

Horizon Client 및 Agent 보안

Horizon Client 3.x/4.x/5.x 및 View Agent 6.2.x/Horizon
Agent 7.x

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 © 2015–2019 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

Horizon Client 및 Agent 보안 5

1 외부 포트 6

통신 프로토콜 이해 6

View Agent 또는 Horizon Agent의 방화벽 규칙 7

클라이언트 및 에이전트에서 사용되는 TCP 및 UDP 포트 8

2 설치된 서비스, 데몬 및 프로세스 12

Windows 시스템의 View Agent 또는 Horizon Agent 설치 관리자에서 설치된 서비스 12

Windows 클라이언트에 설치된 서비스 13

기타 클라이언트 및 Linux 데스크톱에 설치된 데몬 13

3 보안을 유지할 리소스 15

보안 클라이언트 시스템에 모범 사례 구현 15

구성 파일 위치 15

계정 16

4 클라이언트 및 에이전트의 보안 설정 18

인증서 검사 구성 18

View Agent 및 Horizon Agent 구성 템플릿의 보안 관련 설정 19

Linux 데스크톱의 구성 파일에서 옵션 설정 21

HTML Access에 대한 그룹 정책 설정 30

Horizon Client 구성 템플릿의 보안 설정 31

Horizon Client 인증서 확인 모드 구성 35

로컬 보안 기관 보호 구성 36

5 보안 프로토콜 및 암호 제품군 구성 37

보안 프로토콜과 암호 제품군의 기본 정책 37

특정 클라이언트 유형의 보안 프로토콜 및 암호 제품군 구성 46

SSL/TLS에서 취약한 암호 사용 안 함 47

HTML Access Agent의 보안 프로토콜 및 암호 제품군 구성 47

원격 데스크톱에서 제안 정책 구성 48

6 클라이언트 및 에이전트 로그 파일 위치 50

Windows용 Horizon Client 로그 50

Mac용 Horizon Client 로그 52

Linux용 Horizon Client 로그 53

모바일 디바이스의 Horizon Client 로그 54

Windows 시스템의 Horizon Agent 로그 55

Linux 데스크톱 로그 56

7 보안 패치 적용 58

View Agent 또는 Horizon Agent에 패치 적용 58

Horizon Client를 위한 패치 적용 59

Horizon Client 및 Agent 보안

“Horizon Client 및 Agent 보안”에서는 VMware Horizon® Client™ 및 Horizon Agent(Horizon 7용) 또는 VMware View Agent®(Horizon 6용)의 보안 기능에 대한 간단한 참조 정보를 제공합니다. 이 가이드는 VMware Horizon™ 6 및 Horizon 7의 모든 주 버전과 부 버전에 대해 생성된 “Horizon 7 보안” 가이드와 함께 제공됩니다. “Horizon Client 및 Agent 보안” 가이드는 클라이언트 및 에이전트 소프트웨어의 분기별 릴리스와 함께 분기별로 업데이트됩니다.

Horizon Client는 최종 사용자가 원격 애플리케이션이나 데스크톱에 연결하기 위해 클라이언트 디바이스에서 실행하는 애플리케이션입니다. View Agent(Horizon 6용) 또는 Horizon Agent(Horizon 7용)는 원격 데스크톱의 운영 체제 또는 원격 애플리케이션을 제공하는 Microsoft RDS 호스트에서 실행되는 에이전트 소프트웨어입니다. 이 가이드에는 다음과 같은 정보가 포함되어 있습니다.

- 필요한 시스템 로그인 계정. 시스템 설치/부트스트랩 중에 생성되는 계정의 로그인 ID와 기본값을 변경하는 방법에 대한 지침.
- 보안과 관련이 있는 구성 옵션 및 설정.
- 보안 관련 구성 파일 및 암호, 그리고 보안 작업을 위해 권장되는 액세스 제어 등 보호해야 할 리스.
- 로그 파일 위치 및 용도.
- 서비스 사용자에게 할당되는 권한.
- 클라이언트 및 에이전트의 올바른 작동을 위해 열어두거나 사용하도록 설정해야 하는 외부 인터페이스, 포트 및 서비스.
- 고객이 최신 보안 업데이트 또는 패치를 획득하고 적용할 수 있는 방법에 대한 정보.

대상

본 정보는 IT 의사 결정권자, 설계자, 관리자를 비롯해 Horizon 6 또는 Horizon 7의 보안 구성 요소를 숙지해야 하는 기타 사용자(클라이언트 및 에이전트 포함)를 대상으로 합니다.

VMware 기술 자료 용어집

VMware 기술 자료 사이트에서는 익숙하지 않을 수 있는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 문서에 사용되는 용어의 정의를 보려면 <http://www.vmware.com/kr/support/pubs>로 이동하십시오.

외부 포트

1

제품이 적절하게 작동하려면 원격 데스크톱의 클라이언트와 에이전트가 서로 통신할 수 있도록 사용할 기능에 따라 다양한 포트를 열어야 합니다.

본 장은 다음 항목을 포함합니다.

- [통신 프로토콜 이해](#)
- [View Agent 또는 Horizon Agent의 방화벽 규칙](#)
- [클라이언트 및 에이전트에서 사용되는 TCP 및 UDP 포트](#)

통신 프로토콜 이해

Horizon 6 및 Horizon 7 구성 요소는 여러 가지 프로토콜을 사용하여 메시지를 교환합니다.

[표 1-1. 기본 포트](#)에는 각 프로토콜에서 사용하는 기본 포트가 나열되어 있습니다. 필요하다면, 조직 정책을 준수하거나 경합을 피하기 위해 사용되는 포트 번호를 변경할 수 있습니다.

표 1-1. 기본 포트

프로토콜	포트
JMS	TCP 포트 4001 TCP 포트 4002
HTTP	TCP 포트 80
HTTPS	TCP 포트 443
MMR/CDR	멀티미디어 리디렉션 및 클라이언트 드라이브 리디렉션의 경우 TCP 포트 9427
RDP	TCP 포트 3389
PCoIP	TCP 포트 4172 UDP 포트 4172, 50002, 55000
USB 리디렉션	TCP 포트 32111. 이 포트는 시간대 동기화에도 사용됩니다.
VMware Blast Extreme	TCP 포트 8443, 22443 UDP 포트 443, 8443, 22443
HTML Access	TCP 포트 8443, 22443

View Agent 또는 Horizon Agent의 방화벽 규칙

View Agent 및 Horizon Agent 설치 관리자는 필요에 따라 원격 데스크톱 및 RDS 호스트의 Windows 방화벽 규칙을 구성하여 기본 네트워크 포트를 열도록 합니다. 이러한 포트는 다른 설명이 없는 한 수신용입니다.

View Agent 및 Horizon Agent 설치 관리자에서 인바운드 RDP 연결의 로컬 방화벽 규칙을 호스트 운영 체제의 현재 RDP 포트(일반적으로 3389)와 일치하도록 구성합니다.

View Agent 또는 Horizon Agent 설치 관리자에 원격 데스크톱 지원을 사용하지 않도록 설정하면 포트 3389와 32111이 열리지 않으므로 수동으로 열어야 합니다.

설치 후에 RDP 포트 번호를 변경할 경우에는 연결된 방화벽 규칙을 변경해야 합니다. 설치 후에 기본 포트를 변경하려면 업데이트된 포트에 대한 액세스를 허용하도록 Windows 방화벽 규칙을 수동으로 재구성해야 합니다. "Horizon 7 설치" 문서의 "View 서비스의 기본 포트 교체"를 참조하십시오.

RDS 호스트의 View Agent 또는 Horizon Agent에 대한 Windows 방화벽 규칙에서 256개의 인접 UDP 포트 블록이 인바운드 트래픽에 대해 열려 있는 것으로 표시됩니다. 이 포트 블록은 View Agent 또는 Horizon Agent에서 VMware Blast 내부용입니다. RDS 호스트의 특별 Microsoft 서명된 드라이버는 외부 소스에서 이러한 포트로 이동하는 인바운드 트래픽을 차단합니다. 이 드라이버는 Windows 방화벽이 포트를 닫힌 상태로 취급하도록 합니다.

가상 시스템 템플릿을 데스크톱 소스로 사용하면 해당 템플릿이 데스크톱 도메인 구성원일 경우에만 배포된 데스크톱까지 방화벽 예외가 적용됩니다. Microsoft 그룹 정책 설정을 사용해 로컬 방화벽 예외를 관리할 수 있습니다. 자세한 내용은 Microsoft 기술 자료(KB) 문서 875357에 나와 있습니다.

표 1-2. View Agent 또는 Horizon Agent 설치 중 열리는 TCP 및 UDP 포트

프로토콜	포트
RDP	TCP 포트 3389
USB 리디렉션 및 표준 시간대 동기화	TCP 포트 32111
MMR(멀티미디어 리디렉션) 및 CDR(클라이언트 드라이브 리디렉션)	TCP 포트 9427
PCoIP	RDS 호스트의 경우 PCoIP는 TCP 포트 4172 및 UDP 포트 4172(양방향)를 사용합니다. 데스크톱의 경우 PCoIP는 구성 가능한 범위에서 선택한 포트 번호를 사용합니다. 기본적으로 TCP 포트 4172-4173 및 UDP 포트 4172-4182가 이 범위에 해당합니다. 이러한 포트 범위에 대한 방화벽 규칙은 포트 번호를 지정하지 않고 각 PCoIP Server에서 열린 포트를 동적으로 따릅니다. 선택한 포트 번호는 연결 서버 통해 클라이언트에 전달됩니다.
VMware Blast	TCP 포트 22443 UDP 포트 22443(양방향) 참고 UDP는 Linux 데스크톱에서 사용되지 않습니다.
HTML Access	TCP 포트 22443

표 1-2. View Agent 또는 Horizon Agent 설치 중 열리는 TCP 및 UDP 포트 (계속)

프로토콜	포트
XDMCP	UDP 177 참고 이 포트는 Ubuntu 18.04를 실행하는 Linux 데스크톱의 XDMCP 액세스에 대해서만 열립니다. 방화벽 규칙은 이 포트에 대한 모든 외부 호스트 액세스를 차단합니다.
X11	TCP 6100 참고 이 포트는 Ubuntu 18.04를 실행하는 Linux 데스크톱의 XServer 액세스에 대해서만 열립니다. 방화벽 규칙은 이 포트에 대한 모든 외부 호스트 액세스를 차단합니다.

클라이언트 및 에이전트에서 사용되는 TCP 및 UDP 포트

View Agent(Horizon 6용), Horizon Agent(Horizon 7용) 및 Horizon Client에서는 서로, 그리고 다양한 서버 구성 요소와의 네트워크 액세스에 TCP 및 UDP 포트를 사용합니다.

표 1-3. View Agent 또는 Horizon Agent에서 사용되는 TCP 및 UDP 포트

소스	포트	대상	포트	프로토콜	설명
Horizon Client	*	View Agent/ Horizon Agent	3389	TCP	터널 연결 대신 직접 연결을 사용할 경우 원격 데스크톱에 대한 Microsoft RDP 트래픽입니다.
Horizon Client	*	View Agent/ Horizon Agent	9427	TCP	터널 연결 대신 직접 연결이 사용될 경우 Windows Media MMR 리더렉션과 클라이언트 드라이브 리더렉션입니다. 참고 VMware Blast를 사용할 경우 클라이언트 드라이브 리더렉션이 필요하지 않습니다.
Horizon Client	*	View Agent/ Horizon Agent	32111	TCP	터널 연결 대신 직접 연결을 사용할 경우 USB 리더렉션 및 시간대 동기화입니다.
Horizon Client	*	View Agent/ Horizon Agent	4172	TCP 및 UDP	PCoIP 보안 게이트웨이가 사용되지 않을 경우 PCoIP입니다. 참고 소스 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.
Horizon Client	*	Horizon Agent	22443	TCP 및 UDP	터널 연결 대신 직접 연결을 사용할 경우 VMware Blast입니다. 참고 UDP는 Linux 데스크톱에서 사용되지 않습니다.
브라우저	*	View Agent/ Horizon Agent	22443	TCP	터널 연결 대신 직접 연결을 사용할 경우 HTML Access입니다.
보안 서버, 연결 서버 또는 Unified Access Gateway 장치	*	View Agent/ Horizon Agent	3389	TCP	터널 연결을 사용할 경우 Microsoft RDP에서 원격 데스크톱으로 가는 트래픽입니다.

표 1-3. View Agent 또는 Horizon Agent에서 사용되는 TCP 및 UDP 포트 (계속)

소스	포트	대상	포트	프로토콜	설명
보안 서버, 연결 서버 또는 Unified Access Gateway 장치	*	View Agent/ Horizon Agent	9427	TCP	터널 연결을 사용할 경우 Windows Media MMR 리디렉션 및 클라이언트 드라이브 리디렉션입니다.
보안 서버, 연결 서버 또는 Unified Access Gateway 장치	*	View Agent/ Horizon Agent	32111	TCP	터널 연결을 사용할 경우 USB 리디렉션 및 시간대 동기화입니다.
보안 서버, 연결 서버 또는 Unified Access Gateway 장치	55000	View Agent/ Horizon Agent	4172	UDP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP(SALSA20 아님)입니다.
보안 서버, 연결 서버 또는 Unified Access Gateway 장치	*	View Agent/ Horizon Agent	4172	TCP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP입니다.
보안 서버, 연결 서버 또는 Unified Access Gateway 장치	*	Horizon Agent	22443	TCP 및 UDP	Blast 보안 게이트웨이를 사용할 경우 VMware Blast입니다. 참고 UDP는 Linux 데스크톱에서 사용되지 않습니다.
보안 서버, 연결 서버 또는 Unified Access Gateway 장치	*	View Agent/ Horizon Agent	22443	TCP	Blast 보안 게이트웨이를 사용할 경우 HTML Access입니다.
View Agent/ Horizon Agent	*	연결 서버	4001, 4002	TCP	JMS SSL 트래픽입니다.
View Agent/ Horizon Agent	4172	Horizon Client	*	UDP	PCoIP 보안 게이트웨이를 사용하지 않을 경우 PCoIP입니다. 참고 대상 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.
View Agent/ Horizon Agent	4172	연결 서버, 보안 서버 또는 Unified Access Gateway 장치	55000	UDP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP(SALSA20 아님)입니다.

참고 에이전트가 PCoIP에 사용하는 UDP 포트 번호는 변경될 수 있습니다. 포트 50002가 사용 중이면 에이전트가 50003을 고르고, 포트 50003이 사용 중이면 50004를 고르는 방식입니다. 표에 별표 (*)가 나열된 경우 ANY 값으로 방화벽을 구성해야 합니다.

표 1-4. Horizon Client에서 사용되는 TCP 및 UDP 포트

소스	포트	대상	포트	프로토콜	설명
Horizon Client	*	연결 서버, 보안 서버 또는 Unified Access Gateway 장치	443	TCP	Horizon 6 또는 Horizon 7에 로그인하기 위한 HTTPS입니다. (터널 연결을 사용하는 경우 이 포트는 터널링에도 사용됩니다.) 참고 Horizon Client 4.4 이상은 UDP 포트 443(아래 참조)을 지원합니다.
Horizon Client 4.4 이상	*	Unified Access Gateway 장치 2.9 이상	443	UDP	Blast 보안 게이트웨이가 사용되고 UDP 터널 서버가 사용하도록 설정된 경우 Horizon 6 또는 Horizon 7 로그인에 사용되는 HTTPS입니다. (터널 연결을 사용하는 경우 이 포트는 터널링에도 사용됩니다.)
Unified Access Gateway 장치 2.9 이상	443	Horizon Client 4.4 이상	*	UDP	Blast 보안 게이트웨이가 사용되고 UDP 터널 서버가 사용하도록 설정된 경우 Horizon 6 또는 Horizon 7 로그인에 사용되는 HTTPS입니다. (터널 연결을 사용하는 경우 이 포트는 터널링에도 사용됩니다.)
Horizon Client	*	View Agent/ Horizon Agent	22443	TCP	Blast 보안 게이트웨이를 사용하지 않을 경우 HTML Access 및 VMware Blast입니다.
Horizon Client	*	Horizon Agent	22443	UDP	Blast 보안 게이트웨이를 사용하지 않을 경우 VMware Blast입니다. 참고 Linux 데스크톱에 연결할 때는 사용되지 않습니다.
Horizon Agent	22443	Horizon Client	*	UDP	Blast 보안 게이트웨이를 사용하지 않을 경우 VMware Blast입니다. 참고 Linux 데스크톱에 연결할 때는 사용되지 않습니다.
Horizon Client	*	View Agent/ Horizon Agent	3389	TCP	터널 연결 대신 직접 연결을 사용할 경우 원격 데스크톱에 대한 Microsoft RDP 트래픽입니다.
Horizon Client	*	View Agent/ Horizon Agent	9427	TCP	터널 연결 대신 직접 연결이 사용될 경우 Windows Media MMR 리디렉션과 클라이언트 드라이브 리디렉션입니다. 참고 VMware Blast를 사용할 경우 CDR에 필요하지 않습니다.
Horizon Client	*	View Agent/ Horizon Agent	32111	TCP	터널 연결 대신 직접 연결을 사용할 경우 USB 리디렉션 및 시간대 동기화입니다.
Horizon Client	*	View Agent/ Horizon Agent	4172	TCP 및 UDP	PCoIP 보안 게이트웨이가 사용되지 않을 경우 PCoIP입니다. 참고 소스 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.

표 1-4. Horizon Client에서 사용되는 TCP 및 UDP 포트 (계속)

소스	포트	대상	포트	프로토콜	설명
Horizon Client	*	연결 서버, 보안 서버 또는 Unified Access Gateway 장치	4172	TCP 및 UDP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP(SALSA20 아님)입니다. 참고 소스 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.
View Agent/ Horizon Agent	4172	Horizon Client	*	UDP	PCoIP 보안 게이트웨이가 사용되지 않을 경우 PCoIP입니다. 참고 대상 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.
보안 서버, View 연결 서버 또는 Unified Access Gateway 장치	4172	Horizon Client	*	UDP	PCoIP 보안 게이트웨이를 사용할 경우 PCoIP(SALSA20 아님)입니다. 참고 대상 포트가 다양하므로 이 표 아래에 있는 정보를 참고하십시오.
Horizon Client	*	연결 서버, 보안 서버 또는 Unified Access Gateway 장치	8443	TCP	Blast 보안 게이트웨이를 사용할 경우 HTML Access 및 VMware Blast입니다.
Horizon Client	*	연결 서버, 보안 서버 또는 Unified Access Gateway 장치	8443	UDP	Blast 보안 게이트웨이를 사용할 경우 VMware Blast입니다. 참고 Linux 데스크톱에 연결할 때는 사용되지 않습니다.
View 연결 서버, 보안 서버 또는 Unified Access Gateway 장치	8443	Horizon Client	*	UDP	Blast 보안 게이트웨이를 사용할 경우 VMware Blast입니다. 참고 Linux 데스크톱에 연결할 때는 사용되지 않습니다.

참고 클라이언트가 PCoIP 및 VMware Blast에 사용하는 UDP 포트 번호는 변경될 수 있습니다. 포트 50002가 사용 중이면 클라이언트가 50003을 선택하고, 포트 50003이 사용 중이면 50004를 선택하는 방식입니다. 표에 별표(*)가 나열된 경우 ANY 값으로 방화벽을 구성해야 합니다.

설치된 서비스, 데몬 및 프로세스

2

클라이언트 또는 에이전트 설치 관리자를 실행할 때 몇 가지 구성 요소가 설치됩니다.

본 장은 다음 항목을 포함합니다.

- Windows 시스템의 View Agent 또는 Horizon Agent 설치 관리자에서 설치된 서비스
- Windows 클라이언트에 설치된 서비스
- 기타 클라이언트 및 Linux 데스크톱에 설치된 데몬

Windows 시스템의 View Agent 또는 Horizon Agent 설치 관리자에서 설치된 서비스

원격 데스크톱 및 애플리케이션의 작업은 몇 가지 Windows 서비스에 종속됩니다.

표 2-1. View Agent(Horizon 6용) 또는 Horizon Agent(Horizon 7용) 서비스

서비스 이름	시작 유형	설명
VMware Blast	자동	HTML Access를 위한 서비스와 네이티브 클라이언트 연결을 위한 VMware Blast Extreme 프로토콜 서비스를 제공합니다.
VMware Horizon View Agent	자동	View Agent/Horizon Agent의 서비스를 제공합니다.
VMware Horizon View Composer Guest Agent Server	자동	이 가상 시스템이 View Composer 연결된 복제 데스크톱 풀의 일부인 경우 서비스를 제공합니다.
VMware Horizon View Persona Management	기능이 사용 설정된 경우는 자동, 그렇지 않은 경우는 사용 안 함	VMware 개인 설정 관리 기능의 서비스를 제공합니다.
VMware Horizon View Script Host	사용 안 함	데스크톱 세션이 시작되기 전에 데스크톱 보안 정책을 구성하도록 시작 세션 스크립트의 실행 지원을 제공합니다. 정책은 클라이언트 디바이스와 사용자의 위치를 기반으로 합니다.
VMware Netlink Supervisor 서비스	자동	스캐너 리디렉션 기능과 직렬 포트 리디렉션 기능을 지원하기 위해 커널과 사용자 공간 프로세스 사이에서 정보를 전송하는 모니터링 서비스를 제공합니다.
VMware 스캐너 리디렉션 클라이언트 서비스	자동	(View Agent 6.0.2 이상) 스캐너 리디렉션 기능의 서비스를 제공합니다.

표 2-1. View Agent(Horizon 6용) 또는 Horizon Agent(Horizon 7용) 서비스 (계속)

서비스 이름	시작 유형	설명
VMware 직렬 통신 클라이언트 서비스	자동	(View Agent 6.1.1 이상) 직렬 포트 리디렉션 기능의 서비스를 제공합니다.
VMware Snapshot Provider	수동	복제에 사용되는 가상 시스템 스냅샷의 서비스를 제공합니다.
VMware Tools	자동	호스트와 게스트 운영 체제 사이에서 개체를 동기화하여 가상 시스템 게스트 운영 체제의 성능을 향상시키고 가상 시스템의 관리를 강화하기 위한 지원을 제공합니다.
VMware USB Arbitration Service	자동	클라이언트에 연결된 다양한 USB 디바이스를 열거하고 클라이언트에 연결할 디바이스와 원격 데스크톱에 연결할 디바이스를 결정합니다.
VMware View USB	자동	USB 리디렉션 기능의 서비스를 제공합니다.

Windows 클라이언트에 설치된 서비스

Horizon Client의 작업은 몇 가지 Windows 서비스에 종속됩니다.

표 2-2. Horizon Client 서비스

서비스 이름	시작 유형	설명
VMware Horizon Client	자동	Horizon Client 서비스를 제공합니다.
VMware Netlink Supervisor 서비스	자동	스캐너 리디렉션 기능과 직렬 포트 리디렉션 기능을 지원하기 위해 커널과 사용자 공간 프로세스 사이에서 정보를 전송하는 모니터링 서비스를 제공합니다.
VMware 스캐너 리디렉션 클라이언트 서비스	자동	(Horizon Client 3.2 이상) 스캐너 리디렉션 기능의 서비스를 제공합니다.
VMware 직렬 통신 클라이언트 서비스	자동	(Horizon Client 3.4 이상) 직렬 포트 리디렉션 기능의 서비스를 제공합니다.
VMware USB Arbitration Service	자동	클라이언트에 연결된 다양한 USB 디바이스를 열거하고 클라이언트에 연결할 디바이스와 원격 데스크톱에 연결할 디바이스를 결정합니다.
VMware View USB	자동	(Horizon Client 4.3 및 이전) USB 리디렉션 기능의 서비스를 제공합니다. 참고 Horizon Client 4.4 이상에서는 이 서비스가 제거되고 USB 서비스는 <code>vmware-remotemks.exe</code> 프로세스로 이동됩니다.

기타 클라이언트 및 Linux 데스크톱에 설치된 데몬

보안을 위해서는 Horizon Client를 통해 데몬이나 프로세스가 설치되는지 여부를 아는 것이 중요합니다.

표 2-3. Horizon Client에서 설치된 클라이언트 유형별 서비스, 프로세스 또는 데몬

유형	서비스, 프로세스 또는 데몬
Linux 클라이언트	<ul style="list-style-type: none"> ■ <code>vmware-usbarbitrator</code>는 클라이언트에 연결된 다양한 USB 디바이스를 열거하고 클라이언트에 연결할 디바이스와 원격 데스크톱에 연결할 디바이스를 결정합니다. ■ <code>Vmware-view-used</code>는 USB 리디렉션 기능의 서비스를 제공합니다. <p>참고 이러한 데몬은 설치할 때 설치 후에 서비스 등록 및 시작 확인란을 클릭하면 자동으로 시작됩니다. 이러한 프로세스는 루트로 실행됩니다.</p>
Mac 클라이언트	Horizon Client는 데몬을 생성하지 않습니다.
Chrome OS 클라이언트	Horizon Client는 단일 Android 프로세스에서 실행됩니다. Horizon Client는 데몬을 생성하지 않습니다.
iOS 클라이언트	Horizon Client는 데몬을 생성하지 않습니다.
Android 클라이언트	Horizon Client는 단일 Android 프로세스에서 실행됩니다. Horizon Client에서는 데몬을 생성하지 않습니다.
Windows 10 UWP 클라이언트	Horizon Client에서는 시스템 서비스를 생성하거나 트리거하지 않습니다.
Windows 스토어 클라이언트	Horizon Client에서는 시스템 서비스를 생성하거나 트리거하지 않습니다.
Linux 데스크톱	<ul style="list-style-type: none"> ■ <code>StandaloneAgent</code>는 루트 권한으로 실행되며 Linux 시스템이 가동되어 실행 중일 때 시작됩니다. <code>StandaloneAgent</code>는 연결 서버와 통신하여 원격 데스크톱 세션 관리를 수행합니다(세션 설정 및 해체, 연결 서버에서 원격 데스크톱 상태를 브로커로 업데이트). ■ <code>VMwareBlastServer</code>는 연결 서버에서 <code>StartSession</code> 요청을 받으면 <code>StandaloneAgent</code>에서 시작됩니다. <code>VMwareBlastServer</code> 데몬은 <code>vmwblast</code>(Linux Agent를 설치할 때 생성되는 시스템 계정) 권한으로 실행합니다. 내부 <code>MKSControl</code> 채널을 통해 <code>StandaloneAgent</code>와 통신하고 VMware Blast 디스플레이 프로토콜을 사용하여 Horizon Client와 통신합니다.

보안을 유지할 리소스

3

이러한 리소스에는 관련 구성 파일, 암호 및 액세스 제어가 포함됩니다.

본 장은 다음 항목을 포함합니다.

- 보안 클라이언트 시스템에 모범 사례 구현
- 구성 파일 위치
- 계정

보안 클라이언트 시스템에 모범 사례 구현

보안 클라이언트 시스템에 이러한 모범 사례를 구현합니다.

- 일정 기간 사용하지 않으면 절전 상태로 전환되고 사용자가 컴퓨터를 활성화하려면 암호를 입력하도록 클라이언트 시스템을 구성하십시오.
- 사용자가 클라이언트 시스템을 시작할 때 사용자 이름과 암호를 입력하도록 요구하십시오. 자동 로그인을 허용하도록 클라이언트 시스템을 구성하지 마십시오.
- Mac 클라이언트 시스템의 경우 키체인과 사용자 계정의 암호를 다르게 설정하십시오. 암호가 다른 경우에는 시스템에서 사용자 대신 암호를 입력하기 전에 사용자에게 메시지가 표시됩니다. 또한 FileVault 보호 기능 설정을 고려하십시오.

구성 파일 위치

보호해야 할 리소스에는 보안 관련 구성 파일이 포함됩니다.

표 3-1. 클라이언트 유형별 구성 파일 위치

유형	디렉토리 경로
Linux 클라이언트	<p>Horizon Client가 시작되면 구성 설정이 여러 위치에서 다음과 같은 순서로 처리됩니다.</p> <ol style="list-style-type: none"> 1 /etc/vmware/view-default-config 2 ~/.vmware/view-preferences 3 /etc/vmware/view-mandatory-config <p>설정이 여러 위치에서 정의되었다면 사용되는 값은 읽은 마지막 파일 또는 명령줄 옵션의 값이 됩니다.</p>
Windows 클라이언트	<p>비공개 정보가 포함된 사용자 설정이 다음 파일에 있을 수 있습니다.</p> <p>C:\Users\User-name\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt</p>
Mac 클라이언트	<p>Mac 클라이언트를 시작한 후에 생성된 일부 구성 파일입니다.</p> <ul style="list-style-type: none"> ■ \$HOME/Library/Preferences/com.vmware.horizon.plist ■ \$HOME/Library/Preferences/com.vmware.vmr.plist ■ \$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist ■ /Library/Preferences/com.vmware.horizon.plist
Chrome OS 클라이언트	<p>보안 관련 설정은 구성 파일이 아닌 사용자 인터페이스에 나타납니다. 구성 파일은 사용자에게 보이지 않습니다.</p>
iOS 클라이언트	<p>보안 관련 설정은 구성 파일이 아닌 사용자 인터페이스에 나타납니다. 구성 파일은 사용자에게 보이지 않습니다.</p>
Android 클라이언트	<p>보안 관련 설정은 구성 파일이 아닌 사용자 인터페이스에 나타납니다. 구성 파일은 사용자에게 보이지 않습니다.</p>
Windows 10 UWP 클라이언트	<p>보안 관련 설정은 구성 파일이 아닌 사용자 인터페이스에 나타납니다. 구성 파일은 사용자에게 보이지 않습니다.</p>
Windows 스토어 클라이언트	<p>보안 관련 설정은 구성 파일이 아닌 사용자 인터페이스에 나타납니다. 구성 파일은 사용자에게 보이지 않습니다.</p>
View Agent 또는 Horizon Agent(Windows 운영 체제를 사용하는 원격 데스크톱)	<p>보안 관련 설정이 Windows 레지스트리에만 표시됩니다.</p>
Linux 데스크톱	<p>텍스트 편집기를 사용하여 다음 구성 파일을 열고 SSL 관련 설정을 지정할 수 있습니다.</p> <p>/etc/vmware/viewagent-custom.conf</p>

계정

클라이언트 사용자는 Active Directory에 계정이 있어야 합니다.

Horizon Client 사용자 계정

원격 데스크톱과 애플리케이션에 액세스할 수 있는 사용자를 위해 Active Directory에 사용자 계정을 구성합니다. RDP 프로토콜을 사용하려는 경우에는 사용자 계정이 원격 데스크톱 사용자 그룹의 구성원이어야 합니다.

최종 사용자는 보통 Horizon 관리자가 아니어야 합니다. Horizon 관리자가 사용자 환경을 확인해야 하는 경우에는 별도의 테스트 계정을 생성하고 사용 권한을 부여합니다. 데스크톱에서 Horizon 최종 사용자는 관리자와 같이 사용 권한이 있는 그룹의 구성원이 아니어야 합니다. 잠긴 구성 파일과 Windows 레지스트리를 수정할 수 있게 되기 때문입니다.

설치 중에 생성된 시스템 계정

Horizon Client 애플리케이션에서는 어떤 유형의 클라이언트에도 서비스 사용자 계정을 생성하지 않습니다. Windows용 Horizon Client에서 생성된 서비스의 경우 로그인 ID는 Local System입니다.

Mac 클라이언트에서 처음 시작할 때, 사용자는 USB 및 가상 인쇄(ThinPrint) 서비스를 시작할 수 있는 로컬 관리자 액세스 권한을 부여해야 합니다. 이러한 서비스를 처음 시작한 후에 표준 사용자에게는 실행 액세스 권한이 있습니다. 마찬가지로, 설치 중에 **설치 후에 서비스 등록 및 시작** 확인란을 클릭한 경우에는 Linux 클라이언트에서 `vmware-usbarbitrator` 및 `vmware-view-used` 데몬이 자동으로 시작됩니다. 이러한 프로세스는 루트로 실행됩니다.

Windows 데스크톱의 View Agent 또는 Horizon Agent에서는 서비스 사용자 계정이 생성되지 않습니다. Linux 데스크톱에서는 시스템 계정 `vmwblast`가 생성됩니다. Linux 데스크톱에서 StandaloneAgent 데몬은 루트 권한으로 실행되고 VmwareBlastServer 데몬은 `vmwblast` 권한으로 실행됩니다.

클라이언트 및 에이전트의 보안 설정

4

구성의 보안 조정에 몇 가지 클라이언트 및 에이전트 설정을 사용할 수 있습니다. 그룹 정책 개체를 사용하거나 Windows 레지스트리 설정을 편집하여 원격 데스크톱 및 Windows 클라이언트의 설정에 액세스할 수 있습니다.

로그 수집과 관련된 구성 설정은 [장 6 클라이언트 및 에이전트 로그 파일 위치](#)를 참조하십시오. 보안 프로토콜 및 암호 제품군과 관련된 구성 설정은 [장 5 보안 프로토콜 및 암호 제품군 구성](#)을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [인증서 검사 구성](#)
- [View Agent 및 Horizon Agent 구성 템플릿의 보안 관련 설정](#)
- [Linux 데스크톱의 구성 파일에서 옵션 설정](#)
- [HTML Access에 대한 그룹 정책 설정](#)
- [Horizon Client 구성 템플릿의 보안 설정](#)
- [Horizon Client 인증서 확인 모드 구성](#)
- [로컬 보안 기관 보호 구성](#)

인증서 검사 구성

관리자는 인증서 확인 모드를 구성할 수 있습니다(예: 항상 전체 확인이 수행되도록 구성). 관리자는 서버 인증서 검사에 실패할 경우 최종 사용자가 클라이언트 연결 거부를 선택할 수 있는지 여부를 구성할 수 있습니다.

인증서 검사는 연결 서버 인스턴스와 Horizon Client 간에 SSL/TLS 연결이 있을 때 수행됩니다. 관리자는 다음 전략 중 하나를 사용하도록 확인 모드를 구성할 수 있습니다.

- 최종 사용자가 확인 모드를 선택할 수 있습니다. 이 목록의 나머지 부분에서는 세 가지 확인 모드를 설명합니다.
- (확인 안 함) 인증서 검사를 수행하지 않습니다.
- (경고) 서버에서 자체 서명된 인증서를 제시할 경우 최종 사용자에게 경고합니다. 사용자는 이러한 유형의 연결을 허용할지 선택할 수 있습니다.

- (전체 보안) 전체 확인이 수행되고 전체 확인을 통과하지 못한 연결은 거부됩니다.

인증서 검사에는 다음 확인 사항이 포함됩니다.

- 인증서가 해지되었습니까?
- 해당 인증서는 전송자 ID 확인 및 서버 통신 암호화 이외의 용도입니까? 즉, 올바른 유형의 인증서입니까?
- 인증서가 만료되었거나 나중에만 유효합니까? 즉, 컴퓨터 시계에 따라 인증서가 유효합니까?
- 인증서의 공통 이름이 이름을 보내는 서버의 호스트 이름과 일치합니까? 로드 밸런서가 Horizon Client에 입력된 호스트 이름과 일치하지 않는 인증서를 가진 서버에 Horizon Client를 리디렉션하는 경우 불일치가 발생할 수 있습니다. 또는 사용자가 클라이언트의 호스트 이름이 아닌 IP 주소를 입력할 경우 불일치가 발생할 수 있습니다.
- 알 수 없거나 신뢰할 수 없는 인증 기관(CA)에서 서명된 인증서입니까? 자체 서명된 인증서는 신뢰할 수 없는 CA 유형 중 하나입니다.

이 검사를 통과하려면 신뢰할 수 있는 인증서 체인이 디바이스 로컬 인증서 저장소의 루트 위치에 있어야 합니다.

SSL 프록시 서버를 사용하여 클라이언트 환경에서 인터넷으로 전송된 트래픽을 검사하는 경우 SSL 프록시 서버를 통해 보조 연결을 검사하는 인증서를 사용하도록 설정할 수 있습니다. 또한 프록시 서버를 사용하도록 VMware Blast 연결을 구성할 수도 있습니다. 이러한 기능은 Windows, Mac 및 Linux용 Horizon Client 5.2 이상에서 지원됩니다.

특정 유형의 클라이언트에 대해 인증서 검사 및 SSL 프록시 서버 사용을 구성하는 방법에 대한 내용은 해당 클라이언트의 Horizon Client 설치 및 설정 문서를 참조하십시오. 이러한 문서에는 자체 서명된 인증서의 사용에 대한 정보도 포함되어 있습니다.

View Agent 및 Horizon Agent 구성 템플릿의 보안 관련 설정

보안 관련 설정은 View Agent 및 Horizon Agent에 대한 ADM 및 ADMX 템플릿 파일에 제공됩니다. ADM 및 ADMX 템플릿 파일 이름은 Vdm_agent.adm 및 vdm_agent.admx로 지정됩니다. 다른 설명이 없는 한, 설정에는 컴퓨터 구성 설정만 포함됩니다.

보안 설정은 게스트 시스템 레지스트리의 HKLM\Software\VMware, Inc.\VMware VDM\Agent\WConfiguration에 저장됩니다.

표 4-1. View Agent(Horizon 6용) 또는 Horizon Agent(Horizon 7용) 구성 템플릿의 보안 관련 설정

설정	설명
AllowDirectRDP	<p>Horizon Client 디바이스 이외의 클라이언트가 RDP를 사용하여 원격 데스크톱에 직접 연결할 수 있는지 여부를 결정합니다. 이 설정을 사용하지 않도록 설정한 경우 에이전트는 Horizon Client를 통해 Horizon에서 관리하는 연결만 허용합니다.</p> <p>Mac용 Horizon Client에서 원격 데스크톱에 연결할 경우 AllowDirectRDP 설정을 사용하지 않도록 설정하지 마십시오. 이 설정이 사용되지 않도록 설정된 경우, 액세스가 거부된 오류와 함께 연결이 실패합니다.</p> <p>기본적으로 사용자가 원격 데스크톱 세션에 로그인한 동안에는 RDP를 사용하여 가상 시스템에 연결할 수 있습니다. RDP 연결이 설정되면 원격 데스크톱 세션이 종료되고 사용자가 저장하지 않은 데이터와 설정은 손실될 수 있습니다. 외부 RDP 연결이 단절 때까지 사용자는 데스크톱에 로그인할 수 없습니다. 이러한 상황이 발생하지 않도록 방지하려면 AllowDirectRDP 설정을 비활성화합니다.</p> <p>중요 각 데스크톱의 게스트 운영 체제에 Windows 원격 데스크톱 서비스가 실행 중이어야 합니다. 이 설정을 사용하여 사용자가 데스크톱에 대한 직접 RDP 연결을 설정하지 못하도록 할 수 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p> <p>동등한 Windows 레지스트리 값은 AllowDirectRDP입니다.</p>
AllowSingleSignon	<p>사용자를 데스크톱과 애플리케이션에 연결하는 데 SSO(단일 로그인)를 사용할지 여부를 결정합니다. 이 설정이 사용하도록 설정되어 있으면 사용자가 서버에 로그인할 때 자격 증명을 한 번만 입력하면 됩니다. 이 설정을 사용하지 않도록 설정된 경우, 사용자는 원격 연결이 설정될 때 다시 인증해야 합니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p> <p>동등한 Windows 레지스트리 값은 AllowSingleSignon입니다.</p>
CommandsToRunOnConnect	<p>처음 세션이 연결될 때 실행될 명령 스크립트 또는 명령 목록을 지정합니다.</p> <p>기본적으로 지정되는 목록은 없습니다.</p> <p>동등한 Windows 레지스트리 값은 CommandsToRunOnConnect입니다.</p>
CommandsToRunOnDisconnect	<p>세션 연결이 끊어진 후 실행해야 하는 명령 목록 또는 명령 스크립트를 지정합니다.</p> <p>기본적으로 지정되는 목록은 없습니다.</p> <p>동등한 Windows 레지스트리 값은 CommandsToRunOnReconnect입니다.</p>
CommandsToRunOnReconnect	<p>연결이 끊긴 후 세션이 다시 연결될 때 실행될 명령 스크립트 또는 명령 목록을 지정합니다.</p> <p>기본적으로 지정되는 목록은 없습니다.</p> <p>동등한 Windows 레지스트리 값은 CommandsToRunOnDisconnect입니다.</p>

표 4-1. View Agent(Horizon 6용) 또는 Horizon Agent(Horizon 7용) 구성 템플릿의 보안 관련 설정 (계속)

설정	설명
ConnectionTicketTimeout	Horizon 연결 티켓이 유효한 시간을 초로 지정합니다. Horizon Client 디바이스는 에이전트에 연결할 때 확인 및 Single Sign-On을 위해 연결 티켓을 사용합니다. 보안상의 이유로 연결 티켓은 제한된 시간 동안 유효합니다. 사용자가 원격 데스크톱에 연결할 경우 연결 티켓 시간 초과 기간 또는 세션 시간 초과 내에 인증이 실행되어야 합니다. 이 설정이 구성되지 않을 경우 기본 시간 초과 기간은 900초입니다. 동등한 Windows 레지스트리 값은 VdmConnectionTicketTimeout입니다.
CredentialFilterExceptions	CredentialFilter 에이전트 로드에서 허용되지 않는 실행 파일을 지정합니다. 파일 이름에는 경로 또는 접미사가 포함될 수 없습니다. 세미콜론을 사용하여 여러 파일 이름을 구분합니다. 기본적으로 지정되는 목록은 없습니다. 동등한 Windows 레지스트리 값은 CredentialFilterExceptions입니다.

이러한 설정 및 각 설정이 보안에 미치는 영향에 대한 자세한 내용은 "View 관리" 설명서를 참조하십시오.

Linux 데스크톱의 구성 파일에서 옵션 설정

/etc/vmware/config 또는 /etc/vmware/viewagent-custom.conf 파일에 항목을 추가하여 특정 옵션을 구성할 수 있습니다.

Horizon Agent를 설치하는 동안 설치 관리자가 두 개의 구성 템플릿 파일 config.template 및 viewagent-custom.conf.template을 /etc/vmware에 복사합니다. 또한, /etc/vmware/config 및 /etc/vmware/viewagent-custom.conf가 없는 경우에는 설치 관리자가 config.template을 config에 복사하고 viewagent-custom.conf.template을 viewagent-custom.conf에 복사합니다. 템플릿 파일에 모든 구성 옵션이 나열되고 기록됩니다. 옵션을 설정하려면 설명을 제거하고 값을 적절하게 변경합니다.

예를 들어, /etc/vmware/config에서 다음 줄은 무손실 PNG 모드로 빌드되도록 설정합니다.

```
RemoteDisplay.buildToPNG=TRUE
```

구성을 변경하고 나면 변경이 적용되도록 Linux를 재부팅합니다.

/etc/vmware/config의 구성 옵션

VMwareBlastServer 및 관련 플러그인에서는 구성 파일 /etc/vmware/config를 사용합니다.

참고 다음 표에는 Horizon Agent 구성 파일의 USB에 대한 각 에이전트 적용 정책 설정의 설명이 포함되어 있습니다. Horizon Agent는 설정을 사용하여 USB가 호스트 시스템으로 전달될 수 있는지 여부를 결정합니다. 또한 Horizon Agent는 해석 및 강제 적용을 위해 설정을 Horizon Client에 전달합니다. 이러한 강제 적용은 merge (**m**) 수정자를 지정하여 Horizon Client 필터 정책 설정 외에 Horizon Agent 필터 정책 설정을 적용할지 또는 (**o**) 수정자를 사용하여 Horizon Client 필터 정책 설정 대신 Horizon Agent 필터 정책 설정을 사용할지 여부를 기준으로 합니다.

표 4-2. /etc/vmware/config의 구성 옵션

옵션	값/형식	기본값	설명
Clipboard.Direction	0, 1, 2, 또는 3	2	<p>클립보드 리디렉션 정책을 지정하려면 이 옵션을 사용합니다. 유효한 값은 다음과 같습니다.</p> <ul style="list-style-type: none"> ■ 0 - 클립보드 리디렉션을 사용하지 않도록 설정합니다. ■ 1 - 클립보드 리디렉션을 양방향 모두에서 사용하도록 설정합니다. ■ 2 - 클립보드 리디렉션을 클라이언트에서 원격 데스크톱 방향으로만 사용하도록 설정합니다. ■ 3 - 클립보드 리디렉션을 원격 데스크톱에서 클라이언트 방향으로만 사용하도록 설정합니다.
RemoteDisplay.allowAudio	true 또는 false	true	오디오 출력을 사용/사용하지 않으려면 이 옵션을 설정합니다.
RemoteDisplay.allowH264	true 또는 false	true	이 옵션을 설정하여 H.264 인코딩을 사용하거나 사용하지 않도록 설정합니다.
RemoteDisplay.buildToPNG	true 또는 false	false	<p>그래픽 애플리케이션, 특히 그래픽 디자인 애플리케이션에서는 Linux 데스크톱의 클라이언트 디스플레이에서 이미지의 정확한 픽셀 렌더링이 수행되어야 합니다. Linux 데스크톱에서 생성되고 클라이언트 디바이스에서 렌더링되는 이미지 및 비디오 재생을 위해 무손실 PNG 모드 빌드를 구성할 수 있습니다. 이 기능에서는 클라이언트와 ESXi 호스트 사이에 추가 대역폭을 사용합니다. 이 옵션을 사용하도록 설정하면 H.264 인코딩이 사용되지 않도록 설정됩니다.</p>
RemoteDisplay.enableNetworkContinuity	true 또는 false	true	Horizon Agent for Linux에서 네트워크 연속성 기능을 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다.
RemoteDisplay.enableNetworkIntelligence	true 또는 false	true	Horizon Agent for Linux에서 네트워크 인텔리전스 기능을 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다.
RemoteDisplay.enableStats	true 또는 false	false	mks 로그에서 대역폭, FPS, RTT 등과 같은 VMware Blast 디스플레이 프로토콜 통계를 사용하거나 사용하지 않도록 설정합니다.
RemoteDisplay.enableUDP	true 또는 false	true	Horizon Agent for Linux에서 UDP 프로토콜 지원을 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다.
RemoteDisplay.maxBandwidthKbps	정수	1000000	VMware Blast 세션에 대해 초당 킬로비트(kbps)로 최대 대역폭을 지정합니다. 대역폭은 모든 이미징, 오디오, 가상 채널 및 VMware Blast 제어 트래픽을 포함합니다. 유효한 값은 4Gbps(4096000) 미만이어야 합니다.
RemoteDisplay.minBandwidthKbps	정수	256	VMware Blast 세션에 대해 초당 킬로비트(kbps)로 최소 대역폭을 지정합니다. 대역폭은 모든 이미징, 오디오, 가상 채널 및 VMware Blast 제어 트래픽을 포함합니다.

표 4-2. /etc/vmware/config의 구성 옵션 (계속)

옵션	값/형식	기본값	설명
RemoteDisplay.maxFPS	정수	30	화면 업데이트의 최대 속도를 지정합니다. 사용자가 소비하는 평균 대역폭을 관리하려면 이 설정을 사용합니다. 값은 3에서 60 사이여야 합니다. 기본값은 초당 30회 업데이트입니다.
RemoteDisplay.maxQualityJPE G	사용할 수 있는 값 범위: 1-100	90	JPEG/PNG 인코딩의 데스크톱 디스플레이 이미지 품질을 지정합니다. 높은 품질 설정은 더 정적이어서 이미지 품질이 더 좋은 화면 영역에 사용됩니다.
RemoteDisplay.midQualityJPE G	사용할 수 있는 값 범위: 1-100	35	JPEG/PNG 인코딩의 데스크톱 디스플레이 이미지 품질을 지정합니다. 데스크톱 디스플레이의 보통 품질 설정에 사용됩니다.
RemoteDisplay.minQualityJPE G	사용할 수 있는 값 범위: 1-100	25	JPEG/PNG 인코딩의 데스크톱 디스플레이 이미지 품질을 지정합니다. 낮은 품질 설정은 스크롤이 발생하는 경우와 같이 자주 변경되는 화면 영역에 사용됩니다.
RemoteDisplay.qpmaxH264	사용할 수 있는 값 범위: 0-51	36	이 옵션을 사용하여 H.264 인코딩을 사용하도록 구성된 원격 디스플레이에서 최상의 이미지 품질을 지정하는 H264minQP 양자화 매개 변수를 설정합니다. RemoteDisplay.qpminH264에 설정된 값보다 큰 값을 설정합니다.
RemoteDisplay.qpminH264	사용할 수 있는 값 범위: 0-51	10	이 옵션을 사용하여 H.264 인코딩을 사용하도록 구성된 원격 디스플레이에서 최저 이미지 품질을 지정하는 H264maxQP 양자화 매개 변수를 설정합니다. RemoteDisplay.qpmaxH264에 설정된 값보다 작은 값을 설정합니다.
UsbRedirPlugin.log.logLevel	error, warn, info, debug, trace 또는 verbose	info	USB 리디렉션 플러그인의 로그 수준을 설정하려면 이 옵션을 사용합니다.
UsbRedirServer.log.logLevel	error, warn, info, debug, trace 또는 verbose	info	USB 리디렉션 서버의 로그 수준을 설정하려면 이 옵션을 사용합니다.
VMWPKcs11Plugin.log.enable	true 또는 false	false	True SSO 기능에 대해 로깅 모드를 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다.
VMWPKcs11Plugin.log.logLevel	error, warn, info, debug, trace 또는 verbose	info	True SSO 기능의 로그 수준을 설정하려면 이 옵션을 사용합니다.
VVC.RTAV.Enable	true 또는 false	true	오디오 입력을 사용/사용하지 않으려면 이 옵션을 설정합니다.
VVC.ScRedir.Enable	true 또는 false	true	스마트 카드 리디렉션을 사용/사용하지 않으려면 이 옵션을 설정합니다.
VVC.logLevel	fatal error, warn, info, debug 또는 trace	info	VVC 프록시 노드의 로그 수준을 설정하려면 이 옵션을 사용합니다.
cdrrserver.cacheEnable	true 또는 false	true	에이전트에서 클라이언트 측으로의 쓰기 캐싱 기능을 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다.

표 4-2. /etc/vmware/config의 구성 옵션 (계속)

옵션	값/형식	기본값	설명
cdrserver.customizedSharedFolderPath	folder_path	/home/	<p>이 옵션을 사용하여 CDR(클라이언트 드라이브 리더렉션) 공유 폴더 위치를 기본 /home/user/tsclient 디렉토리에서 사용자 지정 디렉토리로 변경합니다.</p> <p>예를 들어, 사용자 test가 CDR 공유 폴더를 /home/test/tsclient 대신 /mnt/test/tsclient에 배치하려는 경우</p> <p>cdrserver.customizedSharedFolderPath=/mnt/를 지정할 수 있습니다.</p> <p>참고 이 옵션을 적용하려면 지정된 폴더가 존재하고 올바른 사용자 사용 권한으로 구성되어야 합니다.</p>
cdrserver.forcedByAdmin	true 또는 false	false	클라이언트가 cdrserver.shareFolders 옵션에 지정되지 않은 추가 폴더를 공유할 수 있는지 여부를 제어하려면 이 옵션을 설정합니다.
cdrserver.logLevel	error, warn, info, debug, trace 또는 verbose	info	vmware-CDRserver.log 파일의 로그 수준을 설정하려면 이 옵션을 사용합니다.
cdrserver.permissions	R	RW	<p>Horizon Client가 공유하는 폴더에 대해 Horizon Agent가 갖는 추가 읽기/쓰기 사용 권한을 적용하려면 이 옵션을 사용합니다. 예:</p> <ul style="list-style-type: none"> ■ Horizon Client가 공유하는 폴더에 read 및 write 사용 권한이 있으며 cdrserver.permissions=R을 설정했으면 Horizon Agent는 read 액세스 사용 권한만 갖습니다. ■ Horizon Client가 공유하는 폴더에 read 사용 권한만 있으며 cdrserver.permissions=RW를 설정했으면 Horizon Agent는 read 액세스 권한을 계속 갖습니다. Horizon Agent에서는 Horizon Client에서 설정한 read 전용 특성을 변경할 수 없습니다. Horizon Agent는 쓰기 액세스 권한만 제거할 수 있습니다. <p>일반적인 사용법은 다음과 같습니다.</p> <ul style="list-style-type: none"> ■ cdrserver.permissions=R ■ #cdrserver.permissions=R(항목의 주석 처리를 해제하거나 삭제)
cdrserver.sharedFolders	file_path1,R; file_path2,; file_path3,R; ...	정의되지 않음	<p>클라이언트가 Linux 데스크톱과 공유할 수 있는 폴더에 대한 하나 이상의 파일 경로를 지정합니다. 예:</p> <ul style="list-style-type: none"> ■ Windows 클라이언트: C:\spreadsheets,;D:\Webbooks,R ■ 비 Windows 클라이언트: 트:/tmp/spreadsheets;/tmp/ebooks,;/home/finance,R
collaboration.logLevel	error, info 또는 debug	info	이 옵션을 사용하여 공동 작업 세션에 사용되는 로그 수준을 설정합니다. 로그 수준이 debug이면 collabui 함수에 대한 모든 호출과 collabor 목록 콘텐츠가 기록됩니다.

표 4-2. /etc/vmware/config의 구성 옵션 (계속)

옵션	값/형식	기본값	설명
collaboration.maxCollabors	10보다 작은 정수	5	세션에 가입하도록 초대할 수 있는 공동 작업자의 최대 수를 지정합니다.
collaboration.enableEmail	true 또는 false	true	설치된 e-메일 애플리케이션을 사용하여 공동 작업 초대 보내기를 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다. 이 옵션을 사용하지 않도록 설정된 경우, e-메일 애플리케이션이 설치되어 있더라도 e-메일을 사용하여 공동 작업자를 초대할 수 없습니다.
collaboration.serverUrl	[URL]	정의되지 않음	공동 작업 초대에 포함할 서버 URL을 지정합니다.
collaboration.enableControlPassing	true 또는 false	true	공동 작업자의 Linux 데스크톱 제어를 허용하거나 제한하려면 이 옵션을 설정합니다. 읽기 전용 공동 작업 세션을 지정하려면 이 옵션을 false 로 설정합니다.
mksVNCServer.useUInputButtonMapping	true 또는 false	false	Ubuntu 또는 RHEL 7.x에서 왼쪽 마우스를 지원하도록 설정하려면 이 옵션을 설정합니다. CentOS 및 RHEL 6.x는 왼쪽 마우스를 지원하므로 이 옵션을 설정할 필요가 없습니다.
mksvhan.clipboardSize	정수	1024	이 옵션을 사용하여 복사하여 붙여넣을 클립보드 최대 크기를 지정합니다.
vdpervice.log.logLevel	fatal error, warn, info, debug 또는 trace	info	vdpervice의 로그 수준을 설정하려면 이 옵션을 사용합니다.
viewusb.AllowAudioIn	{m o}::{true false}	정의되지 않음, true와 동일	오디오 입력 디바이스가 리디렉션되도록 허용하거나 허용하지 않으려면 이 옵션을 사용합니다. 예: o:false
viewusb.AllowAudioOut	{m o}::{true false}	정의되지 않음, false와 동일	오디오 출력 디바이스의 리디렉션을 허용하거나 허용하지 않으려면 이 옵션을 설정합니다.
viewusb.AllowAutoDeviceSplitting	{m o}::{true false}	정의되지 않음, false와 동일	복합 USB 디바이스의 자동 분할을 허용하거나 허용하지 않으려면 이 옵션을 설정합니다. 예: m:true
viewusb.AllowDevDescFailsafe	{m o}::{true false}	정의되지 않음, false와 동일	Horizon Client가 구성 또는 디바이스 설명자를 가져오지 못할 경우에도 디바이스가 리디렉션되도록 허용하거나 허용하지 않으려면 이 옵션을 설정합니다. 구성 또는 디바이스 설명자를 가져오지 못할 경우에도 디바이스를 허용하려면 IncludeVidPid 또는 IncludePath 와 같은 Include 필터에 포함하십시오.
viewusb.AllowHIDBootable	{m o}::{true false}	정의되지 않음, true와 동일	HID 부팅 가능 디바이스로도 알려져 있는, 부팅 시에 사용 가능한 키보드 또는 마우스 이외의 입력 디바이스의 리디렉션을 허용하거나 허용하지 않으려면 이 옵션을 사용합니다.
viewusb.AllowKeyboardMouse	{m o}::{true false}	정의되지 않음, false와 동일	통합형 포인팅 디바이스(예: 마우스, 트랙볼 또는 터치패드)를 사용하여 키보드의 리디렉션을 허용하거나 허용하지 않으려면 이 옵션을 설정합니다.

표 4-2. /etc/vmware/config의 구성 옵션 (계속)

옵션	값/형식	기본값	설명
viewusb.AllowSmartcard	{mlo}:{true false}	정의되지 않음, false와 동일	스마트 카드 디바이스가 리디렉션되도록 허용하거나 허용하지 않으려면 이 옵션을 설정합니다.
viewusb.AllowVideo	{mlo}:{true false}	정의되지 않음, true와 동일	비디오 디바이스가 리디렉션되도록 허용하거나 허용하지 않으려면 이 옵션을 사용합니다.
viewusb.DisableRemoteConfig	{mlo}:{true false}	정의되지 않음, false와 동일	USB 디바이스 필터링을 수행할 때 Horizon Agent 설정을 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다.
viewusb.ExcludeAllDevices	{true false}	정의되지 않음, false와 동일	모든 USB 디바이스를 리디렉션에 포함하거나 리디렉션에서 제외하려면 이 옵션을 사용합니다. true 로 설정되면 기타 정책 설정을 사용하여 특정 디바이스 또는 디바이스 제품군을 리디렉션할 수 있습니다. false 로 설정되면 기타 정책 설정을 사용하여 특정 디바이스 또는 디바이스 제품군이 리디렉션되지 않도록 방지할 수 있습니다. Horizon Agent에서 ExcludeAllDevices 값을 true 로 설정하고 이 설정이 Horizon Client로 전달될 경우, Horizon Agent 설정이 Horizon Client 설정을 재정의합니다.
viewusb.ExcludeFamily	{mlo}:family_name_1[;family_name_2;...]	정의되지 않음	디바이스 제품군을 리디렉션에서 제외하려면 이 옵션을 사용합니다. 예: m:bluetooth;smart-card 자동 디바이스 분할을 사용하도록 설정한 경우 Horizon은 복합 USB 디바이스 각 인터페이스의 디바이스 제품군을 검토하여 제외해야 할 인터페이스를 결정합니다. 자동 디바이스 분할을 사용하지 않도록 설정한 경우, Horizon은 전체 복합 USB 디바이스의 디바이스 제품군을 검토합니다. 참고 기본적으로 마우스 및 키보드는 리디렉션에서 제외되므로 이 설정을 사용하여 제외할 필요가 없습니다.
viewusb.ExcludePath	{mlo}:bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2;...]	정의되지 않음	지정된 허브 또는 포트 경로의 디바이스를 리디렉션에서 제외하려면 이 옵션을 사용합니다. 버스 및 포트 번호를 16진수로 지정해야 합니다. 와일드카드 문자는 경로에 사용할 수 없습니다. 예: m:bus-1/2/3_port-02;bus-1/1/4_port-ff
viewusb.ExcludeVidPid	{mlo}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]	정의되지 않음	지정된 벤더 및 제품 ID를 가진 디바이스를 리디렉션에서 제외하려면 이 옵션을 설정합니다. ID 번호를 16진수로 지정해야 합니다. ID에서 개별 숫자 대신 와일드카드 문자(*)를 사용할 수 있습니다. 예: o:vid-0781_pid-****;vid-0561_pid-554c
viewusb.IncludeFamily	{mlo}:family_name_1[;family_name_2]..	정의되지 않음	리디렉션될 수 있는 디바이스 제품군을 포함하려면 이 옵션을 설정합니다. 예: o:storage; smart-card

표 4-2. /etc/vmware/config의 구성 옵션 (계속)

옵션	값/형식	기본값	설명
viewusb.IncludePath	{mlo}:bus-x1[/y1].../ port-z1;bus-x2[/y2].../ portz2;...]	정의되지 않음	리디렉션될 수 있는 지정된 허브 또는 포트 경로의 디바이스를 포함하려면 이 옵션을 사용합니다. 버스 및 포트 번호를 16진수로 지정해야 합니다. 와일드카드 문자는 경로에 사용할 수 없습니다. 예: m:bus-1/2_port- 02;bus-1/7/1/4_port-0f
viewusb.IncludeVidPid	{mlo}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]	정의되지 않음	리디렉션될 수 있는 지정된 벤더 및 제품 ID를 가진 디바이스를 포함하려면 이 옵션을 설정합니다. ID 번호를 16진수로 지정해야 합니다. ID에서 개별 자릿수 대신 와일드카드 문자(*)를 사용할 수 있습니다. 예: o:vid-***_pid-0001;vid-0561_pid-554c
viewusb.SplitExcludeVidPid	{mlo}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]	정의되지 않음	벤더 및 제품 ID로 분할하여 지정된 복합 USB 디바이스를 제외하거나 포함하려면 이 옵션을 사용합니다. 이 설정의 형식은 vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]입니다. ID 번호는 16진수로 지정해야 합니다. ID에서 개별 자릿수 대신 와일드카드 문자(*)를 사용할 수 있습니다. 예: m:vid-0f0f_pid-55**
viewusb.SplitVidPid	{mlo}: vid-xxxx_pid-yyy[exintf:zz[;exintf:ww]][:...]	정의되지 않음	벤더 및 제품 ID별로 지정된 복합 USB 디바이스의 구성 요소를 개별 디바이스로 처리하려면 이 옵션을 설정합니다. 이 설정의 형식은 vid-xxxx_pid-yyy(exintf:zz[;exintf:ww])입니다. exintf 키워드를 사용하면 인터페이스 번호를 지정하여 구성 요소를 리디렉션에서 제외할 수 있습니다. ID 번호는 16진수로, 인터페이스 번호는 앞에 0이 표시되는 10진수로 지정해야 합니다. ID에서 개별 자릿수 대신 와일드카드 문자(*)를 사용할 수 있습니다. 예: o:vid-0f0f_pid-*** (exintf-01);vid-0781_pid-554c(exintf:01;exintf:02) 참고 Horizon은 명시적으로 제외하지 않은 구성 요소를 자동으로 포함시키지 않습니다. VidPid 디바이스 포함 과 같은 필터 정책을 지정하여 해당 구성 요소를 포함시켜야 합니다.

/etc/vmware/viewagent-custom.conf의 구성 옵션

Java Standalone Agent에서는 구성 파일 /etc/vmware/viewagent-custom.conf를 사용합니다.

표 4-3. /etc/vmware/viewagent-custom.conf의 구성 옵션

옵션	값	기본값	설명
CDREnable	true 또는 false	true	CDR(클라이언트 드라이브 리디렉션) 기능을 사용하거나 사용하지 않도록 설정하려면 이 옵션을 사용합니다.
CollaborationEnable	true 또는 false	true	Linux 데스크톱에서 세션 공동 작업 기능을 사용하거나 사용하지 않도록 설정하려면 이 옵션을 사용합니다.

표 4-3. /etc/vmware/viewagent-custom.conf의 구성 옵션 (계속)

옵션	값	기본값	설명
EndpointVPNEnable	true 또는 false	false	Dynamic Environment Manager 콘솔에서 사용되는 끝점 IP 주소 범위에 대해 끝점 IP 주소를 평가할 때 클라이언트의 물리적 네트워크 카드 IP 주소를 사용할지 또는 VPN IP 주소를 사용할지를 지정하려면 이 옵션을 설정합니다. 이 옵션을 false로 설정하는 경우 클라이언트의 물리적 네트워크 카드 IP 주소가 사용됩니다. 그렇지 않은 경우 VPN IP 주소가 사용됩니다.
HelpDeskEnable	true 또는 false	true	헬프 데스크 도구 기능을 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다.
KeyboardLayoutSync	true 또는 false	true	클라이언트의 시스템 로캘 목록 및 현재 키보드 레이아웃을 Horizon Agent for Linux 데스크톱과 동기화할지 여부를 지정하려면 이 옵션을 사용합니다. 이 설정이 사용되도록 설정되거나 구성되지 않은 경우, 동기화가 허용됩니다. 이 설정이 사용되지 않도록 설정되면 동기화가 허용되지 않습니다. 이 기능은 Windows용 Horizon Client에서만 지원되고 영어, 프랑스어, 독일어, 일본어, 한국어, 스페인어, 중국어 간체 및 중국어 번체 로캘에서만 지원됩니다.
LogCnt	정수	-1	이 옵션을 사용하여 /tmp/vmware-root에서 예약된 로그 파일 수를 설정합니다. <ul style="list-style-type: none"> ■ -1 - 모두 유지 ■ 0 - 모두 삭제 ■ > 0 - 예약된 로그 수
NetbiosDomain	모두 대문자로 된 텍스트 스트링		True SSO를 구성할 때 이 옵션을 사용하여 조직 도메인의 NetBIOS 이름을 설정합니다.
OfflineJoinDomain	pbis 또는 samba	pbis	이 옵션을 사용하여 인스턴트 클론 오프라인 도메인 가입을 설정합니다. 오프라인 도메인 가입을 수행하는 데 사용할 수 있는 방법은 PBISO(PowerBroker Identity Services Open) 인증 및 Samba 오프라인 도메인 가입입니다. 이 속성값이 pbis 또는 samba가 아닌 경우 오프라인 도메인 가입은 무시됩니다.

표 4-3. /etc/vmware/viewagent-custom.conf의 구성 옵션 (계속)

옵션	값	기본값	설명
RunOnceScript			<p>복제된 가상 시스템을 Active Directory에 다시 가입하려면 이 옵션을 사용합니다.</p> <p>호스트 이름이 변경된 후에 RunOnceScript 옵션을 설정합니다. 지정된 스크립트는 첫 번째 호스트 이름이 변경된 후에만 실행됩니다. 스크립트는 에이전트 설치 후에 에이전트 서비스가 시작되고 호스트 이름이 변경되면 루트 사용 권한으로 실행됩니다.</p> <p>예를 들어 Winbind 솔루션의 경우 winbind를 사용하여 기본 가상 시스템을 Active Directory에 가입시키고 이 옵션을 스크립트 경로로 설정해야 합니다. 스크립트에는 도메인 다시 가입 명령(/usr/bin/net ads join -U <ADUserName> %<ADUserPassword>)이 포함되어야 합니다. VM 복제 후에 운영 체제 사용자 지정에 따라 호스트 이름이 변경됩니다. 에이전트 서비스가 시작되면 복제된 가상 시스템을 Active Directory에 가입시키기 위해 이 스크립트가 실행됩니다.</p>
RunOnceScriptTimeout		120	<p>RunOnceScript 옵션의 시간 초과 값을 초 단위로 설정하려면 이 옵션을 사용합니다.</p> <p>예를 들어 RunOnceScriptTimeout=120을 설정합니다.</p>
SSLCiphers	텍스트 문자열	!aNULL:KECDH +AESGCM:ECDH +AESGCM:RSA +AESGCM:KECDH +AES:ECDH+AES:RSA +AES	<p>암호 목록을 지정하려면 이 옵션을 사용합니다. https://www.openssl.org/docs/manmaster/man1/ciphers.html에 정의된 형식을 사용해야 합니다.</p>
SSLProtocols	텍스트 문자열	TLSv1_1:TLSv1_2	<p>보안 프로토콜을 지정하려면 이 옵션을 사용합니다. 지원되는 프로토콜은 TLSv1.0, TLSv1.1 및 TLSv1.2입니다.</p>
SSODesktopType	UseGnomeClassic/A, UseGnomeFlashback, UseGnomeUbuntu, UseMATE 또는 UseKdePlasma		<p>SSO가 사용되도록 설정되면 이 옵션은 기본 데스크톱 환경 대신 사용할 데스크톱 환경을 지정합니다.</p> <p>데스크톱 환경을 사용하도록 지정하기 전에 선택한 데스크톱 환경이 데스크톱에 설치되어 있는지 확인해야 합니다.</p> <p>Ubuntu 16.04/18.04 데스크톱에서 이 옵션을 설정하면 SSO 기능이 사용되도록 설정되었는지에 관계없이 이 옵션이 적용됩니다. RHEL.x/CentOS 7.x 데스크톱에서 이 옵션을 지정한 경우 SSO가 사용되도록 설정된 경우에만 선택한 데스크톱 환경이 사용됩니다.</p> <p>참고 이 옵션은 RHEL/CentOS 8.0 및 RHEL/CentOS 6.x 데스크톱에서 지원되지 않습니다. Horizon 7은 RHEL/CentOS 8.0 데스크톱에서 Gnome 데스크톱 환경만 지원합니다. RHEL/CentOS 6.x 데스크톱에서 SSO가 사용되도록 설정된 경우 KDE를 기본 데스크톱 환경으로 설정하는 방법에 대한 자세한 내용은 #unique_20/unique_20_Connect_42_section_F8FCD42564F3457A9491B067F9F65276의 내용을 참조하십시오.</p>
SSOEnable	true 또는 false	true	<p>SSO(Single Sign On)를 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다.</p>

표 4-3. /etc/vmware/viewagent-custom.conf의 구성 옵션 (계속)

옵션	값	기본값	설명
SSOUserFormat	텍스트 문자열	[username]	<p>Single Sign-On에 로그인 이름 형식을 지정하려면 이 옵션을 사용합니다. 기본값은 사용자 이름만입니다. 도메인 이름도 필요한 경우 이 옵션을 설정합니다. 일반적으로 로그인 이름은 도메인 이름과 특수 문자 뒤에 사용자 이름을 추가한 것입니다. 특수 문자가 백슬래시인 경우에는 백슬래시를 하나 더 사용해서 이스케이프 처리해야 합니다. 로그인 이름 형식의 예는 다음과 같습니다.</p> <ul style="list-style-type: none"> ■ SSOUserFormat=[domain]\\[username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain]
서브넷	CIDR IP 주소 형식	[subnet]	<p>다른 시스템이 Horizon Agent for Linux에 연결하는 데 사용할 수 있는 서브넷에 이 옵션을 설정합니다. 서브넷이 서로 다른 둘 이상의 로컬 IP 주소가 있는 경우 구성된 서브넷의 로컬 IP 주소가 Horizon Agent for Linux에 연결하는 데 사용됩니다. CIDR IP 주소 형식으로 값을 지정해야 합니다. 예: Subnet=123.456.7.8/24.</p>
UEMEnable	true 또는 false	false	<p>Dynamic Environment Manager 스마트 정책을 사용하거나 사용하지 않도록 설정하려면 이 옵션을 설정합니다. 이 옵션을 사용하도록 설정하고 Dynamic Environment Manager 스마트 정책에 대한 조건이 충족되면 정책이 적용됩니다.</p>
UEMNetworkPath	텍스트 문자열		<p>이 옵션을 User Environment Manager 콘솔에서 설정된 동일한 네트워크 경로로 설정해야 합니다. 경로는 //10.111.22.333/view/LinuxAgent/UEMConfig와 유사한 형식이어야 합니다.</p>

참고 세 개의 보안 옵션 SSLCiphers, SSLProtocols 및 SSLCipherServerPreference는 VMwareBlastServer 프로세스에 사용됩니다. VMwareBlastServer 프로세스를 시작할 때 Java Standalone Agent는 다음과 같은 옵션을 매개 변수로 전달합니다. BSG(Blast 보안 게이트웨이)가 사용하도록 설정된 경우 이러한 옵션은 BSG와 Linux 데스크톱 사이의 연결에 영향을 줍니다. BSG가 사용하도록 설정된 경우 이러한 옵션은 클라이언트와 Linux 데스크톱 사이의 연결에 영향을 줍니다.

HTML Access에 대한 그룹 정책 설정

HTML Access에 대한 그룹 정책 설정은 vdm_blast.adm 및 vdm_blast.admx라는 ADM 및 ADMX 템플릿 파일에 지정됩니다. 이 템플릿은 HTML Access에서 사용하는 유일한 디스플레이 프로토콜인 VMware Blast 디스플레이 프로토콜용입니다.

HTML Access 4.0 이상 및 Horizon 7 버전 7.x의 경우 VMware Blast 그룹 정책 설정은 "Horizon 7에서 원격 데스크톱 기능 구성" 문서의 "VMware Blast 정책 설정"에 설명되어 있습니다.

HTML Access 3.5 이하 버전과 Horizon 6 버전 6.2.x 이하 버전이 있는 경우 HTML Access에 적용되는 그룹 정책 설정이 다음 표에 설명되어 있습니다. Horizon 7 버전 7.x 이상에서는 더 많은 VMware Blast 그룹 정책 설정을 사용할 수 있습니다.

표 4-4. HTML Access 3.5 이하 및 Horizon 6 버전 6.2.x 이하 버전에 대한 그룹 정책 설정

설정	설명
화면 공백 표시	<p>HTML Access 세션 동안 Horizon 6 외부에서 원격 가상 시스템을 볼 수 있는지 여부를 제어합니다. 예를 들어 관리자는 vSphere Web Client를 사용하여 사용자가 HTML Access를 통해 데스크톱에 연결되어 있는 동안 가상 시스템에서 콘솔을 열 수 있습니다.</p> <p>이 설정이 사용하도록 설정되어 있거나 구성되어 있지 않고 HTML Access 세션이 활성화되어 있는 동안 어떤 사용자가 Horizon 6의 외부에서 원격 가상 시스템에 액세스하려고 하면, 원격 가상 시스템에 빈 화면이 표시됩니다.</p>
세션 가비지 수집	<p>중단된 원격 세션의 가비지 수집을 제어합니다. 이 설정이 활성화되어 있으면 가비지 수집 간격 및 임계값을 구성할 수 있습니다.</p> <p>간격은 가비지 수집기가 실행되는 빈도를 제어합니다. 간격을 밀리초로 설정합니다.</p> <p>임계값은 세션이 삭제 대상이 되기 전에 중단된 후 경과해야 하는 시간을 결정합니다. 임계값을 초로 설정합니다.</p>
클립보드 리디렉션 구성	<p>클립보드 리디렉션이 허용되는 방향을 결정합니다. 텍스트만 복사 및 붙여넣을 수 있습니다. 다음 값 중 하나를 선택할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 클라이언트에서 서버로만 활성화(즉, 클라이언트 시스템에서 원격 데스크톱으로 복사 및 붙여넣기만 가능합니다.) ■ 양방향으로 비활성화 ■ 양방향으로 사용 ■ 서버에서 클라이언트로만 활성화(즉, 원격 데스크톱에서 클라이언트 시스템으로 복사 및 붙여넣기만 가능합니다.) <p>이 설정은 View Agent 또는 Horizon Agent에만 적용됩니다.</p> <p>이 설정이 비활성화되어 있거나 구성되어 있지 않을 경우 기본값은 클라이언트에서 서버로만 활성화입니다.</p>
HTTP 서비스	<p>Blast Agent 서비스에 대해 보안된(HTTPS) TCP 포트를 변경할 수 있습니다. 기본 포트는 22443입니다.</p> <p>포트 번호를 변경하도록 이 설정을 활성화합니다. 이 설정을 변경하는 경우 영향을 받는 원격 데스크톱(View Agent 또는 Horizon Agent가 설치된 데스크톱)의 방화벽 설정도 업데이트해야 합니다.</p>

Horizon Client 구성 템플릿의 보안 설정

보안 관련 설정은 Horizon Client용 ADM 및 ADMX 템플릿 파일의 보안 섹션 및 스크립팅 정의 섹션에서 제공됩니다. ADM 템플릿 파일 이름은 `vdm_client.adm`으로 지정되고 ADMX 템플릿 파일 이름은 `vdm_client.admx`로 지정됩니다. 다른 설명이 없는 한, 설정에는 컴퓨터 구성 설정만 포함됩니다. 사용자 구성 설정을 사용할 수 있고 그 값을 정의할 경우, 동등한 컴퓨터 구성 설정이 무시됩니다.

다음 표에서는 ADM 및 ADMX 템플릿 파일의 보안 섹션에 있는 설정에 대해 설명합니다.

표 4-5. Horizon Client 구성 템플릿: 보안 설정

설정	설명
Allow command line credentials (컴퓨터 구성 설정)	<p>사용자 자격 증명을 Horizon Client 명령줄 옵션으로 제공할 수 있는지 여부를 지정합니다. 이 설정이 사용되지 않도록 설정된 경우 사용자가 명령줄에서 Horizon Client를 실행할 때 smartCardPIN 및 password 옵션을 사용할 수 없습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p> <p>동등한 Windows 레지스트리 값은 AllowCmdLineCredentials입니다.</p>
Servers Trusted For Delegation (컴퓨터 구성 설정)	<p>사용자가 현재 사용자로 로그인 확인란을 선택할 때 전달된 사용자 ID 및 자격 증명 정보를 허용하는 연결 서버 인스턴스를 지정합니다. 연결 서버 인스턴스를 지정하지 않을 경우, 모든 연결 서버 인스턴스는 이 정보를 허용합니다.</p> <p>연결 서버 인스턴스를 추가하려면 다음 형식 중 하나를 사용하십시오.</p> <ul style="list-style-type: none"> ■ domain\system\$ ■ system\$@domain.com ■ 연결 서버 서비스의 서비스 사용자 이름 (SPN). <p>동등한 Windows 레지스트리 값은 BrokersTrustedForDelegation입니다.</p>
Certificate verification mode (컴퓨터 구성 설정)	<p>Horizon Client에서 수행되는 인증서 검사 수준을 구성합니다. 다음 모드 중 하나를 선택할 수 있습니다.</p> <ul style="list-style-type: none"> ■ No Security. 인증서를 검사하지 않습니다. ■ Warn But Allow. 연결 서버 호스트가 자체 서명된 인증서를 제공하는 경우 경고가 나타나지만 사용자는 연결 서버에 계속 연결할 수 있습니다. 인증서 이름이 Horizon Client에서 사용자가 제공한 연결 서버 이름과 일치할 필요는 없습니다. 다른 인증서 오류 조건이 발생할 경우, 오류 대화상자가 표시되고 사용자가 연결 서버에 연결할 수 없게 됩니다. Warn But Allow이 기본값입니다. ■ Full Security. 임의 유형의 인증서 오류가 발생할 경우 사용자는 연결 서버에 연결할 수 없습니다. 인증서 오류가 표시됩니다. <p>이 그룹 정책 설정이 구성되면 사용자는 Horizon Client에서 선택한 인증서 확인 모드를 볼 수 있지만 설정을 구성할 수는 없습니다. SSL 구성 대화 상자는 사용자에게 관리자가 설정을 차단했다고 알립니다.</p> <p>이 설정이 구성되지 않았거나 사용하지 않도록 설정된 경우, Horizon Client 사용자는 인증서 확인 모드를 선택할 수 있습니다.</p> <p>인증서 확인 설정을 그룹 정책으로 구성하지 않으려면 Windows 레지스트리 설정을 수정하여 인증서 확인을 사용하도록 설정할 수도 있습니다.</p>
Default value of the 'Log in as current user' checkbox (컴퓨터 및 사용자 구성 설정)	<p>Horizon Client 연결 대화 상자에서 현재 사용자로 로그인 확인란의 기본값을 지정합니다.</p> <p>이 설정은 Horizon Client 설치 시 지정한 기본값을 재정의합니다.</p> <p>사용자가 Horizon Client를 명령줄에서 실행하고 logInAsCurrentUser 옵션을 지정하면 해당 값이 이 설정을 재정의합니다.</p> <p>현재 사용자로 로그인 확인란이 선택된 경우, 클라이언트 시스템에 로그인할 때 사용자가 제공한 ID 및 자격 증명 정보가 연결 서버 인스턴스에 전달되고 최종적으로 원격 데스크톱에 전달됩니다. 확인란 선택이 해제된 경우 사용자가 원격 데스크톱에 액세스하려면 ID 및 자격 증명 정보를 여러 번 제공해야 합니다.</p> <p>이 설정은 기본적으로 사용하지 않도록 설정됩니다.</p> <p>동등한 Windows 레지스트리 값은 LogInAsCurrentUser입니다.</p>

표 4-5. Horizon Client 구성 템플릿: 보안 설정 (계속)

설정	설명
Display option to Log in as current user (컴퓨터 및 사용자 구성 설정)	<p>이 설정은 현재 사용자로 로그인 확인란이 Horizon Client 연결 대화 상자에 나타나도록 할지 여부를 지정합니다.</p> <p>확인란이 보일 경우, 사용자는 선택 또는 선택을 해제할 수 있고 해당 기본값을 재정의합니다. 이 확인란이 숨겨져 있으면 사용자가 Horizon Client 연결 대화 상자에서 이 기본값을 재정의할 수 없습니다.</p> <p>Default value of the 'Log in as current user' checkbox 정책을 사용하여 현재 사용자로 로그인 확인란의 기본값을 지정할 수 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p> <p>동등한 Windows 레지스트리 값은 LogInAsCurrentUser_Display입니다.</p>
Enable jump list integration (컴퓨터 구성 설정)	<p>이 설정은 Windows 7 이상 시스템의 작업 표시줄에 있는 Horizon Client 아이콘에 점프 목록이 나타나도록 할지 여부를 지정합니다. 점프 목록을 사용하여 사용자는 최근 연결 서버 인스턴스 및 원격 데스크톱에 연결할 수 있습니다.</p> <p>Horizon Client가 공유된 경우, 사용자가 최근 데스크톱의 이름을 보는 것을 원하지 않을 수 있습니다. 이 설정을 사용하지 않도록 설정하여 점프 목록을 사용하지 않도록 설정할 수 있습니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다.</p> <p>동등한 Windows 레지스트리 값은 EnableJumpList입니다.</p>
Enable SSL encrypted framework channel (컴퓨터 및 사용자 구성 설정)	<p>SSL 암호화된 프레임워크 채널을 사용하도록 설정할지 여부를 결정합니다.</p> <ul style="list-style-type: none"> ■ 사용: SSL을 사용하도록 설정합니다. 하지만 원격 데스크톱에서 SSL이 지원되지 않는 경우에는 이전의 암호화되지 않은 연결로 대체될 수 있습니다. ■ 사용 안 함: SSL을 사용하지 않도록 설정합니다. 이 설정은 권장되지 않지만 디버깅 작업이나 터널링되지 않은 채널에 유용할 수 있으며 WAN 가속기 제품에 의해 최적화될 수 있습니다. ■ 강제 적용: SSL을 사용하도록 설정하며, SSL을 지원하지 않는 데스크톱에 대한 연결은 거부됩니다. <p>동등한 Windows 레지스트리 값은 EnableTicketSSLAuth입니다.</p>

표 4-5. Horizon Client 구성 템플릿: 보안 설정 (계속)

설정	설명
Configures SSL protocols and cryptographic algorithms (컴퓨터 및 사용자 구성 설정)	<p>암호화된 SSL 연결이 설정되기 전에 특정 암호화 알고리즘 및 프로토콜의 사용을 제한하는 암호 목록을 구성합니다. 암호 목록은 콜론으로 구분된 하나 이상의 암호 문자열로 구성됩니다.</p> <p>참고 모든 암호 문자열은 대/소문자를 구분합니다.</p> <ul style="list-style-type: none"> ■ Horizon Client 4.10 이상의 기본값은 TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES입니다. ■ Horizon Client 4.2 이상의 기본값은 TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES입니다. ■ Horizon Client 4.0.1 및 4.1의 기본값은 TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH입니다. ■ Horizon Client 4.0의 기본값은 TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH입니다. ■ Horizon Client 3.5의 기본값은 TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH입니다. ■ Horizon Client 3.3 및 3.4의 기본값은 TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH입니다. ■ Horizon Client 3.2 이하에 대한 값은 SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH입니다. <p>Horizon Client 4.10부터 TLS v1.0은 영구적으로 사용되지 않도록 설정되므로 더 이상 지원되지 않습니다.</p> <p>Horizon Client 4.0.1 ~ 4.9에서는 TLS v1.0, TLS v1.1 및 TLS v1.2가 사용되도록 설정되어 있습니다. (SSL v2.0 및 v3.0은 제거됩니다.) 서버와의 TLS v1.0 호환성이 필요하지 않은 경우 TLS v1.0을 사용하지 않도록 설정할 수 있습니다.</p> <p>Horizon Client 4.0에서는 TLS v1.1 및 TLS v1.2가 사용되도록 설정되어 있습니다. (TLS v1.0은 사용하지 않도록 설정되어 있고 SSL v2.0 및 v3.0은 제거됨)</p> <p>Horizon Client 3.5에서는 TLS v1.0, TLS v1.1 및 TLS v1.2가 사용되도록 설정되어 있습니다. (SSL v2.0 및 v3.0은 사용되지 않도록 설정되어 있습니다.)</p> <p>Horizon Client 3.3 및 3.4에서는 TLS v1.0 및 TLS v1.1이 사용되도록 설정되어 있습니다. (SSL v2.0 및 v3.0과 TLS v1.2는 사용하지 않도록 설정되어 있습니다.)</p> <p>Horizon Client 3.2 이하에서는 SSL v3.0도 사용하도록 설정되어 있습니다. SSL v2.0과 TLS v1.2는 사용되지 않도록 설정되어 있습니다.</p> <p>암호 그룹은 128비트 또는 256비트 AES를 사용하며 익명 DH 알고리즘을 제거한 다음 암호화 알고리즘 키 길이 순서로 현재 암호 목록을 정렬합니다.</p> <p>구성에 대한 참조 링크: http://www.openssl.org/docs/apps/ciphers.html</p> <p>동등한 Windows 레지스트리 값은 SSLCipherList입니다.</p> <p>이 설정을 그룹 정책으로 구성하지 않으려면 SSLCipherList 값 이름을 클라이언트 컴퓨터의 다음 레지스트리 키 중 하나에 추가하여 이를 사용하도록 설정할 수도 있습니다.</p> <ul style="list-style-type: none"> ■ 32비트 Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\WClient\Security ■ 64비트 Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\WClient\Security
Enable Single Sign-On for smart card authentication	<p>스마트 카드 인증을 위해 단일 로그인 사용되도록 설정할지 여부를 지정합니다. 단일 로그인을 사용하도록 설정하면 Horizon Client는 암호화된 스마트 카드 PIN을</p>

표 4-5. Horizon Client 구성 템플릿: 보안 설정 (계속)

설정	설명
(컴퓨터 구성 설정)	임시 메모리에 저장한 후에 연결 서버에 제출합니다. 단일 로그온을 사용하지 않도록 설정하면 Horizon Client에 사용자 지정 PIN 대화 상자가 표시되지 않습니다. 동등한 Windows 레지스트리 값은 EnableSmartCardSSO입니다.

다음 표에서는 ADM 및 ADMX 템플릿 파일의 스크립팅 정의 섹션에 있는 설정에 대해 설명합니다.

표 4-6. 스크립팅 정의 섹션의 보안 관련 설정

설정	설명
Connect all USB devices to the desktop on launch	클라이언트 시스템에서 사용할 수 있는 모든 USB 디바이스를 데스크톱을 시작할 때 데스크톱에 연결할지 여부를 지정합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다. 동등한 Windows 레지스트리 값은 connectUSBOnStartup입니다.
Connect all USB devices to the desktop when they are plugged in	클라이언트 시스템에 전원을 공급할 때 USB 디바이스를 데스크톱에 연결할지 여부를 지정합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다. 동등한 Windows 레지스트리 값은 connectUSBOnInsert입니다.
Logon Password	로그인 중 Horizon Client에서 사용하는 암호를 지정합니다. 암호는 Active Directory에 의해 일반 텍스트로 저장됩니다. 이 설정은 기본적으로 정의되어 있지 않습니다. 동등한 Windows 레지스트리 값은 Password입니다.

이러한 설정 및 각 설정이 보안에 미치는 영향에 대한 자세한 내용은 Windows용 Horizon Client 설명서를 참조하십시오.

Horizon Client 인증서 확인 모드 구성

Windows 클라이언트 컴퓨터의 레지스트리 키에 CertCheckMode 값 이름을 추가하여 Horizon Client 인증서 확인 모드를 구성할 수 있습니다.

32비트 Windows 시스템에서 레지스트리 키는 HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDMWClient\Security입니다. 64비트 Windows 시스템에서 레지스트리 키는 HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDMWClient\Security입니다.

다음 값 중 하나를 레지스트리 키에 사용하십시오.

- 0 - 서버 ID 인증서를 확인하지 않음 옵션을 구현합니다.
- 1 - 신뢰할 수 없는 서버에 연결하기 전에 경고 옵션을 구현합니다.
- 2 - 신뢰할 수 없는 서버에 연결하지 않음 옵션을 구현합니다.

인증서 확인 모드 그룹 정책 설정을 구성하여 Horizon Client 인증서 확인 모드를 구성할 수도 있습니다. 레지스트리 키에 그룹 정책 설정 및 CertCheckMode 설정 모두를 구성할 경우 그룹 정책 설정이 레지스트리 키 값보다 우선합니다.

이 그룹 정책 설정 또는 레지스트리 설정이 구성되면 사용자는 Horizon Client에서 선택한 인증서 확인 모드를 볼 수 있지만 설정을 구성할 수는 없습니다.

인증서 확인 모드 그룹 정책 설정 구성에 대한 자세한 내용은 [Horizon Client 구성 템플릿의 보안 설정](#)을 참조하십시오.

로컬 보안 기관 보호 구성

Horizon Client 및 Horizon Agent는 LSA(Local Security Authority) 보호를 지원합니다. LSA 보호는 보호되지 않은 자격 증명이 있는 사용자가 메모리를 읽고 코드를 삽입하지 않도록 방지합니다.

LSA 보호 구성에 대한 자세한 내용은 Microsoft Windows Server 문서를 읽어보시기 바랍니다.

LSA 보호가 Horizon Client 4.4 이하 버전에 대해 구성되어 있는 경우 다음 기능이 작동되지 않습니다.

- 현재 사용자로 로그인

LSA 보호가 Horizon 7 버전 7.2 이전 버전의 Horizon Agent에 대해 구성되어 있는 경우 다음 기능이 작동되지 않습니다.

- 스마트 카드 인증

- True SSO

보안 프로토콜 및 암호 제품군 구성

5

Horizon Client, View Agent/Horizon Agent 및 서버 구성 요소 사이에서 승인 및 제안되는 보안 프로토콜과 암호 그룹을 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 보안 프로토콜과 암호 제품군의 기본 정책
- 특정 클라이언트 유형의 보안 프로토콜 및 암호 제품군 구성
- SSL/TLS에서 취약한 암호 사용 안 함
- HTML Access Agent의 보안 프로토콜 및 암호 제품군 구성
- 원격 데스크톱에서 제안 정책 구성

보안 프로토콜과 암호 제품군의 기본 정책

전역 수락 및 제안 정책은 기본적으로 특정 보안 프로토콜과 암호 제품군을 사용하도록 설정합니다.

다음 표에는 Horizon Client에 대해 기본적으로 사용하도록 설정된 프로토콜 및 암호 그룹이 나와 있습니다. Windows, Linux 및 Mac용 Horizon Client 3.1 이상에서는 이러한 암호 그룹 및 프로토콜이 USB 채널(USB 서비스 데몬과 View Agent 또는 Horizon Agent 사이의 통신) 암호화에도 사용됩니다. 4.0 이전 버전의 Horizon Client에서 USB 서비스 데몬은 원격 데스크톱에 연결할 때 암호 제어 문자열 끝에 RC4 (:RC4-SHA: +RC4)를 추가합니다. Horizon Client 4.0부터는 더 이상 RC4가 추가되지 않습니다.

Horizon Client 4.2 이상

표 5-1. Horizon Client 4.2 이상에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹

기본 보안 프로토콜	기본 암호 제품군
TLS 1.2	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

참고 Horizon Client 4.10부터 TLS v1.0은 영구적으로 사용되지 않도록 설정되므로 더 이상 지원되지 않습니다.

표 5-1. Horizon Client 4.2 이상에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹 (계속)

기본 보안 프로토콜	기본 암호 제품군
	<ul style="list-style-type: none"> ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Horizon Client 4.10부터 TLS v1.0은 영구적으로 사용되지 않도록 설정되므로 더 이상 지원되지 않습니다.

Horizon Client 4.2 ~ 4.9에서 TLS v1.0은 기본적으로 사용하도록 설정되므로, 기본적으로 Horizon Client에서 Horizon Cloud(호스팅된 인프라 이용) 서버에 연결할 수 있습니다. 기본 암호 문자열은 !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES입니다. 서버와의 TLS v1.0 호환성이 필요하지 않은 경우 TLS v1.0을 사용하지 않도록 설정할 수 있습니다.

Horizon Client 4.0.1 및 4.1

표 5-2. Horizon Client 4.0.1 및 4.1에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹

기본 보안 프로토콜	기본 암호 제품군
TLS 1.2	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

표 5-2. Horizon Client 4.0.1 및 4.1에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹 (계속)

기본 보안 프로토콜	기본 암호 제품군
	<ul style="list-style-type: none"> ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

TLS 1.0은 기본적으로 사용하도록 설정되므로 기본적으로 Horizon Client에서 Horizon Cloud(호스팅된 인프라 이용) 서버에 연결할 수 있습니다. 기본 암호 문자열은 TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH입니다. 서버와의 TLS 1.0 호환성이 필요하지 않는 경우 TLS 1.0을 사용하지 않도록 설정할 수 있습니다.

Horizon Client 4.0

표 5-3. Horizon Client 4.0에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹

기본 보안 프로토콜	기본 암호 제품군
TLS 1.2	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

표 5-3. Horizon Client 4.0에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹 (계속)

기본 보안 프로토콜	기본 암호 제품군
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

중요 TLS 1.0이 기본적으로 사용 안 함으로 설정됩니다. SSL 3.0이 제거되었습니다.

Horizon Client 3.5

표 5-4. Horizon Client 3.5에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹

기본 보안 프로토콜	기본 암호 제품군
TLS 1.2	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
■ TLS 1.0	<ul style="list-style-type: none"> ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

표 5-4. Horizon Client 3.5에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹 (계속)

기본 보안 프로토콜	기본 암호 제품군
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Horizon Client 3.3 및 3.4

표 5-5. Horizon Client 3.3 및 3.4에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹

기본 보안 프로토콜	기본 암호 제품군
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
■ TLS 1.0	■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
	■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
	■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
	■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
	■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
	■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

참고 TLS 1.2도 지원되지만 기본적으로 사용하도록 설정되지는 않습니다. TLS 1.2를 사용하도록 설정하려면 [VMware KB 2121183](#)의 지침에 따르며, 그 후에는 [표 5-4. Horizon Client 3.5에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹](#)에 나열된 암호 제품군이 지원됩니다.

Horizon Client 3.0, 3.1 및 3.2

표 5-6. Horizon Client 3.0, 3.1 및 3.2에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹

기본 보안 프로토콜	기본 암호 제품군
■ TLS 1.1	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
■ TLS 1.0	■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
■ SSL 3.0 (Windows 클라이언트에서만 사용하도록 설정됨)	■ TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022)
	■ TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021)
	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
	■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
	■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
	■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
	■ TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA (0xc01f)
	■ TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA (0xc01e)
	■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
	■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
	■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

참고 TLS 1.2도 지원되지만 기본적으로 사용하도록 설정되지는 않습니다. TLS 1.2를 사용하도록 설정하려면 [VMware KB 2121183](#)의 지침에 따르며, 그 후에는 [표 5-4. Horizon Client 3.5에서 기본적으로 사용하도록 설정되는 보안 프로토콜 및 암호 그룹](#)에 나열된 암호 제품군이 지원됩니다.

특정 클라이언트 유형의 보안 프로토콜 및 암호 제품군 구성

각 클라이언트 유형에 따라 사용되는 프로토콜 및 암호 제품군 구성 방법이 다릅니다.

View Server가 현재 설정을 지원하지 않을 때만 Horizon Client에서 보안 프로토콜을 변경해야 합니다. 클라이언트가 연결되는 View Server에서 사용하도록 설정되어 있지 않은 Horizon Client에 대해 보안 프로토콜을 구성할 경우, TLS/SSL 오류가 발생하고 연결이 실패합니다.

프로토콜 및 암호를 기본값에서 변경하려면 클라이언트 측 메커니즘을 사용합니다.

- Windows 클라이언트 시스템에서는 그룹 정책 설정 또는 Windows 레지스트리 설정을 사용할 수 있습니다.
- Windows 10 UWP 클라이언트 시스템에서는 Horizon Client 옵션의 [SSL 옵션] 설정을 사용할 수 있습니다.
- Linux 클라이언트 시스템에서는 구성 파일 속성 또는 명령줄 옵션을 사용할 수 있습니다.
- Mac 클라이언트 시스템에서는 Horizon Client에서 기본 설정을 사용할 수 있습니다.
- iOS, Android 및 Chrome OS 클라이언트 시스템에서는 Horizon Client 설정의 [고급 SSL 옵션] 설정을 사용할 수 있습니다.

자세한 내용은 Horizon Client 설명서를 참조하십시오.

SSL/TLS에서 취약한 암호 사용 안 함

도메인 정책 GPO(그룹 정책 개체)를 구성하면 View Agent 또는 Horizon Agent를 실행하는 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 새로운 그룹 정책을 적용하려면 View Agent 또는 Horizon Agent 시스템을 다시 시작합니다.

HTML Access Agent의 보안 프로토콜 및 암호 제품군 구성

View Agent 6.2부터는 Windows 레지스트리를 편집하여 HTML Access Agent에서 사용하는 암호 제품군을 구성할 수 있습니다. View Agent 6.2.1부터는 사용되는 보안 프로토콜도 구성할 수 있습니다. GPO(그룹 정책 개체)에 구성을 지정할 수도 있습니다.

View Agent 6.2.1 이상 릴리스에서는 기본적으로 HTML Access Agent에서 TLS 1.1 및 TLS 1.2만 사용합니다. 허용되는 프로토콜은 낮은 것에서 높은 것 순으로 TLS 1.0, TLS 1.1 및 TLS 1.2입니다. SSLv3 이하와 같이 오래된 프로토콜은 허용되지 않습니다. 두 개의 레지스트리 값

SslProtocolLow 및 SslProtocolHigh는 HTML Access Agent에서 수락하는 프로토콜의 범위를 결정합니다. 예를 들어 SslProtocolLow=tls_1.0 및 SslProtocolHigh=tls_1.2를 설정하면 HTML Access Agent에서 TLS 1.0, TLS 1.1 및 TLS 1.2를 수락합니다. 기본 설정은 SslProtocolLow=tls_1.1 및 SslProtocolHigh=tls_1.2입니다.

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>의 CIPHER LIST FORMAT 섹션 아래에 정의된 형식을 사용하여 암호 목록을 지정해야 합니다. 다음과 같은 암호 목록이 기본값입니다.

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

절차

- 1 Windows 레지스트리 편집기를 시작합니다.
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config 레지스트리 키로 이동합니다.
- 3 두 개의 새 문자열(REG_SZ) 값, SslProtocolLow 및 SslProtocolHigh를 추가하여 프로토콜의 범위를 지정합니다.

레지스트리 값의 데이터는 tls_1.0, tls_1.1 또는 tls_1.2여야 합니다. 프로토콜을 하나만 사용하도록 설정하려면 두 레지스트리 값 모두에 같은 프로토콜을 지정합니다. 두 레지스트리 값 중에 하나라도 없거나 데이터가 세 가지 프로토콜 중 하나로 설정되지 않은 경우에는 기본 프로토콜이 사용됩니다.

- 4 암호 제품군 목록을 지정하려면 새 문자열(REG_SZ) 값 SslCiphers를 추가합니다.

레지스트리 값의 데이터 필드에 암호 제품군을 입력하거나 붙여 넣습니다. 예를 들면 다음과 같습니다.

```
ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

- 5 Windows 서비스 VMware Blast를 다시 시작합니다.

기본 암호 목록을 사용하도록 되돌리려면 SslCiphers 레지스트리 값을 삭제하고 Windows 서비스 VMware Blast를 다시 시작합니다. 값의 데이터 부분을 삭제하면 HTML Access Agent는 OpenSSL 암호 목록 형식 정의에 따라 모든 암호를 허용할 수 없는 것으로 처리하므로 이를 삭제하지 마십시오.

HTML Access Agent가 시작될 때 프로토콜 및 암호 정보를 로그 파일에 씁니다. 로그 파일을 검사하여 적용 중인 값을 확인할 수 있습니다.

향후 VMware의 진화하는 네트워크 보안 모범 사례에 따라 기본 프로토콜과 암호 제품군이 변경될 수 있습니다.

원격 데스크톱에서 제안 정책 구성

Windows를 실행하는 원격 데스크톱에서 제안 정책을 구성함으로써 연결 서버에 대한 Message Bus 연결의 보안을 관리할 수 있습니다.

연결 서버가 연결 실패 방지를 위해 동일 정책을 수용하도록 구성되어 있는지 확인하십시오.

절차

- 1 원격 데스크톱에서 Windows 레지스트리 편집기를 시작합니다.

2 HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\WConfiguration 레지스트리 키로 이 동합니다.

3 새 문자열(REG_SZ) 값인 ClientSSLSecureProtocols를 추가합니다.

4 **\LIST:protocol_1,protocol_2,...** 형식으로 암호 제품군 목록에 대한 값을 설정합니다.

최신 프로토콜 순으로 프로토콜을 나열합니다. 예:

```
WL IST:TLSv1.2,TLSv1.1,TLSv1
```

5 새 문자열(REG_SZ) 값인 ClientSSLCipherSuites를 추가합니다.

6 **\LIST:cipher_suite_1,cipher_suite_2,...** 형식으로 암호 제품군 목록에 대한 값을 설정합니 다.

이 목록은 가장 선호하는 암호 제품군부터 선호도 순으로 정렬해야 합니다. 예:

```
WL IST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

클라이언트 및 에이전트 로그 파일 위치

6

클라이언트와 에이전트는 구성 요소의 설치 및 작업을 기록하는 로그 파일을 생성합니다.

본 장은 다음 항목을 포함합니다.

- Windows용 Horizon Client 로그
- Mac용 Horizon Client 로그
- Linux용 Horizon Client 로그
- 모바일 디바이스의 Horizon Client 로그
- Windows 시스템의 Horizon Agent 로그
- Linux 데스크톱 로그

Windows용 Horizon Client 로그

로그 파일은 설치, 디스플레이 제어 및 다양한 기능 구성 요소의 문제 해결에 도움이 될 수 있습니다. 그룹 정책 설정을 사용하여 일부 로그 파일의 위치, 표시 수준, 유지 기간을 구성할 수 있습니다.

로그 위치

다음 표의 파일 이름에서 YYYY는 연도, MM은 월, DD는 일, XXXXXX는 번호를 나타냅니다.

표 6-1. Windows용 Horizon Client 로그 파일

로그 유형	디렉토리 경로	파일 이름
설치	C:\Users\W%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
PCoIP 클라이언트 vmware-remotemks.exe 프로 세스에서	C:\Users\W%username%\AppData\Local\Temp	pcoip_client_YYYY_MM_DD_XXXXXX.txt 참고 GPO를 사용하여 로그 수준을 0에서 3(가장 상세)까지로 구성할 수 있습니다. View PCoIP 클라이언트 세션 변수 ADMX 템플릿 파일(pcoip.admx)을 사용합니다. 이 설정은 PCoIP 이벤트 로그 표시 수준 구성 이라고 합니다.

표 6-1. Windows용 Horizon Client 로그 파일 (계속)

로그 유형	디렉토리 경로	파일 이름
Horizon Client UI vmware-view.exe 프로세스에서	C:\Users\%username%\AppData\Local\VMware\WVDMWLogs	vmware-horizon-viewclient-YYYY-MM-DD-XXXXXX.txt 참고 GPO를 사용하여 로그 위치를 구성할 수 있습니다. View 일반 구성 ADMX 템플릿 파일 (vdm_common.admx)을 사용합니다.
Horizon Client 로그 vmware-view.exe 프로세스에서	C:\Users\%username%\AppData\Local\Temp\Wvmware-username-XXXXXX	vmware-cr tbor a-XXXXXX.log
메시지 프레임워크	C:\Users\%username%\AppData\Local\VMware\WVDMWLogs	log-YYYY-MM-DD-XXXXXX.txt debug-YYYY-MM-DD-XXXXXX.txt
원격 MKS(mouse-keyboard-screen) 로그 vmware-remotemks.exe 프로세스에서	C:\Users\%username%\AppData\Local\Temp\Wvmware-username	ViewMP-Client-XXXXXX.log vmware-mks-XXXXXX.log vmware-r deSvc-XXXXXX.log vmware-vvaClient-XXXXXX.log
Tsdr 클라이언트 vmware-remotemks.exe 프로세스에서	C:\Users\%username%\AppData\Local\Temp\Wvmware-username	vmware-ViewTsdr-Client-XXXXXX.log
Tsmmr 클라이언트 vmware-remotemks.exe 프로세스에서	C:\Users\%username%\AppData\Local\Temp\Wvmware-username	vmware-ViewTsmmr-Client-XXXXXX.log
VdpService 클라이언트 vmware-remotemks.exe 프로세스에서	C:\Users\%username%\AppData\Local\Temp\Wvmware-username	vmware-vdpServiceClient-XXXXXX.log
WSNM 서비스 wsnm.exe 프로세스에서	C:\ProgramData\VMware\WVDMWLogs	debug-yyyy-mm-dd-XXXXXX.txt 참고 GPO를 사용하여 로그 위치를 구성할 수 있습니다. View 일반 구성 ADMX 템플릿 파일 (vdm_common.admx)을 사용합니다.
USB 리디렉션 vmware-view-usbd.exe 또는 vmware-remotemks.exe 프로세스에서	C:\ProgramData\VMware\WVDMWLogs	debug-yyyy-mm-dd-XXXXXX.txt Horizon Client 4.4 이상에서는 vmware-view-usbd.exe 프로세스가 제거되고 USBD 프로세스가 vmware-remotemks.exe 프로세스로 이동됩니다. 참고 GPO를 사용하여 로그 위치를 구성할 수 있습니다. View 일반 구성 ADMX 템플릿 파일 vdm_common.admx를 사용합니다.
직렬 포트 리디렉션 vmwsprddpws.exe 프로세스에서	C:\ProgramData\VMware\WVDMWLogs	Serial*.txt Netlink*.txt
스캐너 리디렉션 ftscanmgr.exe 프로세스에서	C:\ProgramData\VMware\WVDMWLogs	Scanner*.txt Netlink*.txt

로그 구성

그룹 정책 설정을 사용하여 일부 구성을 변경할 수 있습니다.

- PCoIP 클라이언트 로그의 경우는 로그 수준을 0에서 3(가장 상세)까지로 구성할 수 있습니다. View PCoIP 클라이언트 세션 변수 ADMX 템플릿 파일(pcoip.admx)을 사용합니다. 이 설정은 **PCoIP 이벤트 로그 표시 수준 구성**이라고 합니다.
- 클라이언트 UI 로그의 경우는 로그 위치, 표시 수준 및 유지 정책을 구성합니다. View 일반 구성 ADMX 템플릿 파일 vdm_common.admx를 사용합니다.
- USB 리디렉션 로그의 경우는 로그 위치, 표시 수준 및 유지 정책을 구성합니다. View 일반 구성 ADMX 템플릿 파일(vdm_common.admx)을 사용합니다.
- WSNM 서비스 로그의 경우는 로그 위치, 표시 수준 및 유지 정책을 구성합니다. View 일반 구성 ADMX 템플릿 파일(vdm_common.admx)을 사용합니다.

명령줄 명령을 사용하여 표시 수준을 설정할 수도 있습니다. C:\Program Files (x86)\VMware\VMware Horizon View Client\WDCT 디렉토리로 이동하여 다음 명령을 입력합니다.

```
support.bat loglevels
```

새 명령 프롬프트 창이 나타나고 표시 수준을 선택하라는 메시지가 표시됩니다.

로그 번들 수집

클라이언트 UI나 명령줄 명령을 사용하여 로그를 .zip 파일로 수집한 후 VMware 기술 지원으로 보낼 수 있습니다.

- **Horizon Client** 창의 옵션 메뉴에서 **지원 정보**를 선택하고, 대화 상자가 나타나면 **지원 데이터 수집**을 클릭합니다.
- 명령줄에서 C:\Program Files (x86)\VMware\VMware Horizon View Client\WDCT 디렉토리로 이동하여 support.bat 명령을 입력합니다.

Mac용 Horizon Client 로그

로그 파일은 설치, 디스플레이 제어 및 다양한 기능 구성 요소의 문제 해결에 도움이 될 수 있습니다. 구성 파일을 생성하여 자세한 표시 수준을 구성할 수 있습니다.

로그 위치

표 6-2. Mac용 Horizon Client 로그 파일

로그 유형	디렉토리 경로	파일 이름
Horizon Client UI	~/Library/Logs/VMware Horizon Client	
PCoIP 클라이언트	~/Library/Logs/VMware Horizon Client	
실시간 오디오-비디오	~/Library/Logs/VMware	vmware-RTAV-pid.log
USB 리디렉션	~/Library/Logs/VMware	

표 6-2. Mac용 Horizon Client 로그 파일 (계속)

로그 유형	디렉토리 경로	파일 이름
VChan	~/Library/Logs/VMware Horizon Client	
원격 MKS(mouse- keyboard-screen) 로그	~/Library/Logs/VMware	
Crtbora	~/Library/Logs/VMware	

로그 구성

Horizon Client 3.1 이상에서 Horizon Client는 Mac 클라이언트의 ~/Library/Logs/VMware Horizon Client 디렉토리에서 로그 파일을 생성합니다. 관리자는 Mac 클라이언트에 있는 /Library/Preferences/com.vmware.horizon.plist 파일에서 키를 설정하여 최대 로그 파일 수와 로그 파일 최대 보관 일 수를 구성할 수 있습니다.

표 6-3. 로그 파일 수집을 위한 속성 목록(plist) 키

키	설명
MaxDebugLogs	최대 로그 파일 수입니다. 최대값은 100입니다.
MaxDaysToKeepLogs	로그 파일의 최대 보관 일수입니다. 이 값은 제한이 없습니다.

조건에 일치하지 않는 파일은 Horizon Client를 시작할 때 삭제됩니다.

MaxDebugLogs 또는 MaxDaysToKeepLogs 키가 com.vmware.horizon.plist 파일에 설정되어 있지 않을 경우 로그 파일의 기본 수는 5이고, 로그 파일을 보관하는 기본 일 수는 7일입니다.

Linux용 Horizon Client 로그

로그 파일은 설치, 디스플레이 제어 및 다양한 기능 구성 요소의 문제 해결에 도움이 될 수 있습니다. 구성 파일을 생성하여 자세한 표시 수준을 구성할 수 있습니다.

로그 위치

표 6-4. Linux용 Horizon Client 로그 파일

로그 유형	디렉토리 경로	파일 이름
설치	/tmp/vmware-root/	.vmware-installer-pid.log vmware-vmis-pid.log
Horizon Client UI	/tmp/vmware-username/	vmware-horizon-client-pid.log
PCoIP 클라이언트	/tmp/teradici-username/	pcoip_client_YYYY_MM_DD_XXXXXX.log
실시간 오디오-비디오	/tmp/vmware-username/	vmware-RTAV-pid.log
USB 리디렉션	/tmp/vmware-root/	vmware-usbarb-pid.log vmware-view-usbd-pid.log

표 6-4. Linux용 Horizon Client 로그 파일 (계속)

로그 유형	디렉토리 경로	파일 이름
VChan	/tmp/vmware- <i>username</i> /	VChan-Client.log 참고 "export VMW_RDPVC_BRIDGE_LOG_ENABLED=1"을 설정하여 RDPVCBridge 로그를 활성화하면 이 로그가 생성됩니다.
원격 MKS(mouse-keyboard-screen) 로그	/tmp/vmware- <i>username</i> /	vmware-mks-pid.log vmware-MKSVchanClient-pid.log vmware-rdeSvc-pid.log
VdpService 클라이언트	/tmp/vmware- <i>username</i> /	vmware-vdpServiceClient-pid.log
Tsdr 클라이언트	/tmp/vmware- <i>username</i> /	vmware-ViewTsdr-Client-pid.log

로그 구성

구성 속성(view.defaultLogLevel)을 사용하여 클라이언트 로그의 세부 표시 수준을 0(모든 이벤트 수집)에서 6(치명적인 이벤트만 수집)까지로 구성할 수 있습니다.

USB용 로그의 경우는 다음과 같은 명령줄 명령을 사용할 수 있습니다.

```
vmware-usbarbitrator --verbose
vmware-view-usbd -o log:trace
```

로그 번들 수집

로그 수집기는 /usr/bin/vmware-view-log-collector에 있습니다. 로그 수집기를 사용하려면 실행 권한이 있어야 합니다. Linux 명령줄에서 다음 명령을 입력하여 권한을 설정할 수 있습니다.

```
chmod +x /usr/bin/vmware-view-log-collector
```

Linux 명령줄에서 다음 명령을 입력하여 로그 수집기를 실행할 수 있습니다.

```
/usr/bin/vmware-view-log-collector
```

모바일 디바이스의 Horizon Client 로그

모바일 디바이스에서는 타사 프로그램을 설치해서 로그 파일이 저장된 디렉토리로 이동해야 할 수도 있습니다. 모바일 클라이언트에는 로그 번들을 VMware로 보내는 구성 설정이 있습니다. 로깅이 성능에 영향을 미칠 수 있으므로 문제 해결이 필요한 경우에만 로깅을 활성화해야 합니다.

iOS 클라이언트 로그

iOS 클라이언트의 경우, 로그 파일은 *User Programs/Horizon/* 아래의 tmp 및 Documents 디렉토리에 있습니다. 이러한 디렉토리로 이동하려면 먼저 iFunbox와 같은 타사 애플리케이션을 설치해야 합니다.

Horizon Client 설정에서 **로깅** 설정을 켜면 로깅을 사용하도록 설정할 수 있습니다. 이 설정이 활성화되어 있으면 클라이언트가 예기치 않게 종료되거나 클라이언트를 종료한 후 다시 실행했을 때 로그 파일이 병합되어 단일 GZ 파일로 압축됩니다. 그 후에 이메일을 통해 번들을 VMware에 보낼 수 있습니다. 디바이스가 PC 또는 Mac에 연결된 경우 iTunes를 사용하여 로그 파일을 검색할 수도 있습니다.

Android 클라이언트 로그

Android 클라이언트의 경우 로그 파일은 `Android/data/com.vmware.view.client.android/files/` 디렉토리에 있습니다. 이 디렉토리로 이동하려면 먼저 File Explorer 또는 My Files와 같은 타사 애플리케이션을 설치해야 합니다.

기본적으로 로그는 애플리케이션이 예기치 않게 종료된 후에만 생성됩니다. Horizon Client 설정에서 **로그 활성화** 설정을 켜면 이 기본값을 변경할 수 있습니다. 이메일을 통해 로그 번들을 VMware로 보내려는 경우는 클라이언트의 일반 설정에 있는 **로그 보내기** 설정을 사용할 수 있습니다.

Chrome OS 클라이언트 로그

Chrome OS 클라이언트의 경우에는 JavaScript 콘솔을 통해서만 로그를 사용할 수 있습니다.

Windows 10 UWP 클라이언트 로그

Windows 10 UWP 클라이언트의 경우 로그는 `C:\Windows\Users\%username%\AppData\Local\VMware\WDM\logs` 디렉토리에 있습니다.

Horizon Client 옵션의 [로깅] 섹션에서 **고급 로깅 설정** 옵션을 켜고 **지원 정보 수집** 버튼을 클릭하여 로깅을 사용하도록 설정할 수 있습니다. 로그의 폴더를 선택하라는 메시지가 표시되며 다른 폴더와 마찬가지로 폴더를 압축할 수 있습니다.

Windows 스토어 클라이언트 로그

Windows용 Horizon Client가 아니라 Windows 스토어용 Horizon Client가 설치되어 있는 Windows 스토어 클라이언트의 경우에는 로그 파일이 `C:\Users\%username%\AppData\Local\WPackages\VMwareInc.VMwareViewClient_23chmsjxv380w\LocalState\logs` 디렉토리에 있습니다.

Horizon Client [일반 설정]에서 **고급 로깅 설정** 설정을 켜고 **지원 정보 수집** 버튼을 클릭하여 로깅을 사용하도록 설정할 수 있습니다. 로그의 폴더를 선택하라는 메시지가 표시되며 다른 폴더와 마찬가지로 폴더를 압축할 수 있습니다.

Windows 시스템의 Horizon Agent 로그

로그 파일은 설치, 디스플레이 제어 및 다양한 기능 구성 요소의 문제 해결에 도움이 될 수 있습니다. 그룹 정책 설정을 사용하여 일부 로그 파일의 위치, 표시 수준, 유지 기간을 구성할 수 있습니다.

로그 위치

다음 표의 파일 이름에서 *YYYY*는 연도, *MM*은 월, *DD*는 일, *XXXXXX*는 번호를 나타냅니다.

표 6-5. Windows용 Horizon Client 로그 파일

로그 유형	디렉토리 경로	파일 이름
설치	C:\Users\%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
View Agent(Horizon 6 용) 또는 Horizon Agent(Horizon 7 용)	<Drive Letter>:\ProgramData\VMware\VMware View Agent\WDCT	pcoip_agent_YYYY_MM_DD_XXXXXX.txt pcoip_agent_YYYY_MM_DD_XXXXXX.txt vmware-vdpServiceServer-XXXXXX.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-XXXXXX.txt
		참고 GPO를 사용하여 로그 위치를 구성할 수 있습니다. View 일반 구성 ADMX 템플릿 파일 vdm_common.admx를 사용합니다.

로그 구성

로그 옵션을 구성하는 방법에는 몇 가지가 있습니다.

- 그룹 정책 설정을 사용하여 일부 로그 위치, 표시 수준, 유지 정책을 구성할 수 있습니다. View 일반 구성 ADMX 템플릿 파일 vdm_common.admx를 사용합니다.
- 명령줄 명령을 사용하여 표시 수준을 설정할 수 있습니다. C:\Program Files\VMware\VMware View Agent\WDCT 디렉토리로 이동하여 support.bat loglevels 명령을 입력합니다. 새 명령 프롬프트 창이 나타나고 표시 수준을 선택하라는 메시지가 표시됩니다.
- vdmadmin 명령을 -A 옵션과 함께 사용하여 View Agent 또는 Horizon Agent에서 로깅을 구성할 수 있습니다. 자세한 내용은 "Horizon 7 관리" 문서를 참조하십시오.

로그 번들 수집

명령줄 명령을 사용하여 로그를 .zip 파일로 수집한 후 VMware 기술 지원으로 보낼 수 있습니다. 명령줄에서 C:\Program Files\VMware\VMware View Agent\WDCT 디렉토리로 이동하여 support.bat 명령을 입력합니다.

Linux 데스크톱 로그

로그 파일은 설치, 디스플레이 제어 및 다양한 기능 구성 요소의 문제 해결에 도움이 될 수 있습니다. 구성 파일을 생성하여 자세한 표시 수준을 구성할 수 있습니다.

로그 위치

표 6-6. Linux 데스크톱 로그 파일

로그 유형	디렉토리 경로
설치	/tmp/vmware-root
View Agent(Horizon 6용) 또는 Horizon Agent(Horizon 7용)	/var/log/vmware
View Agent(Horizon 6용) 또는 Horizon Agent(Horizon 7용)	/usr/lib/vmware/viewagent/viewagent-debug.log

로그 구성

/etc/vmware/config 파일을 편집하여 로깅을 구성합니다.

로그 번들 수집

시스템의 구성 정보 및 로그를 압축된 tarball에 수집하는 DCT(데이터 수집 도구) 번들을 만들 수 있습니다. Linux 데스크톱에서 명령 프롬프트를 열고 dct-debug.sh 스크립트를 실행합니다.

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

tarball은 스크립트가 실행된 디렉토리(현재 작업 디렉토리)에 생성됩니다. 파일 이름에는 ubuntu-12-vdm-sdct-20150201-0606-agent.tgz와 같이 운영 체제, 타임 스탬프 및 기타 정보가 포함됩니다.

이 명령은 /tmp/vmware-root 디렉토리와 /var/log/vmware 디렉토리에서 로그 파일을 수집하며 다음과 같은 시스템 로그 및 구성 파일도 수집합니다.

- /var/log/messages*
- /var/log/syslog*
- /var/log/boot*.log
- /proc/cpuinfo, /proc/meminfo, /proc/vmstat, /proc/loadavg
- /var/log/audit/audit.log*
- /etc/hosts
- /etc/resolv.conf
- /etc/nsswitch.conf
- /var/log/Xorg*
- /etc/X11/xorg.conf
- /usr/lib/vmware/viewagent의 코어 파일
- /var/crash/_usr_lib_vmware_viewagent*의 모든 충돌 파일

보안 패치 적용

7

패치 릴리스에는 View Composer, 연결 서버, View Agent 또는 Horizon Agent 및 다양한 클라이언트 등의 Horizon 6 또는 Horizon 7 구성 요소를 위한 설치 관리자 파일이 포함될 수 있습니다. 적용해야 할 패치 구성 요소는 배포에 필요한 버그 수정에 따라 다릅니다.

필요한 버그 수정에 따라, 다음 순서로 적용 가능한 Horizon 6 또는 Horizon 7 구성 요소를 설치하십시오.

- 1 View Composer
- 2 연결 서버
- 3 View Agent(Horizon 6용) 또는 Horizon Agent(Horizon 7용)
- 4 Horizon Client

서버 구성 요소에 패치를 적용하는 경우에 대한 지침은 "Horizon 7 업그레이드" 문서를 참조하십시오. 본 장은 다음 항목을 포함합니다.

- [View Agent 또는 Horizon Agent에 패치 적용](#)
- [Horizon Client를 위한 패치 적용](#)

View Agent 또는 Horizon Agent에 패치 적용

패치를 적용하려면 해당 패치 버전의 설치 관리자를 다운로드하여 실행해야 합니다.

다음 단계는 연결된 클론 데스크톱 풀의 상위 가상 시스템, 또는 전체 클론 풀의 각 가상 시스템 데스크톱, 또는 가상 시스템 데스크톱 하나만 포함하는 풀의 개별 데스크톱 가상 시스템에서 수행해야 합니다.

사전 요구 사항

패치 설치 관리자를 실행하는 데 사용할 호스트에 권한을 가진 도메인 사용자 계정이 있는지 확인하십시오.

절차

- 1 모든 상위 가상 시스템, 완전 클론 템플릿에 사용되는 가상 시스템, 풀의 완전 클론 및 수동으로 추가한 개별 가상 시스템에 View Agent(Horizon 6용) 또는 Horizon Agent(Horizon 7용)의 패치 버전을 위한 설치 관리자 파일을 다운로드합니다.

VMware에 문의하면 이 다운로드를 위한 지침이 제공됩니다.

- 2 View Agent 또는 Horizon Agent의 패치 릴리스를 위해 다운로드한 설치 관리자를 실행합니다.

참고 Horizon 6 버전 6.2 이상 릴리스에서는 패치를 설치하기 전에 이전 버전을 제거하지 않아도 됩니다.

- 3 View Composer에 대한 패치 적용 준비를 위한 새 가상 시스템의 프로비저닝을 사용하지 않도록 설정한 경우, 프로비저닝을 다시 사용하도록 지정하십시오.
- 4 연결된 클론 데스크톱 풀을 생성하는 데 사용할 상위 가상 시스템의 경우, 가상 시스템의 스냅샷을 생성하십시오.
스냅샷 생성 지침은 vSphere Client 온라인 도움말을 참조하십시오.
- 5 연결된 클론 데스크톱 풀의 경우, 생성한 스냅샷을 사용하여 데스크톱 풀을 재구성합니다.
- 6 Horizon Client에서 패치가 적용된 데스크톱 풀에 로그인할 수 있는지 확인합니다.
- 7 모든 연결된 클론 데스크톱 풀에 대한 임의의 새로 고침 또는 재구성 작업을 취소한 경우 작업 스케줄을 다시 지정합니다.

Horizon Client를 위한 패치 적용

데스크톱 클라이언트 디바이스에서 패치를 적용하려면 해당 패치 버전의 설치 관리자를 다운로드하여 실행해야 합니다. 모바일 클라이언트에서 패치를 적용하려면 Google Play, Windows 스토어 또는 Apple App Store와 같이 애플리케이션을 판매하는 웹 사이트에서 업데이트를 간단히 설치하기만 하면 됩니다.

절차

- 1 각 클라이언트 시스템에서 Horizon Client의 패치 버전 설치 관리자 파일을 다운로드합니다.

VMware에 문의하면 이 다운로드를 위한 지침이 제공됩니다. 또는 <http://www.vmware.com/go/viewclients>의 클라이언트 다운로드 페이지로 이동할 수 있습니다. 앞서 설명한 것처럼 일부 클라이언트의 경우 App Store에서 패치 릴리스를 구할 수 있습니다.

- 클라이언트 디바이스가 Mac 또는 Linux 데스크톱 또는 랩톱일 경우 해당 디바이스에서 기존 클라이언트 소프트웨어 버전을 제거합니다.

애플리케이션을 제거하려면 일반적인 디바이스 특정 방법을 사용하십시오.

참고 Windows용 Horizon Client 3.5 이상 릴리스에서는 Windows 클라이언트에 패치를 설치하기 전에 이전 버전을 제거하지 않아도 됩니다. Windows용 Horizon Client 4.1 이상 릴리스에서는 Horizon Client 온라인 업그레이드 기능을 사용하도록 설정하여 Windows 클라이언트에서 온라인으로 Horizon Client를 업그레이드할 수 있습니다. Mac용 Horizon Client 4.4 이상에서는 Horizon Client 온라인 업그레이드 기능을 사용하도록 설정하여 Mac 클라이언트에서 온라인으로 Horizon Client를 업그레이드할 수 있습니다.

- 해당되는 경우 Horizon Client의 패치 릴리스를 위해 다운로드한 설치 관리자를 실행합니다.

Apple App Store 또는 Google Play에서 패치를 구한 경우, 애플리케이션이 대개 다운로드할 때 설치되어 설치 관리자를 실행할 필요가 없습니다.

- 새로 패치가 적용된 Horizon Client에서 패치가 적용된 데스크톱 풀에 로그인할 수 있는지 확인합니다.