Chrome용 VMware Horizon Client 설치 및 설정 가이드

2019년 3월 14일

VMware Horizon Client for Chrome 5.0

vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.
https://docs.vmware.com/kr/
VMware 웹 사이트에서는 최신 제품 업데이트도 제공합니다.
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

Chrome용 VMware Horizon Client 설치 및 설정 가이드

이 Chrome용 VMware Horizon Client 설치 및 설정 가이드 문서에서는 Chromebook에서 Chrome용 VMware Horizon® Client™ 소프트웨어를 설치, 구성 및 사용하는 방법에 대한 정보를 제공합니다.

이 정보는 가상 시스템 기술과 데이터 센터 운영을 잘 아는 숙련된 시스템 관리자를 대상으로 작성되었습니다.

최종 사용자인 경우 VMware 설명서에서 Chrome용 VMware Horizon Client 사용자 가이드 문서를 참조하거나 Chrome용 Horizon Client 온라인 도움말을 참조하십시오.

1 설정 및 설치

Horizon Client 설정 중에 클라이언트 디바이스에서 Chrome용 Horizon Client 애플리케이션이 설치되고, 연결 서버가 구성되고, 필요한 포트가 열립니다.

본 장은 다음 항목을 포함합니다.

시스템 요구 사항

Chrome용 Horizon Client를 사용하는 디바이스는 특정 소프트웨어 요구 사항을 충족해야 합니다.

디바이스 모델	Chromebook
운영 체제	Chrome OS 44 이상
CPU 아키텍처	ARM 또는 x86
연결 서버, 보안 서버 및 View Agent 또는 Horizon Agent	Horizon 6 버전 6.2.6 또는 Horizon 7 버전 7.4 이상 릴리스. Horizon 7 버전 7.4 서버에 연결하려면 서버에서 Chrome용 Horizon Client 확장을 등록해야 합니다. 이러한 변경 작업이 Horizon 6 버전 6.2.6 또는 Horizon 7 버전 7.5 이상 서버에서는 필요하지 않습니다. 자세한 내용은 Chrome용 VMware Horizon Client 확장 등록의 내용을 참조하십시오.

	클라이언트 시스템이 회사 방화벽 외부에서 연결되는 경우 VMware는 클라이언트 시스템에 VPN 연결이 필요하지 않도록 보안 서버 또는 Unified Access Gateway 장치를 사용합니다. 자세한 내용은 연결 서버 및 보안 서버 준비의 내용을 참조하십시오.
스마트 카드 인증	스마트 카드 인증 요구 사항의 내용을 참조하십시오.
타사 방화벽	방화벽에서 특정 TCP 포트의 인바운드 트래픽을 허용해야 합니다. 클라이언트 웹 브라우저 액세스에 대한 방화벽 규칙의 내용을 참조하십시오.
디스플레이 프로토콜	VMware Blast(Horizon Agent 7.0 이상 필요)

스마트 카드 인증 요구 사항

사용자 인증에 스마트 카드를 사용하는 Chromebook은 특정 요구 사항을 충족해야 합니다.

클라이언트 하드웨어 및 소프트웨어 요구 사항

실제 스마트 카드를 사용하여 인증하는 사용자는 스마트 카드가 있어야 하며 각 스마트 카드에는 사용자 인증서가 포함되어 있어야 합니다. 지원되는 스마트 카드는 다음과 같습니다.

- 미국 국방부 CAC(Common Access Card)
- FIPS-201 스마트 카드라고도 하는 미국 연방 정부 PIV(Personal Identity Verification) 카드

사용자 인증에 스마트 카드를 사용하는 각 Chromebook에는 다음 하드웨어 및 소프트웨어가 있어야 합니다.

- Chrome용 Horizon Client
- 호환 스마트 카드 판독기
- Google Smart Card Connector 애플리케이션

  이 커넥터 애플리케이션은 Chrome OS에서 스마트 카드에 대한 기본적인 지원을 제공합니다. Chrome 웹 스토어에서 Smart Card Connector 애플리케이션을 다운로드할 수 있습니다. Google Smart Card Connector 애플리케이션 버전 1.2.16.1 이상을 사용하는 것이 좋습니다.

- Charismathics CSSI Smart Card Middleware 애플리케이션

  미들웨어는 스마트 카드 및 다른 클라이언트 인증서와 통신합니다. Chrome 웹 스토어에서 CSSI Smart Card Middleware 애플리케이션을 다운로드할 수 있습니다.

Chromebook에서 루트 및 중간 인증서를 설치해야 할 수 있습니다. 자세한 내용은 Google Chrome OS 설명서를 참조하십시오.

에이전트 소프트웨어 요구 사항

Horizon Administrator는 에이전트 시스템에서 CSSI Smart Card Middleware 애플리케이션을 설치해야 합니다.

지원되는 에이전트 운영 체제에 대해서는 기능 지원 표를 참조하십시오.

추가 스마트 카드 인증 요구 사항

Chrome용 Horizon Client의 스마트 카드 요구 사항을 충족하는 것 외에도 다른 Horizon 구성 요소가 스마트 카드를 지원하기 위한 특정 구성 요구 사항을 충족해야 합니다.

연결 서버 및 보안 서버 호스트	Horizon 7 버전 7.4 이상. 스마트 카드 사용을 지원하도록 연결 서버를 구성하는 방법에 대한 자세한 내용은 Horizon 7 관리 문서를 참조하십시오.
Unified Access Gateway 장치	Unified Access Gateway 3.2 이상. 스마트 카드 사용을 지원하도록 Unified Access Gateway 장치를 구성하는 방법에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성 문서를 참조하십시오.
Active Directory	스마트 카드 인증을 구현하기 위해 관리자가 Active Directory에서 수행해야 하는 작업에 대한 자세한 내용은 Horizon 7 관리 문서를 참조하십시오.

스마트 카드 인증 제한 사항

스마트 카드 인증을 사용하여 스마트 카드 판독기를 Chromebook에 꽂고, 스마트 카드를 삽입하고, Horizon Client에서 서버를 선택합니다. 인증 단계 동안 사용자 이름 및 암호 대신 PIN을 입력합니다. 원격 데스크톱 또는 게시된 애플리케이션을 선택한 후 모든 스마트 카드 명령 및 응답이 원격 데스크톱 또는 게시된 애플리케이션으로 리디렉션됩니다.

스마트 카드 인증을 Chrome용 Horizon Client에서 사용할 때는 특정 제한 사항이 적용됩니다.

- 연결 서버 및 Unified Access Gateway 스마트 카드 사용자 이름 힌트 기능이 지원되지 않습니다.
- 연결 서버 스마트 카드 제거 정책이 지원되지 않습니다.
- Single Sign-on이 지원되지 않습니다. 원격 데스크톱 또는 게시된 애플리케이션에 연결할 때 원격 세션 내에서 스마트 카드 PIN을 다시 입력해야 합니다.
- 스마트 카드를 사용하여 서버에 인증 후에 Active Directory 인증과 같은 기타 인증 방식으로 전환할 수 없습니다. 다음 번에 서버에 연결할 때 다른 인증 방법을 사용하려면 Chrome OS에서 로그아웃하거나 Chromebook을 재부팅해야 합니다.
- 인증서를 선택하고 PIN을 입력한 후, 선택한 인증서는 Chromebook에서 캐시되고 다음 번에 서버에 연결할 때 사용됩니다. 다음 번에 서버에 연결할 때 다른 인증서를 선택하려면 Chromebook을 재부팅해야 합니다.

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 Chrome용 Horizon Client를 사용하기 위해 수행해야 하는 작업의 검사 목록입니다.

1 연결 서버를 설치합니다. 설치 지침을 보려면 Horizon 7 설치 문서를 참조하십시오.

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. 자세한 내용은 Horizon 7 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 Horizon 7 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 Horizon 7 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 규칙의 내용을 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	**도메인** 드롭다운 메뉴는 숨겨져 있습니다. 사용자는 **사용자 이름** 텍스트 상자에 다음 값 중 하나를 입력해야 합니다. ■ 사용자 이름(다중 도메인의 경우 허용되지 않음) ■ **도메인₩사용자 이름** ■ *username@domain.com*
사용 안 함(기본값)	사용 안 함	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. ■ 사용자 이름(다중 도메인의 경우 허용되지 않음) ■ **도메인₩사용자 이름** ■ *username@domain.com*
사용	사용	**도메인** 드롭다운 메뉴는 숨겨져 있습니다. 사용자는 **사용자 이름** 텍스트 상자에 다음 값 중 하나를 입력해야 합니다. ■ 사용자 이름(다중 도메인의 경우 허용되지 않음) ■ **도메인₩사용자 이름** ■ *username@domain.com*
사용	사용 안 함	**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. ■ **도메인₩사용자 이름** ■ *username@domain.com*

서버가 설치된 후 Horizon Administrator에서 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.

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.

Chrome용 Horizon Client 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 임의	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 임의	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 임의	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 임의	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.

Chrome용 Horizon Client 설치 또는 업그레이드

Chrome용 Horizon Client는 Chrome 애플리케이션이며 다른 Chrome 애플리케이션을 설치할 때와 동일한 방식으로 설치합니다.

사전 요구 사항

클라이언트 디바이스가 Chrome용 Horizon Client에 대한 시스템 요구 사항을 충족하는지 확인합니다. 시스템 요구 사항의 내용을 참조하십시오.

절차

1 Chromebook에 로그인합니다.

2 Chrome 웹 스토어에서 Chrome용 VMware Horizon Client를 다운로드하고 설치합니다.

Chrome용 VMware Horizon Client 확장 등록

사용자가 Chrome용 Horizon Client를 사용하여 Horizon 7 버전 7.4 서버에 연결하도록 하려면 Chrome용 VMware Horizon Client 확장을 등록해야 합니다. 이러한 절차는 Horizon 6 버전 6.2.6 또는 Horizon 7 버전 7.5 이상 서버에 연결할 때는 필요하지 않습니다.

사전 요구 사항

클라이언트 디바이스에 Chrome용 VMware Horizon Client를 설치합니다. Chrome용 Horizon Client 설치 또는 업그레이드의 내용을 참조하십시오.

절차

1 연결 서버 호스트에서 *install_directory*₩VMware₩VMware View₩Server₩sslgateway₩conf₩settings.properties 파일로 이동합니다.

2 텍스트 편집기에서 settings.properties 파일을 열고 다음 줄을 추가합니다.

```
chromeExtension.1=ppkfnjlimknmjoaemnpidmdlfchhehel
```

3 settings.properties 파일을 저장합니다.

4 변경 내용을 적용하려면 VMware Horizon View Security Gateway Component 서비스를 다시 시작합니다.

다음에 수행할 작업

Chrome용 Horizon Client를 사용하여 원격 데스크톱 또는 게시된 애플리케이션에 연결할 할 수 있는지 확인합니다. 원격 데스크톱 또는 게시된 애플리케이션에 연결의 내용을 참조하십시오.

Chromebook 디바이스에 대한 서버 목록 및 기본 서버 구성

등록된 Chromebook 디바이스에서 Horizon Client에 대한 연결 서버 인스턴스 목록 및 기본 연결 서버 인스턴스를 구성할 수 있습니다.

서버 목록을 구성한 경우 서버가 Horizon Client에서 바로 가기로 표시됩니다. 기본 서버를 구성한 경우 Horizon Client가 해당 서버에 자동으로 연결됩니다.

서버 목록 또는 기본 서버를 구성하려면 JSON 구성 파일을 생성해야 합니다. Chrome 관리자는 Google 관리 콘솔을 사용하여 Horizon Client 애플리케이션에 대한 JSON 구성 파일을 업로드해야 합니다. Google 관리 콘솔 사용에 대한 자세한 내용은 G Suite 관리자 도움말을 참조하십시오.

예를 들어 다음 JSON 구성 파일은 서버 목록을 지정합니다. 서버 속성은 서버의 IP 주소 또는 호스트 이름을 지정하고 사용자 이름 및 도메인 속성을 사용하여 서버를 사용할 권한이 부여된 사용자의 이름과 도메인을 지정하며 설명 속성을 사용하여 서버의 설명을 지정합니다. 사용자 이름, 도메인 및 설명 속성은 선택 사항입니다.

```
{
  "broker_list": {
    "Value": {
      "settings": {
        "server-list": [{
          "server": "viewserver0.mydomain.com",
          "default": false,
          "description": "View Server 0",
          "username": "User0",
          "desktopId": "RDS2012R2DC",
          "domain": "TestDomain0"
        },{
          "server": "viewserver1.mydomain.com",
```

```
          "description": "View Server 1",
          "username": "User1",
          "domain": "TestDomain1",
          "default": false
        }, {
          "server": "123.456.1.2",
          "description": "View Server 2",
          "username": "User2",
          "default": false,
          "domain": "TestDomain2"
        }, {
          "server": "123.456.1.3",
          "description": "View Server 3",
          "username": "User3",
          "default": false,
          "domain": "TestDomain3"
        }, {
          "server": "viewserver4.mydomain.com",
          "description": "View Server 4",
          "username": "User4",
          "default": false,
          "domain": "TestDomain4"
        }]}
    }
  }
}
```

다음 예에서는 기본 속성을 사용하여 기본 서버를 지정하는 방법을 보여 줍니다. 올바른 값은 true와 false입니다.

```
{
  "broker_list": {
    "Value": {
      "settings": {
        "server-list": [{
          "server": "viewserver0.mydomain.com",
          "default": true,
          "description": "View Server 0",
          "username": "User0",
          "desktopId": "RDS2012R2DC",
          "domain": "TestDomain0"
        }]}
    }
  }
}
```

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 Chrome용 Horizon Client를 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 저장소로 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.

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 가져오기의 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 추가의 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 가져오기의 내용을 참조하십시오.

인증서 지문과 함께 해당 레지스트리 키를 구성합니다. Windows 레지스트리에 인증서 지문 설정의 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 건너뜁니다.
- 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 설정의 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 가져오기의 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 Blast₩Config 레지스트리 키로 이동합니다.

7 SslHash 값을 수정하고 텍스트 상자에 인증서 지문을 붙여넣습니다.

8 Windows를 재부팅합니다.

사용자가 Chrome용 Horizon Client를 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.html의 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.

Unified Access Gateway 에서 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 Chrome용 Horizon Client에 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. Chrome에서 인증서를 설치하는 방법에 대한 내용은 Google Chrome 설명서를 참조하십시오.

Horizon Client 데이터 공유 구성

Horizon 관리자가 고객 환경 향상 프로그램에 참여하기로 선택하면 VMware는 하드웨어 및 소프트웨어 호환성을 최우선적으로 고려하기 위해 클라이언트 시스템에 대한 익명 데이터를 수집하고 수신합니다. Horizon Client에서 설정을 사용하거나 사용하지 않도록 설정하여 클라이언트 시스템에 대한 정보를 공유할지 여부를 구성할 수 있습니다.

Horizon Client 데이터 공유는 기본적으로 사용하도록 설정됩니다. 서버에 연결하기 전에 데이터 공유 설정을 구성해야 합니다. 이 설정은 모든 서버에 적용됩니다. 서버에 연결한 후에는 Horizon Client 데이터 공유 설정을 변경할 수 없습니다.

절차

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

VMware에서 수집하는 데이터

귀사에서 고객 환경 향상 프로그램에 참여하며 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 관리자가 고객 경험 향상 프로그램에 참여하기로 결정하면 VMware는 고객 요구 사항에 대한 VMware의 대응 개선을 위해 배포에 대한 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.

VMware 고객 경험 향상 프로그램에 참여하려면, 관리자가 연결 서버를 설치할 때 연결 서버 설치 마법사 실행 중에 참여 여부를 선택하거나, 설치 후 Horizon Administrator의 옵션을 설정하면 됩니다.

표 1-2. 고객 경험 향상 프로그램을 위해 수집한 클라이언트 데이터

설명	필드 이름	이 필드는 익명으로 처리됩니까?	예시 값
애플리케이션을 제작한 회사	<client_vendor>	아니요	VMware
제품 이름	<client_product>	아니요	Chrome용 VMware Horizon Client
클라이언트 제품 버전	<client_version>	아니요	4.10.0-build_number
클라이언트 바이너리 아키텍처	<client_arch>	아니요	브라우저
브라우저의 기본 아키텍처	<browser_arch>	아니요	ChromeOS
브라우저 사용자 에이전트 문자열	<browser_user_agent>	아니요	Chrome/3.0.1750
브라우저의 내부 버전 문자열	<browser_version>	아니요	3.0.1750(Chrome용)
브라우저의 코어 구현	<browser_core>	아니요	Chrome
브라우저가 핸드헬드 디바이스에서 실행되는지 여부	<browser_is_handheld>	아니요	true

원격 데스크톱 및 게시된 애플리케이션 연결 관리

2

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

원격 데스크톱 또는 게시된 애플리케이션에 연결하려면 서버 이름과 사용자 계정의 자격 증명을 제공해야 합니다.

최종 사용자가 원격 데스크톱 및 게시된 애플리케이션에 액세스할 수 있도록 하기 전에 먼저 클라이언트 디바이스에서 원격 데스크톱 또는 게시된 애플리케이션에 연결할 수 있는지 테스트합니다.

사전 요구 사항

- 사용자 이름/암호, RSA SecurID 사용자 이름/암호, RADIUS 인증 사용자 이름/암호 또는 스마트 카드 PIN(개인 ID 번호)과 같은 로그인 자격 증명을 얻습니다.
- 로그인을 위한 NETBIOS 도메인 이름을 얻습니다. 예를 들어 mycompany.com보다는 mycompany를 사용할 수 있습니다.
- 스마트 카드 인증을 사용하는 경우 모든 스마트 카드 인증 요구 사항이 충족되는지 확인하고 제한 사항을 숙지하십시오. 자세한 내용은 스마트 카드 인증 요구 사항 및 스마트 카드 인증 제한 사항 항목을 참조하십시오.
- 회사 네트워크 외부에 있으며 원격 데스크톱 및 게시된 애플리케이션에 액세스하기 위해 VPN 연결이 필요한 경우 클라이언트 디바이스가 VPN 연결을 사용하도록 설정되어 있는지 확인하고 해당 연결을 켜십시오.

- 원격 데스크톱 또는 게시된 애플리케이션에 액세스하는 서버의 정규화된 도메인 이름(FQDN)이 있는지 확인합니다. 서버 이름에는 밑줄(_)을 사용할 수 없습니다. 포트가 443이 아닌 경우 포트 번호도 필요합니다.

절차

1 Chromebook에 로그인합니다.

2 VPN 연결이 필요한 경우 VPN을 켭니다.

3 VMware Horizon Client 애플리케이션을 엽니다.

4 Smart Card Connector에 대한 액세스 권한을 부여할지 묻는 메시지가 표시되면 **허용**을 클릭합니다.

이 메시지는 Chromebook에서 스마트 카드 인증이 구성된 경우 Horizon Client를 처음 시작할 때 표시됩니다.

5 서버에 연결합니다.

옵션	조치
새 서버에 연결	더하기 기호(+)를 클릭하고, 서버의 이름을 입력하고, 서버에 대한 설명을 입력하고(선택 사항), **연결**을 클릭합니다.
기존 서버에 연결	서버 바로 가기를 클릭합니다.

Horizon Client와 서버 간 연결에는 항상 TLS가 사용됩니다. TLS 연결의 기본 포트는 443입니다. 서버가 기본 포트를 사용하도록 구성되지 않은 경우에는 다음 예의 형식을 사용합니다. `view.company.com:1443`.

6 스마트 카드가 필수 또는 선택 사항일 경우, 사용할 스마트 카드 인증서를 선택하고 PIN을 입력합니다.

7 RSA SecurID 자격 증명 또는 RADIUS 인증 자격 증명을 묻는 메시지가 표시되면 사용자 이름과 인증번호를 입력하고 **로그인**을 클릭합니다.

암호에 PIN 및 토큰에서 생성된 번호가 모두 포함될 수 있습니다.

8 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 암호를 잘못 입력했거나 RSA 서버의 구성 설정이 변경된 경우에만 필요합니다.

9 사용자 이름과 암호를 묻는 메시지가 나타나면 Active Directory 자격 증명을 입력합니다.

a 하나 이상의 데스크톱 또는 애플리케이션 풀에 대한 사용 권한이 있는 사용자의 사용자 이름 및 암호를 입력합니다.

b 도메인을 선택합니다.

도메인을 선택할 수 없는 경우 `domain₩username` 또는 `username@domain` 형식으로 사용자 이름을 입력해야 합니다.

c **로그인**을 누릅니다.

10 (선택 사항) 원격 데스크톱 또는 게시된 애플리케이션을 즐겨찾기로 표시하려면 원격 데스크톱 또는 게시된 애플리케이션 아이콘 안에 있는 회색 별 모양을 클릭합니다.

별 모양 아이콘이 회색에서 노란색으로 바뀝니다. 다음번에 로그인할 때 브라우저 창의 오른쪽 상단에서 별 모양 아이콘을 클릭하여 즐겨찾기 항목만 표시할 수도 있습니다.

11 원격 데스크톱 또는 게시된 애플리케이션에 연결하려면 데스크톱 및 애플리케이션 선택기 창에서 해당 아이콘을 클릭합니다.

12 스마트 카드 인증을 사용하는 경우 원격 세션 내부에서 스마트 카드 PIN을 다시 입력합니다.

원격 데스크톱 또는 게시된 애플리케이션에 연결한 후 브라우저 창 왼쪽에 있는 탭을 클릭하여 탐색 사이드바를 표시할 수 있습니다. 이 사이드바를 사용하여 다른 원격 데스크톱 또는 게시된 애플리케이션에 액세스한 후 **설정** 창을 열고 다른 작업을 수행할 수 있습니다. 자세한 내용은 사이드바 사용의 내용을 참조하십시오.

다음에 수행할 작업

원격 데스크톱 또는 게시된 애플리케이션에 연결한 후에 연결이 바로 끊어지고 링크를 클릭하여 보안 인증서를 승인할 것인지를 묻는 메시지가 표시되는 경우 사용자는 인증서의 신뢰 여부를 선택할 수 있습니다. 자체 서명된 루트 인증서 신뢰의 내용을 참조하십시오.

원격 데스크톱 또는 게시된 애플리케이션의 표준 시간대가 클라이언트 디바이스에 설정된 시간대를 사용하지 않는 경우 표준 시간대를 수동으로 설정합니다. 시간대 설정의 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.

Chrome에는 자체 서명된 인증서를 영구적으로 신뢰하기 위한 옵션을 제공합니다. 인증서를 영구적으로 신뢰하지 않으면 브라우저를 다시 시작할 때마다 인증서를 확인해야 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.

a 주소 표시줄에서 잠금 아이콘을 클릭합니다.

b **인증서 정보** 링크를 클릭합니다.

c 인증서가 회사에서 사용하는 인증서와 일치하는지 확인합니다.

시스템 관리자에게 지원을 요청해야 할 수도 있습니다.

2 보안 인증서를 수락합니다.

Chrome에서는 브라우저 페이지에서 **고급** 링크를 클릭한 후 **server-name에서 계속(비안전)**을 클릭합니다.

원격 데스크톱 또는 게시된 애플리케이션이 시작됩니다.

시간대 설정

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

Horizon Client를 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.

H.264 디코딩 허용

원격 데스크톱 및 게시된 애플리케이션 세션에 대해 클라이언트에서 H.264 디코딩을 허용할 수 있습니다.

H.264 디코딩을 허용할 경우 에이전트에서 H.264 인코딩을 지원하면 Horizon Client에서 H.264 디코딩을 사용합니다. 에이전트에서 H.264 인코딩을 지원하지 않을 경우 Horizon Client에서 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 켤 수 있습니다. 새 설정은 설정을 변경한 후에 연결된 모든 세션에 적용됩니다.

서버 바로 가기 관리

서버에 연결되면 Horizon Client가 서버 바로 가기를 만듭니다. 서버 바로 가기를 편집하고 제거할 수 있습니다.

Horizon Client는 서버 이름을 잘못 입력하거나 잘못된 IP 주소를 입력하더라도 바로 가기에 서버 이름 또는 IP 주소를 저장합니다. 서버 이름 또는 IP 주소를 편집하여 이러한 정보를 삭제하거나 변경할 수 있습니다. 서버 설명을 입력하지 않을 경우, 서버 이름 또는 IP 주소가 서버 설명이 됩니다.

절차

1 서버 바로 가기를 마우스 오른쪽 버튼으로 클릭합니다.

컨텍스트 메뉴가 나타납니다.

2 컨텍스트 메뉴를 사용하여 서버 바로 가기를 삭제하거나 서버 이름 또는 서버 설명을 편집합니다.

3 서버 바로 가기를 편집한 경우에는 **완료**를 클릭하여 변경 사항을 저장합니다.

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	로그오프하고 연결을 끊으려면 사이드바에서 **실행 중** 목록의 원격 데스크톱 이름 옆에 있는 **열기 메뉴** 도구 모음 버튼을 클릭하고 **로그오프**를 선택합니다. 원격 데스크톱에서 열려 있는 파일은 저장되지 않고 닫힙니다. 로그오프하지 않고 연결을 끊으려면 **실행 중** 목록의 원격 데스크톱 이름 옆에 있는 **메뉴 열기** 도구 모음 버튼을 클릭하고 **닫기**를 선택합니다. **참고** Horizon administrator는 연결을 끊을 때 자동으로 로그오프하도록 원격 데스크톱을 구성할 수 있습니다. 그러한 경우, 원격 데스크톱에 열려 있는 모든 애플리케이션은 닫힙니다.

원격 데스크톱 또는 게시된 애플리케이션 사용 3

Horizon Client에서는 친숙하고 개인화된 데스크톱 및 애플리케이션 환경을 제공합니다.

본 장은 다음 항목을 포함합니다.

기능 지원 표

최종 사용자에게 제공할 기능을 계획하는 경우, 다음 정보를 사용하여 기능을 지원하는 게스트 운영 체제를 확인하십시오.

표 3-1. Windows 가상 데스크톱에 대해 지원되는 기능

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

이러한 기능 및 해당 제한 사항에 대한 설명을 보려면 Horizon 7 아키텍처 계획 문서를 참조하십시오.

RDS 호스트의 게시된 데스크톱에 대해 지원되는 기능

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

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

표 3-2. View Agent 6.2.6 이상 또는 Horizon Agent 7.0 이상이 설치된 RDS 호스트에 지원되는 기능

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

표 3-2. View Agent 6.2.6 이상 또는 Horizon Agent 7.0 이상이 설치된 RDS 호스트에 지원되는 기능 (계속)

기능	Windows Server 2008 R2 RDS 호스트	Windows Server 2012 R2 RDS 호스트	Windows Server 2016 RDS 호스트	Windows Server 2019 RDS 호스트
VMware Blast 디스플레이 프로토콜	X	X	Horizon Agent 7.0.2 이상	Horizon Agent 7.7 이상
위치 기반 인쇄	View Agent 6.2.6 ~ Horizon Agent 7.6(가상 시스템 전용) Horizon Agent 7.7 이상(가상 시스템 및 물리적 시스템)	View Agent 6.2.6 ~ Horizon Agent 7.6(가상 시스템 전용) Horizon Agent 7.7 이상(가상 시스템 및 물리적 시스템)	Horizon Agent 7.0.2 ~ 7.6(가상 시스템 전용) Horizon Agent 7.7 이상(가상 시스템 및 물리적 시스템)	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	X	X	X	Horizon Agent 7.7 이상
스마트 카드	X	X	X	Horizon Agent 7.7 이상

지원되는 각 게스트 운영 체제의 버전에 대한 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.

제스처

VMware는 Windows가 아닌 태블릿에서 기존 Windows 사용자 인터페이스 요소를 탐색하는 데 도움이 되는 사용자 상호 작용 보조 기능을 제공하고 있습니다.

클릭

다른 애플리케이션의 경우와 마찬가지로 터치패드를 눌러 사용자 인터페이스 요소를 클릭할 수 있습니다. Chromebook에 터치 화면이 있는 경우 터치하여 사용자 인터페이스 요소를 클릭할 수 있습니다. 외부 마우스를 사용할 수도 있습니다.

오른쪽 클릭

오른쪽 클릭으로 사용할 수 있는 옵션은 다음과 같습니다.

- 두 손가락으로 터치패드를 누릅니다.
- 키보드에서 Alt 키를 누른 채로 한 손가락으로 터치패드를 누르십시오.
- 외부 마우스를 사용하여 마우스 오른쪽 버튼을 클릭합니다.
- Chromebook에 터치 화면이 있는 경우 두 손가락으로 눌러 오른쪽 클릭을 수행합니다.

스크롤 및 스크롤 막대

수직 스크롤에 대해 다음 옵션이 제공됩니다.

- 터치패드를 엄지손가락으로 길게 누른 다음 한 손가락으로 아래로 스크롤합니다. 두 손가락으로 스크롤할 수도 있습니다.
- 외부 마우스를 사용하여 스크롤합니다.
- Chromebook에 터치 화면이 있는 경우 두 손가락으로 누른 후 끌어서 스크롤합니다. 손가락 아래 텍스트가 손가락과 동일한 방향으로 이동합니다.

확대 및 축소

확대 및 축소는 지원되지 않습니다.

창 크기 조정

터치패드를 사용하여 창 크기를 조정하려면 창의 모서리 또는 측면에서 손가락 하나를 길게 터치한 후 끌어서 크기를 조정합니다.

Chromebook에 외부 마우스가 있으면 창 가장자리에 커서를 놓고 창의 테두리를 끌어서 더 넓히거나 더 좁힙니다.

Chromebook에 터치 화면이 있는 경우 창의 모서리 또는 측면에서 손가락 하나를 대고 끌어서 크기를 조정합니다.

사운드, 음악 및 비디오

디바이스 사운드가 켜져 있는 경우 원격 데스크톱에서 오디오를 재생할 수 있습니다.

다중 모니터 기능 제한

다중 모니터 기능이 사용되도록 설정된 경우 터치 제스처가 사용되지 않도록 설정됩니다. 자세한 내용은 다중 모니터 사용의 내용을 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 3-3. 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.
게시된 애플리케이션 또는 원격 데스크톱 검색	■ **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 **X**를 누릅니다.
즐겨찾는 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 **즐겨찾기 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 게시된 애플리케이션에 대해 다중 세션 모드 사용의 내용을 참조하십시오.
실행 중인 원격 데스크톱 닫기	사이드바에서 **실행 중** 목록의 원격 데스크톱 이름 옆에 있는 **메뉴 열기** 버튼을 클릭하고 작업을 선택합니다. ■ 운영 체제에서 로그오프하지 않고 원격 데스크톱의 연결만 해제하려면 **닫기**를 선택합니다. Horizon 관리자는 연결을 끊을 때 자동으로 로그오프하도록 원격 데스크톱을 구성할 수 있습니다. 이 경우 열린 애플리케이션의 저장하지 않은 변경 내용은 손실됩니다. ■ **로그오프**를 선택하여 운영 체제에서 로그오프하고 원격 데스크톱에서 연결을 해제합니다. 열린 애플리케이션의 저장하지 않은 변경 내용은 손실됩니다.
실행 중인 게시된 애플리케이션 닫기	사이드바에서 **실행 중** 목록의 게시된 애플리케이션 이름 아래에 있는 파일 이름 옆의 **X**를 클릭합니다. 게시된 애플리케이션을 종료하고 해당 게시된 애플리케이션에 대해 열려 있는 모든 파일을 닫으려면 게시된 애플리케이션 이름 옆에 있는 **X**를 클릭합니다. 파일에 대한 변경 내용을 저장할지 묻는 메시지가 표시됩니다.
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 3-3. 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 **설정**을 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 **설정**을 클릭한 후 **데스크톱용 Windows 키 사용**을 켭니다. 자세한 내용은 바로 가기 키 조합의 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.
H.264 디코딩 허용	사이드바 맨 위의 **메뉴 열기** 도구 모음 버튼을 클릭하고 **설정**을 클릭한 후 **H.264 디코딩 허용**을 켭니다. 자세한 내용은 H.264 디코딩 허용의 내용을 참조하십시오.
다중 모니터 사용	사이드바 맨 위의 **메뉴 열기** 도구 모음 버튼을 클릭하고 [설정]을 선택한 후 **2대의 모니터가 있는 경우 다중 모니터 사용**을 켭니다. 자세한 내용은 다중 모니터 사용의 내용을 참조하십시오.
도움말 항목 표시	사이드바 맨 위의 **메뉴 열기** 도구 모음 버튼을 클릭한 후 **설정**을 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.

다중 모니터 사용

원격 데스크톱에서 최대 2대의 모니터를 사용할 수 있습니다.

원격 데스크톱에 연결되어 있지 않으면 데스크톱 및 애플리케이션 선택기 창의 오른쪽 상단 모서리에 있는 **설정** 도구 모음 버튼을 클릭하고 **설정** 창의 **모니터가 2대 있을 때 다중 모니터 사용** 옵션을 켭니다. 2대의 모니터를 원격 데스크톱에 연결하는 경우 다중 모니터 기능이 사용됩니다. 모니터가 1대뿐이거나 2대 이상 있는 경우 단일 모니터 모드가 사용됩니다. 다른 원격 데스크톱으로 전환하는 경우 다중 모니터 모드에서 열리고, 이전 원격 데스크톱은 단일 모니터 모드로 돌아갑니다.

원격 데스크톱에 이미 연결된 경우 사이드바에서 사용할 수 있는 **설정** 창에서 **모니터가 2대 있을 때 다중 모니터 사용** 옵션을 켜서 다중 모니터 기능을 사용하도록 설정할 수 있습니다.

다중 모니터 기능에는 다음과 같은 제한이 있습니다.

- 게시된 애플리케이션에서는 지원되지 않습니다.
- 클라이언트 디바이스에 대해 통합 데스크톱 모드가 사용되도록 설정되면 이 기능이 지원되지 않습니다.

통합 데스크톱 모드를 사용하지 않도록 설정하는 방법에 대한 내용은 Google Chrome 설명서를 참조하십시오.

전체 화면 모드 사용

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

다중 모니터를 사용하는 경우에는 전체 화면 모드를 사용할 수 없습니다.

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.

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.

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.

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.

기본 비디오 해상도는 320 x 240입니다. 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 Chrome에서 처음으로 사용 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.

기본 웹캠 또는 마이크 선택

실시간 오디오-비디오 기능을 통해 여러 개의 웹캠 또는 마이크가 로컬 클라이언트 시스템에 연결된 경우 디바이스 중 하나만 원격 데스크톱 또는 게시된 애플리케이션에서 사용됩니다. 기본 웹캠이나 마이크를 지정하려는 경우에는 Horizon Client에서 실시간 오디오-비디오 기능을 구성할 수 있습니다.

사용 가능한 경우 기본 웹캠 또는 마이크가 원격 데스크톱 또는 게시된 애플리케이션에서 사용됩니다. 기본 웹캠 또는 마이크를 사용할 수 없는 경우 다른 웹캠이나 마이크가 사용됩니다.

사전 요구 사항

- 로컬 클라이언트 시스템에 USB 웹캠이나 USB 마이크 또는 다른 유형의 마이크가 설치되어 있고 작동하는지 확인합니다.
- 서버에 연결합니다.

절차

1. 데스크톱 및 애플리케이션 선택기 창의 오른쪽 상단 모서리에 있는 **설정** 도구 모음 버튼을 클릭하고 아래로 스크롤하여 실시간 오디오-비디오 설정으로 이동합니다.
2. **기본 마이크** 드롭다운 메뉴에서 기본 마이크를 선택합니다.
3. **기본 웹캠** 드롭다운 메뉴에서 기본 웹캠을 선택합니다.

다음번에 원격 데스크톱 또는 게시된 애플리케이션을 시작하면 선택한 기본 웹캠 또는 마이크가 원격 세션으로 리디렉션됩니다.

텍스트와 이미지 복사 및 붙여넣기

기본적으로 클라이언트 디바이스에서 원격 데스크톱 또는 게시된 애플리케이션으로 일반 텍스트 및 HTML 형식의 서식 있는 텍스트를 복사하여 붙여넣을 수 있습니다.

또한 Horizon 관리자가 해당 기능을 사용하도록 설정할 경우, 원격 데스크톱이나 게시된 애플리케이션에서 일반 텍스트 및 HTML 형식의 서식 있는 텍스트를 복사하여 클라이언트 디바이스에 붙여넣을 수 있습니다.

Horizon 관리자는 복사 및 붙여넣기 작업이 클라이언트 디바이스에서 원격 데스크톱이나 게시된 애플리케이션으로만 허용, 원격 데스크톱이나 게시된 애플리케이션에서 클라이언트 디바이스로만 허용, 둘 다 허용 또는 둘 다 허용되지 않도록 이 기능을 구성할 수 있습니다.

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

- 클립보드 소스가 Google Docs 같은 Google 애플리케이션인 경우 클라이언트 디바이스가 Google 웹 사이트에 액세스할 수 있을 때에만 이미지를 복사한 후 붙여넣을 수 있습니다.
- 이미지 및 서식 있는 텍스트(또는 일반 텍스트)를 클라이언트 디바이스에서 함께 복사하지만 대상이 WordPad와 같이 서식 있는 텍스트만 지원하는 애플리케이션인 경우 해당 이미지는 폐기되고 텍스트만 복사되고 붙여넣어집니다. Microsoft Word와 같이 대상 애플리케이션에서 HTML/XML 형식의 서식 있는 텍스트를 지원하는 경우 이 제한은 적용되지 않습니다.
- Horizon 관리자는 그룹 정책을 사용하여 복사 및 붙여넣기 작업 중에 클립보드 형식을 제한할 수도 있습니다. Microsoft Office Chart, Smart Art 데이터 및 Microsoft Text Effects 데이터에 대한 클립보드 형식 필터 정책은 지원되지 않습니다. 클립보드 형식 필터 정책에 대한 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오. 원격 데스크톱에서 복사 및 붙여넣기 동작을 제어하기 위해 스마트 정책을 사용하는 것은 지원되지 않습니다.

원격 데스크톱이나 게시된 애플리케이션에서 클라이언트 디바이스로 최대 1MB의 데이터를 복사할 수 있습니다. 이 제한을 초과하는 일반 텍스트는 잘립니다. 서식 있는 텍스트는 일반 텍스트로 변환됩니다.

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.

로깅 복사 및 붙여넣기 작업

클립보드 감사 기능을 사용하도록 설정하면 Horizon Agent는 복사 및 붙여넣기 기능에 대한 정보를 에이전트 시스템의 이벤트 로그에 기록합니다. 클립보드 감사 기능은 기본적으로 사용되지 않도록 설정됩니다.

클립보드 감사 기능을 사용하도록 설정하려면 VMware Blast 또는 PCoIP에 대한 **클립보드 감사 구성** 그룹 정책 설정을 구성해야 합니다.

필요에 따라 VMware Blast 또는 PCoIP에 대한 **클라이언트가 감사를 지원하지 않을 때 클라이언트 측으로의 클립보드 리디렉션을 차단할지 여부** 그룹 정책 설정을 구성하여 클립보드 감사 기능을 지원하지 않는 클라이언트로의 클립보드 리디렉션을 차단할지 여부를 지정할 수 있습니다.

이러한 그룹 정책 설정을 구성하는 방법에 대한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서에서 "VMware Blast 정책 설정" 및 "PCoIP 클립보드 설정" 항목을 참조하십시오.

이 기능을 사용하려면 에이전트 시스템에 Horizon Agent 7.7 이상이 필요합니다.

복사 및 붙여넣기 작업에 대한 정보가 기록되는 이벤트 로그를 VMware Horizon RX 감사라고 합니다. 에이전트 시스템에서 이벤트 로그를 보려면 Windows 이벤트 뷰어를 사용합니다. 중앙 위치에서 이벤트 로그를 보려면 VMware Log Insight 또는 Windows 이벤트 수집기를 구성합니다. Log Insight에 대한 내용은 https://docs.vmware.com/kr/vRealize-Log-Insight/index.html을 참조하십시오. Windows 이벤트 수집기에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

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.
- 크기가 0인 폴더나 파일은 다운로드하거나 업로드할 수 없습니다.
- 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.
- 파일을 업로드할 때 크기가 0이거나 2GB보다 큰 폴더 및 파일을 끌어서 놓는 경우 예상대로 오류 메시지가 표시됩니다. 이 오류 메시지를 닫은 후에는 더 이상 파일을 끌어서 놓기하여 전송할 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 전송의 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 전송의 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.

클라이언트 드라이브 리디렉션을 사용하여 로컬 폴더 및 드라이브에 대한 액세스 공유

클라이언트 드라이브 리디렉션 기능을 사용하여 로컬 클라이언트 시스템의 폴더 또는 드라이브를 원격 데스크톱 및 게시된 애플리케이션과 공유할 수 있습니다.

공유 드라이브는 매핑된 드라이브 및 USB 스토리지 디바이스를 포함할 수 있습니다.

클라이언트 드라이브 리디렉션 기능에는 다음과 같은 제한이 있습니다.

- Windows 레지스트리 키 설정 ForcedByAdmin, 기본 공유 및 사용 권한을 사용하여 클라이언트 드라이브 리디렉션을 구성하는 것은 지원되지 않습니다.
- TCP 및 UDP 쪽 채널은 지원되지 않습니다. 에이전트 시스템이 이러한 측면 채널 중 하나를 사용하도록 구성되면 클라이언트 드라이브 리디렉션 기능을 사용할 수 없습니다.

- User Environment Manager 정책은 지원되지 않습니다.
- 네트워크 복구는 지원되지 않습니다. 세션 연결을 끊었다가 다시 연결하지 않으면 네트워크를 다시 연결한 후에 클라이언트 드라이브 리디렉션을 사용할 수 없습니다.
- 한 번에 하나의 원격 세션에서만 클라이언트 드라이브 리디렉션 기능을 사용할 수 있습니다. 여러 원격 세션은 지원되지 않습니다.
- 원격 데스크톱에서 공유 폴더 또는 파일에 대한 속성을 변경할 수 없습니다.

사전 요구 사항

원격 데스크톱 또는 게시된 애플리케이션과 폴더 및 드라이브를 공유하려면 Horizon administrator가 클라이언트 드라이브 리디렉션 기능을 사용하도록 설정해야 합니다. 이 작업 중에는 Horizon Agent 7.4 이상이 설치되고 에이전트의 **클라이언트 드라이브 리디렉션** 옵션이 사용되도록 설정됩니다. 또한 클라이언트 드라이브 리디렉션 동작을 제어하기 위한 설정 정책도 포함됩니다. 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

절차

1. 데스크톱 및 애플리케이션 선택기 창의 오른쪽 상단 모서리에 있는 **설정** 도구 모음 버튼을 클릭하고 [설정] 창에서 **폴더 공유 사용** 옵션을 켭니다.
2. 공유할 특정 폴더 또는 드라이브를 선택하려면 **선택**을 클릭하고 **추가**를 클릭하여 폴더 또는 드라이브를 찾아 선택하고 **확인**을 클릭합니다.

   여러 폴더 및 드라이브를 추가할 수 있지만 한 번에 하나의 항목만 선택할 수 있습니다. [폴더 공유] 대화상자에서 이름 옆의 **X**를 클릭하여 폴더 또는 드라이브를 제거할 수 있습니다.
3. 설정을 저장하려면 **확인**을 클릭합니다.

   폴더 공유 설정은 모든 원격 데스크톱 및 게시된 애플리케이션에 적용됩니다.

원격 데스크톱에서 공유한 각 폴더 및 드라이브에 대한 네트워크 위치가 표시됩니다. 예를 들어, test1이라는 폴더를 공유하는 경우 원격 데스크톱에 test1(Z:) 네트워크 위치가 나타날 수 있습니다. 각 공유 폴더 및 드라이브에 대한 디바이스도 표시됩니다. 디바이스 이름 형식은 *folder* on Horizon(예: test1 on Horizon)입니다.

게시된 애플리케이션 내에서 **파일 > 열기** 또는 **파일 > 다른 이름으로 저장**(해당되는 경우)을 선택하고 공유 폴더 또는 드라이브로 이동할 수 있습니다.

게시된 애플리케이션에 대해 다중 세션 모드 사용

게시된 애플리케이션에 대해 다중 세션 모드를 사용하도록 설정하면 여러 다른 클라이언트 디바이스에서 서버에 로그온할 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 설정의 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 **설정**을 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.

바로 가기 키 조합

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

Chrome을 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.

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.

데스크톱용 Windows 키 사용을 켠 후 Windows 키 누르기를 시뮬레이트하려면 Ctrl+Search를 눌러야 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 3-4. 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.	

표 3-4. Windows 10 원격 데스크톱 및 Windows Server 2016 원격 데스크톱용 Windows 키 바로 가기 (계속)

키	조치	제한 사항
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+Shift+M	원격 데스크톱에서 최소화된 창을 복원합니다.	
Win+Enter	내레이터를 엽니다.	

표 3-5. 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.	
Win	시작 창을 표시하거나 숨깁니다.	
Win+B	알림 영역에 포커스를 설정합니다.	
Win+C	참 패널을 엽니다.	
Win+D	원격 데스크톱을 표시하고 숨깁니다.	
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+,(쉼표)	키를 계속 누르고 있으면 원격 데스크톱을 일시적으로 표시합니다.	Windows 2012 R2 운영 체제에서는 작동하지 않습니다.
Win+Shift+M	원격 데스크톱에서 최소화된 창을 복원합니다.	
Win+Home	활성 원격 데스크톱 창을 제외한 모든 창을 최소화합니다(Win+Home을 한 번 더 누르면 모든 창이 복원됨).	
Win+Enter	내레이터를 엽니다.	

표 3-6. Windows 7 및 Windows Server 2008 R2 원격 데스크톱용 Windows 키 바로 가기

키	조치	제한 사항
Win	**시작** 메뉴를 열거나 닫습니다.	
Win+D	원격 데스크톱을 표시하고 숨깁니다.	
Win+M	모든 창을 최소화합니다.	
Win+E	컴퓨터 폴더를 엽니다.	
Win+R	실행 대화상자를 엽니다.	
Win+Home	활성 원격 데스크톱 창을 제외한 모든 창을 최소화합니다.	
Win+G	실행 중인 원격 데스크톱 가젯을 따라 순환합니다.	
Win+U	접근성 센터를 엽니다.	

국제화

Horizon Client 사용자 인터페이스와 문서는 한국어, 영어, 일본어, 프랑스어, 독일어, 중국어 간체, 중국어 번체 및 스페인어로 제공됩니다. 또한 해당 언어의 문자를 입력할 수 있습니다.

Horizon Client 문제 해결

4

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 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.

사전 요구 사항

Active Directory 사용자 이름/암호, RSA SecurID 사용자 이름/암호 또는 RADIUS 인증 사용자 이름/암호와 같은 로그인 자격 증명을 얻습니다.

절차

- 사이드바에서 **실행 중** 목록의 원격 데스크톱 이름 옆에 있는 **메뉴 열기** 도구 모음 버튼을 클릭하고 **다시 시작**을 선택합니다.

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 데스크톱 또는 게시된 애플리케이션 재설정

데스크톱 운영 체제가 응답하지 않고 원격 데스크톱을 다시 시작해도 문제가 해결되지 않으면 원격 데스크톱을 재설정해야 할 수 있습니다. 게시된 애플리케이션을 재설정하면 열려 있는 모든 애플리케이션이 종료됩니다.

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 저장되지 않은 데이터를 저장하지 않고 애플리케이션이 종료됩니다. 다른 RDS 서버 팜의 애플리케이션을 비롯하여 열려 있는 모든 게시된 애플리케이션이 닫힙니다.

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 화면에서 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.

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.

Chrome용 Horizon Client 제거

Chrome용 VMware Horizon Client 애플리케이션을 제거하려면 다른 Chromebook 애플리케이션을 제거할 때와 같은 방식으로 제거합니다.

절차

1. Chromebook에 로그인합니다.
2. VMware Horizon Client 애플리케이션을 마우스 오른쪽 버튼으로 클릭하고 **제거**를 선택합니다.

다음에 수행할 작업

Chrome용 VMware Horizon Client 애플리케이션을 다시 설치하려면 Chrome용 Horizon Client 설치 또는 업그레이드 항목을 참조하십시오.

로그 수집 사용

로그 수집을 사용하도록 설정하는 경우 Horizon Client는 VMware에서 Horizon Client 문제를 해결하는 데 도움이 되는 로그 정보를 수집합니다.

원격 데스크톱 또는 게시된 애플리케이션에 연결한 후에는 로그 수집을 사용하도록 설정할 수 없습니다.

사전 요구 사항

서버에 연결합니다.

절차

1. 데스크톱 및 애플리케이션 선택기 창의 오른쪽 상단 모서리에 있는 **설정** 도구 모음 버튼을 클릭합니다.
2. 로그 수집을 사용하도록 설정하려면 **설정** 창에서 **로그 수집 사용** 옵션을 켜고 **기본**, **디버그** 또는 **추적** 로그 수준을 선택합니다.

   로그 파일의 경로가 **설정** 창의 **로그 수집 사용** 옵션 아래에 나타납니다.
3. 로그 파일 경로를 변경하려면 기본 경로를 클릭하고, 로그 파일을 저장할 폴더로 이동한 후 선택하고, **저장**을 클릭합니다.

   새 경로가 **설정** 창의 **로그 수집 사용** 옵션 아래에 나타납니다.
4. **설정** 창을 닫으려면 **닫기**를 클릭합니다.

Horizon Client는 Horizon Client를 종료할 때까지 계속 로깅 정보를 수집하고 저장합니다.