 가장 좋은 접근 방식은 처음 데스크톱 풀을 생성할 때 이 기능을 사용하도록 설정하는 것입니다. 기존 풀을 편집하여 이 기능을 사용하도록 설정하는 경우 연결된 클론이 프로비저닝되기 전에 새 복제본과 다이제스트 디스크를 생성해야 합니다. 새 스냅샷에 풀을 재구성하거나 새 데이터스토어로 풀을 재조정하여 새 복제본을 생성할 수 있습니다. 다이제스트 파일은 전원이 꺼질 때 데스크톱 풀의 가상 시스템에 대해서만 구성될 수 있습니다.

연결된 클론이 포함된 데스크톱 풀과 전체 가상 시스템이 포함된 풀에서 View Storage Accelerator를 사용하도록 설정할 수 있습니다.

기본 NFS 스냅샷 기술(VAAI)은 View Storage Accelerator에 대해 사용하도록 설정된 풀에서 지원되지 않습니다.

View Storage Accelerator는 이제 Horizon 7 복제본 계층화를 사용하는 구성에서 작동할 수 있으며 이 구성에서는 복제본이 연결된 클론이 아닌 개별 데이터스토어에 저장됩니다. View Storage Accelerator와 Horizon 7 복제본 계층화를 함께 사용할 경우 얻을 수 있는 성능 이점은 그리 크지 않지만 별도의 데이터스토어에 복제본을 저장함으로써 특정한 용량 관련 이점을 얻을 수 있습니다. 따라서 이 조합이 테스트 및 지원됩니다.

중요 이 기능을 사용하고자 하며 일부 ESXi 호스트를 공유하는 여러 개의 Horizon 7 포드를 사용하는 경우에는 공유 ESXi 호스트에 있는 모든 풀에 대해 Horizon Storage Accelerator 기능을 사용하도록 설정해야 합니다. 여러 개의 포드에서 설정에 일관성이 없는 경우에는 공유 ESXi 호스트의 가상 시스템에 불안정성이 발생할 수 있습니다.

사전 요구 사항

- vCenter Server 및 ESXi 호스트 버전이 5.1 이상인지 확인하십시오.
ESXi 클러스터에서 모든 호스트의 버전이 5.1 이상인지 확인하십시오.
- vCenter Server에서 vCenter Server 사용자에게 **호스트 > 구성 > 고급 설정** 권한이 할당되었는지 확인합니다.
[vCenter Server](#), [View Composer](#) 및 [인스턴트 클론에 대한 사용자 계정 구성](#)를 참조하십시오.

절차

- 1 Horizon Administrator에서 스토리지 설정 페이지 앞에 나오는 vCenter Server 추가 마법사 페이지를 완료합니다.
 - a **View 구성 > 서버**를 선택합니다.
 - b **vCenter Server** 탭에서 **추가**를 클릭합니다.
 - c vCenter Server 정보, View Composer 설정 및 View Composer 도메인 페이지를 완료합니다.
- 2 스토리지 설정 페이지에서 **View Storage Accelerator 사용** 확인란이 선택되었는지 확인합니다.
이 확인란은 기본적으로 선택되어 있습니다.
- 3 기본 호스트 캐시 크기를 지정합니다.
기본 캐시 크기는 이 vCenter Server 인스턴스에서 관리하는 모든 ESXi 호스트에 적용됩니다.
기본값은 1,024MB입니다. 캐시 크기는 100MB와 2,048MB 사이여야 합니다.

- 4 개별 ESXi 호스트에 다른 캐시 크기를 지정하려면 ESXi 호스트를 선택하고 **캐시 크기 편집**을 클릭하십시오.
 - a 호스트 캐시 대화 상자에서 **기본 호스트 캐시 크기 재정의**를 선택합니다.
 - b 100MB와 2,048MB 사이의 **호스트 캐시 크기**를 입력하고 **확인**을 클릭합니다.
- 5 스토리지 설정 페이지에서 **다음**을 클릭합니다.
- 6 **마침**을 클릭하여 vCenter Server, View Composer 및 스토리지 설정을 Horizon 7에 추가합니다.

다음에 수행할 작업

PCoIP 보안 게이트웨이, 보안 터널 및 클라이언트 연결을 위한 외부 URL을 구성하려면 [Horizon Client 연결 구성](#)을 참조하십시오.

Horizon 7에서 View Storage Accelerator 설정을 완료하려면 데스크톱 풀에 대해 View Storage Accelerator를 구성하십시오. "Horizon 7에서 가상 데스크톱 설정" 문서에서 "데스크톱 풀의 View Storage Accelerator 구성"을 참조하십시오.

vCenter Server 및 View Composer의 동시 작업 수 제한

vCenter Server를 Horizon 7에 추가하거나 vCenter Server 설정을 편집할 때 vCenter Server 및 View Composer에서 수행되는 최대 동시 작업 수를 설정하는 몇 가지 옵션을 구성할 수 있습니다.

이러한 옵션은 vCenter Server 정보 페이지의 고급 설정 패널에서 구성합니다.

표 9-3. vCenter Server 및 View Composer의 동시 작업 수 제한

설정	설명
최대 동시 vCenter 프로비저닝 작업 수	<p>연결 서버가 이 vCenter Server 인스턴스에서 전체 가상 시스템을 프로비저닝 및 삭제할 수 있는 최대 동시 요청 수를 결정합니다.</p> <p>기본값은 20입니다.</p> <p>이 설정은 전체 가상 시스템에만 적용됩니다.</p>
최대 동시 전원 작업 수	<p>이 vCenter Server 인스턴스의 연결 서버가 관리하는 가상 시스템에 대해 수행할 수 있는 최대 동시 전원 작업 수(시작, 종료, 일시 중단 등)를 결정합니다.</p> <p>기본값은 50입니다.</p> <p>이 설정의 값을 계산하는 방법에 대한 지침은 동시 전원 작업 수를 설정하여 원격 데스크톱 로그인 스톱 지원을 참조하십시오.</p> <p>이 설정은 전체 가상 시스템 및 연결된 클론에 적용됩니다.</p>

표 9-3. vCenter Server 및 View Composer의 동시 작업 수 제한 (계속)

설정	설명
최대 동시 View Composer 유지 관리 작업 수	<p>이 View Composer 인스턴스에서 관리하는 연결된 클론에 대해 수행할 수 있는 최대 동시 View Composer 새로 고침, 재구성 및 재조정 작업 수를 결정합니다.</p> <p>기본값은 12입니다.</p> <p>유지 관리 작업을 시작하려면 먼저 활성 세션이 있는 원격 데스크톱을 로그오프해야 합니다. 유지 관리 작업이 시작되는 즉시 사용자를 강제로 로그오프하는 경우 원격 데스크톱에서 로그오프가 필요한 최대 동시 작업 수는 구성된 값의 절반이 됩니다. 예를 들어, 이 설정을 24로 구성하고 강제로 사용자를 로그오프하는 경우 원격 데스크톱에서 로그오프가 필요한 최대 동시 작업 수는 12가 됩니다.</p> <p>이 설정은 연결된 클론에만 적용됩니다.</p>
최대 동시 View Composer 프로비저닝 작업 수	<p>이 View Composer 인스턴스에서 관리하는 연결된 클론에 대해 수행할 수 있는 최대 동시 생성 및 삭제 작업 수를 결정합니다.</p> <p>기본값은 8입니다.</p> <p>이 설정은 연결된 클론에만 적용됩니다.</p>

동시 전원 작업 수를 설정하여 원격 데스크톱 로그인 스톱 지원

최대 동시 전원 작업 수 설정은 vCenter Server 인스턴스의 원격 데스크톱 가상 시스템에서 발생할 수 있는 최대 동시 전원 작업 수를 제어합니다. 이 제한은 기본적으로 50으로 설정됩니다. 이 값을 변경하여 많은 사용자가 동시에 데스크톱에 로그인할 경우 피크 전원 작업 수를 지원할 수 있습니다.

시험 단계를 수행하여 이 설정의 올바른 값을 결정하는 것이 가장 좋습니다. 계획 지침은 "Horizon 7 아키텍처 계획" 문서의 "아키텍처 설계 요소 및 계획 지침"을 참조하십시오.

필요한 동시 전원 작업 수는 데스크톱 전원이 켜지는 피크율과 데스크톱이 켜지고, 부팅되고, 연결할 수 있게 될 때까지 소요되는 시간에 따라 결정됩니다. 일반적으로 권장되는 전원 작업 수 제한은 데스크톱이 시작되는 데 소요되는 총 시간에 피크 전원 가동률을 곱한 값입니다.

예를 들어, 데스크톱이 시작되는데 소요되는 평균 시간은 2~3분입니다. 따라서 동시 전원 작업 수 제한은 피크 전원 가동률의 3배가 되어야 합니다. 기본 설정인 50은 분당 16대의 데스크톱 피크 전원 가동률을 지원할 수 있습니다.

시스템에서 데스크톱이 시작될 때까지 최대 5분 동안 기다립니다. 시작 시간이 더 오래 걸릴 경우 다른 오류가 발생할 수 있습니다. 신중을 기하려면 동시 전원 작업 수 제한을 피크 전원 가동률의 5배로 설정하면 됩니다. 신중하게 접근할 경우 기본값인 50으로 설정하여 분당 10대 데스크톱의 피크 전원 가동률을 지원할 수 있습니다.

로그온과 그에 따른 데스크톱 전원 가동 작업은 보통 특정 시간 동안 정규 분포 방식으로 발생합니다. 전원 가동 작업의 약 40%가 해당 시간의 1/6에 발생하므로 피크 전원 가동 작업이 해당 시간의 중간에 발생한다고 추정하여 피크 전원 가동률의 근사치를 계산할 수 있습니다. 예를 들어, 사용자가 오전 8시에서 오전 9시 사이에 로그인할 경우 시간은 1시간이며 로그온의 40%가 오전 8시 25분과 오전 8시 35분 사이의 10분 동안 발생합니다. 사용자가 2,000명이고 20%의 사용자가 데스크톱 전원을 켜는다면 400개의 데스크톱 전원 가동 작업의 40%가 이 10분 동안 발생합니다. 따라서 피크 전원 가동률은 분당 16대의 데스크톱입니다.

기본 TLS 인증서의 지문 허용

vCenter Server 및 View Composer 인스턴스를 Horizon 7에 추가할 때 vCenter Server 및 View Composer 인스턴스에 사용되는 TLS 인증서가 유효하고 연결 서버에서 이 인증서를 신뢰하는지 확인해야 합니다. vCenter Server 및 View Composer에 설치된 기본 인증서가 있는 경우 이러한 인증서의 지문을 허용할지 결정해야 합니다.

vCenter Server 또는 View Composer 인스턴스가 CA에서 서명한 인증서로 구성되어 있고 연결 서버가 루트 인증서를 신뢰하는 경우 인증서 지문을 허용하지 않아도 됩니다. 따라서 어떠한 작업도 필요하지 않습니다.

기본 인증서를 CA에서 서명한 인증서로 대체하려 하지만 연결 서버가 루트 인증서를 신뢰하지 않는 경우 인증서 지문을 허용할지 결정해야 합니다. 지문은 인증서의 암호화 해시입니다. 지문은 제시된 인증서가 이전에 허용된 인증서 등의 다른 인증서와 동일한지를 빠르게 결정하는 데 사용됩니다.

참고 동일한 Windows Server 호스트에 vCenter Server 및 View Composer를 설치하는 경우 동일한 TLS 인증서를 사용할 수 있지만 각 구성 요소의 인증서를 별도로 구성해야 합니다.

TLS 인증서를 구성하는 방법에 대한 자세한 내용은 [장 8 Horizon 7 서버를 위한 TLS 인증서 구성](#)을 참조하십시오.

먼저 vCenter Server 추가 마법사를 사용해 Horizon Administrator에서 vCenter Server와 View Composer를 추가하십시오. 인증서를 신뢰할 수 없어 지문을 허용하지 않을 경우 vCenter Server와 View Composer를 추가할 수 없습니다.

이러한 서버를 추가한 후에는 vCenter Server 편집 대화상자에서 서버를 재구성할 수 있습니다.

참고 이전 릴리스 및 vCenter Server에서 업그레이드하거나, View Composer 인증서를 신뢰할 수 없거나, 신뢰할 수 있는 인증서를 신뢰할 수 없는 인증서로 바꿀 경우에도 인증서 지문을 허용해야 합니다.

Horizon Administrator 대시보드에서 vCenter Server 또는 View Composer 아이콘이 빨간색으로 바뀌고 [잘못된 인증서가 검색됨] 대화상자가 나타납니다. Horizon Administrator에서 **View 구성 > 서버**를 클릭하고 View Composer 서비스와 연결된 vCenter Server 항목을 편집합니다. 그런 다음 vCenter Server 설정에서 **편집**을 클릭하고 지시에 따라 자체 서명된 인증서를 수락합니다.

마찬가지로 Horizon Administrator에서 연결 서버 인스턴스에 사용할 SAML 인증자를 구성할 수 있습니다. SAML 서버 인증서가 연결 서버에 의해 신뢰되지 않을 경우 인증서 지문을 허용할지 결정해야 합니다. 지문을 허용하지 않으면 Horizon 7에서 SAML 인증자를 구성할 수 없습니다. SAML 인증자가 구성되면 연결 서버 편집 대화 상자에서 인증자를 재구성할 수 있습니다.

절차

- 1 Horizon Administrator에 [잘못된 인증서가 검색됨] 대화상자가 표시되면 **인증서 보기**를 클릭합니다.
- 2 인증서 정보 창에서 인증서 지문을 확인합니다.

- 3 vCenter Server 또는 View Composer 인스턴스에 대해 구성된 인증서 지문을 확인합니다.
 - a vCenter Server 또는 View Composer 호스트에서 MMC 스냅인을 시작하고 Windows 인증서 저장소를 엽니다.
 - b vCenter Server 또는 View Composer 인증서로 이동합니다.
 - c 인증서 세부 정보 탭을 클릭하여 인증서 지문을 표시합니다.
 마찬가지로 SAML 인증자의 인증서 지문을 확인합니다. 해당하는 경우 SAML 인증자 호스트에서 앞의 단계를 수행하십시오.
- 4 인증서 정보 창의 지문이 vCenter Server 또는 View Composer 인스턴스의 지문과 일치하는지 확인합니다.

마찬가지로 SAML 인증자의 지문과 일치하는지 확인합니다.
- 5 인증서 지문을 허용할지 결정합니다.

옵션	설명
지문이 일치합니다.	수락을 클릭하여 기본 인증서를 사용합니다.
지문이 일치하지 않습니다.	거부를 클릭합니다. 인증서 불일치 문제를 해결합니다. 예를 들어 vCenter Server 또는 View Composer의 IP 주소를 잘못 입력했을 수 있습니다.

Horizon Client 연결 구성

클라이언트 끝점은 보안 연결을 통해 연결 서버 또는 보안 서버 호스트와 통신합니다.

사용자가 Horizon Client에 도메인 이름을 제공하면 사용자 인증과 원격 데스크톱 및 애플리케이션 선택에 사용되는 초기 클라이언트 연결이 HTTPS를 통해 생성됩니다. 네트워크 환경에 방화벽과 로드 밸런싱 소프트웨어를 제대로 구성한 경우 이 요청이 연결 서버 또는 보안 서버 호스트에 전달됩니다. 이 연결로 사용자는 인증을 받고 데스크톱 또는 애플리케이션을 선택하지만 원격 데스크톱 또는 애플리케이션에는 아직 연결되지 않은 상태입니다.

사용자가 원격 데스크톱 및 애플리케이션에 연결할 때 기본적으로 클라이언트에서 연결 서버 또는 보안 서버 호스트에 대한 두 번째 연결을 생성합니다. 이 연결은 HTTPS를 통해 RDP 및 다른 데이터를 전송하는 보안 터널을 제공하므로 터널 연결이라고 부릅니다.

사용자가 PCoIP 디스플레이 프로토콜로 원격 데스크톱 및 애플리케이션에 연결할 때 클라이언트는 연결 서버 또는 보안 서버 호스트에서 PCoIP 보안 게이트웨이에 대한 추가 연결을 생성할 수 있습니다. PCoIP 보안 게이트웨이는 인증된 사용자만 PCoIP를 통해 원격 데스크톱 및 애플리케이션과 통신하도록 허용합니다.

VMware Blast 디스플레이 프로토콜을 사용하여 원격 데스크톱 및 애플리케이션에 연결하는 사용자와, HTML Access를 사용하여 원격 데스크톱에 연결하는 외부 사용자에게 보안 연결을 제공할 수도 있습니다. Blast 보안 게이트웨이는 인증된 사용자만 원격 데스크톱과 통신하도록 허용합니다.

사용하고 있는 클라이언트 디바이스의 유형에 따라 USB 리디렉션 데이터 등의 다른 트래픽을 클라이언트 디바이스로 전송하기 위해 추가 채널이 생성됩니다. 이러한 데이터 채널은 보안 터널이 사용하도록 설정된 경우 보안 터널을 통해 트래픽을 라우팅합니다.

보안 터널 및 보안 게이트웨이가 사용되지 않도록 설정된 경우 연결 서버 또는 보안 서버 호스트를 우회하고 클라이언트 디바이스와 원격 시스템 간에 데스크톱 및 애플리케이션 세션이 직접 설정됩니다. 이러한 연결 유형을 직접 연결이라 부릅니다.

연결 서버가 더 이상 실행되지 않아도 직접 연결을 사용하는 데스크톱 및 애플리케이션 세션은 연결 상태를 유지합니다.

일반적으로 WAN을 통해 보안 서버 또는 연결 서버 호스트에 연결하는 외부 클라이언트에 보안 연결을 제공하려면 보안 터널과 PCoIP 보안 게이트웨이는 물론이고, Blast 보안 게이트웨이까지 사용하도록 설정해야 합니다. 보안 터널과 보안 게이트웨이를 사용하지 않도록 설정하면 LAN으로 연결된 내부 클라이언트가 원격 데스크톱 및 애플리케이션에 대한 직접 연결을 설정하도록 할 수 있습니다.

보안 터널과 보안 게이트웨이 중 하나만 사용하도록 설정하는 경우 사용하고 있는 클라이언트 유형에 따라 세션에서 일부 트래픽은 직접 연결을 통해 보내고 다른 일부 트래픽은 연결 서버 또는 보안 서버 호스트를 통해 보낼 수 있습니다.

SSL은 연결 서버 및 보안 서버 호스트에 대한 모든 클라이언트 연결에 필요합니다.

PCoIP 보안 게이트웨이 및 보안 터널 연결 구성

Horizon Administrator를 사용해 보안 터널 및 PCoIP 보안 게이트웨이 사용을 구성합니다. 이들 구성 요소를 사용하면 인증된 사용자만 원격 데스크톱 및 애플리케이션과 통신할 수 있도록 할 수 있습니다.

PCoIP 디스플레이 프로토콜을 사용하는 클라이언트는 PCoIP 보안 게이트웨이를 사용할 수 있습니다. RDP 디스플레이 프로토콜을 사용하는 클라이언트는 보안 터널을 사용할 수 있습니다.

Blast 보안 게이트웨이 구성에 대한 자세한 내용은 [Blast 보안 게이트웨이 구성](#)을 참조하십시오.

중요 외부 클라이언트에 보안 연결을 제공하는 기존 네트워크 구성에는 보안 서버가 포함되어 있습니다. 보안 서버의 보안 터널 및 PCoIP 보안 게이트웨이를 사용 또는 사용하지 않도록 설정하려면 보안 서버에 연결되어 있는 연결 서버 인스턴스를 편집해야 합니다.

외부 클라이언트를 연결 서버 호스트에 직접 연결하는 네트워크 구성에서 Horizon Administrator의 연결 서버 인스턴스를 변경하여 보안 터널과 PCoIP 보안 게이트웨이를 사용하거나 사용하지 않도록 설정할 수 있습니다.

사전 요구 사항

- PCoIP 보안 게이트웨이를 사용하도록 설정할 경우, 연결 서버 인스턴스 및 연결된 보안 서버가 View 4.6 이상인지 확인하십시오.
- PCoIP 보안 게이트웨이를 이미 사용하도록 설정한 연결 서버 인스턴스와 보안 서버를 연결할 경우, 보안 서버가 View 4.6 이상인지 확인하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 연결 서버 패널에서 연결 서버 인스턴스를 선택하고 **편집**을 클릭합니다.

3 보안 터널 사용을 구성하십시오.

옵션	설명
보안 터널 사용 안 함	보안 터널을 사용하여 시스템에 연결을 선택 해제합니다.
보안 터널 사용	보안 터널을 사용하여 시스템에 연결을 선택합니다.

기본적으로 보안 터널을 사용하도록 설정되어 있습니다.

4 PCoIP 보안 게이트웨이 사용을 구성하십시오.

옵션	설명
PCoIP 보안 게이트웨이 사용	시스템에 대한 PCoIP 연결에 PCoIP 보안 게이트웨이 사용을 선택합니다.
PCoIP 보안 게이트웨이 사용 안 함	시스템에 대한 PCoIP 연결에 PCoIP 보안 게이트웨이 사용을 선택 해제합니다.

기본적으로 PCoIP 보안 게이트웨이를 사용하지 않도록 설정되어 있습니다.

5 변경 사항을 저장하려면 **확인**을 클릭합니다.

Blast 보안 게이트웨이 구성

Horizon Administrator에서 Blast 보안 게이트웨이의 사용을 구성하면 HTML Access를 통해 또는 VMware Blast 디스플레이 프로토콜을 사용하는 클라이언트 연결을 통해 원격 데스크톱 및 애플리케이션에 대한 보안 액세스를 제공할 수 있습니다.

Blast Secure Gateway에는 속도가 변하고 패킷이 손실되는 등의 네트워크 상태에 맞게 동적으로 조정되는 BEAT(Blast Extreme Adaptive Transport) 네트워킹이 포함됩니다.

- Blast 보안 게이트웨이는 Unified Access Gateway 장치에서 실행될 때만 BEAT 네트워킹을 지원합니다.
- Unified Access Gateway 장치 버전 3.3 이상에 연결할 경우 IPv4를 사용하는 Horizon Client 및 IPv6를 사용하는 Horizon Client는 TCP 포트 8443 및 UDP 포트 8443(BEAT용)에서 동시에 처리될 수 있습니다.
- 일반적인 네트워크 상태를 사용하는 Horizon Client는 연결 서버(BSG 사용 안 함), 보안 서버(BSG 사용 안 함) 또는 2.8 이후 버전의 Unified Access Gateway 장치에 연결해야 합니다. Horizon Client가 일반적인 네트워크 상태를 사용하여 연결 서버(BSG 사용), 보안 서버(BSG 사용) 또는 2.8 이전 버전의 Unified Access Gateway 장치에 연결하는 경우 클라이언트는 네트워크 상태를 자동으로 감지하고 TCP 네트워킹으로 변경합니다.
- 양호하지 않은 네트워크 상태를 사용하는 Horizon Client는 2.9 이상 버전의 Unified Access Gateway 장치(UDP 터널 서버 사용)에 연결해야 합니다. Horizon Client가 양호하지 않은 네트워크 상태를 사용하여 연결 서버(BSG 사용), 보안 서버(BSG 사용) 또는 2.8 이전 버전의 Unified Access Gateway 장치에 연결하는 경우 클라이언트는 네트워크 상태를 자동으로 감지하고 TCP 네트워킹으로 변경합니다.

- Horizon Client가 암호하지 않은 네트워크 상태를 사용하여 연결 서버(BSG 사용 안 함), 보안 서버(BSG 사용 안 함) 또는 버전 2.9 이상의 Unified Access Gateway 장치(UDP 터널 서버 사용 안 함)나 2.8 버전의 Unified Access Gateway 장치에 연결하는 경우 클라이언트는 네트워크 상태를 자동으로 감지하고 일반적인 네트워크 상태로 변경합니다.

자세한 내용은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>에서 Horizon Client 설명서를 참조하십시오.

참고 보안 서버 대신 Unified Access Gateway 장치를 사용하여 Horizon 7 서버 및 데스크톱에 안전하게 외부에서 액세스할 수 있습니다. Unified Access Gateway 장치를 사용하는 경우에는 연결 서버 인스턴스에서 보안 게이트웨이를 사용하지 않도록 설정하고 Unified Access Gateway 장치에서 이러한 게이트웨이를 사용하도록 설정할 수 있습니다. 자세한 내용은 “Unified Access Gateway 배포 및 구성”의 내용을 참조하십시오.

Blast 보안 게이트웨이가 사용되도록 설정되어 있지 않은 경우에는 클라이언트 디바이스 및 클라이언트 웹 브라우저에서 Blast 보안 게이트웨이를 우회하고 VMware Blast Extreme 프로토콜을 사용하여 원격 데스크톱 가상 시스템 및 애플리케이션에 직접 연결합니다.

중요 외부 사용자에게 보안 연결을 제공하는 일반 네트워크 구성에는 보안 서버가 포함되어 있습니다. 보안 서버의 Blast 보안 게이트웨이를 사용 또는 사용하지 않도록 설정하려면 보안 서버에 연결되어 있는 연결 서버 인스턴스를 편집해야 합니다. 외부 사용자가 연결 서버 호스트에 직접 연결할 경우 연결 서버 인스턴스를 편집하여 Blast 보안 게이트웨이를 사용 또는 사용하지 않도록 설정하십시오.

사전 요구 사항

사용자가 VMware Identity Manager를 통해 원격 데스크톱을 선택할 경우 VMware Identity Manager가 설치되어 있고 연결 서버에서 사용하도록 구성되어 있으며 연결 서버가 SAML 2.0 인증 서버와 연결되어 있는지 확인하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 연결 서버 인스턴스를 선택하고 **편집**을 클릭합니다.
- 3 Blast 보안 게이트웨이 사용을 구성하십시오.

옵션	설명
Blast 보안 게이트웨이 사용	시스템에 Blast 연결용 Blast 보안 게이트웨이 사용 선택
HTML Access에 대해 Blast 보안 게이트웨이 사용	시스템에 대한 HTML Access Blast 연결에만 Blast 보안 게이트웨이 사용 선택
Blast 보안 게이트웨이 사용 안 함	Blast 보안 게이트웨이 사용 안 함 선택

기본적으로 Blast 보안 게이트웨이를 사용하도록 설정되어 있습니다.

- 4 변경 사항을 저장하려면 **확인**을 클릭합니다.

보안 게이트웨이 및 터널 연결용 외부 URL 구성

보안 터널을 사용하려면 클라이언트 시스템에서 클라이언트가 연결 서버 또는 보안 서버 호스트에 연결하는 데 사용하는 IP 주소를 확인할 수 있는 FQDN(정규화된 도메인 이름) 또는 IP 주소에 대한 액세스를 보유하고 있어야 합니다.

PCoIP 보안 게이트웨이를 사용하기 위해 클라이언트는 URL을 이용하여 연결 서버 또는 보안 서버 호스트에 연결합니다. IPv4 환경의 경우 URL은 호스트를 해당 IP 주소로 식별해야 합니다. IPv6 환경의 경우 URL은 호스트를 해당 IP 주소나 FQDN으로 식별할 수 있습니다.

Blast 보안 게이트웨이를 사용하려면 사용자의 끝점 디바이스가 FQDN에 액세스하여 사용자의 웹 브라우저 또는 컴퓨터가 연결 서버 또는 보안 서버 호스트에 도달할 수 있는 IP 주소를 확인할 수 있어야 합니다.

외부 위치에서 터널 연결 사용

기본적으로 연결 서버 또는 보안 서버 호스트는 동일 네트워크에 위치한 터널 클라이언트로만 연결할 수 있으므로 요청한 호스트를 찾을 수 있습니다.

많은 조직의 경우, 특정 IP 주소 또는 클라이언트가 확인할 수 있는 도메인 이름 및 특정 포트를 사용해 사용자가 외부 위치에서 연결할 것을 요구하고 있습니다. 이 정보는 연결 서버 또는 보안 서버 호스트의 실제 주소 및 포트 번호와 유사하거나 다를 수 있습니다. 이 정보는 클라이언트 시스템에 URL 형태로 제공됩니다. 예:

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://10.20.30.40:443`

Horizon 7에서 이러한 주소를 사용하려면 호스트의 FQDN이 아닌 외부 URL을 반환하도록 연결 서버 또는 보안 서버 호스트를 구성해야 합니다.

외부 URL 구성

둘 이상의 외부 URL을 구성합니다. 첫 번째는 클라이언트 시스템에서 터널 연결할 수 있는 URL입니다. 두 번째는 PCoIP를 사용하는 클라이언트가 PCoIP 보안 게이트웨이를 통해 보안 연결할 수 있는 URL입니다. IPv4 환경의 경우 URL은 호스트를 해당 IP 주소로 식별해야 합니다. IPv6 환경의 경우 URL은 호스트를 해당 IP 주소나 FQDN으로 식별할 수 있습니다. 클라이언트는 URL을 통해 외부 위치에서도 연결할 수 있습니다.

세 번째는 사용자가 클라이언트 디바이스나 웹 브라우저에서 Blast 보안 게이트웨이를 통해 보안 연결할 수 있는 URL입니다.

네트워크 구성에 보안 서버가 포함된 경우 보안 서버용 외부 URL을 제공하십시오. 보안 서버에 연결되는 연결 서버 인스턴스에는 외부 URL이 필요하지 않습니다.

외부 URL을 구성하는 프로세스는 연결 서버 인스턴스 및 보안 서버와 다릅니다.

- 연결 서버 인스턴스의 경우 Horizon Administrator의 연결 서버 설정을 편집하여 외부 URL을 설정합니다.

- 보안 서버의 경우 연결 서버 설치 프로그램을 실행할 때 외부 URL을 설정합니다. Horizon Administrator를 사용해 보안 서버용 외부 URL을 수정할 수 있습니다.

연결 서버 인스턴스의 외부 URL 설정

Horizon Administrator를 사용하여 연결 서버 인스턴스의 외부 URL을 구성합니다.

보안 터널 외부 URL, PCoIP 외부 URL 및 Blast 외부 URL은 클라이언트 시스템이 이 연결 서버 인스턴스에 도달하기 위해 사용하는 주소여야 합니다.

사전 요구 사항

- 보안 터널 연결과 PCoIP 보안 게이트웨이가 연결 서버 인스턴스에서 사용하도록 설정되어 있는지 확인하십시오. [PCoIP 보안 게이트웨이 및 보안 터널 연결 구성](#)의 내용을 참조하십시오.
- Blast 외부 URL을 설정하려면 Blast 보안 게이트웨이가 연결 서버 인스턴스에서 사용하도록 설정되어 있는지 확인하십시오. [Blast 보안 게이트웨이 구성](#)의 내용을 참조하십시오.

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 **PCoIP 외부 URL** 텍스트 상자에 PCoIP 보안 게이트웨이 외부 URL을 입력합니다.

IPv4 환경에서는 IP 주소와 포트 번호 4172를 사용하여 PCoIP 외부 URL을 지정합니다. IPv6 환경에서는 IP 주소 또는 정규화된 도메인 이름과 함께 포트 번호 4172를 지정할 수 있습니다. 두 경우 모두 프로토콜 이름은 포함하지 않습니다.

IPv4 환경의 예: `10.20.30.40:4172`

클라이언트는 이 URL을 사용하여 보안 서버에 액세스할 수 있어야 합니다.

- 5 **Blast 외부 URL** 텍스트 상자에 Blast 보안 게이트웨이 외부 URL을 입력하십시오.

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

예: `https://myserver.example.com:8443`

기본적으로 URL에는 보안 터널 외부 URL의 FQDN과 기본 포트 번호 8443이 포함됩니다. URL에는 클라이언트 시스템이 이 연결 서버 호스트에 도달하기 위해 사용할 수 있는 FQDN과 포트 번호가 포함되어야 합니다.

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

보안 서버의 외부 URL 수정

Horizon Administrator를 사용하여 보안 서버의 외부 URL을 수정합니다.

연결 서버 설치 프로그램에서 보안 서버를 설치할 때 이러한 외부 URL을 처음으로 구성합니다.

보안 터널 외부 URL, PCoIP 외부 URL 및 Blast 외부 URL은 클라이언트 시스템에서 이 보안 서버에 도달하기 위해 사용하는 주소여야 합니다.

사전 요구 사항

- 보안 터널 연결과 PCoIP 보안 게이트웨이가 이 보안 서버와 연결된 연결 서버 인스턴스에서 사용하도록 설정되어 있는지 확인하십시오. [PCoIP 보안 게이트웨이 및 보안 터널 연결 구성](#)의 내용을 참조하십시오.
- Blast 외부 URL을 설정하려면 Blast 보안 게이트웨이가 이 보안 서버와 연결된 연결 서버 인스턴스에서 사용하도록 설정되어 있는지 확인하십시오. [Blast 보안 게이트웨이 구성](#)의 내용을 참조하십시오.

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 **PCoIP 외부 URL** 텍스트 상자에 PCoIP 보안 게이트웨이 외부 URL을 입력합니다.

IPv4 환경에서는 IP 주소와 포트 번호 4172를 사용하여 PCoIP 외부 URL을 지정합니다. IPv6 환경에서는 IP 주소 또는 도메인 이름과 함께 포트 번호 4172를 지정할 수 있습니다. 두 경우 모두 프로토콜 이름은 포함하지 않습니다.

IPv4 환경의 예: `10.20.30.40:4172`

클라이언트는 이 URL을 사용하여 보안 서버에 액세스할 수 있어야 합니다.

- 5 **Blast 외부 URL** 텍스트 상자에 Blast 보안 게이트웨이 외부 URL을 입력하십시오.

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

예: `https://myserver.example.com:8443`

기본적으로 URL에는 보안 터널 외부 URL의 FQDN과 기본 포트 번호인 8443이 포함되어야 합니다. URL에는 클라이언트 시스템이 이 보안 서버에 도달하는 데 사용하는 FQDN 및 포트 번호가 포함되어야 합니다.

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

- 7 변경 사항을 저장하려면 **확인**을 클릭합니다.

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

Horizon 연결 서버가 주소 정보를 반환할 때 DNS 이름을 기본 설정으로 사용

기본적으로 Horizon 연결 서버는 데스크톱 시스템 및 RDS 호스트의 주소를 클라이언트와 게이트웨이에 보낼 때 IP 주소를 기본 설정으로 사용합니다. 이 기본 동작은 DNS 이름을 기본 설정으로 사용하도록 Horizon 연결 서버에 지시하는 Horizon 7 LDAP 특성을 사용하여 변경할 수 있습니다. 특정 환경에서는 연결 서버가 클라이언트와 게이트웨이에 DNS 이름을 반환하도록 하여 네트워크 인프라를 보다 유연하게 설계할 수 있습니다.

참고 이 Horizon 7 LDAP 특성은 Horizon 6.0.x 및 이전 릴리스에서 Connect using DNS Name 그룹 정책 설정을 통해 제공되던 데스크톱별 기능을 대체합니다.

Horizon 7 LDAP 특성은 Windows용 Horizon Client 3.3 이상, HTML Access 3.5 이상을 실행하는 클라이언트 및 연결 서버 인스턴스(보안 서버 아님)의 보안 게이트웨이에 영향을 줍니다.

사전 요구 사항

사용하고 있는 Windows Server 운영 체제 버전에서 ADSI 편집 유틸리티를 사용하는 방법은 Microsoft TechNet 웹 사이트를 참조하십시오.

절차

- 1 연결 서버 컴퓨터에서 ADSI 편집 유틸리티를 시작합니다.
- 2 콘솔 트리에서 **연결**을 선택합니다.
- 3 **고유 이름 또는 명명 컨텍스트를 선택하거나 입력합니다** 텍스트 상자에 고유 이름 **DC=vdi**, **DC=vmware**, **DC=int**를 입력합니다.
- 4 **도메인 또는 서버를 선택하거나 입력합니다** 텍스트 상자에서 **localhost:389** 또는 연결 서버 컴퓨터의 FQDN(정규화된 도메인 이름)과 포트 389를 차례로 선택하거나 입력합니다.

예: `localhost:389` 또는 `mycomputer.mydomain.com:389`

5 CN=Common, OU=Global, OU=Properties 개체에서 **pae-PreferDNS** 특성 값을 1로 설정합니다.

이 특성을 1로 설정할 경우, DNS 이름을 사용할 수 있고 수신자가 이름 확인 기능을 지원할 경우 연결 서버는 DNS 이름을 반환합니다. 그렇지 않고 사용자의 환경에 적합한 IP 주소 유형(IPv4 또는 IPv6)이 있으면 연결 서버가 IP 주소를 반환합니다.

이 특성을 설정하지 않거나 0으로 설정할 경우, 올바른 유형의 IP 주소를 사용할 수 있으면 연결 서버가 IP 주소를 반환합니다. 그렇지 않으면 IP 주소 호환성 오류가 반환됩니다.

로드 밸런서를 통한 HTML Access 허용

로드 밸런서나 로드 밸런싱된 게이트웨이 바로 뒤에 있는 연결 서버 인스턴스 및 보안 서버는 사용자가 HTML Access를 사용할 때 로드 밸런서에 연결하는 브라우저의 주소를 알아야 합니다.

게이트웨이 바로 뒤에 있는 연결 서버 인스턴스 및 보안 서버에 대해서는 [게이트웨이를 통한 HTML Access 허용](#)에 설명된 절차를 수행합니다.

로드 밸런서나 로드 밸런싱된 게이트웨이 뒤에 있는 각 Horizon 7 서버에 대해 이 절차를 수행해야 합니다.

절차

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

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\locked.properties`

- 2 `balancedHost` 속성을 추가하고 로드 밸런서의 주소로 설정합니다.

예를 들어, 사용자가 브라우저에 `https://view.example.com`을 입력하여 로드 밸런싱된 Horizon 7 서버에 연결하는 경우에는 `locked.properties` 파일에 `balancedHost=view.example.com`을 추가합니다.

- 3 `locked.properties` 파일을 저장합니다.

- 4 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

게이트웨이를 통한 HTML Access 허용

Access Point와 같이 게이트웨이 바로 뒤에 있는 보안 서버와 연결 서버 인스턴스는 사용자가 HTML Access를 사용할 때 게이트웨이에 연결하는 브라우저의 주소를 알아야 합니다.

로드 밸런서나 로드 밸런싱된 게이트웨이 뒤에 있는 연결 서버 인스턴스 및 보안 서버에 대해서는 [로드 밸런서를 통한 HTML Access 허용](#)에 설명된 절차를 수행합니다.

게이트웨이 뒤에 있는 각 Horizon 7 서버에 대해 이 절차를 수행해야 합니다.

절차

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

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\locked.properties`

2 portalHost 속성을 추가하고 게이트웨이의 주소로 설정합니다.

예를 들어, 게이트웨이를 통해 Horizon 7에 액세스할 때 브라우저에서 사용하는 주소가 `https://view-gateway.example.com`인 경우에는 `locked.properties` 파일에 `portalHost=view-gateway.example.com`을 추가합니다.

연결 서버 인스턴스나 보안 서버가 여러 게이트웨이 뒤에 있는 경우에는 `portalHost` 속성 뒤에 번호를 추가하여 각 게이트웨이를 지정할 수 있습니다. 예:

```
portalHost.1=view-gateway-1.example.com
portalHost.2=view-gateway-2.example.com
```

한 게이트웨이 시스템이 두 개 이상의 이름으로 알려진 경우에도 여러 개의 `portalHost` 속성을 지정해야 합니다.

3 locked.properties 파일을 저장합니다.

4 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

Horizon 7 서비스의 기본 포트 교체

설치 도중 기본적으로 특정 네트워크 포트에서 수신하도록 View 서비스가 설정됩니다. 특정 조직에서는 조직 정책을 준수하거나 경합을 피하기 위해 이러한 포트를 변경해야 합니다. 연결 서버, 보안 서버, PCoIP 보안 게이트웨이 및 View Composer 서비스에 사용되는 기본 포트를 변경할 수 있습니다.

포트 변경은 선택 설정 작업입니다. 배포에 포트 변경이 필요하지 않을 경우 기본 포트를 사용하십시오.

Horizon 7 서버에서 사용되는 기본 TCP 및 UDP 포트 목록을 보려면 "Horizon 7 보안" 문서를 참조하십시오.

Horizon 연결 서버 인스턴스 및 보안 서버의 기본 HTTP 포트 또는 NIC 교체

서버 컴퓨터의 `locked.properties` 파일을 편집하여 연결 서버 인스턴스 또는 보안 서버의 기본 HTTP 포트 또는 NIC를 교체할 수 있습니다. 조직에서 조직 정책을 준수하거나 경합을 피하기 위해 이러한 작업을 수행하도록 요구할 수 있습니다.

기본 SSL 포트는 443입니다. 기본 비 SSL 포트는 80입니다.

이 절차에서 포트를 변경해도 보안 터널 외부 URL에 지정된 포트는 변경되지 않습니다. 네트워크 구성에 따라 보안 터널 외부 URL 포트도 변경해야 할 수 있습니다.

서버 컴퓨터에 여러 개의 NIC가 있는 경우 기본적으로 컴퓨터가 모든 NIC에서 수신합니다. NIC를 하나 선택하고 해당 NIC에 바인딩되는 IP 주소를 지정하여 구성된 포트에서 수신할 수 있습니다.

설치 도중 Horizon 7가 필요한 기본 포트를 열도록 Windows 방화벽을 구성합니다. 포트 번호 또는 수신 NIC를 변경하는 경우 업데이트된 포트를 열도록 Windows 방화벽을 수동으로 재구성해야 클라이언트 디바이스가 서버에 연결할 수 있습니다.

SSL 포트 번호를 변경할 경우 HTTP 리디렉션이 계속 작동해야 한다면 HTTP 리디렉션의 포트 번호도 변경해야 합니다. [연결 서버에 대한 HTTP 리디렉션 포트 번호 변경](#)을 참조하십시오.

사전 요구 사항

이 절차에서 포트를 변경한 후에 연결 서버 인스턴스 또는 보안 서버의 외부 URL에 지정된 포트가 계속해서 유효한지 확인하십시오.

절차

- 1 연결 서버 또는 보안 서버 컴퓨터의 SSL 게이트웨이 구성 폴더에 `locked.properties` 파일을 생성 또는 편집합니다.

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\locked.properties`
`locked.properties` 파일의 속성은 대/소문자를 구분합니다.

- 2 `serverPort` 또는 `serverPortNonSsl` 속성이나 두 속성 모두를 `locked.properties` 파일에 추가합니다.

예:

```
serverPort=4443
serverPortNonSsl=8080
```

- 3 (선택 사항) 서버 컴퓨터에 여러 개의 NIC가 있는 경우 구성된 포트에서 수신할 NIC를 하나 선택합니다.

`serverHost` 및 `serverHostNonSsl` 속성을 추가하여 지정된 NIC에 바인딩되는 IP 주소를 지정합니다.

예:

```
serverHost=10.20.30.40
serverHostNonSsl=10.20.30.40
```

일반적으로 SSL과 비 SSL 수신기는 동일한 NIC를 사용하도록 구성되어 있습니다. 그러나 `serverProtocol=http` 속성을 사용하여 클라이언트 연결의 SSL 부하를 분산시키면 `serverHost` 속성을 개별 NIC에 설정하여 Horizon Administrator를 실행하는 데 사용되는 시스템에 SSL 연결을 제공할 수 있습니다.

동일한 NIC를 사용하도록 SSL 및 비 SSL 연결을 구성하려면 SSL 및 비 SSL 포트가 동일하지 않아야 합니다.

- 4 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

다음에 수행할 작업

필요한 경우 업데이트된 포트를 열도록 Windows 방화벽을 수동으로 구성하십시오.

Horizon 연결 서버 인스턴스 및 보안 서버의 PCoIP 보안 게이트웨이의 기본 포트 또는 NIC 교체

연결 서버 인스턴스 또는 보안 서버에서 실행되는 PCoIP 보안 게이트웨이 서비스의 기본 포트 또는 NIC를 교체할 수 있습니다. 조직에서 조직 정책을 준수하거나 경합을 피하기 위해 이러한 작업을 수행하도록 요구할 수 있습니다.

클라이언트 연결 TCP 및 UDP 연결의 경우 기본적으로 PCoIP 보안 게이트웨이가 포트 4172에서 수신합니다. 원격 데스크톱에 대한 UDP 연결의 경우 기본적으로 PCoIP 보안 게이트웨이가 포트 55000에서 수신합니다.

이 절차에서 포트를 변경해도 PCoIP 외부 URL에 지정된 포트는 변경되지 않습니다. 네트워크 구성에 따라 PCoIP 외부 URL 포트도 변경해야 할 수 있습니다.

PCoIP 보안 게이트웨이가 실행 중인 컴퓨터에 여러 개의 NIC가 있는 경우 기본적으로 컴퓨터가 모든 NIC에서 수신합니다. NIC를 하나 선택하고 해당 NIC에 바인딩되는 IP 주소를 지정하여 구성된 포트에서 수신할 수 있습니다.

사전 요구 사항

이 절차에서 포트를 변경한 후에 연결 서버 인스턴스 또는 보안 서버의 PCoIP 외부 URL에 지정된 포트가 계속해서 유효한지 확인하십시오.

절차

- 1 연결 서버 또는 PCoIP 보안 게이트웨이가 실행 중인 보안 서버 컴퓨터에서 Windows 레지스트리 편집기를 시작합니다.
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway 레지스트리 키로 이동합니다.
- 3 이 레지스트리 키에서 업데이트된 포트 번호와 함께 다음 문자열(REG_SZ) 값 중 하나 이상을 추가합니다.

예:

```
ExternalTCPPort "44172"
ExternalUDPPort "44172"
InternalUDPPort "55111"
```

- 4 (선택 사항) PCoIP 보안 게이트웨이가 실행 중인 컴퓨터에 여러 개의 NIC가 있는 경우 구성된 포트에서 수신할 NIC를 하나 선택하십시오.

동일한 레지스트리 키에서 다음 문자열(REG_SZ) 값을 추가하여 지정된 NIC에 바인딩되는 IP 주소를 지정합니다.

예:

```
ExternalBindIP "10.20.30.40"
InternalBindIP "172.16.17.18"
```

동일한 NIC를 사용하도록 외부 및 내부 연결을 구성하려면 외부 및 내부 UDP 포트가 동일하지 않아야 합니다.

- 5 변경 내용을 적용하려면 VMware Horizon View PCoIP 보안 게이트웨이 서비스를 다시 시작합니다.

연결 서버 인스턴스 및 보안 서버에서 PCoIP 보안 게이트웨이의 기본 제어 포트 교체

연결 서버 인스턴스 또는 보안 서버에서 실행되는 PCoIP 보안 게이트웨이(PSG) 서비스를 제어하는 기본 포트를 교체할 수 있습니다. 포트 경합을 방지하기 위해 이 작업을 수행해야 할 수 있습니다.

PCoIP 보안 게이트웨이는 기본적으로 로컬 TCP 포트 50060에서 제어 연결을 수신 대기합니다.

절차

- 1 PCoIP 보안 게이트가 실행 중인 연결 서버 또는 보안 서버 컴퓨터에서 SSL 게이트웨이 구성 폴더의 `locked.properties` 파일을 생성하거나 편집합니다.

예: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
`locked.properties` 파일의 속성은 대/소문자를 구분합니다.

- 2 `psgControlPort` 속성을 `locked.properties` 파일에 추가합니다.

예:

```
psgControlPort=52060
```

- 3 동일한 시스템에서 Windows 레지스트리 편집기를 시작합니다.
- 4 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` 레지스트리 키로 이동합니다.
- 5 이 레지스트리 키에서 업데이트된 포트 번호로 다음 문자열(REG_SZ) 값을 추가합니다.

예:

```
TCPControlPort "52060"
```

참고 `TCPControlPort`의 포트 번호는 `psgControlPort`의 포트 번호와 동일합니다.

- 6 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

View Composer의 기본 포트 교체

View Composer 서비스에 사용되는 SSL 인증서는 기본적으로 특정 포트에 바인딩됩니다. `SviConfig ChangeCertificateBindingPort` 유틸리티를 사용하여 기본 포트를 교체할 수 있습니다.

`SviConfig ChangeCertificateBindingPort` 유틸리티를 사용해 새 포트를 지정하면 해당 유틸리티가 현재 포트에서 View Composer 인증서의 바인딩을 해제하고 새 포트에 바인딩합니다.

설치 도중 View Composer가 필요한 기본 포트를 열도록 Windows 방화벽을 구성합니다. 포트를 변경하려면 업데이트된 포트를 열고 View Composer 서비스에 연결할 수 있도록 Windows 방화벽을 수동으로 재구성해야 합니다.

사전 요구 사항

지정하려는 포트를 사용할 수 있는지 확인하십시오.

절차

- 1 View Composer 서비스를 중지합니다.
- 2 View Composer가 설치된 Windows Server 호스트에서 명령 프롬프트를 엽니다.
- 3 SviConfig 실행 파일로 이동합니다.

파일은 View Composer 애플리케이션으로 찾을 수 있습니다. 기본 경로는 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe입니다.

- 4 SviConfig ChangeCertificateBindingPort 명령을 입력합니다.

예:

```
sviconfig -operation=ChangeCertificateBindingPort
          -Port=port number
```

여기서 -port=port number는 View Composer가 인증서를 바인딩할 새 포트입니다. -port=port number 매개 변수는 필수입니다.

- 5 변경 내용을 적용하려면 View Composer 서비스를 다시 시작하십시오.

다음에 수행할 작업

필요한 경우 업데이트된 포트를 열도록 View Composer Server에서 Windows 방화벽을 수동으로 재구성하십시오.

연결 서버에 대한 HTTP 리디렉션 포트 번호 변경

Horizon 7 서버의 기본 포트 443을 변경하고 포트 80에 연결을 시도하는 Horizon Client에 HTTP 리디렉션을 허용하려면 Horizon 7 서버에 locked.properties 파일을 구성해야 합니다.

참고 SSL의 부하를 중간 디바이스로 분산한 경우 이 절차는 영향을 미치지 않습니다. SSL 부하 분산을 사용하면 Horizon 7 서버의 HTTP 포트가 클라이언트에 서비스를 제공합니다.

사전 요구 사항

기본 포트 번호를 443에서 변경했는지 확인하십시오. 설치 도중 구성된 기본값을 사용할 경우 HTTP 리디렉션 규칙을 준수하기 위해 이 절차를 수행할 필요가 없습니다.

절차

- 1 연결 서버 또는 보안 서버 컴퓨터의 SSL 게이트웨이 구성 폴더에 locked.properties 파일을 생성 또는 편집합니다.

예: install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties
locked.properties 파일의 속성은 대/소문자를 구분합니다.

- 2 다음 행을 `locked.properties` 파일에 추가하십시오.

```
frontMappingHttpDisabled.1=5:*:moved:https::포트
frontMappingHttpDisabled.2=3:/error/*:file:docroot
frontMappingHttpDisabled.3=1:/admin*:missing
frontMappingHttpDisabled.4=1:/view-vlsi*:missing
```

앞에 있는 행에서 변수 `port`는 클라이언트가 연결해야 하는 포트 번호입니다.

앞에 있는 행을 추가하지 않으면 `port`가 443으로 유지됩니다.

- 3 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

연결 서버에 대한 클라이언트 연결에 HTTP 리디렉션 사용 안 함

Horizon Client가 HTTP를 통해 Horizon 7 서버에 연결하려고 시도할 경우 자동으로 HTTPS로 리디렉션됩니다. 일부 배포에서는 사용자가 웹 브라우저에 `http://`를 입력하지 못하게 하고 강제로 HTTPS를 사용하도록 해야 할 수 있습니다. Horizon Client를 위한 HTTP 리디렉션을 방지하려면 Horizon 7 서버에 `locked.properties` 파일을 구성해야 합니다.

참고 SSL의 부하를 중간 디바이스로 분산한 경우 이 절차는 영향을 미치지 않습니다. SSL 부하 분산을 사용하면 Horizon 7 서버의 HTTP 포트가 클라이언트에 서비스를 제공합니다.

절차

- 1 연결 서버 또는 보안 서버 컴퓨터의 SSL 게이트웨이 구성 폴더에 `locked.properties` 파일을 생성 또는 편집합니다.

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\locked.properties`

`locked.properties` 파일의 속성은 대/소문자를 구분합니다.

- 2 다음 행을 `locked.properties` 파일에 추가하십시오.

```
frontMappingHttpDisabled.1=5:*:missing
frontMappingHttpDisabled.2=3:/error/*:file:docroot
```

- 3 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

연결 서버에서 Horizon 7 성능 카운터에 대한 원격 액세스 사용

연결 서버에서 로컬로 Horizon 7 성능 카운터를 사용할 수 있지만 다른 컴퓨터에서 액세스하면 0이 반환됩니다. 연결 서버에서 Horizon 7 성능 카운터에 대한 원격 액세스를 사용하려면 레지스트리에서 연결 서버의 프레임워크 포트를 구성해야 합니다.

절차

- 1 Windows 레지스트리 편집기를 시작합니다.
- 2 `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager` 레지스트리 키로 이동합니다.
- 3 새 문자열(REG_SZ) 값인 `Management Port`를 추가합니다.

4 Management Port 값을 32111로 설정합니다.

Windows Server 설정을 크기 조정하여 배포 지원

대규모 원격 데스크톱 배포를 지원하도록 연결 서버를 설치할 Windows Server 컴퓨터를 구성할 수 있습니다. 각 컴퓨터에서 Windows 페이지 파일을 크기 조정할 수 있습니다.

Windows Server 2008 R2 및 Windows Server 2012 R2 컴퓨터에서는 임시 포트, TCB 해시 테이블 및 Java 가상 시스템 설정이 기본적으로 크기 조정됩니다. 이렇게 조정하면 컴퓨터에는 예상된 사용자 로드와 함께 올바르게 실행할 적절한 리소스가 생깁니다.

Horizon 연결 서버의 메모리 크기 조정

연결 서버 컴퓨터에서 50개 이상의 원격 데스크톱을 배포하려면 10GB 메모리가 필요합니다. 메모리가 10GB 이상인 Windows Server 컴퓨터는 연결 서버가 지원할 수 있는 최대 개수인 약 2,000개의 동시 터널 세션을 지원하도록 자동으로 구성됩니다.

작은 개념 증명 방식의 배포에는 10GB 미만의 메모리만 구성합니다. 필요한 최소 4GB 메모리가 있을 경우 구성에서 약 500개의 동시 터널 세션을 지원할 수 있으며, 이 구성은 개념 증명 방식의 소규모 배포를 지원하기에 충분합니다.

하지만 해당 환경의 사용자가 늘어남에 따라 기존 배포가 확장될 수 있으므로 항상 메모리를 10GB 이상으로 구성하는 것이 좋습니다. 해당 환경이 확장되지 않고 메모리를 사용할 수 없음을 알고 있는 경우에만 예외로 합니다.

10GB 미만의 메모리를 사용하여 연결 서버를 설치할 경우 Horizon 7가 설치 완료 후 경고 메시지를 생성하여 메모리 권장 사항을 제공합니다. 연결 서버 인스턴스가 소량의 물리적 메모리로 구성되었음을 알리는 이벤트가 12시간마다 트리거됩니다.

대규모 배포를 지원하기 위해 컴퓨터의 메모리를 10GB로 늘리는 경우 JVM 힙 크기가 권장 값으로 자동 증가되도록 연결 서버를 다시 시작해야 합니다. 연결 서버를 다시 설치할 필요는 없습니다.

중요 64비트 Windows Server 컴퓨터에서 JVM 힙 크기를 변경하지 마십시오. 이 값을 변경하면 연결 서버 동작이 불안정해질 수 있습니다. 64비트 컴퓨터에서 연결 서버 서비스가 물리적 메모리에 맞춰 JVM 힙 크기를 설정합니다.

연결 서버의 추가 하드웨어 및 메모리 요구 사항은 [Horizon 연결 서버의 하드웨어 요구 사항](#)을 참조하십시오.

대규모 배포에서 연결 서버를 사용하기 위한 하드웨어 및 메모리 권장 사항은 "Horizon 7 아키텍처 계획"의 "연결 서버 최대값 및 가상 시스템 구성"을 참조하십시오.

시스템 페이지 파일 설정 구성

시스템 페이지 파일 설정을 변경해 연결 서버 인스턴스가 설치된 Windows Server 컴퓨터의 가상 메모리를 최적화할 수 있습니다.

Windows Server를 설치한 경우 Windows는 컴퓨터에 설치된 물리적 메모리에 기초해 초기 및 최대 페이지 파일 크기를 계산합니다. 이러한 기본 설정은 컴퓨터를 다시 시작한 후에도 그대로 유지됩니다.

Windows Server 컴퓨터가 가상 시스템인 경우, vCenter Server를 통해 메모리 크기를 변경할 수 있습니다. 그러나 Windows에서 기본 설정을 사용하면 새 메모리 크기에 맞춰 시스템 페이지 파일 크기가 조정되지 않습니다.

절차

- 1 연결 서버가 설치된 Windows Server 컴퓨터에서 Virtual Memory 대화상자로 이동하십시오.

기본적으로 **사용자 지정 크기**가 선택됩니다. 초기 및 최대 페이지 파일 크기가 표시됩니다.

- 2 **시스템이 관리하는 크기**를 클릭하십시오.

Windows에서 현재 메모리 사용과 사용 가능한 메모리에 기초해 시스템 페이지 파일 크기를 계속해서 다시 계산합니다.

이벤트 보고 구성

10

Horizon 7 이벤트에 대한 정보를 기록하는 이벤트 데이터베이스를 생성할 수 있습니다. 또한 Syslog 서버를 사용하면 Syslog 서버에 이벤트를 보내거나 Syslog 형식으로 기록된 이벤트의 플랫폼 파일을 생성하도록 연결 서버를 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- [Horizon 7 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가](#)
- [이벤트 보고용 SQL Server 데이터베이스 준비](#)
- [이벤트 데이터베이스 구성](#)
- [Syslog 서버의 이벤트 로깅 구성](#)

Horizon 7 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가

기존 데이터베이스 서버에 추가하는 방식을 사용해 이벤트 데이터베이스를 생성할 수 있습니다. 그런 다음 엔터프라이즈 보고 소프트웨어를 사용해 데이터베이스의 이벤트를 분석할 수 있습니다.

이벤트 로깅 작업이 프로비저닝 및 Horizon 7 배포 시 중요한 다른 작업에 영향을 주지 않도록 이벤트 데이터베이스를 위한 데이터베이스 서버를 전용 서버에 배포해야 합니다.

참고 이 데이터베이스에 대해 ODBC 데이터 소스를 생성할 필요가 없습니다.

사전 요구 사항

- 연결 서버 인스턴스에서 액세스할 수 있는 시스템에 지원되는 Microsoft SQL Server 또는 Oracle 데이터베이스 서버가 있는지 확인하십시오. 지원되는 데이터베이스 버전 목록은 [View Composer 및 이벤트 데이터베이스의 데이터베이스 요구 사항](#)을 참조하십시오.
- 데이터베이스 서버에 데이터베이스와 사용자를 생성하는 데 필요한 데이터베이스 권한이 있는지 확인하십시오.
- Microsoft SQL Server 데이터베이스 서버에서 데이터베이스를 생성하는 절차는 [SQL Server에 View Composer 데이터베이스 추가](#)에 나와 있습니다.

- Oracle 데이터베이스 서버에서 데이터베이스를 생성하는 절차는 [Oracle 12c 또는 11g에 View Composer 데이터베이스 추가](#)에 나와 있습니다.

절차

- 1 서버에 새 데이터베이스를 추가하고 HorizonEvents와 같이 설명이 포함된 이름을 지정하십시오.
Oracle 12c 또는 11g 데이터베이스의 경우에는 Horizon Administrator에서 이벤트 데이터베이스를 구성할 때 사용할 Oracle SID(시스템 ID)도 제공하십시오.

- 2 이 데이터베이스에 대해 테이블과 보기를 생성할 수 있는 권한을 가진 사용자를 추가하십시오.
Oracle의 경우, 트리거와 시퀀스를 생성하는 권한을 비롯해 이들 개체를 읽고 쓰는 사용 권한을 가진 사용자를 추가하십시오.

Microsoft SQL Server 데이터베이스의 경우 인증 방법으로 통합 Windows 인증 보안 모델을 사용하지 마십시오. SQL Server 인증 방법을 사용해야 합니다.

데이터베이스는 생성되지만 Horizon Administrator에 데이터베이스를 구성하기 전까지는 스키마가 설치되지 않습니다.

다음에 수행할 작업

[이벤트 데이터베이스 구성](#)의 지침을 따르십시오.

이벤트 보고용 SQL Server 데이터베이스 준비

Horizon Administrator를 사용하여 Microsoft SQL Server에서 이벤트 데이터베이스를 구성하려면 올바른 TCP/IP 속성을 구성하고 서버에서 SQL Server Authentication을 사용해야 합니다.

사전 요구 사항

- 이벤트 보고를 위해 SQL Server 데이터베이스를 생성합니다. [Horizon 7 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가](#) 항목을 참조하십시오.
- 데이터베이스를 구성하기 위해 필요한 데이터베이스 권한이 있는지 확인합니다.
- 데이터베이스 서버는 인증 방법으로 SQL Server Authentication을 사용해야 합니다. Windows Authentication을 사용하지 마십시오.

절차

- 1 SQL Server Configuration Manager를 열고 **SQL Server YYYY 네트워크 구성**을 확장합니다.
- 2 **server_name의 프로토콜**을 선택합니다.
- 3 프로토콜 목록에서 **TCP/IP**를 마우스 오른쪽 단추로 클릭하고 **속성**을 선택합니다.
- 4 **사용** 속성을 **예**로 설정합니다.
- 5 포트가 할당되었는지 확인하거나 필요한 경우 포트를 할당합니다.

정적 및 동적 포트와 그 할당 방법에 대한 자세한 내용은 SQL Server Configuration Manager의 온라인 도움말을 참조하십시오.

6 이 포트가 방화벽으로 차단되는지 확인합니다.

다음에 수행할 작업

Horizon Administrator를 사용하여 데이터베이스를 연결 서버에 연결합니다. [이벤트 데이터베이스 구성](#)의 지침을 따르십시오.

이벤트 데이터베이스 구성

이벤트 데이터베이스는 로그 파일이 아닌 데이터베이스에 기록으로 Horizon 7 이벤트에 대한 정보를 저장합니다.

연결 서버 인스턴스를 설치한 후에 이벤트 데이터베이스를 구성합니다. 연결 서버 그룹에서 호스트를 1개만 구성하면 됩니다. 그룹의 나머지 호스트는 자동으로 구성됩니다.

참고 이벤트 트래픽이 Horizon 7 환경의 상태에 대한 정보로 제한되더라도 연결 서버 인스턴스와 외부 데이터베이스 사이의 데이터베이스 연결 보안은 관리자의 책임입니다. 별도의 예방 조치를 취하려면 IPSec 또는 다른 방법을 통해 이 채널에 대한 보안을 적용하거나 데이터베이스를 연결 서버 컴퓨터에 로컬로 배포할 수 있습니다.

Microsoft SQL Server 또는 Oracle 데이터베이스 보고 도구를 사용해 데이터베이스 테이블의 이벤트를 검토할 수 있습니다. 자세한 내용은 "Horizon 7 통합" 문서를 참조하십시오.

이벤트 데이터가 타사 분석 소프트웨어에 액세스할 수 있도록 Syslog 형식으로 Horizon 7 이벤트를 생성할 수도 있습니다. vdmadmin 명령에 -i 옵션을 사용하여 이벤트 로그 파일에 Syslog 형식으로 Horizon 7 이벤트 메시지를 기록합니다. "Horizon 7 관리" 문서의 "-i 옵션을 사용하여 Syslog 형식으로 Horizon 7 이벤트 로그 메시지 생성"을 참조하십시오.

사전 요구 사항

이벤트 데이터베이스를 구성하려면 다음 정보가 필요합니다.

- 데이터베이스 서버의 DNS 이름 또는 IP 주소.
- 데이터베이스 서버 유형: Microsoft SQL Server 또는 Oracle 지원되는 데이터베이스 서버에 대한 자세한 내용은 [IPv6 환경에서 지원되는 vSphere 데이터베이스 및 Active Directory 버전을](#) 참조하십시오.
- 데이터베이스 서버 액세스 시 사용하는 포트 번호. Oracle의 기본 포트 번호는 1521이고 SQL Server는 1433입니다. SQL Server의 경우 데이터베이스 서버가 명명된 인스턴스이거나 SQL Server Express를 사용하면 포트 번호를 지정해야 할 수도 있습니다. SQL Server의 명명된 인스턴스 연결에 대한 자세한 내용은 <http://support.microsoft.com/kb/265808>의 Microsoft 기술 자료(KB) 문서를 참조하십시오.
- 데이터베이스 서버에 생성한 이벤트 데이터베이스 이름. [Horizon 7 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가](#)의 내용을 참조하십시오.

Oracle 12c 또는 11g 데이터베이스의 경우 Horizon Administrator에서 이벤트 데이터베이스를 구성할 때 Oracle SID(System Identifier)를 데이터베이스 이름으로 사용해야 합니다.

- 이 데이터베이스용으로 생성한 사용자의 사용자 이름과 암호. [Horizon 7 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가](#)의 내용을 참조하십시오.

이 사용자에 대해 SQL Server 인증을 사용하십시오. 통합 Windows 인증 보안 모델을 사용하지 마십시오.

- 이벤트 데이터베이스의 테이블 접두사(예: VE_). 접두사를 사용해 Horizon 7 설치 간에 데이터베이스를 공유할 수 있습니다.

참고 사용하는 데이터베이스 소프트웨어에 유효한 문자를 입력해야 합니다. 대화 상자를 완료할 때 접두사 구문을 검사하지 않습니다. 사용하는 데이터베이스 소프트웨어에 유효하지 않은 문자를 입력하면 연결 서버에서 데이터베이스 서버에 연결할 때 오류가 발생합니다. 로그 파일에는 이러한 오류와 데이터베이스 이름이 유효하지 않을 때 데이터베이스 서버에서 반환되는 다른 오류를 포함한 모든 오류가 기록됩니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 이벤트 구성**을 선택하십시오.
- 2 **이벤트 데이터베이스** 섹션에서 **편집**을 클릭하고 필드에 정보를 입력한 다음 **확인**을 클릭하십시오.
- 3 (선택 사항) 이벤트 설정 창에서 **편집**을 클릭하고 이벤트를 표시할 시간, 이벤트를 새 이벤트로 분류할 일 수를 변경하고 **확인**을 클릭하십시오.

이 설정은 이벤트가 Horizon Administrator 인터페이스에 표시되는 시간에 대한 설정입니다. 이 시점 이후에는 내역 데이터베이스 테이블에서만 이벤트를 볼 수 있습니다.

데이터베이스 구성 창에는 이벤트 데이터베이스의 현재 구성이 표시됩니다.

- 4 **모니터링 > 이벤트**를 선택하여 이벤트 데이터베이스에 연결되었는지 확인하십시오.

연결이 실패한 경우 오류 메시지가 나타납니다. SQL Express를 사용하거나 SQL Server의 명명된 인스턴스를 사용하는 경우, 준비 단계에서 언급했듯이 올바른 포트 번호를 지정해야 합니다.

Horizon Administrator 대시보드의 시스템 구성 요소 상태에 보고 데이터베이스 머리글 아래 이벤트 데이터베이스 서버가 표시됩니다.

Syslog 서버의 이벤트 로깅 구성

이벤트 데이터가 분석 소프트웨어에 액세스할 수 있도록 Syslog 형식으로 Horizon 7 이벤트를 생성할 수 있습니다.

연결 서버 그룹에서 호스트를 1개만 구성하면 됩니다. 그룹의 나머지 호스트는 자동으로 구성됩니다.

파일 기반 이벤트 로깅을 사용하도록 설정하면 이벤트가 로컬 로그 파일에 누적됩니다. 파일 공유를 지정하면 이러한 로그 파일이 해당 공유로 이동합니다.

- 로컬 파일은 구성 중에 신속하게 문제를 해결하는 용도로만 사용합니다. 예를 들어 이벤트 데이터베이스가 구성되기 전에 로컬 파일을 사용하여 이벤트를 확인할 수 있습니다.

가장 오래된 파일을 삭제하지 않은 상태에서 이벤트 로그의 로컬 디렉토리 최대 크기는 단 한 로그 파일을 포함하여 300MB입니다. Syslog 출력의 기본 대상은 %PROGRAMDATA%\VMware\WDM\events\W입니다.

- Syslog 서버가 없거나 현재 Syslog 서버가 요구에 맞지 않을 경우 UNC 경로를 사용하여 이벤트의 장기 기록 로그 파일을 저장합니다.

또는 vdmadmin 명령을 사용하여 Syslog 형식으로 이벤트의 파일 기반 로깅을 구성할 수 있습니다.

“Horizon 7 관리” 문서에서 vdmadmin 명령의 -l 옵션을 사용하여 Syslog 형식으로 Horizon 7 이벤트 로그 메시지를 생성하는 방법과 관련한 항목을 참조하십시오.

중요 Syslog 데이터는 소프트웨어 기반 암호화 없이 네트워크 전체에 전송되며 사용자 이름과 같은 민감한 데이터를 포함할 수 있습니다. IPSEC와 같은 링크 계층 보안을 사용하여 네트워크에서 이 데이터가 모니터링될 가능성을 차단하는 것이 좋습니다.

사전 요구 사항

이벤트를 Syslog 형식으로 기록하거나 Syslog 서버로 전송하거나 또는 둘 다 수행할 수 있도록 연결 서버를 구성하려면 다음 정보가 필요합니다.

- Syslog 서버를 사용해 UDP 포트에서 Horizon 7 이벤트를 수신하려면 Syslog 서버의 DNS 이름 또는 IP 주소와 UDP 포트 번호를 알고 있어야 합니다. 기본 UDP 포트 번호는 514입니다.
- 플랫폼 파일 형식으로 로그를 수집하려면 파일 공유 UNC 경로, 로그 파일을 저장할 폴더, 사용자 이름, 도메인 이름, 파일 공유에 쓰기 가능한 사용 권한이 있는 계정의 암호를 알아야 합니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 이벤트 구성**을 선택하십시오.
- 2 (선택 사항) **Syslog** 영역에서 Syslog 서버로 이벤트를 전송할 수 있도록 연결 서버를 구성하려면 **Syslog 서버에 전송** 옆의 **추가**를 클릭하고 서버 이름 또는 IP 주소와 UDP 포트 번호를 입력합니다.
- 3 (선택 사항) **파일 시스템에 대한 이벤트** 영역에서 이벤트 로그 메시지를 생성하고 로그 파일에 Syslog 형식으로 저장할지를 선택합니다.

옵션	설명
항상	항상 이벤트 로그 메시지를 생성하고 로그 파일에 Syslog 형식으로 저장합니다.
오류 시 파일에 기록(기본값)	이벤트 데이터베이스 또는 Syslog 서버에 이벤트를 쓰는 데 문제가 있는 경우 감사 이벤트를 로그 파일에 기록합니다. 이 옵션은 기본적으로 사용하도록 설정되어 있습니다.
안 함	이벤트 로그 메시지를 생성하여 로그 파일에 Syslog 형식으로 저장하지 않습니다.

파일 공유에 대한 UNC 경로를 지정하지 않으면 로그 파일이 로컬에 보관됩니다.

- 4 (선택 사항) Horizon 7 이벤트 로그 메시지를 파일 공유에 저장하려면 **다음 위치에 복사** 옆의 **추가**를 클릭하고 파일 공유 UNC 경로, 로그 파일을 저장할 폴더, 사용자 이름, 도메인 이름, 파일 공유에 쓰기 가능한 사용 권한이 있는 계정의 암호를 입력합니다.

UNC 경로의 예:

```
\\syslog-server\folder\file
```