

VMware Horizon HTML Access 설치 및 설정 가이드

2019년 12월

VMware Horizon HTML Access 5.3

VMware Horizon 7 7.10



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 © 2013–2019 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

VMware Horizon HTML Access 설치 및 설정 가이드 5

1 설정 및 설치 6

- HTML Access의 시스템 요구 사항 7
- 연결 서버 및 보안 서버 준비 8
 - 클라이언트 웹 브라우저 액세스에 대한 방화벽 규칙 10
- 캐시에서 자격 증명을 제거하도록 Horizon 7 구성 11
- 데스크톱, 풀 및 팜 준비 12
- 세션 공동 작업 기능에 대한 요구 사항 13
- 새 TLS 인증서를 사용하도록 HTML Access Agent 구성 14
 - 원격 데스크톱의 MMC에 인증서 스냅인 추가 15
 - HTML Access Agent용 인증서를 Windows 인증서 저장소로 가져오기 15
 - HTML Access Agent용 루트 및 중간 인증서 가져오기 16
 - Windows 레지스트리에 인증서 지문 설정 17
- 특정 암호 제품군을 사용하도록 HTML Access Agent 구성 18
- CA 서명 인증서를 사용하도록 iOS 구성 18
- Unified Access Gateway에서 CA 서명 인증서 사용 19
- Chrome 및 Safari에서 자동 재생 구성 19
- HTML Access 소프트웨어 업그레이드 19
- 연결 서버에서 HTML Access 구성 요소 제거 19
- Horizon Client 데이터 공유 구성 20
 - 모든 HTML Access 사용자에게 대해 데이터 공유를 사용하지 않도록 설정 20
 - VMware에서 수집하는 데이터 21

2 최종 사용자용 HTML Access 구성 23

- 최종 사용자용 VMware Horizon 웹 포털 페이지 구성 23
- URI를 사용하여 HTML Access 웹 클라이언트 구성 26
 - HTML Access용 URI 생성 구문 26
 - URI의 예 29
- HTML Access 그룹 정책 설정 31

3 원격 데스크톱 및 게시된 애플리케이션 연결 관리 32

- 원격 데스크톱 또는 게시된 애플리케이션에 연결 32
- 자체 서명된 루트 인증서 신뢰 34
- Workspace ONE 모드에서 서버에 연결 35
- 인증되지 않은 액세스를 사용하여 게시된 애플리케이션에 연결 35
- 시간대 설정 36
- H.264 디코딩 허용 37

로그오프 또는 연결 해제 37

4 원격 데스크톱 또는 게시된 애플리케이션 사용 39

기능 지원 표 39

사이드바 사용 41

모니터 및 화면 해상도 43

다중 모니터 사용 44

원격 데스크톱 및 게시된 애플리케이션의 화면 해상도 설정 44

DPI 동기화 사용 45

전체 화면 모드 사용 47

웹캠 및 마이크에 대한 실시간 오디오-비디오 기능 사용 47

원격 데스크톱 세션 공유 48

사용자를 원격 데스크톱 세션에 가입하도록 초대 49

공유 원격 데스크톱 세션 관리 50

원격 데스크톱 세션에 가입 51

텍스트 복사 및 붙여넣기 52

복사 및 붙여넣기 창 사용 53

클라이언트와 원격 데스크톱 또는 게시된 애플리케이션 간에 파일 전송 55

클라이언트 시스템에 원격 데스크톱 또는 게시된 애플리케이션의 파일 다운로드 56

클라이언트 시스템에서 원격 데스크톱 또는 게시된 애플리케이션으로 파일 업로드 56

여러 클라이언트 디바이스에서 게시된 애플리케이션의 다중 세션 사용 57

사운드 57

바로 가기 키 조합 58

국제화 61

국제 키보드 62

5 Horizon Client 문제 해결 63

원격 데스크톱 다시 시작 63

원격 데스크톱 또는 게시된 애플리케이션 재설정 64

VMware Horizon HTML Access 설치 및 설정 가이드

이 가이드 "VMware Horizon HTML Access 설치 및 설정 가이드"에서는 클라이언트 시스템에 소프트웨어를 설치할 필요 없이 가상 데스크톱에 연결되도록 VMware Horizon® HTML Access™ 소프트웨어를 설치, 구성 및 사용하는 방법을 설명합니다.

이 문서의 정보에는 최종 사용자가 웹 브라우저를 사용하여 원격 데스크톱에 액세스할 수 있도록 VMware Horizon 7 서버와 원격 데스크톱 가상 시스템에 HTML Access 소프트웨어를 설치하기 위한 시스템 요구 사항 및 지침이 포함되어 있습니다.

중요 이 정보는 Horizon 7 및 VMware vSphere 사용 경험이 있는 관리자를 대상으로 합니다. Horizon 7 초보자일 경우 "Horizon 7 설치" 설명서 및 "VMware Horizon Console 관리" 설명서에 서 기본 절차의 단계별 지침을 참조해야 할 경우도 있습니다.

설정 및 설치

1

HTML Access용 Horizon 7 배포를 설정할 때는 Horizon Connection Server에 HTML Access를 설치하고, 필요한 포트를 열고, 원격 데스크톱 가상 시스템에 HTML Access 구성 요소를 설치해야 합니다.

그런 다음 최종 사용자는 지원되는 브라우저를 열고 Horizon Connection Server에 대한 URL을 입력하여 원격 데스크톱에 액세스할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- HTML Access의 시스템 요구 사항
- 연결 서버 및 보안 서버 준비
- 캐시에서 자격 증명을 제거하도록 Horizon 7 구성
- 데스크톱, 풀 및 팜 준비
- 세션 공동 작업 기능에 대한 요구 사항
- 새 TLS 인증서를 사용하도록 HTML Access Agent 구성
- 특정 암호 제품군을 사용하도록 HTML Access Agent 구성
- CA 서명 인증서를 사용하도록 iOS 구성
- Unified Access Gateway에서 CA 서명 인증서 사용
- Chrome 및 Safari에서 자동 재생 구성
- HTML Access 소프트웨어 업그레이드
- 연결 서버에서 HTML Access 구성 요소 제거
- Horizon Client 데이터 공유 구성

HTML Access의 시스템 요구 사항

HTML Access를 사용하면 클라이언트 시스템에서는 지원되는 브라우저 이외에 다른 소프트웨어가 필요하지 않습니다. Horizon 7 배포는 특정 소프트웨어 요구 사항을 충족해야 합니다.

클라이언트 시스템의 브라우저

브라우저	버전
Chrome	75, 76
Internet Explorer	11
Safari	12
Firefox	67, 68
Microsoft Edge	42, 44
VMware Workspace ONE Web	Apple App Store(iOS 디바이스) 또는 Google Play Store(Android 디바이스)에서 제공되는 최신 버전입니다.

참고

- Android 디바이스의 Chrome은 Windows 키, 다중 모니터, 시스템에 복사하여 붙여넣기, 파일 전송, 인쇄, H.264 디코딩, 자격 증명 정리 및 외장 마우스를 지원하지 않습니다. 또한 Del, Ctrl+A, Ctrl+C, Ctrl+V, Ctrl+X, Ctrl+Y, Ctrl+Z 등의 키 및 키 조합은 소프트웨어 키보드에서 작동하지 않습니다.
- 모바일 디바이스의 Safari는 외장 마우스, Windows 키, 다중 모니터, 시스템에 복사하여 붙여넣기, 파일 전송, 인쇄, H.264 디코딩 및 자격 증명 정리를 지원하지 않습니다.

클라이언트 운영 체제

운영 체제	버전
Windows	7 SP1(32비트 및 64비트) 8.x(32비트 및 64비트) 10(32비트 및 64비트)
macOS	10.14.x(Mojave) 10.13.x(High Sierra)
iOS	10 이상
Chrome OS	28.x 이상
Android	7 이상

원격 데스크톱

HTML Access는 Horizon Agent 7.0 이상을 필요로 하며 Horizon Agent 7.0이 지원하는 모든 데스크톱 운영 체제를 지원합니다. 자세한 내용은 "Horizon 7 설치" 문서의 버전 7.0 이상에서 "Horizon Agent에 대해 지원되는 운영 체제"를 참조하십시오.

풀 설정

HTML Access를 사용하려면 다음 풀 설정이 필요합니다.

- **모니터 1대의 최대 해상도** 설정이 **1920x1200** 이상이어야 원격 데스크톱에 17.63MB 이상의 비디오 RAM을 사용할 수 있습니다.

3D 애플리케이션을 사용하거나 최종 사용자가 Google Chromebook Pixel 또는 Retina 디스플레이가 장착된 MacBook을 사용하려는 경우 [원격 데스크톱 및 게시된 애플리케이션의 화면 해상도 설정](#)을 참조하십시오.

- **HTML Access** 설정이 활성화되어 있어야 합니다.

구성 지침은 [데스크톱, 풀 및 팜 준비](#)의 내용을 참조하십시오.

연결 서버

HTML Access 옵션을 사용한 연결 서버가 서버에 설치되어 있어야 합니다.

HTML Access 구성 요소를 설치하면 Windows 방화벽에서 **VMware Horizon View 연결 서버(Blast-In)** 규칙이 활성화되어 방화벽이 TCP 포트 8443에 대한 인바운드 트래픽을 허용하도록 자동 구성됩니다.

보안 서버

연결 서버와 동일한 버전이 보안 서버에 설치되어 있어야 합니다.

클라이언트 시스템을 회사 방화벽 외부에서 연결하는 경우에는 보안 서버를 사용하십시오. 보안 서버를 사용하면 클라이언트 시스템에 VPN 연결이 필요하지 않습니다.

참고 단일 보안 서버는 웹 클라이언트에 최대 800개까지 동시 연결을 지원할 수 있습니다.

타사 방화벽

다음 트래픽을 허용하도록 규칙을 추가합니다.

- 서버(보안 서버, 연결 서버 인스턴스 및 복제 서버 포함): TCP 포트 8443에 대한 인바운드 트래픽.
- 원격 데스크톱 가상 시스템: TCP 포트 22443에 대한 서버의 인바운드 트래픽.

Horizon의 디스플레이 프로토콜

VMware Blast

웹 브라우저를 사용하여 원격 데스크톱에 액세스하는 경우 PCoIP 또는 Microsoft RDP가 아닌 VMware Blast 프로토콜이 사용됩니다.

VMware Blast는 HTTPS(SSL/TLS를 통한 HTTP)를 사용합니다.

연결 서버 및 보안 서버 준비

최종 사용자가 서버에 연결하고 원격 데스크톱 또는 게시된 애플리케이션에 액세스할 수 있으려면 먼저 Horizon 관리자가 연결 서버를 설치하고 보안 서버(사용되는 경우)를 설치해야 합니다.

보안 외부 액세스를 위해 보안 서버 대신 Unified Access Gateway 장치를 사용할 수 있습니다. 자세한 내용은 "Unified Access Gateway 배포 및 구성" 문서를 참조하십시오.

다음은 Horizon 관리자가 HTML Access를 사용하기 위해 수행해야 하는 작업의 검사 목록입니다.

- 1 연결 서버 복제 그룹을 구성하는 서버에서 **HTML Access 설치** 설정이 선택된 상태로 연결 서버를 설치합니다. 이 설정을 사용하면 HTML Access 구성 요소가 설치됩니다. 이 설정은 기본적으로 설치 관리자에서 선택됩니다. 자세한 내용은 "Horizon 7 설치" 문서를 참조하십시오.

HTML Access 구성 요소가 설치되었는지 확인하려면 Windows의 프로그램 제거 애플릿을 열고 목록에서 **VMware Horizon 7 HTML Access**를 찾습니다.

- 2 보안 서버를 사용하는 경우에는 보안 서버를 설치합니다. 보안 서버의 버전은 연결 서버 버전과 일치해야 합니다. 설치 지침을 보려면 "Horizon 7 설치" 문서를 참조하십시오.
- 3 각 연결 서버 인스턴스 또는 보안 서버에 웹 브라우저에 입력한 호스트 이름을 사용하여 완전히 확인할 수 있는 TLS 인증서가 있는지 확인하십시오. 자세한 내용은 "Horizon 7 설치" 문서를 참조하십시오.
- 4 RSA SecurID 또는 RADIUS 인증과 같은 2단계 인증을 사용하려면 연결 서버에서 이 기능이 사용되도록 설정되어 있는지 확인합니다. Horizon 7 버전 7.11부터는 RADIUS 인증 로그인 페이지에서 레이블을 사용자 지정할 수 있습니다. 자세한 내용은 "VMware Horizon Console 관리" 문서의 2 요소 인증에 대한 항목을 참조하십시오.
- 5 Horizon Client에서 **도메인** 드롭다운 메뉴를 숨기려면 **클라이언트 사용자 인터페이스에서 도메인 목록 숨기기** 전역 설정을 사용하도록 설정합니다. 이 설정은 Horizon 7 버전 7.1 이상에서 사용할 수 있습니다. Horizon 7 버전 7.8부터 기본적으로 사용하도록 설정됩니다. 자세한 내용은 "VMware Horizon Console 관리" 문서를 참조하십시오.
- 6 Horizon Client로 도메인 목록을 전송하려면 **도메인 목록 보내기** 전역 설정을 사용하도록 설정합니다. 이 설정은 Horizon 7 버전 7.8 이상에서 사용할 수 있으며 기본적으로 사용하지 않도록 설정됩니다. 이전 Horizon 7 버전은 도메인 목록을 보냅니다. 자세한 내용은 Horizon 7 버전 7.8 이상용 "VMware Horizon Console 관리" 문서를 참조하십시오.
- 7 타사 방화벽을 사용하는 경우, 모든 보안 서버 및 복제 그룹의 연결 서버 호스트에 대해 TCP 포트 8443에 대한 인바운드 트래픽을 허용하도록 규칙을 구성하고, 데이터 센터의 원격 데스크톱 가상 시스템 및 RDS 호스트에서 TCP 포트 22443에 대한 서버의 인바운드 트래픽을 허용하도록 규칙을 구성합니다. 자세한 내용은 [클라이언트 웹 브라우저 액세스에 대한 방화벽 규칙](#)의 내용을 참조하십시오.
- 8 게시된 애플리케이션에 대해 인증되지 않은 액세스 권한을 제공하려면 연결 서버에서 이 기능을 사용하도록 설정합니다. 자세한 내용은 "VMware Horizon Console 관리" 문서를 참조하십시오.

다음 표에서는 **도메인 목록 보내기** 및 **클라이언트 사용자 인터페이스에서 도메인 목록 숨기기** 전역 설정에 따라 사용자가 Horizon Client에서 서버에 로그인하는 방법이 어떻게 결정되는지를 보여 줍니다.

도메인 목록 보내기 설정	클라이언트 사용자 인터페이스에서 도메인 목록 숨기기 설정	사용자가 로그인하는 방법
사용 안 함(기본값)	사용	<p>도메인 드롭다운 메뉴는 숨겨져 있습니다. 사용자는 사용자 이름 텍스트 상자에 다음 값 중 하나를 입력해야 합니다.</p> <ul style="list-style-type: none"> ■ 사용자 이름(다중 도메인의 경우 허용되지 않음) ■ 도메인\사용자 이름 ■ username@domain.com
사용 안 함(기본값)	사용 안 함	<p>클라이언트에서 기본 도메인이 구성된 경우 기본 도메인이 도메인 드롭다운 메뉴에 표시됩니다. 클라이언트가 기본 도메인을 알 수 없는 경우 도메인 드롭다운 메뉴에 *DefaultDomain*이 나타납니다. 사용자는 사용자 이름 텍스트 상자에 다음 값 중 하나를 입력해야 합니다.</p> <ul style="list-style-type: none"> ■ 사용자 이름(다중 도메인의 경우 허용되지 않음) ■ 도메인\사용자 이름 ■ username@domain.com
사용	사용	<p>도메인 드롭다운 메뉴는 숨겨져 있습니다. 사용자는 사용자 이름 텍스트 상자에 다음 값 중 하나를 입력해야 합니다.</p> <ul style="list-style-type: none"> ■ 사용자 이름(다중 도메인의 경우 허용되지 않음) ■ 도메인\사용자 이름 ■ username@domain.com
사용	사용 안 함	<p>사용자 이름 텍스트 상자에 사용자 이름을 입력하고 도메인 드롭다운 메뉴에서 도메인을 선택할 수 있습니다. 또는 사용자 이름 텍스트 상자에 다음 값 중 하나를 입력할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 도메인\사용자 이름 ■ username@domain.com

서버가 설치된 후 Horizon Console에서 해당 연결 서버 인스턴스 및 보안 서버에 대해 **Blast 보안 게이트웨이** 설정이 사용되도록 지정됩니다. 또한, 해당 연결 서버 인스턴스 및 보안 서버에서 Blast 보안 게이트웨이를 사용하도록 **Blast 외부 URL** 설정이 구성됩니다. 기본적으로 URL에는 보안 터널 외부 URL의 FQDN과 기본 포트 번호 8443이 포함됩니다. URL에는 클라이언트 시스템이 연결 서버 호스트 또는 보안 서버 호스트에 연결하기 위해 사용할 수 있는 FQDN과 포트 번호가 포함되어야 합니다. 자세한 내용은 "Horizon 7 설치" 문서의 "연결 서버 인스턴스의 외부 URL 설정"을 참조하십시오.

참고 VMware Workspace ONE과 함께 HTML Access를 사용하여 사용자가 HTML5 브라우저에서 자신의 데스크톱에 연결하도록 허용할 수 있습니다. Workspace ONE 설치 및 연결 서버와 함께 사용하기 위한 구성에 대한 자세한 내용은 Workspace ONE 설명서를 참조하십시오. 연결 서버와 SAML 인증 서버를 연결하는 것에 대한 자세한 내용은 "VMware Horizon Console 관리" 문서를 참조하십시오.

클라이언트 웹 브라우저 액세스에 대한 방화벽 규칙

클라이언트 웹 브라우저에서 보안 서버, 연결 서버 인스턴스, 원격 데스크톱 및 게시된 애플리케이션에 연결하도록 하려면, 방화벽이 특정 TCP 포트에서 인바운드 트래픽을 허용해야 합니다.

HTML Access 연결은 HTTPS를 사용해야 합니다. HTTP 연결은 허용되지 않습니다.

기본적으로 연결 서버 인스턴스 또는 보안 서버를 설치할 때 Windows 방화벽에서 **VMware Horizon View 연결 서버(Blast-In)** 규칙이 활성화되며 방화벽이 TCP 포트 8443에 대한 인바운드 트래픽을 허용하도록 구성됩니다.

표 1-1. 클라이언트 브라우저 액세스에 대한 방화벽 규칙

소스	기본 소스 포트	프로토콜	대상	기본 대상 포트	참고
클라이언트 웹 브라우저	TCP 입의	HTTPS	보안 서버 또는 연결 서버 인스턴스	TCP 443	초기 연결을 설정하기 위해 클라이언트 디바이스의 웹 브라우저가 TCP 포트 443에서 보안 서버 또는 연결 서버 인스턴스에 연결됩니다.
클라이언트 웹 브라우저	TCP 입의	HTTPS	Blast 보안 게이트웨이	TCP 8443	초기 연결이 설정된 후 클라이언트 디바이스의 웹 브라우저가 TCP 포트 8443에서 Blast 보안 게이트웨이에 연결됩니다. 이러한 두 번째 연결이 이루어지려면 Blast 보안 게이트웨이가 보안 서버 또는 연결 서버 인스턴스에서 사용되도록 설정되어 있어야 합니다.
Blast 보안 게이트웨이	TCP 입의	HTTPS	HTML Access Agent	TCP 22443	Blast 보안 게이트웨이를 사용하도록 설정할 경우 사용자가 원격 데스크톱 또는 게시된 애플리케이션을 선택하면 Blast 보안 게이트웨이가 원격 데스크톱 가상 시스템 또는 RDS 호스트의 TCP 포트 22443에서 HTML Access Agent에 연결됩니다. 이 에이전트 구성 요소는 Horizon Agent 설치 시 함께 설치됩니다.
클라이언트 웹 브라우저	TCP 입의	HTTPS	HTML Access Agent	TCP 22443	Blast 보안 게이트웨이를 사용하지 않도록 설정할 경우, 사용자가 원격 데스크톱 또는 게시된 애플리케이션을 선택하면 클라이언트 디바이스의 웹 브라우저가 원격 데스크톱 가상 시스템 또는 RDS 호스트의 TCP 포트 22443에서 HTML Access Agent에 직접 연결됩니다. 이 에이전트 구성 요소는 Horizon Agent 설치 시 함께 설치됩니다.

캐시에서 자격 증명을 제거하도록 Horizon 7 구성

사용자가 원격 데스크톱 또는 게시된 애플리케이션으로 연결되는 탭을 닫거나 데스크톱 및 애플리케이션 선택 창으로 연결되는 탭을 닫을 때 캐시에서 사용자의 자격 증명을 제거하도록 Horizon 7을 구성할 수 있습니다.

이 기능이 사용되지 않도록 설정되면(기본 설정) 자격 증명이 캐시에 그대로 남아 있습니다.

참고 이 기능을 사용하도록 설정하면 사용자가 데스크톱 및 애플리케이션 선택 페이지 또는 원격 세션 페이지를 새로 고치거나 원격 세션이 포함된 탭에서 URI 명령을 실행할 때 캐시에서 자격 증명도 제거됩니다. 서버가 자체 서명된 인증서를 제공하는 경우 사용자가 원격 데스크톱 또는 게시된 애플리케이션을 실행하고 보안 경고가 나타날 때 인증서를 수락하면 캐시에서 자격 증명이 제거됩니다.

사전 요구 사항

이 기능에는 Horizon 7 버전 7.0.2 이상이 필요합니다.

절차

- 1 Horizon Console에서 **설정 > 전역 설정**을 선택하고 **일반 설정** 탭을 클릭한 다음 **편집**을 클릭합니다.
- 2 **HTML Access를 위해 탭이 닫힐 때 자격 증명 정리** 확인란을 선택합니다.
- 3 변경 사항을 저장하려면 **확인**을 클릭합니다.

변경 사항이 즉시 적용됩니다. 연결 서버를 다시 시작하지 않아도 됩니다.

데스크톱, 풀 및 팜 준비

최종 사용자가 원격 데스크톱 또는 게시된 애플리케이션에 액세스하려면 먼저 Horizon 관리자가 특정 풀 및 팜 설정을 구성하고 데이터 센터에서 데스크톱 가상 시스템 및 RDS 호스트에 Horizon Agent를 설치해야 합니다.

HTML Access 클라이언트는 클라이언트 시스템에 Horizon Client 소프트웨어가 설치되어 있지 않은 경우에 적합한 대안입니다.

참고 Horizon Client 소프트웨어는 HTML Access 클라이언트보다 더 많은 기능과 우수한 성능을 제공합니다. 예를 들어 HTML Access 클라이언트를 사용할 때 일부 키 조합이 원격 데스크톱에서 작동하지 않지만 Horizon Client에서는 작동합니다.

사전 요구 사항

- Horizon 구성 요소가 HTML Access에 대한 시스템 요구 사항을 충족하는지 확인합니다. [HTML Access의 시스템 요구 사항](#)의 내용을 참조하십시오.
- 호스트에 HTML Access 구성 요소가 연결 서버와 함께 설치되어 있는지, 연결 서버 인스턴스 및 보안 서버의 Windows 방화벽이 TCP 포트 8443에서 인바운드 트래픽을 허용하는지 확인하십시오. [연결 서버 및 보안 서버 준비](#)의 내용을 참조하십시오.
- 타사 방화벽을 사용하는 경우, Horizon Server에서 데이터센터에 있는 데스크톱 가상 시스템 및 RDS 호스트의 TCP 포트 22443으로 인바운드 트래픽을 허용하도록 규칙을 구성합니다. [클라이언트 웹 브라우저 액세스에 대한 방화벽 규칙](#)의 내용을 참조하십시오.
- 데스크톱 소스로 사용하려는 가상 시스템 또는 게시된 데스크톱 및 애플리케이션을 호스팅하는 RDS 호스트에 지원되는 운영 체제와 VMware Tools가 설치되어 있는지 확인합니다. [HTML Access의 시스템 요구 사항](#)의 내용을 참조하십시오.
- 풀 및 팜을 만들고 사용자에게 권한을 부여하는 절차를 잘 숙지하십시오. "Horizon 7에서 가상 데스크톱 설정" 및 "Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정" 문서를 참조하십시오.
- 최종 사용자가 원격 데스크톱 또는 게시된 애플리케이션에 액세스할 수 있는지 확인하려면 클라이언트 시스템에서 Windows용 Horizon Client를 설치합니다. 웹 브라우저에서 연결을 시도하기 전에 Windows용 Horizon Client를 사용하여 연결을 테스트할 수 있습니다. 설치 지침을 보려면 "Windows용 VMware Horizon Client 설치 및 설정 가이드" 문서를 참조하십시오.
- 원격 데스크톱 또는 게시된 애플리케이션에 액세스하는 데 지원되는 브라우저 중 하나가 있는지 확인하십시오. [HTML Access의 시스템 요구 사항](#)의 내용을 참조하십시오.

절차

- 1 게시된 데스크톱 및 애플리케이션의 경우 Horizon Console을 사용하여 팜을 생성하거나 편집하고, 팜 설정에서 **이 팜의 데스크톱 및 애플리케이션에 대한 HTML Access 허용** 옵션을 사용하도록 설정하십시오.
- 2 가상 데스크톱 풀의 경우 HTML Access에서 풀을 사용할 수 있도록 Horizon Console을 사용하여 데스크톱 풀을 편집하십시오.
 - a 데스크톱 풀 설정에서 **HTML Access**를 활성화하십시오.
 - b 풀 설정에서 **모니터 1대의 최대 해상도** 설정이 **1920x1200** 이상인지 확인하십시오.
- 3 **이 팜의 데스크톱 및 애플리케이션에 대한 HTML 액세스 허용** 또는 **HTML Access** 옵션에서 Horizon Agent를 사용하기 위해 풀이 생성되거나, 재구성되거나, 업그레이드된 후에 Windows용 Horizon Client를 사용하여 원격 데스크톱 또는 게시된 애플리케이션에 연결합니다.
이 단계에서 HTML Access 사용을 시도하기 전에 풀이 올바르게 작동되는지 확인하십시오.
- 4 지원되는 브라우저를 열고 연결 서버 인스턴스를 가리키는 URL을 입력합니다.

예:

```
https://horizon.mycompany.com
```

URL에 **https**를 포함해야 합니다.

- 5 표시되는 웹 페이지에서 **VMware Horizon HTML Access**를 클릭하고 Windows용 Horizon Client에서와 같이 로그인합니다.
- 6 나타나는 데스크톱 및 애플리케이션 선택 페이지에서 아이콘을 클릭하여 연결합니다.
이제 웹 브라우저에서 원격 데스크톱 또는 게시된 애플리케이션에 액세스할 수 있습니다.

다음에 수행할 작업

보안을 강화하기 위한 보안 정책에 따라 원격 데스크톱의 HTML Access Agent가 인증 기관의 TLS 인증서를 사용해야 할 경우에는 [새 TLS 인증서를 사용하도록 HTML Access Agent 구성](#)을 참조하십시오.

세션 공동 작업 기능에 대한 요구 사항

세션 공동 작업 기능을 사용하여 기존의 원격 데스크톱 세션에 가입하도록 다른 사용자를 초대할 수 있습니다. 세션 공동 작업 기능을 지원하려면 Horizon 배포가 특정 요구 사항을 충족해야 합니다.

세션 공동 작업자

공동 작업 세션에 가입하려면 클라이언트 시스템에 Windows, Mac 또는 Linux용 Horizon Client 4.7 이상을 설치하거나 HTML Access 4.7 이상을 사용해야 합니다.

Windows 원격 데스크톱

- Horizon Agent 7.4 이상이 Windows 가상 데스크톱 또는 게시된 데스크톱의 RDS 호스트에 설치되어야 합니다.

- 데스크톱 풀 또는 팜 수준에서 세션 공동 작업 기능을 사용하도록 설정해야 합니다. 데스크톱 풀에 대한 세션 공동 작업 기능을 사용하도록 설정하는 방법에 대한 내용은 "Horizon 7에서 가상 데스크톱 설정" 문서를 참조하십시오. 팜에 대한 세션 공동 작업 기능을 사용하도록 설정하는 방법에 대한 내용은 "Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정" 문서를 참조하십시오.

Horizon Agent 그룹 정책 설정을 사용하여 세션 공동 작업 기능을 구성할 수 있습니다. 자세한 내용은 "Horizon 7에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

Linux 원격 데스크톱

Linux 원격 데스크톱 요구 사항에 대해서는 "Horizon 7 for Linux 데스크톱 설정" 문서를 참조하십시오.

연결 서버

세션 공동 작업 기능을 사용하려면 연결 서버 인스턴스가 엔터프라이즈 라이선스를 사용해야 합니다.

디스플레이 프로토콜

VMware Blast

세션 공동 작업 기능은 게시된 애플리케이션 세션을 지원하지 않습니다.

새 TLS 인증서를 사용하도록 HTML Access Agent 구성

산업 또는 보안 규정을 준수하려면 HTML Access Agent가 생성하는 기본 TLS 인증서를 CA(인증 기관)에서 서명한 인증서로 바꿀 수 있습니다.

원격 데스크톱에 HTML Access Agent를 설치하면 HTML Access Agent 서비스로 자체 서명된 기본 인증서가 생성됩니다. 이 서비스는 HTML Access를 사용하는 브라우저에 기본 인증서를 제공합니다.

참고 데스크톱 가상 시스템의 게스트 운영 체제에서는 이 서비스를 VMware Blast 서비스라고 합니다.

기본 인증서를 CA에서 가져온 서명된 인증서로 교체하려면 각 원격 데스크톱의 Windows 로컬 컴퓨터 인증서 저장소에 인증서를 가져와야 합니다. 또한, HTML Access Agent를 통해 새 인증서를 사용할 수 있도록 하는 레지스트리 값을 설정해야 합니다.

기본 HTML Access Agent 인증서를 CA 서명 인증서로 교체할 경우 각 원격 데스크톱에 고유한 인증서를 구성하는 것이 좋습니다. 데스크톱 풀을 생성하는 데 사용하는 상위 가상 시스템 또는 템플릿에서 CA 서명 인증서를 구성하지 마십시오. 이러한 방법을 사용하면 수백 또는 수천 대의 원격 데스크톱이 동일한 인증서를 사용하게 됩니다.

절차

1 원격 데스크톱의 MMC에 인증서 스냅인 추가

Windows 로컬 컴퓨터 인증서 저장소에 인증서를 추가하기 전에 HTML Access Agent가 설치된 원격 데스크톱의 MMC(Microsoft 관리 콘솔)에 인증서 스냅인을 추가해야 합니다.

2 HTML Access Agent용 인증서를 Windows 인증서 저장소로 가져오기

기본 HTML Access Agent 인증서를 CA 서명 인증서로 교체하려면 CA 서명 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다. HTML Access Agent가 설치된 각 원격 데스크톱에서 이 절차를 수행하십시오.

3 HTML Access Agent용 루트 및 중간 인증서 가져오기

인증서 체인의 루트 인증서 및 중간 인증서를 HTML Access Agent용으로 가져온 SSL 인증서와 함께 가져오지 못한 경우, 해당 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다.

4 Windows 레지스트리에 인증서 지문 설정

HTML Access Agent가 Windows 인증서 저장소로 가져온 CA 서명 인증서를 사용하도록 허용하려면 Windows 레지스트리 키에서 인증서 지문을 구성해야 합니다. 기본 인증서를 CA 서명 인증서로 교체한 각 원격 데스크톱에서 이 단계를 적용해야 합니다.

원격 데스크톱의 MMC에 인증서 스냅인 추가

Windows 로컬 컴퓨터 인증서 저장소에 인증서를 추가하기 전에 HTML Access Agent가 설치된 원격 데스크톱의 MMC(Microsoft 관리 콘솔)에 인증서 스냅인을 추가해야 합니다.

사전 요구 사항

HTML Access 에이전트가 설치되어 있는 Windows 게스트 운영 체제에서 MMC와 인증서 스냅인을 사용할 수 있는지 확인하십시오.

절차

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

다음에 수행할 작업

Windows 로컬 컴퓨터 인증서 저장소로 SSL 인증서를 가져옵니다. [HTML Access Agent용 인증서를 Windows 인증서 저장소로 가져오기](#)의 내용을 참조하십시오.

HTML Access Agent용 인증서를 Windows 인증서 저장소로 가져오기

기본 HTML Access Agent 인증서를 CA 서명 인증서로 교체하려면 CA 서명 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다. HTML Access Agent가 설치된 각 원격 데스크톱에서 이 절차를 수행하십시오.

사전 요구 사항

- HTML Access Agent가 원격 데스크톱에 설치되어 있는지 확인하십시오.
- CA 서명 인증서가 원격 데스크톱에 복사되었는지 확인하십시오.
- 인증서 스냅인이 MMC에 추가되었는지 확인하십시오. [원격 데스크톱의 MMC에 인증서 스냅인 추가](#)의 내용을 참조하십시오.

절차

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

인증서 파일 유형을 표시하려면 **파일 이름** 드롭다운 메뉴에서 해당 파일 형식을 선택하십시오.

- 5 인증서 파일에 포함된 개인 키 암호를 입력합니다.
- 6 **이 키를 내보낼 수 있도록 표시**를 선택합니다.
- 7 **확장 가능한 모든 속성 포함**을 선택합니다.
- 8 **다음, 마침**을 차례로 클릭합니다.

새 인증서가 **인증서(로컬 컴퓨터) > 개인 > 인증서** 폴더에 나타납니다.

- 9 새 인증서에 개인 키가 포함되어 있는지 확인합니다.
 - a **인증서(로컬 컴퓨터) > 개인 > 인증서** 폴더에서 새 인증서를 두 번 클릭합니다.
 - b [인증서 정보] 대화상자의 [일반] 탭에 사용자가 이 인증서와 일치하는 개인 키를 갖고 있습니다. 라는 문구가 표시되는지 확인합니다.

다음에 수행할 작업

필요한 경우 루트 인증서 및 중간 인증서를 Windows 인증서 저장소로 가져옵니다. [HTML Access Agent용 루트 및 중간 인증서 가져오기](#)의 내용을 참조하십시오.

인증서 지문과 함께 해당 레지스트리 키를 구성합니다. [Windows 레지스트리에 인증서 지문 설정](#)의 내용을 참조하십시오.

HTML Access Agent용 루트 및 중간 인증서 가져오기

인증서 체인의 루트 인증서 및 중간 인증서를 HTML Access Agent용으로 가져온 SSL 인증서와 함께 가져오지 못한 경우, 해당 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져와야 합니다.

절차

- 1 원격 데스크톱의 MMC 콘솔에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더로 이동합니다.
 - 루트 인증서가 이 폴더에 있고 인증서 체인에 중간 인증서가 없는 경우 이 절차를 건너뛸 수 있습니다.

- 루트 인증서가 이 폴더에 없는 경우 2단계를 진행하십시오.
- 2 신뢰할 수 있는 루트 인증 기관 > 인증서 폴더를 마우스 오른쪽 버튼으로 클릭하고 **모든 작업 > 가져오기**를 클릭합니다.
- 3 인증서 가져오기 마법사에서 **다음**을 클릭하고 루트 CA 인증서가 저장된 위치를 찾습니다.
- 4 루트 CA 인증서 파일을 선택하고 **열기**를 클릭합니다.
- 5 **다음**, **다음**, **마침**을 차례로 클릭합니다.
- 6 중간 CA가 서버 인증서에 서명한 경우 인증서 체인의 모든 중간 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져옵니다.
 - a **인증서(로컬 컴퓨터) > 중간 인증 기관 > 인증서** 폴더로 이동합니다.
 - b 가져와야 할 각 중간 인증서에 대해 3~6단계를 반복합니다.

다음에 수행할 작업

인증서 지문과 함께 해당 레지스트리 키를 구성합니다. [Windows 레지스트리에 인증서 지문 설정](#)의 내용을 참조하십시오.

Windows 레지스트리에 인증서 지문 설정

HTML Access Agent가 Windows 인증서 저장소로 가져온 CA 서명 인증서를 사용하도록 허용하려면 Windows 레지스트리 키에서 인증서 지문을 구성해야 합니다. 기본 인증서를 CA 서명 인증서로 교체한 각 원격 데스크톱에서 이 단계를 적용해야 합니다.

사전 요구 사항

CA 서명 인증서를 Windows 인증서 저장소로 가져왔는지 확인합니다. [HTML Access Agent용 인증서를 Windows 인증서 저장소로 가져오기](#)의 내용을 참조하십시오.

절차

- 1 HTML Access Agent가 설치된 원격 데스크톱의 MMC 창에서 **인증서(로컬 컴퓨터) > 개인 > 인증서** 폴더로 이동합니다.
- 2 Windows 인증서 저장소로 가져온 CA 서명 인증서를 두 번 클릭합니다.
- 3 [인증서] 대화상자에서 [세부 정보] 탭을 클릭하고 아래로 스크롤한 후 **지문** 아이콘을 선택합니다.
- 4 선택된 지문을 텍스트 파일에 복사합니다.

예: 31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e

참고 지문을 복사할 때 앞에 공백을 두지 마십시오. 지문과 함께 선행 공백을 레지스트리에 실수로 붙여넣을 경우(7단계) 인증서 구성이 실패할 수 있습니다. 레지스트리 값 텍스트 상자에 선행 공백이 표시되지 않더라도 이 문제가 발생할 수 있습니다.

- 5 HTML Access Agent가 설치된 데스크톱에서 Windows 레지스트리 편집기를 시작합니다.
- 6 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware BlastWConfig 레지스트리 키로 이동합니다.

7 SslHash 값을 수정하고 텍스트 상자에 인증서 지문을 붙여넣습니다.

8 Windows를 재부팅합니다.

사용자가 HTML Access를 통해 원격 데스크톱에 연결하면 HTML Access Agent는 CA 서명 인증서를 사용자의 브라우저에 표시합니다.

특정 암호 제품군을 사용하도록 HTML Access Agent 구성

기본 암호 세트 대신 특정 암호 제품군을 사용하도록 HTML Access Agent를 구성할 수 있습니다.

기본적으로 HTML Access Agent는 수신 SSL 연결이 네트워크 도청 및 위조에 대해 강력한 보호 기능을 제공하는 특정 암호를 기반으로 한 암호화를 사용하도록 요구합니다. HTML Access Agent가 사용할 대체 암호 목록을 구성할 수 있습니다. 허용되는 암호 세트는 OpenSSL 형식으로 표현됩니다. 자세한 내용은 <https://www.openssl.org/docs/manmaster/man1/ciphers.html>의 내용을 참조하십시오.

절차

- 1 HTML Access Agent가 설치된 데스크톱에서 Windows 레지스트리 편집기를 시작합니다.
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config 레지스트리 키로 이동합니다.
- 3 새 문자열(REG_SZ) 값, SslCiphers를 추가하고 암호 목록을 OpenSSL 형식으로 텍스트 상자에 붙여 넣습니다.
- 4 변경 내용을 적용하려면 VMware Blast 서비스를 다시 시작하십시오.

Windows 게스트 운영 체제에서 HTML Access Agent용 서비스 이름은 VMware Blast입니다.

기본 암호 목록을 사용하도록 되돌리려면 SslCiphers 값을 삭제하고 VMware Blast 서비스를 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 Agent를 시작하면 VMware Blast 서비스의 로그 파일에 암호 정의가 작성됩니다. Windows 레지스트리에 SslCiphers 값이 구성되지 않은 상태로 VMware Blast 서비스가 시작될 경우 로그를 검사하여 현재의 기본 암호 목록을 검색할 수 있습니다.

HTML Access Agent의 기본 암호 정의는 보안 강화를 위해 릴리스마다 달라질 수 있습니다.

CA 서명 인증서를 사용하도록 iOS 구성

iOS 디바이스에서 HTML Access를 사용하려면 Horizon Connection Server 또는 HTML Access Agent에서 생성된 기본 SSL 인증서 대신 CA(인증 기관)에서 서명한 SSL 인증서를 설치해야 합니다.

지침을 보려면 "Horizon 7 설치" 문서의 "루트 및 중간 인증서를 신뢰하도록 iOS용 Horizon Client 구성"을 참조하십시오.

Unified Access Gateway에서 CA 서명 인증서 사용

연결 서버 또는 보안 서버 대신 Unified Access Gateway 장치를 사용하는 경우 SAN(주체 대체 이름)이 구성된 CA 서명 인증서를 설치해야 합니다.

SAN이 구성되지 않은 CA 서명 인증서 또는 자체 서명된 인증서를 사용하는 경우 “전용 연결 아님” 오류 메시지가 표시되며 HTML Access에 연결할 수 없습니다.

참고 연결 서버 인스턴스 또는 보안 서버를 사용하는 경우 사용자는 *ip-address*에서 계속 이동(비안전) 링크를 클릭하여 계속 연결할 수 있습니다.

Horizon 7용 인증서를 설치 및 구성하는 방법에 대한 자세한 내용은 “Horizon 7 설치” 문서를 참조하십시오. TLS 인증서를 사용하도록 HTML Access Agent를 구성하는 방법에 대한 내용은 [새 TLS 인증서를 사용하도록 HTML Access Agent 구성](#)을 참조하십시오.

Chrome 및 Safari에서 자동 재생 구성

Chrome 71 이상 버전 또는 Safari 12에서 HTML Access를 사용하는 경우 원격 데스크톱 또는 게시된 애플리케이션을 처음으로 시작하거나 원격 데스크톱 또는 게시된 애플리케이션을 사용하는 동안 브라우저를 새로 고치면 오디오를 사용하도록 설정하려면 클릭 대화 상자가 표시될 수 있습니다. 이 대화상자에서 **확인**을 클릭하면 오디오가 정상적으로 재생됩니다.

브라우저에서 자동 재생 정책을 구성하여 이 대화상자가 나타나지 않도록 할 수 있습니다.

- Chrome의 탐색 바에 **chrome://flags/#autoplay-policy**를 입력하고 아래로 스크롤하여 **Autoplay policy**로 이동한 후 드롭다운 메뉴에서 **No user gesture required**를 선택합니다.
- Mac의 Safari에서 **Safari > 이 웹 사이트에 대한 설정**을 선택하고 **자동 재생** 오른쪽에 포인터를 둔 다음, 드롭다운 메뉴를 클릭하고 **모든 자동 재생 허용**을 선택합니다.

HTML Access 소프트웨어 업그레이드

대부분의 HTML Access 버전에서는 업그레이드를 수행하면 단순히 Horizon Connection Server 및 Horizon Agent가 업그레이드됩니다.

HTML Access 업그레이드 시, 해당 버전의 Horizon Connection Server가 복제된 그룹의 모든 인스턴스에 설치되어 있는지 확인하십시오.

연결 서버를 업그레이드할 경우 HTML Access는 자동으로 설치되거나 업그레이드됩니다.

참고 HTML Access 구성 요소가 설치되어 있는지 확인하려면 Windows 운영 체제에서 프로그램 제거 애플릿을 열고 목록에서 HTML Access를 찾아볼 수 있습니다.

연결 서버에서 HTML Access 구성 요소 제거

다른 Windows 소프트웨어 제거 방법과 동일한 방법으로 HTML Access 구성 요소를 제거할 수 있습니다.

절차

- 1 HTML Access가 설치된 연결 서버 인스턴스에서 Windows 제어판이 제공하는 프로그램 제거 애플릿을 엽니다.
- 2 **VMware Horizon 7 HTML Access**를 선택하고 **제거**를 클릭합니다.
- 3 (선택 사항) 해당 호스트에 대한 Windows 방화벽에서 TCP 포트 8443이 더는 인바운드 트래픽을 허용하지 않는지 확인합니다.

다음에 수행할 작업

쌍으로 연결된 보안 서버의 Windows 방화벽에서 TCP 포트 8443에 대한 인바운드 트래픽을 허용하지 않습니다. 해당하는 경우, 쌍으로 연결된 모든 보안 서버 및 연결 서버 인스턴스에 대해 타사 방화벽에서 TCP 포트 8443에 대한 인바운드 트래픽을 허용하지 않도록 규칙을 변경합니다.

Horizon Client 데이터 공유 구성

Horizon Administrator가 VMware CEIP(고객 환경 향상 프로그램)에 참여하기로 한 경우 VMware는 연결 서버를 통해 클라이언트 시스템에서 익명 데이터를 수집하고 수신합니다. 이 클라이언트 데이터를 연결 서버와 공유할지 여부를 구성할 수 있습니다.

CEIP에 가입하도록 Horizon을 구성하는 방법에 대한 자세한 내용은 "VMware Horizon Console 관리" 문서를 참조하십시오.

데이터 공유는 기본적으로 HTML Access에서 사용하도록 설정됩니다. 서버에 연결한 후에는 데이터 공유 설정을 변경할 수 없습니다.

Horizon Administrator는 모든 사용자에게 HTML Access에서 데이터 공유를 사용하지 않도록 설정하고, 사용자가 HTML Access의 데이터 공유 설정을 변경하지 못하게 할 수 있습니다. 자세한 내용은 [모든 HTML Access 사용자에게 데이터 공유를 사용하지 않도록 설정](#)의 내용을 참조하십시오.

절차

- 1 Horizon Client를 시작합니다.
- 2 VMware Horizon 로그인 페이지에서 **설정**(톱니바퀴 아이콘)을 클릭합니다.
- 3 **데이터 공유 허용** 옵션을 켜기 또는 끄기로 전환합니다.

모든 HTML Access 사용자에게 데이터 공유를 사용하지 않도록 설정

Horizon Administrator는 모든 HTML Access 사용자에게 데이터 공유를 사용하지 않도록 설정하고 연결 서버 인스턴스에서 C:\Program Files\VMware\VMware View\Server\broker\Webapps\portal\WEB-INF\classes\portal-version.properties 파일에 다음 설정을 추가하여 사용자가 HTML Access에서 **데이터 공유 허용** 옵션을 변경하지 못하게 할 수 있습니다.

```
CEIP.disabled=true
```

이 설정이 **true**로 설정되면 **설정**(톱니바퀴 아이콘)이 HTML Access의 VMware Horizon 로그인 페이지에 나타나지 않습니다.

참고 이 설정은 Horizon Client를 사용하여 연결 서버 인스턴스에 연결하는 사용자에게는 영향을 주지 않습니다. Horizon Client에서 데이터 공유를 사용하지 않도록 설정하는 방법에 대한 내용은 해당 Horizon Client 플랫폼에 대한 설치 및 설정 가이드를 참조하십시오.

VMware에서 수집하는 데이터

귀사에서 VMware CEIP(고객 환경 향상 프로그램)에 참여하며 클라이언트에서 클라이언트 데이터 공유를 사용하도록 설정한 경우 VMware는 클라이언트 시스템에 대한 데이터를 수집합니다.

VMware는 하드웨어 및 소프트웨어 호환성에 대한 우선 순위를 지정하기 위해 클라이언트의 데이터를 수집합니다. Horizon Administrator가 CEIP에 참여하기로 선택했다면 VMware는 고객 요구 사항에 대한 대응을 개선하기 위해 배포에 관한 익명 데이터를 수집합니다. 조직을 식별할 수 있는 데이터는 수집하지 않습니다. 클라이언트 정보는 먼저 연결 서버로 전송된 다음 서버, 데스크톱 풀 및 원격 데스크톱의 데이터와 함께 VMware로 전송됩니다.

CEIP에 참여하려면 연결 서버를 설치하는 관리자가 연결 서버 설치 마법사를 실행하는 동안에 참여를 선택하거나 설치 후 Horizon Console에서 옵션을 설정하면 됩니다.

표 1-2. CEIP를 위해 수집되는 클라이언트 데이터

설명	필드 이름	이 필드는 익명으로 처리됩니까?	예시 값
애플리케이션을 제작한 회사	<client_vendor>	아니요	VMware
제품 이름	<client_product>	아니요	VMware Horizon HTML Access
클라이언트 제품 버전	<client_version>	아니요	5.3.0- <i>build_number</i>
클라이언트 바이너리 아키텍처	<client_arch>	아니요	예시에 포함되는 값은 다음과 같습니다. ■ 브라우저 ■ arm
브라우저의 기본 아키텍처	<browser_arch>	아니요	예시에 포함되는 값은 다음과 같습니다. ■ Win32 ■ Win64 ■ MacIntel ■ iPad ■ Linux armv81(Android Chrome 지원용)

표 1-2. CEIP를 위해 수집되는 클라이언트 데이터 (계속)

설명	필드 이름	이 필드는 익명으로 처리됩니까?	예시 값
브라우저 사용자 에이전트 문자열	<browser_user_agent>	아니요	예시에 포함되는 값은 다음과 같습니다. <ul style="list-style-type: none"> ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (Gecko 와 같은 KHTML) ■ Chrome/3.0.1750 ■ Safari/703.00 ■ Edge/13.10586
브라우저의 내부 버전 문자열	<browser_version>	아니요	예시에 포함되는 값은 다음과 같습니다. <ul style="list-style-type: none"> ■ 7.0.3(Safari용), ■ 44.0(Firefox용) ■ 13.10586(Edge용)
브라우저의 코어 구현	<browser_core>	아니요	예시에 포함되는 값은 다음과 같습니다. <ul style="list-style-type: none"> ■ Chrome ■ Safari ■ Firefox ■ Internet Explorer ■ Edge
브라우저가 핸드헬드 디바이스에서 실행되는지 여부	<browser_is_handheld>	아니요	true

최종 사용자용 HTML Access 구성

2

최종 사용자가 HTML Access에 대한 URL을 입력할 때 표시되는 웹 페이지의 모양을 변경할 수 있습니다. 또한 이미지 품질, 사용된 포트 및 기타 설정을 제어하는 그룹 정책도 설정할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 최종 사용자용 VMware Horizon 웹 포털 페이지 구성
- URI를 사용하여 HTML Access 웹 클라이언트 구성
- HTML Access 그룹 정책 설정

최종 사용자용 VMware Horizon 웹 포털 페이지 구성

HTML Access를 통한 원격 데스크톱 연결 아이콘 또는 Horizon Client 다운로드 아이콘을 표시하거나 숨기도록 이 웹 페이지를 구성할 수 있습니다. 또한 이 페이지에 다른 링크를 구성할 수도 있습니다.

기본적으로 웹 포털 페이지는 기본 Horizon Client 다운로드 및 설치 아이콘과 HTML Access를 통한 연결 아이콘을 둘 다 표시합니다. 사용되는 다운로드 링크는 `portal-links-html-access.properties` 파일에 정의된 기본값에서 결정됩니다.

그러나 링크가 내부 웹 서버를 가리키도록 하거나 고유 서버에서 특정 클라이언트 버전이 사용 가능하도록 만들 수 있습니다. `portal-links-html-access.properties` 파일의 내용을 수정하여 다른 다운로드 URL을 가리키도록 포털 페이지를 재구성할 수 있습니다. 해당 파일이 사용 가능하지 않거나 비어 있고 `oslinks.properties` 파일이 있으면 `oslinks.properties` 파일이 설치 관리자 파일의 링크 값을 결정하는 데 사용됩니다.

`oslinks.properties` 파일은 `설치 디렉토리\VMware\VMware View\Server\broker\Webapps\portal\WEB-INF` 폴더에 설치됩니다. 이 파일이 HTML Access 세션 중에 없으면 다운로드 링크는 기본적으로 `https://www.vmware.com/go/viewclients`로 이동됩니다. 파일에는 다음과 같은 기본값이 포함되어 있습니다.

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
```

```
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipijfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

portal-links-html-access.properties 또는 oslinks.properties 파일에서 특정 클라이언트 운영 체제에 대한 설치 관리자 링크를 만들 수 있습니다. 예를 들어 Mac OS X 시스템에서 포털 페이지를 검색하는 경우 기본 Mac OS X 설치 관리자에 대한 링크가 나타납니다. Windows 또는 Linux 클라이언트의 경우 32비트 및 64비트 설치 관리자 각각에 대한 링크를 만들 수 있습니다.

절차

- 1 연결 서버 호스트에서 텍스트 편집기로 portal-links-html-access.properties 파일을 엽니다.

이 파일의 위치는 *CommonAppDataFolder\VMware\WDM\portal\portal-links-html-access.properties* 입니다. Windows Server 2008 운영 체제의 경우 *CommonAppDataFolder* 디렉토리가 *C:\ProgramData*입니다. Windows Explorer에서 *C:\ProgramData* 폴더를 표시하려면 폴더 옵션 대화 상자를 사용하여 숨겨진 폴더를 표시해야 합니다.

portal-links-html-access.properties 파일이 없고 oslinks.properties 파일이 있으면 <설치 디렉토리>\VMware\VMware View\Server\broker\Webapps\portal\WEB-INF\oslinks.properties 파일을 열고 특정 설치 관리자 파일을 다운로드하는 데 사용할 URL을 수정합니다.

참고 Horizon 7 5.x 이하 릴리스의 사용자 지정은 portal-links.properties 파일에 저장되며, 이 파일은 portal-links-html-access.properties 파일과 동일한 *CommonAppDataFolder\VMware\WDM\portal* 디렉토리에 있습니다.

- 2 구성 속성을 편집하여 적절하게 설정합니다.

기본적으로 설치 관리자 아이콘 및 HTML Access 아이콘이 모두 활성화되어 있으며 링크는 VMware 웹 사이트의 클라이언트 다운로드 페이지를 가리킵니다. 아이콘을 비활성화하여 웹 페이지에서 아이콘을 제거하려면 속성을 false로 설정합니다.

참고 oslinks.properties 파일은 특정 설치 관리자 파일에 대한 링크를 구성하는 데만 사용할 수 있습니다. 아래 나열된 다른 옵션은 지원하지 않습니다.

옵션	속성 설정
HTML Access 비활성화	<p>enable.webclient=false</p> <p>이 옵션이 false로 설정되었지만 enable.download 옵션이 true로 설정된 경우 사용자는 기본 Horizon Client 설치 관리자를 다운로드하는 웹 페이지로 연결됩니다. 두 옵션이 모두 false로 설정되면 사용자에게 다음 메시지가 표시됩니다. "이 연결 서버 액세스에 대한 지침은 로컬 관리자에게 문의하십시오."</p>
Horizon Client 다운로드 비활성화	<p>enable.download=false</p> <p>이 옵션이 false로 설정되었지만 enable.webclient 옵션이 true로 설정된 경우 사용자는 HTML Access 로그인 웹 페이지로 연결됩니다. 두 옵션이 모두 false로 설정되면 사용자에게 다음 메시지가 표시됩니다. "이 연결 서버 액세스에 대한 지침은 로컬 관리자에게 문의하십시오."</p>

옵션	속성 설정
Horizon Client 다운로드용 웹 페이지의 URL 변경	<code>link.download=https://url-of-web-server</code> 고유 웹 페이지를 만들려면 이 속성을 사용합니다.
특정 설치 관리자에 대한 링크 생성	<p>다음 예에서는 전체 URL을 표시하지만 설치 관리자 파일을 downloads 디렉토리에 배치할 경우 상대 URL을 사용할 수 있으며 이 디렉토리는 다음 단계에서 설명한 대로 연결 서버의 C:\Program Files\VMware\VMware View\Server\broker\Webapps\ 디렉토리 아래 위치합니다.</p> <ul style="list-style-type: none"> ■ 설치 관리자를 다운로드하기 위한 일반 링크: <div> <code>link.download=https://server/downloads</code> </div> ■ 32비트 Windows 설치 관리자: <div> <code>link.win32=https://서버/downloads/VMware-Horizon-Client-x86-빌드 번호.exe</code> </div> ■ 64비트 Windows 설치 관리자: <div> <code>link.win64=https://서버/downloads/VMware-Horizon-Client-x86_64-빌드 번호.exe</code> </div> ■ Windows Phone 설치 관리자: <div> <code>link.winmobile=https://서버/downloads/VMware-Horizon-Client-빌드 번호.appx</code> </div> ■ 32비트 Linux 설치 관리자: <div> <code>link.linux32=https://서버/downloads/VMware-Horizon-Client-빌드 번호.x86.bundle</code> </div> ■ 64비트 Linux 설치 관리자: <div> <code>link.linux64=https://서버/downloads/VMware-Horizon-Client-빌드 번호.x64.bundle</code> </div> ■ Mac OS X 설치 관리자: <div> <code>link.mac=https://서버/downloads/VMware-Horizon-Client-빌드 번호.dmg</code> </div> ■ iOS 설치 관리자: <div> <code>link.ios=https://서버/downloads/VMware-Horizon-Client-iPhoneOS-빌드 번호.ipa</code> </div> ■ Android 설치 관리자: <div> <code>link.android=https://서버/downloads/VMware-Horizon-Client-AndroidOS-빌드 번호.apk</code> </div> ■ Chrome OS 설치 관리자: <div> <code>link.chromeos=https://서버/downloads/VMware-Horizon-Client-ChromeOS-빌드 번호.apk</code> </div>
로그인 페이지의 도움말 링크에 대한 URL 변경	<code>link.help</code> 기본적으로 이 링크는 VMware 웹 사이트에서 호스팅되는 도움말 시스템을 가리킵니다. 도움말 링크는 로그인 페이지 맨 아래쪽에 표시됩니다.

- 3 사용자 VMware 웹 사이트 이외의 위치에서 설치 관리자를 다운로드하도록 하려면 설치 관리자 파일이 배치될 HTTP 서버에 설치 관리자 파일을 둡니다.

이 위치는 이전 단계의 `portal-links-html-access.properties` 파일 또는 `oslinks.properties` 파일에서 지정한 URL과 일치해야 합니다. 예를 들어, 연결 서버 호스트의 `downloads` 디렉토리에 파일을 배치하려면 다음 경로를 사용합니다.

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

그런 다음 설치 관리자 파일에 대한 링크는 `/downloads/client-installer-file-name` 형식의 상대 URL을 사용할 수 있습니다.

- 4 Horizon Web Component 서비스를 다시 시작합니다.

URI를 사용하여 HTML Access 웹 클라이언트 구성

URI(Uniform Resource Identifier)를 사용하면 최종 사용자가 클릭하여 HTML Access Web client를 실행하고 Horizon Connection Server에 연결하며 특정 구성 옵션으로 특정 데스크톱 또는 애플리케이션을 실행하는 링크가 포함된 웹 페이지나 이메일을 만들 수 있습니다.

최종 사용자를 위한 웹 또는 e-메일 링크를 생성하여 원격 데스크톱 또는 애플리케이션에 연결하는 프로세스를 간소화할 수 있습니다. 다음 정보의 일부 또는 모두를 제공하는 URI를 구성하여 이러한 링크를 생성해야 최종 사용자가 정보를 제공할 필요가 없어집니다.

- Horizon Connection Server 주소
- Horizon Connection Server의 포트 번호
- Active Directory 사용자 이름
- RADIUS 또는 RSA SecurID 사용자 이름(Active Directory 사용자 이름과 다른 경우)
- 도메인 이름
- 데스크톱 또는 애플리케이션 디스플레이 이름
- 세션 탐색, 재설정, 로그오프, 시작 등의 작업

HTML Access용 URI 생성 구문

구문에는 서버를 지정하는 경로 부분과 필요한 경우 사용자, 원격 데스크톱 또는 게시된 애플리케이션, 작업 또는 구성 옵션을 지정하는 쿼리가 포함됩니다.

URI 규격

다음 구문을 사용하여 HTML Access 시작에 필요한 URI를 만듭니다.

```
https://authority-part[/?query-part]
```

authority-part

서버 주소를 지정하고 필요한 경우 기본값이 아닌 포트 번호를 지정합니다. 서버 이름은 DNS 구문에 따라야 합니다.

포트 번호를 지정하려면 다음 구문을 사용하십시오.

```
server-address:port-number
```

query-part

사용할 구성 옵션이나 수행할 작업을 지정합니다. 쿼리는 대소문자를 구분하지 않습니다. 여러 쿼리를 사용하려면 쿼리 사이에 앰퍼샌드(&)를 사용합니다. 쿼리가 서로 충돌할 경우, 목록의 마지막 쿼리가 사용됩니다. 다음 구문을 사용하십시오.

```
query1=value1[&query2=value2...]
```

쿼리 부분을 생성할 때는 다음 지침을 따라야 합니다.

- 지원되는 쿼리를 하나 이상 사용하지 않을 경우 기본 VMware Horizon 웹 포털 페이지가 표시됩니다.
- 쿼리 부분에서는 일부 특수 문자가 지원되지 않으며 해당 문제에 대해 URL 인코딩 형식을 사용해야 합니다. 즉, 파운드 기호(#)에는 **%23**을, 퍼센트 기호(%)에는 **%25**를, 앰퍼샌드(&)에는 **%26**을, at 기호(@)에는 **%40**을, 백슬래시(\)에는 **%5C**를 사용해야 합니다.

URL 인코딩에 대한 자세한 내용은 http://www.w3schools.com/tags/ref_urlencode.asp를 참조하십시오.

- 쿼리 부분의 비 ASCII 문자는 우선 UTF-8[STD63]에 따라 인코딩되어야 하며 해당 UTF-8 시퀀스의 각 8진수는 URI 문자로 표현되도록 퍼센트로 인코딩되어야 합니다.

ASCII 문자 인코딩에 대한 자세한 내용은 <http://www.utf8-chartable.de/>의 URL 인코딩 참조를 참고하십시오.

지원되는 쿼리

이 항목에서는 HTML Access에 지원되는 쿼리를 나열합니다. 데스크톱 클라이언트 및 모바일 클라이언트 등과 같은 여러 유형의 클라이언트에 대한 URI를 생성하는 경우 각 유형의 클라이언트 시스템에 대한 설치 및 설정 문서를 참조하십시오.

작업

표 2-1. 작업 쿼리와 함께 사용할 수 있는 값

값	설명
browse	지정된 서버에서 호스트된 사용 가능한 원격 데스크톱 및 게시된 애플리케이션 목록을 표시합니다. 이 작업을 사용하면 원격 데스크톱 또는 게시된 애플리케이션을 지정할 필요는 없습니다.
start-session	지정된 원격 데스크톱 또는 게시된 애플리케이션을 시작합니다. 작업 쿼리가 제공되지 않고 원격 데스크톱 또는 게시된 애플리케이션 이름이 제공되는 경우, start-session이 기본 작업입니다.
reset	지정된 원격 데스크톱을 종료하고 다시 시작합니다. 저장하지 않은 데이터는 손실됩니다. 원격 데스크톱 재설정은 PC에 있는 재설정 버튼을 누르는 것과 같습니다. 이 작업은 게시된 애플리케이션에 유효하지 않습니다.

표 2-1. 작업 쿼리와 함께 사용할 수 있는 값 (계속)

값	설명
logoff	원격 데스크톱의 게스트 운영 체제에서 사용자를 로그아웃시킵니다. 이 작업은 게시된 애플리케이션에 유효하지 않습니다.
restart	사용자가 다시 시작 작업 요청을 확인한 후 기본 원격 데스크톱을 종료하고 다시 시작합니다. 이 작업은 게시된 애플리케이션에 유효하지 않습니다.

applicationId

게시된 애플리케이션 표시 이름입니다. 표시 이름은 애플리케이션 풀이 생성될 때 Horizon Console에서 지정한 이름입니다. 표시 이름에 공백이 포함되어 있으면 브라우저는 %20을 사용하여 공백을 나타냅니다.

args

게시된 애플리케이션이 시작될 때 추가할 명령줄 인수를 지정합니다. 구문 args=값을 사용합니다. 여기서 값은 문자열입니다. 다음 문자에는 % 인코딩을 사용하십시오.

- 콜론(:)에는 %3A를 사용합니다.
- 백슬래시(\)에는 %5C를 사용합니다.
- 공백()에는 %20을 사용합니다.
- 큰따옴표 표시(")에는 %22를 사용합니다.

예를 들어 Notepad++ 애플리케이션에 대해 파일 이름 "My new file.txt"를 지정하려면 %22My%20new%20file.txt%22를 사용합니다.

desktopId

원격 데스크톱 표시 이름입니다. 표시 이름은 데스크톱 풀이 생성될 때 Horizon Console에서 지정한 이름입니다. 표시 이름에 공백이 포함되어 있으면 브라우저는 %20을 사용하여 공백을 나타냅니다.

domainName

원격 데스크톱 또는 게시된 애플리케이션에 연결 중인 사용자와 연결된 NETBIOS 도메인 이름입니다. 예를 들어 mycompany.com보다는 mycompany를 사용합니다.

tokenUserName

RSA 또는 RADIUS 사용자 이름입니다. RSA 또는 RADIUS 사용자 이름이 Active Directory 사용자 이름과 다른 경우에만 이 쿼리를 사용합니다. 이 쿼리를 지정하지 않고 RSA 또는 RADIUS 인증이 필요한 경우, Windows 사용자 이름을 사용합니다.

userName

원격 데스크톱 또는 게시된 애플리케이션에 연결 중인 Active Directory 사용자입니다. 사용자 이름은 다음 형식 중 하나로 표시할 수 있습니다.

- *userName*
- *domainName%5CuserName*
- UPN(사용자 계정 이름) 즉, *userName@domainName*

unauthenticatedAccessEnabled

이 옵션을 **true**로 설정하면 인증되지 않은 액세스 기능이 기본적으로 사용되도록 설정됩니다. HTML Access가 시작되고 익명 사용자 계정이 표시됩니다. 구문 예는 **unauthenticatedAccessEnabled=true**입니다.

unauthenticatedAccessAccount

인증되지 않은 액세스 기능이 사용되도록 설정되면 사용할 계정을 설정합니다. 인증되지 않은 액세스가 사용되지 않도록 설정되면 이 쿼리는 무시됩니다. **anonymous1** 사용자 계정을 사용할 때의 구문 예는 **unauthenticatedAccessAccount=anonymous1**입니다.

URI의 예

URI를 사용하여 하이퍼텍스트 링크나 버튼을 만들고 e-메일 또는 웹 페이지에 이 링크를 포함할 수 있습니다. 예를 들어 최종 사용자가 이러한 링크를 클릭하여 특정 원격 데스크톱 또는 애플리케이션을 지정된 시작 옵션으로 열 수 있습니다.

URI 구문 예

각 URI 예에는 최종 사용자가 URI 링크를 클릭할 경우 나타나는 내용에 대한 설명이 이어집니다. 쿼리는 대소문자를 구분하지 않습니다. 예를 들어 **domainName** 또는 **domainname**를 사용할 수 있습니다.

1 `https://horizon.mycompany.com/?domainName=finance&userName=fred`

HTML Access Web client가 실행되고 `horizon.mycompany.com` 서버에 연결됩니다. 로그인 상자에서 **사용자 이름** 텍스트 상자에 **fred**라는 이름이 채워지고 **도메인** 텍스트 상자는 **finance**로 채워집니다. 사용자는 암호만 제공해야 합니다.

2 `https://horizon.mycompany.com/?userName=finance%5Cfred`

HTML Access Web client가 실행되고 `horizon.mycompany.com` 서버에 연결됩니다. 로그인 상자에서 **사용자 이름** 텍스트 상자에 **finance\fred**라는 이름이 채워집니다. 사용자는 암호만 제공해야 합니다.

3 `https://horizon.mycompany.com/?userName=fred@finance`

HTML Access Web client가 실행되고 `horizon.mycompany.com` 서버에 연결됩니다. 로그인 상자에서 **사용자 이름** 텍스트 상자에 **fred@finance**라는 이름이 채워집니다. 사용자는 암호만 제공해야 합니다.

4 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=start-session`

HTML Access Web client가 실행되고 `horizon.mycompany.com` 서버에 연결됩니다. 로그인 상자에서 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인에 성공하고 나면 클라이언트는 디스플레이 이름이 **Primary Desktop**(기본 데스크톱)으로 표시되는 데스크톱에 연결되고 사용자는 게스트 운영 체제에 로그인됩니다.

5 `https://horizon.mycompany.com/?applicationId=Notepad&action=start-session`

HTML Access Web client가 실행되고 `horizon.mycompany.com` 서버에 연결됩니다. 로그인 상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 성공적으로 로그인한 후에 메모장 애플리케이션이 실행됩니다.

6 `https://horizon.mycompany.com:7555/?desktopId=Primary%20Desktop`

예를 들어 연결 서버의 기본 포트 7555를 사용하는 것을 제외하면 이 URI는 이전 예와 동일한 효과를 가집니다. 기본 포트는 443입니다. 데스크톱 식별자가 제공되므로 `start-session` 작업이 URI에 포함되지 않아도 데스크톱이 실행됩니다.

7 `https://horizon.mycompany.com/?applicationId=Primary%20Application&desktopId=Primary%20Desktop`

이 URI는 애플리케이션 및 데스크톱 둘 다를 지정합니다. 애플리케이션과 데스크톱을 모두 지정하면 데스크톱만 실행됩니다.

8 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=reset`

HTML Access 웹 클라이언트가 실행되고 `horizon.mycompany.com` 서버에 연결됩니다. 로그인 상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인에 성공하면 Primary Desktop(기본 데스크톱)에 대한 재설정 작업을 확인하라는 대화 상자가 클라이언트에 표시됩니다.

참고 이 작업은 최종 사용자가 시스템을 재설정할 수 있도록 Horizon 관리자가 허용한 경우에만 사용할 수 있습니다.

9 `https://horizon.mycompany.com/?My%20Notepad++?args=%22My%20new%20file.txt%22`

서버 `horizon.mycompany.com`에서 My Notepad ++를 열고 애플리케이션 실행 명령에 My new file.txt 인수를 전달합니다. 파일 이름은 공백을 포함하므로 큰따옴표로 묶입니다.

10 `https://horizon.mycompany.com/?Notepad++%2012?args=a.txt%20b.txt`

서버 `horizon.mycompany.com`에서 Notepad ++ 12를 열고 애플리케이션 실행 명령에 a.txt b.txt 인수를 전달합니다. 인수가 큰따옴표로 묶여 있지 않기 때문에 파일 이름이 공백으로 구분되며, Notepad ++에서 두 파일이 따로 열립니다.

참고 명령줄 인수를 사용하는 방식은 애플리케이션마다 다를 수 있습니다. 예를 들어 워드패드에 인수 a.txt b.txt를 전달하면 워드패드에서 a.txt 파일 하나만 열립니다.

11 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=restart`

HTML Access Web client가 실행되고 `horizon.mycompany.com` 서버에 연결됩니다. 로그인 상자에 사용자에게 사용자 이름, 도메인 이름 및 암호를 묻는 메시지가 표시됩니다. 로그인에 성공하면 Primary Desktop(기본 데스크톱)에 대한 다시 시작 작업을 확인하라는 대화 상자가 클라이언트에 표시됩니다.

참고 이 작업은 최종 사용자가 시스템을 다시 시작할 수 있도록 Horizon 관리자가 허용한 경우에만 사용할 수 있습니다.

12 `https://horizon.mycompany.com/?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_user1`

HTML Access Web client가 실행되고 **anonymous_user1** 계정을 사용하여 `horizon.mycompany.com` 서버에 연결됩니다.

HTML 코드 예

URI를 사용하여 e-메일 또는 웹 페이지에 포함할 하이퍼텍스트 링크 및 버튼을 만들 수 있습니다. 다음 예는 첫 번째 URI 예를 사용하여 **Test Link**라는 하이퍼텍스트 링크와 **TestButton**이라는 버튼을 코딩하는 방법을 보여줍니다.

```
<html>
<body>

<a href="https://horizon.mycompany.com/?domainName=finance&userName=fred">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'https://horizon.mycompany.com/?domainName=finance&userName=fred'"></form> <br>

</body>
</html>
```

HTML Access 그룹 정책 설정

HTML Access에서는 VMware Blast 프로토콜을 사용합니다. VMware Blast 프로토콜에 대해 그룹 정책을 구성하여 HTML Access에 대한 그룹 정책을 구성합니다.

자세한 내용은 "Horizon 7에서 원격 데스크톱 기능 구성" 문서의 "데스크톱 풀 및 애플리케이션 풀의 정책 구성" 및 "VMware Blast 정책 설정"을 참조하십시오.

원격 데스크톱 및 게시된 애플리케이션 연결 관리

3

최종 사용자는 Horizon Client를 사용하여 서버에 연결하고, 원격 데스크톱에 로그인하거나 로그오프하고, 게시된 애플리케이션을 사용할 수 있습니다. 문제 해결을 위해 최종 사용자는 원격 데스크톱 및 게시된 애플리케이션을 재설정할 수도 있습니다.

본 장은 다음 항목을 포함합니다.

- 원격 데스크톱 또는 게시된 애플리케이션에 연결
- 자체 서명된 루트 인증서 신뢰
- Workspace ONE 모드에서 서버에 연결
- 인증되지 않은 액세스를 사용하여 게시된 애플리케이션에 연결
- 시간대 설정
- H.264 디코딩 허용
- 로그오프 또는 연결 해제

원격 데스크톱 또는 게시된 애플리케이션에 연결

사용 권한이 있는 원격 데스크톱 및 게시된 애플리케이션에 연결하려면 Active Directory 자격 증명을 사용합니다.

사전 요구 사항

- Active Directory 사용자 이름/암호, RSA SecurID 사용자 이름/암호 또는 RADIUS 인증 자격 증명과 같은 로그인 자격 증명을 얻습니다.
- 로그인을 위한 NETBIOS 도메인 이름을 얻습니다. 예를 들어 mycompany.com 대신 mycompany를 사용할 수 있습니다.

절차

- 1 브라우저를 열고 연결 서버 인스턴스에 대한 URL을 입력합니다.

URL에서 **https**를 사용하고 정규화된 도메인 이름(예: <https://horizon.company.com>)을 사용합니다.

연결 서버에 연결할 때는 항상 SSL이 사용됩니다. SSL 연결의 기본 포트는 443입니다. 연결 서버가 기본 포트를 사용하도록 구성되지 않은 경우에는 다음 예의 형식을 사용합니다.

horizon.company.com:1443.

VMware Horizon 웹 포털이 표시됩니다. 기본적으로 이 페이지는 기본 Horizon Client 다운로드 및 설치 아이콘과 HTML Access를 통한 연결 아이콘을 둘 다 표시합니다.

- 2 (선택 사항) 이 화면을 건너뛰고 항상 HTML Access를 사용하려면 여기를 클릭** 확인란을 선택합니다.

선택 사항이 현재 사용 중인 브라우저의 로컬 스토리지에 저장됩니다. 다음번에 동일한 브라우저 유형 및 동일한 클라이언트 시스템을 사용하여 연결 서버 인스턴스에 대한 URL을 입력하면 로그인 화면으로 직접 이동됩니다. 동일한 클라이언트 시스템의 다른 브라우저 유형을 사용하거나 다른 클라이언트 시스템의 동일한 브라우저 유형을 사용하는 경우 VMware Horizon 웹 포털이 나타납니다. VMware Horizon 웹 포털을 표시하려면 브라우저의 캐시를 지웁니다.

- 3 VMware Horizon HTML Access** 아이콘을 클릭합니다.

- 4** 로그인 대화 상자에서 RSA SecurID 자격 증명 또는 RADIUS 인증 자격 증명을 묻는 메시지가 표시되면 사용자 이름과 암호를 입력하고 **로그인**을 클릭합니다.

암호에 PIN 및 토큰에서 생성된 번호가 모두 포함될 수 있습니다.

- 5** RSA SecurID 자격 증명 또는 RADIUS 인증 자격 증명에 대해 묻는 메시지가 다시 표시되면 토큰에서 다음에 생성된 번호를 입력합니다.

PIN을 입력하거나 이전에 입력한 동일한 생성 번호를 입력하지 마십시오. 필요한 경우 새 번호가 생성될 때까지 기다리십시오.

이 단계는 첫 번째 인증번호를 잘못 입력했거나 RSA 서버의 구성 설정이 변경된 경우에만 필요합니다.

- 6** [로그인] 대화 상자에 로그인 자격 증명을 입력합니다.

- a [사용자 이름] 텍스트 상자에 *username*, *domain\username* 또는 *username@domain* 형식으로 유효한 Active Directory 사용자 이름을 입력합니다.

[도메인] 텍스트 상자가 사용되지 않도록 설정된 경우 *domain\username* 또는 *username@domain* 형식을 사용해야 합니다.

- b 암호를 입력하십시오.

- c (선택 사항) [도메인] 텍스트 상자가 사용되도록 설정되어 있지만 올바르게 채워지지 않은 경우 도메인 이름을 선택합니다.

참고 로그인 프로세스를 취소하려면 로그인 프로세스가 완료되기 전에 **취소**를 클릭합니다.

- 7** (선택 사항) 원격 데스크톱 또는 게시된 애플리케이션에서 사용하는 시간대를 수동으로 설정해야 하는 경우 데스크톱 및 애플리케이션 선택기 화면의 오른쪽 상단 모서리에 있는 **설정** 도구 모음 버튼을 클릭합니다. **자동으로 시간대 설정** 옵션을 끄고 드롭다운 메뉴에서 시간대 하나를 선택합니다. **시간대 설정**의 내용을 참조하십시오.

- 8 (선택 사항) 데스크톱 및 애플리케이션 선택기 화면에서 액세스하려는 항목을 선택하기 전에 원격 데스크톱 또는 게시된 애플리케이션을 즐겨찾기로 표시하려면 해당 데스크톱 또는 게시된 애플리케이션 아이콘 안에 있는 회색 별 모양을 클릭합니다.

별 모양 아이콘이 회색에서 노란색으로 바뀝니다. 다음번에 로그인할 때 브라우저 창의 오른쪽 위에서 별 모양 아이콘을 클릭하여 즐겨찾기만 표시할 수도 있습니다.

- 9 액세스하려는 원격 데스크톱 또는 게시된 애플리케이션에 대한 아이콘을 클릭합니다.

원격 데스크톱 또는 게시된 애플리케이션이 브라우저에 표시됩니다. 탐색 사이드바도 사용할 수 있습니다. 브라우저 창 왼쪽의 탭을 클릭하여 사이드바를 표시할 수 있습니다. 사이드바를 사용하여 다른 원격 데스크톱 또는 게시된 애플리케이션에 액세스하고, [설정] 창을 표시하고, 텍스트를 복사한 후 붙여 넣는 등의 작업도 수행할 수 있습니다.

다음에 수행할 작업

데스크톱 또는 게시된 애플리케이션에 연결하자마자 연결이 끊기고, 보안 인증서를 수락하려면 링크를 클릭하라는 메시지가 표시되는 경우 사용자는 인증서의 신뢰 여부를 선택할 수 있습니다. [자체 서명된 루트 인증서 신뢰](#)의 내용을 참조하십시오.

자체 서명된 루트 인증서 신뢰

경우에 따라 원격 데스크톱 또는 게시된 애플리케이션에 처음 연결할 때, 원격 시스템에서 사용하는 자체 서명된 인증서를 수락하라는 메시지가 브라우저에 표시될 수 있습니다. 인증서를 먼저 신뢰해야 원격 데스크톱 또는 게시된 애플리케이션에 연결할 수 있습니다.

대부분의 브라우저에는 자체 서명된 인증서를 영구적으로 신뢰할 수 있는 옵션이 제공됩니다. 인증서를 영구적으로 신뢰하는 경우 브라우저를 다시 시작할 때마다 인증서를 확인해야 합니다. Safari 브라우저를 사용하는 경우, 연결을 설정하려면 보안 인증서를 영구적으로 신뢰해야 합니다.

절차

- 1 브라우저가 신뢰할 수 없는 인증서 경고나 연결이 전용이 아니라는 경고를 표시하면 인증서를 검토하여 회사에서 사용하는 인증서와 일치하는지 확인하십시오.

시스템 관리자에게 지원을 요청해야 할 수도 있습니다. 예를 들어 Chrome의 경우 다음 절차를 사용할 수 있습니다.

- 주소 표시줄에서 잠금 아이콘을 클릭합니다.
- 인증서 정보** 링크를 클릭합니다.
- 인증서가 회사에서 사용하는 인증서와 일치하는지 확인합니다.

시스템 관리자에게 지원을 요청해야 할 수도 있습니다.

- 2 보안 인증서를 수락합니다.

각 브라우저는 인증서를 수락하거나 항상 신뢰하기 위한 브라우저별 프롬프트를 제공합니다. 예를 들어 Chrome 브라우저에서는 브라우저 페이지에서 **고급** 링크를 클릭한 후 **Proceed to *server-name* (unsafe)**를 클릭합니다.

Safari 브라우저에서는 다음 절차를 사용하여 인증서를 영구적으로 신뢰할 수 있습니다.

- a 신뢰할 수 없는 인증서 대화상자가 표시되면 **인증서 표시** 버튼을 클릭합니다.
- b **항상 신뢰** 확인란을 선택하고 **계속**을 클릭합니다.
- c 메시지가 표시되면 암호를 입력하고 **설정 업데이트**를 클릭합니다.

원격 데스크톱 또는 게시된 애플리케이션이 시작됩니다.

Workspace ONE 모드에서 서버에 연결

Horizon 7 버전 7.2부터 Horizon 관리자는 연결 서버 인스턴스에서 Workspace ONE 모드를 사용하도록 설정할 수 있습니다.

Workspace ONE 모드를 사용하도록 설정하면 Workspace ONE 웹 포털을 통해서만 서버에 연결할 수 있습니다. HTML Access를 통해 서버에 연결하려고 하면 Workspace ONE 웹 포털로 리디렉션됩니다. Workspace ONE 웹 포털을 통해 서버에 연결한 후에는 Workspace ONE 웹 포털을 통해서만 원격 데스크톱 및 게시된 애플리케이션을 시작할 수 있습니다.

Workspace ONE 모드를 사용할 때 사이드바에 모든 사용 권한이 표시되지는 않습니다. 현재 실행 중인 데스크톱 및 게시된 애플리케이션만 표시됩니다.

Workspace ONE 모드를 사용하도록 설정하면 다음과 같은 문제가 발생할 수 있습니다.

- HTML Access를 통해 서버에 액세스할 수 없습니다. 서버에 연결하지 못하거나, 서버가 다른 애플리케이션 또는 서버에서 로그인 자격 증명을 받아야 함을 나타내는 메시지가 표시될 수 있습니다.
- Workspace ONE 웹 포털을 통해 원격 데스크톱 또는 게시된 애플리케이션을 시작한 후에는 HTML Access에서 원격 데스크톱 또는 게시된 애플리케이션을 보거나 시작할 수 없습니다.

인증되지 않은 액세스를 사용하여 게시된 애플리케이션에 연결

인증되지 않은 액세스 사용자 계정이 있는 경우 서버에 익명으로 로그인하고 게시된 애플리케이션에 연결할 수 있습니다.

사전 요구 사항

- **연결 서버 및 보안 서버 준비**에 설명된 관리 작업을 수행하십시오.
- 연결 서버 인스턴스에서 인증되지 않은 액세스 사용자를 설정합니다. 자세한 내용은 “VMware Horizon Console 관리” 문서에서 “게시된 애플리케이션에 인증되지 않은 액세스 제공”을 참조하십시오.

절차

- 1 인증되지 않은 액세스 권한이 있는 서버에 연결하려면 브라우저를 열고 URI(Uniform Resource Identifier)를 입력합니다.

다음 URI 구문 중 하나를 사용합니다.

- `https://authority-part?unauthenticatedAccessEnabled=true`
- `https://authority-part?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_account`

*authority-part*는 서버 주소이고 필요한 경우 기본값이 아닌 포트 번호를 지정합니다. 포트 번호를 지정해야 하는 경우 *server-address:port-number*를 입력합니다.

*anonymous_account*는 인증되지 않은 액세스 사용자 계정입니다.

연결할 때는 항상 TLS를 사용합니다. TLS 연결의 기본 포트는 443입니다. 서버가 기본 포트를 사용하도록 구성되지 않은 경우에는 다음 예의 형식을 사용합니다. **horizon.company.com:1443**.

- 2 (선택 사항) URI에 인증되지 않은 액세스 사용자 계정을 지정하지 않은 경우 **사용자 계정** 드롭다운 메뉴에서 인증되지 않은 액세스 사용자 계정을 선택하고, 필요한 경우 **제출**을 클릭합니다.

하나의 인증되지 않은 액세스 사용자 계정만 사용할 수 있으면 해당 사용자 계정이 기본적으로 선택됩니다.

애플리케이션 선택 창이 나타납니다.

- 3 액세스하려는 게시된 애플리케이션에 대한 아이콘을 클릭합니다.

게시된 애플리케이션이 브라우저에 표시됩니다. 탐색 사이드바도 사용할 수 있습니다. 브라우저 왼쪽에 있는 탭을 클릭하여 사이드바를 표시할 수 있습니다. 사이드바를 사용하여 다른 게시된 애플리케이션에 액세스하고, **설정** 창을 표시하고, 텍스트를 복사한 후 붙여넣는 등의 작업도 수행할 수 있습니다.

참고 인증되지 않은 애플리케이션 세션에 다시 연결할 수 없습니다. 사용자가 클라이언트에서 연결 해제되면 로컬 사용자 세션에서 자동으로 로그오프됩니다.

시간대 설정

원격 데스크톱 또는 게시된 애플리케이션이 사용하는 표준 시간대는 자동으로 로컬 시스템의 표준 시간대로 설정됩니다.

HTML Access 클라이언트를 사용하고 있고 서버 타임 정책으로 인해 표준 시간대를 올바르게 확인할 수 없는 경우 표준 시간대를 수동으로 설정해야 할 수도 있습니다.

원격 데스크톱 또는 게시된 애플리케이션에 연결하기 전에 사용하는 올바른 시간대 정보를 수동으로 설정하려면 데스크톱 및 애플리케이션 선택기 창의 오른쪽 위 모서리에 있는 **설정** 도구 모음 버튼을 클릭합니다. **설정** 창에서 **자동으로 시간대 설정** 옵션을 끄고 드롭다운 메뉴에서 시간대 하나를 선택합니다.

선택한 값은 원격 데스크톱 또는 게시된 애플리케이션에 연결 시 사용하는 선호 시간대로 저장됩니다.

이미 원격 데스크톱 또는 게시된 애플리케이션에 연결된 경우 데스크톱 및 애플리케이션 선택기 창으로 돌아가 현재 시간대 설정을 변경합니다.

자동으로 시간대 설정 옵션은 사이드바에서 액세스할 수 있는 **설정** 창에서 사용할 수 없습니다.

참고 Android 디바이스에서 Chrome 브라우저를 사용하고 있고 **자동으로 시간대 설정** 옵션이 **true**로 설정되어 있을 때 Android 시스템의 표준 시간대를 변경하면 새 표준 시간대가 원격 데스크톱과 자동으로 동기화되지 않습니다. 이 문제는 Android 시스템의 Chrome 제한 사항입니다. 선택한 표준 시간대를 동기화하려면 Android 디바이스 및 Chrome 브라우저를 다시 시작해야 합니다.

H.264 디코딩 허용

Chrome 브라우저를 사용하는 경우 원격 데스크톱 및 게시된 애플리케이션 세션에 대해 클라이언트에 서 H.264 디코딩을 허용할 수 있습니다.

H.264는 비디오 압축을 위한 업계 표준으로, 디지털 비디오를 저장하거나 전송할 때 적은 용량이 사용되는 형식으로 변환하는 프로세스입니다.

H.264 디코딩을 허용할 경우 에이전트에서 H.264 인코딩을 지원하면 HTML Access 클라이언트에서 H.264 디코딩을 사용합니다. 에이전트에서 H.264 인코딩을 지원하지 않으면 HTML Access 클라이언트에서 JPEG/PNG 디코딩을 사용합니다.

원격 데스크톱이나 게시된 애플리케이션에 연결된 경우 사이드바에서 사용할 수 있는 **설정** 창의 **H.264 디코딩 허용** 옵션을 켜서 H.264 디코딩을 허용할 수 있습니다. 새 설정을 적용하려면 원격 데스크톱 또는 게시된 애플리케이션에서 연결을 끊었다가 다시 연결해야 합니다.

원격 데스크톱 또는 게시된 애플리케이션에 연결되어 있지 않으면 데스크톱 및 애플리케이션 선택기 창의 오른쪽 위 모서리에 있는 **설정** 도구 모음 버튼을 클릭하고 **설정** 창의 **H.264 디코딩 허용** 옵션을 켜 수 있습니다. 새 설정은 설정을 변경한 후에 연결된 모든 세션에 적용됩니다.

로그오프 또는 연결 해제

로그오프하지 않고 원격 데스크톱과의 연결을 끊을 경우, 원격 데스크톱의 애플리케이션은 열려 있는 상태로 유지될 수 있습니다. 또한 서버와의 연결을 해제하고 게시된 애플리케이션은 실행 중인 상태로 둘 수도 있습니다.

절차

- ◆ 서버에서 로그아웃하고 원격 데스크톱에서 연결 해제(로그아웃하지는 않음)하거나 게시된 애플리케이션을 종료합니다.

옵션	조치
원격 데스크톱 또는 게시된 애플리케이션에 연결하기 전에 데스크톱 및 애플리케이션 선택기 창에서	창 오른쪽 상단 모서리에 있는 로그아웃 도구 모음 버튼을 클릭합니다.
원격 데스크톱 또는 게시된 애플리케이션에 연결되었을 때 사이드바에서	사이드바 맨 위에 있는 로그아웃 도구 막대 버튼을 클릭합니다.

- ◆ 게시된 애플리케이션을 닫습니다.

옵션	조치
게시된 애플리케이션 내에서	게시된 애플리케이션 창의 모서리에 있는 X (닫기) 버튼을 클릭하는 등의 일반적인 방법으로 게시된 애플리케이션을 종료합니다.
사이드바에서	사이드바에서 실행 중 목록에 있는 게시된 애플리케이션 이름 옆의 X 를 클릭합니다.

- ◆ 원격 데스크톱에서 로그오프하거나 연결을 끊습니다.

옵션	조치
원격 데스크톱 내에서	로그오프하려면 Windows 시작 메뉴를 사용하여 로그오프합니다.
사이드바에서	<p>로그오프하고 연결을 끊으려면 사이드바에서 실행 중 목록의 원격 데스크톱 이름 옆에 있는 메뉴 열기 도구 모음 버튼을 클릭하고 로그오프를 선택합니다. 원격 데스크톱에서 열려 있는 파일은 저장되지 않고 닫힙니다.</p> <p>로그오프하지 않고 연결을 끊으려면 실행 중 목록의 원격 데스크톱 이름 옆에 있는 메뉴 열기 도구 모음 버튼을 클릭하고 닫기를 선택합니다.</p> <p>참고 Horizon Administrator는 연결을 끊을 때 자동으로 로그오프하도록 원격 데스크톱을 구성할 수 있습니다. 그러한 경우, 원격 데스크톱에 열려 있는 모든 애플리케이션은 닫힙니다.</p>

원격 데스크톱 또는 게시된 애플리케이션 사용

4

클라이언트는 도구 모음 버튼이 있는 탐색 사이드바를 제공하므로 원격 데스크톱이나 게시된 애플리케이션에서 쉽게 연결 해제하거나 버튼을 클릭하여 Ctrl+Alt+Delete 키 조합과 동일한 작업을 보낼 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 기능 지원 표
- 사이드바 사용
- 모니터 및 화면 해상도
- 전체 화면 모드 사용
- 웹캠 및 마이크에 대한 실시간 오디오-비디오 기능 사용
- 원격 데스크톱 세션 공유
- 텍스트 복사 및 붙여넣기
- 클라이언트와 원격 데스크톱 또는 게시된 애플리케이션 간에 파일 전송
- 여러 클라이언트 디바이스에서 게시된 애플리케이션의 다중 세션 사용
- 사운드
- 바로 가기 키 조합
- 국제화
- 국제 키보드

기능 지원 표

브라우저 기반 HTML Access 클라이언트에서 원격 데스크톱 또는 애플리케이션에 액세스하는 경우 일부 기능은 사용할 수 없습니다.

단일 사용자 가상 시스템 데스크톱에 대한 기능 지원

표 4-1. HTML Access를 통해 지원되는 기능

기능	Windows 7 데스크톱	Windows 8.x 데스크톱	Windows 10 데스크톱	Windows Server 2008 R2 데스크톱	Windows Server 2012 R2 데스크톱	Windows Server 2016 또는 Windows Server 2019 데스크톱
RSA SecurID 또는 RADIUS	X	X	X	X	X	X
단일 로그인	X	X	X	X	X	X
RDP 디스플레이 프로토콜						
PCoIP 디스플레이 프로토콜						
VMware Blast 디스플레이 프로토콜	X	X	X	X	X	X
USB 리디렉션						
실시간 오디오-비디오 (RTAV)	X	X	X	X	X	X
Windows Media MMR						
가상 인쇄						
위치 기반 인쇄	X	X	X	X	X	X
스마트 카드						
다중 모니터	X	X	X	X	X	X

이러한 기능 및 해당 제한 사항에 대한 설명은 “Horizon 7 아키텍처 계획” 문서를 참조하십시오.

RDS 호스트의 세션 기반 데스크톱 및 호스팅된 애플리케이션에 대한 기능 지원

RDS 호스트는 Windows 원격 데스크톱 서비스와 Horizon Agent가 설치되어 있는 서버 컴퓨터입니다. 여러 명의 사용자가 동시에 RDS 호스트에서 데스크톱 및 애플리케이션 세션을 사용할 수 있습니다. RDS 호스트는 물리적 시스템 또는 가상 시스템일 수 있습니다.

참고 다음 표에는 HTML Access를 사용하는 경우에 RDS 호스트에서 사용할 수 있는 기능에 대한 행만 포함되어 있습니다. Windows용 Horizon Client와 같이 원래 설치된 Horizon Client를 사용하는 경우 추가 기능을 사용할 수 있습니다.

표 4-2. RDS 호스트의 HTML Access에 대해 지원되는 기능

기능	Windows Server 2008 R2 RDS 호스트	Windows Server 2012 또는 2012 R2 RDS 호스트	Windows Server 2016	Windows Server 2019
RSA SecurID 또는 RADIUS	X	X	Horizon Agent 7.0.2 이상	Horizon Agent 7.7 이상
단일 로그인	X	X	Horizon Agent 7.0.2 이상	Horizon Agent 7.7 이상

표 4-2. RDS 호스트의 HTML Access에 대해 지원되는 기능 (계속)

기능	Windows Server 2008 R2 RDS 호스트	Windows Server 2012 또는 2012 R2 RDS 호스트	Windows Server 2016	Windows Server 2019
VMware Blast 디스플레이 프로토콜	X	X	Horizon Agent 7.0.2 이상	Horizon Agent 7.7 이상
위치 기반 인쇄	X(가상 시스템만 해당)	X(가상 시스템만 해당)	Horizon Agent 7.0.2 이상(가상 시스템만 해당)	Horizon Agent 7.7 이상
실시간 오디오-비디오 (RTAV)	Horizon Agent 7.0.2 이상	Horizon Agent 7.0.2 이상	Horizon Agent 7.0.3 이상	Horizon Agent 7.7 이상
다중 모니터(세션 기반 데스크톱만 해당)	X	X	X	X

각 게스트 운영 체제의 버전에 대한 자세한 내용은 “Horizon 7 설치” 문서의 “Horizon Agent에 대해 지원되는 운영 체제”를 참조하십시오.

사이드바 사용

원격 데스크톱이나 게시된 애플리케이션에 연결한 후에는 사이드바를 사용하여 다른 원격 데스크톱 및 게시된 애플리케이션을 시작하고, 실행 중인 원격 데스크톱 및 게시된 애플리케이션 간을 전환하고, 기타 작업을 수행할 수 있습니다.

사이드바는 원격 데스크톱 또는 게시된 애플리케이션 창 왼쪽에 나타납니다. 사이드바를 표시하거나 숨기려면 사이드바 탭을 클릭합니다. 탭을 위 또는 아래로 밀 수도 있습니다.

실행 중인 게시된 애플리케이션에서 열린 문서 목록을 보려면 **실행 중** 목록에서 게시된 애플리케이션 옆에 있는 확장기 화살표를 클릭합니다.

참고 두 개의 다른 서버에 호스팅된 동일하지만 별도의 게시된 애플리케이션에서 두 문서가 열려 있는 경우 사이드바의 **실행 중** 목록에 해당 게시된 애플리케이션이 두 번 나타납니다.

사이드바에서 다양한 작업을 수행할 수 있습니다.

표 4-3. 사이드바 작업

조치	절차
사이드바 표시	게시된 애플리케이션 또는 원격 데스크톱이 열려 있으면 사이드바 탭을 클릭합니다. 사이드바가 열려 있어도 게시된 애플리케이션 또는 원격 데스크톱 창에서 여전히 작업을 수행할 수 있습니다.
사이드바 숨기기	사이드바 탭을 클릭합니다.
게시된 애플리케이션 또는 원격 데스크톱 시작	사이드바의 사용 가능 목록에서 게시된 애플리케이션 또는 원격 데스크톱의 이름을 클릭합니다. 원격 데스크톱이 먼저 나열됩니다.

표 4-3. 사이드바 작업 (계속)

조치	절차
게시된 애플리케이션 또는 원격 데스크톱 검색	<ul style="list-style-type: none"> ■ 검색 상자를 클릭하고 게시된 애플리케이션 또는 원격 데스크톱의 이름을 입력하기 시작합니다. ■ 게시된 애플리케이션 또는 원격 데스크톱을 시작하려면 검색 결과에서 해당 이름을 클릭합니다. ■ 사이드바의 홈 보기로 되돌아가려면 검색 상자의 X를 누릅니다.
즐거찾는 게시된 애플리케이션 및 원격 데스크톱 목록 생성	사이드바의 사용 가능 목록에서 원격 데스크톱 또는 게시된 애플리케이션 이름 옆에 있는 회색 별 모양을 클릭합니다. 그런 다음, 사용 가능 옆에 있는 즐거찾기 표시 도구 모음 버튼(별 모양 아이콘)을 클릭하여 즐겨찾기 목록만 표시할 수 있습니다.
게시된 애플리케이션 또는 원격 데스크톱 간 전환	사이드바의 실행 중 목록에서 게시된 애플리케이션 또는 원격 데스크톱 이름을 클릭합니다.
게시된 애플리케이션에 대해 다중 세션 모드 사용	사이드바에서 메뉴 열기 버튼을 클릭하고 설정 을 클릭한 후 아래로 스크롤하여 다중 실행 설정으로 이동합니다. 자세한 내용은 여러 클라이언트 디바이스에서 게시된 애플리케이션의 다중 세션 사용 의 내용을 참조하십시오.
복사 및 붙여넣기 패널 열기	사이드바 맨 위에서 복사 및 붙여넣기 버튼을 클릭합니다. 로컬 클라이언트 시스템의 애플리케이션 간에 텍스트를 복사하려면 이 버튼을 사용하십시오. 자세한 내용은 텍스트 복사 및 붙여넣기 의 내용을 참조하십시오. iOS Safari에서는 복사 및 붙여넣기 기능이 지원되지 않으므로 이 버튼을 사용할 수 없습니다.
파일 전송 창 열기	원격 데스크톱에서 파일을 다운로드하거나 원격 데스크톱으로 파일을 업로드하려면 사이드바 맨 위의 파일 전송 버튼을 클릭합니다. 자세한 내용은 클라이언트 시스템에 원격 데스크톱 또는 게시된 애플리케이션의 파일 다운로드 및 클라이언트 시스템에서 원격 데스크톱 또는 게시된 애플리케이션으로 파일 업로드 를 참조하십시오.
Command-A, Command-C, Command-V 및 Command-X 사용	이 옵션은 Mac을 사용하는 경우에만 설정 창에 표시됩니다. 사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭한 후 설정 을 클릭합니다. 이 기능이 활성화되면 Mac의 Command 키가 원격 Windows 데스크톱 또는 애플리케이션의 Ctrl 키에 매핑됩니다. 예를 들어 Mac 키보드에서 Command-A를 누르면 원격 Windows 데스크톱 또는 애플리케이션에서 Ctrl+A를 누르는 것과 같은 결과가 나타납니다.
실행 중인 원격 데스크톱 닫기	<p>사이드바에서 실행 중 목록의 원격 데스크톱 이름 옆에 있는 메뉴 열기 버튼을 클릭하고 작업을 선택합니다.</p> <ul style="list-style-type: none"> ■ 운영 체제에서 로그오프하지 않고 원격 데스크톱의 연결만 해제하려면 닫기를 선택합니다. Horizon 관리자는 연결을 끊을 때 자동으로 로그오프하도록 원격 데스크톱을 구성할 수 있습니다. 이 경우 열린 애플리케이션의 저장하지 않은 변경 내용은 손실됩니다. ■ 로그오프를 선택하여 운영 체제에서 로그오프하고 원격 데스크톱에서 연결을 해제합니다. 열린 애플리케이션의 저장하지 않은 변경 내용은 손실됩니다.
실행 중인 게시된 애플리케이션 닫기	<p>사이드바에서 실행 중 목록의 게시된 애플리케이션 이름 아래에 있는 파일 이름 옆의 X를 클릭합니다. 게시된 애플리케이션을 종료하고 해당 게시된 애플리케이션에 대해 열려 있는 모든 파일을 닫으려면 게시된 애플리케이션 이름 옆에 있는 X를 클릭합니다.</p> <p>파일에 대한 변경 내용을 저장할지 묻는 메시지가 표시됩니다.</p>
원격 데스크톱 재설정	사이드바에서 실행 중 목록의 원격 데스크톱 이름 옆에 있는 메뉴 열기 버튼을 클릭하고 재설정 을 선택합니다. 원격 데스크톱에서 열려 있는 모든 파일이 우선 저장되지 않고 닫힙니다. Horizon 관리자가 기능을 활성화한 경우에만 원격 데스크톱을 재설정할 수 있습니다.

표 4-3. 사이드바 작업 (계속)

조치	절차
원격 데스크톱 다시 시작	사이드바에서 실행 중 목록의 원격 데스크톱 이름 옆에 있는 메뉴 열기 버튼을 클릭하고 다시 시작 을 선택합니다. 다시 시작되기 전에 저장하지 않은 데이터를 저장하라는 메시지가 일반적으로 원격 데스크톱 운영 체제에 표시됩니다. Horizon 관리자가 기능을 활성화한 경우에만 원격 데스크톱을 다시 시작할 수 있습니다.
실행 중인 모든 게시된 애플리케이션 재설정	사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭하고 설정을 클릭한 후 실행 중인 모든 애플리케이션 재설정 을 클릭합니다. 저장하지 않은 모든 변경 내용은 손실됩니다.
Windows 키를 포함하는 키 조합 사용	사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭하고 설정을 클릭한 후 데스크톱용 Windows 키 사용 을 켭니다. 자세한 내용은 바로 가기 키 조합 의 내용을 참조하십시오.
현재 작업 영역으로 Ctrl+Alt+Del 보내기	사이드바 맨 위에 있는 Ctrl+Alt+Del 보내기 도구 모음 버튼을 클릭합니다.
서버에서 연결 끊기	사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭한 후 로그아웃 을 클릭합니다.
고해상도 디스플레이(예: Retina Macbook Pro)가 있는 시스템에서 고해상도 모드 사용	사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭하고 설정을 클릭한 후 고해상도 모드를 켭니다.
H.264 디코딩 허용	(Chrome만 해당) 사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭하고 설정을 클릭한 후 H.264 디코딩 허용 을 켭니다. 자세한 내용은 H.264 디코딩 허용 의 내용을 참조하십시오.
다중 모니터 사용	(Chrome 버전 55 이상만 해당) 사이드바 상단의 메뉴 열기 도구 모음 버튼을 클릭하고 디스플레이 설정 을 선택합니다. 자세한 내용은 다중 모니터 사용 을 참조하십시오.
소프트 키보드 호출 또는 닫기	(iOS Safari만 해당) 사이드바 맨 위의 키보드 아이콘을 클릭합니다. 손가락 3개로 화면을 눌러 소프트 키보드를 호출하거나 해제할 수도 있습니다.
도움말 항목 표시	사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭한 후 설정을 클릭하고 도움말 을 클릭합니다. 사이드바 맨 위의 Horizon 로고를 클릭하고 도움말 을 클릭할 수도 있습니다.
[VMware Horizon Client 정보] 대화상자가 표시됩니다.	사이드바 맨 위의 메뉴 열기 도구 모음 버튼 또는 Horizon 로고를 클릭하고 정보 를 클릭합니다. 사이드바 맨 위의 Horizon 로고를 클릭할 수도 있습니다.
원격 데스크톱 또는 게시된 애플리케이션을 전체 화면 모드로 표시	사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭한 후 전체 화면 을 클릭합니다.
전체 화면 모드 종료	사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭한 후 전체 화면 종료 를 클릭합니다.
전체 화면 모드일 때 원격 데스크톱 또는 게시된 애플리케이션으로 Esc 전송	사이드바 맨 위의 메뉴 열기 도구 모음 버튼을 클릭한 후 ESC 전송 을 클릭합니다.

모니터 및 화면 해상도

원격 데스크톱 또는 게시된 애플리케이션을 다중 모니터로 확장할 수 있습니다. 고해상도 모니터가 있다면 원격 데스크톱 또는 게시된 애플리케이션을 전체 해상도로 볼 수 있습니다.

다중 모니터 사용

Chrome 브라우저(버전 55 이상)를 사용하여 HTML Access의 다중 모니터에 원격 데스크톱 창을 표시할 수 있습니다.

최대 한 대의 추가 모니터를 기본 모니터에 추가하여 현재 연결되어 있는 원격 데스크톱 창을 표시할 수 있습니다. 예를 들어 모니터가 3대 있다면 원격 데스크톱 창이 3대 중 2대의 모니터에만 표시되도록 지정할 수 있습니다. 다중 모니터 설정에서 인접한 모니터를 선택해야 합니다. 모니터를 나란히 또는 수직으로 배치할 수 있습니다.

절차

- 1 HTML Access를 시작하고 서버에 로그인합니다.
- 2 데스크톱 및 애플리케이션 선택 창에서 액세스하려는 원격 데스크톱의 아이콘을 클릭합니다.
- 3 사이드바를 표시하려면 사이드바 탭을 클릭합니다.
- 4 사이드바 맨 위의 **메뉴 열기** 도구 모음 버튼을 클릭한 후 **다중 모니터**를 선택합니다.
- 5 다중 모니터 창에서 **디스플레이 추가**를 클릭합니다.

참고 [디스플레이 선택기] 브라우저 창이 나타나지 않으면 서버의 FQDN 주소를 브라우저 **콘텐츠 설정** 창의 팝업 예외 섹션에 추가합니다.

- 6 사용하려는 다른 모니터 디스플레이에 나타나도록 **디스플레이 선택기** 브라우저 창을 끌어 놓습니다.

디스플레이 선택기 브라우저 창의 메시지가 변경되며 회색 직사각형 아이콘이 추가됩니다.

- 7 **디스플레이 선택기** 브라우저 창에서 + 모니터 아이콘을 클릭하여 현재 모니터 디스플레이를 사용할 것임을 확인합니다.

다른 디스플레이를 기다리는 중 메시지가 현재 모니터 디스플레이에 표시되며 기본 디스플레이의 **다중 모니터** 창에 있는 회색 모니터 아이콘이 녹색으로 변경됩니다.

- 8 세션에서 사용하려는 모니터 디스플레이를 추가했으면 **다중 모니터** 창에서 **확인**을 클릭합니다.

다중 모니터 창이 해제되며 기본이 아닌 모니터 디스플레이에서 다른 디스플레이를 기다리는 중 메시지가 지워지고 원격 데스크톱 창이 표시됩니다.

- 9 다중 디스플레이 모드를 종료하려면 Esc를 누르고 **다중 디스플레이 모드 종료** 대화 상자에서 **예**를 클릭하여 확인합니다.

참고 원격 데스크톱에서 Esc 키를 사용해야 할 때마다 사이드바 탭을 열고 사이드바 맨 위의 **메뉴 열기** 도구 모음 버튼을 클릭한 후 **ESC 전송**을 선택해야 합니다.

원격 데스크톱 및 게시된 애플리케이션의 화면 해상도 설정

Horizon 관리자가 올바른 크기의 비디오 RAM으로 원격 데스크톱을 구성하는 경우 HTML Access는 브라우저 창 크기에 맞게 원격 데스크톱 크기를 조정할 수 있습니다. 3D 애플리케이션을 사용하지 않는 경우 기본 구성은 최소 요구 사항 16MB보다 많은 36MB의 VRAM(비디오 RAM)입니다.

Retina 디스플레이를 장착한 MacBook이나 Google Chromebook Pixel과 같이 고해상도 브라우저나 Chrome 디바이스를 사용하는 경우 해당 해상도를 사용하도록 원격 데스크톱 또는 게시된 애플리케이션을 설정할 수 있습니다. 사이드바에서 사용할 수 있는 **설정** 창에서 **고해상도 모드** 옵션을 켭니다. 이 옵션은 고해상도 디스플레이 또는 100%보다 큰 비율을 사용하는 일반 디스플레이를 사용하는 경우에만 **설정** 창에 나타납니다.

고해상도 모드 기능으로 활성 원격 세션에 대한 해상도는 변경할 수 없습니다. 이 기능을 적용하려면 로그아웃했다가 다시 로그인해야 합니다.

3D 렌더링 기능을 사용하려면 각 원격 데스크톱에 충분한 VRAM을 할당해야 합니다.

- vSphere 5.0 이상에서 제공되는 소프트웨어 가속 그래픽 기능을 통해 Windows Aero 테마 또는 Google Earth와 같은 3D 애플리케이션을 사용할 수 있습니다. 이 기능을 사용하려면 64MB ~ 128MB의 VRAM이 필요합니다.
- vSphere 5.1 이상과 함께 사용할 수 있는 공유 하드웨어 가속 그래픽 기능(vSGA)을 통해 설계, 모델링 및 멀티미디어용 3D 애플리케이션을 사용할 수 있습니다. 이 기능을 사용하려면 64MB ~ 512MB의 VRAM이 필요합니다. 기본값은 96MB입니다.
- vSphere 5.5 이상에서 제공되는 전용 하드웨어 가속 그래픽 기능(vDGA)은 ESXi 호스트의 단일 물리적 GPU(그래픽 처리 장치)를 단일 가상 시스템 전용으로 지정합니다. 고급 하드웨어 가속 워크스테이션 그래픽이 필요할 경우 이 기능을 사용합니다. 이 기능을 사용하려면 64MB ~ 512MB의 VRAM이 필요합니다. 기본값은 96MB입니다.

3D 렌더링을 사용하도록 설정하면 최대 모니터 수는 1대가 되며 최대 해상도는 3840 x 2160이 됩니다.

마찬가지로 Retina 디스플레이를 장착한 MacBook이나 Google Chromebook Pixel과 같은 고해상도 디바이스에서 브라우저를 사용하는 경우 각 원격 데스크톱에 충분한 VRAM을 할당해야 합니다.

중요 VMware Blast 디스플레이 프로토콜에 필요한 VRAM의 양을 추정하는 방법은 PCoIP 디스플레이 프로토콜에 필요한 VRAM 양을 추정하는 방법과 비슷합니다. 지침에 대해서는 “Horizon 7 아키텍처 계획” 문서에서 “가상 데스크톱에 대한 메모리 요구 사항 추정”을 참조하십시오.

DPI 동기화 사용

DPI 동기화 기능은 원격 데스크톱 또는 게시된 애플리케이션의 DPI 설정이 클라이언트 시스템의 DPI 설정과 일치하는지 확인합니다.

DPI 동기화를 사용하지 않도록 설정하면 디스플레이 크기 조정이 사용됩니다. 디스플레이 크기 조정 기능을 통해 원격 데스크톱 또는 게시된 애플리케이션 크기를 적절히 조정할 수 있습니다.

해상도를 수동으로 설정하려는 경우 **고해상도 모드** 설정을 사용하도록 설정할 수 있습니다. 자세한 정보는 **원격 데스크톱 및 게시된 애플리케이션의 화면 해상도 설정**의 내용을 참조하십시오.

DPI 동기화 에이전트 그룹 정책 설정은 DPI 동기화 기능의 사용 여부를 결정합니다. 이 기능은 기본적으로 사용하도록 설정됩니다. DPI 동기화를 사용할 경우 원격 데스크톱 또는 게시된 애플리케이션에 연결하면 원격 세션의 DPI 값이 클라이언트 시스템의 DPI 값과 일치하도록 변경됩니다. DPI 동기화 기능에는 Horizon Agent 7.0.2 이상이 필요합니다.

DPI 동기화 그룹 정책 설정 외에 **연결당 DPI 동기화** 에이전트 그룹 정책 설정이 사용하도록 설정된 경우 원격 데스크톱에 다시 연결하면 DPI 동기화가 지원됩니다. 이 기능은 기본적으로 사용하지 않도록 설정됩니다. 연결당 DPI 동기화 기능에는 Horizon Agent 7.8 이상이 필요합니다.

DPI 동기화 및 **연결당 DPI 동기화** 그룹 정책 설정에 대한 자세한 내용은 "Horizon 7에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

가상 데스크톱의 경우 DPI 동기화 기능이 다음 게스트 운영 체제에서 지원됩니다.

- 32비트 또는 64비트 Windows 7
- 32비트 또는 64비트 Windows 8.x
- 32비트 또는 64비트 Windows 10
- Windows Server 2008 R2(데스크톱으로 구성)
- Windows Server 2012 R2(데스크톱으로 구성)
- Windows Server 2016(데스크톱으로 구성)
- Windows Server 2019(데스크톱으로 구성)

게시된 데스크톱 및 게시된 애플리케이션의 경우 DPI 동기화 기능이 다음 RDS 호스트에서 지원됩니다.

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

가상 데스크톱의 경우 연결당 DPI 동기화 기능이 다음 게스트 운영 체제에서 지원됩니다.

- Windows 10 버전 1607 이상
- Windows Server 2016 이상(데스크톱으로 구성)

연결당 DPI 동기화 기능은 게시된 데스크톱 또는 게시된 애플리케이션에서 지원되지 않습니다.

다음은 DPI 동기화 기능의 사용에 대한 팁입니다.

- 클라이언트 시스템에서는 DPI 설정을 변경했으나 원격 데스크톱에서 DPI 설정이 변경되지 않으면 로그아웃했다가 다시 로그인하여 Horizon Client에서 클라이언트 시스템의 새 DPI 설정이 인식되도록 해야 할 수 있습니다.
- DPI 설정이 100% 이상인 클라이언트 시스템에서 원격 세션을 시작한 다음 DPI 설정이 100% 이상의 다른 값으로 설정된 다른 클라이언트 시스템에서 같은 세션을 사용하는 경우, 두 번째 클라이언트 시스템에서 DPI 동기화가 작동하도록 하려면 두 번째 클라이언트 시스템에서 원격 세션을 로그아웃했다가 다시 로그인해야 할 수 있습니다.
- Windows 10 및 Windows 8.x 시스템이 다양한 모니터에서 다양한 DPI 설정을 지원하더라도 DPI 동기화 기능은 HTML Access 클라이언트 세션 실행에 사용되는 웹 브라우저가 있는 클라이언트 시스템의 모니터에 설정된 DPI 값을 사용합니다. HTML Access는 여러 모니터에서의 여러 다른 DPI 설정을 지원하지 않습니다.

- 다른 DPI 설정이 있는 또 다른 모니터와 동기화하려는 경우 원격 데스크톱 또는 게시된 애플리케이션에서 로그아웃하고, HTML Access 클라이언트 세션 실행에 사용되는 웹 브라우저를 다른 모니터로 끌어 놓은 다음, 원격 데스크톱 또는 게시된 애플리케이션에 다시 로그인하여 클라이언트 시스템과 원격 데스크톱 또는 게시된 애플리케이션 간의 DPI 설정이 일치하도록 해야 합니다.

전체 화면 모드 사용

원격 데스크톱 또는 게시된 애플리케이션을 전체 화면 모드로 표시할 수 있습니다.

다음과 같은 경우 전체 화면 모드를 사용할 수 없습니다.

- 다중 모니터를 사용하고 있습니다.
- 브라우저가 전체 화면 모드이거나 마우스를 끌어서 최대화한 상태입니다.
- Safari를 사용하고 있습니다.

사전 요구 사항

원격 데스크톱 또는 게시된 애플리케이션에 연결합니다.

절차

- ◆ 원격 데스크톱 또는 게시된 애플리케이션을 전체 화면 모드로 표시하려면 사이드바 맨 위의 **메뉴 열기** 버튼을 클릭하고 **전체 화면**을 클릭합니다.
- ◆ 전체 화면 모드를 종료하려면 사이드바 맨 위의 **메뉴 열기** 버튼을 클릭하고 **전체 화면 종료**를 클릭합니다.

또는 클라이언트 시스템의 키보드에서 Esc 키를 누르십시오.

웹캠 및 마이크에 대한 실시간 오디오-비디오 기능 사용

실시간 오디오-비디오 기능을 통해 원격 데스크톱 또는 게시된 애플리케이션에서 클라이언트 시스템의 웹캠 또는 마이크를 사용할 수 있습니다. 실시간 오디오-비디오는 표준 회의 애플리케이션 및 브라우저 기반 비디오 애플리케이션과 호환되며 표준 웹캠, 오디오 USB 디바이스 및 아날로그 오디오 입력을 지원합니다.

실시간 오디오-비디오는 Chrome, Microsoft Edge 및 Firefox에서만 지원됩니다. 기본 비디오 해상도는 320 x 240픽셀입니다. 기본 실시간 오디오-비디오 설정은 대부분의 웹캠 및 오디오 애플리케이션에서 잘 작동합니다.

실시간 오디오-비디오 설정 변경에 대한 내용은 "Horizon 7에서 원격 데스크톱 기능 구성" 문서의 "실시간 오디오-비디오 그룹 정책 설정 구성"을 참조하십시오.

원격 데스크톱 또는 게시된 애플리케이션이 클라이언트 시스템의 웹캠 또는 마이크에 연결된 경우 원격 데스크톱 또는 게시된 애플리케이션에서 웹캠 또는 마이크를 사용하기 전에 브라우저에서 권한을 요청할 수 있습니다. 브라우저마다 다르게 동작합니다.

- Microsoft Edge는 매번 권한을 요청하며 이 동작은 변경할 수 없습니다. 자세한 내용은 <https://blogs.windows.com/msedgedev/2015/05/13/announcing-media-capture-functionality-in-microsoft-edge>의 내용을 참조하십시오.
- Firefox는 매번 권한을 요청하지만 이 동작을 변경할 수 있습니다. 자세한 내용은 <https://support.mozilla.org/en-US/kb/permissions-manager-give-ability-store-passwords-set-cookies-more?redirectlocale=en-US&redirectslug=how-do-i-manage-website-permissions>의 내용을 참조하십시오.
- Chrome은 처음에 권한을 요청합니다. 디바이스 사용을 허용하는 경우 Chrome은 권한을 다시 요청하지 않습니다.

원격 데스크톱이 클라이언트 시스템의 웹캠 또는 마이크에 연결되면 각 디바이스의 아이콘이 사이드바 위쪽에 표시됩니다. 사이드바의 디바이스 아이콘 위에 권한 요청을 나타내는 빨간색 물음표가 표시됩니다. 디바이스 사용을 허용하는 경우 빨간색 물음표가 사라집니다. 권한 요청을 거부하면 디바이스 아이콘이 사라집니다.

실시간 오디오-비디오가 원격 데스크톱 또는 게시된 애플리케이션 세션에서 사용 중일 때 두 번째 원격 데스크톱 또는 게시된 애플리케이션에 대한 연결을 열 경우 및 보안 경고가 나타난 경우(예: 올바른 인증서가 설치되지 않은 경우)에 경고를 무시하고 두 번째 원격 데스크톱 또는 게시된 애플리케이션에 계속 연결하면 실시간 오디오-비디오가 첫 번째 세션에서 작동을 중단합니다.

원격 데스크톱 세션 공유

세션 공동 작업 기능을 사용하여 기존의 원격 데스크톱 세션에 가입하도록 다른 사용자를 초대할 수 있습니다. 이와 같은 방식으로 공유되는 원격 데스크톱 세션을 공동 작업 세션이라고 합니다. 세션을 다른 사용자와 공유하는 사용자를 세션 소유자라고 하며, 공유 세션에 가입하는 사용자를 세션 공동 작업자라고 합니다.

Horizon 관리자는 세션 공동 작업 기능을 사용하도록 설정해야 합니다.

Windows 데스크톱의 경우 이를 위해 데스크톱 풀 또는 팜 수준에서 세션 공동 작업 기능을 사용하도록 설정해야 합니다. 또한 그룹 정책을 사용하여 사용 가능한 초대 방법과 같은 세션 공동 작업 기능을 구성해야 할 수도 있습니다. 전체 요구 사항을 보려면 [세션 공동 작업 기능에 대한 요구 사항](#)을 참조하십시오.

Windows 데스크톱에 대한 세션 공동 작업 기능을 사용하도록 설정하는 방법에 대한 내용은 "Horizon 7에서 가상 데스크톱 설정" 문서를 참조하십시오. 팜에 대한 세션 공동 작업 기능을 사용하도록 설정하는 방법에 대한 내용은 "Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정" 문서를 참조하십시오. 그룹 정책 설정을 사용하여 세션 공동 작업 기능을 구성하는 방법에 대한 내용은 "Horizon 7에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

Linux 데스크톱의 세션 공동 작업 기능을 사용하도록 설정하는 방법에 대한 내용은 "Horizon 7 for Linux 데스크톱 설정" 문서를 참조하십시오.

사용자를 원격 데스크톱 세션에 가입하도록 초대

세션 공동 작업 기능을 사용하면 이메일, 인스턴트 메시지(Windows 원격 데스크톱만 해당)로 공동 작업 초대를 보내거나 클립보드에 링크를 복사하고 사용자에게 전달하여 원격 데스크톱 세션에 참여하도록 사용자를 초대할 수 있습니다.

서버가 인증할 수 있는 도메인에 속하는 사용자만 초대할 수 있습니다. 기본적으로 최대 5명의 사용자를 초대할 수 있습니다. Horizon 관리자는 초대할 수 있는 사용자의 최대 수를 변경할 수 있습니다.


세션 공동 작업 기능에는 다음과 같은 제한이 있습니다.

- 다중 모니터를 사용하는 경우 세션 공동 작업자에게 기본 모니터만 표시됩니다.
- 공유할 원격 데스크톱 세션을 생성하는 경우에는 VMware Blast 디스플레이 프로토콜을 선택해야 합니다. 세션 공동 작업 기능은 PCoIP 또는 RDP 세션을 지원하지 않습니다.
- H.264 하드웨어 인코딩은 지원되지 않습니다. 세션 소유자가 하드웨어 인코딩을 사용하고 공동 작업자가 세션에 가입하는 경우 둘 다 소프트웨어 인코딩으로 폴백됩니다.
- 익명 공동 작업은 지원되지 않습니다. 세션 공동 작업자는 Horizon에서 지원하는 인증 메커니즘을 통해 식별할 수 있어야 합니다.
- 세션 공동 작업자는 Windows, Mac 또는 Linux용 Horizon Client 4.7 이상을 설치하거나 HTML Access 4.7 이상을 사용해야 합니다.
- 세션 공동 작업자에게 지원되지 않는 버전의 Horizon Client가 있는 경우 사용자가 공동 작업 링크를 클릭하면 오류 메시지가 표시됩니다.
- 게시된 애플리케이션 세션을 공유할 때는 세션 공동 작업 기능을 사용할 수 없습니다.

사전 요구 사항

- 세션 공동 작업 기능을 사용하도록 설정하고 구성해야 합니다.
- 이메일 초대 방법을 사용하려면 이메일 애플리케이션을 설치해야 합니다.
- Windows 원격 데스크톱에 대해 IM 초대 방법을 사용하려면 비즈니스용 Skype를 설치하고 구성해야 합니다.

절차

- 1 세션 공동 작업 기능이 사용되도록 설정된 원격 데스크톱에 연결합니다.
VMware Blast 디스플레이 프로토콜을 사용해야 합니다.
- 2 원격 데스크톱의 시스템 트레이에서 **VMware Horizon 공동 작업** 아이콘(예: )을 클릭합니다.
공동 작업 아이콘은 운영 체제 버전에 따라 다르게 보일 수 있습니다.

- 3 VMware Horizon 공동 작업 대화 상자가 열리면 원격 데스크톱 세션에 가입하게 하려는 사용자의 사용자 이름(예: **testuser** 또는 **domain\testuser**) 또는 이메일 주소를 입력합니다.

특정 사용자의 사용자 이름 또는 이메일 주소를 처음 입력할 때는 **"사용자" 찾기**를 클릭하고 쉼표 (,)를 입력하거나 **Enter** 키를 눌러 사용자가 유효한지 확인해야 합니다. Windows 원격 데스크톱의 경우 세션 공동 작업 기능은 다음번에 사용자의 사용자 이름 또는 이메일 주소를 입력할 때 저장된 데이터를 제공합니다.

- 4 초대 방법을 선택합니다.

모든 초대 방법을 사용할 수 있는 것은 아닙니다.

옵션	조치
e-메일	클립보드에 공동 작업 초대를 복사하고 기본 이메일 애플리케이션에서 새 이메일 메시지를 엽니다. 이 초대 방법을 사용하려면 이메일 애플리케이션이 설치되어 있어야 합니다.
IM	(Windows 원격 데스크톱만 해당) 클립보드에 공동 작업 초대를 복사하고 비즈니스용 Skype에서 새 창을 엽니다. Ctrl+V를 눌러 비즈니스용 Skype 창에 링크를 붙여 넣습니다. 이 초대 방법을 사용하려면 비즈니스용 Skype를 설치하고 구성해야 합니다.
링크 복사	클립보드에 공동 작업 초대를 복사합니다. 메모장 등의 다른 애플리케이션을 수동으로 열고 Ctrl+V를 눌러 초대를 붙여 넣어야 합니다.

초대를 보낸 후 VMware Horizon 공동 작업 아이콘이 바탕 화면에도 나타나고 세션 공동 작업 사용자 인터페이스는 공동 작업 세션의 현재 상태를 표시하고 특정 작업을 수행할 수 있는 대시보드로 전환됩니다.

세션 공동 작업자가 초대를 수락하여 Windows 원격 데스크톱 세션에 가입하면 세션 공동 작업 기능은 알림을 표시하며 시스템 트레이의 VMware Horizon 공동 작업 아이콘에 빨간색 점이 표시됩니다. 세션 공동 작업자가 초대를 수락하여 Linux 원격 데스크톱 세션에 가입하면 기본 세션 데스크톱에 알림이 표시됩니다.

다음에 수행할 작업

VMware Horizon 공동 작업 대화 상자에서 원격 데스크톱 세션을 관리합니다. [공유 원격 데스크톱 세션 관리](#)의 내용을 참조하십시오.

공유 원격 데스크톱 세션 관리

세션 공동 작업 초대를 보낸 후 세션 공동 작업 사용자 인터페이스는 공유 원격 데스크톱 세션(공동 작업 세션)의 현재 상태를 표시하고 특정 작업을 수행할 수 있는 대시보드로 전환됩니다.

Horizon 관리자는 세션 공동 작업자에게 제어권이 전달되지 않도록 할 수 있습니다. Windows 원격 데스크톱의 경우 "Horizon 7에서 원격 데스크톱 기능 구성" 문서에서 **공동 작업자에 대한 제어 전달 허용** 그룹 정책 설정을 참조하십시오. Linux 원격 데스크톱의 경우 "Horizon 7 for Linux 데스크톱 설정" 문서에서 `collaboration.enableControlPassing` 매개 변수를 참조하십시오.

사전 요구 사항

공동 작업 세션을 시작합니다. [사용자를 원격 데스크톱 세션에 가입하도록 초대](#)의 내용을 참조하십시오.

절차

- 1 원격 데스크톱에서 시스템 트레이의 **VMware Horizon 공동 작업** 아이콘을 클릭합니다.
[이름] 옆에 모든 세션 공동 작업자의 이름이 표시되고 해당 상태가 [상태] 옆에 표시됩니다.
- 2 VMware Horizon 세션 공동 작업 대시보드를 사용하여 공동 작업 세션을 관리합니다.

옵션	조치
초대 취소 또는 공동 작업자 제거	[상태] 옆에서 제거 를 클릭합니다.
공동 작업자에게 제어권 제공	세션 공동 작업자가 세션에 참가한 후 [제어] 옆의 스위치를 켜기 로 전환합니다. 세션에 대한 제어를 재개하려면 두 번 클릭하거나 아무 키나 누르십시오. 세션 공동 작업자도 [제어] 옆의 스위치를 끄기 로 전환하거나 제어권 반환 버튼을 클릭하여 제어권을 다시 반환할 수 있습니다.
공동 작업자 추가	공동 작업자 추가 를 클릭합니다.
공동 작업 세션 종료	공동 작업 종료 를 클릭합니다. 모든 활성 공동 작업자의 연결이 끊어집니다. Windows 원격 데스크톱에서 VMware Horizon 세션 공동 작업 아이콘 옆에 있는 중지 버튼을 클릭하여 공동 작업 세션을 끝낼 수도 있습니다. Linux 원격 데스크톱에서는 중지 버튼을 사용할 수 없습니다.

원격 데스크톱 세션에 가입

세션 공동 작업 기능을 통해 공동 작업 초대의 링크를 클릭하여 원격 데스크톱 세션에 가입할 수 있습니다. 링크는 이메일 또는 인스턴트 메시지가 세션 소유자가 사용자에게 전달한 문서에 있을 수도 있습니다. 또는 서버에 로그인하고 원격 데스크톱 및 애플리케이션 선택기 창에서 세션에 대한 아이콘을 두 번 클릭합니다.

이 절차에서는 공동 작업 초대에서 원격 데스크톱 세션에 가입하는 방법을 설명합니다.

참고 Cloud Pod 아키텍처 환경에서 세션 소유자의 포트에 로그인하지 않으면 서버에 로그인해도 공동 작업 세션에 가입할 수 없습니다.

세션 공동 작업 기능을 사용하여 원격 데스크톱 세션에 가입하면 원격 데스크톱 세션에서 다음 기능을 사용할 수 없습니다.

- 실시간 오디오-비디오(RTAV)
- 위치 기반 인쇄
- 클립보드 리디렉션

원격 데스크톱 세션에서 원격 데스크톱 해상도 또한 변경할 수 없습니다.

사전 요구 사항

세션 공동 작업 기능을 사용하여 원격 데스크톱 세션에 가입하려면 클라이언트 시스템에 Windows, Mac 또는 Linux용 Horizon Client 4.7을 설치하거나 HTML Access 4.7 이상을 사용해야 합니다.

절차

- 1 공동 작업 초대 링크를 클릭합니다.

Horizon Client가 클라이언트 시스템에서 열립니다.

- 2 자격 증명을 입력하여 Horizon Client에 로그인합니다.

성공적으로 인증되면 공동 작업 세션이 시작되고 세션 소유자의 원격 데스크톱을 볼 수 있습니다. 세션 소유자가 마우스 및 키보드 제어권을 사용자에게 이전할 경우 원격 데스크톱을 사용할 수 있습니다.

- 3 마우스 및 키보드 제어권을 세션 소유자에게 반환하려면 시스템 트레이에서 **VMware Horizon 공동 작업** 아이콘을 클릭하고 [제어] 열의 스위치를 **끄기**로 전환하거나 **제어 권한 반환** 버튼을 클릭합니다.

- 4 공동 작업 세션을 종료하려면 사이드바에서 **닫기**를 클릭합니다.

텍스트 복사 및 붙여넣기


클라이언트 디바이스에서 원격 데스크톱 또는 게시된 애플리케이션으로 또는 클라이언트 디바이스로 일반 텍스트 및 HTML 형식의 서식 있는 텍스트를 복사하여 붙여넣을 수 있습니다. Horizon 관리자는 복사 및 붙여넣기 작업이 클라이언트 시스템에서 원격 데스크톱이나 게시된 애플리케이션으로만 허용, 원격 데스크톱이나 게시된 애플리케이션에서 클라이언트 시스템으로만 허용, 둘 다 허용 또는 둘 다 허용되지 않도록 이 기능을 구성할 수 있습니다.

Horizon 관리자는 원격 데스크톱의 View Agent 또는 Horizon Agent와 관련된 그룹 정책 설정을 사용하여 복사 및 붙여넣기 기능을 구성할 수 있습니다. 자세한 내용은 [HTML Access 그룹 정책 설정](#)의 내용을 참조하십시오.

서식 있는 텍스트를 복사하여 붙여넣을 때는 다음과 같은 제한 사항이 적용됩니다.

- 이미지 복사 및 붙여넣기는 지원되지 않습니다.
- 클라이언트 디바이스에서 서식 있는 텍스트를 복사하며 대상이 워드패드 애플리케이션인 경우 일반 텍스트만 복사되어 붙여 넣어집니다.
- 서식 있는 텍스트 복사 및 붙여넣기는 IE(Internet Explorer), Microsoft Edge 또는 Safari 브라우저에서 HTML Access를 사용하는 경우 지원되지 않습니다. **복사 및 붙여넣기 창**을 사용해야 합니다. **복사 및 붙여넣기 창 사용**의 내용을 참조하십시오.
- Horizon 관리자는 그룹 정책 설정을 사용하여 복사 및 붙여넣기 작업 중에 클립보드 형식을 제한할 수 있습니다. HTML Access는 클립보드에 있는 텍스트만 전송하는 기능을 지원하므로 텍스트 필터만 HTML Access에서 작동합니다. 클립보드 형식 필터 정책 설정에 대한 자세한 내용은 "Horizon 7에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.

HTML Access를 Chrome 또는 Firefox 브라우저에서 사용하는 경우 클립보드 기능 사용에 관한 다음 팁을 참조하십시오.

- 원격 데스크톱 또는 게시된 애플리케이션에 처음 연결하면 클립보드 사용자 가이드 대화상자가 나타납니다. **확인**을 클릭하여 대화상자를 닫고 다시 표시되지 않도록 합니다.
- 기본적으로 사이드바의 클립보드 아이콘  이 선택되고 회색으로 나타납니다.
 - 클립보드 아이콘이 선택된 경우 원격 데스크톱 또는 게시된 애플리케이션에서 텍스트를 복사하면 로컬 클라이언트 시스템의 클립보드에 텍스트를 복사할지 확인하라는 대화상자가 나타납니다. **확인**을 클릭합니다.
 - 클립보드 아이콘을 선택 취소하는 경우 원격 데스크톱 또는 게시된 애플리케이션의 텍스트를 로컬 클라이언트 시스템의 클립보드에 복사할 때 확인 대화상자가 나타나지 않습니다.
- 사이드바에서 클립보드 아이콘 위로 마우스를 가져가면 툴팁에 클립보드 기능이 수행하는 작업이 표시됩니다.

클립보드는 모든 유형의 복사 및 붙여넣기 작업에 최대 1MB의 데이터를 수용할 수 있습니다. 일반 텍스트 및 서식 있는 텍스트 데이터의 합계가 최대 클립보드 크기 미만을 사용하는 경우 서식이 지정된 텍스트를 붙여넣습니다. 종종 텍스트 및 서식에서 최대 클립보드 크기 이상을 사용하는 경우 서식 있는 텍스트를 폐기하고 일반 텍스트를 붙여넣기 위해 서식 있는 텍스트를 잘라낼 수 없습니다. 서식이 지정된 모든 텍스트를 한 번의 작업으로 모두 선택하여 붙여넣을 수 없는 경우 각 작업에서 더 적은 양을 복사 및 붙여넣어야 합니다.

그래픽은 복사하여 붙여 넣을 수 없습니다. 또한, 클라이언트 컴퓨터의 파일 시스템과 원격 데스크톱 간에는 파일을 복사하고 붙여넣을 수 없습니다.

참고 복사 및 붙여넣기 기능은 iOS Safari 및 Android 디바이스에서 지원되지 않습니다.

복사 및 붙여넣기 창 사용

IE(Internet Explorer), Microsoft Edge 또는 Safari 브라우저에서 텍스트를 복사하여 붙여넣으려면 사이드바 맨 위에 있는 **복사 및 붙여넣기** 버튼을 사용하여 **복사 및 붙여넣기** 창을 표시해야 합니다.

이 절차에서는 **복사 및 붙여넣기** 창을 사용하여 로컬 클라이언트 시스템의 IE, Edge 또는 Safari 브라우저에서 원격 데스크톱의 애플리케이션 또는 게시된 애플리케이션으로 텍스트를 복사하는 방법과 원격 데스크톱의 애플리케이션 또는 게시된 애플리케이션에서 클라이언트 시스템으로 텍스트를 복사하는 방법에 대해 설명합니다.

게시된 애플리케이션 간에 또는 원격 데스크톱 간에 텍스트를 복사 및 붙여넣는 경우에는 일반적인 상황과 마찬가지로 간단히 복사 및 붙여넣을 수 있으며 **복사 및 붙여넣기** 창을 사용할 필요가 없습니다.

IE, Edge 또는 Safari 브라우저를 사용하는 경우에는 로컬 시스템의 클립보드를 원격 시스템의 클립보드와 동기화할 때만 **복사 및 붙여넣기** 창이 필요합니다.

복사 및 붙여넣기 창에는 사용자가 내용을 복사 및 붙여넣을 수 있는 방향을 나타내는 다음 메시지 중 하나가 표시됩니다.

- 이 패널을 사용하여 로컬 클라이언트와 원격 데스크톱/애플리케이션 간에 내용을 복사하여 붙여 넣습니다.

- 이 패널을 사용하여 로컬 클라이언트에서 내용을 복사하여 원격 데스크톱/애플리케이션으로 붙여넣습니다.
- 이 패널을 사용하여 원격 데스크톱/애플리케이션에서 내용을 복사하여 로컬 클라이언트로 붙여넣습니다.

참고 기본 클립보드 리디렉션 그룹 정책 설정을 사용하면 클라이언트 시스템에서만 복사한 후 원격 데스크톱 또는 게시된 애플리케이션에 붙여넣을 수 있습니다. 원격 데스크톱 또는 게시된 애플리케이션에서 클라이언트 시스템으로 복사할 수 있으려면, 양방향으로 그룹 정책 설정을 사용하도록 설정해야 합니다.

사전 요구 사항

Mac을 사용하는 경우, 키 조합을 통해 텍스트를 선택하고 복사하고 붙여넣을 때 Command 키를 Windows Ctrl 키에 매핑하기 위한 설정을 활성화했는지 확인합니다. 사이드바에서 **설정 창 열기** 도구 모음 버튼을 클릭하고 **Command-A, Command-C, Command-V 및 Command-X 사용**을 켭니다. Mac을 사용하는 경우 **설정** 창에만 이 옵션이 나타납니다.

Horizon 관리자는 기본 정책을 적용한 상태로 두어 사용자가 클라이언트 시스템에서 복사하여 원격 데스크톱 및 게시된 애플리케이션에 붙여넣을 수 있도록 하거나 복사 및 붙여넣기를 허용하는 다른 정책을 구성해야 합니다. 자세한 내용은 [HTML Access 그룹 정책 설정](#)의 내용을 참조하십시오.

절차

- ◆ 클라이언트 시스템에서 원격 데스크톱의 애플리케이션으로 또는 클라이언트 시스템에서 게시된 애플리케이션으로 텍스트를 복사하려면 다음 단계를 수행합니다.
 - a 로컬 클라이언트 애플리케이션에서 텍스트를 복사합니다.
 - b HTML Access에서 사이드바를 열고 사이드바 맨 위의 **복사 및 붙여넣기**를 클릭합니다.

복사 및 붙여넣기 창이 나타납니다. 이전에 복사한 텍스트가 창에 이미 나타나는 경우 새로 복사한 텍스트에 붙여넣으면 해당 텍스트가 바뀝니다.
 - c **복사 및 붙여넣기** 창에 텍스트를 붙여넣으려면 Windows 시스템에서는 Ctrl+V를, Mac에서는 Command-V를 누릅니다.

"원격 클립보드 동기화됨" 메시지가 잠깐 표시됩니다.
 - d 텍스트를 붙여넣을 애플리케이션을 클릭하고 Ctrl+V를 누릅니다.

텍스트를 애플리케이션에 붙여 넣었습니다.
- ◆ 원격 데스크톱의 애플리케이션에서 클라이언트 시스템으로 또는 게시된 애플리케이션에서 클라이언트 시스템으로 텍스트를 복사하려면 다음 단계를 수행합니다.
 - a 애플리케이션에서 텍스트를 복사합니다.
 - b HTML Access에서 사이드바를 열고 사이드바 맨 위의 **복사 및 붙여넣기**를 클릭합니다.

복사 및 붙여넣기 창이 나타나고 붙여넣은 텍스트가 표시됩니다. "원격 클립보드 동기화됨" 메시지가 잠깐 표시됩니다.

- c 텍스트를 다시 복사하려면 **복사 및 붙여넣기** 창을 클릭하고 Windows 시스템에서는 Ctrl+C를, Mac에서는 Command-C를 누릅니다.

이 작업을 수행할 때는 텍스트가 선택되지 않으므로 텍스트를 선택할 수 없습니다. "클립보드 패널에서 복사함" 메시지가 잠깐 표시됩니다.

- d 클라이언트 시스템에서 텍스트를 붙여넣을 위치를 클릭하고 Ctrl+V를 누릅니다.

텍스트가 클라이언트 시스템의 애플리케이션으로 붙여넣어집니다.

클라이언트와 원격 데스크톱 또는 게시된 애플리케이션 간에 파일 전송

파일 전송 기능을 사용하여 클라이언트 시스템과 원격 데스크톱 또는 게시된 애플리케이션 간에 파일을 전송할 수 있습니다.

Horizon 관리자는 VMware Blast의 **파일 전송 구성** 그룹 정책 설정을 수정하여 파일 전송을 허용하거나, 허용하지 않거나, 한 방향으로만 허용하도록 구성할 수 있습니다. 이 그룹 정책 설정에는 다음과 같은 값이 있습니다.

- **업로드 및 다운로드 모두 사용 안 함** 값을 선택하는 경우 **파일 전송** 버튼이 사용되지 않도록 설정됩니다.
- **파일 업로드만 사용** 값을 선택하는 경우(기본 설정), **파일 전송** 창에 **업로드** 탭만 표시됩니다.
- **파일 다운로드만 사용** 값을 선택하는 경우 **파일 전송** 창에 **다운로드** 탭만 표시됩니다.

서버에서 클라이언트로의 **클립보드 리디렉션 구성** 그룹 정책 설정을 사용하지 않도록 설정하면 파일 다운로드도 사용되지 않도록 설정됩니다.

이러한 그룹 정책 설정에 대한 자세한 내용은 "Horizon 7에서 원격 데스크톱 기능 구성" 문서를 참조하십시오.


이 기능의 제한 사항은 다음과 같습니다.

- 최대 500MB 파일을 다운로드하고 최대 2GB 파일을 업로드할 수 있습니다.
- 32비트 Internet Explorer 11에서는 300MB보다 큰 파일을 다운로드할 수 없습니다. 이 문제를 해결하려면 Internet Explorer 11을 64비트 모드에서 실행합니다.
- 크기가 0인 폴더나 파일은 다운로드하거나 업로드할 수 없습니다.
- iOS의 Safari 및 Safari 8은 업로드 또는 다운로드를 지원하지 않습니다. Safari 9 이상에서는 다운로드를 지원하지 않습니다.
- 원격 세션에서 파일 전송이 진행 중이며 두 번째 원격 세션에 대한 연결을 여는 경우, 보안 경고가 나타나는 경우, 이러한 경고를 무시하고 두 번째 원격 세션에 계속 연결하는 경우 첫 번째 세션의 파일 전송이 중단됩니다.
- Internet Explorer 11 또는 Chromebook의 Chrome을 사용하여 파일을 업로드하는 경우, 크기가 0이거나 2GB보다 큰 폴더 및 파일을 끌어서 놓으면 예상대로 오류 메시지가 표시됩니다. 이 오류 메시지를 닫은 후에는 더 이상 파일을 끌어서 놓기하여 전송할 수 없습니다.
- Linux 원격 데스크톱 또는 Android 디바이스에서는 이 기능을 사용할 수 없습니다.

클라이언트 시스템에 원격 데스크톱 또는 게시된 애플리케이션의 파일 다운로드

원격 데스크톱 또는 게시된 애플리케이션에서 클라이언트 시스템으로 파일을 다운로드할 수 있습니다. Horizon 관리자는 이 기능을 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 [클라이언트와 원격 데스크톱 또는 게시된 애플리케이션 간에 파일 전송](#)의 내용을 참조하십시오.

절차

- 1 원격 데스크톱 또는 게시된 애플리케이션에 연결합니다.
- 2 사이드바를 표시하려면 사이드바 탭을 클릭합니다.
- 3 사이드바 맨 위에 있는 파일 전송 아이콘 을 클릭합니다.

파일 전송 창이 나타납니다.

- 4 **파일 전송** 창에서 **다운로드**를 클릭합니다.
- 5 다운로드할 파일을 하나 이상 선택합니다.
- 6 파일 전송을 시작하려면 Ctrl+C를 누릅니다.

파일이 **파일 전송** 창의 **다운로드** 탭에 표시됩니다.

- 7 다운로드 아이콘(아래쪽 화살표)을 클릭하여 클라이언트 시스템에 파일을 다운로드합니다.


파일이 클라이언트 시스템의 다운로드 폴더에 표시됩니다.

클라이언트 시스템에서 원격 데스크톱 또는 게시된 애플리케이션으로 파일 업로드

클라이언트 시스템에서 원격 데스크톱 또는 게시된 애플리케이션으로 파일을 업로드할 수 있습니다.

Horizon 관리자는 이 기능을 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 [클라이언트와 원격 데스크톱 또는 게시된 애플리케이션 간에 파일 전송](#)의 내용을 참조하십시오.

절차

- 1 원격 데스크톱 또는 게시된 애플리케이션에 연결합니다.
- 2 사이드바를 표시하려면 사이드바 탭을 클릭합니다.
- 3 사이드바 맨 위에 있는 파일 전송 아이콘 을 클릭합니다.

파일 전송 창이 나타납니다.

- 4 파일을 업로드하려면 **파일 전송** 창의 **업로드** 탭으로 파일을 끌어서 놓거나 **업로드** 탭에서 **파일 선택**을 클릭하고 업로드할 파일을 선택합니다.

업로드한 파일은 문서 폴더에 표시됩니다.

여러 클라이언트 디바이스에서 게시된 애플리케이션의 다중 세션 사용

게시된 애플리케이션에 대해 다중 세션 모드를 사용하도록 설정하면 여러 다른 클라이언트 디바이스에서 서버에 로그인할 때 동일한 게시된 애플리케이션의 여러 세션을 사용할 수 있습니다.

예를 들어, 클라이언트 A에서 게시된 애플리케이션을 다중 세션 모드로 연 다음, 클라이언트 B에서 동일한 게시된 애플리케이션을 열면, 게시된 애플리케이션이 클라이언트 A에서 열린 상태로 남아 있고 게시된 애플리케이션의 새 세션이 클라이언트 B에서 열립니다. 비교해보면 다중 세션 모드가 사용되지 않도록 설정된 경우(단일 세션 모드) 클라이언트 A에서 게시된 애플리케이션 세션의 연결이 끊어졌다가 클라이언트 B에서 다시 연결됩니다.

다중 세션 모드 기능에는 다음과 같은 제한 사항이 있습니다.

- 다중 세션 모드는 비즈니스용 Skype 등과 같이 다중 인스턴스를 지원하지 않는 애플리케이션에는 작동하지 않습니다.
- 다중 세션 모드에서 게시된 애플리케이션을 사용하는 동안 애플리케이션 세션 연결이 해제되면 자동으로 로그오프되고 저장되지 않은 모든 데이터는 손실됩니다.

사전 요구 사항

Horizon 관리자는 애플리케이션 풀에 대해 다중 세션 모드를 사용하도록 설정해야 합니다. Horizon 관리자가 허용하지 않으면 사용자는 게시된 애플리케이션에 대한 다중 세션 모드를 수정할 수 없습니다. "Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정"의 내용을 참조하십시오. 이 기능에는 Horizon 7 버전 7.7 이상이 필요합니다.

절차

- 1 서버에 연결합니다.
- 2 데스크톱 및 애플리케이션 선택기 창의 오른쪽 상단 모서리에 있는 **설정** 도구 모음 버튼을 클릭하고 아래로 스크롤하여 **다중 실행** 설정으로 이동한 후 **설정**을 클릭합니다.

또는 이전에 원격 데스크톱 또는 게시된 애플리케이션을 시작한 경우 사이드바에서 **메뉴 열기** 버튼을 클릭하고 **설정을** 클릭한 후 아래로 스크롤하여 **다중 실행** 설정으로 이동할 수 있습니다. 다중 세션 모드에서 사용할 수 있는 게시된 애플리케이션이 없는 경우 **다중 실행** 설정이 흐리게 표시됩니다.
- 3 다중 세션 모드에서 사용하려는 게시된 애플리케이션을 선택하고 **확인**을 클릭합니다.

Horizon 관리자가 게시된 애플리케이션에 대해 다중 세션 모드를 적용하면 이 설정을 변경할 수 없습니다.

사운드

원격 데스크톱 및 게시된 애플리케이션에서 사운드를 재생할 수 있지만 일부 제한이 적용됩니다.

기본적으로 원격 데스크톱 및 게시된 애플리케이션에 대해 사운드 재생이 활성화되어 있지만 Horizon 관리자가 사운드 재생을 비활성화하도록 정책을 설정할 수 있습니다.

원격 데스크톱 및 게시된 애플리케이션의 사운드 재생에 다음과 같은 제한 사항이 적용됩니다.

- 볼륨을 높이려면 원격 데스크톱의 사운드 컨트롤이 아닌 클라이언트 시스템의 사운드 컨트롤을 사용하십시오.
- 경우에 따라 사운드가 비디오와 동기화되지 않을 수 있습니다.
- 네트워크 트래픽이 많은 경우 또는 브라우저가 많은 작업을 수행하는 경우 사운드 품질이 떨어질 수 있습니다. 일부 브라우저의 경우 이와 관련하여 보다 우수한 사운드 성능을 제공합니다.

바로 가기 키 조합

일부 키 조합은 사용하는 언어와 관계없이 원격 데스크톱 또는 게시된 애플리케이션으로 전송할 수 없습니다.

웹 브라우저를 통해 클라이언트 시스템 및 대상 시스템 모두에 키 누름과 키 조합을 보낼 수 있습니다. 기타 키 및 키 조합의 경우 입력은 로컬로만 처리되며 대상 시스템에 전송되지 않습니다. 시스템에서 작동되는 키 조합은 브라우저 소프트웨어, 클라이언트 운영 체제 및 언어 설정에 따라 달라집니다.

참고 Mac을 사용하는 경우 키 조합을 통해 텍스트를 선택하고 복사하고 붙여넣을 때 명령 키를 Windows Ctrl 키에 매핑할 수 있습니다. 이 기능을 활성화하려면 사이드바에서 **설정 창 열기** 도구 모음 버튼을 클릭하고 **Command-A, Command-C, Command-V 및 Command-X 사용**을 켭니다. 이 옵션은 Mac 클라이언트 시스템을 사용하는 경우에만 **설정** 창에 표시됩니다.

다음 키 및 키 조합은 원격 데스크톱에서는 종종 작동하지 않습니다.

- Ctrl+T
- Ctrl+W
- Ctrl+N
- 명령 키
- Alt+Enter
- Ctrl+Alt+ *any_key*

중요 Ctrl+Alt+Del을 입력하려면 사이드바 맨 위의 **Ctrl+Alt+Delete 보내기** 도구 모음 버튼을 사용하십시오.

- Caps Lock+ *modifier_key*(예: Alt 또는 Shift)
- Chromebook의 기능 키
- Windows 키 조합

원격 데스크톱용 Windows 키를 사용하도록 설정하면 원격 데스크톱에서 다음 Windows 키 조합이 작동하지 않습니다. 이 키를 사용하도록 설정하려면 사이드바에서 **설정 창 열기** 도구 모음 버튼을 클릭하고 **데스크톱용 Windows 키 사용**을 켭니다.

중요 데스크톱용 Windows 키 사용을 켜 후에는 Ctrl+Win(Windows 시스템), Ctrl+Command(Macs) 또는 Ctrl+Search(Chromebook)를 눌러 Windows 키 누르기를 시뮬레이트해야 합니다.

이러한 키 조합은 게시된 애플리케이션에는 작동하지 않습니다. 이러한 키 조합은 Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 원격 데스크톱 및 게시된 데스크톱에서 작동합니다.

Windows 8.x 또는 Windows Server 2012 R2 운영 체제가 있는 원격 데스크톱에서 작동하는 일부 키 조합은 Windows 7, Windows Server 2008 R2 또는 Windows 10 운영 체제가 설치된 원격 데스크톱에서는 작동하지 않습니다.

표 4-4. Windows 10 원격 데스크톱 및 Windows Server 2016 원격 데스크톱용 Windows 키 바로 가기

키	조치	제한 사항
Win	시작을 열거나 닫습니다.	
Win+A	관리 센터를 엽니다.	
Win+E	파일 탐색기를 엽니다.	
Win+G	게임이 열려 있으면 게임 바를 엽니다.	
Win+H	공유 참을 엽니다.	
Win+I	설정 참을 엽니다.	
Win+K	연결 바로 가기를 엽니다.	
Win+M	모든 창을 최소화합니다.	
Win+R	실행 대화상자를 엽니다.	
Win+S	검색을 엽니다.	
Win+X	빠른 연결 메뉴를 엽니다.	
Win+, (쉼표)	원격 데스크톱에서 잠깐 미리 봅니다.	
Win+Pause	시스템 속성 대화상자를 표시합니다.	Chromebook 또는 Mac에는 Pause 키가 없습니다.
Win+Shift+M	원격 데스크톱에서 최소화된 창을 복원합니다.	Safari에서는 작동하지 않습니다.
Win+Alt+Num	원격 데스크톱을 열고 숫자가 지정하는 위치의 작업 표시줄에 고정된 애플리케이션에 대한 점프 목록을 엽니다.	Chromebook에서는 작동하지 않습니다.
Win+Enter	내레이터를 엽니다.	

표 4-5. Windows 8.x 및 Windows Server 2012 R2 원격 데스크톱용 Windows 키 바로 가기

키	조치	제한 사항
Win+F1	Windows 도움말 및 지원을 엽니다.	Safari에서는 작동하지 않습니다.
Win	시작 창을 표시하거나 숨깁니다.	

표 4-5. Windows 8.x 및 Windows Server 2012 R2 원격 데스크톱용 Windows 키 바로 가기 (계속)

키	조치	제한 사항
Win+B	알림 영역에 포커스를 설정합니다.	
Win+C	참 패널을 엽니다.	
Win+D	원격 데스크톱을 표시하고 숨깁니다.	Safari에서는 작동하지 않습니다. Mac에서 Command-D를 누릅니다.
Win+E	파일 탐색기를 엽니다.	
Win+H	공유 참을 엽니다.	
Win+I	설정 참을 엽니다.	
Win+K	디바이스 참을 엽니다.	
Win+M	모든 창을 최소화합니다.	
Win+Q	아무 위치에서나 또는 열린 애플리케이션 내에서 검색하려면 애플리케이션이 애플리케이션 검색을 지원하는 경우 [검색] 참을 엽니다.	
Win+R	실행 대화상자를 엽니다.	
Win+S	Windows 및 웹을 검색하려면 [검색] 참을 엽니다.	
Win+X	빠른 연결 메뉴를 엽니다.	
Win+Z	애플리케이션에서 사용할 수 있는 명령을 표시합니다.	
Win+, (선택표)	키를 계속 누르고 있으면 원격 데스크톱을 일시적으로 표시합니다.	Windows 2012 R2 운영 체제에서는 작동하지 않습니다.
Win+Pause	[시스템 속성] 대화상자를 표시합니다.	Chromebook 및 Mac에는 Pause 키가 없습니다.
Win+Shift+M	원격 데스크톱에서 최소화된 창을 복원합니다.	Safari에서는 작동하지 않습니다. Mac에서 Command-D를 누릅니다.
Win+Alt+Num	원격 데스크톱을 열고 숫자가 지정하는 위치의 작업 표시줄에 고정된 애플리케이션에 대한 점프 목록을 엽니다.	Chromebook에서는 작동하지 않습니다.
Win+위쪽 화살표	창을 최대화합니다.	Chromebook에서는 작동하지 않습니다.
Win+아래쪽 화살표	화면에서 현재 애플리케이션을 제거하거나 원격 데스크톱 창을 최소화합니다.	Chromebook에서는 작동하지 않습니다.
Win+왼쪽 화살표	애플리케이션이나 원격 데스크톱 창을 화면 왼쪽으로 최대화합니다.	Chromebook에서는 작동하지 않습니다.
Win+오른쪽 화살표	애플리케이션이나 원격 데스크톱 창을 화면 오른쪽으로 최대화합니다.	Chromebook에서는 작동하지 않습니다.
Win+Home	활성 원격 데스크톱 창을 제외한 모든 창을 최소화합니다(Win+Home을 한 번 더 누르면 모든 창이 복원됨).	Safari 브라우저에서는 작동하지 않습니다.
Win+Shift+위쪽 화살표	화면 맨 위쪽과 맨 아래쪽으로 원격 데스크톱 창을 펼칩니다.	Chromebook에서는 작동하지 않습니다.

표 4-5. Windows 8.x 및 Windows Server 2012 R2 원격 데스크톱용 Windows 키 바로 가기 (계속)

키	조치	제한 사항
Win + Shift + 아래쪽 화살표	Win + Shift + 위쪽 화살표를 눌러 창을 펼친 후 폭을 유지하면서 원격 데스크톱 창을 수직 방향으로 복원합니다. 또는 활성 원격 데스크톱 창을 최소화합니다.	Chromebook에서는 작동하지 않습니다.
Win + Enter	내레이터를 엽니다.	

표 4-6. Windows 7 및 Windows Server 2008 R2 원격 데스크톱용 Windows 키 바로 가기

키	조치	제한 사항
Win	시작 메뉴를 열거나 닫습니다.	
Win + Pause	[시스템 속성] 대화상자를 표시합니다.	Chromebook 및 Mac에는 Pause 키가 없습니다.
Win + D	원격 데스크톱을 표시하고 숨깁니다.	Safari에서는 작동하지 않습니다. Mac에서 Command-D를 누릅니다.
Win + M	모든 창을 최소화합니다.	
Win + E	컴퓨터 폴더를 엽니다.	
Win + R	실행 대화상자를 엽니다.	
Win + 위쪽 화살표	창을 최대화합니다.	Chromebook에서는 작동하지 않습니다.
Win + 아래쪽 화살표	창을 최소화합니다.	Chromebook에서는 작동하지 않습니다.
Win + 왼쪽 화살표	애플리케이션이나 원격 데스크톱 창을 창 왼쪽으로 최대화합니다.	Chromebook에서는 작동하지 않습니다.
Win + 오른쪽 화살표	애플리케이션이나 원격 데스크톱 창을 창 오른쪽으로 최대화합니다.	Chromebook에서는 작동하지 않습니다.
Win + Home	활성 원격 데스크톱 창을 제외한 모든 창을 최소화합니다.	Safari에서는 작동하지 않습니다.
Win + Shift + 위쪽 화살표	화면 맨 위쪽과 맨 아래쪽으로 원격 데스크톱 창을 펼칩니다.	Chromebook에서는 작동하지 않습니다.
Win + G	실행 중인 원격 데스크톱 가젯을 따라 순환합니다.	
Win + U	접근성 센터를 엽니다.	

국제화

사용자 인터페이스와 문서는 한국어, 영어, 일본어, 프랑스어, 독일어, 중국어 간체, 중국어 번체 및 스페인어로 제공됩니다.

클라이언트 시스템, 브라우저 및 원격 데스크톱에서 사용해야 할 언어 팩에 대한 자세한 내용은 [국제 키보드](#)를 참조하십시오.

국제 키보드

영어가 아닌 키보드 및 로컬 사용 시 클라이언트 시스템, 브라우저 및 원격 데스크톱에서 특정 설정을 사용해야 합니다. 일부 언어의 경우 원격 데스크톱에서 IME(입력기)를 사용해야 합니다.

올바른 로컬 설정 및 입력 방법이 설치되어 있는 경우, 한국어, 영어, 일본어, 프랑스어, 독일어, 중국어 간체, 중국어 번체 및 스페인어 문자를 입력할 수 있습니다.

표 4-7. 필수 입력 언어 설정

언어	로컬 클라이언트 시스템의 입력 언어	로컬 클라이언트 시스템에 IME가 필요합니까?	원격 데스크톱의 브라우저 및 입력 언어	원격 데스크톱에서 IME가 필요합니까?
영어	영어	아니요	영어	아니요
프랑스어	프랑스어	아니요	프랑스어	아니요
독일어	독일어	아니요	독일어	아니요
중국어(간체)	중국어(간체)	영어 입력 모드	중국어(간체)	예
중국어(번체)	중국어(번체)	영어 입력 모드	중국어(번체)	예
일본어	일본어	영어 입력 모드	일본어	예
한국어	한국어	영어 입력 모드	한국어	예
스페인어	스페인어	아니요	스페인어	아니요

Horizon Client 문제 해결

5

원격 데스크톱 또는 게시된 애플리케이션을 다시 시작 또는 재설정하거나, Horizon Client를 다시 설치하여 대부분의 Horizon Client 문제를 해결할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 원격 데스크톱 다시 시작
- 원격 데스크톱 또는 게시된 애플리케이션 재설정

원격 데스크톱 다시 시작

원격 데스크톱 운영 체제가 더 이상 응답하지 않을 경우 원격 데스크톱을 다시 시작해야 합니다. 원격 데스크톱을 다시 시작하는 것은 Windows 운영 체제 다시 시작 명령을 사용하는 것과 같습니다. 다시 시작되기 전에 저장하지 않은 데이터를 저장하라는 메시지가 일반적으로 원격 데스크톱 운영 체제에 표시됩니다.

Horizon Administrator가 원격 데스크톱 다시 시작 기능을 사용하도록 설정한 경우에만 원격 데스크톱을 다시 시작할 수 있습니다.

데스크톱 다시 시작 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 "Horizon 7에서 가상 데스크톱 설정" 또는 "Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정" 문서를 참조하십시오.

절차

- ◆ 다시 시작 명령을 사용하십시오.

옵션	조치
사이드바에서	원격 데스크톱에 연결되어 있는 경우 사이드바에서 실행 중 목록의 원격 데스크톱 이름 옆에 있는 메뉴 열기 도구 모음 버튼을 클릭하고 다시 시작 을 선택합니다.
URI 사용	데스크톱을 다시 시작하려면 URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=restart</code> 을 사용하십시오.

원격 데스크톱의 운영 체제가 다시 시작되고 Horizon Client 연결이 끊어진 후 원격 데스크톱에서 로그오프됩니다.

다음에 수행할 작업

원격 데스크톱에 재연결을 시도하기 전에 시스템 다시 시작을 위해 적당한 시간 동안 기다려 주십시오.

원격 데스크톱을 다시 시작해도 문제가 해결되지 않으면 원격 데스크톱을 재설정해야 할 수 있습니다.

[원격 데스크톱 또는 게시된 애플리케이션 재설정](#)의 내용을 참조하십시오.

원격 데스크톱 또는 게시된 애플리케이션 재설정

데스크톱 운영 체제가 응답하지 않고 원격 데스크톱을 다시 시작해도 문제가 해결되지 않으면 원격 데스크톱을 재설정해야 할 수 있습니다.

원격 데스크톱 재설정은 물리적 PC의 재설정 버튼을 눌러 PC를 강제로 다시 시작하는 것과 같습니다.

원격 데스크톱에서 열려 있는 모든 파일은 저장되지 않고 닫힙니다.

게시된 애플리케이션을 재설정하면 열려 있는 모든 애플리케이션이 종료됩니다.

Horizon administrator가 원격 데스크톱의 재설정 기능을 사용하도록 설정한 경우에만 원격 데스크톱을 재설정할 수 있습니다.

데스크톱 재설정 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 "Horizon 7에서 가상 데스크톱 설정" 또는 "Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정" 문서를 참조하십시오.

절차

- ◆ **재설정** 명령을 사용하십시오.

옵션	조치
애플리케이션 선택기 창에서 게시된 애플리케이션 재설정	데스크톱 및 애플리케이션 선택기 창에서 원격 데스크톱 또는 게시된 애플리케이션에 연결하기 전에 실행 중인 모든 게시된 애플리케이션을 재설정하려면 화면의 오른쪽 상단 모서리에 있는 설정 도구 모음 버튼을 클릭하고 재설정 을 클릭합니다.
사이드바에서 원격 데스크톱 재설정	원격 데스크톱에 연결되어 있는 경우 사이드바에서 실행 중 목록의 데스크톱 이름 옆에 있는 열기 메뉴 도구 모음 버튼을 클릭하고 재설정 을 선택합니다.
사이드바에서 게시된 애플리케이션 재설정	실행 중인 모든 애플리케이션을 재설정하려면 사이드바 맨 위쪽의 설정 창 열기 도구 모음 버튼을 클릭한 후 재설정 을 클릭합니다.
URI를 사용하여 원격 데스크톱 재설정	원격 데스크톱을 재설정하려면 URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=reset</code> 을 사용하십시오.

원격 데스크톱을 재설정하면 원격 데스크톱의 운영 체제가 다시 시작되고 Horizon Client 연결이 끊어진 후 원격 데스크톱에서 로그오프됩니다. 게시된 애플리케이션을 재설정하면 게시된 애플리케이션이 종료됩니다.

다음에 수행할 작업

원격 데스크톱 또는 게시된 애플리케이션에 재연결을 시도하기 전에 시스템이 다시 시작하도록 적당한 시간 동안 기다려 주십시오.