

View Agent Direct- Connection 플러그인 관리

2020년 3월

VMware Horizon 7 7.12



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

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

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

목차

View Agent Direct-Connection 플러그인 관리	4
1 View Agent Direct-Connection 플러그인 설치	5
View Agent Direct-Connection 플러그인 시스템 요구 사항	5
View Agent Direct-Connection 플러그인 설치	6
View Agent Direct-Connection 플러그인 자동 설치	6
2 View Agent Direct-Connection 플러그인 고급 구성	8
View Agent Direct-Connection 플러그인 구성 설정	8
SSL/TLS에서 취약한 암호 사용 안 함	11
기본 자체 서명된 TLS 서버 인증서 교체	12
데스크톱 및 애플리케이션에 대한 Horizon Client 액세스 권한 부여	12
네트워크 주소 변환 및 포트 매핑 사용	13
고급 주소 지정 체계	15
Windows 인증서 저장소에 인증 기관 추가	16
3 HTML Access 설정	17
HTML Access용 Horizon 7 Agent 설치	17
정적 콘텐츠 전송 설정	18
신뢰할 수 있는 CA 서명이 있는 TLS 서버 인증서 설정	19
Windows 10 및 Windows 2016 데스크톱에서 HTTP/2 프로토콜 사용 안 함	20
4 원격 데스크톱 서비스 호스트에 View Agent Direct Connection 설정	21
원격 데스크톱 서비스 호스트	21
게시된 데스크톱 및 애플리케이션에 대한 사용 권한 부여	22
5 View Agent Direct-Connection 플러그인 문제 해결	23
잘못된 그래픽 드라이버가 설치됨	23
비디오 RAM 부족	24
TRACE 및 DEBUG 정보를 포함하도록 전체 로깅 사용	24

View Agent Direct-Connection 플러그인 관리

"View Agent Direct-Connection 플러그인 관리"에서는 View Agent Direct-Connection 플러그인을 설치 및 구성하는 방법에 대한 정보를 제공합니다. 이 플러그인은 Horizon 연결 서버를 사용하지 않고도 Horizon Client에서 가상 시스템 기반 데스크톱, 게시된 데스크톱 또는 애플리케이션에 직접 연결할 수 있도록 해 주는 Horizon Agent의 설치 가능한 확장 프로그램입니다. 모든 데스크톱 및 애플리케이션 기능은 사용자가 연결 서버를 통해 연결했을 때와 동일하게 작동합니다.

대상

이 정보는 가상 시스템 기반 데스크톱 또는 RDS 호스트에 View Agent Direct-Connection 플러그인을 설치, 업그레이드 또는 구성하려는 관리자를 대상으로 합니다. 이 가이드는 가상 시스템 기술과 데이터 센터 운영에 익숙한 숙련된 Windows 시스템 관리자를 대상으로 작성되었습니다.

View Agent Direct-Connection 플러그인 설치

1

VADC(View Agent Direct-Connection) 플러그인을 사용하면 Horizon Client가 가상 시스템 기반 데스크톱, 게시된 데스크톱 또는 애플리케이션에 직접 연결할 수 있습니다. VADC 플러그인은 Horizon 7 Agent의 확장 기능으로, 가상 시스템 기반 데스크톱이나 RDS 호스트에 설치됩니다.

본 장은 다음 항목을 포함합니다.

- View Agent Direct-Connection 플러그인 시스템 요구 사항
- View Agent Direct-Connection 플러그인 설치
- View Agent Direct-Connection 플러그인 자동 설치

View Agent Direct-Connection 플러그인 시스템 요구 사항

VADC(View Agent Direct-Connection) 플러그인은 Horizon 7 Agent가 이미 설치되어 있는 시스템에 설치됩니다. Horizon 7 Agent가 지원하는 운영 체제 목록은 "Horizon 7 설치" 문서의 "Horizon Agent 지원 운영 체제"를 참조하십시오.

VADC 플러그인의 추가 요구 사항은 다음과 같습니다.

- 올바르게 작동하려면 VADC 플러그인이 설치된 가상 또는 물리적 시스템에 최소 128MB의 비디오 RAM이 있어야 합니다.
- 가상 시스템의 경우 Horizon 7 Agent를 설치하기 전에 VMware Tools를 설치해야 합니다.
- 물리적 시스템은 Windows 10 Enterprise 버전 1803 또는 버전 1809를 지원합니다.

VADC 플러그인 지원 프로토콜은 다음과 같습니다.

- VADC 플러그인이 설치된 가상 시스템은 Blast 및 PCoIP 프로토콜을 지원합니다.
- VADC 플러그인이 설치된 물리적 시스템은 Blast 프로토콜만 지원합니다.

참고 VADC를 지원하는 가상 시스템 기반 데스크톱은 Microsoft Active Directory 도메인에 가입하거나 작업 그룹의 구성원일 수 있습니다.

View Agent Direct-Connection 플러그인 설치

VADC(View Agent Direct-Connection) 플러그인은 VMware 웹 사이트에서 다운로드하여 설치할 수 있는 Windows Installer 파일로 패키징됩니다.

사전 요구 사항

- Horizon 7 Agent가 설치되어 있는지 확인합니다. 환경에 Horizon 7 연결 서버가 포함되어 있지 않은 경우 명령줄에서 Horizon 7 Agent를 설치하고 Horizon 7 Agent를 Horizon 7 연결 서버에 등록하지 않도록 지시하는 매개 변수를 지정합니다. [HTML Access용 Horizon 7 Agent 설치](#)의 내용을 참조하십시오.
- vSphere 6.0 이상에서 가상 시스템에 대한 화면 DMA 설정을 사용하도록 설정합니다. 화면 DMA가 비활성화된 경우 원격 데스크톱에 연결하면 검은 화면이 표시됩니다. 화면 DMA 설정 방법에 대한 자세한 내용은 VMware KB(기술 자료) 문서 2144475 <http://kb.vmware.com/kb/2144475>를 참조하십시오.

절차

- 1 VMware 다운로드 페이지(<http://www.vmware.com/go/downloadview>)에서 VADC 플러그인 설치 관리자 파일을 다운로드합니다.

설치 관리자 파일 이름은 64비트 Windows의 경우 VMware-viewagent-direct-connection-x86_64-y.y.y-xxxxxx.exe이고, 32비트 Windows의 경우에는 VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe입니다. 여기서 y.y.y는 버전 번호이고 xxxxxx는 빌드 번호입니다.
- 2 설치 관리자 파일을 두 번 클릭합니다.
- 3 (선택 사항) TCP 포트 번호를 변경합니다.

기본 포트 번호는 443입니다.
- 4 (선택 사항) Windows 방화벽 서비스 구성 방법을 선택합니다.

기본적으로 **자동으로 Windows 방화벽 구성**이 선택되어 있고 설치 관리자는 필요한 네트워크 연결을 허용하도록 Windows 방화벽을 구성합니다.
- 5 (선택 사항) SSL 3.0을 사용하지 않도록 설정할지 여부를 선택합니다.

기본적으로 **SSLv3에 대한 지원을 자동으로 사용하지 않음(권장)**이 선택되어 있고 설치 관리자가 운영 체제 수준에서 SSL 3.0을 사용하지 않도록 설정합니다. SSL 3.0이 레지스트리에서 이미 명시적으로 사용하거나 사용하지 않도록 설정된 경우 이 옵션이 표시되지 않으며 설치 관리자가 아무런 작업을 수행하지 않습니다. 이 옵션이 선택 취소된 경우에도 설치 관리자가 아무런 작업을 수행하지 않습니다.
- 6 표시되는 메시지에 따라 설치를 완료합니다.

View Agent Direct-Connection 플러그인 자동 설치

Microsoft Windows Installer(MSI)의 자동 설치 기능을 사용하여 VADC(View Agent Direct-Connection) 플러그인을 설치할 수 있습니다. 자동 설치에는 명령줄을 사용하여 진행되며 마법사 메시지에 응답하지 않아도 됩니다.

자동 설치를 사용하면 대규모 조직에 VADC 플러그인을 효과적으로 배포할 수 있습니다. Windows Installer에 대한 자세한 내용은 "Horizon 7에서 가상 데스크톱 설정" 문서에서 "Microsoft Windows Installer 명령줄 옵션"을 참조하십시오. VADC 플러그인은 다음과 같은 MSI 속성을 지원합니다.

표 1-1. View Agent Direct-Connection 플러그인 자동 설치를 위한 MSI 속성

MSI 속성	설명	기본 값
LISTENPORT	VADC 플러그인이 원격 연결을 수신하는 데 사용하는 TCP 포트입니다. 기본적으로 설치 관리자는 해당 포트에서 트래픽을 허용하도록 Windows 방화벽을 구성합니다.	443
MODIFYFIREWALL	값을 1로 설정하면 설치 관리자는 LISTENPORT에서 트래픽을 허용하도록 Windows 방화벽을 구성합니다. 값을 0으로 설정하면 설치 관리자가 그렇게 구성하지 않습니다.	1
DISABLE_SSLV3	SSL 3.0이 레지스트리에서 이미 명시적으로 사용하거나 사용하지 않도록 설정된 경우 설치 관리자가 이 속성을 무시합니다. 그렇지 않으면 이 속성이 1로 설정되어 있는 경우 설치 관리자가 운영 체제 수준에서 SSL 3.0을 사용하지 않도록 설정하고, 이 속성이 0으로 설정되어 있는 경우 설치 관리자가 아무런 작업을 수행하지 않습니다.	1

사전 요구 사항

- Horizon Agent가 설치되어 있는지 확인합니다. 환경에 Horizon 연결 서버가 포함되어 있지 않은 경우 명령줄에서 Horizon Agent를 설치하고 Horizon Agent를 Horizon 연결 서버에 등록하지 않도록 지시하는 매개 변수를 지정합니다. [HTML Access용 Horizon 7 Agent 설치](#)를 참조하십시오.

절차

- 1 Windows 명령 프롬프트를 엽니다.
- 2 자동 설치를 지정하는 명령줄 옵션을 사용하여 VADC 플러그인 설치 관리자 파일을 실행합니다. 필요에 따라 추가적인 MSI 속성을 지정할 수도 있습니다.

다음 예에서는 기본 옵션을 사용하여 VADC 플러그인을 설치합니다.

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s
```

다음 예에서는 VADC 플러그인을 설치하면서 vadc가 원격 연결을 수신 대기할 TCP 포트를 지정합니다.

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s /v"/qn LISTENPORT=9999"
```

View Agent Direct-Connection 플러그인 고급 구성

2

기본 View Direct-Connection 플러그인 구성 설정을 사용하거나, Windows Active Directory 그룹 정책 개체 (GPO)를 사용하거나 특정 Windows 레지스트리 설정을 수정하는 방법으로 해당 설정을 사용자 지정할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- View Agent Direct-Connection 플러그인 구성 설정
- SSL/TLS에서 취약한 암호 사용 안 함
- 기본 자체 서명된 TLS 서버 인증서 교체
- 데스크톱 및 애플리케이션에 대한 Horizon Client 액세스 권한 부여
- 네트워크 주소 변환 및 포트 매핑 사용
- Windows 인증서 저장소에 인증 기관 추가

View Agent Direct-Connection 플러그인 구성 설정

VMware View Agent 구성 ADMX 템플릿 파일(view_agent_direct_connection.admx)에 View Agent Direct-Connection 플러그인과 관련된 정책 설정이 포함되어 있습니다.

View Agent Direct-Connection 구성 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 관리 템플릿 > VMware View Agent 구성 > View Agent Direct-Connection**에 있습니다.

표 2-1. View Agent Direct-Connection 플러그인 구성 설정

설정	설명
애플리케이션 사용	이 설정은 원격 데스크톱 세션 호스트에서 애플리케이션을 시작하도록 지원합니다. 기본 설정은 사용입니다.
클라이언트 구성 이름 값 쌍	form name=value 형식을 갖는 클라이언트에 전달될 값 목록입니다. 예: clientCredentialCacheTimeout=1440.
클라이언트 자격 증명 캐시 시간 초과	Horizon Client에서 사용자가 저장된 암호를 사용할 수 있는 시간(분)입니다. 0은 저장된 암호를 다시 사용할 수 없음을 의미하고 -1은 저장된 암호를 항상 다시 사용할 수 있음을 의미합니다. 이 설정에 유효한 값을 설정한 경우 Horizon Client에서는 사용자가 암호를 저장할 수 있는 옵션을 제공합니다. 기본값은 0(허용 안 함)입니다.

표 2-1. View Agent Direct-Connection 플러그인 구성 설정 (계속)

설정	설명
클라이언트 세션 시간 초과	클라이언트가 연결되지 않을 경우 세션이 활성 상태로 유지되는 최대 시간(초)입니다. 기본값은 36000초(10시간)입니다.
클라이언트 설정: AlwaysConnect	이 값은 TRUE 또는 FALSE로 설정할 수 있습니다. AlwaysConnect 설정은 Horizon Client에 전송됩니다. 이 정책을 TRUE로 설정할 경우 저장된 모든 클라이언트 환경설정을 재정의합니다. 기본적으로 값이 설정되지 않습니다. 이 정책을 사용하도록 설정하면 값이 TRUE로 설정됩니다. 이 정책을 사용하지 않도록 설정하면 값이 FALSE로 설정됩니다.
클라이언트 설정: AutoConnect	이 설정은 저장된 모든 Horizon Client 환경설정을 재정의합니다. 기본적으로 값이 설정되지 않습니다. 이 정책을 사용하도록 설정하면 값이 true로 설정되고 이 정책을 사용하지 않도록 설정하면 값이 false로 설정됩니다.
클라이언트 설정: ScreenSize	ScreenSize 설정이 Horizon Client로 전송됩니다. 사용하도록 설정되면 저장된 모든 클라이언트 환경설정이 재정의됩니다. 구성되지 않거나 사용하지 않도록 설정되면 클라이언트 환경설정이 사용됩니다.
기본 프로토콜	Horizon Client에서 데스크톱에 연결하기 위해 사용하는 기본 디스플레이 프로토콜입니다. 값이 설정되지 않으면 기본값은 BLAST입니다.
고지 사항 사용	이 값은 TRUE 또는 FALSE로 설정할 수 있습니다. TRUE로 설정하면 로그인 시 사용자가 수락하도록 고지 사항 텍스트가 표시됩니다. 이 텍스트는 '고지 사항 텍스트'(작성할 경우) 또는 GPO Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interactive logon에서 표시되었습니다. disclaimerEnabled의 기본 설정은 FALSE입니다.
고지 사항 텍스트	로그인 시 Horizon Client 사용자에게 표시되는 고지 사항 텍스트입니다. 고지 사항 사용 정책이 TRUE로 설정되어 있어야 합니다. 텍스트를 지정하지 않으면 Windows 정책 Configuration\Windows Settings\Security Settings\Local Policies\Security Options의 값이 기본적으로 사용됩니다.
외부 Blast 포트	HTML5/Blast 프로토콜에 사용되는 대상 TCP 포트 번호로 Horizon Client에 전송되는 포트 번호입니다. 숫자 앞에 표시되는 + 문자는 HTTPS에 사용되는 포트 번호에 상대적인 번호를 나타냅니다. 이 값은 외부에 노출되는 포트 번호와 서비스가 수신하는 포트가 일치하지 않는 경우에만 설정하십시오. 일반적으로 이 포트 번호는 NAT 환경에 포함됩니다. 기본적으로 값이 설정되지 않습니다.
외부 프레임워크 채널 포트	프레임워크 채널 프로토콜에 사용되는 대상 TCP 포트 번호로 Horizon Client에 전송되는 포트 번호입니다. 숫자 앞에 표시되는 + 문자는 HTTPS에 사용되는 포트 번호에 상대적인 번호를 나타냅니다. 이 값은 외부에 노출되는 포트 번호와 서비스가 수신하는 포트가 일치하지 않는 경우에만 설정하십시오. 일반적으로 이 포트 번호는 NAT 환경에 포함됩니다. 기본적으로 값이 설정되지 않습니다.
외부 IP 주소	보조 프로토콜(RDP, PCoIP, 프레임워크 채널 등)에 사용되는 대상 IP 주소로 Horizon Client에 전송되는 IPV4 주소입니다. 이 값은 외부에 노출되는 주소와 데스크톱 시스템의 주소가 일치하지 않는 경우에만 설정하십시오. 일반적으로 이 주소는 NAT 환경에 포함됩니다. 기본적으로 값이 설정되지 않습니다.
외부 PCoIP 포트	PCoIP 프로토콜에 사용되는 대상 TCP/UDP 포트 번호로 Horizon Client에 전송되는 포트 번호입니다. 숫자 앞에 표시되는 + 문자는 HTTPS에 사용되는 포트 번호에 상대적인 번호를 나타냅니다. 이 값은 외부에 노출되는 포트 번호와 서비스가 수신하는 포트가 일치하지 않는 경우에만 설정하십시오. 일반적으로 이 포트 번호는 NAT 환경에 포함됩니다. 기본적으로 값이 설정되지 않습니다.

표 2-1. View Agent Direct-Connection 플러그인 구성 설정 (계속)

설정	설명
외부 RDP 포트	RDP 프로토콜에 사용되는 대상 TCP 포트 번호로 Horizon Client 에 전송되는 포트 번호입니다. 숫자 앞에 표시되는 + 문자는 HTTPS 에 사용되는 포트 번호에 상대적인 번호를 나타냅니다. 이 값은 외부에 노출되는 포트 번호와 서비스가 수신하는 포트가 일치하지 않는 경우에만 설정하십시오. 일반적으로 이 포트 번호는 NAT 환경에 포함됩니다. 기본적으로 값이 설정되지 않습니다.
HTTPS 포트 번호	플러그인이 Horizon Client 로부터 들어오는 HTTPS 요청을 수신하는 TCP 포트입니다. 이 값을 변경하면 들어오는 트래픽을 허용하도록 Windows 방화벽에서도 해당 값을 변경해야 합니다. 기본값은 443 입니다.
MMR(멀티미디어 리디렉션) 사용	클라이언트 시스템에 대해 MMR 이 사용되도록 설정되어 있는지 여부를 결정합니다. MMR 은 멀티미디어 데이터를 TCP 소켓을 통해 직접 Horizon 데스크톱의 특정 코덱에서 클라이언트 시스템에 전달하는 Microsoft DirectShow 필터입니다. 그런 다음 데이터는 재생되는 클라이언트 시스템에서 바로 디코딩됩니다. 기본값은 사용 안 함입니다. 클라이언트 시스템의 비디오 디스플레이 하드웨어에 오버레이 지원이 없는 경우 MMR 은 올바르게 작동하지 않습니다. 클라이언트 시스템에 로컬 멀티미디어 디코딩을 처리할 만큼 충분한 리소스가 없을 수 있습니다.
재설정 사용	이 값은 TRUE 또는 FALSE 로 설정할 수 있습니다. TRUE 로 설정하면 인증된 Horizon Client 가 운영 체제 수준의 재부팅을 수행할 수 있습니다. 이 정책은 기본적으로 사용하지 않도록 설정됩니다(FALSE).
세션 시간 초과	사용자가 Horizon Client 에 로그인한 후 세션을 열어 둘 수 있는 시간입니다. 분 단위로 값을 설정합니다. 기본값은 600 분입니다. 이 시간 초과 값에 도달하면 사용자의 모든 데스크톱 및 애플리케이션 세션의 연결이 해제됩니다.
USB 자동 연결	이 값은 TRUE 또는 FALSE 로 설정할 수 있습니다. 전원 연결 시 USB 디바이스를 데스크톱에 연결합니다. 이 정책을 설정할 경우, 저장되어 있는 모든 클라이언트 환경설정을 재정의합니다. 기본적으로 값이 설정되지 않습니다.
USB 사용	이 값은 TRUE 또는 FALSE 로 설정할 수 있습니다. 데스크톱에서 클라이언트에 연결된 USB 디바이스를 사용할 수 있는지 여부를 결정합니다. 기본값은 사용입니다. 보안상의 이유로 외부 디바이스의 사용을 차단하려면 이 설정을 사용하지 않도록(FALSE) 변경하십시오.
사용자 유희 시간 초과	여기에 지정한 시간 동안 Horizon Client 에서 사용자의 작업이 없으면 사용자의 데스크톱 및 애플리케이션 세션 연결이 해제됩니다. 초 단위로 값을 설정합니다. 기본값은 900초(15분) 입니다.
X509 인증서 인증	스마트 카드 X.509 인증서 인증이 사용되지 않도록 설정되는지, 허용되는지 또는 필수인지를 결정합니다.
X509 SSL 인증서 인증 사용	스마트 카드 X.509 인증서 인증이 Horizon Client 에서의 직접 SSL 연결을 통해 사용되도록 설정되는지 여부를 결정합니다. X.509 인증서 인증이 중간 SSL 종료 지점을 통해 처리되는 경우에는 이 옵션이 필요하지 않습니다. 이 설정을 변경하려면 Horizon Agent 를 다시 시작해야 합니다.

외부 포트 번호 및 외부 IP 주소 값은 **NAT(네트워크 주소 변환)** 및 포트 매핑을 지원하는 데 사용됩니다. 자세한 내용은 **네트워크 주소 변환 및 포트 매핑 사용** 항목을 참조하십시오.

스마트 카드 인증의 경우 스마트 카드 인증서를 서명하는 CA(인증 기관)가 Windows 인증서 저장소에 있어야 합니다. 인증 기관을 추가하는 방법에 대한 자세한 내용은 [Windows 인증서 저장소에 인증 기관 추가](#) 항목을 참조하십시오.

참고 사용자가 스마트 카드를 사용하여 Windows 7 또는 Windows Server 2008 R2 시스템에 로그인하려고 시도하고 스마트 카드 인증서가 중간 CA에 의해 서명된 경우 Windows가 클라이언트에 중간 CA 이름이 포함되어 있지 않은 신뢰할 수 있는 발급자 목록을 전송할 수 있어 이러한 시도가 실패할 수 있습니다. 이 경우 클라이언트는 적절한 스마트 카드 인증서를 선택할 수 없습니다. 이 문제를 방지하려면 레지스트리 키 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL에서 레지스트리 값 SendTrustedIssuerList(REG_DWORD)를 0으로 설정합니다. 이 레지스트리 값이 0으로 설정되면 Windows가 클라이언트에 신뢰할 수 있는 발급자 목록을 전송하지 않아 스마트 카드에서 모든 유효한 인증서를 선택할 수 있습니다.

SSL/TLS에서 취약한 암호 사용 안 함

보안을 한층 강화하려면 도메인 정책 GPO(그룹 정책 개체)를 구성하여 Horizon Client 및 가상 시스템 기반 데스크톱 또는 RDS 호스트 사이에서 SSL/TLS 프로토콜을 사용하는 통신이 취약한 암호를 허용하지 않도록 할 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 VADC 시스템을 다시 시작합니다.

결과

참고 가상 데스크톱 운영 체제에서 지원하는 모든 암호를 지원하도록 Horizon Client가 구성되어 있지 않으면 TLS/SSL 협상이 실패하여 클라이언트가 연결할 수 없게 됩니다.

Horizon Client에서 지원되는 암호 제품군을 구성하는 방법은 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html에서 Horizon Client 설명서를 참조하십시오.

기본 자체 서명된 TLS 서버 인증서 교체

자체 서명된 TLS 서버 인증서는 임의 변경 및 도청 위험과 관련하여 Horizon Client에 충분한 보호 성능을 제공할 수 없습니다. 이러한 위험으로부터 데스크톱을 보호하려면 생성된 자체 서명된 인증서를 교체해야 합니다.

View Agent Direct-Connection 플러그인을 설치한 후 처음 시작하면 자체 서명된 TLS 서버 인증서가 자동으로 생성되어 Windows 인증서 저장소에 저장됩니다. TLS 서버 인증서는 TLS 프로토콜 협상 중에 클라이언트에 이 데스크톱에 대한 정보를 제공하기 위해 Horizon Client에 제공됩니다. 클라이언트가 신뢰할 수 있고 Horizon Client 인증서 검사를 통해 완전히 검증된 CA(인증 기관)에서 서명한 인증서로 교체하지 않을 경우 이 기본 자체 서명된 TLS 서버 인증서는 이 데스크톱의 안전을 보장할 수 없습니다.

이 인증서를 Windows 인증서 저장소에 저장하는 절차와 적절한 CA 서명 인증서로 교체하는 절차는 Horizon 7 연결 서버에 사용되는 것과 동일합니다. 이 인증서 교체 절차에 대한 자세한 내용은 "Horizon 7 설치" 문서의 "Horizon 7 Server를 위한 TLS 인증서 구성"을 참조하십시오.

제목 대체 이름(SAN)이 있는 인증서와 와일드카드 인증서가 지원됩니다.

참고 View Agent Direct-Connection 플러그인을 사용하여 다수의 데스크톱에 CA 서명 TLS 서버 인증서를 배포하려면 Active Directory 등록을 사용하여 각 가상 시스템에 인증서를 배포하십시오. 자세한 내용은 <http://technet.microsoft.com/en-us/library/cc732625.aspx> 항목을 참조하십시오.

데스크톱 및 애플리케이션에 대한 Horizon Client 액세스 권한 부여

사용자가 데스크톱 및 애플리케이션에 액세스할 수 있게 권한을 부여하는 메커니즘은 **View Agent Direct-Connection 사용자**라고 하는 로컬 운영 체제 그룹 내에서 제어됩니다.

이 그룹의 구성원인 사용자에게는 가상 시스템 기반 데스크톱, 게시된 데스크톱 또는 게시된 애플리케이션에 연결할 수 있는 권한이 부여됩니다. 플러그인을 처음 설치하면 이 로컬 그룹이 생성되고 인증된 사용자 그룹이 기본적으로 포함됩니다. 플러그인을 통해 인증된 모든 사용자는 데스크톱 또는 애플리케이션에 액세스할 수 있는 권한을 갖습니다.

이 데스크톱 또는 RDS 호스트에 대한 액세스를 제한하려면 이 그룹의 구성원 자격을 수정하여 사용자 및 사용자 그룹을 지정하면 됩니다. 여기에 지정하는 사용자는 로컬 또는 도메인의 사용자와 사용자 그룹일 수 있습니다. 사용자가 이 그룹에 속해 있지 않으면 인증 단계가 진행된 후 이 가상 시스템 기반 데스크톱이나 RDS 호스트에서 호스팅되는 게시된 데스크톱과 애플리케이션에 액세스할 수 있는 권한이 없다는 메시지가 표시됩니다.

네트워크 주소 변환 및 포트 매핑 사용

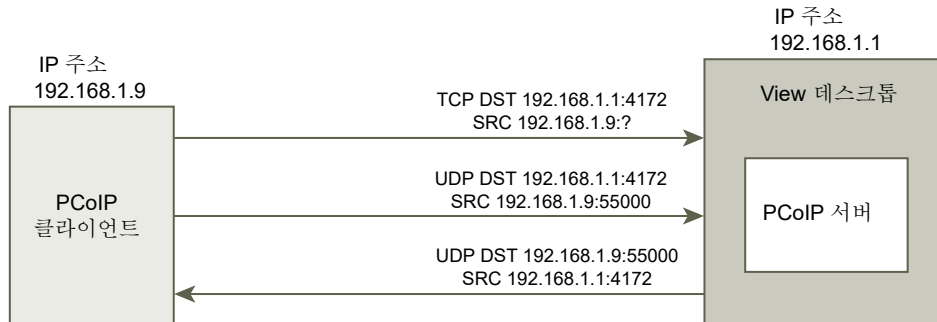
Horizon Client를 여러 네트워크의 가상 시스템 기반 데스크톱에 연결해야 하는 경우에는 NAT(네트워크 주소 변환)와 포트 매핑을 구성해야 합니다.

여기에 포함된 예에서는 Horizon Client가 NAT 또는 포트 매핑 디바이스를 사용하여 데스크톱에 연결할 때 사용할 외부 주소 지정 정보를 데스크톱에 구성해야 합니다. 이 URL은 Horizon 7 연결 서버와 보안 서버에 있는 외부 URL 및 PCoIP 외부 URL 설정과 동일합니다.

Horizon Client가 다른 네트워크에 있고, 플러그인을 실행하는 데스크톱과 Horizon Client 사이에 NAT 디바이스가 있는 경우에는 NAT 또는 포트 매핑 구성이 필요합니다. 예를 들어, Horizon Client와 데스크톱 사이에 방화벽이 있으면 방화벽이 NAT 또는 포트 매핑 디바이스 역할을 합니다.

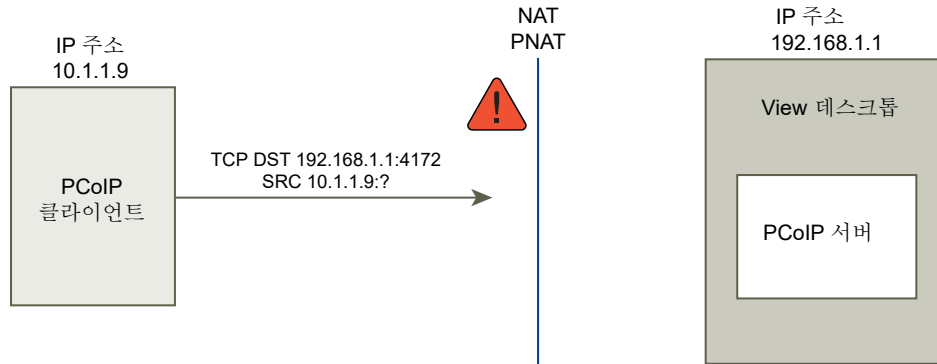
IP 주소가 192.168.1.1인 데스크톱을 배포하는 예에서는 NAT 또는 포트 매핑 구성을 보여 줍니다. 같은 네트워크에서 IP 주소가 192.168.1.9인 Horizon Client 시스템은 TCP 및 UDP를 사용하여 PCoIP 연결을 설정합니다. 이 연결은 NAT 또는 포트 매핑 구성이 없는 직접 연결입니다.

그림 2-1. 같은 네트워크에 있는 클라이언트의 직접 PCoIP



클라이언트와 데스크톱이 서로 다른 주소 공간에서 작동하도록 둘 사이에 NAT 디바이스를 추가한 후 플러그인의 구성을 변경하지 않으면 PCoIP 패킷이 제대로 라우팅되지 않고 오류가 발생합니다. 이 예에서 클라이언트는 다른 주소 공간을 사용하고 IP 주소는 10.1.1.9입니다. 클라이언트가 데스크톱의 주소를 사용하여 TCP 및 UDP PCoIP 패킷을 보내기 때문에 이 설정은 실패합니다. 또한 대상 주소인 192.168.1.1도 클라이언트 네트워크에서 작동하지 않기 때문에 클라이언트에 검은색 화면이 표시될 수 있습니다.

그림 2-2. NAT 디바이스를 통한 클라이언트 PCoIP의 오류

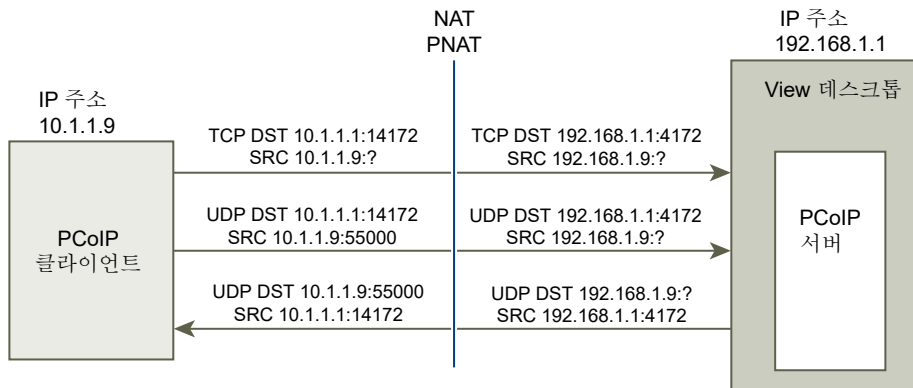


이 문제를 해결하려면 외부 IP 주소를 사용하도록 플러그인을 구성해야 합니다. 이 데스크톱의 `externalIPAddress`가 10.1.1.1로 구성되어 있으면 플러그인은 데스크톱에 데스크톱 프로토콜 연결을 설정할 때 10.1.1.1을 클라이언트 IP 주소로 할당합니다. PCoIP의 경우 이 설정을 사용하려면 데스크톱에서 PCoIP 보안 게이트웨이 서비스를 시작해야 합니다.

포트 매핑의 경우 데스크톱에서는 표준 PCoIP 포트 4172를 사용하지만, 클라이언트가 포트 매핑 디바이스의 포트 4172에 매핑된 다른 대상 포트를 사용해야 할 경우에는 이 설정에 맞게 플러그인을 구성해야 합니다. 포트 매핑 디바이스가 포트 14172를 포트 4172에 매핑할 경우 클라이언트는 PCoIP에 대상 포트 14172를 사용해야 합니다. PCoIP에 대해 이 설정을 구성해야 합니다. 플러그인의 `externalPCoIPPort`를 14172로 설정하십시오.

NAT 및 포트 매핑을 사용하는 구성에서 `externalIPAddress`는 10.1.1.1(네트워크에서 192.168.1.1로 변환됨)로 설정되고, `externalPCoIPPort`는 14172(4172 포트에 매핑됨)로 설정됩니다.

그림 2-3. NAT 디바이스 및 포트 매핑을 통한 클라이언트의 PCoIP



PCoIP를 위한 외부 PCoIP TCP/UDP 포트 구성과 마찬가지로 RDP 포트(3389)나 Framework 채널 포트(32111)를 매핑하는 경우, `externalRDPPort` 및 `externalFrameworkChannelPort`를 구성하여 클라이언트가 포트 매핑 디바이스를 통해 이와 같이 연결하는 데 사용할 TCP 포트 번호를 지정해야 합니다.

고급 주소 지정 체계

동일한 외부 IP 주소에서 NAT 및 포트 매핑 디바이스를 통해 액세스할 수 있도록 가상 시스템 기반 데스크톱을 구성할 경우 고유한 포트 번호 집합을 각 데스크톱에 제공해야 합니다. 그러면 클라이언트가 동일한 대상 IP 주소를 사용하지만 고유한 TCP 포트 번호를 HTTPS 연결에 사용하여 특정 가상 데스크톱에 직접 연결할 수 있습니다.

예를 들어, HTTPS 포트 1000은 한 데스크톱에 연결하고 HTTPS 포트 1005는 다른 데스크톱에 연결하며 둘 다 동일한 대상 IP 주소를 사용하는 경우를 가정해 보겠습니다. 이 경우 데스크톱 프로토콜 연결을 위해 모든 데스크톱에 대해 고유한 외부 포트 번호를 구성하는 것은 너무 복잡합니다. 따라서

`externalIPCoIPPort`, `externalRDPPort` 및 `externalFrameworkChannelPort` 플러그인 설정에서 고정 값 대신 관계식(선택 사항)을 사용하여 클라이언트가 사용하는 기본 HTTPS 포트 번호를 기준으로 포트 번호를 정의할 수 있습니다.

포트 매핑 디바이스가 TCP 443에 매핑된 포트 번호 1000을 HTTPS에, TCP 3389에 매핑된 포트 번호 1001을 RDP에, TCP 및 UDP 4172에 매핑된 포트 번호 1002를 PCoIP에, TCP 32111에 매핑된 포트 번호 1003을 프레임워크 채널에 사용하여 구성을 간소화하는 경우 외부 포트 번호를 `externalRDPPort=+1`, `externalIPCoIPPort=+2` 및 `externalFrameworkChannelPort=+3`으로 구성할 수 있습니다. HTTPS 연결이 HTTPS 대상 포트 번호 1000을 사용한 클라이언트에서 시작되면 이 포트 번호 1000을 기준으로 외부 포트 번호가 자동으로 계산되고 1001, 1002 및 1003이 각각 사용됩니다.

다른 가상 데스크톱을 배포하기 위해 포트 매핑 디바이스가 TCP 443에 매핑된 포트 번호 1005를 HTTPS에, TCP 3389에 매핑된 포트 번호 1006을 RDP에, TCP 및 UDP 4172에 매핑된 포트 번호 1007을 PCoIP에, TCP 32111에 매핑된 포트 번호 1008을 프레임워크 채널에 사용했고 데스크톱에 정확히 동일한 외부 포트 구성(+1, +2, +3 등)이 있는 경우 HTTPS 연결이 HTTPS 대상 포트 번호 1005를 사용한 클라이언트에서 시작되면 이 포트 번호 1005를 기준으로 외부 포트 번호가 자동으로 계산되고 1006, 1007 및 1008이 각각 사용됩니다.

이 체계를 사용하면 모든 데스크톱을 동일하게 구성하지만 모두 동일한 외부 IP 주소를 공유할 수 있습니다. 기본 HTTPS 포트 번호의 경우 포트 번호가 5단위(1000, 1005, 1010 ...)로 할당되므로 동일한 IP 주소에서 12,000개가 넘는 가상 데스크톱에 액세스할 수 있습니다. 기본 포트 번호를 사용하여 포트 매핑 디바이스 구성을 기반으로 연결을 라우팅할 대상이 되는 가상 데스크톱을 결정합니다. 모든 가상 데스크톱에 구성된 `externalIPAddress=10.20.30.40`, `externalRDPPort=+1`, `externalIPCoIPPort=+2` 및 `externalFrameworkChannelPort=+3`의 경우 NAT 및 포트 매핑 테이블에 설명된 대로 가상 데스크톱에 대한 매핑이 이루어집니다.

표 2-2. NAT 및 포트 매핑 값

VM 번호	데스크톱 IP 주소	HTTPS	RDP	PCoIP(TCP 및 UDP)	프레임워크 채널
0	192.168.0.0	10.20.30.40:1000 -> 192.168.0.0:443	10.20.30.40:1001 -> 192.168.0.0:3389	10.20.30.40:1002 -> 192.168.0.0:4172	10.20.30.40:1003 -> 192.168.0.0:32111
1	192.168.0.1	10.20.30.40:1005 -> 192.168.0.1:443	10.20.30.40:1006 -> 192.168.0.1:3389	10.20.30.40:1007 -> 192.168.0.1:4172	10.20.30.40:1008 -> 192.168.0.1:32111

표 2-2. NAT 및 포트 매핑 값 (계속)

VM 번호	데스크톱 IP 주소	HTTPS	RDP	PCoIP(TCP 및 UDP)	프레임워크 채널
2	192.168.0.2	10.20.30.40:1010 -> 192.168.0.2:443	10.20.30.40:1011 -> 192.168.0.2:3389	10.20.30.40:1012 -> 192.168.0.2:4172	10.20.30.40:1013 -> 192.168.0.2:32111
3	192.168.0.3	10.20.30.40:1015 -> 192.168.0.3:443	10.20.30.40:1016 -> 192.168.0.3:3389	10.20.30.40:1017 -> 192.168.0.3:4172	10.20.30.40:1018 -> 192.168.0.3:32111

이 예에서 Horizon Client는 IP 주소 10.20.30.40과 HTTPS 대상 포트 번호($1000 + n * 5$)에 연결합니다. 여기서 n 은 데스크톱 번호입니다. 데스크톱 3에 연결하려면 클라이언트가 10.20.30.40:1015에 연결합니다. 이 주소 지정 체계는 각 데스크톱의 구성 설정을 대폭 간소화합니다. 모든 데스크톱이 동일한 외부 주소 및 포트 구성을 사용하여 구성됩니다. NAT 및 포트 매핑 구성은 이 일관된 패턴을 사용하여 NAT 및 포트 매핑 디바이스 내에서 수행되고 모든 데스크톱은 단일 공용 IP 주소에서 액세스할 수 있습니다. 클라이언트는 대개 이 IP 주소로 확인되는 단일 공용 DNS 이름을 사용합니다.

Windows 인증서 저장소에 인증 기관 추가

스마트 카드 인증의 경우 스마트 카드 인증서를 서명하는 CA(인증 기관)가 Windows 인증서 저장소에 있어야 합니다. 그렇지 않으면 CA를 Windows 인증서 저장소에 추가할 수 있습니다.

사전 요구 사항

MMC(Microsoft Management Console)에 인증서 스냅인이 있는지 확인합니다. "Horizon 7 설치" 문서의 "MMC에 인증서 스냅인 추가"를 참조하십시오.

절차

- 1 MMC를 시작합니다.
- 2 MMC 콘솔에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더로 이동합니다.

루트 인증서가 있고 인증서 체인에 중간 인증서가 없는 경우 MMC를 종료합니다.
- 3 **신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **모든 작업 > 가져오기**를 클릭합니다.
- 4 **인증서 가져오기** 마법사에서 **다음**을 클릭하고 루트 CA 인증서가 저장된 위치를 찾습니다.
- 5 루트 CA 인증서 파일을 선택하고 **열기**를 클릭합니다.
- 6 **다음, 다음, 마침**을 차례로 클릭합니다.
- 7 스마트 카드 인증서가 중간 CA에 의해 발급된 경우 인증서 체인의 모든 중간 인증서를 가져옵니다.
 - a **인증서(로컬 컴퓨터) > 중간 인증 기관 > 인증서** 폴더로 이동합니다.
 - b 각 중간 인증서에 대해 3~6단계를 반복합니다.

HTML Access 설정

3

VADC(View Agent Direct-Connection) 플러그인은 가상 시스템 기반 데스크톱 및 게시된 데스크톱에 대한 HTML Access를 지원합니다. 게시된 애플리케이션에 대한 HTML Access는 지원되지 않습니다.

본 장은 다음 항목을 포함합니다.

- HTML Access용 Horizon 7 Agent 설치
- 정적 콘텐츠 전송 설정
- 신뢰할 수 있는 CA 서명이 있는 TLS 서버 인증서 설정
- Windows 10 및 Windows 2016 데스크톱에서 HTTP/2 프로토콜 사용 안 함

HTML Access용 Horizon 7 Agent 설치

HTML Access를 지원하려면 특수 매개 변수를 사용하여 가상 시스템 기반 데스크톱에 Horizon 7 Agent를 설치해야 합니다.

사전 요구 사항

- <http://www.vmware.com/go/downloadview>의 VMware 다운로드 페이지에서 Horizon Agent 설치 관리자 파일을 다운로드합니다.

설치 관리자 파일 이름은 VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe이며, 여기서 y.y.y는 버전 번호이고 xxxxxx는 빌드 번호입니다.

절차

- ◆ 명령줄에서 Horizon 7 Agent를 설치하고 Horizon 7 Agent를 Horizon 7 연결 서버에 등록하지 않도록 지시하는 매개 변수를 지정합니다.

이 예에서는 Horizon 7 에이전트를 설치합니다.

```
VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /v VDM_SKIP_BROKER_REGISTRATION=1
```

다음에 수행할 작업

View Agent Direct-Connection 플러그인을 설치합니다. [View Agent Direct-Connection 플러그인 설치](#)의 내용을 참조하십시오.

정적 콘텐츠 전송 설정

HTML Access 클라이언트에서 데스크톱을 사용하려면 데스크톱에서 몇 가지 설정 작업을 수행해야 합니다. 이렇게 하면 사용자가 브라우저에서 데스크톱을 직접 가리키도록 설정할 수 있습니다.

사전 요구 사항

- VMware 다운로드 페이지(<http://www.vmware.com/go/downloadview>)에서 Horizon HTML Access portal.war zip 파일을 다운로드합니다.

파일 이름은 VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip이며, 여기서 y.y.y는 버전 번호이고 xxxxxx는 빌드 번호입니다.

절차

- 1 제어판을 엽니다.
- 2 프로그램 및 기능 > Windows 기능 사용/사용 안 함으로 이동합니다.
- 3 인터넷 정보 서비스 확인란을 선택하고 확인을 클릭합니다.
- 4 제어판에서 관리 도구 > IIS(인터넷 정보 서비스) 관리자로 이동합니다.
- 5 왼쪽 창의 항목을 확장합니다.
- 6 기본 웹 사이트를 마우스 오른쪽 단추로 클릭하고 바인딩 편집...을 선택합니다.
- 7 추가를 클릭합니다.
- 8 https, 지정하지 않은 모든 IP 및 포트 443을 선택합니다.
- 9 SSL 인증서 필드에서 올바른 인증서를 선택합니다.

옵션	조치
인증서 vdm이 있는 경우	vdm을 선택하고 확인을 클릭합니다.
인증서 vdm이 없는 경우	vdmdefault를 선택하고 확인을 클릭합니다.

- 10 사이트 바인딩 대화 상자에서 http 포트 80에 해당하는 항목을 제거하고 닫기를 클릭합니다.
- 11 기본 웹 사이트를 클릭합니다.
- 12 MIME 형식을 두 번 클릭합니다.
- 13 파일 이름 확장명 .json이 존재하지 않을 경우 작업 창에서 추가...를 클릭합니다. 그렇지 않으면 다음 2 단계를 건너뛰십시오.
- 14 파일 이름 확장명에 .json을 입력합니다.
- 15 MIME 형식으로 text/h323을 입력하고 확인을 클릭합니다.
- 16 파일 이름 확장명에 .mem을 입력합니다.
- 17 MIME 형식으로 text/plain을 입력하고 확인을 클릭합니다.
- 18 VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip을 임시 폴더에 복사합니다.

19 VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip의 압축을 풉니다.

portal.war이라는 파일이 표시됩니다.

20 portal.war의 이름을 portal.zip으로 바꿉니다.

21 C:\inetpub\wwwroot 폴더에 portal.zip의 압축을 풉니다.

필요한 경우, 파일을 추가할 수 있도록 폴더에 대한 사용 권한을 조정하십시오.

폴더 C:\inetpub\wwwroot\portal이 생성됩니다.

22 메모장을 엽니다.

23 다음 내용이 포함된 C:\inetpub\wwwroot\Default.htm 파일을 생성합니다. <IP address or DNS name of desktop>을 데스크톱의 실제 IP 주소 또는 DNS 이름으로 바꾸십시오.

```
<HEAD>
<noscript>
  <meta HTTP-EQUIV="REFRESH" content="0; url=https://<IP address or DNS name of desktop>/portal/
webclient/index.html">
</noscript>
</HEAD>
<script>
  var destination = 'https://<IP address or DNS name of desktop>/portal/webclient/index.html';
  var isSearch = !!window.location.search;
  window.location.href = destination + (isSearch ? window.location.search + '&' : '?') +
'vadc=1' + (window.location.hash || '');
</script>
```

신뢰할 수 있는 CA 서명이 있는 TLS 서버 인증서 설정

신뢰할 수 있는 CA 서명이 있는 TLS 서버 인증서를 설정하여 클라이언트와 데스크톱 사이에 사기성 트래픽을 사전에 차단할 수 있습니다.

사전 요구 사항

- 기본 자체 서명된 TLS 서버 인증서를 신뢰할 수 있는 CA 서명이 있는 TLS 서버 인증서로 대체합니다. [기본 자체 서명된 TLS 서버 인증서 교체](#)를 참조하십시오. 이렇게 하면 표시 이름 값이 vdm인 인증서가 생성됩니다.
- 데스크톱이 클라이언트의 정적 콘텐츠를 제공하는 경우에는 정적 콘텐츠 전송을 설정합니다. [정적 콘텐츠 전송 설정](#)의 내용을 참조하십시오.
- Windows 인증서 저장소에 대한 내용을 숙지합니다. "Horizon 7 설치" 문서에서 "새로운 TLS 인증서를 사용하도록 연결 서버, 보안 서버 또는 View Composer 구성"을 참조하십시오.

절차

- 1 Windows 인증서 저장소에서 **개인 > 인증서**로 이동합니다.
- 2 표시 이름이 vdm인 인증서를 두 번 클릭합니다.

- 3 세부 정보 탭을 클릭합니다.
- 4 지문 값을 복사합니다.
- 5 Windows 레지스트리 편집기를 시작합니다.
- 6 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config 레지스트리 키로 이동합니다.
- 7 새로운 문자열 값(REG_SZ) SSLHash를 이 레지스트리 키에 추가합니다.
- 8 SSLHash 값을 지문 값으로 설정합니다.

Windows 10 및 Windows 2016 데스크톱에서 HTTP/2 프로토콜 사용 안 함

일부 웹 브라우저에서 Windows 10 VADC 또는 Windows 2016 VADC 데스크톱에 액세스할 때 ERR_SPDY_PROTOCOL_ERROR 오류가 발생할 수 있습니다. 데스크톱에서 HTTP/2 프로토콜을 사용하지 않도록 설정하여 이 오류를 방지할 수 있습니다.

절차

- 1 Windows 레지스트리 편집기를 시작합니다.
- 2 레지스트리 키 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters로 이동합니다.
- 3 이 레지스트리 키에 2개의 새 REG_DWORD 값인 EnableHttp2Tls와 EnableHttp2Cleartext를 추가합니다.
- 4 두 값을 0으로 설정합니다.
- 5 데스크톱을 다시 부팅합니다.

원격 데스크톱 서비스 호스트에 View Agent Direct Connection 설정

4

Horizon 7은 사용자가 Horizon Client에서 액세스할 수 있는 게시된 데스크톱 및 애플리케이션을 제공하는 RDS(원격 데스크톱 서비스) 호스트를 지원합니다. 게시된 데스크톱은 RDS 호스트에 대한 데스크톱 세션을 기반으로 합니다. 일반적인 Horizon 7 배포에서는 클라이언트가 Horizon 연결 서버를 통해 데스크톱 및 애플리케이션에 연결합니다. 그러나 RDS 호스트에 View Agent Direct-Connection 플러그인을 설치하면 클라이언트가 Horizon 연결 서버를 사용하지 않고 게시된 데스크톱 또는 애플리케이션에 직접 연결할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 원격 데스크톱 서비스 호스트
- 게시된 데스크톱 및 애플리케이션에 대한 사용 권한 부여

원격 데스크톱 서비스 호스트

RDS(원격 데스크톱 서비스) 호스트는 원격 액세스를 위해 애플리케이션과 데스크톱을 호스팅하는 서버 구성 요소입니다.

Horizon 7 배포에서 RDS 호스트는 Microsoft 원격 데스크톱 서비스 역할, Microsoft 원격 데스크톱 세션 호스트 서비스 및 Horizon Agent가 설치되어 있는 Windows 서버입니다. VADC 플러그인도 설치되어 있으면 RDS 호스트가 VADC(View Agent Direct Connection)를 지원할 수 있습니다. RDS 호스트 설정 및 Horizon 7 Agent 설치에 대한 자세한 내용은 "Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정" 문서에서 “원격 데스크톱 서비스 호스트 설정”을 참조하십시오. VADC 플러그인 설치에 대한 자세한 내용은 [장 1 View Agent Direct-Connection 플러그인 설치](#)를 참조하십시오.

참고 Horizon Agent를 설치할 때 설치 관리자는 Horizon Agent가 연결될 Horizon 연결 서버의 호스트 이름 또는 IP 주소를 요청합니다. 설치 관리자를 매개 변수와 함께 실행하면 설치 관리자가 이 단계를 건너뛰게 할 수 있습니다.

```
VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"
```

RDS 호스트를 설정하고 VADC 플러그인을 설치한 후에는 RDS 데스크톱 및 애플리케이션에 자격을 부여해야 합니다. [게시된 데스크톱 및 애플리케이션에 대한 사용 권한 부여](#)의 내용을 참조하십시오.

게시된 데스크톱 및 애플리케이션에 대한 사용 권한 부여

게시된 데스크톱 및 애플리케이션에 대한 사용 권한을 부여해야 사용자가 해당 데스크톱 및 애플리케이션에 액세스할 수 있습니다.

RDS 호스트에서 Windows Server 2008 R2 SP1이 실행되고 있는 경우 **RemoteApp 관리자**를 실행하여 권한을 구성하십시오.

RDS 호스트에서 Windows Server 2012 또는 2012 R2가 실행되고 있는 경우에는 **서버 관리자**를 실행하고 **원격 데스크톱 서비스**로 이동하여 권한을 구성하십시오.

데스크톱 권한

사용자에게 게시된 데스크톱 시작 권한을 부여하려면 다음 단계를 수행하십시오.

- 사용자가 로컬 그룹 **View Agent Direct-Connection 사용자**의 구성원인지 확인합니다. 기본적으로 인증된 사용자는 모두 이 그룹의 구성원입니다.
- Windows Server 2008 R2 SP1의 경우 **RemoteApp 관리자**에서 RD 세션 호스트 서버가 이 **RD 세션 호스트 서버에 대한 원격 데스크톱 연결을 RD 웹 액세스에 표시**로 구성되어 있는지 확인합니다.
- Windows 2012 또는 2012 R2의 경우 **서버 관리자**를 실행하고 **원격 데스크톱 서비스**로 이동하여 권한을 구성합니다. 빠른 시작 마법사를 사용하여 RDSH 서비스를 배포합니다.

애플리케이션 권한

사용자에게 애플리케이션 시작 권한을 부여하려면 다음 단계를 수행하십시오.

- 사용자가 로컬 그룹 **View Agent Direct-Connection 사용자**의 구성원인지 확인합니다. 기본적으로 인증된 사용자는 모두 이 그룹의 구성원입니다.
- Windows Server 2008 R2 SP1의 경우 **RemoteApp 관리자**에서 애플리케이션이 **RemoteApp 프로그램** 아래에 나열되어 있고 **RD 웹 액세스**용으로 설정되어 있으며 모든 사용자, 이 사용자 또는 사용자가 속한 그룹에 대해 설정된 사용자 할당이 있는지 확인합니다.
- Windows 2012 또는 2012 R2의 경우 **서버 관리자**를 실행하고 **원격 데스크톱 서비스**로 이동하여 권한을 구성합니다.

View Agent Direct-Connection 플러그인 문제 해결

5

View Agent Direct-Connection 플러그인을 사용할 경우 알려진 문제가 발생할 수 있습니다.

View Agent Direct-Connection 플러그인의 문제를 조사할 경우 올바른 버전이 설치되어 실행되고 있는지 확인하십시오.

VMware에 지원 문제를 제기해야 할 경우 항상 전체 로깅을 사용하도록 설정하고 문제를 재현한 다음 DCT(데이터 수집 도구) 로그 집합을 생성하십시오. 그러면 VMware 기술 지원 담당자가 해당 로그를 분석할 수 있습니다. DCT 로그 집합 생성에 대한 자세한 내용은 VMware에 대한 진단 정보 수집 KB(기술 자료) 문서(<http://kb.vmware.com/kb/1017939>)를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 잘못된 그래픽 드라이버가 설치됨
- 비디오 RAM 부족
- TRACE 및 DEBUG 정보를 포함하도록 전체 로깅 사용

잘못된 그래픽 드라이버가 설치됨

올바른 버전의 그래픽 드라이버를 설치해야 PCoIP가 제대로 작동합니다.

문제

사용자가 PCoIP를 사용하는 데스크톱이나 애플리케이션에 연결하면 검은색 화면이 표시됩니다.

원인

잘못된 버전의 그래픽 드라이버가 실행되고 있습니다. 이 문제는 Horizon 7 Agent 설치 후 잘못된 버전의 VMware Tools가 설치된 경우에 발생할 수 있습니다.

해결책

- ◆ Horizon 7 Agent를 다시 설치합니다.

비디오 RAM 부족

PCoIP를 지원하려면 데스크톱 또는 RDS 호스트를 실행하는 가상 시스템에 적어도 128MB의 비디오 RAM이 있어야 합니다.

문제

사용자가 PCoIP를 사용하여 데스크톱이나 애플리케이션에 연결하면 검은색 화면이 표시됩니다.

원인

가상 시스템의 비디오 RAM이 부족합니다.

해결책

- ◆ 각 가상 시스템에 적어도 128MB의 비디오 RAM을 구성하십시오.

TRACE 및 DEBUG 정보를 포함하도록 전체 로깅 사용

View Agent Direct-Connection 플러그인은 표준 Horizon Agent 로그에 로그 항목을 기록합니다. TRACE 및 DEBUG 정보는 기본적으로 로그에 포함되지 않습니다.

문제

Horizon 7 Agent 로그에 TRACE 및 DEBUG 정보가 포함되지 않습니다.

원인

전체 로깅을 사용하도록 설정하지 않았습니다. 전체 로깅을 사용하도록 설정해야 TRACE 및 DEBUG 정보가 Horizon Agent 로그에 포함됩니다.

해결책

- 1 명령 프롬프트를 열고 C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels를 실행하십시오.
- 2 전체 로깅을 위해 3을 입력합니다.

디버그 로그 파일은 %ALLUSERSPROFILE%\VMware\VDM\logs에 있습니다. 파일 debug*.log에는 Horizon Agent 및 플러그인에서 로깅된 정보가 있습니다. 플러그인 로그 줄을 찾으려면 wsnm_xmlapi를 검색합니다.

Horizon Agent가 시작될 때 다음과 같이 플러그인 버전이 로깅됩니다.

```
2012-10-01T12:09:59.078+01:00 INFO (09E4-0C08) <logloaded> [MessageFrameWork] Plugin 'wsnm_xmlapi - VMware View Agent XML API Handler Plugin' loaded, version=e.x.p build-855808, buildtype=release
```

```
2012-10-01T12:09:59.078+01:00 TRACE (09E4-06E4) <PluginInitThread> [wsnm_xmlapi] Agent XML API Protocol Handler starting
```