

Horizon 7 아키텍처 계획

2019년 3월 14일

VMware Horizon 7 7.8



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

Horizon 7 아키텍처 계획 5

1 Horizon 7 소개 6

Horizon 7 를 사용할 경우의 장점 6

Horizon 7 기능 9

구성 요소를 서로 맞추는 방법 11

Horizon 7 통합 및 사용자 지정 16

2 풍부한 사용자 환경 계획 22

Horizon Agent 용 기능 지원 표 22

디스플레이 프로토콜 선택 23

게시된 애플리케이션 사용 29

Horizon Persona Management를 사용하여 사용자 데이터 및 설정 유지 30

원격 데스크톱 및 애플리케이션에서 USB 디바이스 사용 32

웹캠 및 마이크에 대한 실시간 오디오-비디오 기능 사용 32

3D 그래픽 애플리케이션 사용 33

원격 데스크톱에 멀티미디어 스트리밍 34

원격 데스크톱에서 인쇄 34

로그인에 Single Sign-On 사용 35

모니터 및 화면 해상도 35

3 한 곳에서 데스크톱 및 애플리케이션 풀 관리 38

데스크톱 풀의 장점 38

애플리케이션 풀의 장점 39

스토리지 요구 사항 축소 및 관리 40

애플리케이션 프로비저닝 49

Active Directory GPO를 사용한 사용자 및 데스크톱 관리 53

4 원격 데스크톱 배포를 위한 아키텍처 설계 요소 및 계획 지침 55

원격 데스크톱의 가상 시스템 요구 사항 56

Horizon 7 ESXi 노드 61

특정 작업자 유형의 데스크톱 풀 62

데스크톱 가상 시스템 구성 66

RDS 호스트 가상 시스템 구성 67

vCenter Server 및 View Composer 가상 시스템 구성 67

Horizon 연결 서버 최대값 및 가상 시스템 구성 69

vSphere 클러스터 72

스토리지 및 대역폭 요구 사항 74

Horizon 7 빌드 블록 83

Horizon 7 팟 84

팟에서 다중 vCenter Server를 사용할 경우의 장점 87

5 보안 기능 계획 90

클라이언트 연결 이해 90

사용자 인증 방법 선택 93

원격 데스크톱 액세스 제한 96

그룹 정책 설정을 사용하여 원격 데스크톱 및 애플리케이션 보안 유지 97

스마트 정책 사용 98

보안 클라이언트 시스템에 모범 사례 구현 98

관리자 역할 할당 98

보안 서버 사용 준비 99

통신 프로토콜 이해 105

6 Horizon 7 환경 설정 단계 개요 113

Horizon 7 아키텍처 계획

Horizon 7 아키텍처 계획에서는 VMware Horizon™ 7의 주요 기능과 배포 옵션을 설명하고 운영 환경에서 일반적으로 해당 구성 요소를 설정하는 방법에 대한 개요 등을 소개합니다.

이 설명서에서 다음 질문에 대한 답변을 확인할 수 있습니다.

- 이 제품이 문제를 해결해줍니까?
- 이 솔루션이 기업에서 구현하기에 적당하고 비용 효율적입니까?

VMware Horizon 7의 일부 특징과 기능은 버전에 따라 제공되지 않을 수 있습니다. 버전별 기능 세트 비교는

<http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>를 참조하십시오.

이 설명서에서는 사용자의 설치를 보호하기 위한 보안 기능에 대해서도 논의합니다.

대상

본 정보는 IT 의사 결정자, 설계자, 관리자를 비롯해 이 제품의 구성 요소 및 기능을 숙지해야 하는 기타 사용자를 대상으로 제작되었습니다. 설계자와 기획자는 이 정보를 통해 Horizon 7가 최종 사용자에게 효율적이고 안전하게 Windows 데스크톱과 애플리케이션을 제공하기 위한 기업의 요구 사항을 충족하는지 확인할 수 있습니다. 예제 아키텍처를 통해 설계자가 대규모 배포에 필요한 하드웨어 요구 사항과 설치 작업을 보다 쉽게 이해할 수 있도록 돕습니다.

Horizon 7 소개

IT 부서는 Horizon 7을 사용해 데이터 센터에서 원격 데스크톱 및 애플리케이션을 실행하고 직원들에게 이러한 데스크톱 및 애플리케이션을 관리 서비스로 제공할 수 있습니다. 최종 사용자는 다양한 디바이스를 사용해 회사나 가정 어디에서나 익숙하고 개인화된 환경에 액세스할 수 있습니다. 관리자는 데이터 센터에 데스크톱 데이터를 보관해 중앙 집중화된 제어, 효율성, 보안을 확보할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- Horizon 7를 사용할 경우의 장점
- Horizon 7 기능
- 구성 요소를 서로 맞추는 방법
- Horizon 7 통합 및 사용자 지정

Horizon 7 를 사용할 경우의 장점

Horizon 7로 회사 데스크톱을 관리하면 신뢰성과 보안, 하드웨어 독립성, 편리성 등을 개선할 수 있습니다.

신뢰성 및 보안

VMware vSphere®와 통합하고 서버, 스토리지, 네트워킹 리소스를 가상화하여 데스크톱 및 애플리케이션을 중앙 집중화할 수 있습니다. 데이터 센터 서버에 데스크톱 운영 체제와 애플리케이션을 배치하면 다음과 같은 이점이 있습니다.

- 데이터에 대한 액세스를 쉽게 제한할 수 있습니다. 원격 직원의 가정용 컴퓨터로 중요한 데이터를 복사하지 못하도록 방지할 수 있습니다.
- RADIUS 지원은 2 요소 인증 벤더 사이에서 선택할 때 유연성을 제공합니다. 지원되는 벤더에는 특히 RSA SecureID, VASCO DIGIPASS, SMS Passcode 및 SafeNet이 포함됩니다.
- VMware Identity Manager와 통합함으로써 최종 사용자가 필요할 때 SaaS, Web, Windows 애플리케이션에 액세스하는 데 사용하는 동일한 웹 기반 애플리케이션 카탈로그를 통해 원격 데스크톱에 액세스할 수 있습니다. 원격 데스크톱 내에서 사용자는 또한 이 사용자 지정 애플리케이션 저장소를 통해 애플리케이션에 액세스할 수 있습니다.
- 사전 생성된 Active Directory 계정으로 원격 데스크톱을 프로비저닝하는 기능은 읽기 전용 액세스 정책이 적용된 잠긴 Active Directory 환경의 요구 사항을 해결합니다.

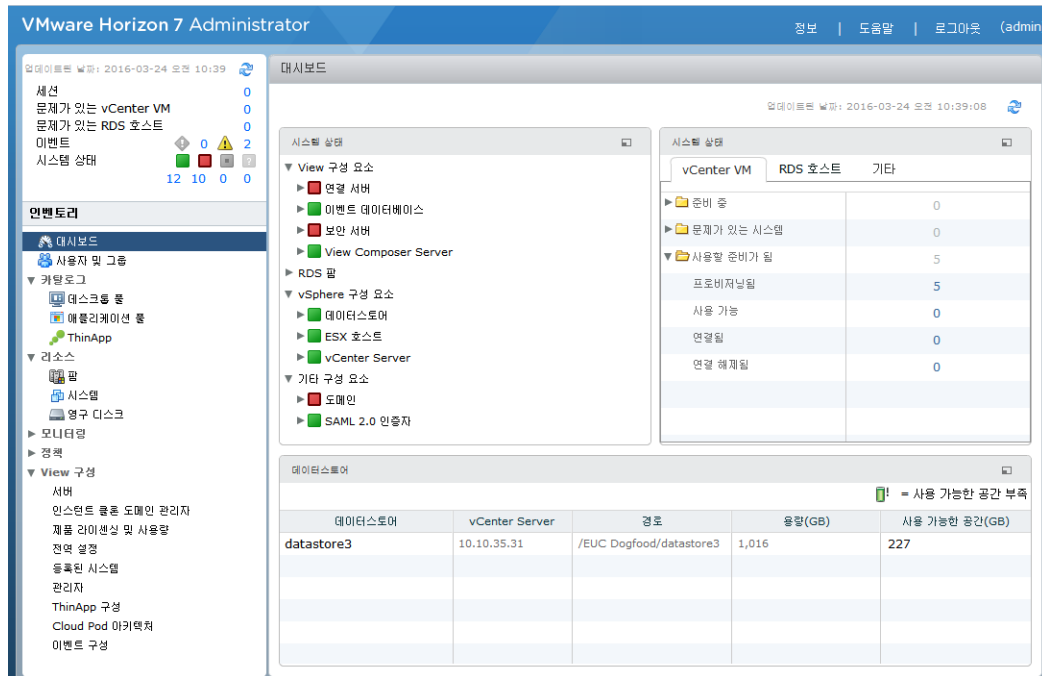
- 최종 사용자의 시스템 종료 시간에 관계 없이 데이터 백업 작업을 예약할 수 있습니다.
- 데이터 센터에서 호스팅되는 원격 데스크톱 및 애플리케이션에는 다운타임이 거의 또는 전혀 발생하지 않습니다. VMware 서버의 고가용성 클러스터에 가상 시스템을 배치할 수 있습니다.

가상 데스크톱을 백엔드 물리적 시스템 및 Microsoft RDS(원격 데스크톱 서비스) 호스트에도 연결할 수 있습니다.

편리성

통합 관리 콘솔은 확장성을 지원하도록 개발되었으므로 최대 규모의 Horizon 7 배포도 단일 관리 인터페이스에서 효율적으로 관리할 수 있습니다. 마법사와 대시보드로 워크플로를 강화하고 드릴다운을 용이하게 하여 자세한 내용을 확인하고 설정을 변경할 수 있습니다. [그림 1-1](#)에서는 Horizon Administrator용 브라우저 기반 사용자 인터페이스의 예를 제공합니다.

그림 1-1. 대시보드 보기를 표시하는 관리 콘솔



편의를 높이는 다른 기능에는 VMware 원격 디스플레이 프로토콜, PCoIP(PC over IP) 및 Blast Extreme이 있습니다. 이러한 디스플레이 프로토콜은 물리적 PC를 사용하는 것과 동일한 최종 사용자 경험을 제공합니다.

- LAN에서는 기존 원격 디스플레이보다 빠르고 원활하게 디스플레이를 구현할 수 있습니다.
- WAN의 경우, 디스플레이 프로토콜은 지연 시간 증가나 대역폭 감소를 보완하여 최종 사용자가 네트워크 조건에 관계 없이 생산성을 유지할 수 있습니다.

관리 효율성

최종 사용자를 위한 데스크톱 및 애플리케이션의 프로비저닝은 신속한 프로세스입니다. 각 최종 사용자의 물리적 PC에 애플리케이션을 하나씩 설치할 필요가 없습니다. 최종 사용자는 애플리케이션이 완벽하게 구축된 원격 데스크톱 또는 게시된 애플리케이션에 연결합니다. 최종 사용자는 다양한 위치에서 다양한 디바이스를 사용해 동일한 원격 데스크톱 또는 애플리케이션에 액세스할 수 있습니다.

VMware vSphere를 사용하여 가상 데스크톱 및 RDS 호스트 서버를 호스팅하면 다음과 같은 장점을 얻을 수 있습니다.

- 관리 작업이 줄어듭니다. 관리자는 사용자의 물리적 PC에 손대지 않고 애플리케이션과 운영 체제를 업그레이드하고 패치를 설치할 수 있습니다.
- VMware Identity Manager와 통합을 통해 IT 관리자는 웹 기반 VMware Identity Manager 관리 인터페이스를 사용하여 원격 데스크톱에 대한 사용자 및 그룹 권한을 모니터링할 수 있습니다.
- 실시간 애플리케이션 제공 시스템인 VMware App Volumes와의 통합 덕분에 기업에서 애플리케이션을 대규모로 제공 및 관리할 수 있습니다. 사용자가 데스크톱에 로그인해 있는 동안에도 App Volumes를 사용하여 애플리케이션을 사용자, 그룹 또는 대상 컴퓨터에 연결합니다. 애플리케이션을 실시간으로 프로비저닝, 제공, 업데이트 및 제거할 수도 있습니다.
- Horizon Persona Management가 있는 경우, 사용자 프로파일, 애플리케이션 권한, 정책, 성능 및 기타 설정을 포함한 물리적 및 가상 데스크톱을 중앙에서 관리할 수 있습니다. 가상 데스크톱으로 변환하기 전에 개인 설정 관리를 물리적 데스크톱에 배포하십시오.
- VMware User Environment Manager를 사용하면 최종 사용자가 사용자의 상황에 따라 조정되는 개인 설정 Windows 데스크톱을 얻을 수 있으므로 역할, 디바이스 및 위치와 같은 측면에 따라 필요한 IT 리소스에 대한 액세스 권한이 제공됩니다.
- 스토리지 관리 작업이 간소화됩니다. VMware vSphere를 사용하면 볼륨과 파일 시스템을 가상화할 수 있어 스토리지 디바이스를 별도로 관리할 필요가 없습니다.
- vSphere 6.0 이상 릴리스를 통해 VVol(가상 볼륨)을 사용할 수 있습니다. 이 기능은 가상 디스크와 파생물, 클론, 스냅샷 및 복제본을 가상 볼륨이라고 하는 스토리지 시스템의 개체에 직접 매핑합니다. 이 매핑을 통해 vSphere가 스냅샷 생성 및 복제와 같은 중점 스토리지 작업을 스토리지 시스템으로 오프로드할 수 있습니다. 예를 들어 이전에 1시간이 걸렸던 복제 작업이 가상 볼륨을 사용하여 이제는 단 몇 분만 소요됩니다.
- vSphere 5.5 업데이트 1 이상 릴리스에서는 vSAN을 사용할 수 있습니다. 이 기능은 여러 ESXi™ 호스트에서 사용 가능한 물리적 로컬 SSD(solid-state disk)와 하드 디스크 드라이브를 클러스터의 모든 호스트에서 공유되는 단일 데이터스토어로 가상화합니다. 데스크톱 풀을 생성할 때 하나의 데이터스토어만 지정하면 가상 시스템 파일, 복제본, 사용자 데이터 및 운영 체제 파일과 같은 다양한 구성 요소가 적절한 SSD 디스크 또는 하드 드라이브 디스크에 배치됩니다.

용량, 성능 및 가용성과 같은 가상 시스템 스토리지 요구 사항을 데스크톱 풀을 생성할 때 자동으로 생성되는 기본 스토리지 정책 프로파일의 형태로 관리합니다.
- Horizon 7 Storage Accelerator가 있는 경우, IOPS 스토리지 로드가 극적으로 감소되어 특별한 스토리지 어레이 기술 필요 없이 더 큰 스케일로 최종 사용자 로그인을 지원합니다.

- 원격 데스크톱이 vSphere 5.1 이상에서 제공되는 공간 효율적인 디스크 형식을 사용하는 경우 지우기 및 축소 프로세스를 통해 게스트 운영 체제 내의 오래되거나 삭제된 데이터가 자동으로 재사용됩니다.

하드웨어 독립성

원격 데스크톱과 게시된 애플리케이션은 하드웨어 독립적입니다. 예를 들어 원격 데스크톱은 데이터 센터의 서버에서 실행되고 클라이언트 디바이스에서만 액세스되므로 원격 데스크톱에서 클라이언트 디바이스의 하드웨어와 호환되지 않는 운영 체제를 사용할 수 있습니다.

PC, Mac, 썬 클라이언트뿐 아니라 썬 클라이언트, 태블릿 및 전화기로 용도가 변경된 PC에서도 원격 데스크톱을 실행할 수 있습니다. 게시된 애플리케이션은 이러한 디바이스 중 일부에서 실행됩니다. 새 디바이스 지원 기능은 분기별로 추가됩니다.

HTML Access 기능을 사용하면 최종 사용자가 클라이언트 시스템이나 디바이스에 클라이언트 애플리케이션을 설치할 필요 없이 브라우저 내에서 원격 데스크톱 또는 애플리케이션을 열 수 있습니다.

Horizon 7 기능

Horizon 7에 포함된 기능은 사용성, 보안, 중앙 집중식 제어 및 확장성을 지원합니다.

다음 기능은 최종 사용자에게 친숙한 환경을 제공합니다.

- 일부 클라이언트 디바이스의 경우 가상 데스크톱에서 클라이언트 디바이스에 정의된 로컬 또는 네트워크 프린터로 인쇄합니다. 이 가상 프린터 기능은 호환성 문제를 해결해주므로 가상 시스템에 추가 인쇄 드라이버를 설치할 필요가 없습니다.
- 대부분의 클라이언트 디바이스에서, 위치 기반 인쇄 기능을 사용하여 클라이언트 시스템에 물리적으로 근접한 프린터로 매핑합니다. 위치 기반 인쇄를 위해 인쇄 드라이버를 가상 시스템에 설치해야 합니다.
- 로컬 프린터 리디렉션은 다음과 같은 사용 사례에 맞게 고안되었습니다.
 - 클라이언트의 USB 또는 직렬 포트에 직접 연결된 프린터
 - 클라이언트에 연결된 바코드 프린터 및 레이블 프린터와 같은 특수 프린터
 - 가상 세션에서 주소를 지정할 수 없는 원격 네트워크의 네트워크 프린터
- 다중 모니터를 사용합니다. PCoIP 및 Blast Extreme 디스플레이 프로토콜에서 다중 모니터 지원이란 각 모니터에 대해 디스플레이 해상도와 회전을 개별적으로 조정할 수 있는 것을 의미합니다.
- 가상 데스크톱을 표시하는 로컬 디바이스에 연결된 기타 주변 기기 및 USB 디바이스에 액세스합니다.

최종 사용자가 연결할 수 있는 USB 디바이스의 유형을 지정할 수 있습니다. 비디오 입력 디바이스 및 스토리지 디바이스와 같은 여러 디바이스 유형을 포함하는 복합 디바이스의 경우, 하나의 디바이스(예: 비디오 입력 디바이스)는 허용되지만 다른 디바이스(예: 스토리지 디바이스)는 허용되지 않도록 디바이스를 분할할 수 있습니다.

- 데스크톱을 새로 고치거나 재구성한 후에도 세션 간에 사용자 설정 및 데이터를 유지하려면 Horizon Persona Management를 사용하십시오. 개인 설정 관리를 사용하면 원하는 주기마다 사용자 프로파일을 원격 프로파일 저장소(CIFS 공유)로 복제할 수 있습니다.

또한 Horizon 7으로 관리되지 않는 가상 시스템 및 물리적 컴퓨터에서 개인 설정 관리의 독립 실행형 버전을 사용할 수 있습니다.

Horizon 7는 특히 다음 보안 기능을 제공합니다.

- RSA SecurID 또는 RADIUS(Remote Authentication Dial-In User Service)와 같은 2 요소 인증 또는 스마트 카드를 사용하여 로그인합니다.
- Active Directory를 위한 읽기 전용 액세스 정책이 있는 환경에서 원격 데스크톱 및 애플리케이션을 프로비저닝할 때 미리 만든 Active Directory 계정을 사용합니다.
- SSL/TLS 터널링을 사용하여 모든 연결이 완벽하게 암호화되었는지 확인합니다.
- VMware High Availability를 사용하여 자동 페일오버를 보장합니다.

확장성 기능은 데스크톱 및 서버 모두를 관리하는 VMware 가상화 플랫폼에 따라 다릅니다.

- VMware vSphere와 통합하여 원격 데스크톱 및 애플리케이션에 대한 비용 효율적인 밀도, 높은 수준의 가용성 및 고급 리소스 할당 제어를 구현합니다.
- Horizon 7 Storage Accelerator 기능을 사용하여 동일한 스토리지 리소스로 더 큰 규모의 최종 사용자 로그인을 지원합니다. 이 Storage Accelerator는 vSphere 5 플랫폼의 기능을 사용하여 공통 블록 읽기의 호스트 메모리 캐시를 생성합니다.
- 최종 사용자와 이러한 사용자에게 액세스 권한이 부여된 원격 데스크톱/애플리케이션 사이의 연결을 브로커링하도록 Horizon 연결 서버를 구성합니다.
- 마스터 이미지와 가상 디스크를 공유하는 데스크톱 이미지를 빠르게 생성하려면 View Composer를 사용하십시오. 이 방법으로 연결된 클론을 사용하면 디스크 공간이 절약되며 운영 체제에 대한 패치 및 업데이트 관리가 간소화됩니다.
- Horizon 7에 도입된 인스턴트 클론 기능을 사용하여 가상 디스크 및 메모리를 상위 이미지와 공유하는 데스크톱 이미지를 빠르게 만들 수 있습니다. 인스턴트 클론은 View Composer 연결된 클론의 공간 효율을 갖추고 있을 뿐만 아니라 새로 고침, 재구성, 재조정도 필요가 없으므로 운영 체제의 패치 및 업데이트 관리가 더 단순합니다. 인스턴트 클론을 사용하면 데스크톱 유지 보수 기간을 따로 지정할 필요가 없습니다.

다음 기능은 집중 관리를 제공합니다.

- Microsoft Active Directory를 사용하여 원격 데스크톱 및 애플리케이션에 대한 액세스를 관리하고 정책을 관리합니다.
- 개인 설정 관리를 사용하여 물리적 데스크톱에서 가상 데스크톱으로 마이그레이션을 단순화 및 간소화합니다.
- 웹 기반 관리 콘솔을 사용하여 임의의 위치에서 원격 데스크톱 및 애플리케이션을 관리합니다.
- Horizon Administrator를 사용해 VMware ThinApp[™]으로 패키징된 애플리케이션을 배포 및 관리합니다.
- 템플릿 또는 마스터 이미지를 사용하여 데스크톱의 풀을 빠르게 생성하고 프로비저닝합니다.

- 사용자 설정, 데이터 또는 환경 설정에 영향을 주지 않은 채 가상 데스크톱으로 업데이트 및 패치를 보냅니다.
- VMware Identity Manager과 통합되어 최종 사용자가 웹의 사용자 포털을 통해 원격 데스크톱에 액세스하고 원격 데스크톱 내의 브라우저에서 VMware Identity Manager를 사용할 수도 있습니다.
- Mirage™ 및 Horizon FLEX™와 통합되어 로컬에 설치된 가상 시스템 데스크톱을 관리하고, 사용자 설치 애플리케이션을 덮어쓰지 않고도 전용 전체 클론 원격 데스크톱에서 애플리케이션을 배포 및 업데이트합니다.

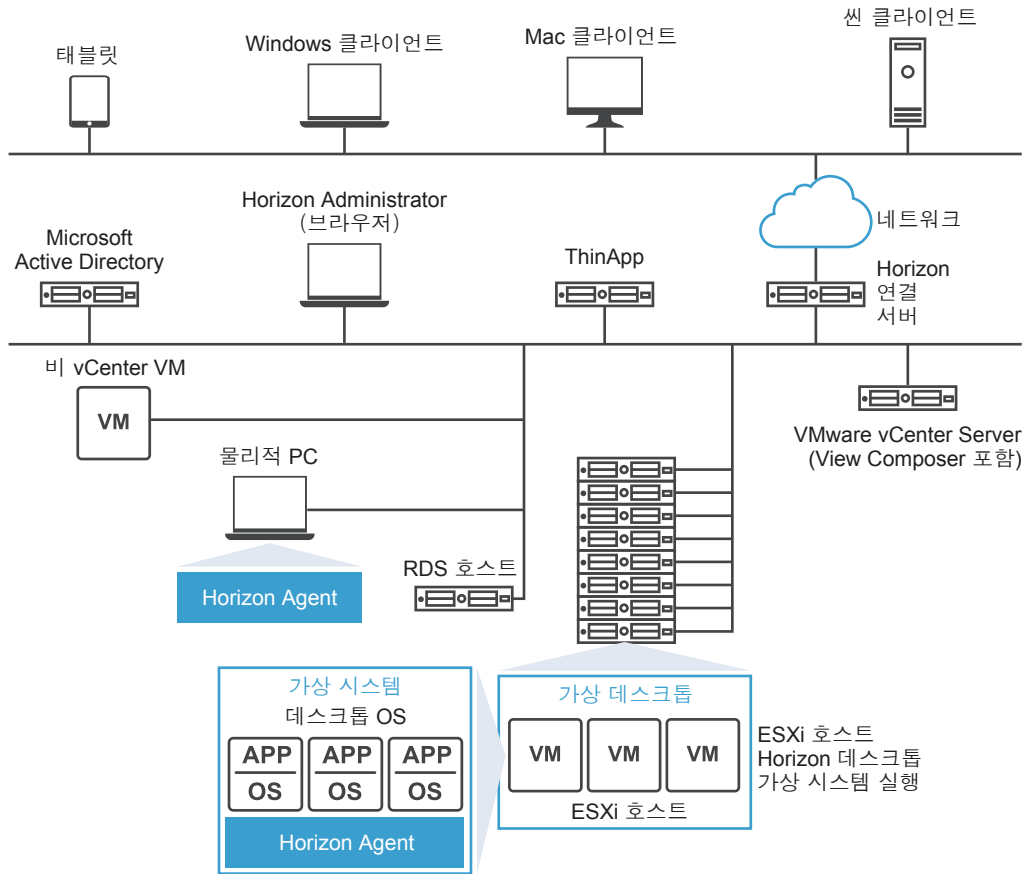
구성 요소를 서로 맞추는 방법

최종 사용자는 Horizon Client를 시작해 Horizon 연결 서버에 로그인합니다. Windows Active Directory와 통합되는 이 서버는 VMware vSphere 서버, 물리적 PC 또는 Microsoft RDS 호스트에서 호스팅되는 원격 데스크톱에 액세스할 수 있도록 합니다. 또한 Horizon Client는 Microsoft RDS 호스트의 게시된 애플리케이션에 액세스할 수 있도록 합니다.

참고 Horizon 7은 AD DS(Active Directory 도메인 서비스) 도메인 기능 수준을 지원합니다. 지원되는 AD DS 도메인 기능 수준에 대한 자세한 내용은 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2150351>를 참조하십시오.

그림 1-2에서는 Horizon 7 배포의 주요 구성 요소 간 관계를 보여 줍니다.

그림 1-2. Horizon 7 환경의 개괄적인 예



클라이언트 디바이스

Horizon 7 사용을 통해 얻을 수 있는 주요 장점은 디바이스 또는 위치에 관계없이 최종 사용자가 원격 데스크톱 및 애플리케이션을 사용할 수 있다는 점입니다. 사용자는 회사 랩톱, 가정용 PC, 썬 클라이언트 디바이스, Mac, 태블릿 또는 전화기에서 개인화된 가상 데스크톱 또는 원격 애플리케이션에 액세스할 수 있습니다.

최종 사용자가 Horizon Client를 열어 자신의 원격 데스크톱 및 애플리케이션을 표시합니다. 썬 클라이언트 디바이스는 Horizon 7 썬 클라이언트 소프트웨어를 사용하고 구성될 수 있기 때문에 사용자는 애플리케이션 가운데 Horizon 7 Thin Client만 디바이스에서 직접 시작할 수 있습니다. 레거시 PC를 썬 클라이언트 데스크톱으로 재설정하면 하드웨어 수명을 3-5년 가량 연장할 수 있습니다. 예를 들어 썬 데스크톱에서 Horizon 7를 사용하면 이전 데스크톱 하드웨어에서 Windows 8.x와 같은 최신 운영 체제를 사용할 수 있습니다.

HTML Access 기능을 사용하면 최종 사용자가 클라이언트 시스템이나 디바이스에 클라이언트 애플리케이션을 설치할 필요 없이 브라우저 내에서 원격 데스크톱을 열 수 있습니다.

Horizon 연결 서버

이 소프트웨어 서비스는 클라이언트 연결의 브로커 역할을 합니다. Horizon 연결 서버는 Windows Active Directory를 통해 사용자를 인증하고 요청을 해당 가상 시스템, 물리적 PC 또는 Microsoft RDS 호스트에 전달합니다.

연결 서버는 다음 관리 기능을 제공합니다.

- 사용자 인증
- 사용자에게 특정 데스크톱 및 풀에 대한 권한 부여
- VMware ThinApp과 패키징된 애플리케이션을 특정 데스크톱 및 풀에 할당
- 원격 데스크톱 및 애플리케이션 세션 관리
- 사용자와 원격 데스크톱 및 애플리케이션 간 보안 연결 설정
- 단일 로그인을 사용하도록 설정
- 정책 설정 및 적용

회사 방화벽 내에 두 개 이상의 연결 서버 인스턴스의 그룹을 설치 및 구성합니다. 해당 구성 데이터는 내장된 LDAP 디렉토리에 저장되고 그룹의 구성원 사이에서 복제됩니다.

회사 방화벽 외부의 DMZ에서는 연결 서버를 보안 서버로 설치 및 구성하거나 Unified Access Gateway 장치를 설치할 수 있습니다. DMZ의 보안 서버 및 Unified Access Gateway 장치는 회사 방화벽 내 연결 서버와 통신합니다. 보안 서버와 Unified Access Gateway 장치는 확실히 인증된 사용자를 대신하는 원격 데스크톱 및 애플리케이션 트래픽만이 회사 데이터 센터에 들어갈 수 있음을 보장합니다. 사용자는 액세스 권한을 부여받은 리소스에만 액세스할 수 있습니다.

보안 서버는 하위 집합 기능을 제공하며 Active Directory 도메인에 있지 않아도 됩니다. 연결 서버를 Windows Server 2008 R2 또는 Windows Server 2012 R2 서버에 설치합니다. 가능하면 VMware 가상 시스템에 설치하는 것이 좋습니다. Unified Access Gateway 장치에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성을 참조하십시오.

중요 연결 서버를 사용하지 않는 Horizon 7 설정을 생성할 수 있습니다. 원격 가상 시스템 데스크톱에서 Horizon 7 Agent Direct Connect 플러그인을 설치하는 경우 클라이언트에서 가상 시스템에 직접 연결할 수 있습니다. PCoIP, HTML Access, RDP, USB 리디렉션 및 세션 관리를 비롯한 모든 원격 데스크톱 기능이 사용자가 연결 서버를 통해 연결한 것처럼 동일한 방식으로 작동합니다. 자세한 내용은 Horizon 7 Agent Direct-Connection 플러그인 관리를 참조하십시오.

Horizon Client

원격 데스크톱 및 애플리케이션에 액세스하기 위한 클라이언트 소프트웨어는 태블릿, 전화기, Windows/Linux/Mac PC 또는 랩톱, 쉘 클라이언트 등에서 실행할 수 있습니다.

로그인 후 사용자는 사용 권한이 있는 원격 데스크톱 및 애플리케이션 목록에서 선택합니다. 인증에는 Active Directory 자격 증명, UPN, 스마트 카드 PIN이나 RSA SecurID 또는 다른 2 요소 인증 토큰이 필요할 수 있습니다.

관리자는 최종 사용자가 디스플레이 프로토콜을 선택할 수 있도록 Horizon Client를 구성할 수 있습니다. 프로토콜에는 원격 데스크톱을 위한 PCoIP, Blast Extreme 및 Microsoft RDP가 포함됩니다. PCoIP 및 Blast Extreme의 속도와 디스플레이 품질은 물리적 PC의 속도 및 디스플레이 품질에 못지 않습니다.

사용하는 Horizon Client에 따라 기능이 달라집니다. 이 가이드에서는 Windows용 Horizon Client를 중심으로 설명합니다. 다음 클라이언트 유형은 이 안내서에서 자세히 다루지 않습니다.

- 태블릿, Linux 클라이언트 및 Mac 클라이언트용 Horizon Client에 대한 자세한 내용은 Horizon Client 설명서(<https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>)를 참조하십시오.
- HTML Access Web client는 클라이언트 시스템 또는 디바이스에 Horizon Client 애플리케이션이 설치되지 않았을 경우 브라우저 내에서 원격 데스크톱을 열 수 있도록 해 줍니다. 이 애플리케이션에 대한 자세한 내용은 Horizon Client 설명서(<https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>)를 참조하십시오.
- 다양한 타사 썬 클라이언트 및 제로 클라이언트(인증된 파트너를 통해서만 사용할 수 있음).
- View Open Client(VMware 파트너 인증 프로그램 지원). View Open Client는 공식 클라이언트 애플리케이션이 아니며 그 자체로는 지원되지 않습니다.

VMware Horizon 사용자 웹 포털

클라이언트 디바이스에 있는 웹 브라우저에서 최종 사용자는 원격 데스크톱 및 애플리케이션에 연결하고, 설치되어 있을 경우 Horizon Client를 자동으로 시작하거나 Horizon Client 설치 관리자를 다운로드할 수 있습니다.

브라우저를 열고 Horizon Connection Server 인스턴스의 URL을 입력할 때 나타나는 웹 페이지에는 Horizon Client 다운로드를 위한 [VMware 다운로드 사이트](#)에 대한 링크가 있습니다. 그러나 이 웹 페이지의 링크는 구성 가능합니다. 예를 들어, 내부 웹 서버를 가리키도록 링크를 구성하거나 해당 고유 연결 서버에 사용할 수 있는 클라이언트 버전을 제한할 수 있습니다.

HTML Access 기능을 사용하는 경우에도 지원되는 브라우저 내에서 원격 데스크톱 및 애플리케이션에 액세스할 수 있는 링크가 웹 페이지에 표시됩니다. 이 기능을 사용하면 Horizon Client 애플리케이션이 클라이언트 시스템 또는 디바이스에 설치되지 않습니다. 자세한 내용은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>의 Horizon Client 설명서를 참조하십시오.

Horizon Agent

원격 데스크톱 및 애플리케이션의 소스로 사용하는 모든 가상 시스템, 물리적 시스템 및 Microsoft RDS 호스트에 Horizon Agent 서비스를 설치합니다. 가상 시스템에서 이 에이전트는 Horizon Client와 통신하여 연결 모니터링, 가상 인쇄, Horizon Persona Management 그리고 로컬로 연결된 USB 디바이스 액세스 등의 기능을 제공합니다.

데스크톱 소스가 가상 시스템인 경우 먼저 해당 가상 시스템에 Horizon Agent 서비스를 설치한 다음 템플릿 또는 연결된 클론 또는 인스턴트 클론의 상위 항목으로 가상 시스템을 사용합니다. 이 가상 시스템에서 풀을 생성할 때 에이전트가 모든 원격 데스크톱에 자동으로 설치됩니다.

단일 로그인 옵션을 사용하여 에이전트를 설치할 수 있습니다. Single Sign-On을 사용하는 경우 사용자가 Horizon 연결 서버에 연결할 때만 로그인 메시지가 나타나며 원격 데스크톱 또는 애플리케이션에 연결할 때는 메시지가 다시 나타나지 않습니다.

Horizon Administrator

이 웹 기반 애플리케이션을 사용하여 관리자는 Horizon 연결 서버를 구성하고, 원격 데스크톱 및 애플리케이션을 배포 및 관리하고, 사용자 인증을 제어하며, 최종 사용자 문제를 해결할 수 있습니다.

연결 서버 인스턴스를 설치할 때 Horizon Administrator 애플리케이션도 설치됩니다. 이 애플리케이션을 사용하여 로컬 컴퓨터에 애플리케이션을 설치할 필요 없이 어디에서든 연결 서버 인스턴스를 관리할 수 있습니다.

View Composer

가상 시스템을 관리하는 vCenter Server 인스턴스 또는 개별 서버에 이 소프트웨어 서비스를 설치할 수 있습니다. 그런 다음 View Composer는 지정한 상위 가상 시스템에서 연결된 클론의 풀을 생성할 수 있습니다. 이 전략으로 스토리지 비용이 최고 90%까지 감소됩니다.

각 연결된 클론은 고유 호스트 이름 및 IP 주소를 사용하여 독립 데스크톱처럼 작동하지만 기본 이미지를 상위 이미지와 공유하기 때문에 연결된 클론은 매우 적은 양의 스토리지를 필요로 합니다. 연결된 클론 데스크톱 풀에서 기본 이미지를 공유하기 때문에 상위 가상 시스템만 업데이트해 업데이트 및 패치를 신속하게 배포할 수 있습니다. 최종 사용자의 설정, 데이터 및 애플리케이션은 영향 받지 않습니다.

또한 View Composer를 사용하여 연결된 클론 Microsoft RDS 호스트의 자동화된 팜을 만들 수도 있으며, 이렇게 하면 게시된 애플리케이션을 최종 사용자에게 제공할 수 있습니다.

서버 호스트에 View Composer를 설치할 수 있지만 View Composer 서비스는 vCenter Server 인스턴스 하나와만 작동할 수 있습니다. 마찬가지로 vCenter Server 인스턴스는 View Composer 서비스 하나와만 연결될 수 있습니다.

중요 View Composer는 선택 구성 요소입니다. 인스턴트 클론을 프로비저닝할 계획인 경우에는 View Composer를 설치할 필요가 없습니다.

vCenter Server

이 서비스는 네트워크로 연결된 VMware ESXi 서버의 중앙 관리자 역할을 합니다.

vCenter Server를 사용하면 한곳에서 데이터 센터의 가상 시스템을 구성, 프로비저닝 및 관리할 수 있습니다.

이러한 가상 시스템을 가상 시스템 데스크톱 풀의 소스로 사용하는 것 외에도 가상 시스템을 사용하여 Horizon Connection Server 인스턴스, Active Directory 서버, Microsoft RDS 호스트 및 vCenter Server 인스턴스를 포함한 Horizon 7의 서버 구성 요소를 호스팅할 수 있습니다.

vCenter Server와 동일한 서버 또는 다른 서버에 View Composer를 설치할 수 있습니다. 그런 다음 vCenter Server에서 물리적 서버 및 스토리지에 대한 가상 시스템 할당을 관리하고 가상 시스템에 대한 CPU 및 메모리 리소스 할당을 관리합니다.

vCenter Server를 VMware 가상 장치로 설치하거나, vCenter Server를 Windows Server 2008 R2 서버 또는 Windows Server 2012 R2 서버에 설치할 수 있습니다(VMware 가상 시스템에 설치 권장).

Horizon 7 통합 및 사용자 지정

여러 가지 인터페이스를 사용해 Horizon 7와 외부 애플리케이션을 통합하거나 명령줄 또는 배치 모드에서 실행할 수 있는 관리 스크립트를 생성함으로써 조직에서 Horizon 7의 효율성을 향상할 수 있습니다.

다른 구성 요소와 통합

Horizon 7은 이러한 VMware 제품과 통합됩니다.

VMware Cloud on AWS

VMware Cloud on AWS에서는 Amazon Web Services에서 vSphere 데이터 센터를 생성할 수 있습니다. 이러한 vSphere 데이터 센터에는 데이터 센터, 스토리지에 대한 vSAN 및 네트워킹을 위한 VMware NSX를 관리하기 위한 vCenter Server가 포함되어 있습니다. 온-프레미스 데이터 센터를 클라우드 SDDC에 연결하고, 단일 vSphere Client 인터페이스에서 둘 다를 관리할 수 있습니다. 연결된 AWS 계정을 사용하여, SDDC의 가상 시스템에서 EC2 및 S3와 같은 AWS 서비스에 액세스할 수 있습니다. 자세한 내용은 <https://docs.vmware.com/kr/VMware-Cloud-on-AWS/index.html>의 VMware Cloud on AWS 설명서를 참조하십시오.

Horizon 7 버전 7.5부터는 VMware Cloud on AWS에 Horizon 7의 전체 클론을 배포할 수 있습니다. 예를 들어, 온-프레미스 데이터 센터 및 VMware Cloud on AWS 인스턴스에서 Cloud Pod 아키텍처를 사용하는 Horizon 7 환경을 배포할 수 있습니다. 이렇게 하면 Horizon 7이 하이브리드 클라우드 환경에서 쉽게 실행되고 SDDC 인프라 관리를 VMware로 아웃소싱할 수 있습니다.

VMware Identity Manager

VMware Identity Manager와 Horizon 7를 통합하여 IT 관리자와 최종 사용자에게 다음과 같은 장점을 제공할 수 있습니다.

- 최종 사용자는 필요할 때 SaaS, Web, Windows 애플리케이션에 액세스하는 데 사용하는 동일한 웹 기반 사용자 포털을 통해 동일한 단일 로그인 기능을 사용하여 원격 데스크톱 및 애플리케이션에 액세스할 수 있습니다.

True SSO 기능을 이용하면 스마트 카드나 2요소 인증을 사용하는 사용자가 Active Directory 자격 증명을 제공하지 않고도 원격 데스크톱 및 애플리케이션에 액세스할 수 있습니다.

- 최종 사용자는 원격 데스크톱 내에서 웹 기반 VMware Identity Manager에 액세스하여 필요한 애플리케이션을 사용할 수 있습니다.
- 또한 HTML Access 기능을 사용하면 최종 사용자가 클라이언트 시스템이나 디바이스에 클라이언트 애플리케이션을 설치할 필요 없이 브라우저 내에서 원격 데스크톱을 열 수 있습니다.
- IT 관리자는 VMware Identity Manager의 브라우저 기반 관리 콘솔을 사용하여 원격 데스크톱에 대한 사용자 및 그룹 권한을 모니터링할 수 있습니다.

VMware Mirage 및 Horizon FLEX

Mirage 및 Horizon FLEX를 통해 사용자가 설치한 애플리케이션 또는 데이터를 덮어쓰지 않고 전용 전체 클론 원격 데스크톱에서 애플리케이션을 배포하고 업데이트할 수 있습니다.

Mirage는 이전에 Horizon 7에 포함되어 있던 Local Mode 기능보다 뛰어난 오프라인 가상 데스크톱 솔루션을 제공합니다. Mirage에는 다음과 같이 오프라인 데스크톱을 위한 보안 및 관리 기능이 포함되어 있습니다.

- 로컬에 설치된 가상 시스템을 암호화하고 사용자가 보안 컨테이너의 무결성에 영향을 미치는 가상 시스템 설정을 수정하지 못하도록 합니다.
- VMware Fusion™ Professional 및 VMware® Player Plus™에서 사용할 수 있는 만료 정책 등의 정책을 제공합니다. 이 정책은 이전 Local Mode 기능에서 제공된 정책과 비슷합니다. Fusion Pro와 Player Plus는 Mirage에 포함되어 있습니다.
- 사용자는 업데이트를 수신하기 위해 데스크톱을 체크인하거나 체크아웃할 필요가 없습니다.
- 관리자는 Mirage 계층화 기능, 백업 기능 및 파일 포털을 활용할 수 있습니다.

VMware App Volumes

VMware App Volumes는 Horizon 7 및 기타 가상 환경을 위한 통합 애플리케이션 제공 및 사용자 관리 시스템입니다. App Volumes로 관리하는 애플리케이션 및 데이터는 로그인 또는 재부팅 시에 각 Windows 사용자 세션에 연결되는, AppStacks라는 특화된 VMDK 또는 VHD에서 유지됩니다. 이 전략을 사용하면 최신 애플리케이션 및 데이터를 사용자에게 제공할 수 있습니다. 또한 App Volumes는 영구 사용자 설치 애플리케이션 및 설정에 대해 쓰기 가능한 볼륨이라고 하는 다른 컨테이너를 제공하는데, 이 볼륨은 로그인 또는 재부팅 시에도 로드됩니다. 사용자 프로파일 및 정책 설정도 App Volumes 플랫폼을 사용하여 관리할 수 있습니다.

VMware User Environment Manager

스마트 정책 기능을 사용하여 특정 원격 데스크톱의 USB 리디렉션, 가상 인쇄, 클립보드 리디렉션, 클라이언트 드라이브 리디렉션, PCoIP 디스플레이 프로토콜 기능의 동작을 제어하는 정책을 만들 수 있습니다. User Environment Manager를 사용하면 IT에서 사용자가 개인 설정할 수 있는 설정을 제어하고 네트워크 및 위치별 프린터와 같은 환경 설정을 매핑할 수 있습니다. 스마트 정책을 사용하면 특정 조건이 충족된 경우에만 적용되는 정책을 만들 수 있습니다. 예를 들어, 사용자가 회사 네트워크 외부에서 원격 데스크톱에 연결한 경우 클라이언트 드라이브 리디렉션 기능을 사용하지 않도록 설정하는 정책을 구성할 수 있습니다.

VMware Unified Access Gateway

Unified Access Gateway는 회사 방화벽 외부에서 원격 데스크톱 및 애플리케이션에 액세스하려는 사용자에게 보안 게이트웨이로 사용됩니다. Unified Access Gateway는 DMZ(예외 구역)에 설치되는 장치입니다. Unified Access Gateway를 사용하여 강력하게 인증된 원격 사용자에게 대한 트래픽만 회사 데이터 센터로 유입되도록 합니다. Horizon 7 보안 서버 대신 Unified Access Gateway 장치를 사용할 수 있습니다. 자세한 내용은 Unified Access Gateway 설명서를 참조하십시오.

일반적인 비디오 회의 소프트웨어와 통합

이러한 오디오 및 비디오 회의 소프트웨어를 Horizon 7에서 사용할 수 있습니다.

플래시 URL 리디렉션

Adobe Media Server에서 클라이언트 끝점으로 플래시 콘텐츠를 직접 스트리밍하면 데이터 센터 ESXi 호스트에 대한 부하를 줄이고, 데이터 센터를 통해 추가 라우팅을 제거하고, 여러 클라이언트 끝점에 라이브 비디오 이벤트를 동시에 스트리밍하는 데 필요한 대역폭을 줄여줍니다.

플래시 URL 리디렉션 기능은 웹 페이지 관리자에 의해 웹 페이지 내에 포함된 JavaScript를 사용합니다. 가상 데스크톱 사용자가 웹 페이지 내에서 지정된 URL 링크를 클릭할 때마다 JavaScript는 가상 데스크톱 세션에서 클라이언트 끝점으로 ShockWave 파일(SWF)을 가로채서 리디렉션합니다. 그런 다음 끝점은 가상 데스크톱 세션 외부에서 로컬 VMware Flash Projector를 열고 로컬로 미디어 스트림을 재생합니다.

참고 플래시 URL 리디렉션을 사용하면 멀티캐스트 또는 유니캐스트 스트림이 조직의 방화벽 외부에 있을 수 있는 클라이언트 디바이스에 리디렉션됩니다. 클라이언트가 멀티캐스트 또는 유니캐스트 스트림을 시작하는 ShockWave Flash(SWF) 파일을 호스팅하는 Adobe Web 서버에 액세스할 수 있어야 합니다. 필요할 경우, 해당 포트를 열 수 있도록 방화벽을 구성하여 클라이언트 디바이스가 이 서버에 액세스할 수 있게 허용합니다.

이 기능은 일부 유형의 클라이언트에서만 지원됩니다. 특정 유형의 클라이언트에서 이 기능이 지원되는지 여부를 확인하려면, “VMware Horizon Client 사용” 문서에 포함된 기능 지원 매트릭스를 참조하여 지원되는 특정 유형의 데스크톱 또는 모바일 클라이언트 디바이스를 확인하십시오. 자세한 사항은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>의 내용을 참조하십시오.

Microsoft Lync 2013

원격 데스크톱에서 Microsoft Lync 2013 클라이언트를 사용하여 Lync 인증 USB 오디오 및 비디오 디바이스로 비디오 채팅 호출 및 UC(Unified Communications) VoIP에 참여할 수 있습니다. 더 이상 전용 IP 휴대 전화가 필요하지 않습니다.

이 아키텍처를 사용하려면 원격 데스크톱에 Microsoft Lync 2013 클라이언트를 설치하고 Windows 7 또는 8 클라이언트 끝점에 Microsoft Lync VDI 플러그인을 설치해야 합니다. 고객은 상태, 인스턴트 메시징, 웹 회의 및 Microsoft Office 기능에 Microsoft Lync 2013을 사용할 수 있습니다.

Lync VoIP 또는 비디오 채팅 호출이 발생할 때마다 Lync VDI 플러그인은 데이터 센터 서버에서 클라이언트 끝점으로 모든 미디어 처리를 오프로드하고 Lync 최적 오디오 및 비디오 코덱으로 모든 미디어를 인코딩합니다. 이 최적화된 아키텍처는 고도로 확장 가능하며 네트워크 대역폭 사용을 낮추고 고품질 실시간 VoIP 및 비디오 지원으로 지점간 미디어 전달을 제공합니다. 자세한 내용은

<http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf>에서 VMware Horizon 6 및 Microsoft Lync 2013에 대한 백서를 참조하십시오.

참고 오디오 기록은 아직 지원되지 않습니다. 이 통합에는 PCoIP 또는 Blast Extreme 디스플레이 프로토콜만 지원됩니다.

비즈니스용 Skype

최종 사용자는 비즈니스용 Skype를 사용하여 가상 인프라에 부정적인 영향을 주거나 네트워크에 과부하를 주지 않고도 가상 데스크톱 내에서 최적화된 음성 및 영상 통화를 할 수 있습니다. Skype 음성 및 영상 통화 동안 모든 미디어 처리는 가상 데스크톱 대신 클라이언트 시스템에서 수행됩니다.

비즈니스용 Skype의 가상화 팩 소프트웨어는 기본적으로 Windows용 Horizon Client(4.6 이상), Linux용 Horizon Client(4.6 이상) 및 Mac용 Horizon Client(4.7 이상) 설치 관리자의 일부로 설치됩니다. 또한 Horizon 관리자는 Horizon Agent 설치 중에 가상 데스크톱에 비

즈니스용 Skype에 대한 VMware 가상화 팩 기능을 설치해야 합니다. 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 문서를 참조하십시오. 비즈니스용 Skype를 구성하려면 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

Horizon 7 에 비즈니스 인텔리전스 소프트웨어 통합

Microsoft SQL Server 또는 Oracle 데이터베이스에 이벤트를 기록하도록 Horizon 연결 서버를 구성할 수 있습니다.

- 데스크톱 세션 시작 및 로그인과 같은 최종 사용자 작업
- 권한 부여 추가 및 데스크톱 풀 생성과 같은 관리자 작업.
- 시스템 장애 및 오류를 보고하는 경고.
- 24시간 동안 최대 사용자 수 기록과 같은 통계 샘플링.

Crystal Reports, IBM Cognos, MicroStrategy 9, Oracle Enterprise Performance Management System과 같은 비즈니스 인텔리전스 보고 엔진을 사용해 이벤트 데이터베이스에 액세스하고 분석할 수 있습니다.

자세한 내용은 Horizon 7 통합 문서를 참조하십시오.

분석 소프트웨어에서 이벤트 데이터에 액세스할 수 있도록 Syslog 형식으로 Horizon 7 이벤트를 생성할 수 있습니다. 파일 기반 이벤트 로깅을 사용하도록 설정하면 이벤트가 로컬 로그 파일에 누적됩니다. 파일 공유를 지정하면 이러한 로그 파일이 해당 공유로 이동합니다. 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.

Horizon PowerCLI cmdlet을 사용한 관리 스크립트 생성

VMware PowerCLI에서 Horizon PowerCLI cmdlet을 사용할 수 있습니다. Horizon PowerCLI cmdlet을 사용하여 Horizon 구성 요소에 대해 다양한 관리 작업을 수행할 수 있습니다.

Horizon PowerCLI cmdlet에 대한 자세한 내용은 VMware PowerCLI Cmdlet 참조를 읽어보시기 바랍니다.

Horizon PowerCLI와 함께 사용할 고급 기능 및 스크립트를 생성하기 위한 API 사양에 대한 자세한 내용은 [VMware 개발자 센터](#)에서 View API 참조를 확인하십시오.

자체 Horizon PowerCLI 스크립트를 생성하는 데 사용할 수 있는 샘플 스크립트에 대한 자세한 내용은 [GitHub의 Horizon PowerCLI 커뮤니티](#)를 확인하십시오.

Horizon PowerCLI cmdlet을 사용해 Horizon 7 구성 요소에서 다양한 관리 작업을 수행할 수 있습니다.

- 데스크톱 풀을 생성하고 및 업데이트합니다.
- 여러 네트워크 레이블을 구성하여 풀의 가상 시스템에 할당할 수 있는 IP 주소의 수를 크게 늘릴 수 있습니다.
- 전체 가상 시스템 또는 연결된 클론 풀에 데이터 센터 리소스를 추가합니다.

- 연결된 클론 데스크톱에 재조정, 새로 고침, 재구성 작업을 수행합니다.
- 특정 데스크톱 또는 데스크톱 풀의 점진적 사용량 표본을 조사합니다.
- 이벤트 데이터베이스를 쿼리합니다.
- 서비스 상태를 쿼리합니다.

Horizon 7 의 LDAP 구성 데이터 수정

Horizon Administrator를 사용해 Horizon 7 구성을 수정하는 경우에는 저장소의 해당 LDAP 데이터가 업데이트됩니다. Horizon 연결 서버는 LDAP 호환 저장소에 구성 정보를 저장합니다. 예를 들어 데스크톱 풀을 추가하면 연결 서버는 사용자, 사용자 그룹, 권한 정보를 LDAP에 저장합니다.

VMware와 Microsoft 명령줄 도구를 사용하여 LDIF(LDAP Data Interchange Format) 파일의 LDAP 구성 데이터를 Horizon 7에서 내보내거나 가져올 수 있습니다. 이들 명령은 Horizon Administrator 또는 Horizon PowerCLI를 사용하지 않고 스크립트를 사용해 구성 데이터를 업데이트하려는 고급 관리자용입니다.

LDIF 파일을 사용해 다양한 작업을 수행할 수 있습니다.

- 연결 서버 인스턴스 간 구성 데이터를 전송합니다.
- 데스크톱 풀과 같은 다수의 Horizon 7 개체를 정의하고 Horizon Administrator 또는 Horizon PowerCLI를 사용하지 않은 채 연결 서버 인스턴스에 이들 개체를 추가합니다.
- 연결 서버 인스턴스 상태를 복원할 수 있도록 구성을 백업합니다.

자세한 내용은 Horizon 7 통합 문서를 참조하십시오.

vdmadmin 명령 사용

vdmadmin 명령줄 인터페이스를 사용해 연결 서버 인스턴스에서 다양한 관리 작업을 수행할 수 있습니다. vdmadmin을 사용해 Horizon Administrator 사용자 인터페이스에서 실행할 수 없거나 스크립트에서 자동으로 실행해야 하는 관리 작업을 수행할 수 있습니다.

자세한 내용은 Horizon 7 관리 문서를 참조하십시오.

풍부한 사용자 환경 계획

Horizon 7은 최종 사용자가 기대하는 친숙하고 개인화된 데스크톱 환경을 제공합니다. 예를 들어, 몇몇 클라이언트 시스템에서 최종 사용자는 로컬 컴퓨터에 연결된 USB 및 다른 디바이스에 액세스하고 로컬 컴퓨터에서 감지할 수 있는 임의의 프린터에 문서를 전송하고 스마트 카드로 인증하며 다중 디스플레이 모니터를 사용할 수 있습니다.

Horizon 7에는 최종 사용자에게 제공할 수 있는 다양한 기능이 포함되어 있습니다. 사용할 기능을 결정하기 전에 각 기능의 제한 사항을 확인해야 합니다.

본 장은 다음 항목을 포함합니다.

- Horizon Agent용 기능 지원 표
- 디스플레이 프로토콜 선택
- 게시된 애플리케이션 사용
- Horizon Persona Management를 사용하여 사용자 데이터 및 설정 유지
- 원격 데스크톱 및 애플리케이션에서 USB 디바이스 사용
- 웹캠 및 마이크에 대한 실시간 오디오-비디오 기능 사용
- 3D 그래픽 애플리케이션 사용
- 원격 데스크톱에 멀티미디어 스트리밍
- 원격 데스크톱에서 인쇄
- 로그인에 Single Sign-On 사용
- 모니터 및 화면 해상도

Horizon Agent 용 기능 지원 표

최종 사용자에게 제공할 디스플레이 프로토콜 및 기능을 계획하는 경우 다음 정보를 참조하여 해당 기능을 지원하는 에이전트(원격 데스크톱 및 애플리케이션) 운영 체제를 결정합니다.

지원되는 게스트 운영 체제의 유형 및 버전은 Windows 버전에 따라 다릅니다. 지원되는 Windows 10 운영 체제 목록 업데이트를 보려면 VMware KB(기술 자료) 문서

<http://kb.vmware.com/kb/2149393>을 참조하십시오. Windows 10 이외의 Windows 운영 체제의 경우 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2150295>를 참조하십시오.

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

참고 다양한 유형의 클라이언트 디바이스에서 지원되는 기능에 대한 자세한 내용은 Horizon Client 설명서(<https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>)를 참조하십시오.

또한 다수의 VMware 파트너가 Horizon 7 배포에 썬 및 제로 클라이언트 디바이스를 제공합니다. 벤더, 모델 및 기업에서 사용하기로 선택하는 구성에 따라 각 썬 또는 제로 클라이언트 디바이스에서 사용할 수 있는 기능이 결정됩니다. 썬 클라이언트 및 제로 클라이언트 디바이스의 모델 및 공급업체에 대한 자세한 내용은 VMware 웹 사이트에서 [VMware 호환성 가이드](#)를 참조하십시오.

디스플레이 프로토콜 선택

디스플레이 프로토콜은 최종 사용자에게 데이터 센터에 있는 원격 데스크톱 또는 애플리케이션에 대한 그래픽 인터페이스를 제공합니다. 어떠한 유형의 클라이언트 디바이스를 보유하고 있는지에 따라 VMware에서 제공하는 Blast Extreme 및 PCoIP(PC-over-IP)나 Microsoft RDP(Remote Desktop Protocol)를 선택할 수 있습니다.

사용할 프로토콜을 제어하거나 사용자가 데스크톱 로그인 시 프로토콜을 선택하도록 정책을 설정할 수 있습니다.

참고 몇몇 클라이언트 유형의 경우, PCoIP나 RDP 원격 디바이스 프로토콜 중 어떠한 것도 사용되지 않습니다. 예를 들어 HTML Access 기능을 사용할 수 있는 HTML Access 클라이언트를 사용할 경우 PCoIP 또는 RDP가 아닌 Blast Extreme 프로토콜이 사용됩니다. 마찬가지로, 원격 Linux 데스크톱을 사용하는 경우에는 Blast Extreme이 사용됩니다.

VMware Blast Extreme

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

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

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

VMware Blast Extreme 기능

VMware Blast Extreme의 주요 기능에는 다음 내용이 포함됩니다.

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

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

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

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

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



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

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

Wake-on-LAN

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

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

- 연결 서버와 Horizon Agent간의 모든 라우터는 구성됩니다. 이를 통해 잠금 해제하려는 물리적 시스템의 대상 서버넷에 대해 IP 전달 브로드캐스트 패킷을 허용합니다.

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

권장된 게스트 운영 체제 설정

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

비디오 품질 요구 사항

480p 형식 비디오

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

720p 형식 비디오

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

1080p 형식 비디오

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

3D 렌더링

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

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

3D 기능에 대한 자세한 내용은 [3D 그래픽 애플리케이션 사용](#)을 참조하십시오.

클라이언트 시스템의 하드웨어 요구 사항

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

PCoIP

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

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

PCoIP 기능

PCoIP의 키 기능에는 다음 내용이 포함됩니다.

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

특정 PCoIP 기능을 지원하는 데스크톱 운영 체제 유형에 대한 정보는 [Horizon Agent용 기능 지원 표](#)를 참조하십시오.

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

권장된 게스트 운영 체제 설정

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

비디오 품질 요구 사항

480p 형식 비디오

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

720p 형식 비디오

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

1080p 형식 비디오

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

3D 렌더링

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

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

3D 기능에 대한 자세한 내용은 [3D 그래픽 애플리케이션 사용](#)을 참조하십시오.

클라이언트 시스템의 하드웨어 요구 사항

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

Microsoft RDP

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

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

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

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

클라이언트 시스템의 하드웨어 요구 사항

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

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

게시된 애플리케이션 사용

Horizon Client를 사용하여 Windows 기반 게시된 애플리케이션 및 원격 데스크톱에 안전하게 액세스할 수 있습니다.

이 기능을 사용하면 사용자가 Horizon Client를 실행하고 Horizon 7 Server에 로그인한 후 사용 권한이 부여된 모든 게시된 애플리케이션과 원격 데스크톱이 표시됩니다. 애플리케이션을 선택하면 로컬 클라이언트 디바이스에 있는 해당 애플리케이션의 창이 열리며, 이 애플리케이션은 로컬에 설치된 것처럼 표시되고 작동합니다.

예를 들어 Windows 클라이언트 컴퓨터에서 애플리케이션 창을 최소화하면 이 애플리케이션 항목이 작업 표시줄에 유지되고 로컬 Windows 컴퓨터에 설치되었을 때와 동일한 방식으로 표시됩니다. 또한 클라이언트 데스크톱에 표시되는 애플리케이션 바로 가기를 로컬에 설치된 애플리케이션 바로 가기와 똑같이 만들 수도 있습니다.

다음과 같은 경우 완전한 원격 데스크톱을 배포하는 것보다 이러한 방식으로 게시된 애플리케이션을 배포하는 것이 더 적절할 수 있습니다.

- 애플리케이션이 다중 계층 아키텍처로 설정되어 있어 각 구성 요소가 지리적으로 서로 근접한 위치에 있어야 더 잘 작동하는 경우 게시된 애플리케이션을 사용하는 것이 좋습니다.

예를 들어 사용자가 원격으로 데이터베이스에 액세스해야 할 때 WAN을 통해 대량의 데이터를 전송해야 하는 경우 일반적으로 성능이 영향을 받게 됩니다. 게시된 애플리케이션을 사용하면 애플리케이션의 모든 요소가 데이터베이스와 동일한 데이터 센터에 있을 수 있으므로 트래픽이 격리되고 화면 업데이트만 WAN을 통해 전송됩니다.

- 모바일 디바이스의 경우 개별 애플리케이션에 액세스하는 것이 원격 Windows 데스크톱을 연 후 해당 애플리케이션으로 이동하는 것보다 간단합니다.

이 기능을 사용하려면 애플리케이션을 Microsoft RDS 호스트에 설치합니다. 이런 점에서, Horizon 7 게시된 애플리케이션은 다른 애플리케이션 원격 솔루션과 비슷하게 작동합니다. Horizon 7 게시된 애플리케이션은 최적화된 사용자 경험을 위해 Blast Extreme 디스플레이 프로토콜이나 PCoIP 디스플레이 프로토콜을 사용하여 전달됩니다.

Horizon Persona Management를 사용하여 사용자 데이터 및 설정 유지

원격 데스크톱과 Horizon 7으로 관리되지 않는 가상 시스템 및 물리적 컴퓨터에서 Horizon Persona Management를 사용할 수 있습니다. 개인 설정 관리는 사용자가 해당 프로파일에 대해 수행한 변경 내용을 유지합니다. 사용자 프로파일은 다양한 사용자 생성 정보로 구성됩니다.

- 사용자가 로그인한 데스크톱과 관계 없이 데스크톱의 모습을 동일하게 유지해주는 사용자별 데이터 및 데스크톱 설정.
- 애플리케이션 데이터 및 설정. 예를 들어 이러한 설정을 통해 애플리케이션이 도구 모음 위치 및 기본 설정을 기억할 수 있습니다.
- 사용자 애플리케이션으로 구성된 Windows 레지스트리 항목.

이러한 기능을 활용하려면, 개인 설정 관리에서 사용자 로컬 프로파일의 크기보다 크거나 동일한 CIFS 공유 스토리지가 필요합니다.

로그온 및 로그오프 시간 최소화

개인 설정 관리는 데스크톱 로그인 및 로그오프 시간을 최소화합니다. 로그인 시 Horizon 7는 기본적으로 사용자 레지스트리 파일 등 Windows에 필요한 파일만 다운로드합니다. Horizon 7는 정해진 주기마다 원격 데스크톱의 프로파일에 최근 변경 내용을 가져와 원격 저장소에 복사합니다.

개인 설정 관리를 사용하면, 관리되는 프로파일을 만들기 위해 Active Directory를 변경하지 않아도 됩니다. 개인 설정 관리를 구성하려면, Active Directory에서 사용자 속성을 변경하지 않고 중앙 저장소를 지정하십시오. 이 중앙 저장소를 사용하면 사용자가 로그인할 수 있는 물리적 시스템에 영향을 주지 않고 특정 환경에서 사용자 프로파일을 관리할 수 있습니다.

개인 설정 관리에서, VMware ThinApp 애플리케이션을 사용하여 데스크톱을 프로비저닝할 경우, ThinApp 샌드박스 데이터도 사용자 프로파일에 저장될 수 있습니다. 이 데이터는 사용자와 함께 로밍될 수 있지만 로그인 시간에는 크게 영향을 주지 않습니다. 이 전략은 데이터 손실 또는 손실에 대한 적절한 보호를 제공합니다.

구성 옵션

배포 시 단일 원격 데스크톱, 데스크톱 풀, OU 또는 모든 원격 데스크톱과 같은 여러 수준으로 Horizon 7 개인 설정을 구성할 수 있습니다. 또한 Horizon 7으로 관리되지 않는 가상 시스템 및 물리적 컴퓨터에서 개인 설정 관리의 독립 실행형 버전을 사용할 수 있습니다.

그룹 정책(GPO)을 설정하여 개인 설정에 포함할 파일 및 폴더를 개별적으로 제어할 수 있습니다. 로컬 설정 폴더의 포함 여부, 로그인할 때 로드할 파일, 사용자가 로그인한 후에 배경에서 다운로드할 파일, 사용자의 개인 설정에서 개인 설정 관리 대신 Windows 로밍 프로파일 기능으로 관리할 파일을 지정할 수 있습니다.

Windows 로밍 프로파일처럼 폴더 리디렉션을 구성할 수 있습니다. 다음 폴더를 네트워크 공유로 리디렉션할 수 있습니다.

연락처	내 문서	Save Games
쿠키	내 음악	검색
데스크톱	내 그림	시작 메뉴
다운로드	내 비디오	시작 항목
즐거찾기	네트워크 환경	Templates
History	Printer Neighborhood	Temporary Internet Files
Links	최근 문서	

제한 사항

개인 설정 관리는 다음과 같은 제한 사항이 있습니다.

- 인스턴트 클론 데스크톱 풀에서는 이 기능이 지원되지 않습니다.
- Persona Management 구성 요소를 포함하는 Horizon 7 라이선스를 보유하고 있어야 합니다.
- 개인 설정 관리를 위해 CIFS(Common Internet File System) 공유가 필요합니다.

- 이 기능을 Windows 10 연결된 클론 데스크톱 풀의 영구 디스크에는 사용할 수 없습니다.

원격 데스크톱 및 애플리케이션에서 USB 디바이스 사용

관리자는 가상 데스크톱에서 썸 플래시 드라이브, 카메라, VoIP(Voice-over-IP) 디바이스, 프린터와 같은 USB 디바이스를 사용하는 기능을 구성할 수 있습니다. 이 기능을 USB 리디렉션이라 부릅니다. 가상 데스크톱 하나에서 최대 128개의 USB 디바이스를 수용할 수 있습니다.

게시된 데스크톱 및 애플리케이션에서 사용하도록 로컬로 연결된 특정 USB 디바이스를 리디렉션할 수도 있습니다. 지원되는 특정 유형의 디바이스에 대한 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

단일 사용자 시스템에 배포된 데스크톱 풀에서 이 기능을 사용하면 로컬 클라이언트 시스템에 연결된 대부분의 USB 디바이스를 원격 데스크톱에서 사용할 수 있습니다. 원격 데스크톱에서 iPad에 연결하여 이 디바이스를 관리할 수도 있습니다. 예를 들어 원격 데스크톱에 설치된 iTunes와 iPad를 동기화할 수 있습니다. Windows 및 Mac 컴퓨터 같은 일부 클라이언트 디바이스에서는 USB 디바이스가 Horizon Client의 메뉴에 나열됩니다. 디바이스를 연결 및 연결 해제하는 메뉴를 사용합니다.

대부분의 경우 USB 디바이스를 클라이언트 시스템과 원격 데스크톱에서 동시에 사용할 수 없습니다. 일부 유형의 USB 디바이스만 원격 데스크톱과 로컬 컴퓨터 간에 공유할 수 있습니다. 이러한 디바이스에는 스마트 카드 판독기와 키보드 및 포인팅 디바이스 같은 휴먼 인터페이스 디바이스가 포함됩니다.

관리자는 최종 사용자가 연결할 수 있는 USB 디바이스의 유형을 지정할 수 있습니다. 비디오 입력 디바이스 및 스토리지 디바이스와 같은 여러 디바이스 유형을 포함하는 복합 디바이스의 경우 관리자는 일부 클라이언트 시스템에서 하나의 디바이스(예: 비디오 입력 디바이스)는 허용되지만 다른 디바이스(예: 스토리지 디바이스)는 허용되지 않도록 디바이스를 분할할 수 있습니다.

USB 리디렉션 기능은 특정 유형의 클라이언트에서만 사용할 수 있습니다. 특정 클라이언트에서 이 기능이 지원되는지 여부를 확인하려면 해당 클라이언트에 대한 Horizon Client 설치 및 설정 문서에 포함된 기능 지원 표를 참조하십시오.

웹캠 및 마이크에 대한 실시간 오디오-비디오 기능 사용

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

최종 사용자가 자신의 원격 데스크톱에서 Skype, Webex, Google Hangouts 및 기타 온라인 회의 애플리케이션을 실행할 수 있습니다. 이 기능은 USB 리디렉션을 사용할 경우 얻을 수 있는 대역폭에 비해 적은 대역폭을 사용하여 비디오 및 오디오 데이터를 에이전트 시스템으로 리디렉션합니다. 실시간 오디오-비디오를 사용하면 웹캠 이미지 및 오디오 입력이 클라이언트 시스템에서 인코딩된 다음, 에이전트 시스템에 전송됩니다. 에이전트 시스템에서 가상 웹캠 및 가상 마이크는 타사 애플리케이션에서 사용할 수 있도록 스트림을 디코딩하고 재생할 수 있습니다.

특별한 구성이 필요하지는 않지만, 관리자는 에이전트 측 그룹 정책 및 레지스트리 키를 설정하여 프레임 속도 및 이미지 해상도를 구성하거나 기능을 해제할 수 있습니다. 기본적으로 해상도는 초당 15프레임에서 320 x 240픽셀입니다. 필요한 경우 관리자는 클라이언트 측 구성 설정을 사용하여 기본 웹캠 또는 오디오 디바이스를 설정할 수도 있습니다.

참고 이 기능은 일부 유형의 클라이언트에서만 지원됩니다. 특정 유형의 클라이언트에서 이 기능이 지원되는지 여부를 확인하려면, 설치 및 설정 문서에 포함된 기능 지원 매트릭스를 참조하여 특정 유형의 데스크톱 또는 모바일 클라이언트 디바이스를 확인하십시오.

3D 그래픽 애플리케이션 사용

Blast Extreme 또는 PCoIP 디스플레이 프로토콜에서 제공되는 소프트웨어 및 하드웨어 가속 그래픽 기능을 통해 원격 데스크톱 사용자는 Google Earth와 CAD는 물론 기타 그래픽 위주의 애플리케이션까지 포함하여 광범위한 3D 애플리케이션을 실행할 수 있습니다.

NVIDIA GRID vGPU(공유 GPU 하드웨어 가속화)

vSphere 6.0 이상에서 제공되는 이 기능을 통해 가상 시스템에서 ESXi 호스트의 물리적 GPU(그래픽 처리 장치)를 공유할 수 있습니다. 고급 하드웨어 가속 워크스테이션 그래픽이 필요할 경우 이 기능을 사용합니다.

vDGA를 사용하는 AMD Multiuser GPU

vSphere 6.0 이상에서 사용할 수 있는 이 기능을 통해 GPU가 여러 개의 PCI 패스스루 디바이스로 표시되게 하고 여러 개의 가상 시스템에서 AMD GPU를 공유할 수 있습니다. 이 기능은 경량급 3D 작업자부터 최첨단 워크스테이션 그래픽 고급 사용자에게 이르기까지 유연한 하드웨어 가속 3D 프로파일을 제공합니다.

vDGA(Virtual Dedicated Graphics Acceleration)

vSphere 5.5 업데이트 2 이상에서 제공되는 이 기능은 ESXi 호스트의 단일 물리적 GPU를 단일 가상 시스템 전용으로 지정합니다. 고급 하드웨어 가속 워크스테이션 그래픽이 필요할 경우 이 기능을 사용합니다.

참고 일부 Intel vDGA 카드에는 특정 vSphere 6 버전이 필요합니다.

<http://www.vmware.com/resources/compatibility/search.php>에서 VMware 하드웨어 호환성 목록을 참조하십시오. 또한 Intel vDGA의 경우 다른 벤더에서와 마찬가지로 개별 GPU보다는 Intel 통합 GPU를 사용합니다.

vSGA(가상 공유 그래픽 가속화)

vSphere 5.5 업데이트 2 이상에서 제공되는 이 기능을 통해 여러 가상 시스템에서 ESXi 호스트의 물리적 GPU를 공유할 수 있습니다. 또한 설계, 모델링 및 멀티미디어에 3D 애플리케이션을 활용할 수 있습니다.

Soft 3D

vSphere 5.5 업데이트 2 이상에서 제공되는 소프트웨어 가속 그래픽 기능을 통해 물리적 GPU를 사용하지 않고 DirectX 9 및 OpenGL 2.1 애플리케이션을 실행할 수 있습니다. Windows Aero 테마, Microsoft Office 2010 및 Google Earth와 같은 덜 까다로운 3D 애플리케이션에 이 기능을 사용합니다.

NVIDIA GRID vGPU 및 vDGA도 Microsoft RDS 호스트에서 실행되는 게시된 애플리케이션에서 지원됩니다.

중요 3D 렌더링을 위한 다양한 선택과 요구 사항에 대한 자세한 내용은 그래픽 가속에 관한 [VMware 백서](#), [VMware Horizon 6.1용 NVIDIA GRID vGPU 배포 가이드](#) 및 [NVIDIA GRID 가상 GPU 사용자 가이드](#)를 참조하십시오.

원격 데스크톱에 멀티미디어 스트리밍

Windows 7 및 Windows 8/8.1 데스크톱 및 클라이언트를 위한 Windows Media MMR(멀티미디어 리디렉션) 기능은 멀티미디어 파일이 원격 데스크톱으로 스트리밍될 때 Windows 클라이언트 컴퓨터에서 고화질 재생을 지원합니다.

MMR을 사용하면 멀티미디어 스트림이 처리됩니다. 즉, Windows 클라이언트 시스템에서 디코딩됩니다. 클라이언트 시스템은 미디어 콘텐츠를 재생하여 ESXi 호스트에 대한 요청 부담을 덜어줍니다. Windows Media Player에서 지원되는 미디어 형식이 지원됩니다(예: M4V, MOV, MP4, WMP, MPEG-4 Part 2, WMV 7, 8 및 9, WMA, AVI, ACE, MP3, WAV).

참고 방화벽 소프트웨어에 예외적으로 MMR 포트를 추가해야 합니다. MMR의 기본 포트는 9427입니다.

원격 데스크톱에서 인쇄

가상 인쇄 기능을 사용하면 일부 클라이언트 시스템의 최종 사용자가 추가 인쇄 드라이버를 원격 데스크톱 운영 체제에 설치할 필요 없이 원격 데스크톱에서 로컬 또는 네트워크 프린터를 사용할 수 있습니다. 위치 기반 인쇄 기능을 사용하여 끝점 클라이언트 디바이스에서 가장 가까운 프린터에 원격 데스크톱을 매핑할 수 있습니다.

가상 인쇄를 사용할 경우 프린터가 로컬 클라이언트 컴퓨터에 추가되면 원격 데스크톱에서 사용할 수 있는 프린터 목록에 해당 프린터가 자동으로 추가됩니다. 추가 구성은 필요하지 않습니다. 이 기능을 통해 사용할 수 있는 각 프린터의 경우 데이터 압축, 인쇄 품질, 양면 인쇄, 색상 등의 환경을 설정할 수 있습니다. 관리자 권한을 가진 사용자는 가상 인쇄 구성 요소와의 충돌 없이 원격 데스크톱에 프린터 드라이버를 계속 설치할 수 있습니다.

로컬 프린터 리디렉션은 다음과 같은 사용 사례에 맞게 고안되었습니다.

- 클라이언트 디바이스의 USB 또는 직렬 포트에 직접 연결된 프린터
- 클라이언트에 연결된 바코드 프린터 및 레이블 프린터와 같은 특수 프린터
- 가상 세션에서 주소를 지정할 수 없는 원격 네트워크의 네트워크 프린터

USB 프린터로 인쇄 작업을 보내려면 USB 리디렉션 기능을 사용하거나 가상 인쇄 기능을 사용할 수 있습니다.

위치 기반 인쇄 기능을 사용하여 IT 조직은 끝점 클라이언트 디바이스에서 가장 가까운 프린터에 원격 데스크톱을 매핑할 수 있습니다. 예를 들어 의사는 병실 사이를 이동하기 때문에 의사가 문서를 인쇄할 때마다 가장 가까운 프린터로 인쇄 작업이 전송됩니다. 이 기능을 사용하려면 올바른 프린터 드라이버가 원격 데스크톱에 설치되어 있어야 합니다.

참고 이와 같은 인쇄 기능은 일부 유형의 클라이언트에서만 사용할 수 있습니다. 특정 유형의 클라이언트에서 인쇄 기능이 지원되는지 여부를 확인하려면, 설치 및 설정 가이드에 포함된 기능 지원 매트릭스를 참조하여 특정 유형의 데스크톱 또는 모바일 클라이언트 디바이스를 확인하십시오.

<https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>로 이동하십시오.

로그인에 Single Sign-On 사용

SSO(Single Sign-On) 기능을 통해 최종 사용자는 Active Directory 로그인 자격 증명을 한 번만 제공하면 됩니다.

단일 로그인 기능을 사용하지 않을 경우 최종 사용자는 두 번 로그인해야 합니다. Active Directory 자격 증명을 입력하여 Horizon 연결 서버에 로그인하라는 메시지가 먼저 표시된 다음 원격 데스크톱에 로그인하라는 메시지가 표시됩니다. 또한 스마트 카드를 사용할 경우 스마트 카드 판독기에서 PIN에 대해 메시지를 표시할 때 사용자가 또 로그인해야 하기 때문에 최종 사용자는 세 번 로그인해야 합니다.

원격 데스크톱의 경우 이 기능에는 자격 증명 공급자 동적 링크 라이브러리가 포함되어 있습니다.

True SSO

True SSO 기능을 사용하는 경우 더 이상 Active Directory 자격 증명을 제공할 필요가 없습니다. 사용자가 RSA SecurID 또는 RADIUS 인증과 같은 AD 외의 방법을 사용하여 VMware Identity Manager에 로그인한 후에 사용자가 원격 데스크톱이나 애플리케이션을 사용하기 위해 Active Directory 자격 증명을 입력할 필요도 없습니다.

사용자가 스마트 카드나 Active Directory 자격 증명을 사용하여 인증된 경우에는 True SSO 기능이 필요 없지만 이런 경우에도 True SSO를 사용하도록 구성할 수 있습니다. 그러면 사용자가 제공하는 AD 자격 증명이 무시되고 True SSO가 사용됩니다.

True SSO는 Windows 로그인 프로세스에 수명이 짧고 고유한 인증서를 생성하는 방식으로 작동합니다. 사용자를 대신해서 수명이 짧은 인증서를 생성하려면, CA(인증 기관)를 설정하고(아직 없는 경우) 인증서 등록 서버를 설정해야 합니다. 연결 서버 설치 관리자를 실행하고 등록 서버 옵션을 선택하여 등록 서버를 설치합니다.

True SSO는 인증(사용자의 ID 검증)과 액세스(Windows 데스크톱 또는 애플리케이션 등에 대한)를 분리합니다. 사용자 자격 증명은 디지털 인증서를 사용하여 보호됩니다. 암호는 데이터 센터에서 보관되거나 전송되지 않습니다. 자세한 내용은 Horizon 7 관리 문서를 참조하십시오.

모니터 및 화면 해상도

원격 데스크톱을 여러 모니터로 확장할 수 있습니다. 고해상도 모니터가 있다면 원격 데스크톱 또는 애플리케이션을 전체 해상도로 볼 수 있습니다.

다중 모니터에 원격 데스크톱을 표시하려면 [모든 모니터] 디스플레이 모드를 선택할 수 있습니다. [모든 모니터] 모드를 사용하고 있을 때 [최소화] 버튼을 클릭한 다음 다시 창을 최대화하면 창이 [모든 모니터] 모드로 돌아갑니다. 마찬가지로 [전체 화면] 모드를 사용하고 있을 때 창을 최소화한 다음 다시 최대화하면 창이 단일 모니터의 [전체 화면] 모드로 돌아갑니다.

다중 모니터 설정에서 모든 모니터 사용

디스플레이 프로토콜과 관계없이 원격 데스크톱에서 다중 모니터를 사용할 수 있습니다.

Horizon Client가 모든 모니터를 사용하도록 지정한 경우 애플리케이션 창을 최대화하면 창이 해당 창을 포함하는 모니터의 전체 화면으로만 확장됩니다.

Horizon Client는 다음 모니터 구성을 지원합니다.

- 2대의 모니터를 사용할 경우, 모니터는 동일한 모드에 있지 않아도 됩니다. 예를 들어, 외부 모니터에 연결된 노트북을 사용할 경우, 외부 모니터는 세로 모드나 가로 모드여도 됩니다.
- 모니터 2대를 사용 중이고 전체 높이가 4096픽셀보다 작은 경우에만 모니터를 나란히 놓거나, 2x2로 쌓거나, 수직으로 쌓을 수 있습니다.
- 3D 렌더링 기능을 사용하려면 VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용해야 합니다. 모니터를 2대까지 사용할 수 있으며 최대 해상도는 1920x1200입니다. 해상도가 4K(3840 X 2160)인 경우 모니터 1대만 지원합니다.
- VMware Blast 디스플레이 프로토콜이나 PCoIP 디스플레이 프로토콜을 사용하면 4K(3840 x 2160)의 원격 데스크톱 화면 해상도가 지원됩니다. 지원되는 4K 디스플레이 수는 데스크톱 가상 시스템의 하드웨어 버전 및 Windows 버전에 따라 다릅니다.

하드웨어 버전	Windows 버전	지원되는 4K 디스플레이 수
10(ESXi 5.5.x 호환)	7, 8, 8.x, 10	1
11(ESXi 6.0 호환)	7 (3D 렌더링 기능 사용 안 함 및 Windows Aero 사용 안 함)	3
11	7 (3D 렌더링 기능 사용)	1
11	8, 8.x, 10	1
13 또는 14	8, 8.x, 10	3
13 또는 14	8, 8.x, 10 (3D 렌더링 기능 사용)	1

- Microsoft RDP 7을 사용하는 경우 원격 데스크톱을 표시하기 위해 사용할 수 있는 최대 모니터 수는 16대입니다.
- Microsoft RDP 디스플레이 프로토콜을 사용하는 경우 Microsoft RDC(Remote Desktop Connection) 6.0 이상이 원격 데스크톱에 설치되어 있어야 합니다.

다중 모니터 설정에서 단일 모니터 사용

여러 대의 모니터가 있으나 Horizon Client에서 하나의 모니터만 사용하도록 하려면 원격 데스크톱 창이 [모든 모니터] 이외의 모드에서 열리도록 하면 됩니다. 기본적으로 창은 기본 모니터에서 열립니다. 자세한 내용은 Windows용 VMware Horizon Client 설치 및 설정 가이드 문서를 참조하십시오.

고해상도 모드 사용

또한 클라이언트 유형에 따라서는 VMware Blast 디스플레이 프로토콜 또는 PCoIP 디스플레이 프로토콜을 사용할 경우 Horizon Client에서 고해상도 디스플레이가 있는 클라이언트 시스템에 고해상도를 지원합니다. 클라이언트 시스템에서 고해상도 디스플레이를 지원할 경우에만 [고해상도 모드] 옵션이 나타납니다.

가상 시스템에서 vGPU를 구성한 후에 기본적으로 하드웨어 인코딩이 사용되도록 설정됩니다. 지원되는 모든 다중 모니터 구성에서 하드웨어 인코딩이 사용되도록 설정되지만, 예외적으로 1GB보다 작은 비디오 메모리를 사용하는 vGPU 프로파일은 NVENC 메모리 제한으로 인해 소프트웨어 디코더를 사용합니다. <https://docs.nvidia.com/grid/4.3/grid-vgpu-release-notes-vmware-vmware/index.html>에서 NVENC에 1GB 이상의 프레임 버퍼 필요를 참조하십시오.

한 곳에서 데스크톱 및 애플리케이션 풀 관리

3

원격 데스크톱 한 대, 수백 대, 수천 대를 포함하는 풀을 생성할 수 있습니다. 가상 시스템, 물리적 시스템, Windows RDS(원격 데스크톱 서비스) 호스트를 데스크톱 소스로 사용할 수 있습니다. 가상 시스템 1대를 기본 이미지로 생성하면 Horizon 7에서 해당 이미지를 사용해 원격 데스크톱 풀을 생성할 수 있습니다. 또한 사용자에게 애플리케이션에 대한 원격 액세스를 제공하는 애플리케이션 풀을 생성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 데스크톱 풀의 장점
- 애플리케이션 풀의 장점
- 스토리지 요구 사항 축소 및 관리
- 애플리케이션 프로비저닝
- Active Directory GPO를 사용한 사용자 및 데스크톱 관리

데스크톱 풀의 장점

Horizon 7에서는 중앙 집중화된 관리의 기본 기능으로 데스크톱의 풀을 생성하고 프로비저닝할 수 있는 기능을 제공합니다.

다음 소스 중 하나에서 원격 데스크톱 풀을 생성합니다.

- 물리적 데스크톱 PC와 같은 물리적 시스템
- ESXi 호스트에서 호스팅되며 vCenter Server에 의해 관리되는 가상 시스템
- Horizon Agent를 지원하는 vCenter Server 이외의 가상화 플랫폼에서 실행되는 가상 시스템입니다.
- RDS 호스트의 세션 기반 데스크톱. RDS 호스트에서 데스크톱 풀 생성에 대한 자세한 내용은 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.

vSphere 가상 시스템을 데스크톱 소스로 사용하면 가상 데스크톱 생성 프로세스를 자동화하고, 동일한 가상 데스크톱을 원하는 대로 만들 수 있습니다. 풀에 대해 생성할 최소 및 최대 가상 데스크톱 수를 설정할 수 있습니다. 이들 매개 변수를 설정하면 리소스를 과도하게 사용할 정도는 아니지만 즉시 사용할 수 있는 원격 데스크톱을 항상 확보할 수 있습니다.

데스크톱을 관리하는 풀을 사용해 풀에 있는 모든 원격 데스크톱에 애플리케이션을 배포하거나 설정을 적용할 수 있습니다. 다음은 사용할 수 있는 설정의 일부 예입니다.

- 원격 데스크톱의 기본값으로 사용할 원격 디스플레이 프로토콜과 최종 사용자의 기본값 무시 허용 여부를 지정합니다.
- View Composer 연결된 클론 가상 시스템이나 전체 클론 가상 시스템의 경우, 사용하지 않는 동안 가상 시스템의 전원을 끌 것인지 아예 삭제할 것인지를 지정합니다. 인스턴트 클론 가상 시스템은 항상 전원이 켜져 있습니다.
- View Composer 연결된 클론 가상 시스템의 경우 Microsoft Sysprep 사용자 지정 규격과 VMware의 QuickPrep 중에 어느 것을 사용하는지 지정할 수 있습니다. Sysprep은 풀의 각 가상 시스템에 대해 고유한 SID 및 GUID를 생성합니다. 인스턴트 클론에는 VMware의 ClonePrep이라는 다른 사용자 지정 규격이 필요합니다.

풀에서 데스크톱에 사용자를 할당하는 방법을 지정할 수도 있습니다.

전용 할당 풀

특정 원격 데스크톱에 각 사용자를 할당하고 각 로그인 시 동일한 데스크톱으로 돌아갑니다. 전용 할당 풀에는 데스크톱과 사용자 사이의 일대일 관계가 필요합니다. 예를 들어, 데스크톱 100대로 이루어진 풀에는 사용자 100명으로 구성된 그룹이 필요합니다.

부동 할당 풀

부동 할당 풀을 사용하면 교대 근무 사용자들이 사용할 수 있는 데스크톱 풀을 생성할 수도 있습니다. 예를 들어 사용자가 한 번에 100명씩 교대 근무를 하는 경우, 사용자 300명이 데스크톱 100대로 구성된 풀을 사용할 수 있습니다. 엄격하게 통제된 환경을 제공하여 각자 사용 후 원격 데스크톱을 선택적으로 삭제하고 재생성할 수 있습니다.

애플리케이션 풀의 장점

애플리케이션 풀을 사용하면 개인용 컴퓨터 또는 디바이스가 아닌 데이터 센터의 서버에서 실행되는 애플리케이션에 대한 액세스 권한을 사용자에게 부여할 수 있습니다.

애플리케이션 풀은 다음과 같은 여러 가지 중요한 이점을 제공합니다.

■ 액세스 지원

사용자가 네트워크의 어느 위치에서든 애플리케이션에 액세스할 수 있습니다. 또한 보안 네트워크 액세스를 구성할 수도 있습니다.

■ 디바이스 독립성

애플리케이션 풀을 사용하면 스마트폰, 태블릿, 랩톱, 썬 클라이언트, 개인용 컴퓨터 같은 광범위한 클라이언트 디바이스를 지원할 수 있습니다. 클라이언트 디바이스에서 Windows, iOS, Mac OS, Android 등의 다양한 운영 체제를 실행할 수 있습니다.

■ 액세스 제어

한 명의 사용자 또는 사용자 그룹에 대해 쉽고 빠르게 애플리케이션 액세스 권한을 부여하거나 제거할 수 있습니다.

- 빠른 배포

애플리케이션 풀을 사용하면 애플리케이션을 데이터 센터의 서버에만 배포하고 각 서버가 여러 사용자를 지원할 수 있으므로 애플리케이션을 신속하게 배포할 수 있습니다.

- 관리 효율성

클라이언트 컴퓨터 및 디바이스에 배포된 소프트웨어를 관리하기 위해서는 대개 상당한 리소스가 필요합니다. 관리 작업에는 배포, 구성, 유지 관리, 지원 및 업그레이드가 포함됩니다. 애플리케이션 풀을 사용하면 소프트웨어가 데이터 센터의 서버에서 실행되어 필요한 소프트웨어 설치 사본 수가 줄어들기 때문에 기업에서 간편하게 소프트웨어를 관리할 수 있습니다.

- 보안 및 규정 준수

애플리케이션 풀을 사용하면 애플리케이션 및 관련 데이터가 중앙 집중식으로 데이터 센터에 위치하므로 보안을 강화할 수 있습니다. 데이터를 중앙 집중식으로 유지하면 보안 문제와 규정 준수 문제를 해결할 수 있습니다.

- 비용 절감

소프트웨어 라이선스 계약에 따라 데이터 센터에서 애플리케이션을 호스팅하는 것이 더 비용 효율적일 수 있습니다. 신속한 배포 및 관리 효율성 향상과 같은 기타 요인을 통해서도 기업 내 소프트웨어 비용을 줄일 수 있습니다.

스토리지 요구 사항 축소 및 관리

vCenter Server로 관리되는 가상 시스템에 데스크톱을 배포하면 이전에는 가상화된 서버에만 지원되었던 모든 스토리지 효율성이 제공됩니다. 인스턴트 클론이나 View Composer 연결된 클론을 데스크톱 시스템으로 사용하면 풀에 있는 모든 가상 시스템이 기본 이미지가 있는 가상 디스크를 공유하므로 스토리지가 절약됩니다.

- [vSphere로 스토리지 관리](#)

vSphere로 디스크 볼륨과 파일 시스템을 가상화하면 데이터가 물리적으로 저장되어 있는 위치를 고려할 필요 없이 스토리지를 관리하고 구성할 수 있습니다.

- [고성능 스토리지 및 정책 기반 관리에 VMware vSAN 사용](#)

VMware vSAN은 vSphere 5.5 업데이트 2 이상 릴리스에서 사용할 수 있는 소프트웨어 정의 스토리지 계층으로, vSphere 호스트의 클러스터에서 사용할 수 있는 로컬 물리적 스토리지 디스크를 가상화합니다. 자동화된 데스크톱 풀 또는 자동화된 팜을 생성할 때 하나의 데이터스토어만 지정하면 가상 시스템 파일, 복제본, 사용자 데이터 및 운영 체제 파일과 같은 다양한 구성 요소가 적절한 SSD(반도체 드라이브) 디스크 또는 직접 연결된 HDD(하드 디스크)에 배치됩니다.

- [가상 볼륨을 사용하여 가상 시스템 중심 스토리지 및 정책 기반 관리 지원](#)

vSphere 6.0 이상 릴리스에서 제공되는 VVol(가상 볼륨)에서는 데이터스토어가 아닌 개별 가상 시스템이 스토리지 관리 단위가 됩니다. 스토리지 하드웨어는 가상 디스크 콘텐츠, 레이어아웃 및 관리에 대한 제어 권한을 가집니다.

- View Composer로 스토리지 요구 사항 축소

View Composer는 기본 이미지와 가상 디스크를 공유하는 데스크톱 이미지를 생성하기 때문에 필요한 스토리지 용량을 50%에서 90%로 줄일 수 있습니다.

- 인스턴트 클론을 사용한 스토리지 요구 사항 감소

인스턴트 클론 기능에서는 vSphere vmFork 기술(vSphere 6.0U1 이상에서 사용 가능)을 활용하여 실행 중인 기본 이미지나 상위 가상 시스템을 중지하고 가상 데스크톱 풀을 빠르게 생성하고 사용자 지정합니다.

vSphere 로 스토리지 관리

vSphere로 디스크 볼륨과 파일 시스템을 가상화하면 데이터가 물리적으로 저장되어 있는 위치를 고려할 필요 없이 스토리지를 관리하고 구성할 수 있습니다.

Fibre Channel SAN 어레이, iSCSI SAN 어레이, NAS 어레이는 폭넓게 사용되는 스토리지 기술로 vSphere는 이들 기술을 지원해 다양한 데이터 센터 스토리지의 요건을 충족합니다.

SAN(Storage Area Network)을 통해 서버 그룹 간에 스토리지 어레이를 연결하고 공유합니다. 이러한 배열을 통해 스토리지 리소스를 집계하고 가상 시스템으로 이를 더욱 유연하게 프로비저닝할 수 있습니다.

호환되는 vSphere 5.5 업데이트 2 이상 기능

vSphere 5.5 업데이트 2 이상 릴리스에서는 vSAN을 사용할 수 있습니다. 이 기능은 여러 ESXi 호스트에서 사용 가능한 물리적 로컬 SSD(Solid State Disk)와 하드 디스크 드라이브를 클러스터의 모든 호스트에서 공유되는 단일 데이터스토어로 가상화합니다. vSAN은 정책 기반 관리와 함께 고가용성 스토리지를 제공하므로 데스크톱 풀을 생성할 때 하나의 데이터스토어만 지정하면 가상 시스템 파일, 복제본, 사용자 데이터 및 운영 체제 파일과 같은 다양한 구성 요소가 적절한 SSD(solid-state disk) 디스크 또는 직접 연결된 HDD(하드 디스크)에 배치됩니다.

또한 vSAN을 사용하면 스토리지 정책 프로파일을 통해 가상 시스템 스토리지 및 성능을 관리할 수 있습니다. 호스트, 디스크 또는 네트워크 오류나 워크로드 변경으로 인해 정책이 준수되지 않을 경우 vSAN은 영향을 받는 가상 시스템의 데이터를 다시 구성하고 클러스터에서 리소스 사용을 최적화합니다. 클러스터에 최대 20대의 ESXi 호스트를 포함하는 데스크톱 풀을 배포할 수 있습니다.

HA, vMotion 및 DRS와 같이 공유 스토리지가 필요한 VMware 기능을 지원하는 동시에 vSAN은 외부 공유 스토리지의 필요성을 제거하고 스토리지 구성 및 가상 시스템 프로비저닝 작업을 간소화합니다.

중요 vSphere 6.0 이상 릴리스에 제공되는 vSAN 기능에는 많은 성능 향상 기능이 포함되어 있습니다. 이 vSphere 6.0의 기능은 보다 광범위한 HCL(하드웨어 호환성)도 지원합니다. vSphere 6 이상의 vSAN에 대한 자세한 내용은 VMware vSAN 관리 문서를 참조하십시오.

참고 vSAN은 View Storage Accelerator 기능과는 호환되지만 디스크를 지우고 축소하여 디스크 공간을 회수하는 공간 효율적인 디스크 형식 기능과는 호환되지 않습니다.

vSphere 5.5 업데이트 2 이상 릴리스를 통해 다음 기능을 사용할 수 있습니다.

- View Storage Accelerator 기능이 있는 경우, 가상 시스템 디스크 데이터를 캐시하도록 ESXi 호스트를 구성할 수 있습니다.

동시에 많은 시스템이 시작되고 바이러스 백신 스캔을 실행할 때 이 CBRC(Content Based Read Cache)를 사용하면 부트 스톱이 발생하는 동안 IOPS를 줄여 성능을 높일 수 있습니다. 스토리지 시스템에서 전체 OS를 반복해서 읽는 대신, 호스트는 캐시에서 공통 데이터 블록을 읽을 수 있습니다.

- 원격 데스크톱이 vSphere 5.1 이상에서 제공되는 공간 효율적인 디스크 형식을 사용하는 경우 지우기 및 축소 프로세스를 통해 게스트 운영 체제 내의 오래되거나 삭제된 데이터가 자동으로 재사용됩니다.
- 복제 디스크는 VMFS5 이상의 데이터스토어나 NFS 데이터스토어에 저장되어야 합니다. 복제본을 VMFS5 이전의 VMFS 버전에 저장할 경우, 클러스터는 최대 8개의 호스트만을 가질 수 있습니다. OS 디스크와 영구 디스크는 NFS 또는 VMFS 데이터스토어에 저장할 수 있습니다.

호환되는 vSphere 6.0 이상 기능

vSphere 6.0 이상 릴리스를 통해 VVol(가상 볼륨)을 사용할 수 있습니다. 이 기능은 가상 디스크와 파생물, 클론, 스냅샷 및 복제본을 가상 볼륨이라고 하는 스토리지 시스템의 개체에 직접 매핑합니다. 이 매핑을 통해 vSphere가 스냅샷 생성 및 복제와 같은 중점 스토리지 작업을 스토리지 시스템으로 오프로드할 수 있습니다.

또한 가상 볼륨을 사용하면 vSphere의 스토리지 정책 프로필 통해 가상 시스템 스토리지 및 성능을 관리할 수 있습니다. 이러한 스토리지 정책 프로파일은 가상 시스템 단위의 스토리지 서비스를 요구합니다. 이러한 세분화된 프로비저닝 유형은 용량 사용률을 높입니다. 클러스터에 최대 32대의 ESXi 호스트를 포함하는 데스크톱 풀을 배포할 수 있습니다.

참고 가상 볼륨은 View Storage Accelerator 기능과는 호환되지만 디스크를 지우고 축소하여 디스크 공간을 회수하는 공간 효율적인 디스크 형식 기능과는 호환되지 않습니다.

참고 인스턴트 클론에서는 Virtual Volumes를 지원하지 않습니다.

고성능 스토리지 및 정책 기반 관리에 VMware vSAN 사용

VMware VMware vSAN은 vSphere 5.5 업데이트 2 이상 릴리스에서 사용할 수 있는 소프트웨어 정의 스토리지 계층으로, vSphere 호스트의 클러스터에서 사용할 수 있는 로컬 물리적 스토리지 디스크를 가상화합니다. 자동화된 데스크톱 풀 또는 자동화된 팜을 생성할 때 하나의 데이터스토어만 지정하면 가상 시스템 파일, 복제본, 사용자 데이터 및 운영 체제 파일과 같은 다양한 구성 요소가 적절한 SSD(반도체 드라이브) 디스크 또는 직접 연결된 HDD(하드 디스크)에 배치됩니다.

vSAN은 스토리지 관리에 정책 기반 방식을 구현합니다. vSAN을 사용하면 Horizon 7이 용량, 성능, 가용성 등의 가상 시스템 스토리지 요구 사항을 기본 스토리지 정책 프로파일 형태로 정의하고 vCenter Server의 가상 데스크톱에 대해 자동으로 배포합니다. 정책은 디스크(vSAN 개체)를 기준으로 자동으로 개별적으로 적용되고 가상 데스크톱 수명 주기 동안 유지 관리됩니다. 스토리지가 프로비저닝되고 할당된 정책에 따라 자동으로 구성됩니다. vCenter에서 이러한 정책을 수정할 수 있습니다. Horizon은 Horizon 클러스터마다 연결된 클론 데스크톱 풀, 인스턴트 클론 데스크톱 풀, 전체 클론 데스크톱 풀 또는 자동화된 팜에 대한 vSAN 정책을 생성합니다.

vSAN 클러스터에 대한 암호화를 사용하도록 설정하여 vSAN 데이터스토어의 모든 미사용 데이터를 암호화할 수 있습니다. vSAN 암호화는 vSAN 버전 6.6 이상에서 사용할 수 있습니다. vSAN 클러스터를 암호화하는 방법에 대한 자세한 내용은 VMware vSAN 설명서를 참조하십시오.

각 가상 시스템은 클러스터에서의 물리적 위치에 관계없이 자체 정책을 유지 보수합니다. 호스트, 디스크 또는 네트워크 오류나 워크로드 변경으로 인해 정책이 준수되지 않을 경우 vSAN은 영향을 받는 가상 시스템의 데이터를 다시 구성하고 재조정하여 각 가상 시스템의 정책을 충족합니다.

HA, vMotion 및 DRS와 같이 공유 스토리지가 필요한 VMware 기능을 지원하는 동시에 vSAN은 외부 공유 스토리지 인프라의 필요성을 제거하고 스토리지 구성 및 가상 시스템 프로비저닝 작업을 간소화합니다.

중요 vSphere 6.0 이상 릴리스에서 제공되는 vSAN 기능에는 vSphere 5.5 업데이트 2에서 제공되었던 기능 이상의 많은 성능 향상 기능이 포함되어 있습니다. 이 vSphere 6.0의 기능은 보다 광범위한 HCL(하드웨어 호환성)도 지원합니다. 또한 VMware vSAN 6.0은 캐싱과 영구 스토리지 모두에 대해 플래시 기반 디바이스를 사용하는 올 플래시 아키텍처를 지원합니다.

요구 사항 및 제한 사항

vSAN 기능을 Horizon 7 배포에서 사용할 경우 다음과 같은 제한 사항이 있습니다.

- 이 릴리스에서는 디스크를 지우고 축소하여 디스크 공간을 회수하는 Horizon 7 공간 효율적인 디스크 형식 기능의 사용을 지원하지 않습니다.
- vSAN은 NAS 디바이스를 사용하지 않기 때문에 vSAN은 VCAI(View Composer Array Integration) 기능을 지원하지 않습니다.

참고 vSAN은 View Storage Accelerator 기능과 호환됩니다. vSAN은 SSD 디스크에서 캐시 계층을 제공하고 View Storage Accelerator 기능은 부트 스톱 중 IOPS를 감소시키고 성능을 향상시키는 콘텐츠 기반 캐시를 제공합니다.

vSAN 기능의 요구 사항은 다음과 같습니다.

- vSphere 5.5 업데이트 2 이상 릴리스
- 적절한 하드웨어. 예를 들어 각 용량 기여 노드에 하나 이상의 SSD와 HDD 및 10GB NIC를 사용하는 것이 좋습니다. 자세한 내용은 [VMware 호환성 가이드](#)를 참조하십시오.
- 3대 이상의 ESXi 호스트로 구성된 클러스터. vSAN 확장 클러스터에서 2개의 ESXi 호스트를 사용하더라도 설정을 수용할 수 있는 충분한 ESXi 호스트가 필요합니다. 자세한 내용은 vSphere 구성 최대값 문서를 참조하십시오.

- HDD 용량의 10% 이상에 해당하는 SSD 용량
- 현재 설정을 수용하기에 충분한 HDD. 자기 디스크의 사용률이 75%를 초과하지 않도록 하십시오.

vSAN 요구 사항에 대한 자세한 내용은 vSphere 5.5 업데이트 2 스토리지 문서에서 "vSAN 사용"을 참조하십시오. vSphere 6 이상의 경우 VMware vSAN 관리 문서를 참조하십시오.

VMware vSAN을 위한 Horizon 7 가상 데스크톱 인프라의 주요 구성 요소 크기 지정 및 설계에 대한 지침은

<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>에 있는 백서를 참조하십시오.

가상 볼륨을 사용하여 가상 시스템 중심 스토리지 및 정책 기반 관리 지원

vSphere 6.0 이상 릴리스에서 제공되는 VVol(가상 볼륨)에서는 데이터스토어가 아닌 개별 가상 시스템이 스토리지 관리 단위가 됩니다. 스토리지 하드웨어는 가상 디스크 콘텐츠, 레이아웃 및 관리에 대한 제어 권한을 가집니다.

가상 볼륨을 통해 추상 스토리지 컨테이너는 LUN 또는 NFS 공유를 기반으로 기존 스토리지 볼륨을 교체합니다. 가상 볼륨은 가상 디스크와 파생물, 클론, 스냅샷 및 복제본을 가상 볼륨이라고 하는 스토리지 시스템의 개체에 직접 매핑합니다. 이 매핑을 통해 vSphere가 스냅샷 생성 및 복제와 같은 중점 스토리지 작업을 스토리지 시스템으로 오프로드할 수 있습니다. 그 결과의 한 가지 예는 이전에 1시간이 걸렸던 복제 작업이 가상 볼륨을 사용하여 이제는 몇 분만 소요된다는 것입니다.

중요 가상 볼륨의 주요 이점 중 하나는 SPBM(소프트웨어 정책 기반 관리)을 사용할 수 있다는 것입니다. 그러나 이 릴리스에서는 Horizon 7이 해당 vSAN이 생성하는 기본적인 세분화된 스토리지 정책을 생성하지 않습니다. 대신 vCenter Server에서 모든 가상 볼륨 데이터스토어에 적용될 전역 기본 스토리지 정책을 설정할 수 있습니다.

가상 볼륨은 다음과 같은 이점이 있습니다.

- 가상 볼륨은 많은 작업을 스토리지 하드웨어로 오프로드하는 것을 지원합니다. 이러한 작업에는 스냅샷 생성, 복제 및 Storage DRS가 포함됩니다.
- 가상 볼륨을 통해 개별 가상 디스크에 대한 복제, 암호화, 중복 제거 및 압축이 포함된 고급 스토리지 서비스를 사용할 수 있습니다.
- 가상 볼륨은 vMotion, Storage vMotion, 스냅샷, 연결된 클론, Flash Read Cache 및 DRS와 같은 vSphere 기능을 지원합니다.
- 가상 볼륨과 함께 VAAI(vSphere APIs for Array Integration)를 지원하는 스토리지 어레이를 사용할 수 있습니다.

요구 사항 및 제한 사항

가상 볼륨 기능을 Horizon 7 배포에서 사용할 경우 다음과 같은 제한 사항이 있습니다.

- 이 릴리스에서는 디스크를 지우고 축소하여 디스크 공간을 재사용하는 Horizon 7 공간 효율적인 디스크 형식 기능의 사용을 지원하지 않습니다.
- 가상 볼륨은 VCAI(View Composer Array Integration) 사용을 지원하지 않습니다.

- Virtual Volumes 데이터스토어는 인스턴트 클론 데스크톱 풀에서 지원되지 않습니다.

참고 가상 볼륨은 View Storage Accelerator 기능과 호환됩니다. vSAN은 SSD 디스크에서 캐시 계층을 제공하고 View Storage Accelerator 기능은 부트 스톱 중 IOPS를 감소시키고 성능을 향상시키는 컨텐츠 기반 캐시를 제공합니다.

가상 볼륨 기능의 요구 사항은 다음과 같습니다.

- vSphere 6.0 이상 릴리스.
- 적절한 하드웨어. 특정 스토리지 벤더는 vSphere와 통합될 수 있고 가상 볼륨에 대한 지원을 제공할 수 있는 스토리지 공급자 제공에 대한 책임이 있습니다. 모든 스토리지 공급자는 VMware에 의해 인증되어야 하며 올바르게 배포되어야 합니다.
- 가상 데이터스토어에서 프로비저닝하는 모든 가상 디스크는 1MB의 짝수 배수여야 합니다.

가상 볼륨은 vSphere 6.0 기능입니다. 관련 요구 사항, 기능, 백그라운드 및 설정 요구 사항에 대한 자세한 내용은 vSphere 스토리지 문서에서 가상 볼륨에 대한 항목을 참조하십시오.

View Composer로 스토리지 요구 사항 축소

View Composer는 기본 이미지와 가상 디스크를 공유하는 데스크톱 이미지를 생성하기 때문에 필요한 스토리지 용량을 50%에서 90%로 줄일 수 있습니다.

View Composer는 기본 이미지 또는 상위 가상 시스템을 사용하고 최고 2,000개의 연결된 클론 가상 시스템의 풀을 생성합니다. 각 연결된 클론은 고유 호스트 이름 및 IP 주소를 사용하여 독립 데스크톱처럼 작동하지만 연결된 클론은 매우 적은 양의 스토리지를 필요로 합니다.

동일한 데이터스토어의 복제 및 연결된 클론

연결된 클론 데스크톱 풀 또는 Microsoft RDS 호스트 팜을 만들면 먼저 상위 가상 시스템에서 전체 클론이 생성됩니다. 전체 클론 또는 복제본 및 연결된 클론은 동일한 데이터스토어 또는 LUN(논리 장치 번호)에 배치될 수 있습니다. 필요한 경우 재조정 기능을 사용하여 복제본 및 연결된 클론 데스크톱 풀을 한 LUN에서 다른 LUN으로 이동하거나, 연결된 클론 데스크톱 풀을 LUN에서 vSAN 데이터스토어로 이동하거나, vSAN 데이터스토어에서 LUN으로 이동할 수 있습니다.

다른 데이터스토어의 복제 및 연결된 클론

또는 다른 성능 특징을 가진 개별 데이터스토어에 View Composer 복제본 및 연결된 클론을 배치할 수 있습니다. 예를 들어 SSD(반도체 드라이브)에 복제 가상 시스템을 저장할 수 있습니다. SSD는 스토리지 용량이 적고 읽기 성능이 높아 일반적으로 초당 수만 개의 IOPS(초당 입출력)를 지원합니다. 일반적인 회전 미디어 백업 데이터스토어에 연결된 클론을 저장할 수 있습니다. 이러한 디스크는 성능은 낮지만 비용이 높지 않고 스토리지 용량은 더 높아 큰 풀에 연결된 클론을 많이 저장하는 데 적합합니다. 계층별 스토리지 구성은 많은 가상 시스템의 동시 재부팅 또는 예정된 안티바이러스 스캔 실행과 같이 많은 I/O 시나리오를 최저 비용으로 처리하는 데 사용될 수 있습니다.

자세한 내용은 VMware View를 위한 스토리지 고려 사항 모범 사례 안내를 참조하십시오.

vSAN 데이터스토어 또는 가상 볼륨 데이터스토어를 사용하는 경우 복제본 및 연결된 클론에 대해 서로 다른 데이터스토어를 수동으로 선택할 수 없습니다. vSAN 및 가상 볼륨 기능은 자동으로 개체를 적절한 디스크 유형에 배치하고 모든 I/O 작업을 캐시하기 때문에 vSAN 및 가상 볼륨 데이터스토어에 복제본 계층화를 사용할 필요가 없습니다.

페이징 및 임시 파일의 삭제 가능한 디스크

또한 연결된 클론 풀 또는 팜을 생성할 경우 삭제 가능한 개별 가상 디스크를 선택적으로 구성하여 사용자 세션 중에 생성된 게스트 운영 체제의 페이징 및 임시 파일을 저장할 수도 있습니다. 가상 시스템의 전원이 꺼지면 삭제 가능한 디스크가 삭제됩니다. 삭제 가능한 디스크를 사용하면 연결된 클론이 커지는 속도를 늦추고 전원이 꺼진 가상 시스템에서 사용한 공간을 줄여 스토리지 공간을 저장할 수 있습니다.

전용 데스크톱의 영구 디스크

또한 전용 할당 데스크톱 풀을 생성할 때 View Composer는 각 가상 데스크톱의 개별적인 영구 가상 디스크를 선택적으로 생성할 수 있습니다. 최종 사용자의 Windows 프로파일 및 애플리케이션 데이터는 영구 디스크에 저장됩니다. 연결된 클론을 새로 고치거나 재구성되거나 재조정되더라도 영구 가상 디스크의 콘텐츠가 보존됩니다. VMware에서는 개별 데이터스토어에 View Composer 영구 디스크를 보관할 것을 권장합니다. 그런 다음 영구 디스크를 보관하는 전체 LUN을 백업할 수 있습니다.

부동, 상태 비저장 데스크톱용 로컬 데이터스토어

연결된 클론 데스크톱은 ESXi 호스트의 내부 예비용 디스크인 로컬 데이터스토어에 저장될 수 있습니다. 로컬 스토리지는 저렴한 하드웨어, 빠른 가상 시스템 프로비저닝, 고성능 전원 작업 및 단순한 관리와 같은 장점을 제공합니다. 그러나 로컬 스토리지를 사용하면 사용 가능한 vSphere 인프라 구성 옵션이 제한됩니다. 로컬 스토리지 사용은 특정 환경에서는 유용하지만 다른 환경에서는 적절하지 않습니다.

참고 이 섹션에서 설명한 제한 사항은 vSAN에 대한 이전 섹션에서 설명한 것처럼 로컬 스토리지 디스크를 사용하기는 하지만 특정 하드웨어가 필요한 vSAN 데이터스토어에는 적용되지 않습니다.

사용자 환경의 원격 데스크톱이 상태를 저장하지 않는 경우, 로컬 데이터스토어를 사용하는 것이 좋습니다. 예를 들어, 상태 비저장 키오스크 또는 교실 및 훈련 스테이션을 배포하는 경우, 로컬 데이터스토어를 사용할 수 있습니다.

로컬 스토리지의 장점을 이용하려는 경우, 다음 제한 사항을 주의 깊게 고려해야 합니다.

- VMotion, VMware HA(High Availability) 또는 vSphere DRS(Distributed Resource Scheduler)를 사용할 수 없습니다.
- 리소스 풀에서 가상 시스템의 부하를 분산하기 위해 View Composer 재조정 작업을 사용할 수 없습니다.
- 개별 데이터스토어에 View Composer 복제본 및 연결된 클론을 저장할 수 없고 실제로 VMware에서는 동일한 볼륨에 저장하는 것을 권장합니다.

가상 시스템의 수와 디스크 증가 속도를 제어하여 로컬 디스크 사용을 관리하는 경우와 부동 할당을 사용하고 정기적인 새로 고침을 수행하여 작업을 삭제하는 경우, 연결된 클론을 로컬 데이터스토어에 배포할 수 있습니다.

자세한 내용은 Horizon 7에서 가상 데스크톱 설정 문서의 데스크톱 풀 생성에 대한 장을 참조하십시오.

인스턴트 클론을 사용한 스토리지 요구 사항 감소

인스턴트 클론 기능에서는 vSphere vmFork 기술(vSphere 6.0U1 이상에서 사용 가능)을 활용하여 실행 중인 기본 이미지나 상위 가상 시스템을 중지하고 가상 데스크톱 풀을 빠르게 생성하고 사용자 지정합니다.

인스턴트 클론은 생성될 때 상위 가상 시스템과 가상 디스크를 공유할 뿐만 아니라 상위의 메모리도 공유합니다. 각 인스턴트 클론은 고유 호스트 이름 및 IP 주소를 사용하여 독립 데스크톱처럼 작동하지만 인스턴트 클론은 매우 적은 양의 스토리지를 필요로 합니다. 인스턴트 클론을 사용하면 필수 스토리지 용량을 50~90퍼센트 줄일 수 있습니다. 클론을 만들 때 전체적인 메모리 요구 사항도 감소합니다. 스토리지 요구 사항 및 크기 조정 제한에 대한 자세한 내용은 VMware KB(기술 자료) 문서

<https://kb.vmware.com/kb/2150348>을 참조하십시오.

Horizon 7 버전 7.8부터 인스턴트 클론은 vSAN 데이터스토어에 대한 vSphere TRIM 및 UNMAP 기능을 지원합니다.

동일한 데이터스토어의 복제 및 인스턴트 클론

인스턴트 클론 데스크톱 풀을 생성할 경우 전체 클론이 먼저 마스터 가상 시스템에서 만들어집니다. 전체 클론 또는 복제본 및 연결된 클론은 동일한 데이터스토어 또는 LUN(논리 장치 번호)에 배치될 수 있습니다.

다른 데이터스토어의 복제 및 인스턴트 클론

또는 다른 성능 특징을 가진 개별 데이터스토어에 인스턴트 클론 복제본 및 인스턴트 클론을 배치할 수 있습니다. 예를 들어 SSD(반도체 드라이브)에 복제 가상 시스템을 저장할 수 있습니다. SSD는 스토리지 용량이 적고 읽기 성능이 높아 일반적으로 초당 수만 개의 IOPS(초당 입출력)를 지원합니다.

일반적인 회전 미디어 백업 데이터스토어에 인스턴트 클론을 저장할 수 있습니다. 이러한 디스크는 성능은 낮지만 비용이 저렴하고 스토리지 용량은 더 커서 대용량 풀에 인스턴트 클론을 많이 저장하는 데 적합합니다. 계층별 스토리지 구성은 예정된 안티바이러스 스캔의 동시 실행과 같이 많은 I/O 시나리오를 비용 효율적으로 처리하는 데 사용될 수 있습니다.

vSAN 데이터스토어를 사용하는 경우 복제본 및 인스턴트 클론에 대해 서로 다른 데이터스토어를 수동으로 선택할 수 없습니다. vSAN은 자동으로 개체를 적절한 디스크 유형에 배치하고 모든 I/O 작업을 캐시하기 때문에 vSAN 데이터스토어에 복제본 계층화를 사용할 필요가 없습니다. vSAN 데이터스토어에서는 인스턴트 클론 풀이 지원됩니다.

로컬 데이터스토어에 인스턴트 클론 저장

인스턴트 클론 가상 시스템은 ESXi 호스트의 내부 예비 디스크인 로컬 데이터스토어에 저장될 수 있습니다. 로컬 스토리지는 저렴한 하드웨어, 빠른 가상 시스템 프로비저닝, 고성능 전원 작업 및 단순한 관리와 같은 장점을 제공합니다. 그러나 로컬 스토리지를 사용하면 사용 가능한 vSphere 인프라 구성 옵션이 제한됩니다. 로컬 스토리지 사용은 특정 Horizon 7 환경에서는 유용하지만 다른 환경에서는 적절하지 않습니다.

참고 로컬 스토리지 디스크도 사용하지만 특정한 하드웨어를 필요로 하는 vSAN 데이터스토어에는 이 항목에 설명된 제한 사항이 적용되지 않습니다.

사용자 환경의 Horizon 7 데스크톱이 상태 비저장인 경우, 로컬 데이터스토어를 사용하면 잘 작동됩니다. 예를 들어, 상태 비저장 키오스크 또는 교실 및 훈련 스테이션을 배포하는 경우, 로컬 데이터스토어를 사용할 수 있습니다.

가상 시스템에 부동 할당이 있고, 개별 사용자 전용이 아니고, 사용자 로그오프 시와 같이 정기적인 간격으로 삭제 또는 새로 고칠 수 있는 경우 로컬 데이터스토어를 사용해 보십시오. 이 방식을 사용하면 데이터스토어 간에 가상 시스템을 이동하거나 로드 밸런싱하지 않고 각 로컬 데이터스토어의 디스크 사용량을 제어할 수 있습니다.

단, 다음과 같이 Horizon 7 데스크톱 또는 팜 배포 시 로컬 데이터스토어 사용에 적용되는 제한 사항을 고려해야 합니다.

- VMotion을 사용하여 가상 볼륨을 관리할 수 없습니다.
- VMware High Availability를 사용할 수 없습니다.
- vSphere DRS(Distributed Resource Scheduler)를 사용할 수 없습니다.

로컬 데이터스토어가 있는 단일 ESXi 호스트에 인스턴트 클론을 배포하는 경우 해당 단일 ESXi 호스트를 포함하는 클러스터를 구성해야 합니다. 로컬 데이터스토어가 있는 둘 이상의 ESXi 호스트 클러스터가 있는 경우 클러스터의 각 호스트에서 로컬 데이터스토어를 선택합니다. 그렇지 않으면 인스턴트 클론 생성이 실패합니다. 이 동작은 View Composer 연결된 클론이 있는 로컬 데이터스토어의 동작과는 다릅니다.

- 복제본 및 인스턴트 클론을 별도 데이터스토어에 저장할 수 없습니다.
- 로컬 회전 디스크 드라이브를 선택하는 경우 성능이 시판 중인 스토리지 어레이의 성능과 일치하지 않을 수 있습니다. 로컬 회전 디스크 드라이브와 스토리지 어레이의 용량은 비슷할 수 있지만 로컬 회전 디스크 드라이브와 스토리지 어레이의 처리량은 동일하지 않습니다. 스핀들 수가 늘어날수록 처리량이 증가합니다. 직접 연결 SSD(반도체 디스크)를 선택하는 경우 해당 성능이 많은 스토리지 어레이의 성능을 초과할 가능성이 높습니다.
- 로컬 스토리지의 이점을 활용하려면 VMotion, 고가용성, DRS 및 기타 기능을 사용할 수 없을 때 나타나는 결과를 신중하게 고려해야 합니다. 가상 시스템의 수와 디스크 증가 속도를 제어하여 로컬 디스크 사용량을 관리하는 경우, 부동 할당을 사용하면서 정기적인 새로 고침 및 삭제 작업을 수행하면 인스턴트 클론을 로컬 데이터스토어에 성공적으로 배포할 수 있습니다.
- 인스턴트 클론에 대한 로컬 데이터스토어 지원은 가상 데스크톱 및 게시된 데스크톱 둘 다에서 사용할 수 있습니다.

인스턴트 클론과 View Composer 연결된 클론의 차이

인스턴트 클론은 연결된 클론보다 훨씬 더 빠르게 만들 수 있으므로 인스턴트 클론의 풀을 프로비저닝할 때는 연결된 클론의 다음과 같은 기능이 더 이상 필요하지 않습니다.

- 인스턴트 클론 풀은 게스트 운영 체제의 페이징 및 임시 파일을 저장하기 위한 별도의 삭제 가능한 가상 디스크를 구성하도록 지원하지 않습니다. 사용자가 인스턴트 클론 데스크톱에서 로그아웃할 때마다 View에서 자동으로 클론을 삭제하고 풀에서 사용할 수 있는 최신 OS 이미지를 기반으로 다른 인스턴트 클론을 프로비저닝하여 전원을 켭니다. 모든 게스트 운영 체제 페이징 및 임시 파일은 로그오프 과정에서 자동으로 삭제됩니다.
- 인스턴트 클론 풀에서는 각 가상 데스크톱에 대한 별도의 영구 가상 디스크 생성을 지원하지 않습니다. 대신, 최종 사용자의 Windows 프로파일과 애플리케이션 데이터를 사용자 쓰기 가능한 App Volumes의 디스크에 저장할 수 있습니다. 최종 사용자의 사용자 쓰기 가능한 디스크는 최종 사용자가 로그인할 때 인스턴트 클론 데스크톱에 연결됩니다. 또한, 사용자 쓰기 가능한 디스크를 사용하여 사용자 설치 애플리케이션을 유지시킬 수 있습니다.
- 인스턴트 클론 데스크톱은 수명이 짧기 때문에 지우기와 축소 프로세스를 사용하는 공간 효율적 디스크 형식(SE 스파스)을 지원하지 않습니다.
- 인스턴트 클론 데스크톱 풀은 Storage vMotion과 호환됩니다. View Composer 연결된 클론 데스크톱 풀은 Storage vMotion과 호환되지 않습니다.

애플리케이션 프로비저닝

Horizon 7에서는 애플리케이션 프로비저닝에 몇 가지 옵션을 사용할 수 있습니다. 기존의 애플리케이션 프로비저닝 기술을 사용할 수도 있고, 원격 데스크톱이 아닌 게시된 애플리케이션을 제공할 수도 있고, VMware ThinApp으로 만든 애플리케이션 패키지를 배포할 수도 있고, View Composer나 인스턴트 클론 기본 이미지의 일부로 애플리케이션을 배포할 수도 있고, App Volumes를 사용해서 애플리케이션을 연결할 수도 있습니다.

- **RDS 호스트를 사용하여 개별 애플리케이션 배포**
최종 사용자에게 원격 데스크톱 대신 게시된 애플리케이션을 제공하도록 선택할 수도 있습니다. 소형 모바일 디바이스에서는 개별 게시된 애플리케이션을 탐색하는 것이 더 간편할 수 있습니다.
- **View Composer로 애플리케이션 및 시스템 업데이트 배포**
연결된 클론 데스크톱 풀에서 기본 이미지를 공유하기 때문에 상위 가상 시스템을 업데이트해 업데이트 및 패치를 신속하게 배포할 수 있습니다.
- **인스턴트 클론으로 애플리케이션 및 시스템 업데이트 배포**
인스턴트 클론 데스크톱 풀에서 기본 이미지를 공유하기 때문에 상위 가상 시스템을 업데이트해 업데이트 및 패치를 신속하게 배포할 수 있습니다.
- **Horizon Administrator에서 VMware ThinApp 애플리케이션 관리**
VMware ThinApp™은 애플리케이션을 가상화된 애플리케이션 샌드박스에서 실행하는 단일 파일로 패키징할 수 있습니다. 이 전략을 통해 충돌 없이 유연하게 애플리케이션을 프로비저닝할 수 있습니다.

■ App Volumes를 사용한 애플리케이션 배포 및 관리

VMware App Volumes에서는 운영 체제 위의 애플리케이션을 가상화하여 애플리케이션을 관리하는 다른 방법을 제공합니다. 이 전략을 사용하면 애플리케이션, 데이터 파일, 설정, 미들웨어, 구성이 별도의 계층 컨테이너로 작동합니다.

■ 애플리케이션 프로비저닝에 기존 프로세스 또는 VMware Mirage 사용

Horizon 7를 사용하면 회사에서 현재 사용하는 애플리케이션 프로비저닝 기술을 계속 사용할 수 있고 Mirage를 사용할 수도 있습니다. 서버 CPU 사용 및 스토리지 I/O를 관리하고 사용자가 애플리케이션을 설치하도록 허용되는지 여부를 결정하는 두 가지 추가 고려 사항이 있습니다.

RDS 호스트를 사용하여 개별 애플리케이션 배포

최종 사용자에게 원격 데스크톱 대신 게시된 애플리케이션을 제공하도록 선택할 수도 있습니다. 소형 모바일 디바이스에서는 개별 게시된 애플리케이션을 탐색하는 것이 더 간편할 수 있습니다.

최종 사용자는 이전에 원격 데스크톱에 액세스할 때 사용했던 것과 동일한 Horizon Client를 통해 Windows 기반 게시된 애플리케이션에 액세스할 수 있으며, 동일한 Blast Extreme 또는 PCoIP 디스플레이 프로토콜을 사용합니다.

게시된 애플리케이션을 제공하려면 Microsoft RDS(원격 데스크톱 세션) 호스트에 애플리케이션을 설치해야 합니다. 하나 이상의 RDS 호스트는 팜을 구성하고 이 팜에서 관리자는 데스크톱 풀을 생성할 때와 비슷한 방식으로 애플리케이션 풀을 생성할 수 있습니다. 팜 크기 조정 권장 사항에 대해서는 VMware KB(기술 자료) 문서 <http://kb.vmware.com/kb/2150348>를 참조하십시오.

이와 같은 전략을 사용하면 간편하게 애플리케이션을 추가, 제거 및 업데이트하고, 애플리케이션에 대한 사용자 권한을 추가 또는 제거하고, 모든 디바이스 또는 네트워크에서 중앙 집중식 또는 분산형 애플리케이션 팜에 대한 액세스를 제공할 수 있습니다.

View Composer로 애플리케이션 및 시스템 업데이트 배포

연결된 클론 데스크톱 풀에서 기본 이미지를 공유하기 때문에 상위 가상 시스템을 업데이트해 업데이트 및 패치를 신속하게 배포할 수 있습니다.

재구성 기능을 사용해 상위 가상 시스템을 변경하고 새 상태의 스냅샷을 생성하고 새 버전 또는 하위 집합의 이미지를 전체 사용자와 데스크톱에 적용할 수 있습니다. 이 기능으로 다음 작업을 수행할 수 있습니다.

- 운영 체제와 소프트웨어 패치 및 업데이트 적용
- 서비스 팩 적용
- 애플리케이션 추가
- 가상 디바이스 추가
- 기타 가상 시스템 설정 변경(예: 사용 가능 메모리)

참고 View Composer를 사용하여 연결된 클론 Microsoft RDS 호스트의 팜을 만들 수도 있으므로 재구성 기능을 통해 RDS 호스트에서 게스트 운영 체제와 애플리케이션을 업데이트할 수 있습니다.

사용자 설정 및 기타 사용자 생성 데이터를 포함하는 View Composer 영구 디스크를 만들 수 있습니다. 이 영구 디스크는 재구성 작업에 영향을 받지 않습니다. 연결된 클론을 삭제할 때 사용자 데이터를 보존할 수 있습니다. 직원이 퇴사하는 경우 다른 직원이 퇴사한 직원의 사용자 데이터에 액세스할 수 있습니다. 여러 데스크톱을 보유한 사용자는 단일 데스크톱에 사용자 데이터를 통합할 수 있습니다.

새로 고침 기능을 사용해 데스크톱을 기본값으로 되돌리면 사용자가 소프트웨어를 추가 또는 삭제하거나 설정을 변경하지 못하도록 설정할 수 있습니다. 또한 이 기능을 사용하면 시간에 따라 점진적으로 증가하는 연결된 클론 크기를 축소할 수 있습니다.

인스턴트 클론으로 애플리케이션 및 시스템 업데이트 배포

인스턴트 클론 데스크톱 풀에서 기본 이미지를 공유하기 때문에 상위 가상 시스템을 업데이트해 업데이트 및 패치를 신속하게 배포할 수 있습니다.

푸시 이미지 기능을 사용해 상위 가상 시스템을 변경하고 새 상태의 스냅샷을 생성하고 롤링 방식으로 새 버전의 이미지를 전체 사용자와 데스크톱에 푸시할 수 있습니다. 롤링 업데이트를 사용하여 풀 유지보수와 관련된 다운타임을 최소화할 수 있습니다. 사용자가 인스턴트 클론 가상 데스크톱에서 로그인하면 Horizon 7에서 인스턴트 클론을 삭제하고 최신 버전의 이미지에서 새 인스턴트 클론을 만들며, 새 클론은 사용자가 다음 로그인할 때 준비됩니다.

이 기능으로 다음 작업을 수행할 수 있습니다.

- 운영 체제와 소프트웨어 패치 및 업데이트 적용
- 서비스 팩 적용
- 애플리케이션 추가
- 가상 디바이스 추가
- 기타 가상 시스템 설정 변경(예: 사용 가능 메모리)

Horizon Administrator에서 VMware ThinApp 애플리케이션 관리

VMware ThinApp™은 애플리케이션을 가상화된 애플리케이션 샌드박스에서 실행하는 단일 파일로 패키징할 수 있습니다. 이 전략을 통해 충돌 없이 유연하게 애플리케이션을 프로비저닝할 수 있습니다.

VMware ThinApp은 기본 운영 체제와 해당 라이브러리 및 프레임워크에서 애플리케이션을 분리한 후 단일 실행 파일로 묶어 애플리케이션 패키지를 생성함으로써 애플리케이션을 가상화합니다. Horizon Administrator를 사용해 VMware ThinApp 애플리케이션을 데스크톱과 풀에 배포할 수 있습니다.

중요 ThinApp을 데스크톱과 풀에 할당하여 배포하는 대신 ThinApp을 Active Directory 사용자 및 그룹에 할당할 경우 VMware Identity Manager를 사용할 수 있습니다.

VMware ThinApp으로 가상화된 애플리케이션을 생성한 후에 공유 파일 서버에서 애플리케이션을 스트리밍하거나 가상 데스크톱에 애플리케이션을 설치할 수 있습니다. 스트리밍을 위해 가상화된 애플리케이션을 구성하려면 다음과 같은 아키텍처 고려 사항을 해결해야 합니다.

- 해당 애플리케이션 패키지가 저장된 특정 애플리케이션 저장소에 액세스할 수 있도록 특정 사용자 그룹에 권한 부여
- 애플리케이션 저장소에 대한 스토리지 구성
- 주로 애플리케이션 유형에 따라 달라지는 스트리밍에서 생성된 네트워크 트래픽

스트리밍된 애플리케이션의 경우 사용자는 데스크톱 바로 가기를 사용해 애플리케이션을 시작합니다.

ThinApp 패키지를 할당하여 가상 데스크톱에 설치하는 경우에는 기존 MSI 기반 소프트웨어 프로비저닝을 사용할 때와 유사한 아키텍처 고려 사항을 해결해야 합니다. 스트리밍된 애플리케이션과 원격 데스크톱에 설치된 ThinApp 패키지 모두 애플리케이션 저장소용 스토리지를 고려하여 구성합니다.

App Volumes를 사용한 애플리케이션 배포 및 관리

VMware App Volumes에서는 운영 체제 위의 애플리케이션을 가상화하여 애플리케이션을 관리하는 다른 방법을 제공합니다. 이 전략을 사용하면 애플리케이션, 데이터 파일, 설정, 미들웨어, 구성이 별도의 계층 컨테이너로 작동합니다.

읽기 전용 모드에 있거나 읽기/쓰기 모드의 쓰기 가능한 볼륨에 있을 경우 이러한 컨테이너를 애플리케이션 스택(AppStacks)이라고 합니다. 관리자는 App Volumes Manager를 사용하여 AppStacks를 만들고 애플리케이션 사용 권한을 할당하거나, 프로비저닝된 AppStacks를 시스템이나 사용자/그룹에 제공할 수 있습니다. App Volumes로 제공되는 애플리케이션은 모양과 느낌이 기본적으로 설치된 것과 같으며 여러 세션과 디바이스에 걸쳐 사용자에게 유지됩니다. 관리자는 애플리케이션을 실시간으로 업데이트하거나 교체하고, 할당된 애플리케이션을 즉시(사용자가 로그인한 상태에서) 또는 다음 로그인이나 재부팅 시에 제거할 수 있습니다.

자세한 내용은 <https://docs.vmware.com/kr/VMware-App-Volumes/index.html>에서 사용할 수 있는 VMware App Volumes 설명서를 참조하십시오.

애플리케이션 프로비저닝에 기존 프로세스 또는 VMware Mirage 사용

Horizon 7를 사용하면 회사에서 현재 사용하는 애플리케이션 프로비저닝 기술을 계속 사용할 수 있고 Mirage를 사용할 수도 있습니다. 서버 CPU 사용 및 스토리지 I/O를 관리하고 사용자가 애플리케이션을 설치하도록 허용되는지 여부를 결정하는 두 가지 추가 고려 사항이 있습니다.

동시에 많은 원격 데스크톱으로 애플리케이션을 푸시(push)할 경우 CPU 및 스토리지 I/O 사용량이 급격히 많아지는 것을 볼 수 있습니다. 이러한 피크 워크로드는 데스크톱 성능에 적지 않은 영향을 미칠 수 있습니다. 모범 사례로 애플리케이션 업데이트를 사용량이 적은 시간 중에 하도록 지정하고, 가능한 경우 데스크톱에 대한 업데이트를 분산시킵니다. 또한 스토리지 솔루션이 그러한 워크로드를 지원하도록 설계되었는지 확인해야 합니다.

회사에서 사용자가 애플리케이션을 설치할 수 있도록 허용하는 경우 현재 정책은 연장할 수 있지만 데스크톱 새로 고침 및 재구성과 같은 View Composer 기능은 사용할 수 없습니다. View Composer에서 애플리케이션이 가상화되지 않거나 반대로 사용자 프로파일 또는 데이터 설정에 포함되지 않을 경우 View Composer 새로 고침, 재구성 또는 재조정 작업이 발생할 때마다 해당 애플리케이션이 삭제됩니다. 많은 경우 설치할 애플리케이션을 완전히 제어하는 이 기능은 이점이 됩니다. View Composer 데스크톱은 성공한 구성을 따르기 때문에 지원하기 쉽습니다.

사용자가 자신의 애플리케이션을 설치하고 원격 데스크톱의 수명이 지속되는 동안 그 애플리케이션을 유지하게 해 달라고 요청하는 경우에는 애플리케이션 프로비저닝에 View Composer를 사용하지 않고 인스턴트 클론과 App Volumes를 함께 사용할 수 있습니다. 다른 해결 방법은 전체 클론 전용 데스크톱을 만들고, 사용자가 애플리케이션을 설치할 수 있도록 한 다음 사용자 설치 애플리케이션을 덮어쓰지 않고 Mirage를 사용하여 데스크톱을 관리 및 업데이트하는 것입니다.

중요 또한 Mirage를 사용하여 로컬에 설치된 오프라인 데스크톱 및 해당 애플리케이션을 관리할 수 있습니다. 자세한 내용은 [Mirage 설명서 페이지](#)를 참조하십시오.

Active Directory GPO를 사용한 사용자 및 데스크톱 관리

Horizon 7에는 Horizon 7 구성 요소 및 원격 데스크톱의 관리 및 구성을 중앙 집중화하기 위한 다수의 그룹 정책 관리 ADMX 템플릿이 있습니다.

이러한 템플릿을 Active Directory로 가져온 다음 이를 사용하여 다음 그룹 및 구성 요소에 적용할 정책을 설정할 수 있습니다.

- 사용자 로그인과 관계 없이 모든 시스템
- 로그인하는 시스템과 관계 없이 모든 사용자
- 연결 서버 구성
- Horizon Client 구성
- Horizon Agent 구성

GPO가 적용되고 나면 속성은 지정한 구성 요소의 로컬 Windows 레지스트리에 저장됩니다.

GPO를 사용하여 Horizon Administrator 사용자 인터페이스(UI)에서 사용할 수 있는 모든 정책을 설정할 수 있습니다. 또한 GPO를 사용하여 UI에서 사용할 수 없는 정책을 설정할 수 있습니다.

ADMX 템플릿을 통해 사용할 수 있는 전체 설정 목록 및 설명은 Horizon 7에서 원격 데스크톱 기능 구성의 내용을 참조하십시오.

스마트 정책 사용

스마트 정책을 사용하여 특정 원격 데스크톱의 USB 리디렉션, 가상 인쇄, 클립보드 리디렉션, 클라이언트 드라이브 리디렉션, PCoIP 디스플레이 프로토콜 기능의 동작을 제어하는 정책을 만들 수도 있습니다. 이 기능에는 User Environment Manager가 필요합니다.

스마트 정책을 사용하면 특정 조건이 충족된 경우에만 적용되는 정책을 만들 수 있습니다. 예를 들어, 사용자가 회사 네트워크 외부에서 원격 데스크톱에 연결한 경우 클라이언트 드라이브 리디렉션 기능을 사용하지 않도록 설정하는 정책을 구성할 수 있습니다.

일반적으로 User Environment Manager에서 원격 데스크톱 기능에 대해 구성한 Horizon 정책 설정이 이와 동등한 레지스트리 키 및 그룹 정책 설정을 재정의합니다.

원격 데스크톱 배포를 위한 아키텍처 설계 요소 및 계획 지침

4

일반적인 Horizon 7 아키텍처 설계는 포드 전략을 사용합니다. 포드 정의는 하드웨어 구성, 사용한 Horizon 7 및 vSphere 소프트웨어 버전, 기타 환경별 설계 요소에 따라 다를 수 있습니다.

이 문서의 예는 확장 가능한 표준 설계를 제공하므로 기업 환경 및 별도의 요구 사항에 적용될 수 있습니다. 이 장에서는 IT 설계자와 기획자가 Horizon 7 솔루션 배포에 실질적으로 필요한 사항을 이해할 수 있도록 메모리, CPU, 스토리지 용량, 네트워크 구성 요소, 하드웨어 요구 사항에 대해 자세히 설명합니다.

중요 이 장에서 다음 주제는 다루지 않습니다.

호스팅되는 애플리케이션의 아키텍처 설계	Horizon 7 포드는 각 팜에 RDS 호스트가 포함되는 Microsoft RDS 호스트 팜을 지원할 수 있습니다. 자세한 내용은 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정의 내용을 참조하십시오. RDS 호스트에 가상 시스템을 사용할 계획이면 RDS 호스트 가상 시스템 구성 도 함께 참조하십시오.
Horizon 7 Agent Direct Connect 플러그인의 아키텍처 설계	이 플러그인을 원격 가상 시스템 데스크톱에서 실행하면 클라이언트가 가상 시스템에 직접 연결할 수 있습니다. PCoIP, HTML Access, RDP, USB 리디렉션 및 세션 관리를 비롯한 모든 원격 데스크톱 기능이 사용자가 View 연결 서버를 통해 연결한 것처럼 동일한 방식으로 작동합니다. 자세한 내용은 Horizon 7 Agent Direct-Connection 플러그인 관리를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [원격 데스크톱의 가상 시스템 요구 사항](#)
- [Horizon 7 ESXi 노드](#)
- [특정 작업자 유형의 데스크톱 풀](#)
- [데스크톱 가상 시스템 구성](#)
- [RDS 호스트 가상 시스템 구성](#)
- [vCenter Server 및 View Composer 가상 시스템 구성](#)
- [Horizon 연결 서버 최대값 및 가상 시스템 구성](#)
- [vSphere 클러스터](#)
- [스토리지 및 대역폭 요구 사항](#)
- [Horizon 7 빌드 블록](#)
- [Horizon 7 팜](#)

- **팻에서 다중 vCenter Server를 사용할 경우의 장점**

원격 데스크톱의 가상 시스템 요구 사항

원격 데스크톱의 규격을 계획할 때 RAM, CPU 및 디스크 공간에 관한 선택 사항은 서버 및 스토리지 하드웨어 및 지출에 대한 선택 사항에 중요한 영향을 미칩니다.

- **작업자 유형에 기반한 계획**

가상 데스크톱과 설치하는 애플리케이션을 사용하는 작업자 유형에 따라 RAM, CPU, 스토리지 크기 등과 같은 많은 구성 요소의 요구 사항이 다릅니다.

- **가상 시스템 데스크톱의 메모리 요구 사항 계산**

RAM은 PC용보다 서버용이 더 비쌉니다. RAM이 전체 서버 하드웨어 비용에서 차지하는 비율이 높고 총 스토리지 용량이 필요하므로 데스크톱 배포 계획에서 메모리 할당량을 올바르게 결정하는 것이 중요합니다.

- **가상 시스템 데스크톱의 CPU 요구 사항 계산**

CPU를 계산하려면 회사 내 다양한 작업자 유형의 평균 CPU 사용률 정보를 수집해야 합니다.

- **적절한 시스템 디스크 크기 선택**

디스크 공간을 할당할 때는 운영 체제와 애플리케이션을 비롯해 사용자가 설치 또는 생성할 수 있는 추가 콘텐츠에 대한 공간만 충분히 제공하십시오. 일반적으로 이 공간은 물리적 PC의 디스크 크기보다 작습니다.

작업자 유형에 기반한 계획

가상 데스크톱과 설치하는 애플리케이션을 사용하는 작업자 유형에 따라 RAM, CPU, 스토리지 크기 등과 같은 많은 구성 요소의 요구 사항이 다릅니다.

작업자를 몇 가지 유형으로 분류해 아키텍처를 계획할 수 있습니다.

일반 작업자

일반 작업자와 관리 작업자는 일반적으로 고정된 컴퓨터에서 소규모 애플리케이션 집합으로 반복적인 작업을 수행합니다. 일반적으로 지식 작업자가 사용하는 애플리케이션보다 CPU와 메모리를 적게 사용하는 애플리케이션을 사용합니다. 특정 시간에 교대 근무하는 작업자가 모두 동시에 가상 데스크톱에 로그인할 수 있습니다. 일반 작업자에는 콜 센터 분석자, 소매업체 직원, 창고 작업자 등이 있습니다.

지식 작업자

지식 작업자는 인터넷 액세스, e-메일 사용을 비롯해 복잡한 문서, 프리젠테이션 및 스프레드시트 생성 등과 같은 작업을 수행합니다. 지식 작업자에는 회계사, 판매 관리자, 마케팅 조사 분석가 등이 있습니다.

고급 사용자

고급 사용자에는 애플리케이션 개발자와 그래픽을 많이 다루는 애플리케이션을 사용하는 작업자 등이 있습니다.

키오스크 사용자

이들 사용자는 공용 위치에 있는 데스크톱을 공유해야 합니다. 키오스크 사용자에는 교실이나 간호사실에서 공유 컴퓨터를 사용하는 학생, 간호사를 비롯해 구인 구직에 사용되는 컴퓨터 등이 있습니다. 이들 데스크톱은 자동 로그인 기능을 사용해야 합니다. 필요한 경우 특정 애플리케이션을 통해 인증할 수 있습니다.

가상 시스템 데스크톱의 메모리 요구 사항 계산

RAM은 PC용보다 서버용이 더 비쌉니다. RAM이 전체 서버 하드웨어 비용에서 차지하는 비율이 높고 총 스토리지 용량이 필요하므로 데스크톱 배포 계획에서 메모리 할당량을 올바르게 결정하는 것이 중요합니다.

RAM을 너무 낮게 할당하면 Windows 페이지징이 너무 많이 발생하여 스토리지 입출력에 악영향을 미칠 수 있습니다. RAM을 너무 높게 할당하면 각 가상 시스템에 대한 게스트 운영 체제의 페이지징 파일과 스왑 및 일시 중단 파일이 너무 커져 스토리지 용량에 악영향을 미칠 수 있습니다.

RAM 크기가 성능에 미치는 영향

RAM을 할당할 때는 지나치게 보수적인 설정을 선택하지 마십시오. 다음을 고려하십시오.

- RAM 할당이 부족하면 Windows 페이지징이 과도하게 발생해 성능 저하와 스토리지 입출력 로드 증가를 유발하는 입출력이 생성될 수 있습니다.
- VMware ESXi는 투명한 페이지 공유 및 메모리 팽창과 같은 정교한 메모리 리소스 관리 알고리즘을 지원하여, 지정된 게스트 RAM 할당 지원에 필요한 물리적 RAM을 크게 줄일 수 있습니다. 예를 들어 가상 데스크톱에 2GB를 할당하더라도 물리적 RAM에서는 이 가운데 일부만 사용합니다.
- 가상 데스크톱 성능은 응답 시간에 민감하므로 ESXi 호스트에서는 RAM 예약 설정 값을 0 이외의 값으로 설정하십시오. 작업이 없지만 사용 중인 데스크톱에 일부 RAM을 예약하면 디스크에 완전히 스와핑되지 않습니다. 이는 또한 ESXi 스왑 파일에서 사용하는 스토리지 공간을 줄일 수 있습니다. 그러나 예약 설정이 높으면 ESXi 호스트에 메모리를 오버커밋하는 능력에 영향을 미치고 vMotion 유지 관리 작업에도 영향을 미칠 수 있습니다.

RAM 크기가 스토리지에 미치는 영향

가상 시스템에 할당하는 RAM 양은 가상 시스템에서 사용하는 특정 파일 크기와 직접 관련되어 있습니다. 다음 목록에 있는 파일에 액세스하려면 Windows 게스트 운영 체제를 사용해 Windows 페이지징과 최대 절전 모드 파일을 찾고 ESXi 호스트의 파일 시스템을 사용해 ESXi 스왑 및 일시 중단 파일을 찾습니다.

Windows 페이지 파일

기본적으로 파일 크기는 게스트 RAM의 150%에 해당합니다. 기본적으로 C:\pagefile.sys에 위치한 이 파일에 빈번하게 액세스하기 때문에 쉘 프로비저닝된 스토리지 용량이 커집니다. View Composer 연결된 클론 가상 시스템에서 가상 시스템 전원이 꺼지면 삭제되는 개별 가상 디스크

에 페이지 파일과 임시 파일이 리디렉션될 수 있습니다. 삭제 가능한 페이지 파일 리디렉션은 스토리지를 절약하고 연결된 클론 증가 속도를 낮춰 성능을 향상할 수 있습니다. Windows에서 이 크기를 조정할 수 있지만 이는 애플리케이션 성능에 악영향을 미칠 수 있습니다.

인스턴트 클론의 경우는 로그오프 작업을 수행하는 동안 게스트 운영 체제 페이징 및 임시 파일이 자동으로 삭제되므로 크기가 심하게 커지지는 않습니다. 사용자가 인스턴트 클론 데스크톱에서 로그아웃할 때마다 Horizon에서 클론을 삭제하고 풀에서 사용할 수 있는 최신 OS 이미지를 기반으로 다른 인스턴트 클론을 프로비저닝하여 전원을 켭니다.

랩톱용 Windows 최대 절전 모드 파일

파일 크기는 게스트 RAM의 100%와 동일합니다. 이 파일은 Horizon 배포에 불필요하기 때문에 삭제해도 무방합니다.

ESXi 스왑 파일

확장명은 .vswp이며 가상 시스템 RAM의 100% 미만을 예약하는 경우 생성됩니다. 이 스왑 파일의 크기는 게스트 RAM에서 예약되지 않은 부분과 동일합니다. 예를 들어 게스트 RAM의 50%가 예약되어 있고 게스트 RAM이 2GB이면 ESXi 스왑 파일은 1GB입니다. ESXi 호스트 또는 클러스터의 로컬 데이터스토어에 이 파일을 저장할 수 있습니다.

ESXi 일시 중단 파일

확장명이 .vmss인 이 파일은 데스크톱 풀 로그오프 정책을 설정해 최종 사용자의 로그오프로 가상 데스크톱이 일시 중단될 때 생성됩니다. 파일 크기는 게스트 RAM 크기와 동일합니다.

PCoIP 또는 Blast Extreme 사용 시 특정 모니터 구성을 위한 RAM 크기

가상 시스템에서는 시스템 메모리뿐만 아니라, 비디오 오버헤드용 ESXi 호스트에서 약간의 RAM도 필요로 합니다. 이 VRAM 크기 요구 사항은 디스플레이 해상도와 최종 사용자를 위해 구성된 모니터 수에 따라 달라집니다. 표 4-1은 다양한 구성에 필요한 오버헤드 RAM 양을 보여줍니다. 열에 표시된 메모리 양은 다른 PCoIP 또는 Blast Extreme 기능에 필요한 메모리 양을 더한 값입니다.

표 4-1. PCoIP 또는 Blast Extreme 클라이언트 디스플레이 오버헤드

화면 해상도 표준	너비(픽셀)	높이(픽셀)	1-모니터 오버헤드	2-모니터 오버헤드	3-모니터 오버헤드	4-모니터 오버헤드
VGA	640	480	1.20MB	3.20MB	4.80MB	5.60MB
WXGA	1280	800	4.00MB	12.50MB	18.75MB	25.00MB
1080p	1920	1080	8.00MB	25.40MB	38.00MB	50.60MB
WQXGA	2560	1600	16.00MB	60.00MB	84.80MB	109.60MB
UHD(4K)	3840	2160	32.00MB	78.00MB	124.00MB	지원되지 않음

시스템 요구 사항 계산 시에는 VRAM 값이 가상 시스템의 기본 시스템 RAM에 더해집니다. Horizon Administrator에서 최대 모니터 수를 지정하고 디스플레이 해상도를 선택하면 오버헤드 메모리는 자동으로 계산 및 구성됩니다.

3D 렌더링 기능을 사용하고 Soft3D 또는 vSGA를 선택할 경우 3D 게스트를 위한 VRAM 구성을 위해 Horizon Administrator 제어에서 추가 VRAM 값을 사용하여 재계산할 수 있습니다. 또는, Soft3D 및 vSGA를 비롯한 다른 그래픽 가속 유형의 경우 vSphere Client를 사용하여 VRAM을 관리하면 VRAM의 정확한 크기를 지정할 수 있습니다.

기본적으로 다중 모니터 구성은 호스트 토폴로지와 일치합니다. 추가 토폴로지 체계를 수용할 수 있도록 2대 이상의 모니터에 대해 추가 오버헤드가 미리 계산되어 있습니다. 원격 데스크톱 세션을 시작할 때 검은색 화면이 나타날 경우 Horizon Administrator에 설정되어 있는 모니터 수와 디스플레이 해상도의 값이 호스트 시스템과 일치하는지 확인하거나, Horizon Administrator에서 **vSphere Client를 사용한 관리**를 선택한 다음 총 비디오 메모리 값을 최대값인 128MB로 설정하여 메모리 양을 수동으로 조정합니다.

특정 워크로드 및 운영 체제를 위한 RAM 크기

작업자 유형에 따라 필요한 RAM 양이 많이 다르기 때문에 많은 기업은 다양한 작업자 풀의 올바른 설정을 결정하기 위해 시험 단계를 거칩니다.

처음에는 32비트 Windows 7 이상 데스크톱에 1GB를 할당하고 64비트 Windows 7 이상 데스크톱에 2GB를 할당하는 것이 좋습니다. 3D 워크로드에 하드웨어 가속 그래픽 기능 중 하나를 사용하려면 2개의 가상 CPU와 4GB RAM을 사용하는 것이 좋습니다. 시험 단계에서는 다양한 작업자 유형이 사용하는 디스크 공간과 성능을 모니터링하고 각 작업자 풀에 가장 적합한 설정을 찾을 때까지 조정하십시오.

가상 시스템 데스크톱의 CPU 요구 사항 계산

CPU를 계산하려면 회사 내 다양한 작업자 유형의 평균 CPU 사용률 정보를 수집해야 합니다.

작업자 유형에 따라 CPU 요구 사항이 다릅니다. 시험 단계에서는 가상 시스템의 Perfmon, ESXi의 esxtop 또는 vCenter Server 성능 모니터링 도구와 같은 성능 모니터링 도구를 사용해 이들 작업자 그룹의 평균 및 피크 CPU 사용 수준을 확인합니다. 또한 다음 지침을 따릅니다.

- 소프트웨어 개발자나 고성능이 필요한 다른 고급 사용자는 지식 작업자와 일반 작업자보다 훨씬 높은 CPU 요구 사항이 필요할 수 있습니다. CAD 애플리케이션 사용, HD 비디오 재생 또는 4K 디스플레이 해상도 사용과 같이 계산 집약적인 작업을 실행하는 64비트 Windows 7 가상 시스템의 경우 듀얼 또는 쿼드 가상 CPU가 권장됩니다.
- 다른 경우에는 일반적으로 단일 가상 CPU를 권장합니다.

단일 서버에서 다수의 가상 시스템을 실행하기 때문에 바이러스 백신 에이전트 등과 같은 에이전트에서 정확히 같은 시간에 업데이트를 모두 확인하는 경우에는 CPU 사용량이 크게 많아질 수 있습니다. 어떤 에이전트 그리고 얼마나 많은 에이전트가 성능 문제를 유발하는지 확인하고 전략을 채택하여 이들 문제를 해결합니다. 예를 들어 다음 전략이 유용할 수 있습니다.

- 소프트웨어 관리 에이전트를 사용해 개별 가상 데스크톱에 소프트웨어 업데이트를 다운로드하기보다 인스턴트 클론이나 View Composer 연결된 클론으로 이미지를 업데이트합니다.
- 소수의 사용자가 로그인해 사용량이 적을 시간에 바이러스 백신 및 소프트웨어 업데이트를 예약합니다.
- 업데이트 시간을 분산 또는 무작위로 설정합니다.

- VMware vShield API와 호환되는 안티바이러스 제품을 사용하십시오. 예를 들어 API가 VMware vCloud[®] Networking and Security 5.1 이상과 통합되었습니다.

비공식적 방법으로 처음 크기를 계산하려면 각 가상 시스템당 최소 계산 능력으로 CPU 코어의 1/8~1/10이 필요하다고 가정합니다. 즉 코어당 가상 시스템 8~10대를 사용하는 시험 단계를 계획하십시오. 예를 들어 코어당 가상 시스템 8대를 예상하고 2소켓 8코어 ESXi 호스트를 보유하고 있는 경우에는 시험 기간 동안 가상 시스템 128대를 서버에 호스팅할 수 있습니다. 이 기간에 호스트의 전체 CPU 사용량을 모니터링하고 사용량이 높아질 경우에 대비해 여유를 충분히 확보해 안전 여유(예: 80%)를 거의 초과하지 않도록 하십시오.

적절한 시스템 디스크 크기 선택

디스크 공간을 할당할 때는 운영 체제와 애플리케이션을 비롯해 사용자가 설치 또는 생성할 수 있는 추가 콘텐츠에 대한 공간만 충분히 제공하십시오. 일반적으로 이 공간은 물리적 PC의 디스크 크기보다 작습니다.

일반적으로 데이터 센터 디스크 공간은 기존 PC 배포의 데스크톱 또는 랩톱 디스크 공간보다 기가바이트당 비용이 많이 들어가므로 운영 체제 이미지 크기를 최적화하십시오. 다음은 이미지 크기 최적화에 도움이 되는 제안 사항입니다.

- 불필요한 파일을 제거하십시오. 예를 들어, 임시 인터넷 파일에 대한 할당량을 축소하십시오.
- 인덱싱 서비스, 조각 모음 서비스, 복원 지점과 같은 Windows 서비스를 중단하십시오. 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 문서를 참조하십시오.
- 앞으로의 확장에 대비하면서도 과도하지 않은 가상 디스크 크기를 선택하십시오.
- 사용자 생성 콘텐츠 및 사용자 설치 애플리케이션에 대해 중앙 집중화된 파일 공유 또는 View Composer 영구 디스크 또는 App Volumes를 사용하십시오.
- vSphere 5.1 이상을 사용하고 있다면 vCenter Server 및 연결된 클론 데스크톱 풀을 위하여 공간 재사용 기능을 활성화하십시오.

가상 시스템 데스크톱이 vSphere 5.1 이상에서 제공되는 공간 효율적인 디스크 형식을 사용할 경우 지우기 및 축소 프로세스를 통해 게스트 운영 체제 내의 오래된 데이터 또는 삭제된 데이터가 자동으로 재사용됩니다.

각 가상 데스크톱에 대해 다음 파일을 고려하여 필요한 스토리지 공간을 계산해야 합니다.

- ESXi 일시 중단 파일은 가상 시스템에 할당된 RAM 용량과 같습니다.
- 기본적으로, Windows 페이지 파일은 RAM의 150%와 동일합니다.
- 로그 파일은 각 가상 시스템마다 약 100MB의 공간을 차지할 수 있습니다.
- 가상 디스크 또는 .vmdk 파일은 운영 체제, 애플리케이션, 향후 애플리케이션 및 소프트웨어 업데이트를 수용해야 합니다. 가상 디스크는 또한 로컬 사용자 데이터와 사용자 설치 애플리케이션이 파일 공유가 아닌 가상 데스크톱에 위치해 있는 경우 이를 수용해야 합니다.

View Composer를 사용하면 .vmdk 파일 크기가 점차 늘어나지만 View Composer 새로 고침 작업을 예약하고, 가상 시스템 데스크톱 풀의 스토리지 오버 커밋 정책을 설정하고, 별도의 비영구 디스크로 Windows 페이지와 임시 파일을 리디렉션하여 증가량을 제어할 수 있습니다.

인스턴트 클론을 사용하는 경우는 로그인 세션이 지속되는 동안 .vmdk 파일이 갈수록 커집니다. 사용자가 로그아웃할 때마다 인스턴트 클론 데스크톱이 삭제되고 다음 사용자가 로그인할 수 있도록 새 인스턴트 클론이 생성 및 준비됩니다. 이 절차를 통해 데스크톱을 효율적으로 새로 고치고 원래 크기로 되돌립니다.

사용자의 디스크 공간이 부족하지 않도록 이 예상 크기에 15%를 추가할 수 있습니다.

Horizon 7 ESXi 노트

노드는 Horizon 7 배포에서 가상 시스템 데스크톱을 호스트하는 단일 ESXi 호스트입니다.

Horizon 7는 통합 비율(ESXi 호스트에서 호스팅되는 데스크톱의 수)을 최대화할 때 가장 비용 효과적입니다. 많은 요소들이 서버 선택에 영향을 주지만 취득 비용을 엄격히 최적화하려면 처리 능력 및 메모리의 밸런스가 적절한 서버 구성을 찾아야 합니다.

환경 및 하드웨어 구성에 대한 적절한 통합 비율을 결정하기 위해 시범 단계와 같이 실제 시나리오에서 성능을 측정할 수 있는 대안이 없습니다. 통합 비율은 사용 패턴 및 환경 요소에 따라 매우 다양할 수 있으므로 다음 지침을 사용합니다.

- 일반적인 프레임워크로서 CPU 코어 당 8대~10대의 가상 데스크톱 식으로 계산 용량을 고려합니다. 각 가상 시스템의 CPU 요구 사항 계산에 대한 자세한 내용은 [가상 시스템 데스크톱의 CPU 요구 사항 계산](#)에 나와 있습니다.
- 가상 데스크톱 RAM, 호스트 RAM 및 오버커밋 비율의 식으로 메모리 용량을 생각해 봅니다. CPU 코어당 8대에서 10대 사이의 가상 데스크톱이 있을 수 있지만, 가상 데스크톱에 1GB 이상의 RAM이 있는 경우 물리적 RAM 요구 사항도 신중하게 고려해야 합니다. 가상 시스템당 필요한 RAM 양 계산에 대한 자세한 내용은 [가상 시스템 데스크톱의 메모리 요구 사항 계산](#)의 내용을 참조하십시오.
- 물리적 RAM 비용은 선형적이지 않고 일부 상황에서는 비싼 DIMM 칩을 사용하지 않는 더 작은 서버를 구입하는 것이 비용 효과적일 수 있습니다. 다른 경우 랙 밀도, 스토리지 연결성, 관리 효율성 및 다른 고려 사항으로 볼 때 배포에서 서버 수를 최소화하는 것이 더 나올 수 있습니다.
- Horizon 7에서는 View Storage Accelerator 기능이 기본으로 켜져 있어 ESXi 5.5 업데이트 2 이상의 호스트가 일반 가상 시스템 디스크 데이터를 캐시하도록 허용한다는 점에 유의하십시오. View Storage Accelerator는 성능을 향상시키고 추가 스토리지 I/O 대역폭 요구를 감소시켜 부팅 스톱 및 바이러스 백신 스캐닝 I/O 스톱을 관리할 수 있습니다. 이 기능은 ESXi 호스트당 1GB의 RAM을 필요로 합니다.
- 끝으로 클러스터 요구 사항 및 모든 패일오버 요구 사항을 고려합니다. 자세한 내용은 [고가용성 요구 사항 확인](#)의 내용을 참조하십시오.

vSphere에서 ESXi 호스트의 사양에 관한 정보는 VMware vSphere 구성 최대값 문서에 나와 있습니다.

특정 작업자 유형의 데스크톱 풀

Horizon 7는 다양한 기능을 통해 다양한 용도에 필요한 처리량을 줄이고 스토리지를 절약할 수 있도록 지원합니다. 이 가운데 많은 기능은 풀 설정으로 사용할 수 있습니다.

가장 기본적으로 특정 유형의 사용자가 상태 저장 데스크톱 이미지 또는 상태 비저장 데스크톱 이미지를 필요로 하는지 고려해야 합니다. 상태 저장 데스크톱 이미지가 필요한 사용자는 보존, 유지 관리, 백업해야 하는 운영 체제 이미지 자체 내에 데이터를 가지고 있습니다. 예를 들어, 이들 사용자는 자신의 애플리케이션을 설치하거나 파일 서버 또는 애플리케이션 데이터베이스 등 가상 시스템 외부에는 저장할 수 없는 데이터를 보유하고 있습니다.

상태 비저장 데스크톱 이미지 비영구 데스크톱이라고도 하는 상태 비저장 아키텍처는 보다 간편한 지원, 스토리지 비용 절감 등 다양한 장점을 제공합니다. 그 외에도 가상 시스템 백업 필요성을 줄이고, 보다 간단하고 저렴하게 재난 복구 및 무중단 업무 운영 옵션 등을 제공합니다.

상태 저장 데스크톱 이미지 영구 데스크톱이라고도 하는 이러한 이미지에는 기존 이미지 관리 기술이 필요할 수도 있습니다. 상태 저장 이미지는 특정 스토리지 시스템 기술을 함께 사용해 스토리지 비용을 절감할 수 있습니다. 백업, 재난 복구, 무중단 업무 운영 전략을 고려할 때는 VMware Site Recovery Manager와 같은 백업 및 복구 방법이 중요합니다.

Horizon 7에서 상태 비저장 데스크톱 이미지를 만드는 방법은 두 가지입니다.

- 인스턴트 클론 가상 시스템의 부동 할당 풀 또는 전용 할당 풀을 생성할 수 있습니다. 선택적으로 폴더 리디렉션 및 로밍 프로파일을 사용하여 사용자 데이터를 저장할 수 있습니다.
- View Composer를 사용하여 연결된 클론 가상 시스템의 부동 또는 전용 할당 풀을 만들 수 있습니다. 폴더 리디렉션 및 로밍 프로파일을 선택적으로 사용하여 사용자 데이터를 저장하거나 사용자 데이터를 유지하도록 영구 디스크를 구성할 수 있습니다.

Horizon 7에서 상태 저장 데스크톱 이미지를 만드는 방법에는 다음과 같이 몇 가지가 있습니다.

- 전체 클론 또는 전체 가상 시스템을 만들 수 있습니다. 일부 스토리지 벤더에는 전체 클론에 대한 비용 효율적인 스토리지 솔루션이 있습니다. 이러한 벤더들은 고유한 모범 사례와 프로비저닝 유틸리티를 보유하고 있는 경우도 있습니다. 이들 공급업체와 작업하면 수동 전용 할당 풀을 생성해야 하는 경우도 있습니다.
- 인스턴트 클론 또는 연결된 클론 가상 시스템의 풀을 만들고 App Volumes 사용자 쓰기 가능 볼륨을 사용하여 사용자 데이터 및 사용자 설치 애플리케이션을 연결할 수 있습니다.

상태 저장 데스크톱을 사용할지 또는 상태 비저장 데스크톱을 사용할지 여부는 특정 작업자 유형에 따라 달라집니다.

■ 일반 작업자 풀

항상 이미지가 잘 알려져 있고 쉽게 지원할 수 있는 구성을 갖도록 하고 작업자가 임의의 사용 가능한 데스크톱에 로그인할 수 있도록 작업자를 위한 상태 비저장 데스크톱 이미지를 표준화할 수 있습니다.

■ 지식 작업자 및 고급 사용자 풀

지식 작업자는 복합 문서를 생성하고 이를 데스크톱에서 계속 유지할 수 있어야 합니다. 고급 사용자는 애플리케이션을 설치하고 이를 계속 유지할 수 있어야 합니다. 보관해야 할 개인 데이터의 종류 및 양에 따라 데스크톱은 상태 저장이 될 수도 있고 상태 비저장이 될 수도 있습니다.

■ 키오스크 사용자 풀

키오스크 사용자는 항공사 체크인 스테이션 고객, 교실이나 도서관을 사용하는 학생, 의료 데이터 입력 사무실의 의료 관계자 또는 셀프 서비스 장소 고객 등이 있습니다. 사용자는 클라이언트 디바이스나 원격 데스크톱을 사용하기 위해 로그인할 필요가 없기 때문에 사용자가 아닌 클라이언트 디바이스와 연결된 계정에 이 데스크톱 풀의 사용 권한이 부여됩니다. 일부 애플리케이션은 사용자가 인증 자격 증명을 제공해야 사용할 수 있습니다.

일반 작업자 풀

항상 이미지가 잘 알려져 있고 쉽게 지원할 수 있는 구성을 갖도록 하고 작업자가 임의의 사용 가능한 데스크톱에 로그인할 수 있도록 작업자를 위한 상태 비저장 데스크톱 이미지를 표준화할 수 있습니다.

일반 작업자는 작은 애플리케이션 집합 내에서 반복 작업을 실행하기 때문에 관리자가 스토리지 공간 및 처리 요구 사항을 확보하는 데 도움을 주는 상태 비저장 데스크톱 이미지를 생성할 수 있습니다.

인스턴트 클론 데스크톱 풀에 대해 다음 풀 설정을 사용합니다.

- 인스턴트 클론 풀에서 리소스 사용률을 최적화하려면 요청 시 프로비저닝을 통해 사용량에 따라 풀을 확대하거나 축소합니다. 여분의 데스크톱을 로그인 속도를 충족하기에 충분하게 지정해야 합니다.
- 인스턴트 클론 데스크톱 풀에서는 사용자가 로그아웃할 때마다 Horizon 7에서 자동으로 인스턴트 클론을 삭제합니다. 다음 사용자가 로그인할 수 있도록 새로운 인스턴트 클론이 생성 및 준비되므로 로그아웃할 때마다 효과적으로 데스크톱을 새로 고칠 수 있습니다.

View Composer 연결된 클론 데스크톱 풀에 대해 다음 풀 설정을 사용하십시오.

- View Composer 데스크톱 풀에서는 사용자가 로그오프할 때 수행할 작업을 결정합니다(있는 경우). 시간이 경과하면 디스크 크기가 커집니다. 사용자가 로그 오프할 때 원래의 상태로 데스크톱을 새로 고쳐 디스크 공간을 확보할 수 있습니다. 또한 정기적으로 데스크톱을 새로 고치도록 설정할 수 있습니다. 예를 들어 데스크톱을 매일, 매주 또는 매달 새로 고치도록 설정할 수 있습니다.
- View Composer 연결된 클론 풀을 사용하는 경우에는 로컬 ESXi 데이터스토어에 데스크톱을 저장할 수도 있습니다. 이 전략은 저렴한 하드웨어, 빠른 가상 시스템 프로비저닝, 고성능 전원 작업 및 단순한 관리와 같은 장점을 제공할 수 있습니다. 제한 사항의 목록은 [부동, 상태 비저장 데스크톱용 로컬 데이터스토어](#)에 나와 있습니다. 로컬 데이터스토어에서는 인스턴트 클론 풀이 지원되지 않습니다.

참고 다른 유형의 스토리지 옵션에 대한 자세한 내용은 [스토리지 요구 사항 축소 및 관리](#) 항목을 참조하십시오.

- Windows 사용자 프로파일처럼, 사용자가 선호하는 데스크톱 모양 및 애플리케이션 설정을 항상 유지할 수 있도록 개인 설정 관리 기능을 사용합니다. 로그오프 시 새로 고치거나 삭제하도록 데스크톱을 설정하지 않은 경우 로그오프 시 개인 설정을 제거하도록 구성할 수 있습니다.

중요 개인 설정 관리는 세션 간의 설정을 유지하려는 사용자를 위한 부동 할당 풀 구현을 용이하게 합니다. 이전의 부동 할당 데스크톱 제약 중 하나는 최종 사용자가 로그오프할 때 원격 데스크톱에 저장된 모든 구성 설정과 데이터가 손실된다는 점이었습니다.

최종 사용자가 로그인할 때마다 데스크톱 백그라운드가 기본 배경 무늬로 설정되었고 각 애플리케이션의 기본 설정을 다시 구성해야 했습니다. 개인 설정 관리를 사용하면 부동 할당 데스크톱의 최종 사용자가 해당 세션 및 전용 할당 데스크톱의 세션 간의 차이점을 구분할 수 없습니다.

모든 데스크톱 풀에 대해 다음 일반 풀 설정을 사용합니다.

- 데스크톱이 풀 생성 시 생성되거나 풀 사용을 기반으로 요구 시 생성될 수 있도록 자동화된 풀을 생성합니다.
- 사용 가능한 임의의 데스크톱에 사용자가 로그인할 수 있도록 부동 할당을 사용합니다. 이렇게 설정하면 모든 사람이 동시에 로그인할 필요가 없는 경우에는 필요한 데스크톱 수가 줄어듭니다.
- 데스크톱이 동일한 기본 이미지를 공유하며 전체 가상 시스템보다 데이터 센터의 스토리지 공간을 덜 사용하도록 인스턴트 클론 또는 View Composer 연결된 클론 데스크톱을 생성합니다.

지식 작업자 및 고급 사용자 풀

지식 작업자는 복합 문서를 생성하고 이를 데스크톱에서 계속 유지할 수 있어야 합니다. 고급 사용자는 애플리케이션을 설치하고 이를 계속 유지할 수 있어야 합니다. 보관해야 할 개인 데이터의 종류 및 양에 따라 데스크톱은 상태 저장이 될 수도 있고 상태 비저장이 될 수도 있습니다.

지식 작업자는 임시 사용을 제외하면 사용자 설치 애플리케이션이 필요하지 않기 때문에 상태 비저장 데스크톱 이미지를 생성하고 가상 시스템 외부, 파일 서버 또는 애플리케이션 데이터베이스에 모든 개인 데이터를 저장할 수 있습니다. 다른 지식 작업자 및 고급 사용자의 경우 상태 저장 데스크톱 이미지를 생성할 수 있습니다.

인스턴트 클론 데스크톱 풀에 대해 다음 풀 설정을 사용합니다.

- 인스턴트 클론 데스크톱을 사용하는 경우에는 파일 공유, 로밍 프로파일 또는 다른 프로파일 관리 솔루션을 구현하십시오.

View Composer 연결된 클론 데스크톱 풀에 대해 다음 풀 설정을 사용하십시오.

- vSphere 가상 데스크톱과 함께 View Composer를 사용하는 경우 vCenter Server 및 데스크톱 풀을 위해 공간 재사용 기능을 활성화하십시오. 공간 재사용 기능을 사용하면 지우기 및 축소 프로세스를 통해 게스트 운영 체제 내의 오래된 데이터 또는 삭제된 데이터가 자동으로 재사용됩니다.
- View Composer 연결된 클론 데스크톱을 사용하는 경우 개인 설정 관리, 로밍 프로파일 또는 다른 프로파일 관리 솔루션을 구현합니다. 연결된 클론 OS 디스크를 새로 고치고 재구성하는 동시에 영구 디스크에 사용자 프로파일의 복사본을 보관할 수 있도록 영구 디스크를 구성할 수도 있습니다.

- Windows 사용자 프로파일처럼, 사용자가 선호하는 데스크톱 모양 및 애플리케이션 설정을 항상 유지할 수 있도록 개인 설정 관리 기능을 사용합니다.

모든 데스크톱 풀에 대해 다음 일반 풀 설정을 사용합니다.

- 일부 고급 사용자와 회계사, 판매 관리자, 마케팅 조사 분석가 등의 지식 작업자는 매번 같은 데스크톱에 로그인해야 할 수도 있습니다. 그런 경우에는 전용 할당 풀을 만듭니다.
- 처음에는 각 데스크톱이 초기 작업에 필요한 디스크 스토리지 공간 만큼만 사용할 수 있도록 vStorage Thin Provisioning을 사용합니다.
- 고유 애플리케이션을 설치하여 운영 체제 디스크에 데이터를 추가해야 하는 고급 사용자 및 지식 작업자의 경우 두 가지 옵션을 사용할 수 있습니다. 한 가지 옵션은 전체 가상 시스템 데스크톱을 생성하는 것입니다.

다른 옵션은 연결된 클론 또는 인스턴트 클론의 풀을 만든 후 App Volumes를 사용하여 사용자 설치 애플리케이션 및 사용자 데이터를 로그인에 걸쳐 유지시키는 것입니다.

- 임시 사용인 경우는 제외하고, 지식 작업자가 사용자 설치 애플리케이션이 필요하지 않은 경우 View Composer 연결된 클론 데스크톱이나 인스턴트 클론 데스크톱을 생성할 수 있습니다. 데스크톱 이미지는 동일한 기본 이미지를 공유하며 전체 가상 시스템보다 스토리지 공간을 덜 사용합니다.

키오스크 사용자 풀

키오스크 사용자는 항공사 체크인 스테이션 고객, 교실이나 도서관을 사용하는 학생, 의료 데이터 입력 사무실의 의료 관계자 또는 셀프 서비스 장소 고객 등이 있습니다. 사용자는 클라이언트 디바이스나 원격 데스크톱을 사용하기 위해 로그인할 필요가 없기 때문에 사용자가 아닌 클라이언트 디바이스와 연결된 계정에 이 데스크톱 풀의 사용 권한이 부여됩니다. 일부 애플리케이션은 사용자가 인증 자격 증명을 제공해야 사용할 수 있습니다.

키오스크 모드에서 실행되도록 설정된 가상 시스템 데스크톱은 운영 체제 디스크에 사용자 데이터를 저장할 필요가 없기 때문에 상태 비저장 데스크톱 이미지를 사용합니다. 키오스크 모드 데스크톱은 켜진 클라이언트 디바이스 또는 잠긴 PC와 함께 사용합니다. 데스크톱 애플리케이션이 보안 트랜잭션에 대해 인증 메커니즘을 구현하고, 물리적 네트워크를 임의 변경 및 침해로부터 보호하고 네트워크에 연결된 모든 디바이스를 신뢰할 수 있도록 보장해야 합니다.

모범 사례로서, 전용 연결 서버 인스턴스를 사용해 키오스크 모드에서 클라이언트를 처리하고 Active Directory에서 이들 클라이언트 계정에 대한 전용 조직 단위 및 그룹을 생성하십시오. 이 사례는 시스템을 분할해 허가 받지 않은 침입에 대비할 뿐 아니라 클라이언트를 보다 쉽게 구성 및 관리하도록 지원됩니다.

키오스크 모드를 설정하려면 vdmadmin 명령줄 인터페이스를 사용하고 Horizon 7 관리 문서의 키오스크 모드 항목에서 설명한 몇 가지 절차를 수행해야 합니다.

이 설치의 일부로 다음과 같은 인스턴트 클론 데스크톱 풀 설정을 사용할 수 있습니다.

- 인스턴트 클론 데스크톱 풀을 사용하는 경우 사용자가 로그아웃할 때마다 Horizon 7에서 자동으로 인스턴트 클론을 삭제합니다. 다음 사용자가 로그인할 수 있도록 새로운 인스턴트 클론이 생성 및 준비되므로 로그아웃할 때마다 효과적으로 데스크톱을 새로 고칠 수 있습니다.

이 설치의 일부로 다음과 같은 View Composer 연결된 클론 데스크톱 풀 설정을 사용할 수 있습니다.

- View Composer 연결된 클론 데스크톱을 사용하는 경우에는 데스크톱을 자주 새로 고치도록 (예: 사용자가 로그오프할 때마다) 새로 고침 정책을 적용합니다.
- 데스크톱을 로컬 ESXi 데이터스토어에 저장하는 것을 고려해 보십시오. 이 전략은 저렴한 하드웨어, 빠른 가상 시스템 프로비저닝, 고성능 전원 작업 및 단순한 관리와 같은 장점을 제공할 수 있습니다. 제한 사항의 목록은 [부동, 상태 비저장 데스크톱용 로컬 데이터스토어](#)에 나와 있습니다. 로컬 데이터스토어에서는 인스턴트 클론 풀이 지원되지 않습니다.

참고 다른 유형의 스토리지 옵션에 대한 자세한 내용은 [스토리지 요구 사항 축소 및 관리](#) 항목을 참조하십시오.

이 설치의 일부로 모든 데스크톱 풀에 대해 다음과 같은 일반 설정을 사용할 수 있습니다.

- 데스크톱이 풀 생성 시 생성되거나 풀 사용을 기반으로 요구 시 생성될 수 있도록 자동화된 풀을 생성합니다.
- 사용자가 풀에서 사용 가능한 임의의 데스크톱에 액세스할 수 있도록 부동 할당을 사용하십시오.
- 데스크톱이 동일한 기본 이미지를 공유하며 전체 가상 시스템보다 데이터 센터의 스토리지 공간을 덜 사용하도록 인스턴트 클론 또는 View Composer 연결된 클론 데스크톱을 생성합니다.
- 데스크톱에서 가장 가까운 프린터를 사용할 수 있도록 Active Directory GPO(그룹 정책 개체)를 사용해 위치 기반 인쇄를 구성하십시오. 그룹 정책 관리(ADMX) 템플릿을 통해 사용할 수 있는 전체 설정 목록 및 설명은 Horizon 7에서 원격 데스크톱 기능 구성을(를) 참조하십시오.
- 데스크톱을 실행하거나 클라이언트 컴퓨터에 USB 디바이스를 연결할 때 로컬 USB 디바이스가 데스크톱에 연결되는지 여부를 제어하려면 GPO 또는 스마트 정책을 사용합니다.

데스크톱 가상 시스템 구성

메모리, 가상 프로세서 수, 디스크 공간과 같은 항목에 대한 예제 설정은 Horizon 7에만 적용됩니다.

기본 이미지에 필요한 애플리케이션 수에 따라 필요한 시스템 디스크 공간이 다릅니다. VMware는 8GB의 디스크 공간을 포함하여 설치한 경우를 검증했습니다. Microsoft Word, Excel, PowerPoint, Adobe Reader, Internet Explorer, McAfee Antivirus, PKZIP 등 애플리케이션이 포함되어 있습니다.

사용자 데이터에 필요한 디스크 공간은 최종 사용자의 역할과 조직의 데이터 스토리지 정책에 따라 다릅니다. View Composer를 사용하면 영구 디스크에 이 데이터가 보관됩니다.

다음 표에 나열된 지침은 표준 Windows 7 이상 버전의 가상 시스템 데스크톱에 적용됩니다.

표 4-2. Windows 7 또는 Windows 8용 데스크톱 가상 시스템 예

항목	예
운영 체제	32비트 또는 64비트 Windows 7 이상(최신 서비스 팩 포함)
RAM	1GB(사용자에게 3D 렌더링을 위한 하드웨어 가속 그래픽이 필요할 경우 4GB)
가상 CPU	1(64비트 시스템 또는 사용자가 고화질 또는 전체 화면 비디오를 재생해야 하는 경우 2)

표 4-2. Windows 7 또는 Windows 8용 데스크톱 가상 시스템 예 (계속)

항목	예
시스템 디스크 용량	24GB(표준보다 다소 적음)
사용자 데이터 용량(영구 디스크)	5GB(시작 용량)
가상 SCSI 어댑터 유형	LSI Logic SAS(기본)
가상 네트워크 어댑터	VMXNET 3

RDS 호스트 가상 시스템 구성

RDS(원격 데스크톱 서비스) 호스트를 사용하여 게시된 애플리케이션과 세션 기반 원격 데스크톱을 최종 사용자에게 제공할 수 있습니다.

RDS 호스트는 물리적 시스템 또는 가상 시스템일 수 있습니다. 이 예에서는 아래의 표에 나와 있는 규격을 갖춘 가상 시스템을 사용합니다. 이 가상 시스템의 ESXi 호스트는 물리적 서버 장애에 대해 보호하는 VMware HA 클러스터의 일부일 수 있습니다.

표 4-3. RDS 호스트 가상 시스템 예

항목	예
운영 체제	64비트 Windows Server 2008 R2 또는 Windows Server 2012 R2
RAM	24GB
가상 CPU	4
시스템 디스크 용량	40GB
가상 SCSI 어댑터 유형	LSI Logic SAS(Windows Server 2008의 기본값)
가상 네트워크 어댑터	VMXNET 3
1 NIC	1기가비트
총 최대 클라이언트 연결 수(세션 기반 원격 데스크톱 연결 및 게시된 애플리케이션 연결 포함)	50

참고 리소스 사양의 낮은 수준으로 RDS 호스트를 구성하는 경우 기본 설치 대신 모든 기능을 사용할 경우 리소스 제약 조건이 발생할 수 있습니다.

RDS 호스트 구성 및 테스트된 워크로드에 대한 자세한 내용은

<http://www.vmware.com/files/pdf/techpaper/VMware-Reference-Architecture-Horizon-6-View-Mirage-Workspace.pdf>에 있는 VMware Horizon 6 참조 아키텍처 백서를 참조하십시오.

vCenter Server 및 View Composer 가상 시스템 구성

동일한 가상 시스템이나 별도의 서버에 vCenter Server와 View Composer를 설치할 수 있습니다. 이러한 서버는 데스크톱 가상 시스템 보다 더 많은 메모리와 처리 능력을 필요로 합니다.

VMware는 vSphere 5.1 이상을 사용하여 View Composer가 풀당 2,000대의 데스크톱을 생성하고 프로비저닝하는지를 테스트했습니다. 또한 View Composer가 한 번에 2,000개의 데스크톱에서 재구성을 수행하도록 시험하였습니다. 이 테스트에서는 vCenter Server와 View Composer가 별도의 가상 시스템에 설치되었습니다.

데스크톱 풀 크기는 다음 요소에 의해 제한됩니다.

- 각 데스크톱 풀에는 하나의 vSphere 클러스터만 포함될 수 있습니다.
- 일부 설정에서 클러스터는 최대 32대의 호스트를 포함할 수 있습니다. 기타 설정에서 클러스터는 8대의 호스트로 제한됩니다. 자세한 내용은 [vSphere 클러스터](#)의 내용을 참조하십시오.
- 각 CPU 코어는 가상 데스크톱 8대 ~ 10대에 해당하는 계산 용량을 제공합니다.
- 서버넷에 대해 사용 가능한 IP 주소 수에 따라 풀의 데스크톱 수가 제한됩니다. 예를 들어 풀의 서버넷에 256개의 사용 가능한 IP 주소만 포함되도록 네트워크를 설정한 경우 풀 크기가 256개의 데스크톱으로 제한됩니다. 하지만 여러 네트워크 레이블을 구성하여 풀의 가상 시스템에 할당할 수 있는 IP 주소의 수를 크게 늘릴 수 있습니다.

물리적 시스템에 vCenter Server 및 View Composer를 설치할 수 있지만 이 예에서는 다음 표에 나열된 규격을 준수하는 별도의 가상 시스템을 사용합니다. 이 가상 시스템의 ESXi 호스트는 물리적 서버 장애에 대비하는 VMware HA 클러스터의 일부일 수 있습니다.

이 예에서는 Horizon 7를 vSphere 5.1 이상의 버전 그리고 vCenter Server 5.1 이상의 버전과 함께 사용하는 것으로 가정합니다.

중요 또한 View Composer와 vCenter Server가 별도의 가상 시스템에 설치되어 있는 것으로 가정합니다.

표 4-4. vCenter Server 가상 시스템 예

항목	10,000대의 데스크톱을 관리하는 vCenter Server 예	2,000대의 데스크톱을 관리하는 vCenter Server 예
운영 체제	64비트 Windows Server 2008 R2 Enterprise	64비트 Windows Server 2008 R2 Enterprise
RAM	48GB	vSphere 버전에 따라 10-24GB
가상 CPU	16	vSphere 버전에 따라 2-8개
시스템 디스크 용량	180GB	40GB
가상 SCSI 어댑터 유형	LSI Logic SAS(Windows Server 2008의 기본값)	LSI Logic SAS(Windows Server 2008의 기본값)
가상 네트워크 어댑터	E1000(기본값)	VMXNET 3(기본값인 E1000을 사용해도 됨)
최대 동시 vCenter 프로비저닝 작업 수	20	20
최대 동시 전원 작업 수	50	50

표 4-5. View Composer 가상 시스템 예

항목	10,000개의 데스크톱을 관리하는 View Composer 예	2,000개의 데스크톱을 관리하는 View Composer 예
운영 체제	64비트 Windows Server 2008 R2 Enterprise	64비트 Windows Server 2008 R2 Enterprise
RAM	vSphere 버전에 따라 10GB 이상	vSphere 버전에 따라 4-10GB
가상 CPU	vSphere 버전에 따라 4개 이상	vSphere 버전에 따라 2-4개
시스템 디스크 용량	50GB	40GB
가상 SCSI 어댑터 유형	LSI Logic SAS(Windows Server 2008의 기본값)	LSI Logic SAS(Windows Server 2008의 기본값)
가상 네트워크 어댑터	VMXNET 3	VMXNET 3
최대 View Composer 풀 크기	2,000개의 데스크톱	1,000개의 데스크톱
최대 동시 View Composer 유지 관리 작업 수	12	12
최대 동시 View Composer 프로비저닝 작업 수	8	8

중요 개별 가상 시스템에 vCenter Server 및 View Composer가 연결할 데이터베이스를 배치하는 것이 좋습니다.

Horizon 연결 서버 최대값 및 가상 시스템 구성

Horizon 연결 서버를 설치할 때 Horizon Administrator 사용자 인터페이스도 설치됩니다.

연결 서버 구성

물리적 시스템에 연결 서버를 설치할 수 있지만 이 예제는 연결 서버 가상 시스템 예에 나열된 규격의 가상 시스템을 사용합니다. 이 가상 시스템의 ESXi 호스트는 물리적 서버 장애에 대해 보호하는 VMware HA 클러스터의 일부일 수 있습니다.

표 4-6. 연결 서버 가상 시스템의 예

항목	예
운영 체제	Horizon 7 설치 문서에서 지원되는 운영 체제를 참조하십시오.
RAM	10GB
가상 CPU	4
시스템 디스크 용량	70GB
가상 SCSI 어댑터 유형	LSI Logic SAS(Windows Server 2008의 기본값)
가상 네트워크 어댑터	VMXNET 3
네트워크 어댑터	1Gbps NIC

연결 서버 클러스터 설계 고려 사항

여러 복제된 연결 서버 인스턴스를 한 그룹에 배포하여 로드 밸런싱 및 고가용성을 지원할 수 있습니다. 복제된 인스턴스 그룹은 LAN 연결 단일 데이터 센터 환경에서 클러스터링을 지원하도록 디자인되었습니다.

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

연결 서버의 최대 연결 수

원격 데스크톱 연결에는 Horizon 7 배포에서 수용할 수 있는 동시 연결 수와 관련하여 테스트된 한도에 대한 정보가 나와 있습니다.

표 4-7. 원격 데스크톱 연결

배포 당 연결 서버	연결 유형	최대 동시 연결 수
1대의 연결 서버	직접 연결, RDP, Blast Extreme 또는 PCoIP	4,000(테스트된 구성)
1대의 연결 서버	터널링된 연결, RDP	2,000(기본 구성) 4,000(테스트된 구성)
1대의 연결 서버	PCoIP 보안 게이트웨이 연결	2,000(기본 구성) 4,000(테스트된 구성)
1대의 연결 서버	Blast 보안 게이트웨이 연결	2,000(기본 구성) 4,000(테스트된 구성)
1대의 연결 서버	물리적 PC에 대한 통일된 액세스	2,000(테스트된 구성)
1대의 연결 서버	RDS 호스트에 대한 통일된 액세스	2,000(테스트된 구성)
7대의 연결 서버	직접 연결, RDP, Blast Extreme 또는 PCoIP	20,000(테스트된 구성)

참고 테스트된 구성은 완전히 지원됩니다. 터널링된 연결, PCoIP 보안 게이트웨이 및 Blast 보안 게이트웨이에 대한 단일 연결 서버에서 테스트된 최대 4,000개의 동시 연결 구성을 달성하려면 연결 서버가 설치된 가상 시스템의 C:\Program Files\VMware\VMware View\Server\ssl\gateway\conf에 locked.properties 파일을 생성하십시오. 그런 다음 locked.properties 파일에 maxConnections=4000을 설정하고 연결 서버를 다시 시작합니다. Unified Access Gateway는 현재 2,000개 세션을 지원하므로 20,000개 세션을 테스트하는 동안 14대의 Unified Access Gateway 장치가 사용되었습니다.

PCoIP 보안 게이트웨이 연결은 회사 네트워크 외부에서 PCoIP 연결을 위해 보안 서버 또는 Unified Access Gateway 장치를 사용할 경우 필요합니다. Blast 보안 게이트웨이 연결은 회사 네트워크 외부에서 Blast Extreme 또는 HTML Access 연결을 위해 보안 서버 또는 Unified Access Gateway 장치를 사용할 경우 필요합니다. 회사 네트워크 외부에서의 RDP 연결과 PCoIP 또는 Blast 보안 게이트웨이에 연결된 USB 및 MMR(멀티미디어 리디렉션) 가속을 위해 보안 서버 또는 Unified Access Gateway 장치를 사용할 경우에는 터널링된 연결이 필요합니다. 연결 서버 인스턴스 하나에 여러 보안 서버를 연결할 수 있습니다.

단일 보안 서버 또는 Unified Access Gateway 장치는 최대 2,000개의 동시 연결을 지원할 수 있지만 연결 서버 인스턴스(2,000개의 세션 포함)당 단일 보안 서버를 사용하지 않고 2 또는 4를 사용하도록 선택할 수 있습니다. 보안 서버 모니터링은 2,000명의 사용자에 대한 활동이 너무 크을 나타낼 수 있습니다. 필요한 메모리 및 CPU 사용량은 로드를 분산하기 위해 연결 서버 인스턴스당 더 많은 보안 서버를 추가하도록 요구할 수 있습니다. 예를 들어 각각 1,000개의 연결을 처리하는 2대의 보안 서버를 사용하거나 각각 500개의 연결을 처리하는 4대의 보안 서버를 사용할 수 있습니다. 연결 서버 인스턴스에 대한 보안 서버의 비율은 특정 환경의 요구 사항에 따라 다릅니다.

Unified Access Gateway 장치당 연결 수는 보안 서버의 연결 수와 비슷합니다.

Unified Access Gateway 장치에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성을 참조하십시오.

참고 이 예에서는 5개의 연결 서버 인스턴스(적절히 구성된)가 20,000개의 연결을 처리할 수 있지만 회사 네트워크 내/외부 모두의 연결을 수용하려는 가용성 계획을 위해 표에는 7이라고 표시되어 있습니다.

예를 들어 20,000명의 사용자가 있고 그중 16,000명은 회사 네트워크 내부에서 연결할 경우 회사 네트워크 내부에 5개의 연결 서버 인스턴스가 필요합니다. 이렇게 하면 인스턴스 중 하나가 사용할 수 없게 될 경우 나머지 4대의 인스턴스가 로드를 처리할 수 있습니다. 마찬가지로 회사 네트워크 외부에서 4,000개의 연결이 필요할 경우 2개의 연결 서버 인스턴스를 사용하면 하나가 사용할 수 없게 되어도 나머지 한 인스턴스에서 계속 로드를 처리할 수 있습니다.

이러한 수치는 외부 연결이 게이트웨이 통해 제공된다고 가정합니다. 이 예에서 하나가 사용할 수 없게 되면 나머지 2개의 보안 서버가 로드를 처리할 수 있도록, 외부 연결을 처리하는 각 연결 서버 인스턴스는 3개의 보안 서버와 연결됩니다. 보안 서버 대신 Unified Access Gateway 장치를 사용하는 경우 하나가 사용할 수 없게 되면 나머지 2개의 장치가 로드를 처리할 수 있도록, 두 연결 서버 인스턴스에서 로드 밸런싱된 총 3개의 장치가 필요합니다.

어떤 경우든 사용자는 사용하고 있던 연결 서버 또는 게이트웨이를 사용할 수 없게 된 경우 다시 연결해야 합니다.

Horizon 7의 Unified Access Gateway에 대한 하드웨어 요구 사항

VMware에서는 Horizon 7에 사용할 경우 최대 연결 수를 지원할 수 있도록 Unified Access Gateway 장치에 4개의 vCPU와 10GB RAM을 사용할 것을 권장합니다.

표 4-8. Unified Access Gateway 에 대한 하드웨어 요구 사항

항목	예
운영 체제	OVA(SUSE Linux Enterprise 12(64비트))
RAM	4GB
가상 CPU	4
시스템 디스크 용량	20GB(기본 로그 수준을 변경하려면 추가 공간 필요)
가상 SCSI 어댑터 유형	LSI Logic Parallel(OVA의 기본값)
가상 네트워크 어댑터	VMXNET 3
네트워크 어댑터	1Gbps NIC
네트워크 매핑	단일 NIC 옵션

vSphere 클러스터

Horizon 7 배포에서는 VMware HA 클러스터를 사용하여 물리적 서버 장애에 대비할 수 있습니다. 현재 설정에 따라 클러스터에는 최대 32개의 노드를 포함할 수 있습니다.

vSphere 및 vCenter Server는 가상 시스템 데스크톱을 호스팅하는 서버의 클러스터를 관리하기 위한 고급 기능 집합을 제공합니다. 또한 각 가상 시스템 데스크톱 풀이 vCenter Server 리소스 풀과 연결되어 있어야 하기 때문에 클러스터 구성이 중요합니다. 따라서 풀 당 데스크톱의 최대 수는 클러스터 당 실행할 서버 및 가상 시스템의 수와 관련이 있습니다.

규모가 큰 Horizon 7 배포에서 데이터 센터 개체당 클러스터 개체를 하나만 지정하면 vCenter Server의 성능 및 응답성이 향상될 수 있습니다(기본 동작은 아님). 기본적으로 vCenter Server는 동일한 데이터 센터 개체에 새 클러스터를 생성합니다.

참고 Horizon 7 크기 조정 제한 및 권장 사항에 대한 최신 업데이트를 보려면 VMware KB(기술 자료) 문서 <https://kb.vmware.com/s/article/2150348>을 참조하십시오.

다음과 같은 조건에서 vSphere 클러스터에는 최대 32개의 ESXi 호스트 또는 노드를 포함할 수 있습니다.

- View Composer 연결된 클론 풀이 포함된 vSphere 5.1 이상, 그리고 NFS 데이터스토어 또는 VMFS5 이상 데이터스토어에 복제 디스크를 저장합니다.
- vSphere 6.0 이상, 그리고 가상 볼륨 데이터스토어에 풀을 저장합니다.

vSphere 5.5 업데이트 1 이상이 있으며 vSAN 데이터스토어에 풀을 저장하는 경우 vSphere 클러스터에 최대 20대의 ESXi 호스트를 포함할 수 있습니다.

View Composer 복제본을 VMFS5 이전의 VMFS 버전에 저장할 경우, 클러스터는 최대 8개의 호스트만을 가질 수 있습니다. OS 디스크와 영구 디스크는 NFS 또는 VMFS 데이터스토어에 저장할 수 있습니다.

자세한 내용은 Horizon 7에서 가상 데스크톱 설정 문서의 데스크톱 풀 생성에 대한 장을 참조하십시오. 네트워킹 요구 사항은 서버 유형, 네트워크 어댑터 수 및 VMotion 구성 방식에 따라 다릅니다.

고가용성 요구 사항 확인

vSphere는 효율성 및 리소스 관리를 통해 업계 최고 수준의 서버 당 가상 시스템을 구현할 수 있습니다. 그러나 서버 당 가상 시스템의 밀도가 더 높다는 것은 서버가 실패할 경우 더 많은 사용자가 영향을 받을 수 있다는 뜻입니다.

고가용성에 대한 요구 사항은 데스크톱 풀의 목적에 따라 상당히 다를 수 있습니다. 예를 들어 상태 비저장 데스크톱 이미지(부동 할당) 풀은 상태 저장 데스크톱 이미지(전용 할당) 풀과 복구 지점 목표(RPO)가 다를 수 있습니다. 부동 할당 풀의 경우 가능한 해결책은 사용 중인 데스크톱을 사용할 수 없게 될 경우 사용자가 다른 데스크톱에 로그인하는 것입니다.

가용성 요구 사항이 높은 경우 VMware HA를 적절하게 구성해야 합니다. VMware HA를 사용하고 서버 당 데스크톱 수를 고정시킬 경우 각 서버를 감소된 용량으로 실행합니다. 서버가 실패할 경우 데스크톱을 다른 호스트에서 다시 시작할 때 서버 당 데스크톱의 용량은 초과되지 않습니다.

예를 들어 각 호스트가 128대의 데스크톱을 실행할 수 있고 단일 서버 실패를 허용하는 것이 목표인 8 호스트 클러스터의 경우 해당 클러스터에서 실행 중인 데스크톱이 $128 * (8 - 1) = 896$ 대를 넘지 않아야 합니다. 또한 VMware DRS(Distributed Resource Scheduler)를 사용하여 8대 호스트 모두에서 데스크톱의 밸런싱을 도울 수 있습니다. 모든 핫스페어 리소스를 유휴 상태로 두지 않고 임시 서버 용량을 모두 사용합니다. 또한 DRS는 실패한 서버의 서비스가 복원된 후 클러스터 재조정을 도울 수 있습니다.

또한 서버 실패에 대한 응답으로 한 번에 많은 가상 시스템을 다시 시작하게 만드는 I/O 로드를 지원하도록 스토리지를 올바르게 구성해야 합니다. 스토리지 IOPS는 서버 실패 시 데스크톱을 빨리 복구하는 방법에 가장 큰 영향을 줍니다.

예제:클러스터 구성의 예

다음 표에 나열된 설정은 Horizon 7에 특정합니다. vSphere에서 HA 클러스터의 제한에 관한 정보는 VMware vSphere 구성 최대값 문서에 나와 있습니다.

참고 다음의 인프라 예는 View 5.2 및 vSphere 5.1로 테스트되었습니다. 이 예에서는 테스트를 View 5.2로 수행했기 때문에 인스턴트 클론이 아닌 View Composer 연결된 클론을 사용합니다. 인스턴트 클론 기능은 Horizon 7에서 도입되었습니다. View 5.2에서 사용할 수 없었던 다른 기능에는 vSAN 및 Virtual Volumes가 포함됩니다.

표 4-9. Horizon 7 인프라 클러스터 예

항목	예
가상 시스템	vCenter Server 인스턴스, Active Directory, SQL 데이터베이스 서버, View Composer, 연결 서버 인스턴스, 보안 서버, 데스크톱 풀 소스로 사용하기 위한 상위 가상 시스템
노드(ESXi 호스트)	6 Dell PowerEdge R720 서버(각 호스트에 16 코어 * 2 GHz, 192GB RAM)
SSD 스토리지	vCenter Server용 가상 시스템, View Composer, SQL 데이터베이스 서버, 상위 가상 시스템
비 SSD 스토리지	Active Directory, 연결 서버, 보안 서버용 가상 시스템
클러스터 유형	DRS(Distributed Resource Scheduler)/HA

표 4-10. 가상 시스템 데스크톱 클러스터 예

항목	예
클러스터 수	5
클러스터당 데스크톱 및 풀 수	1개의 클러스터 당 2,000 개의 데스크톱(가상 시스템)으로 구성된 1개의 풀
노드(ESXi 호스트)	다음은 각 클러스터를 위하여 사용될 수 있는 여러 서버 예입니다. <ul style="list-style-type: none"> ■ Dell PowerEdge R720 12대(각 호스트에 16코어 * 2GHz, 192GB RAM) ■ Dell PowerEdge R710 16대(각 호스트에 12코어 * 2.526GHz, 144GB RAM) ■ Dell PowerEdge R810 8대(각 호스트에 24코어 * 2GHz, 256GB RAM) ■ 6 Dell PowerEdge R810 + 3 PowerEdge R720
SSD 스토리지	복제된 가상 시스템
비 SSD 스토리지	클론용 32개의 비 SSD 데이터스토어(데이터스토어당 450 GB)
클러스터 유형	DRS(Distributed Resource Scheduler)/HA

스토리지 및 대역폭 요구 사항

가상 시스템 데스크톱의 공유 스토리지 계획, I/O 스톱과 관련된 스토리지 대역폭 요구 사항 계획, 네트워크 대역폭 필요성 계획에 대한 몇 가지를 고려해야 합니다.

VMware의 시험 설정에서 사용되는 스토리지 및 네트워크 구성 요소에 관한 자세한 내용은 관련 항목에서 제공됩니다.

■ 공유 스토리지 예

View 5.2 테스트 환경에서 View Composer 복제본 가상 시스템이 수만 개의 IOPS(초당 입출력)를 지원하는 읽기 성능이 높은 SSD(solid-state disk)에 배치되었습니다. 보다 저렴하고 보다 높은 스토리지 용량을 제공하는 일반적이고 보다 낮은 성능의 회전 미디어 백업 데이터 스토어에 연결된 클론이 배치되었습니다. 이 예에서는 테스트를 View 5.2로 수행했기 때문에 인스턴트 클론이 아닌 View Composer 연결된 클론을 사용합니다. 인스턴트 클론 기능은 Horizon 7에서 도입되었습니다.

■ 스토리지 대역폭 고려 사항

Horizon 7 환경에서 대역폭 요구 사항을 결정할 때는 로그인 스톱을 주로 고려해야 합니다.

■ 네트워크 대역폭 고려 사항

일반 워크로드를 수용하려면 특정 가상 및 물리 네트워킹 구성 요소가 필요합니다.

■ View Composer 성능 시험 결과

이 테스트 결과에서는 하나의 vCenter Server 5.1 인스턴스가 각각 2,000대 가상 시스템 데스크톱으로 구성된 5개의 풀을 관리하는 10,000개의 데스크톱으로 구성된 5.2 설정에 대해 설명합니다. 하나의 새로운 풀을 프로비저닝하거나 2000개 가상 시스템으로 구성된 기존 풀을 재구성, 새로 고침, 재조정하기 위하여 오직 하나의 관리 기간만이 필요하였습니다. 10,000명 사용자의 로그인 스톱 역시 시험되었습니다.

■ WAN 지원

광역 네트워크(WAN)의 경우 대역폭 제약 조건 및 지연 문제를 고려해야 합니다. VMware에서 제공하는 PCoIP 및 Blast Extreme 디스플레이 프로토콜은 다양한 지연 시간 및 대역폭 조건에 맞게 조정됩니다.

공유 스토리지 예

View 5.2 테스트 환경에서 View Composer 복제본 가상 시스템이 수만 개의 IOPS(초당 입출력)를 지원하는 읽기 성능이 높은 SSD(solid-state disk)에 배치되었습니다. 보다 저렴하고 보다 높은 스토리지 용량을 제공하는 일반적이고 보다 낮은 성능의 회전 미디어 백업 데이터 스토어에 연결된 클론이 배치되었습니다. 이 예에서는 테스트를 View 5.2로 수행했기 때문에 인스턴트 클론이 아닌 View Composer 연결된 클론을 사용합니다. 인스턴트 클론 기능은 Horizon 7에서 도입되었습니다.

스토리지 설계 고려 사항은 성공적인 Horizon 7 아키텍처의 가장 중요한 요소 중 하나입니다. 아키텍처에 미치는 영향이 가장 큰 결정은 연결된 클론 기술을 사용하는 View Composer 데스크톱의 사용 여부입니다. ESXi 바이너리, 가상 시스템 스왑 파일 및 상위 가상 시스템의 View Composer 복제본은 공유 스토리지 시스템에 저장됩니다.

vSphere에서 사용하는 외부 스토리지 시스템은 Fibre Channel, iSCSI SAN(Storage Area Network) 또는 NFS(Network File System) NAS(네트워크 연결 스토리지)일 수 있습니다. vSphere 5.5 업데이트 1 이상에서 사용할 수 있는 vSAN 기능을 통해 이 스토리지 시스템도 로컬 서버 연결 스토리지로 집계될 수 있습니다.

다음 예에서는 하나의 vCenter Server가 10,000대의 데스크톱을 관리하는 View 5.2 테스트 설정에서 사용되는 계층화된 스토리지 전략을 설명합니다.

참고 이 예는 VMware vSAN의 릴리스 이전에 수행된 View 5.2 설정에서 사용되었습니다.

VMware vSAN을 위한 View 가상 데스크톱 인프라의 주요 구성 요소 크기 지정 및 설계에 대한 지침은

<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>에 있는 백서를 참조하십시오.

vSphere 6.0 이상 릴리스에서 제공되는 vSAN 기능에는 vSphere 5.5 업데이트 1에서 제공되었던 기능 이상의 많은 성능 향상 기능이 포함되어 있습니다. 이 vSphere 6.0의 기능은 보다 광범위한 HCL(하드웨어 호환성)도 지원합니다. vSphere 6 이상의 vSAN에 대한 자세한 내용은 VMware vSAN 관리 문서를 참조하십시오.

물리적인 스토리지

- EMC VNX7500-블록
- 1.8TB Fast Cache(SSD)
- 8개의 10Gbit FCoE 프론트엔드 연결(컨트롤러당 4개)

SSD 스토리지 계층

단일 RAID5 스토리지 풀:

- 12 * 200GB EFD
- 상위 이미지용 250GB LUN

가상 시스템 데스크톱 스토리지 계층

- 인프라용 500GB
- 복제 스토어용 75GB LUN(풀 클러스터 당 1개)

2개의 RAID 1/0 스토리지 풀:

풀 1:

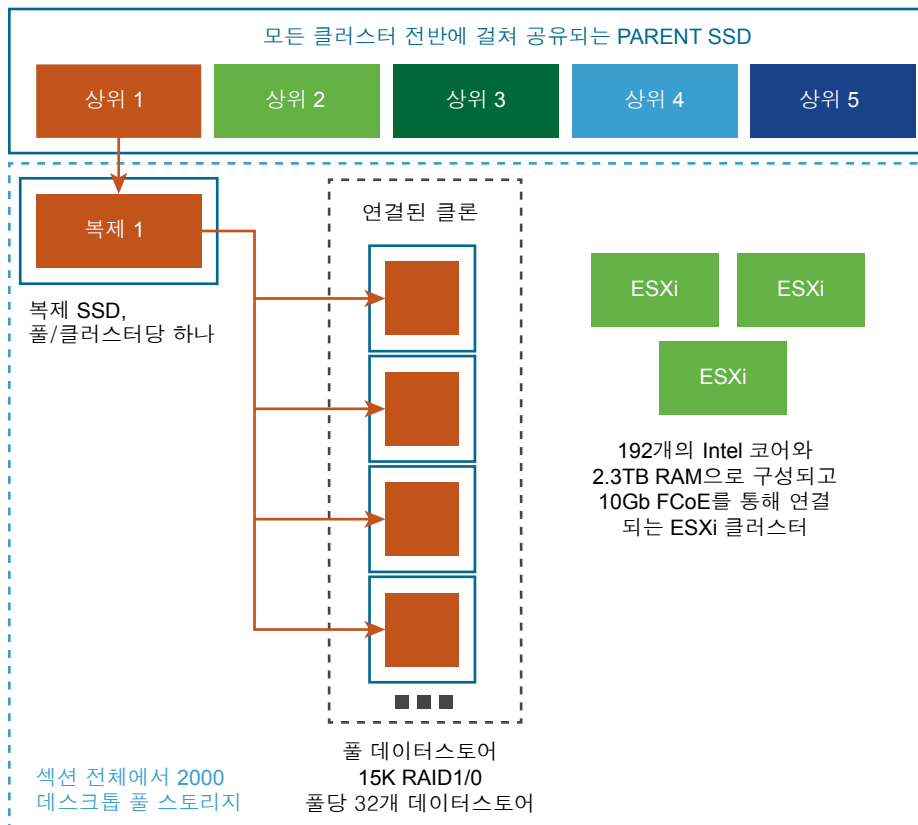
- 360 15K 300GB HDD(47TB 사용 가능)
- 데스크톱용 97,450GB

풀 2:

- 296 15K 300GB HDD(39TB 사용 가능)
- 인프라용 7 450GB LUN
- 데스크톱용 85,450GB

이 스토리지 전략이 다음 그림에 설명되어 있습니다.

그림 4-1. 큰 데스크톱 풀을 위한 계층화 스토리지 예



아키텍처 관점에서 볼 때, View Composer는 기본 이미지를 공유하는 데스크톱 이미지를 생성하며, 이로 인해 스토리지 요구 사항을 50% 이상 줄일 수 있습니다. 정기적으로 데스크톱을 원래의 상태로 되돌리고 마지막 새로 고침 작업 이후의 변경 내용을 추적하는 데 사용되는 공간을 이용하는 새로 고침 정책을 설정하여 스토리지 요구 사항을 더 감소시킬 수 있습니다.

vSphere 5.1 이상의 가상 시스템 데스크톱에 View Composer를 사용하는 경우 공간 재사용 기능을 사용할 수 있습니다. 이러한 기능을 통하여, 사용하지 않는 디스크 공간이 특정 임계값에 도달하면 지우기 및 축소 프로세스를 통해 게스트 운영 체제 내의 오래된 데이터 또는 삭제된 데이터가 자동으로 재사용됩니다. vSAN 데이터스토어를 사용하는 경우에는 공간 재사용 기능이 지원되지 않습니다.

또한 사용자 프로파일 및 사용자 문서의 기본 저장소로 View Composer 영구 디스크 또는 공유 파일 서버를 사용하여 운영 체제 디스크 공간을 줄일 수 있습니다. View Composer를 사용하여 운영 체제에서 개별 사용자 데이터를 분리할 수 있기 때문에 영구 디스크만 백업하거나 복제하면 스토리지 요구 사항이 더 감소합니다. 자세한 내용은 [View Composer로 스토리지 요구 사항 축소](#)의 내용을 참조하십시오.

참고 전용 스토리지 구성 요소와 관련한 의사 결정은 시험 단계 중에 수행하는 것이 가장 좋습니다. 기본 고려 사항은 IOPS(초당 입출력)입니다. 계층화된 스토리지 전략 또는 vSAN 스토리지를 시험하여 성능 향상 및 비용 절감을 최대화할 수 있습니다.

자세한 내용은 VMware View를 위한 스토리지 고려 사항 모범 사례 안내를 참조하십시오.

스토리지 대역폭 고려 사항

Horizon 7 환경에서 대역폭 요구 사항을 결정할 때는 로그인 스톱을 주로 고려해야 합니다.

Horizon 7 환경을 지원하는 스토리지 시스템을 설계하기 위해서는 많은 요소가 중요하지만 서버 구성 관점에서 보면 적절한 스토리지 대역폭 계획이 필수적입니다. 또한 포트 통합 하드웨어의 효과를 고려해야 합니다.

Horizon 7 환경에서 모든 가상 시스템이 동시에 작업을 수행하는 동안 가끔 I/O 스톱 로드를 경험할 수 있습니다. I/O 스톱은 안티바이러스 소프트웨어 또는 소프트웨어 업데이트 에이전트와 같은 게스트 기반 에이전트로 인해 발생할 수 있습니다. 또한 I/O 스톱은 아침에 거의 동시에 모든 고용인들이 로그인할 때와 같이 사람의 동작으로 발생할 수도 있습니다. VMware는 10,000개의 데스크톱에 대하여 로그인 스톱 시나리오를 시험하였습니다. 자세한 내용은 [View Composer 성능 시험 결과](#)의 내용을 참조하십시오.

다른 가상 시스템으로 업데이트를 분산하는 것과 같이 작업 모범 사례를 통해 이러한 스톱 워크로드를 최소화할 수 있습니다. 또한 사용자가 로그오프할 때 가상 시스템을 일시 중단할지 또는 전원을 끌지 결정하기 위해 시험 단계 중 다양한 로그오프 정책을 테스트할 수 있습니다. 개별적인 고성능 데이터스토어에 View Composer 복제본을 저장하여 I/O 스톱 로드를 해결하기 위해 많은 동시 읽기 작업 속도를 높일 수 있습니다. 예를 들어 다음과 같은 스토리지 전략 중 하나를 사용할 수 있습니다.

- 복제본이 개별 고성능 데이터스토어에 저장되도록 풀 설정을 수동으로 구성합니다.
- vSphere 5.5 업데이트 1 이상에서 제공되며, 소프트웨어 정책 기반 관리를 사용하여 복제본에 사용할 디스크 종류를 결정하는 vSAN을 사용합니다.
- vSphere 6.0 이상에서 제공되며, 소프트웨어 정책 기반 관리를 사용하여 복제본에 사용할 디스크 종류를 결정하는 가상 볼륨을 사용합니다.

모범 사례를 결정하는 것 외에도 VMware에서는 평균 대역폭이 10배 미만일 수 있어도 100개의 가상 시스템 당 1Gbps의 대역폭을 제공할 것을 권장합니다. 그러한 보수적인 계획은 피크 로드에서 충분한 스토리지 연결성을 보장합니다.

네트워크 대역폭 고려 사항

일반 워크로드를 수용하려면 특정 가상 및 물리 네트워킹 구성 요소가 필요합니다.

디스플레이 트래픽의 경우 사용되는 프로토콜, 모니터 해상도 및 구성, 워크로드의 멀티미디어 콘텐츠 양과 같은 다양한 요소가 네트워크 대역폭에 영향을 미칠 수 있습니다. 여러 애플리케이션의 동시 스트리밍도 급격한 사용량을 유발할 수 있습니다.

이들 문제가 매우 다양한 영향을 미칠 수 있기 때문에 많은 기업은 시험 프로젝트 과정에서 대역폭 사용량을 모니터링합니다. 시험 프로젝트 초기에는 일반적인 지식 작업자에 대해 150-200Kbps의 용량을 계획하십시오.

100Mb LAN 또는 1Gb 스위치 네트워크를 보유한 기업에서 PCoIP 또는 Blast Extreme 디스플레이 프로토콜을 사용하는 경우 다음 조건에서 최종 사용자에게 최고의 성능을 제공할 수 있습니다.

- 모니터 두 대(1920 x 1080)
- Microsoft Office 애플리케이션의 많은 사용량
- Flash 내장 웹 검색의 많은 사용량
- 제한적인 전체 스크린 모드로 멀티미디어를 빈번하게 사용
- USB 기반 주변 기기의 빈번한 사용
- 네트워크 기반 인쇄

자세한 내용은 PCoIP 디스플레이 프로토콜: 정보 및 시나리오 기반 네트워크 크기 조정 가이드 정보 가이드를 참조하십시오.

PCoIP 및 Blast Extreme에서 최적화 컨트롤 사용 가능

VMware의 PCoIP 또는 Blast Extreme 디스플레이 프로토콜을 사용할 경우 대역폭 사용에 영향을 주는 여러 요소를 조정할 수 있습니다.

- 네트워크 정체 기간 동안 사용되는 이미지 품질 수준 및 프레임 속도를 구성할 수 있습니다. 품질 수준 설정을 통해 디스플레이 이미지의 변경된 영역의 초기 품질을 제한할 수 있습니다. 프레임 속도를 조정할 수도 있습니다.

이러한 조정은 업데이트할 필요가 없는 정적 화면 내용 또는 일부분만 새로 고쳐야 하는 경우에 효과적입니다.

- 세션 대역폭 측면에서, 4Mbit/s 인터넷 연결과 같이 네트워크 연결 유형에 해당하는 최대 대역폭을 초당 킬로비트로 구성할 수 있습니다. 대역폭은 모든 이미징, 오디오, 가상 채널, USB, 그리고 PCoIP 또는 Blast 제어 트래픽을 포함합니다.

세션에 예약된 대역폭에 대해 초당 킬로비트로 더 낮은 제한을 구성하면 사용자가 대역폭을 사용할 수 있을 때까지 기다리지 않아도 됩니다. 세션의 UDP 패킷을 위한 최대 전송 단위(MTU) 크기를 500 ~ 1,500바이트 사이에서 지정할 수 있습니다.

자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성의 "PCoIP 일반 설정"과 "VMware Blast 정책 설정" 섹션을 참조하십시오.

네트워크 구성 예

하나의 vCenter Server 5.1 인스턴스가 각각 2,000개의 가상 시스템으로 구성된 5개의 풀을 관리하는 View 5.2 테스트 포드에서 각 ESXi 호스트의 네트워크 관련 하드웨어 및 소프트웨어 요구 사항은 다음과 같습니다.

참고 이 예는 VMware vSAN의 릴리스 이전에 수행된 View 5.2 설정에서 사용되었습니다.

VMware vSAN을 위한 View 가상 데스크톱 인프라의 주요 구성 요소 크기 지정 및 설계에 대한 지침은

<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>에 있는 백서를 참조하십시오. 또한 이 예에서는 테스트를 View 5.2로 수행했기 때문에 인스턴트 클론이 아닌 View Composer 연결된 클론을 사용합니다. 인스턴트 클론 기능은 Horizon 7에서 도입되었습니다.

각 호스트에 대한 물리적 구성 요소

- 네트워크 및 스토리지 트래픽을 위하여 10Gig Ethernet 및 FCoE를 각각 사용하는 Brocade 1860 Fabric Adapter
- 6개의 VDX6720-60 스위치로 구성된 Brocade VCS Ethernet Fabric에 연결. Juniper J6350 라우터에 2개의 1GB 연결을 통하여 네트워크의 나머지에 업링크된 스위치

vLAN 요약

- 데스크톱 풀당 1개의 10Gb vLAN(5개의 풀)
- 관리 네트워크를 위한 1개의 1Gb vLAN
- VMotion 네트워크를 위한 1개의 1Gb vLAN
- 인프라 네트워크를 위한 1개의 10Gb vLAN

가상 VMotion-dvswitch(호스트당 1개의 업링크)

인프라, 상위, 데스크톱 가상 시스템의 ESXi 호스트가 이 스위치를 사용하였습니다.

- Jumbo Frame(9000 MTU)
- Ephemeral 분산 포트 그룹 1개
- Private VLAN 및 192.168.x.x 어드레싱

Infra-dvswitch(호스트당 2개의 업링크)

인프라 가상 시스템의 ESXi 호스트가 이 스위치를 사용하였습니다.

- 점보 프레임(9000 MTU)
- Ephemeral 분산 포트 그룹 1개
- 인프라 VLAN /24(256개 주소)

Desktop-dvswitch(호스트당 2개의 업링크)

상위, 데스크톱 가상 시스템의 ESXi 호스트가 이 스위치를 사용하였습니다.

- Jumbo frame(9000 MTU)
- Ephemeral 분산 포트 그룹 6개

- 5개의 Desktop 포트 그룹(폴당 1개)
- 각 네트워크는 /21이며 이는 2048개의 주소에 해당합니다.

View Composer 성능 시험 결과

이 테스트 결과에서는 하나의 vCenter Server 5.1 인스턴스가 각각 2,000대 가상 시스템 데스크톱으로 구성된 5개의 풀을 관리하는 10,000개의 데스크톱으로 구성된 5.2 설정에 대해 설명합니다. 하나의 새로운 풀을 프로비저닝하거나 2000개 가상 시스템으로 구성된 기존 풀을 재구성, 새로 고침, 재조정하기 위하여 오직 하나의 관리 기간만이 필요하였습니다. 10,000명 사용자의 로그인 스톱 역시 시험되었습니다.

다음 항목에 설명된 소프트웨어, 하드웨어, 구성 설정을 통하여 여기에 제공된 시험 결과를 얻을 수 있었습니다.

- [Horizon 연결 서버 최대값 및 가상 시스템 구성](#)에 기술된 데스크톱 및 풀 구성
- [공유 스토리지 예](#)에 기술된 계층화된 스토리지 구성 요소
- [네트워크 대역폭 고려 사항](#)에 기술된 네트워킹 구성 요소

1시간 동안 10,000명 사용자의 로그인 스톱을 위한 용량

참고 이 예는 VMware vSAN의 릴리스 이전에 수행된 View 5.2 설정에서 사용되었습니다.

VMware vSAN을 위한 View 가상 데스크톱 인프라의 주요 구성 요소 크기 지정 및 설계에 대한 지침은

<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf>에 있는 백서를 참조하십시오. 다양한 워크로드의 테스트 결과와 vSAN 사용 시 View 작업은

<http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-virtual-san-reference-architecture.pdf>에 있는 참조 아키텍처 백서를 참조하십시오.

vSphere 6.0 이상 릴리스에서 제공되는 vSAN 기능에는 vSphere 5.5 업데이트 1에서 제공되었던 기능 이상의 많은 성능 향상 기능이 포함되어 있습니다. 이 vSphere 6.0의 기능은 보다 광범위한 HCL(하드웨어 호환성)도 지원합니다. vSphere 6 이상의 vSAN에 대한 자세한 내용은 VMware vSAN 관리 문서를 참조하십시오.

테스트 설정에서 다음 데스크톱 및 풀 구성이 10,000대의 데스크톱에 대한 로그인 스톱 시나리오에 사용되었습니다. 데스크톱의 전원 정책이 항상 켜짐으로 설정되었습니다.

10,000대의 데스크톱에 대해 정상적인 로그인 시간 분배를 사용해 로그인 스톱이 60분 동안 발생했습니다. 가상 시스템의 전원이 켜졌고 로그인 스톱이 시작되기 전에 가상 시스템을 사용할 수 있었습니다. 로그인하면 Adobe Reader, Microsoft Outlook, Internet Explorer, Microsoft Word 및 메모장 등 애플리케이션이 포함된 워크로드가 시작되었습니다.

다음은 테스트 도중 지속된 로그인 스톱의 추가 상세 정보입니다.

- +/- 2 표준 편차 시간(40분) 내에 발생한 로그인의 95%.
- +/- 1 표준 편차 시간(20분) 내에 발생한 로그인의 68%.

- 피크 로그인 비율은 400/분 또는 6.67/초였습니다.

풀을 프로비저닝하는데 필요한 시간

사용자에게 풀이 할당되기 때문에, 풀을 생성하거나 필요할 경우 풀이 미리 프로비저닝됩니다. 프로비저닝은 정확한 운영 체제 이미지와 네트워크 설정을 사용할 수 있도록 가상 시스템을 생성하고 구성하는 것을 의미합니다.

2,000 개의 가상 시스템으로 각 풀을 구성하여 총 4개의 풀을 포함한 시험 설정에서 2,000개의 가상 시스템으로 구성된 5번째 풀을 프로비저닝 하는데 4시간이 소요되었습니다. 모든 가상 시스템은 미리 프로비저닝되었습니다.

풀을 재구성하는데 필요한 시간

재구성 작업을 통하여 운영 체제 패치를 제공하고, 애플리케이션을 설치 또는 업데이트하고, 풀에서 가상 시스템의 데스크톱 하드웨어 설정을 변경할 수 있습니다. 풀을 재구성하기 전에, 새롭게 구성된 가상 시스템의 스냅샷을 생성합니다. 재구성 작업은 이 스냅샷을 사용하며 풀의 모든 가상 시스템을 업데이트합니다.

각 풀이 2,000개의 가상 시스템으로 구성된 5개의 풀에 대한 시험 설정에서 2,000개의 가상 시스템으로 구성된 1개의 풀을 재구성하기 위하여 6시간 40분이 소요되었습니다. 재구성 작업을 시작하기 전에 모든 가상 시스템의 전원은 켜져 이용 가능한 상태였습니다.

풀을 새로 고침하는데 필요한 시간

디스크는 시간이 지남에 따라 커지기 때문에, 사용자가 로그오프할 때 데스크톱을 원래의 상태로 새로 고침하여 디스크 공간을 확보하거나 주기적으로 데스크톱을 새로 고침할 수 있도록 일정을 정할 수 있습니다. 예를 들어 데스크톱을 매일, 매주 또는 매달 새로 고치도록 설정할 수 있습니다.

각 풀이 2,000개의 가상 시스템으로 구성된 5개의 풀에 대한 시험 설정에서 2,000개의 가상 시스템으로 구성된 1개의 풀을 새로 고침하기 위하여 2시간 40분이 소요되었습니다. 새로 고침 작업을 시작하기 전에 모든 가상 시스템의 전원은 켜져 이용 가능한 상태였습니다.

풀을 재조정하는데 필요한 시간

데스크톱 재조정 작업은 사용 가능한 논리 드라이브 사이에 연결된 클론 데스크톱을 균등하게 재배포합니다. 재조정 작업은 오버로드된 드라이브에 스토리지 공간을 저장하고 충분히 이용하지 않은 드라이브가 있는지 확인합니다. 또한 재조정 작업을 통해 데스크톱 풀의 모든 가상 시스템을 vSAN 데이터스토어로 마이그레이션하거나 이 데이터스토어로부터 마이그레이션할 수 있습니다.

각 풀이 2,000 개의 가상 시스템으로 구성된 총 5개의 풀을 포함한 시험 팟에서 1회 시험을 위하여 팟에 2개의 데이터스토어가 추가되었습니다. 다른 시험에서는 팟에서 2개의 데이터스토어가 제거되었습니다. 데이터스토어가 추가 또는 제거된 후, 하나의 풀에서 재조정 작업이 수행되었습니다. 2,000개의 가상 시스템으로 구성된 1개의 풀을 재조정하기 위하여 9시간이 소요되었습니다. 재조정 작업을 시작하기 전에 모든 가상 시스템의 전원은 켜져 이용 가능한 상태였습니다.

WAN 지원

광역 네트워크(WAN)의 경우 대역폭 제약 조건 및 지연 문제를 고려해야 합니다. VMware에서 제공하는 PCoIP 및 Blast Extreme 디스플레이 프로토콜은 다양한 지연 시간 및 대역폭 조건에 맞게 조정됩니다.

RDP 디스플레이 프로토콜을 사용할 경우 지점 또는 작은 사무실의 사용자의 애플리케이션을 가속화하기 위해 WAN 최적화 제품이 있어야 합니다. PCoIP 및 Blast Extreme에서는 많은 WAN 최적화 기술이 기본 프로토콜에 내장되어 있습니다.

- 이러한 프로토콜에는 클라이언트 및 서버 간 많은 핸드셰이크가 필요하기 때문에 WAN 최적화는 RDP와 같은 TCP 기반 프로토콜에 유용합니다. 이러한 핸드셰이크 지연은 매우 커질 수 있습니다. WAN 가속기 스푸핑은 프로토콜의 네트워크 지연이 숨겨지도록 핸드셰이크에 응답합니다. PCoIP 및 Blast Extreme이 UDP 기반이기 때문에 이러한 형태의 WAN 가속화는 필요가 없습니다.
- 또한 WAN 가속기는 클라이언트 및 서버 간 네트워크 트래픽을 압축하지만 이 압축은 대개 2:1 압축 비율로 제한됩니다. PCoIP 및 Blast Extreme의 압축률이 훨씬 높습니다.

PCoIP 및 Blast Extreme의 대역폭 소비 방법을 조정하는 데 사용되는 컨트롤에 대한 자세한 내용은 [PCoIP 및 Blast Extreme에서 최적화 컨트롤 사용 가능](#)을 참조하십시오.

다양한 사용자 유형의 대역폭 요구 사항

PCoIP의 최소 대역폭 요구 사항을 결정할 때는 다음과 같은 추정치로 계획하십시오.

- 기본 오피스 생산성 데스크톱을 위한 100 ~ 150Kbps 평균 대역폭: 비디오, 3D 그래픽과 기본 Windows 및 Horizon 7 설정이 없는 일반적인 오피스 애플리케이션.
- 최적화된 오피스 생산성 데스크톱을 위한 50 ~ 100Kbps 평균 대역폭: 비디오, 3D 그래픽, 최적화된 Windows 데스크톱 설정, 최적화된 Horizon 7 설정이 없는 일반적인 오피스 애플리케이션.
- 다중 모니터, 3D, Aero 및 Microsoft Office를 활용하는 가상 데스크톱을 위한 400 ~ 600Kbps 평균 대역폭.
- 디스플레이 변경 버스트에 여유 공간을 제공하기 위한 500Kbps ~ 1Mbps 최소 피크 대역폭. 일반적으로는 평균 대역폭을 사용하여 네트워크를 크기 조정하지만 큰 화면 변경과 관련된 이미징 트래픽의 버스트를 수용하는 피크 대역폭을 고려해야 합니다.

- 구성된 프레임 속도 제한 및 비디오 유형에 따라 동시에 480p 비디오를 실행하는 사용자당 2Mbps가 필요합니다.

참고 일반적인 사용자당 50 ~ 150Kbps라는 추정치는 모든 사용자가 계속 작업 중이며 하루에 8 ~ 10시간 넘게 유사한 작업을 수행한다는 가정을 기반으로 합니다. 50Kbps 대역폭 사용 수치는 Build-to-Lossless 기능이 사용되지 않도록 설정된 LAN의 View Planner 테스트를 통해 나온 결과입니다. 일부 사용자가 비활성 상태일 수 있고 대역폭을 거의 사용하지 않는 상황이 달라질 수 있어 링크마다 더 많은 사용자를 허용합니다. 따라서 이러한 지침은 더 자세한 대역폭 계획 및 테스트를 위한 시작점을 제공하기 위한 것입니다.

다음 예제는 1.5Mbps T1 라인이 있는 지점 또는 원격 사무실의 동시 사용자 수 계산 방법을 표시합니다.

지점 또는 원격 사무실 시나리오

- 사용자에게 기본 Microsoft Office 생산성 애플리케이션이 있고 비디오와 3D 그래픽은 없으며 USB 키보드 및 마우스 디바이스가 있습니다.
- Horizon 7의 일반 오피스 사용자당 필요한 대역폭은 50 ~ 150Kbps부터입니다.
- T1 네트워크 용량은 1.5Mbps입니다.
- 대역폭 사용률은 80퍼센트입니다(사용률 계수 0.8).

지원된 사용자 수 결정 공식

- 최악의 경우, 사용자에게 150Kbps 필요: $(1.5\text{Mbps} * .8) / 150\text{Kbps} = (1500 * .8) / 150 =$ 사용자 8명
- 최선의 경우, 사용자에게 50Kbps 필요: $(1.5\text{Mbps} * .8) / 50\text{Kbps} = (1500 * .8) / 50 =$ 사용자 24명

결과

이 원격 사무실은 1.5Mbps 용량으로 T1 라인당 8 ~ 24명의 사용자를 동시에 지원할 수 있습니다.

중요 이 사용자 밀도를 얻으려면 Horizon 7 및 Windows 데스크톱 설정 모두를 최적화해야 할 수 있습니다.

Horizon 7 빌드 블록

빌드 블록은 물리적 서버, vSphere 인프라, Horizon 7 서버, 공유 스토리지 및 최종 사용자를 위한 가상 시스템 데스크톱으로 구성됩니다. 빌드 블록은 논리적 구성이며 2,000개 이하의 Horizon 데스크톱으로 구성되어야 합니다. 일반적으로 고객은 Horizon 7 포트 하나에 최대 다섯 개의 빌드 블록을 포함하지만, 이론적으로는 포트가 10,000개의 세션 및 7개의 Horizon 연결 서버 인스턴스를 초과하지만 않으면 더 많은 블록을 사용할 수 있습니다.

표 4-11. 2,000대의 가상 시스템 데스크톱을 위한 LAN 기반 Horizon 빌드 블록의 예

항목	예
vSphere 클러스터	1 이상
80 포트 네트워크 스위치	1
공유 스토리지 시스템	1
동일한 호스트에 View Composer를 갖고 있는 vCenter Server	1(블록 자체에서 실행될 수 있음)
데이터베이스	MS SQL Server 또는 Oracle 데이터베이스 서버(블록 자체에서 실행될 수 있음)
VLAN	3(1Gbit 이더넷 네트워크: 각 관리 네트워크, 스토리지 네트워크 및 VMotion 네트워크용)

각 vCenter Server는 최대 10,000대의 가상 시스템을 지원할 수 있습니다. 이 지원을 통해 2,000대 이상의 가상 시스템 데스크톱을 포함하는 빌드 블록을 보유할 수 있습니다. 그러나 실제 블록 크기에는 다른 Horizon 7 관련 제한 사항도 적용됩니다.

포드에 빌드 블록이 하나뿐인 경우 이중화를 위해 두 개의 연결 서버 인스턴스를 사용합니다.

Horizon 7 팟

팟은 Horizon 7 확장성 제한에 따라 결정되는 조직의 단위입니다.

3개의 빌드 블록을 사용하는 팟 예

일반적인 Horizon 7 팟은 2,000명의 사용자로 구성된 빌드 블록 다섯 개를 하나의 엔터티로 관리할 수 있도록 통합합니다.

표 4-12. 5개의 빌드 블록으로 구성된 LAN 기반 Horizon 7 팟의 예

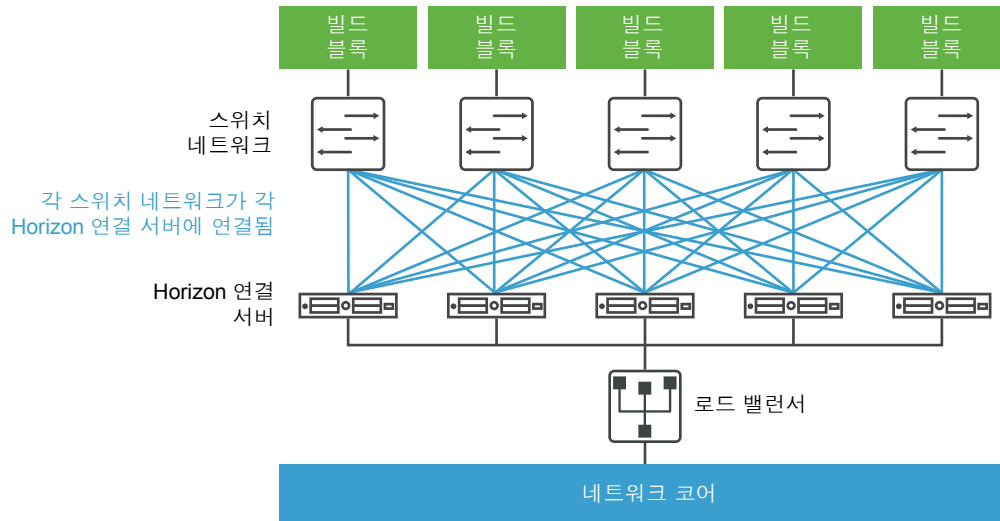
항목	수
Horizon 7 팟에 대한 빌드 블록	5
vCenter Server 및 View Composer	5(각 빌드 블록 내에서 2개 모두를 호스팅하는 1개의 가상 시스템)
데이터베이스 서버	5(각 빌드 블록 내 1개의 독립 실행형 데이터베이스 서버) MS SQL Server 또는 Oracle 데이터베이스 서버
연결 서버	7(회사 네트워크 내부 연결용 5개와 외부 연결용 2개)
vLAN	표 4-11 의 내용을 참조하십시오.
10Gb 이더넷 모듈	1
모듈식 네트워킹 스위치	1

각 vCenter Server는 최대 35,000대의 등록된 가상 시스템을 지원할 수 있습니다. 이 지원을 통해 2,000대 이상의 가상 시스템 데스크톱을 포함하는 빌드 블록을 보유할 수 있습니다. 그러나 실제 블록 크기에는 다른 Horizon 7 관련 제한 사항도 적용됩니다.

여기에 제시한 2가지 예에서는 네트워크 코어가 연결 서버 인스턴스에 대해 들어오는 요청을 로드 밸런싱합니다. 이중화 및 페일오버 메커니즘에 대한 지원은 일반적으로 네트워크 수준에서 로드 밸런서가 단일 실패 지점이 되지 않도록 방지할 수 있습니다. 예를 들어, 가상 라우터 중복 프로토콜(VRRP)은 이중화 및 페일오버 기능을 추가하도록 로드 밸런서와 통신합니다.

연결 서버 인스턴스가 실패하거나 활성 세션 중 응답하지 않을 경우에도 사용자 데이터는 손실되지 않습니다. 사용자가 다른 연결 서버 인스턴스에 연결할 수 있도록 가상 시스템 데스크톱에서 데스크톱 상태가 유지되며 해당 데스크톱 세션은 실패가 발생했었던 바로 그 지점에서 다시 시작됩니다.

그림 4-2. 가상 시스템 데스크톱 10,000대를 지원하는 팟 다이어그램



하나의 vCenter Server 를 사용하는 팟 예

이전 세션에서는 Horizon 7 팟이 여러 개의 빌드 블록으로 구성되어 있었습니다. 각 빌드 블록은 단일 vCenter Server를 통하여 2,000대의 가상 시스템을 지원하였습니다. VMware는 단일 vCenter Server를 사용하여 Horizon 7 팟을 관리할 수 있도록 많은 고객과 파트너 요청을 수신하였습니다. vCenter Server의 단일 인스턴스가 10,000대의 가상 시스템을 지원할 수 있다는 사실로 인하여 이러한 요청이 발생하였습니다. 고객은 단일 vCenter Server를 사용하여 10,000개의 데스크톱 환경을 관리할 수 있습니다. 이 항목은 10,000대의 데스크톱을 관리하기 위하여 단일 vCenter Server를 사용하는 것에 기반을 둔 아키텍처를 설명합니다.

10,000대의 데스크톱을 위하여 단일 vCenter Server와 단일 View Composer를 사용할 수는 있지만, 이 경우 단일 실패 지점이 생성될 수 있습니다. 단일 vCenter Server를 손실하게 되면 전체 데스크톱 배포에서 전원, 프로비저닝, 다시 맞춤 작업을 이용할 수 없게 됩니다. 이러한 이유로 인하여 전체 구성 요소 복원성을 위한 요구 사항을 충족하는 배치 아키텍처를 선택하십시오.

예를 들어 10,000명의 사용자 팟은 물리적 서버, vSphere 인프라, Horizon 7 서버, 공유 스토리지, 클러스터당 2,000대의 가상 데스크톱으로 구성된 5개의 클러스터로 구성됩니다.

표 4-13. 하나의 vCenter Server 를 사용하는 LAN 기반 Horizon 7 팟 예

항목	예
vSphere 클러스터	6(클러스터당 1개의 연결된 클론 풀을 갖춘 5개의 클러스터와 1개의 인프라 클러스터)
vCenter Server	1
View Composer	1(독립 실행형)
데이터베이스 서버	1(독립 실행형) MS SQL 서버 또는 Oracle 데이터베이스 서버
Active Directory 서버	1 또는 2
연결 서버 인스턴스	5
보안 서버	5
vLAN	8(데스크톱 풀 클러스터용 5개, 관리, VMotion, 인프라 클러스터용으로 각각 1개)

Cloud Pod 아키텍처 개요

Horizon 배포가 여러 데이터 센터에 걸쳐 이루어져야 하는 경우 복제된 연결 서버 인스턴스 그룹을 WAN, MAN(Metropolitan Area Network) 또는 LAN이 아닌 기타 네트워크에서 사용하려면 Cloud Pod 아키텍처 기능을 사용해야 합니다.

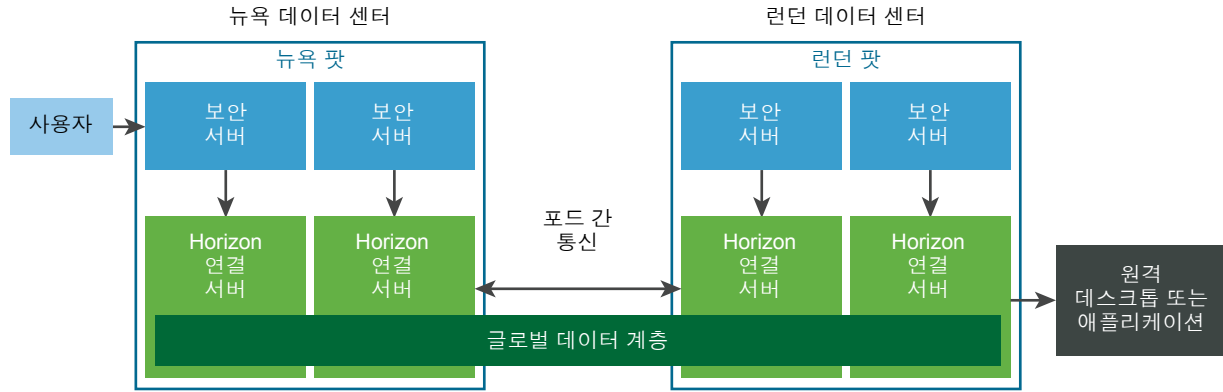
이 기능은 표준 Horizon 구성 요소를 사용하여 데이터 센터 간 관리, 전역적이고 유연한 사용자-데스크톱 매핑, 고가용성 데스크톱 및 재해 복구 기능을 제공합니다.

일반적인 Cloud Pod 아키텍처 토폴로지는 포드 페더레이션에서 함께 연결되는 두개 이상의 포드로 구성됩니다. 팟 페더레이션에는 특정한 제한이 따릅니다.

표 4-14. 팟 페더레이션 제한

개체	제한
총 세션	250,000
팟	50
포드당 세션	10,000
사이트	15
포드당 연결 서버 인스턴스	7
총 연결 서버 인스턴스	350

다음 다이어그램은 기본적인 Cloud Pod 아키텍처 토폴로지의 예를 보여 줍니다.



이 예제 토폴로지에서는 이전에 서로 다른 데이터 센터에 있던 두 개의 독립 실행형 포드가 서로 결합하여 단일 포드 페더레이션을 구성합니다. 이 환경의 최종 사용자는 뉴욕 데이터 센터의 연결 서버 인스턴스에 연결하여 런던 데이터 센터의 데스크톱 또는 애플리케이션을 수신할 수 있습니다.

Cloud Pod 아키텍처 기능은 IPv6 환경에서는 지원되지 않습니다.

자세한 내용은 Horizon 7에서 Cloud Pod 아키텍처 관리 문서를 참조하십시오.

팟에서 다중 vCenter Server를 사용할 경우의 장점

500대 이상의 데스크톱을 수용하는 Horizon 7 운영 환경을 설계할 때 여러 인스턴스가 아닌 하나의 vCenter Server 인스턴스를 사용할지 여부와 관련하여 몇 가지 사항을 고려해야 합니다.

View 5.2부터 VMware는 단일 vCenter 5.1 이상 서버를 통해 단일 Horizon 7 포드 내에서 최대 10,000대의 데스크톱 가상 시스템 관리를 지원합니다. 단일 vCenter Server 인스턴스를 사용하여 10,000대의 가상 시스템을 관리하려면 먼저 다음 사항을 고려하십시오.

- 회사 유지 관리 창고의 지속 기간
- Horizon 7 구성 요소 장애 허용 역량
- 전원, 프로비저닝, 다시 맞춤 작업 빈도
- 인프라의 간소함

유지 관리 창고의 지속 기간

가상 시스템의 전원, 프로비저닝 및 유지 관리 작업에 대한 동시 설정은 vCenter Server 인스턴스에 따라 결정됩니다.

하나의 vCenter Server 인스턴스를 이용한 팟 설계

동시 설정은 전체 Horizon 7 팟에 대해 한 번에 대기열에 넣을 수 있는 작업 수를 결정합니다.

예를 들어 동시 프로비저닝 작업 수를 20으로 설정하고 팟에 하나의 vCenter Server 인스턴스만 있을 경우 작업 수가 20개가 넘는 데스크톱 풀이 있으면 프로비저닝 작업이 직렬화됩니다. 20개의 동시 작업이 동시에 대기한 후에, 다음 작업이 시작되기 전에 하나의 작업이 완료되어야 합니다. 대규모 Horizon 7 배포에서는 이러한 프로비저닝 작업이 오래 걸릴 수 있습니다.

여러 vCenter Server 인스턴스를 사용한 팟 설계

각 인스턴스는 20개의 가상 시스템을 동시에 프로비저닝할 수 있습니다.

하나의 유지 관리 기간에서 보다 많은 작업이 동시에 완료될 수 있도록 하려면 여러 vCenter Server 인스턴스(최대 5개)를 팻에 추가할 수 있으며, 개별 vCenter Server 인스턴스에서 관리하는 vSphere 클러스터에 여러 데스크톱 풀을 배포할 수 있습니다. vSphere 클러스터는 한 번에 하나의 vCenter Server 인스턴스에서만 관리될 수 있습니다. 전체 vCenter Server 인스턴스에서 동시성을 실현하려면 이에 따라 데스크톱 풀을 배포해야 합니다.

구성요소 장애가 허용되는 있는 역량

Horizon 7 팻에서 vCenter Server의 역할은 전원, 프로비저닝, 다시 맞춤(새로 고침, 재구성, 재조정) 작업을 제공하는 것입니다. 가상 시스템 데스크톱이 배포되고 전원이 켜지면 Horizon 7는 일반적인 작업 과정에서 vCenter Server를 사용하지 않게 됩니다.

각 vSphere 클러스터가 단일 vCenter Server 인스턴스에서 관리되어야 하므로 이 서버는 모든 Horizon 7 설계에서 단일 실패 지점을 나타냅니다. 각 View Composer 인스턴스에도 이러한 위험이 적용됩니다. 각 View Composer 인스턴스와 vCenter Server 인스턴스가 일대일로 매핑되기 때문입니다. 다음 제품 중 하나를 사용하면 vCenter Server 또는 View Composer 중단의 영향을 완화할 수 있습니다.

- VMware vSphere High Availability (HA)
- 타사 호환 페일오버 제품

중요 이러한 페일오버 전략 중 하나를 사용하려면 vCenter Server 인스턴스가 관리하는 클러스터의 일부가 되는 가상 시스템에 vCenter Server 인스턴스가 설치되어 있지 않아야 합니다.

vCenter Server 페일오버에 대한 이러한 자동화된 옵션 외에도, 새로운 가상 시스템 또는 물리적 서버에서 장애가 발생한 서버를 재구축하도록 선택할 수도 있습니다. 대부분의 주요 정보는 vCenter Server 데이터베이스에 저장됩니다.

팻 설계에서 하나 이상의 vCenter Server 인스턴스를 사용해야 하는지 여부를 결정하는 데 있어 위험 허용 능력은 중요한 요인입니다. 작업에서 모든 데스크톱의 전원 작업 및 다시 맞춤 작업과 같은 데스크톱 관리 작업을 동시에 수행할 수 있어야 할 경우 여러 vCenter Server 인스턴스를 배포하여 중단의 영향을 더 적은 수의 데스크톱으로 분산해야 합니다. 장기간 동안 관리 또는 프로비저닝 작업에 사용할 수 없는 데스크톱 환경을 허용할 수 있거나 수동 재구축 프로세스를 사용하도록 선택할 경우 팻에 대해 단일 vCenter Server 인스턴스를 배포할 수 있습니다.

전원, 프로비저닝, 다시 맞춤 작업 빈도

특정 가상 시스템 데스크톱 전원, 프로비저닝 및 다시 맞춤 작업은 관리자 작업을 통해서만 시작할 수 있으며, 일반적으로 예측 및 제어가 가능하고 설정된 유지 관리 기간으로만 제한할 수 있습니다. 다른 가상 시스템 데스크톱 전원 및 다시 맞춤 작업은 로그오프 시 새로 고침 또는 로그오프 시 일시 중단 설정 같은 사용자의 동작이나, 사용자가 작업하지 않는 기간 동안 유휴 ESXi 호스트의 전원을 끄기 위해 DPM(Distributed Power Management)을 사용하는 등의 스크립트 작업을 통해 트리거됩니다.

Horizon 7 설계 특성상, 사용자가 트리거하는 전원 및 다시 맞춤 작업이 필요하지 않을 경우 단일 vCenter Server 인스턴스가 적합할 수 있습니다. 사용자가 트리거하는 전원 및 다시 맞춤 작업의 빈도가 높지 않다면 작업 대기열이 길게 누적되지 않으므로 Horizon 연결 서버가 vCenter Server에서 정의된 동시 설정 제한 내에 요청한 작업을 완료할 때까지 대기하는 시간이 초과되지 않습니다.

많은 고객들이 부동 풀을 배포하는 것을 선택하며 로그오프 시 새로 고침 설정을 사용하여 기존 세션의 오래된 데이터가 없는 데스크톱을 지속적으로 전송하고 있습니다. 오래된 데이터의 예로는 pagefile.sys 또는 Windows temp 파일의 언클레임드 메모리 페이지가 포함됩니다. 부동 풀은 데스크톱을 알려진 클린 상태로 자주 재설정하여 맬웨어의 영향을 최소화할 수도 있습니다.

일부 고객은 vSphere DRS(Distributed Resources Scheduler)가 실행 중인 가상 시스템을 최소한의 ESXi 호스트로 통합할 수 있도록, Horizon 7가 사용되고 있지 않은 데스크톱의 전원을 끄도록 구성함으로써 전기 사용량을 줄이고 있습니다. VMware Distributed Power Management는 이후 유휴 호스트의 전원을 차단합니다. 이러한 시나리오에서 여러 vCenter Server 인스턴스는 필요한 높은 빈도의 전원 및 다시 맞춤 작업을 효율적으로 수용하여 작업 시간 초과를 방지할 수 있습니다.

인프라의 간소함

대규모 Horizon 7 설계의 단일 vCenter Server 인스턴스는 한 곳에서 골든 마스터 이미지와 상위 가상 시스템을 관리하도록 지원하고, Horizon Administrator 콘솔 보기와 일치하는 단일 vCenter Server 보기를 제공하고, 운영 백엔드 데이터베이스 및 데이터베이스 서버 수를 줄이는 등 여러 가지 뛰어난 이점을 제공합니다. 단일 vCenter Server 인스턴스는 여러 인스턴스에 비해 재해 복구 계획이 보다 간소합니다. 상위 가상 시스템 이미지 관리로 인한 추가 관리 오버헤드와 필요한 인프라 구성 요소 수 증가와 같은 단점과 비교하여, 유지 관리의 지속 기간과 전원 및 다시 맞춤 작업의 빈도와 같은 다중 vCenter Server 인스턴스의 장점을 가중시켜야 합니다.

하이브리드 접근법을 통하여 설계에서 혜택을 얻을 수 있습니다. 단일 vCenter Server 인스턴스로 매우 크고 상당히 정적인 풀을 관리하도록 선택하거나 여러 vCenter Server 인스턴스로 좀 더 작고 보다 동적인 여러 데스크톱 풀을 관리하도록 선택할 수 있습니다. 기존의 대형 팟을 업그레이드하기 위한 최선의 전략은 먼저 기존 팟의 VMware 소프트웨어 구성 요소를 업그레이드하는 것입니다. 팟 설계를 변경하기 전에 최신 버전의 전원, 프로비저닝 및 다시 맞춤 작업에 대한 개선 영향을 판단한 후 데스크톱 풀의 크기를 늘리고 실험하여 더 적은 수의 vCenter Server 인스턴스에 대해 보다 큰 데스크톱 풀을 사용할 수 있는 적절한 균형을 찾으십시오.

보안 기능 계획

Horizon 7는 강력한 네트워크 보안을 통해 중요한 기업 데이터를 보호합니다. 보안을 추가한 경우 Horizon 7에 특정 타사 사용자 인증 솔루션을 통합하고 보안 서버를 사용하고 제한된 권한 기능을 구현할 수 있습니다.

중요 Horizon 6 버전 6.2 이상 릴리스에서는 FIPS(Federal Information Processing Standard) 140-2 규격 알고리즘을 사용한 암호화 작업을 수행할 수 있습니다. Horizon 7을 FIPS 모드에서 설치하면 이러한 알고리즘을 사용하도록 설정할 수 있습니다. 모든 기능이 FIPS 모드에서 지원되는 것은 아닙니다. 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 클라이언트 연결 이해
- 사용자 인증 방법 선택
- 원격 데스크톱 액세스 제한
- 그룹 정책 설정을 사용하여 원격 데스크톱 및 애플리케이션 보안 유지
- 스마트 정책 사용
- 보안 클라이언트 시스템에 모범 사례 구현
- 관리자 역할 할당
- 보안 서버 사용 준비
- 통신 프로토콜 이해

클라이언트 연결 이해

Horizon Client 및 Horizon Administrator는 보안 HTTPS 연결을 통해 Horizon 연결 서버 호스트와 통신합니다. 연결 서버의 서버 인증서 관련 정보는 클라이언트와 서버 간 TLS 핸드셰이크 과정에서 클라이언트로 전달됩니다.

사용자 인증과 원격 데스크톱 및 애플리케이션 선택에 사용되는 초기 Horizon Client 연결은 사용자가 Horizon Client를 열고 연결 서버, 보안 서버 또는 Unified Access Gateway 호스트의 FQDN(정규화된 도메인 이름)을 제공하면 생성됩니다. Horizon Administrator 연결은 관리자가 웹 브라우저에 Horizon Administrator URL을 입력할 때 생성됩니다.

기본 TLS 서버 인증서는 연결 서버 설치 중 생성됩니다. 기본적으로 TLS 클라이언트는 Horizon Administrator와 같은 보안 페이지를 방문할 때 이 인증서를 제공받습니다.

테스트를 위해 기본 인증서를 사용할 수 있지만 가능한 한 빨리 자신의 인증서로 대체해야 합니다. 기본 인증서는 상업용 인증 기관(CA)에 의해 서명되지 않았습니니다. 비공인 인증서를 사용할 경우 신뢰할 수 없는 당사자가 서버로 가장하여 트래픽을 인터셉트할 수 있습니다.

■ PCoIP 및 Blast 보안 게이트웨이를 사용한 클라이언트 연결

클라이언트가 VMware의 PCoIP 또는 Blast Extreme 디스플레이 프로토콜로 원격 데스크톱 또는 애플리케이션에 연결하는 경우 Horizon Client는 Horizon 연결 서버 인스턴스, 보안 서버 또는 Unified Access Gateway 장치의 해당 보안 게이트웨이 구성 요소에 두 번째 연결을 설정할 수 있습니다. 이 연결은 인터넷에서 원격 데스크톱 및 애플리케이션에 액세스할 때 필요한 보안 및 연결 수준을 제공합니다.

■ Microsoft RDP로 터널링된 클라이언트 연결

사용자가 Microsoft RDP 디스플레이 프로토콜을 사용하여 원격 데스크톱에 연결할 때 Horizon Client는 Horizon 연결 서버 호스트에 보조 HTTPS 연결을 설정할 수 있습니다. 이 연결은 RDP 데이터 이동을 위한 터널을 제공하기 때문에 터널 연결이라고 합니다.

■ 클라이언트 직접 연결

관리자는 클라이언트 시스템과 게시된 애플리케이션 또는 데스크톱 가상 시스템 사이에 직접 원격 데스크톱 및 게시된 애플리케이션 세션을 설정하여 View 연결 서버 호스트를 우회하도록 Horizon 연결 서버 설정을 구성할 수 있습니다. 이러한 연결 유형을 클라이언트 직접 연결이라 부릅니다.

PCoIP 및 Blast 보안 게이트웨이를 사용한 클라이언트 연결

클라이언트가 VMware의 PCoIP 또는 Blast Extreme 디스플레이 프로토콜로 원격 데스크톱 또는 애플리케이션에 연결하는 경우 Horizon Client는 Horizon 연결 서버 인스턴스, 보안 서버 또는 Unified Access Gateway 장치의 해당 보안 게이트웨이 구성 요소에 두 번째 연결을 설정할 수 있습니다. 이 연결은 인터넷에서 원격 데스크톱 및 애플리케이션에 액세스할 때 필요한 보안 및 연결 수준을 제공합니다.

보안 서버 및 Unified Access Gateway 장치에는 다음과 같은 이점을 제공하는 PCoIP 보안 게이트웨이 구성 요소와 Blast 보안 게이트웨이 구성 요소가 포함됩니다.

- 확실히 인증된 사용자를 대변하는 원격 데스크톱 및 애플리케이션 트래픽만 기업 데이터 센터에 들어갈 수 있습니다.
- 사용자는 액세스 권한을 부여받은 리소스에만 액세스할 수 있습니다.
- PCoIP 보안 게이트웨이 연결에서는 PCoIP를 지원하고, Blast 보안 게이트웨이 연결에서는 Blast Extreme을 지원합니다. 두 가지 모두 비디오 디스플레이 패킷을 TCP가 아닌 UDP에 캡슐화하여 네트워크의 사용 효율을 높이는 고급 원격 디스플레이 프로토콜입니다.
- PCoIP 및 Blast Extreme 보안에는 기본적으로 AES-128 암호화를 사용합니다. 하지만 암호화 암호를 AES-256으로 변경할 수 있습니다.

- 네트워킹 구성 요소로 인해 디스플레이 프로토콜이 차단되지 않는 한 VPN은 필요 없습니다. 예를 들어 호텔 객실 안에서 원격 데스크톱 또는 애플리케이션에 액세스하려고 하면 호텔에서 사용하는 프록시가 UDP 패킷을 전달하도록 구성되어 있지 않음을 알 수 있습니다.

자세한 내용은 [DMZ 기반 보안 서버의 방화벽 규칙](#)의 내용을 참조하십시오.

보안 서버는 Windows Server 2008 R2 및 Windows Server 2012 R2 운영 체제에서 실행되며 64비트 아키텍처를 완전히 활용합니다. 이 보안 서버는 또한 AESNI(AES New Instruction)를 지원하는 Intel 프로세서를 사용하여 암호화와 암호 해독 성능을 고도로 최적화합니다.

Unified Access Gateway 가상 장치에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성을 참조하십시오.

Microsoft RDP로 터널링된 클라이언트 연결

사용자가 Microsoft RDP 디스플레이 프로토콜을 사용하여 원격 데스크톱에 연결할 때 Horizon Client는 Horizon 연결 서버 호스트에 보조 HTTPS 연결을 설정할 수 있습니다. 이 연결은 RDP 데이터 이동을 위한 터널을 제공하기 때문에 터널 연결이라고 합니다.

터널 연결의 이점은 다음과 같습니다.

- RDP 데이터는 HTTPS를 통해 터널링되고 SSL을 사용하여 암호화됩니다. 이 강력한 보안 프로토콜은 다른 보안 웹 사이트에서 제공된 보안(예: 온라인 बैंकिंग 및 신용 카드 결제에 사용)과 일치합니다.
- 클라이언트는 전체 프로토콜 오버헤드를 줄이는 단일 HTTPS 연결을 통해 여러 데스크톱에 액세스할 수 있습니다.
- Horizon 7가 HTTPS 연결을 관리하기 때문에 기본 프로토콜의 신뢰성이 눈에 띄게 향상됩니다. 사용자의 네트워크 연결이 임시로 끊긴 경우 네트워크 연결이 복원되어 사용자가 다시 연결하고 다시 로그인할 필요 없이 RDP 연결이 자동으로 재개된 후 HTTP 연결이 재설정됩니다.

연결 서버 인스턴스의 표준 배포의 경우 HTTPS 보안 연결은 연결 서버에서 종료됩니다. DMZ 배포의 경우 HTTPS 보안 연결은 보안 서버 또는 Unified Access Gateway 장치에서 종료됩니다. DMZ 배포 및 보안 서버에 대한 자세한 내용은 [보안 서버 사용 준비](#)를 참조하십시오.

PCoIP 또는 Blast Extreme 디스플레이 프로토콜을 사용하는 클라이언트는 USB 리디렉션 및 MMR(멀티미디어 리디렉션) 가속에 터널 연결을 사용할 수 있지만, 다른 모든 데이터의 경우는 보안 서버나 Unified Access Gateway 장치에서 PCoIP는 PCoIP 보안 게이트웨이를 사용하고 Blast Extreme은 Blast 보안 게이트웨이를 사용합니다. 자세한 내용은 [PCoIP 및 Blast 보안 게이트웨이를 사용한 클라이언트 연결](#)의 내용을 참조하십시오.

Unified Access Gateway 가상 장치에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성을 참조하십시오.

클라이언트 직접 연결

관리자는 클라이언트 시스템과 게시된 애플리케이션 또는 데스크톱 가상 시스템 사이에 직접 원격 데스크톱 및 게시된 애플리케이션 세션을 설정하여 View 연결 서버 호스트를 우회하도록 Horizon 연결 서버 설정을 구성할 수 있습니다. 이러한 연결 유형을 클라이언트 직접 연결이라 부릅니다.

클라이언트 직접 연결을 사용하는 경우 사용자가 원격 데스크톱 및 게시된 애플리케이션을 인증하고 선택할 수 있도록 클라이언트와 연결 서버 호스트 사이에 HTTPS 연결이 계속 설정되지만 두 번째 HTTPS 연결(터널 연결)은 사용되지 않습니다.

직접 PCoIP 및 Blast Extreme 연결에서는 다음과 같은 기본 제공 보안 기능을 사용할 수 있습니다.

- 기본적으로 사용되는 AES(Advanced Encryption Standard) 암호화 지원과 IPsec(IP 보안)
- 타사 VPN 클라이언트 지원

Microsoft RDP 디스플레이 프로토콜을 사용하는 클라이언트의 경우에는 회사 네트워크 내에 배포하는 경우에만 클라이언트와 원격 데스크톱 간의 직접 연결을 권장합니다. 클라이언트 직접 연결을 사용할 경우 RDP 트래픽은 클라이언트와 데스크톱 가상 시스템 간의 연결을 통해 암호화되지 않은 상태로 전송됩니다.

사용자 인증 방법 선택

Horizon 7는 사용자의 기존 Active Directory 인프라를 사용해 사용자를 인증하고 관리합니다. 보안 추가를 위해 RSA SecurID 및 RADIUS와 같은 2 요소 인증 솔루션 및 스마트 카드 인증 솔루션과 Horizon 7를 통합할 수 있습니다.

■ Active Directory 인증

각 Horizon 연결 서버 인스턴스는 Active Directory 도메인에 가입되어 있으며 사용자는 Active Directory의 가입된 도메인에 대해 인증받습니다. 사용자는 또한 신뢰 계약이 있는 모든 추가 사용자 도메인에 대해서도 인증 받습니다.

■ 2 요소 인증 사용

사용자가 RSA SecurID 인증 또는 RADIUS(Remote Authentication Dial-In User Service) 인증을 사용해야만 하도록 Horizon 연결 서버 인스턴스를 구성할 수 있습니다.

■ 스마트 카드 인증

스마트 카드는 컴퓨터 칩이 내장된 소형 플라스틱 카드입니다. 많은 정부 기관 및 대기업에서는 스마트 카드를 사용하여 컴퓨터 네트워크에 액세스하는 사용자를 인증합니다. 미국 국방부에서 사용하는 한 가지 유형의 스마트 카드를 CAC(Common Access Card)라고 합니다.

■ Windows 기반 Horizon Client에서 제공하는 현재 사용자로 로그인 기능 사용

Windows용 Horizon Client에서는 사용자가 **옵션** 메뉴에서 **현재 사용자로 로그인**을 선택하면 클라이언트 시스템에 로그인할 때 입력했던 자격 증명을 사용해 Horizon 연결 서버 인스턴스와 원격 데스크톱에 대해 사용자를 인증합니다. 추가 사용자 인증은 필요하지 않습니다.

Active Directory 인증

각 Horizon 연결 서버 인스턴스는 Active Directory 도메인에 가입되어 있으며 사용자는 Active Directory의 가입된 도메인에 대해 인증받습니다. 사용자는 또한 신뢰 계약이 있는 모든 추가 사용자 도메인에 대해서도 인증 받습니다.

예를 들어 연결 서버 인스턴스가 도메인 A의 구성원이고 도메인 A와 도메인 B 간에 신뢰 계약이 존재하면 도메인 A와 도메인 B 사용자 모두 Horizon Client에서 연결 서버 인스턴스에 연결할 수 있습니다.

마찬가지로 혼합 도메인 환경에서 도메인 A와 MIT Kerberos 영역 간에 신뢰 계약이 존재하면 Kerberos 영역의 사용자는 Horizon Client에서 연결 서버 인스턴스에 연결할 때 Kerberos 영역 이름을 선택할 수 있습니다.

사용자와 그룹을 다음 Active Directory 도메인에 배치할 수 있습니다.

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

연결 서버는 호스트가 있는 도메인부터 신뢰 관계를 탐색하여 액세스할 수 있는 도메인을 확인합니다. 규모가 작고 서로 잘 연결되어 있는 도메인 집합의 경우 연결 서버는 신속하게 도메인 전체 목록을 확인할 수 있지만 도메인 수가 증가하거나 도메인 간의 연결성이 떨어질수록 확인하는 데 더 많은 시간이 걸립니다. 목록에는 사용자가 원격 데스크톱 및 애플리케이션에 로그인할 때 사용자에게 제공하기 원하는 도메인이 포함될 수도 있습니다.

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

기존 Active Directory 운영 절차를 통해 로그인 허용 시간 제한, 암호 만료 날짜 설정 등과 같은 정책을 처리할 수 있습니다.

2 요소 인증 사용

사용자가 RSA SecurID 인증 또는 RADIUS(Remote Authentication Dial-In User Service) 인증을 사용해야만 하도록 Horizon 연결 서버 인스턴스를 구성할 수 있습니다.

- RADIUS 지원은 다양한 대체 2 요소 토큰 기반 인증 옵션을 제공합니다.
- 또한 Horizon 7는 타사 솔루션 공급자가 고급 인증 확장을 Horizon 7에 통합할 수 있는 개방형 표준 확장 인터페이스를 제공합니다.

RSA SecurID 및 RADIUS와 같은 2 요소 인증 솔루션은 별도의 서버에 설치되어 인증 관리자와 함께 작동하므로 그러한 서버가 연결 서버 호스트에 액세스할 수 있도록 구성해야 합니다. 예를 들어, RSA SecurID를 사용할 경우 인증 관리자는 RSA 인증 관리자가 됩니다. RADIUS를 사용할 경우 인증 관리자는 RADIUS 서버가 됩니다.

2 요소 인증을 사용하려면 각 사용자에게 인증 관리자에 등록된 RSA SecurID 토큰과 같은 토큰이 있어야 합니다. 2 요소 인증 토큰은 고정 간격으로 인증 코드를 생성하는 하드웨어 또는 소프트웨어의 일부입니다. 보통 인증을 수행하려면 PIN과 인증 코드를 알아야 합니다.

여러 연결 서버 인스턴스가 있는 경우, 일부 인스턴스에 2 요소 인증을 구성하고 나머지는 다른 사용자 인증 방법을 구성할 수 있습니다. 예를 들어 인터넷을 통해 회사 네트워크 외부에서 원격 데스크톱 및 애플리케이션에 액세스하는 사용자 전용으로 2 요소 인증을 구성할 수 있습니다.

Horizon 7는 RSA SecurID 준비 프로그램을 통해 인증되며 새 PIN 모드, 다음 토큰 코드 모드, RSA 인증 관리자 및 로드 밸런싱을 포함하여 SecurID 기능의 전 범위를 지원합니다.

스마트 카드 인증

스마트 카드는 컴퓨터 칩이 내장된 소형 플라스틱 카드입니다. 많은 정부 기관 및 대기업에서는 스마트 카드를 사용하여 컴퓨터 네트워크에 액세스하는 사용자를 인증합니다. 미국 국방부에서 사용하는 한 가지 유형의 스마트 카드를 CAC(Common Access Card)라고 합니다.

관리자는 스마트 카드 인증을 위해 개별 연결 서버 인스턴스를 사용하도록 설정할 수 있습니다. 스마트 카드 인증을 사용하도록 연결 서버 인스턴스를 설정하려면 일반적으로 truststore 파일에 루트 인증서를 추가한 후 연결 서버 설정을 수정해야 합니다.

스마트 카드 인증을 사용하는 클라이언트 연결을 포함하여 모든 클라이언트 연결은 TLS/SSL을 사용하도록 설정되어 있습니다.

스마트 카드를 사용하려면 클라이언트 시스템에 스마트 카드 미들웨어 및 스마트 카드 판독기가 있어야 합니다. 스마트 카드에 인증서를 설치하려면 등록 스테이션 역할을 하도록 컴퓨터를 설정해야 합니다.

특정 유형의 Horizon Client에서 스마트 카드를 지원하는지 여부에 대한 내용은

<https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>의 Horizon Client 설명서를 참조하십시오.

Windows 기반 Horizon Client 에서 제공하는 현재 사용자로 로그인 기능 사용

Windows용 Horizon Client에서는 사용자가 **옵션** 메뉴에서 **현재 사용자로 로그인**을 선택하면 클라이언트 시스템에 로그인할 때 입력했던 자격 증명을 사용해 Horizon 연결 서버 인스턴스와 원격 데스크톱에 대해 사용자를 인증합니다. 추가 사용자 인증은 필요하지 않습니다.

이 기능을 사용하려면 연결 서버 인스턴스와 클라이언트 시스템에 사용자 자격 증명에 저장되어 있어야 합니다.

- 연결 서버 인스턴스에서는 사용자 이름, 도메인, 선택적 UPN과 함께 사용자 자격 증명에 암호화되어 사용자 세션에 저장됩니다. 자격 증명은 인증 작업 수행 시 추가되고 세션 개체 삭제 시 제거됩니다. 사용자가 로그아웃하거나 세션 시간이 초과하거나 인증이 실패하면 세션 개체가 지워집니다. 세션 개체는 휘발성 메모리에 상주하며 Horizon LDAP 또는 디스크 파일에 저장되지 않습니다.
- 연결 서버 인스턴스에서 **현재 사용자로 로그인** 수락 설정을 사용하도록 설정하여 사용자가 Horizon Client의 **옵션** 메뉴에서 **현재 사용자로 로그인**을 선택할 때 제공된 사용자 ID 및 자격 증명 정보를 연결 서버 인스턴스가 수락하도록 합니다.

중요 이 설정을 사용하도록 설정하기 전에 보안 위험을 파악해야 합니다. Horizon 7 보안 문서에서 "사용자 인증에 대한 보안 관련 서버 설정"을 참조하십시오.

- 클라이언트 시스템에서는 사용자 자격 증명에 암호화되어 Horizon Client의 구성 요소인 인증 패키지에 있는 테이블에 저장됩니다. 자격 증명은 사용자가 로그인하면 테이블에 추가되고 사용자가 로그아웃하면 테이블에서 제거됩니다. 테이블은 휘발성 메모리에 상주합니다.

관리자는 Horizon Client 그룹 정책 설정을 사용하여 **옵션** 메뉴에 있는 **현재 사용자로 로그인** 설정의 사용 가능 여부를 제어하고 기본값을 지정합니다. 관리자는 또한 그룹 정책을 통해 사용자가 Horizon Client에서 **현재 사용자로 로그인**을 선택할 때 전달되는 사용자 ID 및 자격 증명 정보를 수락할 연결 서버 인스턴스를 지정합니다.

재귀 잠금 해제 기능은 사용자가 현재 사용자로 로그인 기능을 사용해서 연결 서버에 로그인한 후에 사용되도록 설정됩니다. 재귀 잠금 해제 기능은 클라이언트 시스템이 잠금 해제된 후에 모든 원격 세션의 잠금을 해제합니다. 관리자는 Horizon Client의 **클라이언트 시스템이 잠금 해제될 때 원격 세션 잠금 해제** 글로벌 정책 설정으로 재귀 잠금 해제 기능을 제어할 수 있습니다. Horizon Client에 대한 글로벌 정책 설정에 대한 자세한 내용은 [VMware Horizon Clients 설명서](#) 웹 페이지에서 Horizon Client 설명서를 참조하십시오.

현재 사용자로 로그인 기능은 다음과 같은 제한 사항이 있습니다.

- 연결 서버 인스턴스에 대해 스마트 카드 인증이 [필수]로 설정되어 있는 경우 사용자가 **현재 사용자로 로그인**을 선택하고 연결 서버 인스턴스에 연결하면 인증에 실패합니다. 이들 사용자는 연결 서버에 로그인할 때 스마트 카드와 PIN으로 재인증해야 합니다.
- 클라이언트가 로그인하는 시스템 시간과 연결 서버 호스트 시간이 동기화되어 있어야 합니다.
- 클라이언트 시스템에서 기본 **네트워크에서 이 컴퓨터 액세스** 사용자 권한 할당을 수정한 경우 VMware 기술 자료(KB) 문서 1025691에 따라 수정해야 합니다.
- 클라이언트 시스템은 기업 Active Directory 서버와 통신할 수 있어야 하며 캐시된 자격 증명을 인증에 사용하면 안 됩니다. 예를 들어 사용자가 기업 네트워크 외부에서 클라이언트 시스템으로 로그인할 경우, 캐시된 자격 증명이 인증에 사용됩니다. 사용자가 VPN 연결을 먼저 설정하지 않고 보안 서버 또는 연결 서버 인스턴스에 연결할 경우, 사용자에게 자격 증명을 묻는 메시지가 나타나며 현재 사용자로 로그인 기능이 작동하지 않습니다.

원격 데스크톱 액세스 제한

제한된 권한 기능을 사용하여 사용자가 연결하는 Horizon 연결 서버 인스턴스를 기반으로 원격 데스크톱 액세스를 제한할 수 있습니다.

제한된 권한을 사용하여 연결 서버 인스턴스에 하나 이상의 태그를 할당합니다. 그런 다음 데스크톱 풀을 구성할 때 데스크톱 풀에 액세스하려는 연결 서버 인스턴스 태그를 선택합니다. 태그가 지정된 연결 서버 인스턴스로 사용자가 로그인할 경우 일치하는 태그가 최소한 하나이거나 태그가 없는 해당 데스크톱 풀에만 액세스할 수 있습니다.

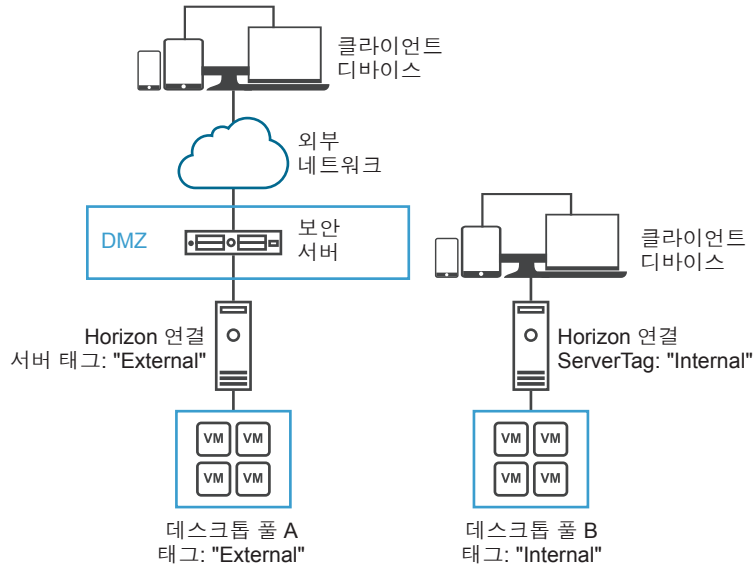
예를 들어 Horizon 7 배포에는 두 개의 연결 서버 인스턴스가 포함될 수 있습니다. 첫 번째 인스턴스는 내부 사용자를 지원합니다. 두 번째 인스턴스는 보안 서버와 연결되며 외부 사용자를 지원합니다. 외부 사용자가 특정 데스크톱에 액세스하지 못하도록 하기 위해 다음과 같이 제한된 권한을 설정할 수 있습니다.

- 내부 사용자를 지원하는 연결 서버 인스턴스에 "Internal" 태그를 할당합니다.
- 보안 서버와 연결되고 외부 사용자를 지원하는 연결 서버 인스턴스에 "External" 태그를 할당합니다.
- 내부 사용자만 액세스할 수 있는 데스크톱 풀에 "Internal" 태그를 할당합니다.

- 외부 사용자만 액세스할 수 있는 데스크톱 풀에 "External" 태그를 할당합니다.

외부 사용자는 External로 태그가 지정된 연결 서버를 통해 로그인하기 때문에 Internal로 태그가 지정된 데스크톱 풀을 볼 수 없으며 내부 사용자는 Internal로 태그가 지정된 연결 서버를 통해 로그인하기 때문에 External로 태그가 지정된 데스크톱 풀을 볼 수 없습니다. [그림 5-1](#)에서는 이러한 구성을 보여줍니다.

그림 5-1. 제한된 권한의 예



또한 제한된 권한을 사용하여 특정 연결 서버 인스턴스에 대해 구성하는 사용자 인증 방법을 기반으로 데스크톱 액세스를 제어할 수 있습니다. 예를 들어 스마트 카드를 사용하여 인증된 사용자만 사용할 수 있는 특정 데스크톱 풀을 만들 수 있습니다.

제한된 권한 기능은 태그 일치만 강제로 수행합니다. 네트워크 토폴로지를 디자인하여 특정 연결 서버 인스턴스를 통해 특정 클라이언트를 강제로 연결해야 합니다.

그룹 정책 설정을 사용하여 원격 데스크톱 및 애플리케이션 보안 유지

Horizon 7은 원격 데스크톱 및 애플리케이션 보안에 사용할 수 있는 보안 관련 그룹 정책 설정이 포함된 그룹 정책 관리 ADMX 템플릿을 포함합니다.

예를 들어 그룹 정책 설정을 사용하여 다음 작업을 수행할 수 있습니다.

- 사용자가 Windows용 Horizon Client에서 **현재 사용자로 로그인** 확인란을 선택할 때 전달된 사용자 ID 및 자격 증명 정보를 수락할 수 있는 연결 서버 인스턴스를 지정합니다.
- Horizon Client의 스마트 카드 인증을 위해 단일 로그온을 사용하도록 설정합니다.
- Horizon Client에서 서버 TLS 인증서 확인을 구성합니다.
- 사용자가 Horizon Client 명령줄 옵션을 사용하여 자격 증명 정보를 제공하지 못하도록 합니다.

- 비 Horizon Client 시스템이 RDP를 사용하여 원격 데스크톱에 연결하지 못하도록 합니다. 연결을 Horizon Client에서 관리하도록, 즉 사용자가 Horizon 7를 사용하여 원격 데스크톱에 연결해야 하도록 이 정책을 설정할 수 있습니다.

원격 데스크톱 및 Horizon Client 그룹 정책 설정 사용에 대한 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성의 내용을 참조하십시오.

스마트 정책 사용

스마트 정책을 사용하여 특정 원격 데스크톱의 USB 리디렉션, 가상 인쇄, 클립보드 리디렉션, 클라이언트 드라이브 리디렉션, PCoIP 디스플레이 프로토콜 기능의 동작을 제어하는 정책을 만들 수 있습니다. 스마트 정책을 사용하여 게시된 애플리케이션의 동작을 제어하는 정책을 생성할 수도 있습니다.

스마트 정책을 사용하면 특정 조건이 충족된 경우에만 적용되는 정책을 만들 수 있습니다. 예를 들어, 사용자가 회사 네트워크 외부에서 원격 데스크톱에 연결한 경우 클라이언트 드라이브 리디렉션 기능을 사용하지 않도록 설정하는 정책을 구성할 수 있습니다.

스마트 정책 기능에는 User Environment Manager가 필요합니다. 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성에서 스마트 정책에 대한 항목을 참조하십시오.

보안 클라이언트 시스템에 모범 사례 구현

보안 클라이언트 시스템에 이러한 모범 사례를 구현합니다.

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

Horizon 7가 제공하는 모든 보안 기능에 대한 간단한 참조를 확인하려면 Horizon 7 보안 문서를 확인하십시오.

관리자 역할 할당

Horizon 7 환경에서 주요 관리 작업은 Horizon Administrator를 이용할 수 있는 사용자와 이들 사용자에게 권한을 부여할 작업을 결정하는 것입니다.

Horizon Administrator에서 작업 수행 권한은 관리자 역할과 권한으로 구성되는 액세스 제어 시스템에서 관리합니다. 역할은 권한의 집합입니다. 권한은 사용자에게 데스크톱 풀에 대한 권한 부여 또는 구성 설정 변경 등과 같은 특정 작업을 수행할 수 있는 능력을 부여합니다. 또한 권한은 관리자가 Horizon Administrator에서 볼 수 있는 내용을 제어합니다.

관리자는 폴더를 생성해 데스크톱 풀을 세분화하고 Horizon Administrator의 다른 관리자에게 특정 데스크톱 풀 관리를 위임할 수 있습니다. 관리자는 사용자에게 폴더에 대한 역할을 할당하여 해당 폴더의 리소스에 대한 관리자 액세스를 구성합니다. 관리자는 역할을 할당 받은 폴더에 있는 리소스에만 액세스할 수 있습니다. 폴더에 대해 관리자가 가지고 있는 역할에 따라 해당 폴더의 리소스에 대한 관리자의 액세스 수준이 결정됩니다.

Horizon Administrator에는 미리 정의된 역할 집합이 포함되어 있습니다. 관리자는 또한 선택한 권한을 조합하여 사용자 지정 역할을 생성할 수 있습니다.

보안 서버 사용 준비

보안 서버는 Horizon 연결 서버 기능의 하위 집합을 실행하는 연결 서버의 특별한 인스턴스입니다. 보안 서버를 사용하여 인터넷과 내부 네트워크 사이에 추가 보안 계층을 제공할 수 있습니다.

중요 Horizon 6 버전 6.2 이상 릴리스에서는 보안 서버 대신 Unified Access Gateway 장치를 사용할 수 있습니다. Unified Access Gateway 장치는 강화된 가상 장치로 배포되며 보안 액세스를 제공하도록 사용자 지정된 Linux 장치를 기반으로 합니다. Unified Access Gateway 가상 장치에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성을 참조하십시오.

보안 서버는 DMZ에 상주하며 신뢰할 수 있는 네트워크 내 연결을 위한 프록시 호스트 역할을 합니다. 각 보안 서버는 연결 서버의 인스턴스와 연결되며 모든 트래픽을 해당 인스턴스로 전달합니다. 연결 서버 하나에 여러 보안 서버를 연결할 수 있습니다. 이 설계에서는 공용 인터넷에서 연결 서버 인스턴스를 보호하고 보안 서버를 통해 보호되지 않은 모든 세션을 강제로 요청하여 추가 보안 계층을 제공합니다.

DMZ 기반 보안 서버를 배포하려면 클라이언트를 DMZ 내 보안 서버와 연결시키는 방화벽에서 일부 포트를 열어야 합니다. 또한 내부 네트워크의 연결 서버 인스턴스 및 보안 서버 간 통신을 위해 포트를 구성해야 합니다. 특정 포트에 대한 자세한 내용은 [DMZ 기반 보안 서버의 방화벽 규칙](#)을 참조하십시오.

사용자는 내부 네트워크 내 임의의 연결 서버 인스턴스와 직접 연결할 수 있기 때문에 LAN 기반 배포에 보안 서버를 구현할 필요가 없습니다.

참고 보안 서버에는 PCoIP 보안 게이트웨이 구성 요소와 Blast 보안 게이트웨이 구성 요소가 포함되어 있으므로 PCoIP 또는 Blast Extreme 디스플레이 프로토콜을 사용하는 클라이언트에서 VPN이 아닌 보안 서버를 사용할 수 있습니다.

PCoIP를 사용하기 위한 VPN 설정에 대한 자세한 내용은

<http://www.vmware.com/products/view/resources.html>에 있는 기술 리소스 센터의 기술 파트너 리소스 섹션에서 제공하는 VPN 솔루션 개요를 참조하십시오.

보안 서버 배포의 모범 사례

DMZ에서 보안 서버를 운영할 때는 모범 사례 보안 정책 및 절차를 따르십시오.

VMware Infrastructure로 DMZ 가상화 백서에는 가상화된 DMZ에 대한 모범 사례의 예가 포함되어 있습니다. 본 백서의 다양한 권장 사항은 물리적 DMZ에도 적용할 수 있습니다.

프레임 브로드캐스트의 범위를 제한하려면 보안 서버에 연결된 Horizon 연결 서버 인스턴스를 격리된 네트워크에 배포해야 합니다. 이 토폴로지를 통해 악성 사용자가 내부 네트워크에서 보안 서버와 연결 서버 인스턴스 간의 통신을 모니터링하지 못하도록 방지할 수 있습니다.

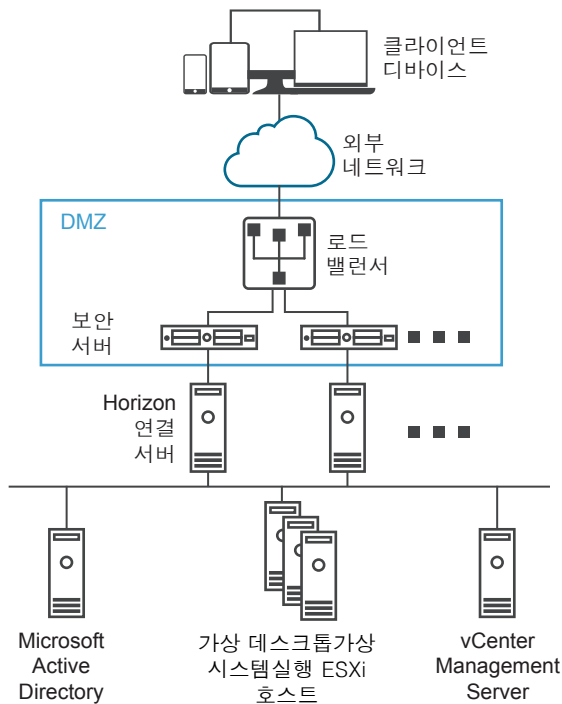
또는 네트워크 스위치의 고급 보안 기능을 사용해 보안 서버와 연결 서버 통신에 대한 악성 모니터링을 방지하고 ARP Cache Poisoning 등과 같은 모니터링 공격에 대비할 수 있습니다. 네트워크 장비에 대한 자세한 내용은 관리 설명서를 참조하십시오.

보안 서버 토폴로지

여러 가지의 보안 서버 토폴로지를 구현할 수 있습니다.

그림5-2에 나와 있는 토폴로지는 DMZ에 로드 밸런싱된 보안 서버 두 개가 포함된 고가용성 환경을 보여 줍니다. 보안 서버는 내부 네트워크 내 두 개의 Horizon 연결 서버 인스턴스와 통신합니다.

그림 5-2. DMZ의 로드 밸런싱된 보안 서버

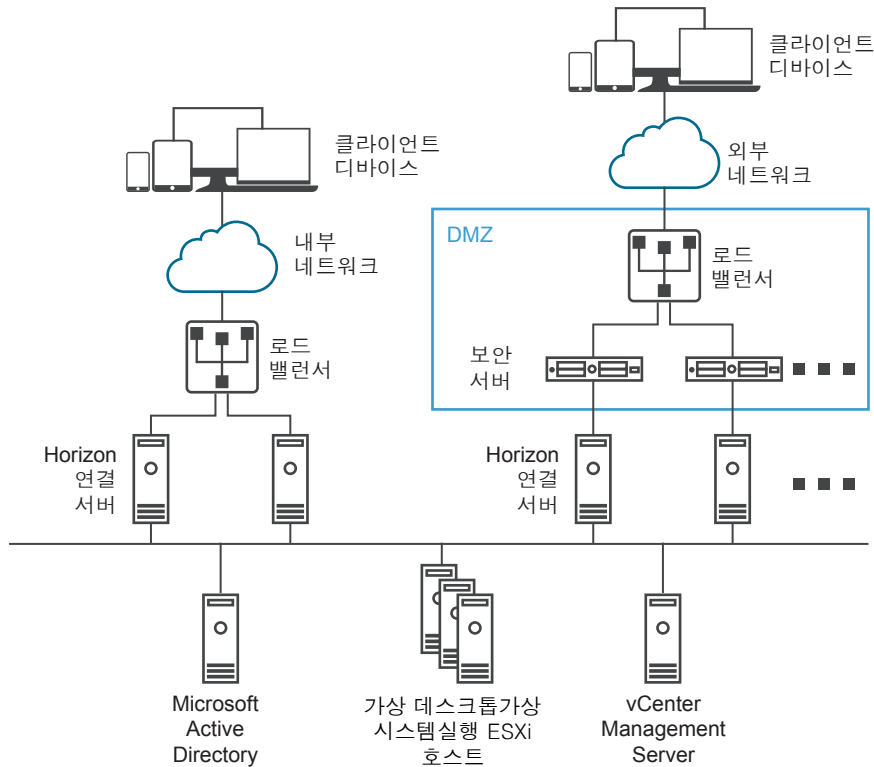


사용자가 회사 네트워크 외부에서 보안 서버에 연결하는 경우 인증에 성공해야 원격 데스크톱 및 애플리케이션에 액세스할 수 있습니다. DMZ 양쪽에 적절한 방화벽 규칙이 있는 경우 이 토폴로지는 인터넷에 위치한 클라이언트 디바이스에서 원격 데스크톱 및 애플리케이션에 액세스하는 데 적합합니다.

연결 서버의 각 인스턴스에 여러 보안 서버를 연결할 수 있습니다. 또한 표준 배포와 DMZ 배포를 조합하여 내부 사용자 및 외부 사용자에 대해 액세스를 제공할 수 있습니다.

그림5-3에 나와 있는 토폴로지는 연결 서버의 인스턴스 네 개가 하나의 그룹 역할을 하는 환경을 보여 줍니다. 내부 네트워크의 인스턴스는 내부 네트워크 사용자 전용이며 외부 네트워크의 인스턴스는 외부 네트워크 사용자 전용입니다. 보안 서버와 연결된 연결 서버 인스턴스를 RSA SecurID 인증에 사용할 수 있는 경우 RSA SecurID 토큰을 사용하여 모든 외부 네트워크 사용자를 인증해야 합니다.

그림 5-3. 다중 보안 서버



두 개 이상의 보안 서버를 설치할 경우 하드웨어 또는 소프트웨어 로드 밸런싱 솔루션을 구현해야 합니다. 연결 서버는 자체의 로드 밸런싱 기능을 제공하지 않습니다. 연결 서버는 타사 로드 밸런싱 솔루션과 함께 사용할 수 있습니다.

DMZ 기반 보안 서버의 방화벽

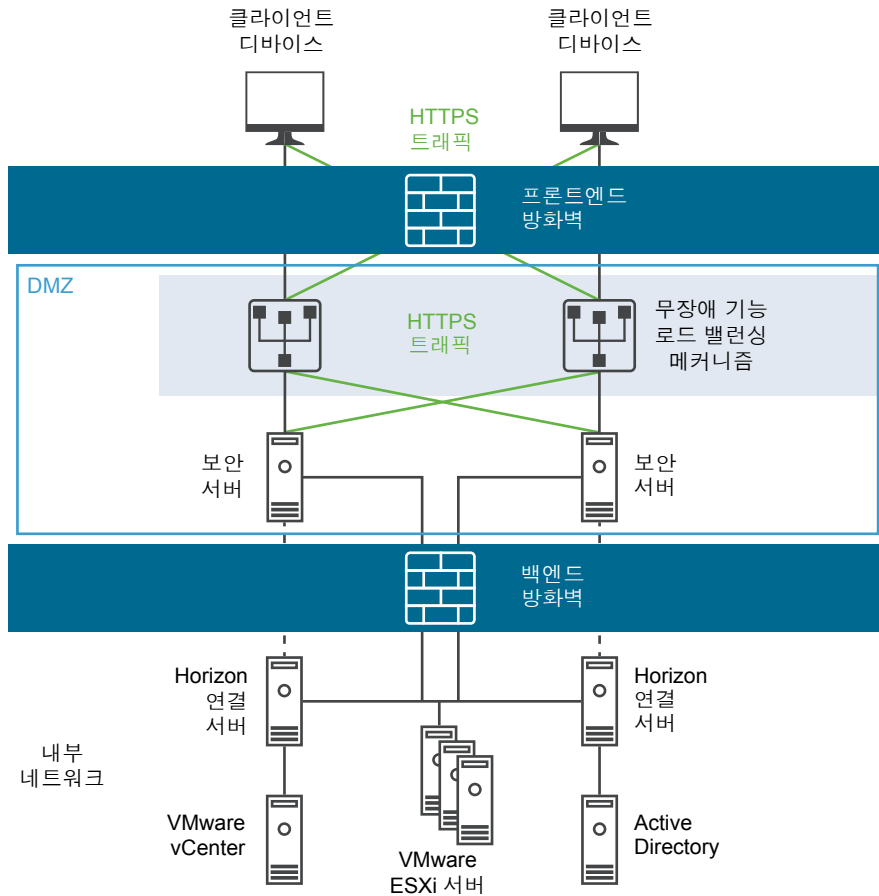
DMZ 기반 보안 서버를 배포할 때는 2개 방화벽을 포함해야 합니다.

- 외부 네트워크 지향 프론트엔드 방화벽은 DMZ와 내부 네트워크를 보호해야 합니다. 외부 네트워크 트래픽이 DMZ에 도달할 수 있도록 방화벽을 구성합니다.
- DMZ와 내부 네트워크 사이의 백엔드 방화벽은 두 번째 보안 계층을 제공하기 위해 필요합니다. DMZ 내에 있는 서비스에서 발생한 트래픽만 허용하도록 방화벽을 구성합니다.

방화벽 정책은 DMZ 서비스의 인바운드 통신을 철저하게 제어하여 내부 네트워크 손상 위험을 크게 줄입니다. 보안 서버를 구성하는 데 필요한 포트에 대한 자세한 내용은 Horizon 7 보안 문서를 참조하십시오.

다음 그림에서는 프론트엔드 및 백엔드 방화벽을 포함하는 구성의 예를 보여줍니다.

그림 5-4. 이중 방화벽 토폴로지



DMZ 기반 보안 서버의 방화벽 규칙

DMZ 기반 보안 서버는 프론트엔드와 백엔드 방화벽에 대해 특정 방화벽 규칙이 필요합니다. 설치 도중 기본적으로 특정 네트워크 포트에서 수신하도록 Horizon 7 서비스가 설정됩니다. 필요하다면, 조직 정책을 준수하거나 경합을 피하기 위해 사용되는 포트 번호를 변경할 수 있습니다.

중요 자세한 내용과 보안 권장 사항에 대해서는 Horizon 7 보안 문서를 참조하십시오.

프론트엔드 방화벽 규칙

외부 클라이언트 디바이스가 DMZ 내에 있는 보안 서버에 연결할 수 있도록 허용하려면 프론트엔드 방화벽에서 특정 TCP와 UDP 포트에 대한 트래픽을 허용해야 합니다. 표 5-1에는 프론트엔드 방화벽 규칙에 대한 요약이 나와 있습니다.

표 5-1. 프론트엔드 방화벽 규칙

소스	기본 포트	프로토콜	대상	기본 포트	참고
Horizon Client	TCP 임의	HTTP	보안 서버	TCP 80	(선택 사항) 외부 클라이언트 디바이스는 TCP 포트 80의 DMZ 내에 있는 보안 서버에 연결되어 HTTPS에 자동으로 연결됩니다. 사용자가 HTTPS가 아닌 HTTP로 연결할 수 있도록 허용하는 것과 관련된 보안 고려 사항에 대한 정보는 Horizon 7 보안 가이드를 참조하십시오.
Horizon Client	TCP 임의	HTTPS	보안 서버	TCP 443	외부 클라이언트 디바이스가 TCP 포트 443에서 DMZ 내에 있는 보안 서버에 연결하여 연결 서버 인스턴스 및 원격 데스크톱/애플리케이션과 통신합니다.
Horizon Client	TCP 임의 UDP 임의	PCoIP	보안 서버	TCP 4172 UDP 4172	외부 클라이언트 디바이스가 TCP 포트 4172 및 UDP 포트 4172에서 DMZ 내에 있는 보안 서버에 연결하여 PCoIP를 통해 원격 데스크톱 또는 애플리케이션과 통신합니다.
보안 서버	UDP 4172	PCoIP	Horizon Client	UDP 임의	보안 서버가 UDP 포트 4172에서 외부 클라이언트 디바이스로 PCoIP 데이터를 다시 보냅니다. 대상 UDP 포트는 수신된 UDP 패킷의 소스 포트입니다. 이러한 패킷에는 응답 데이터가 포함되므로 대개 이 트래픽에 대한 명시적 방화벽 규칙을 추가할 필요가 없습니다.
Horizon Client 또는 클라이언트 웹 브라우저	TCP 임의	HTTPS	보안 서버	TCP 8443 UDP 8443	외부 클라이언트 디바이스 및 외부 웹 클라이언트(HTML Access)는 HTTPS 포트 8443의 DMZ에 있는 보안 서버에 연결하여 원격 데스크톱과 통신합니다.

백엔드 방화벽 규칙

보안 서버에서 내부 네트워크에 있는 각 View 연결 서버 인스턴스와의 통신을 허용하려면 백엔드 방화벽에서 특정 TCP 포트에 대한 인바운드 트래픽을 허용해야 합니다. 원격 데스크톱 애플리케이션과 연결 서버 인스턴스가 서로 통신할 수 있도록 백엔드 방화벽 뒤에 있는 내부 방화벽을 유사하게 구성해야 합니다. 표 5-2는 백엔드 방화벽 규칙을 요약 설명합니다.

표 5-2. 백엔드 방화벽 규칙

소스	기본 포트	프로토콜	대상	기본 포트	참고
보안 서버	UDP 500	IPSec	연결 서버	UDP 500	보안 서버는 UDP 포트 500에서 연결 서버 인스턴스와 IPSec를 조정합니다.
연결 서버	UDP 500	IPSec	보안 서버	UDP 500	연결 서버 인스턴스는 UDP 포트 500에서 보안 서버에 응답합니다.
보안 서버	UDP 4500	NAT-T ISAKMP	연결 서버	UDP 4500	NAT가 보안 서버와 연결된 연결 서버 인스턴스 간에 사용될 때 필요합니다. 보안 서버는 UDP 포트 500을 사용하여 NAT를 탐색하고 IPsec 보안을 조정합니다.
연결 서버	UDP 4500	NAT-T ISAKMP	보안 서버	UDP 4500	NAT가 사용되면 연결 서버 인스턴스는 UDP 포트 4500에서 보안 서버에 응답합니다.

표 5-2. 백엔드 방화벽 규칙 (계속)

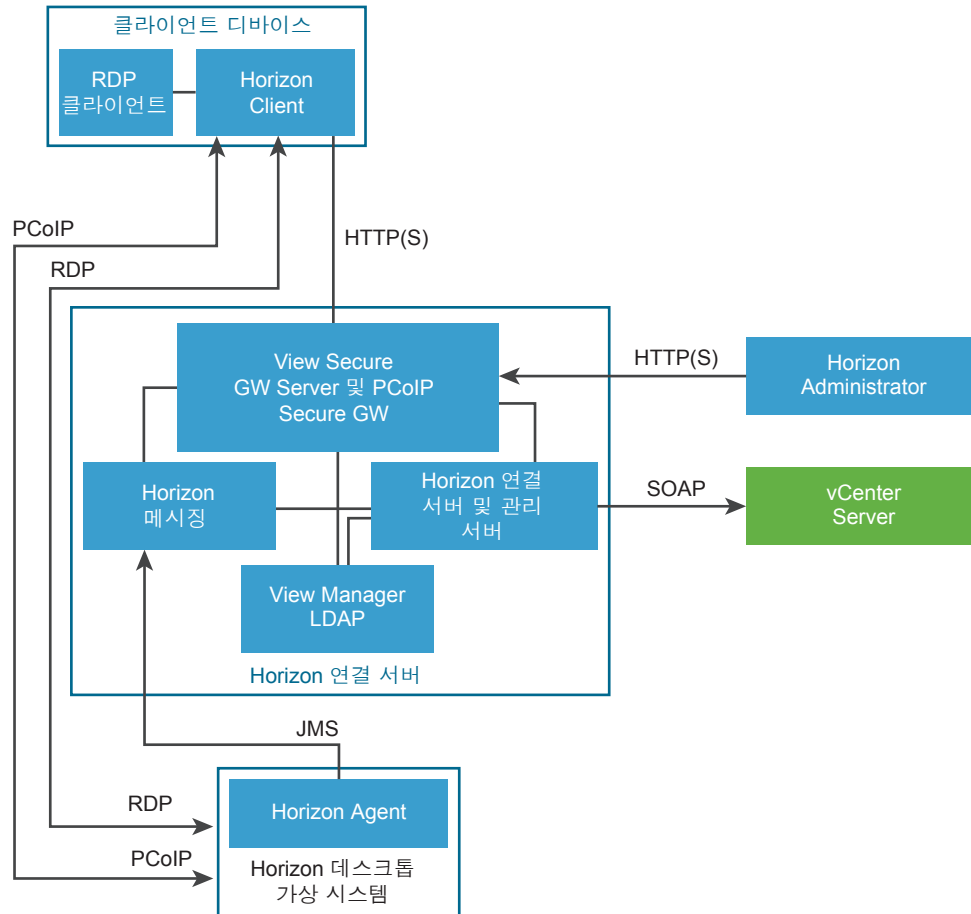
소스	기본 포트	프로토콜	대상	기본 포트	참고
보안 서버	TCP 임의	AJP13	연결 서버	TCP 8009	보안 서버는 TCP 포트 8009에서 연결 서버 인스턴스에 연결되어 외부 클라이언트 디바이스의 웹 트래픽을 전달합니다. IPSec를 사용하도록 설정하면 연결 후 AJP13 트래픽이 TCP 포트 8009를 사용하지 않습니다. 대신 NAT-T(UDP 포트 4500) 또는 ESP를 통해 전송됩니다.
보안 서버	TCP 임의	JMS	연결 서버	TCP 4001	보안 서버가 TCP 포트 4001의 연결 서버 인스턴스에 연결되어 JMS(Java Message Service) 트래픽을 교환합니다.
보안 서버	TCP 임의	JMS	연결 서버	TCP 4002	보안 서버가 TCP 포트 4002에서 연결 서버 인스턴스에 연결되어 보안 JMS(Java Message Service) 트래픽을 교환합니다.
보안 서버	TCP 임의	RDP	원격 데스크톱	TCP 3389	보안 서버가 TCP 포트 3389에서 원격 데스크톱에 연결하여 RDP 트래픽을 교환합니다.
보안 서버	TCP 임의	MMR	원격 데스크톱	TCP 9427	보안 서버가 TCP 포트 9427의 원격 데스크톱에 연결되어 MMR(멀티미디어 리디렉션) 및 클라이언트 드라이브 리디렉션에 관련된 트래픽을 수신합니다.
보안 서버	TCP 임의 UDP 55000	PCoIP	원격 데스크톱 또는 애플리케이션	TCP 4172 UDP 4172	보안 서버가 TCP 포트 4172 및 UDP 포트 4172에서 원격 데스크톱 및 애플리케이션에 연결하여 PCoIP 트래픽을 교환합니다.
원격 데스크톱 또는 애플리케이션	UDP 4172	PCoIP	보안 서버	UDP 55000	원격 데스크톱 및 애플리케이션이 UDP 포트 4172에서 보안 서버로 PCoIP 데이터를 다시 보냅니다. 대상 UDP 포트가 수신된 UDP 패킷의 소스 포트여서 이것이 응답 데이터일 때는 보통 이에 대한 명시적 방화벽 규칙을 추가할 필요가 없습니다.
보안 서버	TCP 임의	USB-R	원격 데스크톱	TCP 32111	보안 서버가 TCP 포트 32111에서 원격 데스크톱에 연결하여 외부 클라이언트 디바이스 및 원격 데스크톱 사이에서 USB 리디렉션 트래픽을 교환합니다.
보안 서버	TCP 또는 UDP 임의	Blast Extreme	원격 데스크톱 또는 애플리케이션	TCP 또는 UDP 22443	보안 서버가 TCP 및 UDP 포트 22443에서 원격 데스크톱 및 애플리케이션에 연결하여 Blast Extreme 트래픽을 교환합니다.
보안 서버	TCP 임의	HTTPS	원격 데스크톱	TCP 22443	HTML Access를 사용할 경우 보안 서버가 HTTPS 포트 22443에서 원격 데스크톱에 연결하여 Blast Extreme 에이전트와 통신합니다.
보안 서버		ESP	연결 서버		NAT 통과가 필요하지 않을 경우 AJP13 트래픽이 캡슐화됩니다. ESP는 IP 프로토콜 50이고 포트 번호는 지정되지 않습니다.
연결 서버		ESP	보안 서버		NAT 통과가 필요하지 않을 경우 AJP13 트래픽이 캡슐화됩니다. ESP는 IP 프로토콜 50이고 포트 번호는 지정되지 않습니다.

통신 프로토콜 이해

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

그림5-5에는 보안 서버가 구성되지 않았을 때 각 구성 요소가 통신에 사용하는 프로토콜이 나타나 있습니다. 즉, RDP용 보안 터널, Blast 보안 게이트웨이 및 PCoIP 보안 게이트웨이가 꺼져 있습니다. 이 구성은 일반 LAN 배포에 사용될 수 있습니다.

그림 5-5. 보안 서버가 없는 Horizon 6 및 Horizon 7 구성 요소 및 프로토콜



참고 이 그림은 PCoIP 또는 RDP를 사용하는 클라이언트의 직접 연결을 보여줍니다. 그러나 기본 설정은 PCoIP의 직접 연결 및 RDP의 터널 연결을 설정하는 것입니다.

각 프로토콜에 사용되는 기본 포트는 표5-3를 참조하십시오.

그림5-6에는 보안 서버가 구성되었을 때 각 구성 요소가 통신에 사용하는 프로토콜이 나타나 있습니다. 이 구성은 일반 WAN 배포에 사용될 수 있습니다.

그림 5-6. 보안 서버가 있는 Horizon 6 및 Horizon 7 구성 요소 및 프로토콜

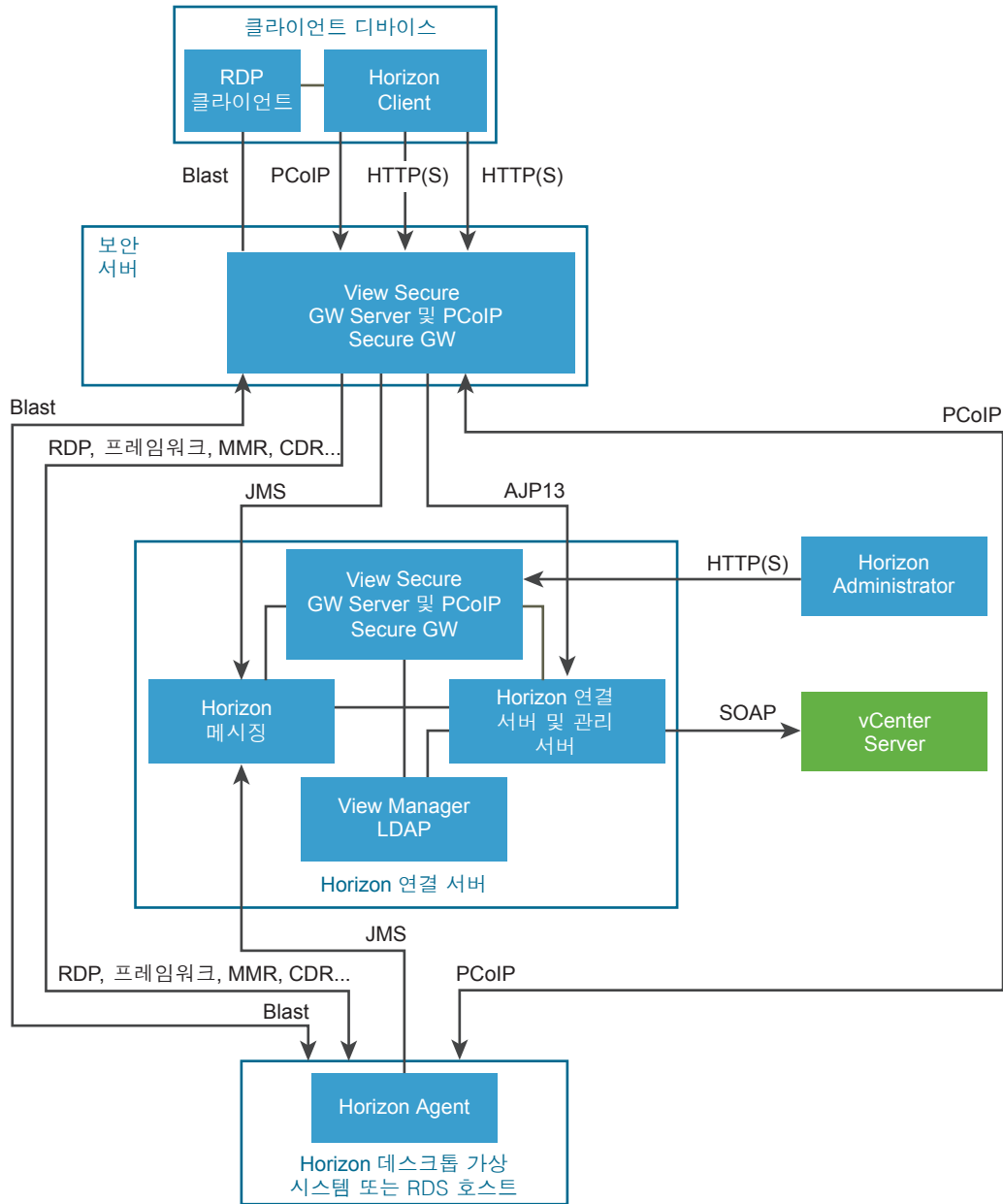


표 5-3에는 각 프로토콜에서 사용하는 기본 포트가 나열되어 있습니다. 필요하다면, 조직 정책을 준수하거나 경합을 피하기 위해 사용되는 포트 번호를 변경할 수 있습니다.

표 5-3. 기본 포트

프로토콜	포트
JMS	TCP 포트 4001 TCP 포트 4002
AJP13	TCP 포트 8009
참고	AJP13은 보안 서버 구성에만 사용됩니다.
HTTP	TCP 포트 80

표 5-3. 기본 포트 (계속)

프로토콜	포트
HTTPS	TCP 포트 443
MMR/CDR	멀티미디어 리디렉션 및 클라이언트 드라이브 리디렉션의 경우 TCP 포트 9427
RDP	TCP 포트 3389 참고 연결 서버 인스턴스가 클라이언트 직접 연결을 위해 구성된 경우 이러한 프로토콜은 클라이언트에서 원격 데스크톱으로 바로 연결되며 View Secure GW Server 구성 요소를 통해 터널링되지 않습니다.
SOAP	TCP 포트 80 또는 443
PCoIP	TCP 포트 4172 UDP 포트 4172, 50002, 55000
USB 리디렉션	TCP 포트 32111. 이 포트는 시간대 동기화에도 사용됩니다.
VMware Blast Extreme	TCP 포트 8443, 22443 UDP 포트 443, 8443, 22443
HTML Access	TCP 포트 8443, 22443

연결 서버 상호 통신용 TCP 포트

그룹에 포함된 연결 서버 인스턴스는 추가 TCP 포트를 사용하여 서로 통신합니다. 예를 들어 연결 서버 인스턴스는 포트 4100 또는 4101을 사용해 서로 JMSIR(JMS inter-router) 트래픽을 전송합니다. 일반적으로 그룹 내 연결 서버 인스턴스 간에는 방화벽을 사용하지 않습니다.

View Secure Gateway Server

View Secure Gateway Server는 클라이언트 시스템 및 보안 서버, Unified Access Gateway 장치 또는 연결 서버 인스턴스 간 보안 HTTPS 연결을 위한 서버 측 구성 요소입니다.

연결 서버, RDP, USB 및 MMR(멀티미디어 리디렉션)에 대한 터널 연결을 구성할 때 트래픽은 View 보안 게이트웨이 구성 요소를 통해 터널링됩니다. 클라이언트 직접 연결을 구성할 때 이러한 프로토콜은 클라이언트에서 원격 데스크톱으로 직접 연결되며 View Secure Gateway Server 구성 요소를 통해 터널링되지 않습니다.

참고 PCoIP 또는 Blast Extreme 디스플레이 프로토콜을 사용하는 클라이언트는 USB 리디렉션 및 MMR(멀티미디어 리디렉션) 가속에 터널 연결을 사용할 수 있지만, 다른 모든 데이터의 경우는 보안 서버나 Unified Access Gateway 장치에서 PCoIP는 PCoIP 보안 게이트웨이를 사용하고 Blast Extreme은 Blast 보안 게이트웨이를 사용합니다.

또한 View Secure Gateway Server는 사용자 인증 및 데스크톱/애플리케이션 선택 트래픽을 포함하여 클라이언트에서 연결 서버로 다른 웹 트래픽을 전달하는 역할을 합니다. 또한 View Secure Gateway Server는 Horizon Administrator 클라이언트 웹 트래픽을 관리 서버 구성 요소로 전달합니다.

Blast 보안 게이트웨이

보안 서버 및 Unified Access Gateway 장치에는 Blast 보안 게이트웨이 구성 요소가 포함되어 있습니다. Blast 보안 게이트웨이를 사용하도록 설정하는 경우 인증 후 Blast Extreme 또는 HTML Access를 사용하는 클라이언트에서 보안 서버나 Unified Access Gateway 장치에 대해 또 다른 보안 연결을 설정할 수 있습니다. 이 연결을 통해 클라이언트가 인터넷에서 원격 데스크톱 및 애플리케이션에 액세스할 수 있습니다.

Blast 보안 게이트웨이 구성 요소를 사용하도록 설정하면 Blast Extreme 트래픽이 보안 서버 또는 Unified Access Gateway 장치를 통해 원격 데스크톱 및 애플리케이션에 전달됩니다. Blast Extreme을 사용하는 클라이언트가 USB 리디렉션 기능 또는 MMR(멀티미디어 리디렉션) 가속도 사용하는 경우, View Secure Gateway 구성 요소를 사용하도록 설정하여 해당 데이터를 전달할 수 있습니다.

클라이언트 직접 연결을 구성하면 Blast Extreme 트래픽과 기타 트래픽이 클라이언트에서 원격 데스크톱 또는 애플리케이션으로 바로 이동합니다.

가정 또는 모바일 작업자와 같은 최종 사용자가 인터넷을 통해 데스크톱에 액세스하는 경우 보안 서버 또는 Unified Access Gateway 장치에서 필요한 보안 및 연결 수준을 제공하므로 VPN을 연결하지 않아도 됩니다. Blast 보안 게이트웨이 구성 요소는 확실히 인증된 사용자를 대변하는 원격 트래픽만 기업 데이터 센터에 들어갈 수 있도록 허용합니다. 최종 사용자는 액세스 권한을 부여받은 리소스에만 액세스할 수 있습니다.

Blast 보안 게이트웨이를 통해 작동하는 Blast 기본 클라이언트는 Blast 세션 TLS 연결이 Blast 보안 게이트웨이에 구성되어 있는 TLS 인증서로 인증될 것으로 예상합니다. 클라이언트의 Blast 연결 중에 다른 TLS 인증서가 확인되면 연결은 삭제되고 클라이언트는 인증서 지문 불일치를 보고합니다.

클라이언트를 클라이언트와 Blast 보안 게이트웨이 간에 배치된 TLS 중단 프록시에 연결하도록 선택하는 경우 클라이언트의 인증서 요구 사항을 충족하고, 프록시가 Blast 보안 게이트웨이의 인증서(및 개인 키) 사본을 제공하도록 정렬하여 지문 불일치 오류를 방지함으로써 클라이언트에서 Blast에 성공적으로 연결하도록 허용할 수 있습니다.

프록시에 Blast 보안 게이트웨이의 인증서를 복사하는 대신, 프록시에 자체 TLS 인증서를 제공한 후 클라이언트가 Blast 보안 게이트웨이의 인증서가 아닌 프록시의 인증서를 요구하고 수락하도록 Blast 보안 게이트웨이를 구성할 수 있습니다.

Unified Access Gateway Horizon 설정의 **Blast 프록시 인증서**에서 프록시 인증서를 업로드하여 Unified Access Gateway에서 Blast 보안 게이트웨이를 구성할 수 있습니다.

<https://docs.vmware.com/kr/Unified-Access-Gateway/index.html>에서 VMware Unified Access Gateway 배포 및 구성 문서를 참조하십시오.

참고 프록시 인증서만 업로드됩니다. 해당 개인 키는 Unified Access Gateway에 노출되지 않습니다.

PCoIP 보안 게이트웨이

보안 서버 및 Unified Access Gateway 장치에는 PCoIP 보안 게이트웨이 구성 요소가 포함되어 있습니다. PCoIP 보안 게이트웨이를 사용하도록 설정하는 경우 인증 후 PCoIP를 사용하는 클라이언트에서 보안 서버나 Unified Access Gateway 장치에 대해 또 다른 보안 연결을 설정할 수 있습니다. 이 연결을 통해 클라이언트가 인터넷에서 원격 데스크톱 및 애플리케이션에 액세스할 수 있습니다.

PCoIP 보안 게이트웨이 구성 요소를 사용하도록 설정하면 PCoIP 트래픽이 보안 서버 또는 Unified Access Gateway 장치를 통해 원격 데스크톱 및 애플리케이션에 전달됩니다. PCoIP를 사용하는 클라이언트가 USB 리디렉션 기능 또는 MMR(멀티미디어 리디렉션) 가속을 사용하는 경우, View Secure Gateway 구성 요소를 사용하도록 설정하여 해당 데이터를 전달할 수 있습니다.

클라이언트 직접 연결을 구성하면 PCoIP 트래픽과 기타 트래픽이 클라이언트에서 원격 데스크톱 또는 애플리케이션으로 바로 이동합니다.

가정 또는 모바일 작업자와 같은 최종 사용자가 인터넷을 통해 데스크톱에 액세스하는 경우 보안 서버 또는 Unified Access Gateway 장치에서 필요한 보안 및 연결 수준을 제공하므로 VPN을 연결하지 않아도 됩니다. PCoIP 보안 게이트웨이 구성 요소는 확실히 인증된 사용자를 대변하는 원격 트래픽만 기업 데이터 센터에 들어갈 수 있도록 허용합니다. 최종 사용자는 액세스 권한을 부여받은 리소스에만 액세스할 수 있습니다.

View LDAP

View LDAP는 View 연결 서버의 내장된 LDAP 디렉토리이며 모든 Horizon 7 구성 데이터의 구성 저장소입니다.

View LDAP에는 각 원격 데스크톱 및 애플리케이션, 액세스 가능한 각 원격 데스크톱, 함께 관리되는 여러 원격 데스크톱 및 Horizon 7 구성 요소 구성 설정을 나타내는 항목이 포함됩니다.

또한 View LDAP에는 다른 Horizon 7 구성 요소를 위한 자동화 및 알림 서비스를 제공하는 Horizon 7 플러그인 DLL 집합도 포함됩니다.

Horizon 메시징

Horizon 메시징 구성 요소는 Horizon Connection Server 구성 요소 간의 통신과 Horizon Agent 및 연결 서버 간의 통신을 위해 메시징 라우터를 제공합니다.

이 구성 요소는 Horizon 7의 메시징에 사용되는 JMS(Java Message Service) API를 지원합니다.

구성 요소 간의 메시지 유효성 검사에는 DSA 키를 사용합니다. 키 크기는 기본적으로 512비트이지만, FIPS 모드에서는 키 크기가 2048비트입니다.

참고 메시지 보안 모드가 **항상**으로 설정된 경우 SSL/TLS가 메시지당 암호화를 사용하는 대신 JMS 연결의 보안을 유지하는 데 사용됩니다. 항상된 메시지 보안 모드에서는 유효성 검사가 한 메시지 유형에만 적용됩니다. 항상된 메시지 모드에서는 키 크기를 2048비트로 높이는 것이 좋습니다. 키 크기가 성능과 확장성에 영향을 주기 때문에, 항상된 메시지 보안 모드를 사용하지 않는 경우에는 기본값인 512를 변경하지 않는 것이 좋습니다.

모든 키를 1024비트로 만들려면 첫 번째 연결 서버 인스턴스가 설치된 직후와 추가 서버 및 데스크톱이 생성되기 직전에 RSA 키 크기를 변경해야 합니다. 자세한 내용은 VMware 기술 자료(KB) 문서 1024431에 나와 있습니다.

Horizon 연결 서버의 방화벽 규칙

연결 서버 인스턴스와 보안 서버의 방화벽에서 특정 포트를 열어야 합니다.

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

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

표 5-4. Horizon 연결 서버 설치 중 열리는 포트

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

View Agent 또는 Horizon Agent 의 방화벽 규칙

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

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

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

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

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

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

표 5-5. View Agent 또는 Horizon Agent 설치 중 열리는 TCP 및 UDP 포트

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

표 5-5. View Agent 또는 Horizon Agent 설치 중 열리는 TCP 및 UDP 포트 (계속)

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

Active Directory의 방화벽 규칙

Horizon 7 환경과 Active Directory 서버 사이에 방화벽이 있으면 필요한 포트가 모두 열렸는지 확인하십시오.

예를 들어 View 연결 서버는 Active Directory Global Catalog와 LDAP(Lightweight Directory Access Protocol) 서버에 액세스할 수 있어야 합니다. 방화벽 소프트웨어에서 Global Catalog와 LDAP 포트를 차단하면 관리자는 사용자 권한 구성 시 문제에 부딪칠 수 있습니다.

방화벽을 통해 제대로 작동하기 위해 Active Directory용으로 열어야 하는 포트 정보는 사용하는 Active Directory 서버 버전의 Microsoft 설명서를 참조하십시오.

Horizon 7 환경 설정 단계 개요

Horizon 7을 설치하고 초기 배포 구성을 수행하려면 다음의 개괄적인 작업을 완료해야 합니다.

표 6-1. Horizon 7 설치 및 설정 확인 목록

단계	작업
1	Active Directory에 필요한 관리자 사용자 및 그룹을 설정하십시오. 지침: Horizon 7 설치 및 vSphere 설명서
2	아직 ESXi 호스트와 vCenter Server를 설치하고 설정하지 않았으면 지금 설치하고 설정합니다. 지침: VMware vSphere 설명서.
3	(선택 사항) 연결된 클론 데스크톱을 배포하려는 경우 View Composer를 vCenter Server 시스템 또는 별도의 서버에 설치합니다. View Composer 데이터베이스도 설치합니다. 지침: Horizon 7 설치 문서.
4	Horizon 연결 서버를 설치하고 설정합니다. 이벤트 데이터베이스도 설치합니다. 지침: Horizon 7 설치 문서.
5	전체 클론 데스크톱 풀의 템플릿 또는 연결된 클론 데스크톱 풀이나 인스턴트 클론 데스크톱 풀의 상위 풀로 사용할 수 있는 가상 시스템을 하나 이상 만듭니다. 지침: Horizon 7에서 가상 데스크톱 설정.
6	(선택 사항) RDS 호스트를 설정하고 최종 사용자에게 원격으로 제공할 애플리케이션을 설치합니다. 지침: Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정.
7	데스크톱 풀이나 애플리케이션 풀 또는 둘 다를 생성합니다. 지침: Horizon 7에서 가상 데스크톱 설정 및 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정.
8	데스크톱에 대한 사용자 액세스를 제어합니다. 지침: Horizon 7에서 원격 데스크톱 기능 구성.
9	최종 사용자의 시스템에 Horizon Client를 설치하고 최종 사용자가 자신의 원격 데스크톱 및 애플리케이션에 액세스할 수 있도록 합니다. 지침: Horizon Client 설명서(https://docs.vmware.com/kr/VMware-Horizon-Client/index.html)
10	(선택 사항) 특정 인벤토리 개체 및 설정에 액세스할 수 있는 여러 레벨을 허용할 수 있도록 추가로 관리자를 만들고 구성합니다. 지침: Horizon 7 관리 문서.
11	(선택 사항) Horizon 7 구성 요소, 데스크톱/애플리케이션 풀 및 최종 사용자의 동작을 제어하는 정책을 구성합니다. 지침: Horizon 7에서 원격 데스크톱 기능 구성.

표 6-1. Horizon 7 설치 및 설정 확인 목록 (계속)

단계	작업
12	(선택 사항) 사용자가 데스크톱에 로그인할 때마다 개인 데이터 및 설정에 대한 액세스를 제공하는 Horizon Persona Management를 구성합니다. 지침: Horizon 7에서 가상 데스크톱 설정.
13	(선택 사항) 보안 추가를 위해 스마트 카드 인증 또는 RADIUS 2 요소 인증 솔루션을 통합합니다. 지침: Horizon 7 관리 문서.