VMware View 아키텍처 계획

View 5.1
View Manager 5.1
View Composer 3.0

이 문서는 새 버전으로 교체되기 전까지 나열된 각 제품 버전 및 모든 이후 버전을 지원합니다. 이 문서에 대한 최신 버전을 확인하려면 http://www.vmware.com/support/pubs 를 참조하십시오.

KO-000729-00

vmware®

VMware 웹 사이트 (http://www.vmware.com/kr/support) 에서 최신 기술 문서를 확인할 수 있습니다.
또한 VMware 웹 사이트에서 최신 제품 업데이트를 제공합니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com 으로 사용자 의견을 보내주십시오.

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

목차

VMware View 아키텍처 계획 5

1 VMware View 소개 7
VMware View 사용의 장점 7
VMware View 기능 9
VMware View 구성 요소를 서로 맞추는 방법 11
VMware View 통합 및 사용자 지정 14

2 풍부한 사용자 환경 계획 17
기능 지원 표 17
디스플레이 프로토콜 선택 19
View 개인 설정 관리를 사용하여 사용자 데이터 및 설정 유지 21
Local Mode 에서 View 데스크톱 사용 시 장점 23
로컬 컴퓨터에 연결된 USB 디바이스에 액세스 25
View 데스크톱에서 인쇄 25
View 데스크톱에 멀티미디어 스트리밍 26
단일 로그온을 사용한 View 데스크톱 로그인 26
View 데스크톱에 다중 모니터 사용 26

3 한 곳에서 데스크톱 풀 관리 29
데스크톱 풀의 장점 29
스토리지 요구 사항 축소 및 관리 30
애플리케이션 프로비저닝 32
Active Directory GPO 를 사용한 사용자 및 데스크톱 관리 34

4 아키텍처 설계 요소 및 계획 지침 35
가상 시스템 요구 사항 35
VMware View ESX/ESXi 노드 40
특정 작업자 유형의 데스크톱 풀 41
데스크톱 가상 시스템 구성 45
vCenter 및 View Composer 가상 시스템 구성과 데스크톱 풀 최대값 46
View Connection Server 최대값 및 가상 시스템 구성 47
View 전송 서버 가상 시스템 구성 및 스토리지 48
vSphere 클러스터 49
VMware View 빌드 블록 50
VMware View 팟 54

5 보안 기능 계획 57
클라이언트 연결 이해 57
사용자 인증 방법 선택 60

View 데스크톱 액세스 제한 62
그룹 정책 설정을 사용한 View 데스크톱 보안 64
보안 클라이언트 시스템에 모범 사례 구현 64
관리자 역할 할당 64
보안 서버 사용 준비 65
VMware View 통신 프로토콜 이해 70

6 VMware View 환경 설정 단계 개요 77

색인 79

VMware View 아키텍처 계획

*VMware View 아키텍처 계획*에서는 VMware® View™의 주요 기능과 배포 옵션을 설명하고 운영 환경에서 일반적으로 VMware View 구성 요소를 설정하는 방법에 대한 개요 등을 소개합니다.

이 설명서에서 다음 질문에 대한 답변을 확인할 수 있습니다.

- VMware View가 문제를 해결해줍니까?
- VMware View 솔루션이 기업에서 구축하기에 적당하고 비용 효율적입니까?

이 설명서에서는 사용자의 VMware View 설치를 보호하기 위한 보안 기능에 대해서도 논의합니다.

대상

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

1 VMware View 소개

IT 부서는 VMware View 를 사용해 데이터 센터에서 가상 데스크톱을 실행하고 직원들에게 데스크톱을 관리 서비스로서 전달할 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.

이 장에서는 다음 주제에 대해 설명합니다.

- "VMware View 사용의 장점," (7 페이지)
- "VMware View 기능," (9 페이지)
- "VMware View 구성 요소를 서로 맞추는 방법," (11 페이지)
- "VMware View 통합 및 사용자 지정," (14 페이지)

VMware View 사용의 장점

VMware View 데스크톱으로 기업 데스크톱을 관리하면 신뢰성과 보안, 하드웨어 독립성, 편리성 등을 개선할 수 있습니다.

신뢰성 및 보안

VMware vSphere 와 통합하고 서버, 스토리지, 네트워킹 리소스를 가상화하면 가상 데스크톱을 중앙 집중화할 수 있습니다. 데이터 센터 서버에 데스크톱 운영 체제와 애플리케이션을 배치하면 다음과 같은 장점을 얻을 수 있습니다.

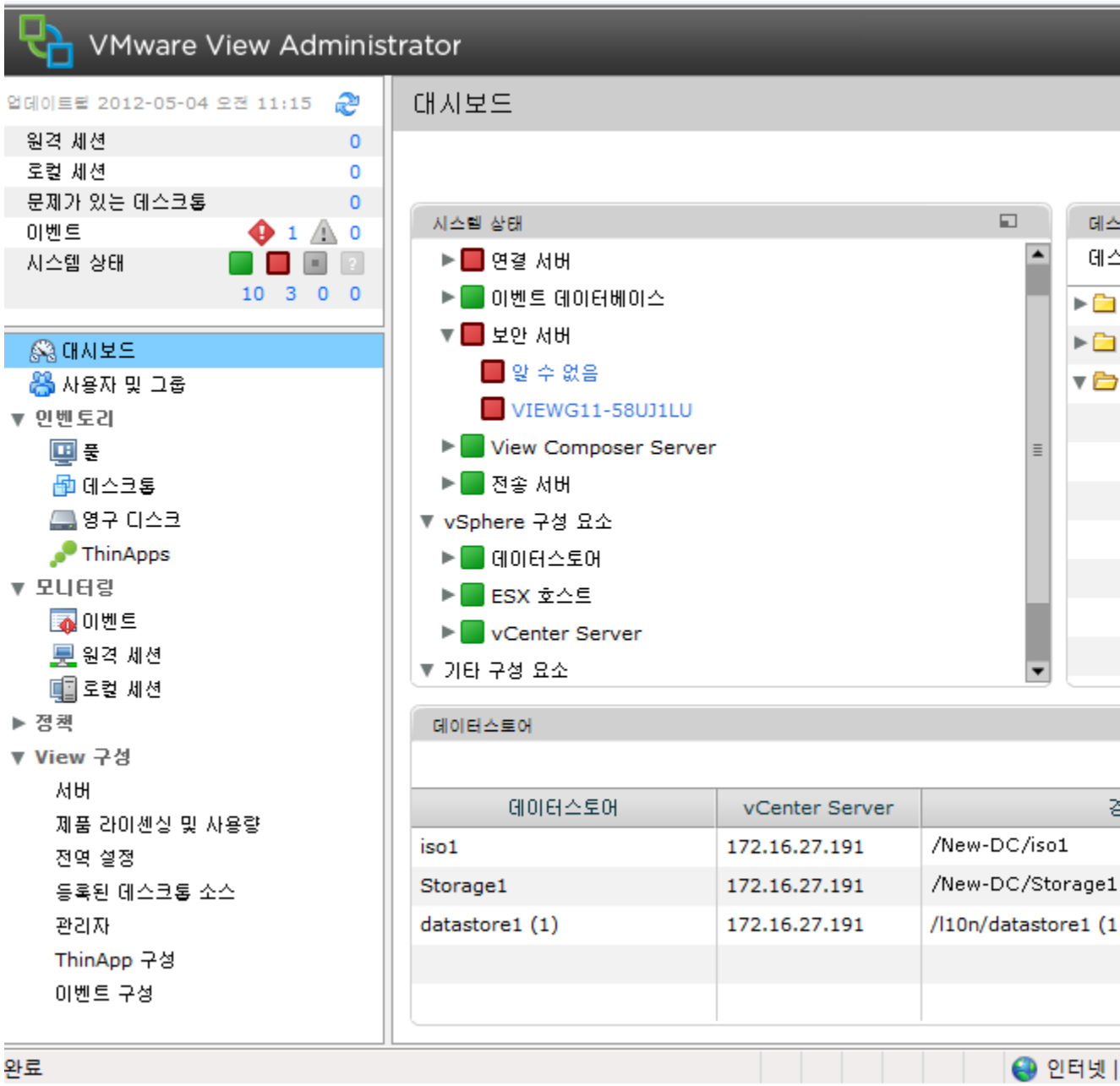
- 데이터에 대한 액세스를 쉽게 제한할 수 있습니다. 원격 직원의 가정용 컴퓨터로 중요한 데이터를 복사하지 못하도록 방지할 수 있습니다.
- RADIUS 지원은 2 요소 인증 벤더 사이에서 선택할 때 유연성을 제공합니다. 지원되는 벤더에는 특히 RSA SecureID, VASCO DIGIPASS, SMS Passcode 및 SafeNet 이 포함됩니다.
- 미리 만든 Active Directory 계정을 가진 View 데스크톱을 프로비저닝하는 기능은 읽기 전용 액세스 정책이 있는 잠긴 Active Directory 환경의 요구 사항을 해결합니다.
- 최종 사용자의 시스템 종료 시간에 관계 없이 데이터 백업 작업을 예약할 수 있습니다.
- 데이터 센터에 호스팅된 가상 데스크톱에 다운타임이 거의 발생하지 않습니다. VMware 서버의 고가용성 클러스터에 가상 시스템을 배치할 수 있습니다.

백엔드 물리적 시스템 및 Windows 터미널 서비스 서버에 가상 데스크톱을 연결할 수도 있습니다.

편리성

통합 관리 콘솔을 생성하여 Adobe Flex 에서 확장성을 확보하면 단일 View Manager 인터페이스에서 대규모 View 배포도 효율적으로 관리할 수 있습니다. 마법사와 대시보드로 워크플로우를 강화하고 드릴 다운을 용이하게 하여 자세한 내용을 확인하고 설정을 변경할 수 있습니다. 그림 1-1 은 View Administrator 용 브라우저 기반 사용자 인터페이스의 예시입니다.

그림 1-1. 대시보드 보기를 표시하는 View Manager 의 관리 콘솔



그 외에 편리한 기능으로는 VMware 원격 디스플레이 프로토콜 PCoIP 가 있습니다. PCoIP(PC-over-IP) 디스플레이 프로토콜은 물리적 PC 를 사용하는 것과 동일한 최종 사용자 경험을 제공합니다.

- LAN 에서는 기존 원격 디스플레이보다 빠르고 원활하게 디스플레이를 구현할 수 있습니다.

- WAN 의 경우, 디스플레이 프로토콜이 지연 증가와 대역폭 감소 현상을 보완해 최종 사용자가 네트워크 조건에 관계 없이 생산성을 유지할 수 있습니다.

관리 효율성

최종 사용자를 위한 데스크톱의 프로비저닝은 신속한 프로세스입니다. 각 최종 사용자의 물리적 PC 에 애플리케이션을 하나씩 설치할 필요가 없습니다. 최종 사용자는 애플리케이션이 완벽하게 설치된 가상 데스크톱에 연결합니다. 최종 사용자는 다양한 장소에서 다양한 디바이스를 사용해 동일한 가상 데스크톱에 액세스할 수 있습니다.

VMware vSphere 를 가상 데스크톱 호스팅에 사용하면 다음과 같은 장점을 얻을 수 있습니다.

- 관리 작업이 줄어듭니다. 관리자는 사용자의 물리적 PC 에 손대지 않고 애플리케이션과 운영 체제를 업그레이드하고 패치를 설치할 수 있습니다.
- View 개인 설정 관리가 있는 경우, 사용자 프로파일, 애플리케이션 권한, 정책, 성능 및 기타 설정을 포함한 물리적 및 가상 데스크톱을 중앙에서 관리할 수 있습니다. 가상 데스크톱으로 변환하기 전에 View 개인 설정 관리를 물리적 데스크톱에 배포하십시오.
- 스토리지 관리 작업이 간소화됩니다. VMware vSphere 를 사용하면 볼륨과 파일 시스템을 가상화할 수 있어 스토리지 디바이스를 별도로 관리할 필요가 없습니다.
- View 스토리지 가속기가 있는 경우, IOPS 스토리지 로드가 극적으로 감소되어 특별한 스토리지 어레이 기술 필요 없이 더 큰 스케일로 최종 사용자 로그인을 지원합니다.

하드웨어 독립성

가상 시스템은 하드웨어 독립적입니다. 데이터 센터 서버에서 View 데스크톱을 실행하고 클라이언트 디바이스로만 액세스할 수 있기 때문에 View 데스크톱은 클라이언트 디바이스의 하드웨어와 호환되지 않는 운영 체제를 사용할 수 있습니다.

예를 들어 Windows 7 은 Windows7 사용 가능 컴퓨터에서만 실행할 수 있지만, 가상 시스템에 Windows 7 을 설치할 경우, 이 가상 시스템을 Windows 7 을 사용할 수 없는 PC 에서 사용할 수 있습니다.

PC, Mac, 씬 클라이언트, 씬 클라이언트로 용도를 변경한 PC 를 비롯해 태블릿 및 Kindle Fire 와 같은 iPad 및 Android 디바이스에서 가상 데스크톱을 실행할 수 있습니다.

VMware View 기능

VMware View 에 포함된 기능은 사용성, 보안, 집중 컨트롤 및 확장성을 지원합니다.

다음 기능은 최종 사용자에게 친숙한 환경을 제공합니다.

- Microsoft Windows 클라이언트 디바이스의 경우 가상 데스크톱에서 Windows 클라이언트 디바이스에 정의된 로컬 또는 네트워크 프린터로 인쇄합니다. 이 가상 프린터 기능은 호환성 문제를 해결해 주므로 가상 시스템에 추가 인쇄 드라이버를 설치할 필요가 없습니다.
- 임의의 클라이언트 디바이스에서, 위치 기반 인쇄 기능을 사용하여 클라이언트 시스템에 물리적으로 근접한 프린터로 매핑합니다. 위치 기반 인쇄를 위해 인쇄 드라이버를 가상 시스템에 설치해야 합니다.
- 다중 모니터를 사용합니다. PCoIP 다중 모니터가 지원되는 경우 각 모니터에 대해 디스플레이 해상도 및 회전을 개별적으로 조정할 수 있습니다.

- 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 View 개인 설정 관리를 사용하십시오. View 개인 설정 관리를 사용하면 원하는 주기마다 사용자 프로파일을 원격 프로파일 저장소(CIFS 공유)로 복제할 수 있습니다.

  또한 View로 관리되지 않는 가상 시스템 및 물리적 컴퓨터에서 View 개인 설정 관리의 독립 실행형 버전을 사용할 수 있습니다.

VMware View는 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 View 데스크톱을 프로비저닝할 때 미리 만든 Active Directory 계정을 사용합니다.
- SSL 터널링을 사용하여 모든 연결이 완벽하게 암호화되었는지 확인합니다.
- VMware High Availability를 사용하여 데스크톱을 호스팅하고 자동 페일오버를 확인합니다.

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

- 가상 데스크톱의 비용 효과적인 밀도, 높은 수준의 가용성 및 고급 리소스 할당 컨트롤을 얻기 위해 VMware vSphere와 통합하십시오.
- View 스토리지 가속기 기능을 사용하여 동일한 스토리지 리소스를 보유하고 더 큰 스케일로 최종 사용자 로그인을 지원합니다. 이 스토리지 가속기는 vSphere 5 플랫폼에 있는 기능을 사용하여 공통 블록 읽기의 호스트 메모리 캐시를 생성합니다.
- 최종 사용자 및 액세스할 수 있는 가상 데스크톱 사이의 브로커 연결을 위해 View 연결 서버를 구성합니다.
- 마스터 이미지와 가상 디스크를 공유하는 데스크톱 이미지를 빠르게 생성하려면 View Composer를 사용하십시오. 이 방법으로 링크드 클론을 사용하면 디스크 공간이 절약되며 운영 체제에 대한 패치 및 업데이트 관리가 간소화됩니다.

다음 기능은 집중 관리를 제공합니다.

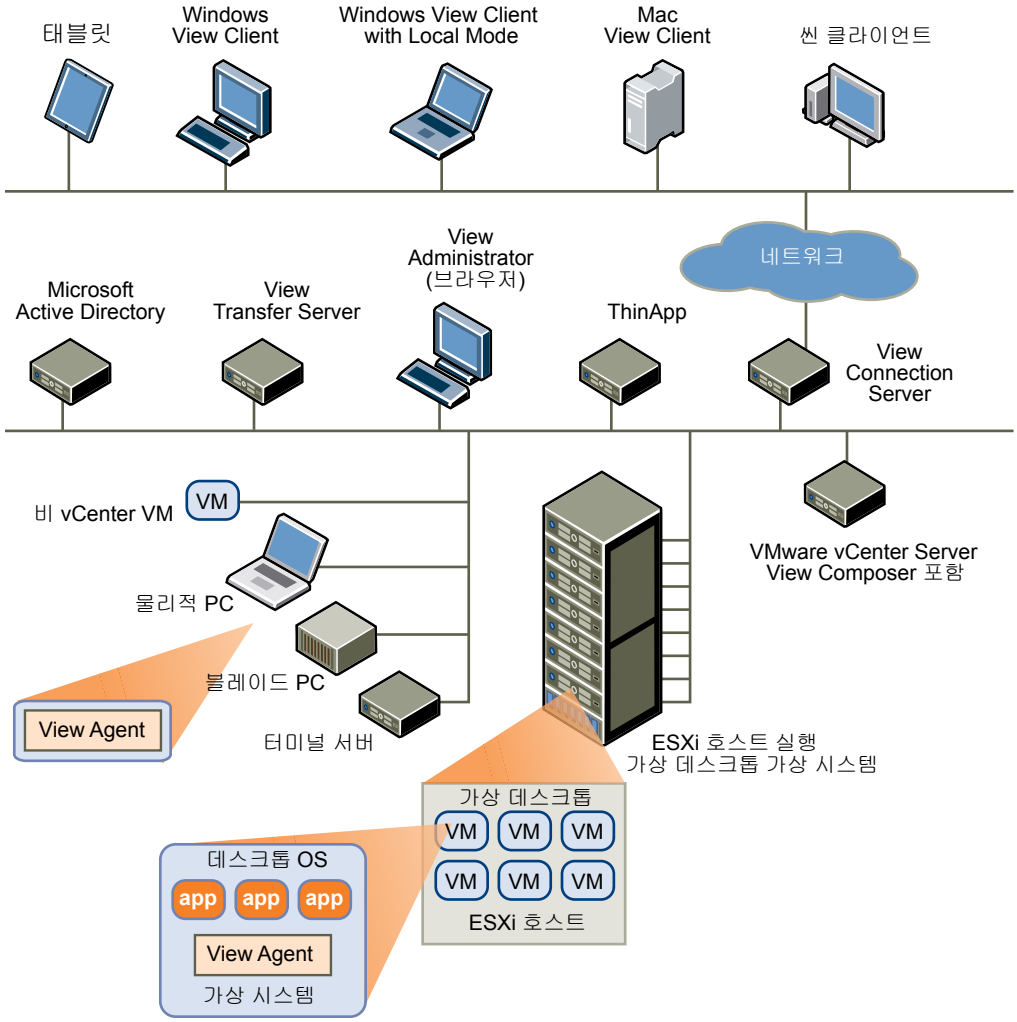
- Microsoft Active Directory를 사용하여 가상 데스크톱에 대한 액세스를 관리하고 정책을 관리합니다.
- View 개인 설정 관리를 사용하여 물리적 데스크톱에서 가상 데스크톱으로 마이그레이션을 단순화 및 간소화합니다.
- 웹 기반 관리 콘솔을 사용하여 임의의 위치에서 가상 데스크톱을 관리합니다.
- 템플릿 또는 마스터 이미지를 사용하여 데스크톱의 풀을 빠르게 생성하고 프로비저닝합니다.
- 사용자 설정, 데이터 또는 환경 설정에 영향을 주지 않은 채 가상 데스크톱으로 업데이트 및 패치를 보냅니다.

VMware View 구성 요소를 서로 맞추는 방법

최종 사용자는 View Client 를 시작해 View Connection Server 에 로그인합니다. 이 서버를 Windows Active Directory 와 통합해 VMware vSphere 환경, 블레이드 또는 물리적 PC, 또는 Windows 터미널 서비스 서버에 호스팅된 가상 데스크톱에 대한 액세스 권한을 제공합니다.

그림 1-2 는 VMware View 배포의 주요 구성 요소 간 관계를 보여줍니다.

그림 1-2. VMware View 환경의 고수준 예



클라이언트 디바이스

VMware View 의 주요 장점은 디바이스 또는 위치에 관계없이 최종 사용자가 데스크톱을 사용할 수 있다는 점입니다. 사용자는 회사 랩톱, 가정용 PC, 씬 클라이언트 디바이스 또는 Mac 이나 태블릿에서 개인화된 가상 데스크톱에 액세스할 수 있습니다.

최종 사용자는 태블릿과 Mac, Linux 및 Windows 랩톱과 PC 에서 View Client 를 열고 View 데스크톱을 표시할 수 있습니다. 씬 클라이언트 디바이스는 View 씬 클라이언트 소프트웨어를 사용하고 구성될 수 있기 때문에 사용자는 애플리케이션 가운데 View Thin Client 만 디바이스에서 직접 시작할 수 있습니다. 레거시 PC 를 씬 클라이언트 데스크톱으로 재설정하면 하드웨어 수명을 3-5 년 가량 연장할 수 있습니다. 예를 들어 씬 데스크톱에서 VMware View 를 사용하면 이전 데스크톱 하드웨어에서 Windows 7 과 같은 최신 운영 체제를 사용할 수 있습니다.

View Connection Server

이 소프트웨어 서비스는 클라이언트 연결의 브로커 역할을 합니다. View Connection Server 는 Windows Active Directory 를 통해 사용자를 인증하고 요청을 해당 가상 시스템, 물리적 또는 블레이드 PC 또는 Windows 터미널 서비스 서버로 지시합니다.

View Connection Server 는 다음 관리 기능을 제공합니다.

- 사용자 인증
- 사용자에게 특정 데스크톱 및 풀에 대한 권한 부여
- VMware ThinApp 과 패키징된 애플리케이션을 특정 데스크톱 및 풀에 할당
- 로컬 및 원격 데스크톱 세션 관리
- 사용자 및 데스크톱 사이의 보안 연결 설정
- 단일 로그온을 사용하도록 설정
- 정책 설정 및 적용

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

회사 방화벽 외부 DMZ 에 보안 서버로서 View Connection Server 를 설치 및 구성할 수 있습니다. DMZ 의 보안 서버는 회사 방화벽 내 View Connection Server 와 통신합니다. 보안 서버는 회사 데이터 센터에 들어갈 수 있는 원격 데스크톱 트래픽만 확실히 인증된 사용자를 위한 트래픽임을 보장합니다. 사용자는 액세스 권한을 부여받은 데스크톱 리소스에만 액세스할 수 있습니다.

보안 서버는 하위 집합 기능을 제공하며 Active Directory 도메인에 있지 않아도 됩니다. Windows Server 2008 서버에, 가능하면 VMware 가상 시스템에 View Connection Server 를 설치합니다.

View Client

View 데스크톱에 액세스하기 위한 클라이언트 소프트웨어는 태블릿, Windows, Linux 나 Mac PC 또는 랩톱, 씬 클라이언트 등에서 실행할 수 있습니다.

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

관리자는 View Client 를 구성하여 최종 사용자가 디스플레이 프로토콜을 선택하도록 허용할 수 있습니다. 프로토콜에는 PCoIP 및 Microsoft RDP 가 포함됩니다. PCoIP 속도 및 디스플레이 품질은 물리적 PC 의 속도 및 디스플레이 품질에 못지 않습니다.

View Client with Local Mode(이전에는 Offline Desktop 이라고 불렀음)는 네트워크 연결 여부와 관계 없이 최종 사용자가 가상 시스템을 다운로드하여 로컬 Windows 시스템에서 사용하도록 확장된 View Client 버전입니다.

사용하는 View Client 에 따라 기능이 다릅니다. 이 설명서는 Windows 용 View Client 를 중심으로 설명합니다. 다음 클라이언트 유형은 이 안내서에서 자세히 다루지 않았습니다.

- 태블릿, Linux 클라이언트 및 Mac 클라이언트용 View Client 에 대한 자세한 내용은 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html 에서 VMware View Client 설명서를 참조하십시오.
- 다양한 타사 씬 클라이언트 및 제로 클라이언트(인증된 파트너를 통해서만 사용할 수 있음).
- View Open Client(VMware 파트너 인증 프로그램 지원). View Open Client 는 공식 View 클라이언트가 아니며 그 자체로는 지원되지 않습니다.

View Portal

View Portal 을 사용하려면 Windows, Linux, Mac PC 또는 노트북의 최종 사용자가 웹 브라우저를 열고 View 연결 서버 인스턴스 URL 을 방문해야 합니다. View Portal 은 전체 View Client 의 설치 관리자 다운로드를 위한 링크를 제공합니다.

기본적으로 브라우저를 열고 View 연결 서버 인스턴스의 URL 을 입력할 때 나타나는 View Portal 페이지에는 View Client 다운로드를 위한 VMware 다운로드 사이트에 대한 링크가 포함됩니다. 그러나 View Portal 페이지의 링크는 구성 가능합니다. 예를 들어, 내부 웹 서버를 가리키도록 링크를 구성하거나 해당 고유 View 연결 서버에 사용할 수 있는 클라이언트 버전을 제한할 수 있습니다.

View Agent

View 데스크톱의 소스로 사용하는 모든 가상 시스템, 물리적 시스템 및 터미널 서비스 서버에 View Agent 서비스를 설치합니다. 가상 시스템에서 이 에이전트는 View Client 와 통신하여 연결 모니터링, 가상 인쇄, View 개인 설정 관리 그리고 로컬로 연결된 USB 디바이스 액세스 등의 기능을 제공합니다.

데스크톱 소스가 가상 시스템인 경우 먼저 해당 가상 시스템에 View Agent 서비스를 설치한 다음 템플릿 또는 상위 연결된 클론으로 가상 시스템을 사용합니다. 이 가상 시스템에서 풀을 생성할 때 에이전트가 모든 가상 데스크톱에 자동으로 설치됩니다.

단일 로그온 옵션을 사용하여 에이전트를 설치할 수 있습니다. 단일 로그온을 사용하여 사용자가 View Connection Server 에 연결할 때에만 로그인 메시지가 나타나며 가상 데스크톱에 연결할 때에는 메시지가 다시 나타나지 않습니다.

View Administrator

이 웹 기반 애플리케이션을 사용하여 관리자는 View Connection Server 를 구성하고 View 데스크톱을 관리하고 사용자 인증을 제어하며 최종 사용자 문제를 해결할 수 있습니다.

View Connection Server 인스턴스를 설치할 때 View Administrator 애플리케이션도 설치됩니다. 이 애플리케이션을 사용하여 로컬 컴퓨터에 애플리케이션을 설치할 필요 없이 어디에서든 View Connection Server 인스턴스를 관리할 수 있습니다.

View Composer

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

각 링크드 클론은 고유 호스트 이름 및 IP 주소를 사용하여 독립 데스크톱처럼 작동하지만 기본 이미지를 상위 이미지와 공유하기 때문에 링크드 클론은 매우 적은 양의 스토리지를 필요로 합니다.

링크드 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 로컬 시스템을 사용하기 위해 다운로드하고 체크아웃하는 View 데스크톱의 링크드 클론 기술을 사용할 수 있습니다.

View 5.1 을 사용하는 경우, 해당 고유 서버 호스트에 View Composer 를 설치할 수 있지만 View Composer 서비스는 vCenter Server 인스턴스 1 개와만 작동할 수 있습니다. 마찬가지로 vCenter Server 인스턴스는 View Composer 서비스 하나와만 연결될 수 있습니다.

vCenter Server

이 서비스는 네트워크로 연결된 VMware ESX/ESXi 서버의 중앙 관리자 역할을 합니다. VMware VirtualCenter 로 불리던 vCenter Server 는 데이터 센터의 가상 시스템을 구성, 프로비저닝 및 관리하기 위한 중심점을 제공합니다.

View 데스크톱 풀의 소스로 이러한 가상 시스템을 사용하는 것 외에도 가상 시스템을 사용하여 Connection Server 인스턴스, Active Directory 서버 및 vCenter Server 인스턴스를 포함한 VMware View 의 서버 구성 요소를 호스팅할 수 있습니다.

vCenter Server 와 동일한 서버에 View Composer 를 설치하여 연결된 클론 데스크톱 풀을 생성할 수 있습니다. 그러고 나면 vCenter Server 는 물리적 서버 및 스토리지에 대한 가상 시스템 할당을 관리하고 가상 시스템에 대한 CPU 및 메모리 리소스 할당을 관리합니다.

Windows Server 2008 서버에, 가능하면 VMware 가상 시스템에 vCenter Server 를 설치합니다.

View Transfer Server

이 소프트웨어는 최종 사용자의 로컬 시스템에서 사용하기 위해 체크아웃된 View 데스크톱 및 데이터 센터 사이에서 데이터 전송을 관리하고 간소화합니다. View Transfer Server 는 View Client with Local Mode(이전에는 Offline Desktop 이라고 불렀음)를 실행하는 데스크톱을 지원합니다.

여러 작업에서 View Transfer Server 를 사용하여 vCenter Server 의 View 데스크톱 및 클라이언트 시스템의 해당 로컬 데스크톱 사이에서 데이터를 전송합니다.

- 사용자가 데스크톱을 체크인 또는 체크아웃할 때 View Manager 는 작업을 인증 및 관리합니다. View Transfer Server 는 데이터 센터 및 로컬 데스크톱 사이에서 파일을 전송합니다.
- View Transfer Server 는 데이터 센터에 사용자 변경 내용을 복제하여 데이터 센터의 해당 데스크톱과 로컬 데스크톱을 동기화합니다.

  복제는 로컬 모드 정책에서 지정한 간격으로 발생합니다. 또한 View Administrator 에서 복제를 시작할 수 있습니다. 사용자가 로컬 데스크톱에서 복제를 시작할 수 있도록 정책을 설정할 수 있습니다.
- View Transfer Server 는 데이터 센터에서 로컬 클라이언트로 일반 시스템 데이터를 배포합니다. View Transfer Server 는 Transfer Server 저장소에서 로컬 데스크톱으로 View Composer 기본 이미지를 다운로드합니다.

VMware View 통합 및 사용자 지정

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

View 에 비즈니스 인텔리전스 소프트웨어 통합

Microsoft SQL Server 또는 Oracle 데이터베이스에 이벤트를 기록하도록 VMware View 를 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.
- 24 시간 동안 최대 사용자 수 기록과 같은 통계 샘플링.

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

자세한 내용은 *VMware View Integration*(VMware View 통합) 설명서를 참조하십시오.

View PowerCLI 를 사용한 관리 스크립트 생성

Windows PowerShell 은 Microsoft Windows 용으로 만들어진 명령줄 및 스크립팅 환경입니다. PowerShell 은 .NET 개체 모델을 사용해 관리자에게 관리 및 자동화 기능을 제공합니다. 다른 콘솔 환경처럼 명령을 실행해 PowerShell 을 사용하며 이를 PowerShell cmdlets 라 부릅니다.

View PowerCLI 는 VMware View 에 사용하기 쉬운 PowerShell 인터페이스를 제공합니다. View PowerCLI cmdlets 를 사용해 View 구성 요소에서 다양한 관리 작업을 수행할 수 있습니다.

- 데스크톱 풀을 생성하고 및 업데이트합니다.
- 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.
- View 서비스 상태를 쿼리합니다.

vSphere PowerCLI cmdlets 와 cmdlets 를 함께 사용해 VMware vSphere 제품에 관리 인터페이스를 제공할 수 있습니다.

자세한 내용은 *VMware View Integration*(VMware View 통합) 설명서를 참조하십시오.

View 의 LDAP 구성 데이터 수정

View Administrator 를 사용해 VMware View 구성을 수정하는 경우에는 저장소의 해당 LDAP 데이터가 업데이트됩니다. VMware View 는 LDAP 호환 저장소에 구성 정보를 저장합니다. 예를 들어 데스크톱 풀을 추가하면 VMware View 는 사용자, 사용자 그룹, 권한 정보를 LDAP 에 저장합니다.

VMware 와 Microsoft 명령 도구를 사용해 LDIF(LDAP Data Interchange Format) 파일의 LDAP 구성 데이터를 VMware View 에서 내보내거나 가져올 수 있습니다. 이들 명령은 View Administrator 또는 View PowerCLI 를 사용하지 않고 스크립트를 사용해 구성 데이터를 업데이트하려는 고급 관리자용입니다.

LDIF 파일을 사용해 다양한 작업을 수행할 수 있습니다.

- View Connection Server 인스턴스 간 구성 데이터를 전송합니다.
- 데스크톱 풀과 같은 다수의 View 객체를 정의하고 View Administrator 또는 View PowerCLI 를 사용하지 않고 View Connection Server 인스턴스에 이들 객체를 추가합니다.
- View Connection Server 인스턴스 상태를 복원할 수 있도록 View 구성을 백업합니다.

자세한 내용은 *VMware View Integration*(VMware View 통합) 설명서를 참조하십시오.

SCOM 을 사용한 View 구성 요소 모니터링

Microsoft SCOM(System Center Operations Manager)을 사용해 View Connection Server 인스턴스, 보안 서버, 이들 호스트에서 실행되는 View 서비스와 같은 VMware View 구성 요소 성능 상태를 모니터링할 수 있습니다.

자세한 내용은 *VMware View Integration*(VMware View 통합) 설명서를 참조하십시오.

vdmadmin 명령을 사용한 View 관리

vdmadmin 명령줄 인터페이스를 사용해 View Connection Server 인스턴스에서 다양한 관리 작업을 수행할 수 있습니다. vdmadmin 을 사용해 View Administrator 사용자 인터페이스에서 실행할 수 없거나 스크립트에서 자동으로 실행해야 하는 관리 작업을 수행할 수 있습니다.

자세한 내용은 *VMware View 관리* 설명서를 참조하십시오.

풍부한 사용자 환경 계획 2

VMware View는 최종 사용자가 기대하는 친숙하고 개인화된 데스크톱 환경을 제공합니다. 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.

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

이 장에서는 다음 주제에 대해 설명합니다.

- "기능 지원 표," (17 페이지)
- "디스플레이 프로토콜 선택," (19 페이지)
- "View 개인 설정 관리를 사용하여 사용자 데이터 및 설정 유지," (21 페이지)
- "Local Mode에서 View 데스크톱 사용 시 장점," (23 페이지)
- "로컬 컴퓨터에 연결된 USB 디바이스에 액세스," (25 페이지)
- "View 데스크톱에서 인쇄," (25 페이지)
- "View 데스크톱에 멀티미디어 스트리밍," (26 페이지)
- "단일 로그온을 사용한 View 데스크톱 로그인," (26 페이지)
- "View 데스크톱에 다중 모니터 사용," (26 페이지)

기능 지원 표

RSA SecurID 인증, 위치 기반 인쇄, PCoIP 프로토콜과 같은 여러 기능이 대부분의 클라이언트 운영 체제에서 지원됩니다. 각 기능을 View 데스크톱 운영 체제에서 지원하는지 고려해야 합니다.

최종 사용자에게 사용을 허용할 디스플레이 프로토콜과 기능을 계획할 때는 다음 정보를 사용하여 해당 기능을 지원하는 클라이언트 운영 체제와 에이전트(View 데스크톱) 운영 체제를 확인합니다.

Windows Vista 버전에는 Windows Vista Home, Enterprise, Ultimate, Business가 있습니다. Windows 7 버전에는 Home, Professional, Enterprise, Ultimate이 있습니다. Windows 터미널 서버는 Standard Edition 버전이 있습니다.

표 2-1. View 데스크톱용 운영 체제에서 지원하는 기능(View Agent 가 설치된 경우)

기능	Windows XP Pro SP3, 32 비트	Windows Vista SP1 및 SP2, 32 비트	Windows 7 및 SP1, 32 비트 및 64 비트	Windows 2008 SP2/2008 R2 및 SP1 Terminal Server 64 비트
USB 액세스	X	X	X	
RDP 디스플레이 프로토콜	X	X	X	X
PCoIP 디스플레이 프로토콜	X	X	X	
개인 설정 관리	X	X	X	
Wyse MMR	X	X		
위치 기반 인쇄	X	X	X	
가상 인쇄	X	X	X	
스마트 카드	X	X	X	X
RSA SecurID 또는 RADIUS	X	X	X	해당 없음
단일 로그온	X	X	X	X
다중 모니터	X	X	X	RDP 7 사용
Local Mode	X	X	X	

표 2-2. Windows 클라이언트용 VMware View 에서 지원되는 기능

기능	Windows XP Home/Pro SP3, 32 비트 클라이언트	Windows Vista SP2, 32 비트 클라이언트	Windows 7 및 SP1, 32 비트 및 64 비트 클라이언트
USB 액세스	X	X	X
RDP 디스플레이 프로토콜	X	X	X
PCoIP 디스플레이 프로토콜	X	X	X
개인 설정 관리	X(로컬 모드 제외)	X(로컬 모드 제외)	X(로컬 모드 제외)
Wyse MMR	X	X	
위치 기반 인쇄	X	X	X
가상 인쇄	X	X	X
스마트 카드	X	X	X
RSA SecurID 또는 RADIUS	X	X	X
단일 로그온	X	X	X
다중 모니터	X	X	X
Local Mode	X	X	X

그리고 여러 VMware 파트너에서 VMware View 배포용 씬 클라이언트 디바이스를 제공합니다. 공급업체와 모델, 기업이 사용하기로 결정한 구성에 따라 각 씬 클라이언트 디바이스에서 사용할 수 있는 기능이 다릅니다. 씬 클라이언트 디바이스 공급업체 및 모델에 대한 자세한 내용은 VMware 웹 사이트의 *Thin Client Compatibility Guide*(씬 클라이언트 호환성 설명서)에서 확인할 수 있습니다.

참고 Mac OS X, Linux 클라이언트 또는 태블릿에서 지원하는 기능에 대한 자세한 내용은 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html 의 VMware View Client 설명서를 참조하십시오.

디스플레이 프로토콜 선택

디스플레이 프로토콜은 최종 사용자에게 데이터 센터에 있는 View 데스크톱에 대한 그래픽 인터페이스를 제공합니다. VMware 에서 제공하는 PCoIP(PC-over-IP) 또는 Microsoft RDP(Remote Desktop Protocol)를 사용할 수 있습니다.

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

참고 로컬 클라이언트 시스템에서 사용하기 위해 데스크톱을 체크아웃하는 경우에는 PCoIP 또는 RDP 원격 디스플레이 프로토콜이 사용되지 않습니다.

PCoIP 포함 VMware View

PCoIP 는 LAN 또는 WAN 의 많은 사용자에게 애플리케이션, 이미지, 오디오 및 비디오 컨텐츠를 포함한 전체 데스크톱 환경의 전송을 위해 최적화된 데스크톱 환경을 제공합니다. PCoIP 는 지연 증가 또는 대역폭 감소를 보완하여 네트워크 상태와 상관없이 최종 사용자가 효율적으로 유지할 수 있도록 합니다.

PCoIP 는 Teradici 호스트 카드를 포함한 가상 컴퓨터 및 물리적 컴퓨터를 사용하여 View 데스크톱의 디스플레이 프로토콜로 지원됩니다.

PCoIP 기능

PCoIP 의 키 기능에는 다음 내용이 포함됩니다.

- 회사 방화벽 외부 사용자의 경우 회사의 가상 개인 네트워크 또는 View 보안 서버와 이 프로토콜을 함께 사용할 수 있습니다.
- AES(Advanced Encryption Standard) 128 비트 암호화가 지원되며 기본적으로 사용됩니다.
- 모든 유형의 View 클라이언트로부터 연결. 자세한 내용은 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html 을 참조하십시오.
- MMR 리디렉션이 Windows XP 및 Vista 클라이언트용으로 지원됩니다. MMR 리디렉션은 Windows 7 View Client 에 지원되지 않으며 Windows 7 View 데스크톱에서 지원되지 않습니다.
- USB 리디렉션이 지원됩니다.
- LAN 및 WAN 의 동적 오디오 품질 조정이 포함된 오디오 리디렉션이 지원됩니다.
- LAN 및 WAN 에서 대역폭 사용량을 줄이기 위한 최적화 관리.
- 다중 모니터가 지원됩니다. 최고 4 대의 모니터를 사용하고 각 모니터의 해상도를 디스플레이당 최고 2560 x 1600 의 해상도를 사용하여 개별적으로 조정할 수 있습니다. 피벗 디스플레이 및 자동 맞춤도 지원됩니다.

  3D 기능을 사용할 경우 최대 2 대의 모니터가 최대 해상도인 1920x1200 으로 지원됩니다.
- 32 비트 색상이 가상 디스플레이를 위해 지원됩니다.

- ClearType 글꼴이 지원됩니다.
- 로컬 Windows 클라이언트 시스템과 데스크톱 간의 텍스트와 이미지 복사 및 붙여넣기가 지원됩니다(최대 1MB). 지원되는 파일 형식에는 텍스트, 이미지 및 RTF(서식 있는 텍스트)가 포함됩니다. 시스템 사이에서 폴더 및 파일과 같은 시스템 개체를 복사하고 붙여 넣을 수 없습니다.

비디오 품질

480p 형식 비디오	View 데스크톱에 단일 가상 CPU 가 있는 경우 기본 해상도에서 480p 이하로 비디오를 재생할 수 있습니다. 운영 체제가 Windows 7 이고 고화질 Flash 또는 전체 화면 모드로 비디오를 재생할 경우 데스크톱에 이중 가상 CPU 가 필요합니다.
720p 형식 비디오	View 데스크톱에 이중 가상 CPU 가 있는 경우 기본 해상도에서 720p 로 비디오를 재생할 수 있습니다. 고화질 또는 전체 화면 모드로 720p 에서 비디오를 재생할 경우 성능이 영향을 받을 수 있습니다.
1080p 형식 비디오	View 데스크톱에 이중 가상 CPU 가 있는 경우 미디어 플레이어의 창 크기를 더 작게 조정해야 할 수도 있지만 1080p 형식 비디오를 재생할 수 있습니다.
3D	Windows Aero 테마 또는 Google Earth 와 같은 3D 애플리케이션을 사용할 경우, Windows 7 View 데스크톱에 vSphere 5 이상에서 사용 가능한 가상 하드웨어 버전 8 이 있어야 합니다. 또한 **Windows 7 3D 렌더링**이라는 풀 설정을 사용하도록 설정해야 합니다. 최대 2 대 모니터가 지원되며 최대 화면 해상도는 1920 x 1200 입니다. 이 비하드웨어 가속 그래픽 기능을 사용하면 물리적 GPU 필요 없이 DirectX 9 및 OpenGL 2.1 애플리케이션을 실행할 수 있습니다.

권장된 게스트 운영 체제 설정

권장된 게스트 운영 체제 설정에는 다음 설정이 포함됩니다.

- Windows XP 데스크톱의 경우 768MB RAM 이상 및 단일 CPU
- Windows 7 데스크톱의 경우 1GB RAM 및 이중 CPU

데스크톱 클라이언트 하드웨어 요구 사항

클라이언트 하드웨어 요구 사항에는 다음이 포함됩니다.

- 프로세서 속도가 800MHz 이상인 x86 기반 프로세서(SSE2 확장).
- 프로세서 속도가 1Ghz 이상인 ARM 프로세서(NEON(권장) 또는 WMMX2 확장).
- 다양한 모니터 설정을 지원하려면 RAM 이 시스템 요구 사항 이상으로 충분해야 합니다. 일반적으로 다음 수식을 사용하면 됩니다.

  20MB + (24 * (모니터 수) * (모니터 너비) * (모니터 높이))

  다음과 같은 간단한 계산이 가능합니다.

  1 대의 모니터: 1600 x 1200: 64MB
  2 대의 모니터: 1600 x 1200: 128MB
  3 대의 모니터: 1600 x 1200: 256MB

참고 모바일 클라이언트 하드웨어 요구 사항에 대해서는 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html 을 참조하십시오.

Microsoft RDP

원격 데스크톱 프로토콜은 가정용 컴퓨터에서 회사 컴퓨터에 액세스할 때 많이 사용하는 다중 채널 프로토콜과 동일합니다. Microsoft RDC(원격 데스크톱 연결)은 RDP 를 사용해 데이터를 전송합니다.

Microsoft RDP 는 다음과 같은 기능을 제공합니다.

- RDP 6 의 경우 스팬 모드에서 다중 모니터를 사용할 수 있습니다. RDP 7 은 최대 16 대의 다중 모니터 지원이 가능합니다.
- 로컬 시스템과 View 데스크톱 간에 폴더 및 파일과 같은 텍스트 및 시스템 개체를 복사 및 붙여 넣을 수 있습니다.
- RDP 는 32 비트 컬러를 지원합니다.
- RDP 는 128 비트 암호화를 지원합니다.
- 이 프로토콜을 사용해 기업 DMZ 의 View 보안 서버에 대한 안전하고 암호화된 연결을 생성할 수 있습니다.

다음은 다른 Windows 운영 체제 및 기능을 위한 RDP 관련 요구 사항 및 고려 사항입니다.

- Windows XP 및 Windows XP Embedded 시스템의 경우 Microsoft RDC 6.x 을 사용해야 합니다.
- Windows Vista 에는 RDC 6.x 가 설치되어 있지만 RDC 7 을 권장합니다.
- Windows 7 에는 RDC 7 이 설치되어 있습니다. Windows 7 SP1 에는 RDC 7.1 이 설치되어 있습니다.
- 다중 모니터를 사용하려면 RDC 6.0 이상이 있어야 합니다.
- Windows XP 데스크톱 가상 컴퓨터의 경우 Microsoft 기술 자료(KB) 문서 323497 및 884020 에 나열된 RDP 패치를 설치해야 합니다. RDP 패치를 설치하지 않은 경우 Windows Sockets 실패 오류 메시지가 클라이언트에 나타날 수 있습니다.
- View Agent 설치 관리자는 인바운드 RDP 연결을 위한 로컬 방화벽 규칙을 구성하여 일반적으로 3389 인 호스트 운영 체제의 현재 RDP 포트와 일치시킵니다. RDP 포트 번호를 변경하는 경우 관련된 방화벽 규칙을 변경해야 합니다.

Microsoft 웹 사이트에서 RDC 버전을 다운로드할 수 있습니다.

데스크톱 클라이언트 하드웨어 요구 사항

클라이언트 하드웨어 요구 사항에는 다음이 포함됩니다.

- 프로세서 속도가 800MHz 이상인 x86 기반 프로세서(SSE2 확장).
- 프로세서 속도가 600MHz 이상인 ARM 프로세서(NEON(권장) 또는 WMMX2 확장).
- 128MB RAM.

참고 iPad 및 Android 등의 모바일 클라이언트는 PCoIP 디스플레이 프로토콜만 사용합니다.

View 개인 설정 관리를 사용하여 사용자 데이터 및 설정 유지

View 데스크톱과 View 로 관리되지 않는 가상 시스템 및 물리적 컴퓨터에서 View 개인 설정 관리를 사용할 수 있습니다. View 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, View 개인 설정 관리에서 사용자 로컬 프로파일의 크기보다 크거나 동일한 CIFS 공유 저장소가 필요합니다.

로그온 및 로그오프 시간 최소화

View 개인 설정 관리는 데스크톱 로그온 및 로그오프 시간을 최소화합니다.

- View 는 View 데스크톱의 프로파일에 최근 변경 내용을 보관하고 정해진 주기마다 원격 저장소에 복사합니다. 기본값은 매 10 분입니다. 이와는 대조적으로, Windows 로밍 프로파일은 로그오프될 때까지 기다린 후 로그오프 시 모든 변경 내용을 서버에 복사합니다.
- 로그온 중 View 는 사용자 레지스트리 파일 등 Windows 에 필요한 파일만 다운로드합니다. 기타 파일은 사용자 또는 애플리케이션에 의해 View 데스크톱의 프로파일 폴더에서 열릴 때 View 데스크톱에 복사됩니다.
- View 개인 설정 관리를 사용하면 로그오프 중 마지막 복제 이후에 업데이트된 파일만 원격 저장소에 복사됩니다.

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

View 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 로그온 시간에는 크게 영향을 주지 않습니다. 이 전략은 데이터 손실 또는 손실에 대한 적절한 보호를 제공합니다.

구성 옵션

다음과 같은 여러 수준에서 View 개인 설정을 구성할 수 있습니다. 단일 View 데스크톱, 데스크톱 풀, OU 또는 배포 시 모든 View 데스크톱. 또한 View 로 관리되지 않는 가상 시스템 및 물리적 컴퓨터에서 View 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 폴더에 포함할지 여부를 지정할 수 있습니다. Windows 7 또는 Windows Vista 의 경우, 이 정책은 AppDataWLocal 폴더에 영향을 줍니다. Windows XP 의 경우, 이 정책은 Local Settings 폴더에 영향을 줍니다.
- 로그인할 때 로드할 파일 및 폴더를 지정합니다. 예: Application DataWMicrosoftWCertificates. 또한 폴더 내에서 제외할 파일을 지정할 수 있습니다.
- 사용자가 데스크톱에 로그인한 후 백그라운드로 다운로드할 파일 및 폴더를 지정합니다. 또한 폴더 내에서 제외할 파일을 지정할 수 있습니다.
- View 개인 설정 관리 대신 Windows 로밍 프로파일 기능을 사용하여, 관리할 사용자 개인 설정 내의 파일 및 폴더를 지정합니다. 또한 폴더 내에서 제외할 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
즐겨찾기	네트워크 환경	Templates
History	Printer Neighborhood	Temporary Internet Files
Links	최근 문서	

개인 설정을 저장하기 위한 원격 저장소를 구성하려는 경우, 네트워크 공유를 사용하거나 Windows 로밍 프로파일을 위해 구성한 기존 Active Directory 사용자 프로파일 경로를 사용할 수 있습니다. 네트워크 공유는 서버, NAS(네트워크 연결 스토리지) 디바이스 또는 네트워크 서버의 폴더일 수 있습니다. 대량 View 배포를 지원하기 위해 데스크톱 풀마다 개별 저장소를 따로 구성할 수 있습니다.

View 5.1 이상을 사용하는 경우, 다음 목표를 성취할 수 있도록 View 로 관리되지 않는 가상 시스템 및 물리적 컴퓨터에 View 개인 설정 관리의 독립 실행형 버전을 설치할 수 있습니다.

- 독립 실행형 시스템 및 View 데스크톱에서 프로파일을 공유하고 관리합니다.
- 물리적 시스템에서 View 데스크톱으로 사용자 프로파일을 마이그레이션합니다.
- 물리적 시스템에서 View 데스크톱으로 준비된 마이그레이션을 수행합니다.
- 사용자가 오프라인으로 전환할 때 최신 프로파일을 지원합니다.

제한 사항

View 개인 설정 관리는 다음과 같은 제한 사항이 있습니다.

- View 개인 설정 관리 구성 요소를 포함하는 View 라이센스를 보유하고 있어야 합니다.
- View 개인 설정 관리를 위해 CIFS(Common Internet File System) 공유가 필요합니다.
- 로컬 모드로 실행되는 데스크톱에서 View 개인 설정 관리를 사용할 수 없습니다.
- 사용자가 v1 사용자 프로파일 및 v2 사용자 프로파일이 있는 데스크톱 사이에서 전환할 경우, 사용자는 동일한 프로파일에 액세스할 수 없습니다. 그러나 리디렉션된 폴더를 v1 및 v2 프로파일 간에 공유할 수 있습니다. Windows XP 는 v1 프로파일을 사용합니다. Windows Vista 및 Windows 7 은 v2 프로파일을 사용합니다.

Local Mode 에서 View 데스크톱 사용 시 장점

사용자는 View Client with Local Mode 로 노트북 컴퓨터와 같은 로컬 시스템에 View 데스크톱을 체크아웃하고 다운로드할 수 있습니다. 관리자는 백업 및 서버와의 연결 빈도, USB 장치에 대한 액세스, 데스크톱 체크인 사용 권한 등에 대한 정책을 설정해 이들 로컬 View 데스크톱을 관리할 수 있습니다.

네트워크 연결이 안 좋은 원격 사무실에서 근무하는 직원의 경우 원격 데스크톱보다 로컬 View 데스크톱에서 보다 빠르게 애플리케이션을 실행할 수 있습니다. 또한 사용자는 네트워크 연결 상태에 상관 없이 데스크톱 로컬 버전을 사용할 수 있습니다.

클라이언트 시스템에 네트워크가 연결되어 있는 경우 체크아웃된 데스크톱은 View 연결 서버와 계속 통신해 정책을 업데이트하고 로컬로 캐시된 인증 조건을 최신으로 유지합니다. 기본적으로 6 분마다 연결을 시도합니다.

View 데스크톱은 로컬 모드에서 원격 데스크톱과 동일한 방식으로 작동하지만 로컬 리소스를 활용할 수 있습니다. 레거시는 제거되고 성능은 향상됩니다. 사용자는 로컬 View 데스크톱과 연결을 끊고 View 연결 서버에 연결하지 않고 다시 로그인할 수 있습니다. 네트워크 액세스를 복원한 이후 또는 사용자가 준비되었을 때 체크아웃된 가상 컴퓨터를 백업, 롤백 또는 체크인할 수 있습니다.

로컬 리소스 사용률

로컬 데스크톱을 체크아웃한 후에 로컬 시스템의 메모리와 CPU 기능을 활용할 수 있습니다. 예를 들어 호스트와 게스트 운영 체제에 필요한 것 이상을 사용할 수 있는 메모리는 vCenter Server 의 가상 컴퓨터에 지정된 메모리 설정에 관계 없이 호스트와 로컬 View 데스크톱에 분할되는 것이 일반적입니다. 마찬가지로 로컬 View 데스크톱은 로컬 시스템에서 사용할 수 있는 CPU 를 2 개까지 자동으로 사용할 수 있으며 CPU 를 최대 4 개까지 사용할 수 있도록 로컬 데스크톱을 구성할 수 있습니다.

로컬 데스크톱에서 로컬 리소스를 사용할 수 있지만 ESX/ESXi 3.5 호스트에서 생성된 Windows 7 또는 Windows Vista View 데스크톱은 3D 와 Windows Aero 효과를 사용할 수 없습니다. Windows 7 또는 Windows Vista 호스트에서 로컬로 사용하기 위해 데스크톱을 체크아웃하더라도 이러한 제한 사항은 적용됩니다. Windows Aero 및 3D 효과는 vSphere 4.x 이상을 사용하여 View 데스크톱을 생성하는 경우에만 사용할 수 있습니다.

로컬 모드를 요구하여 데이터 센터 리소스 절약

로컬 모드에서만 View 데스크톱을 다운로드하고 사용하도록 요구하면 대역폭, 메모리 및 CPU 리소스와 관련된 데이터 센터 비용을 절감할 수 있습니다. 이 전략은 직원 및 계약자의 자기 PC 가져오기 프로그램으로도 불립니다.

체크아웃

View 데스크톱을 체크아웃하는 경우 가상 컴퓨터의 상태를 보존하기 위해 vCenter 에 스냅샷이 생성됩니다. 다른 사용자가 액세스할 수 없도록 데스크톱의 vCenter Server 버전은 잠겨 있습니다. View 데스크톱이 잠기면 온라인 데스크톱 전원 켜기, 스냅샷 생성, 가상 컴퓨터 설정 변경 등과 같은 작업을 포함한 vCenter Server 작업을 사용할 수 없습니다. 그러나 View 관리자는 여전히 로컬 세션을 모니터링하고 vCenter Server 버전에 액세스하여 액세스를 제거하거나 데스크톱을 롤백할 수 있습니다.

백업

백업하는 동안 체크아웃된 가상 컴퓨터의 상태를 보존하기 위해 클라이언트 시스템에 스냅샷이 생성됩니다. 이 스냅샷과 vCenter 스냅샷 간의 델타가 vCenter 에 복제되고 이곳의 스냅샷과 병합됩니다. 모든 새 데이터와 구성으로 vCenter Server 의 View 데스크톱을 업데이트하지만 로컬 데스크톱은 로컬 시스템에서 체크아웃 상태를 유지하고 vCenter Server 에서는 계속 잠겨 있습니다.

롤백

롤백하는 동안 로컬 View 데스크톱이 삭제되고 vCenter Server 에서 잠금이 해제됩니다. 데스크톱을 다시 체크아웃할 때까지 클라이언트가 vCenter Server 의 View 데스크톱에 직접 연결됩니다.

체크인

View 데스크톱을 체크인하는 경우 가상 컴퓨터의 상태를 보존하기 위해 클라이언트 시스템에 스냅샷이 생성됩니다. 이 스냅샷과 vCenter 스냅샷 간의 델타가 vCenter 에 복제되고 이곳의 스냅샷과 병합됩니다. vCenter Server 의 가상 컴퓨터가 잠금 해제됩니다. 데스크톱을 다시 체크아웃할 때까지 클라이언트가 vCenter Server 의 View 데스크톱에 직접 연결됩니다.

각 로컬 시스템의 데이터는 AES 로 암호화되어 있습니다. 기본값은 128 비트 암호화이지만 192 비트 또는 256 비트 암호화도 구성할 수 있습니다. 데스크톱 수명은 정책을 통해 제어됩니다. 클라이언트와 View 연결 서버 간의 연결이 끊어질 경우, 사용자는 서버와 연결되지 않고 사용할 수 있는 최대 시간 동안만 데스크톱을 사용할 수 있으며 그 이후에는 액세스가 거부됩니다. 마찬가지로 사용자 액세스 권한이 제거되는 경우 캐시가 만료될 때 또는 클라이언트가 View 연결 서버를 통해 이 변경 사항을 감지한 후에는 클라이언트 시스템에 액세스할 수 없습니다.

View Client with Local Mode 는 다음과 같은 제한 사항이 있습니다.

- Local Mode 구성 요소를 포함하는 View 라이센스를 보유하고 있어야 합니다.
- 롤백 또는 체크인하는 동안에는 최종 사용자가 로컬 데스크톱에 액세스할 수 없습니다.
- 이 기능은 vCenter Server 에서 관리하는 가상 컴퓨터에서만 사용할 수 있습니다.
- 로컬 모드로 실행되는 데스크톱에서 View 개인 설정 관리를 사용할 수 없습니다.
- 로컬 모드에 다운로드하여 사용하는 View 데스크톱의 경우, VMware ThinApp 으로 생성한 애플리케이션 패키지 할당을 지원하지 않습니다. 데스크톱 롤백으로 인해 View 연결 서버가 롤백된 데스크톱의 ThinApp 에 대해 잘못된 정보를 갖게 될 수 있습니다.
- 보안 상 이유로 View 데스크톱에서 호스트 CD-ROM 에 액세스할 수 없습니다.
- 또한 보안 상 이유로 로컬 시스템과 View 데스크톱 간에 파일 및 폴더와 같은 시스템 개체 또는 텍스트를 복사 및 붙여 넣을 수 없습니다.

로컬 컴퓨터에 연결된 USB 디바이스에 액세스

관리자는 View 데스크톱에서 썸 플래시 드라이브, VoIP(voice-over-IP) 디바이스, 프린터와 같은 USB 디바이스를 사용하는 기능을 구성할 수 있습니다. 이러한 기능을 USB 리디렉션이라 부릅니다.

이 기능을 사용하면 로컬 클라이언트 시스템에 연결된 USB 디바이스의 대부분을 View Client 메뉴에서 사용할 수 있습니다. 메뉴를 사용해 디바이스를 연결하거나 연결을 끊습니다.

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.

참고 USB 리디렉션 기능이 있는 경우, View 데스크톱에서 iPad 에 연결하고 관리할 수 있습니다. 예를 들어, View 데스크톱에 설치된 iTunes 와 iPad 를 동기화할 수 있습니다.

키보드와 포인팅 디바이스와 같은 휴먼 인터페이스 디바이스와 스마트 카드 판독기 등 USB 디바이스는 메뉴로 나타나지 않지만 View 데스크톱에서 사용할 수 있습니다. View 데스크톱과 로컬 컴퓨터는 이들 디바이스를 동시에 사용합니다.

이 기능은 다음과 같은 제한 사항이 있습니다.

- View Client 의 메뉴를 통해 USB 디바이스에 액세스하여 View 데스크톱에서 해당 디바이스를 사용하는 경우, 로컬 컴퓨터에서는 디바이스에 접근할 수 없습니다.
- Microsoft 터미널 서버에 연결된 View 데스크톱 또는 Windows 2000 시스템에서는 USB 리디렉션을 지원하지 않습니다.

View 데스크톱에서 인쇄

가상 인쇄 기능을 사용하면 Windows 시스템에서 View Client 를 사용하는 최종 사용자가 추가 인쇄 드라이버를 View 데스크톱에 설치할 필요 없이 View 데스크톱에서 로컬 또는 네트워크 프린터를 사용할 수 있습니다. 위치 기반 인쇄 기능을 사용하여 끝점 클라이언트 디바이스에서 가장 가까운 프린터에 View 데스크톱을 매핑할 수 있습니다.

가상 인쇄를 사용할 경우, 프린터가 로컬 Windows 컴퓨터에 추가되고 나면 View 는 View 데스크톱에서 사용할 수 있는 프린터 목록에 해당 프린터를 추가합니다. 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 View 데스크톱에 프린터 드라이버를 계속 설치할 수 있습니다.

USB 프린터에 인쇄 작업을 보내기 위해 USB 리디렉션 기능을 사용하거나 가상 인쇄 기능을 사용할 수 있습니다.

위치 기반 인쇄 기능은 Windows 및 비 Windows 클라이언트 시스템 모두에서 사용할 수 있습니다. 위치 기반 인쇄 기능을 사용하여 IT 조직은 끝점 클라이언트 디바이스에서 가장 가까운 프린터에 View 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 View 데스크톱에 설치되어 있어야 합니다.

View 데스크톱에 멀티미디어 스트리밍

Wyse MMR(멀티미디어 리디렉션)은 멀티미디어 파일이 View 데스크톱으로 스트리밍될 때 고화질 재생이 사용되도록 설정합니다.

로컬 디코더가 클라이언트에 존재해야 하기 때문에 MMR 기능은 클라이언트 시스템이 지원하는 미디어 파일 형식을 지원합니다. 파일 형식에는 특히 MPEG2, WMV, AVI 및 WAV 가 포함됩니다.

이 기능은 다음과 같은 제한 사항이 있습니다.

- 최고의 품질을 위해 Windows Media Player 10 이상을 사용하고 이를 로컬 컴퓨터 또는 클라이언트 액세스 디바이스 및 View 데스크톱 모두에 설치합니다.
- 기본적으로 9427 인 Wyse MMR 포트는 View 데스크톱의 방화벽 예외로서 추가되어야 합니다.
- MMR 은 Windows 7 클라이언트 또는 가상 데스크톱에서 지원되지 않습니다.

  MMR 은 Windows 7 가상 데스크톱에서 지원되지 않지만 Windows 7 에 RAM 1GB 및 2 개의 가상 CPU 가 있는 경우 PCoIP 를 사용하여 기본 해상도에서 480p 및 720p 형식 비디오를 재생할 수 있습니다. 1080p 의 경우 HD 품질을 얻으려면 창 크기를 더 작게 조정해야 할 수 있습니다.

단일 로그온을 사용한 View 데스크톱 로그인

단일 로그온(SSO) 기능을 사용하여 최종 사용자에게 로그인하라는 메시지가 한 번만 나타나도록 View Manager 를 구성할 수 있습니다.

단일 로그온 기능을 사용하지 않을 경우 최종 사용자는 두 번 로그인해야 합니다. View Connection Server 에 로그인하라는 메시지가 먼저 나온 다음 View 데스크톱에 로그인하라는 메시지가 나타납니다. 또한 스마트 카드를 사용할 경우 스마트 카드 판독기에서 PIN 에 대해 메시지를 표시할 때 사용자가 또 로그인해야 하기 때문에 최종 사용자는 세 번 로그인해야 합니다.

이 기능에는 Windows XP 의 GINA(Graphical Identification and Authentication) 동적 연결 라이브러리 및 Windows Vista 의 자격 증명 공급자 동적 연결 라이브러리가 포함됩니다.

View 데스크톱에 다중 모니터 사용

디스플레이 프로토콜과 관계 없이 여러 모니터를 View 데스크톱과 사용할 수 있습니다.

VMware 의 디스플레이 프로토콜 PCoIP 를 사용할 경우 각 모니터에 대해 디스플레이 해상도 및 회전을 개별적으로 조정할 수 있습니다. PCoIP 는 스팬 모드 세션이 아니라 다중 모니터 세션을 허용합니다.

스팬 모드 원격 세션은 실제로 단일 모니터 세션입니다. 여러 모니터의 크기 및 해상도가 동일해야 하며 모니터 레이아웃이 경계선 상자 내에 맞아야 합니다. 애플리케이션 창을 최대화하면 창이 모든 모니터에 나뉘어 표시됩니다. Microsoft RDP 6 은 스팬 모드를 사용합니다.

다중 모니터 세션에서 모니터마다 해상도와 크기는 다를 수 있으며 모니터를 세로로 회전시킬 수 있습니다. 애플리케이션 창을 최대화하면 창이 해당 모니터의 전체 화면으로 확대됩니다.

이 기능은 다음과 같은 제한 사항이 있습니다.

- PCoIP 를 사용하는 경우 View 데스크톱을 표시하는 데 사용할 수 있는 모니터는 최대 4 대입니다. 3D 기능이 활성화되면 최대 2 대의 모니터가 최대 해상도인 1920x1200 으로 지원됩니다. 회전식 모니터는 지원하지만 스택형 모니터는 지원하지 않습니다.
- Microsoft RDP 7 을 사용할 경우, View 데스크톱을 표시하는 데 사용할 수 있는 최대 모니터 수는 16 대입니다.
- Microsoft RDP 디스플레이 프로토콜을 사용할 경우 Microsoft RDC(Remote Desktop Connection) 6.0 이상이 View 데스크톱에 설치되어 있어야 합니다.
- View 데스크톱을 로컬 모드에서 사용할 경우 원격 디스플레이 프로토콜은 사용되지 않습니다. 스팬 모드에서 최대 2 대의 모니터를 사용할 수 있습니다.

3 한 곳에서 데스크톱 풀 관리

가상 데스크톱 한 대 또는 수백 대를 포함하는 풀을 생성할 수 있습니다. 가상 시스템, 물리적 시스템, Windows 터미널 서비스 서버를 데스크톱 소스로 사용할 수 있습니다. 가상 시스템 1 대를 기본 이미지로 생성하면 VMware View 에서 해당 이미지를 사용해 가상 데스크톱 풀을 생성할 수 있습니다. VMware ThinApp 으로 애플리케이션을 쉽게 설치하거나 풀로 스트리밍할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- "데스크톱 풀의 장점," (29 페이지)
- "스토리지 요구 사항 축소 및 관리," (30 페이지)
- "애플리케이션 프로비저닝," (32 페이지)
- "Active Directory GPO 를 사용한 사용자 및 데스크톱 관리," (34 페이지)

데스크톱 풀의 장점

VMware View 는 중앙 집중화된 관리 기능으로 데스크톱의 풀을 생성하고 프로비저닝할 수 있습니다.

다음 소스 중 하나에서 가상 데스크톱 풀을 생성합니다.

- 물리적 데스크톱 PC 또는 Windows 터미널 서비스 서버와 같은 물리적 시스템
- ESX/ESXi 호스트에 호스팅되고 vCenter Server 에서 관리하는 가상 시스템
- VMware Server 또는 View Agent 를 지원하는 다른 가상 플랫폼에서 실행되는 가상 시스템

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 View 데스크톱을 항상 확보할 수 있습니다.

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

- View 데스크톱의 기본값으로 사용할 원격 디스플레이 프로토콜과 최종 사용자의 기본값 무시 허용 여부를 지정합니다.
- Adobe Flash 애니메이션을 조절하는 디스플레이 품질과 대역폭을 구성합니다.
- 가상 시스템을 사용하는 경우 사용하지 않을 때 가상 시스템 전원을 끌지, 함께 삭제할지 여부를 지정합니다.
- vSphere 4.1 이상을 사용하는 경우 Microsoft Sysprep 사용자 지정 규격 또는 VMware 에서 QuickPrep 사용 여부를 지정합니다. Sysprep 은 풀의 각 가상 시스템에 대해 고유한 SID 및 GUID 를 생성합니다.

- View 데스크톱을 다운로드하여 로컬 클라이언트 시스템에서 실행할 수 있을지 또는 실행해야 하는지 여부를 지정합니다.

그 외에도 데스크톱 풀은 다양한 장점을 제공합니다.

전용 할당 풀 특정 View 데스크톱에 각 사용자를 할당하고 각 로그인 시 동일한 가상 데스크톱으로 돌아갑니다. 사용자는 데스크톱을 개인 설정하고 애플리케이션을 설치하고 데이터를 저장할 수 있습니다.

부동 할당 풀 엄격하게 통제된 환경을 제공하여 각자 사용 후 가상 데스크톱을 선택적으로 삭제하고 재생성할 수 있습니다. 부동 할당 데스크톱은 각 데스크톱에 필요한 애플리케이션을 로드하고 모든 데스크톱이 필요한 데이터에 대한 액세스 권한을 가지고 있는 컴퓨터 랩 또는 키오스크 환경과 유사합니다.

부동 할당 풀을 사용하면 교대 근무 사용자들이 사용할 수 있는 데스크톱 풀을 생성할 수도 있습니다. 예를 들어 사용자가 한 번에 100 명씩 교대 근무를 하는 경우, 사용자 300 명이 데스크톱 100 대로 구성된 풀을 사용할 수 있습니다.

스토리지 요구 사항 축소 및 관리

vCenter Server 로 관리되는 가상 데스크톱을 사용하면 이전에 가상화된 서버에만 사용할 수 있던 모든 스토리지 효율성이 제공됩니다. 풀의 모든 데스크톱이 가상 디스크를 기본 이미지와 공유하기 때문에 View Composer 를 사용하면 스토리지가 더 많이 절약됩니다.

- vSphere 로 스토리지 관리(30 페이지)

  VMware vSphere 로 디스크 볼륨과 파일 시스템을 가상화하면 데이터의 물리적 보관 장소를 고려할 필요 없이 스토리지를 관리하고 구성할 수 있습니다.

- View Composer 로 스토리지 요구 사항 축소(31 페이지)

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

vSphere 로 스토리지 관리

VMware vSphere 로 디스크 볼륨과 파일 시스템을 가상화하면 데이터의 물리적 보관 장소를 고려할 필요 없이 스토리지를 관리하고 구성할 수 있습니다.

Fibre Channel SAN 어레이, iSCSI SAN 어레이, NAS 어레이는 폭넓게 사용되는 스토리지 기술로 VMware vSphere 는 이들 기술을 지원해 다양한 데이터 센터 스토리지의 요건을 충족시킵니다. 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.

View 4.5 이상 및 vSphere 4.1 이상에서는 다음 기능을 사용할 수 있습니다.

- vStorage 씬 프로비저닝을 통해 최소한의 디스크 공간에서 시작하고 이후에 필요한 디스크 공간 추가
- 계층화된 스토리지를 통해 고성능 스토리지, 저비용 스토리지 계층의 View 환경에 가상 디스크를 배포해 성능과 비용 효율성 극대화
- 게스트 운영 체제의 가상 시스템 스왑 파일에 대한 ESX/ESXi 호스트의 로컬 스토리지

View 5.1 이상 및 vSphere 5.0 이상에서는 다음 기능을 사용할 수 있습니다.

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

  동시에 많은 데스크톱이 시작되고 바이러스 백신 스캔을 실행할 때 이 CBRC(Content Based Read Cache)를 사용하면 부트 스톰이 발생하는 동안 IOPS 를 줄여 성능을 향상시킬 수 있습니다. 스토리지 시스템에서 전체 OS 를 반복해서 읽는 대신, 호스트는 캐시에서 공통 데이터 블록을 읽을 수 있습니다.

- ESXi 호스트가 최대 32 대인 클러스터에 데스크톱 풀을 배포할 수 있지만 NFS 데이터스토어에 복제 디스크를 저장해야 합니다.

  복제 디스크는 NFS 데이터스토어에 저장되어야 하지만 OS 디스크 및 영구 디스크는 NFS 또는 VMFS 데이터스토어에 저장될 수 있습니다.

View Composer 로 스토리지 요구 사항 축소

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

View Composer 는 기본 이미지 또는 상위 가상 시스템을 사용하고 최고 1,000 개의 링크드 클론 가상 시스템의 풀을 생성합니다. 각 링크드 클론은 고유 호스트 이름 및 IP 주소를 사용하여 독립 데스크톱처럼 작동하지만 링크드 클론은 매우 적은 양의 스토리지를 필요로 합니다.

동일한 데이터스토어의 복제 및 링크드 클론

링크드 클론 데스크톱 풀을 생성할 경우 전체 클론이 먼저 상위 가상 시스템에서 만들어집니다. 전체 클론 또는 복제본 및 링크드 클론은 동일한 데이터스토어 또는 LUN(논리 장치 번호)에 배치될 수 있습니다. 필요한 경우 재조정 기능을 사용하여 한 LUN 에서 다른 LUN 으로 복제 및 링크드 클론을 이동시킬 수 있습니다.

다른 데이터스토어의 복제 및 링크드 클론

또는 다른 성능 특징을 가진 개별 데이터스토어에 View Composer 복제본 및 링크드 클론을 배치할 수 있습니다. 예를 들어 SSD(반도체 드라이브)에 복제 가상 시스템을 저장할 수 있습니다. SSD 는 스토리지 용량이 적고 읽기 성능이 높아 일반적으로 초당 수만 개의 IOPS(초당 입출력)를 지원합니다. 일반적인 회전 미디어 백업 데이터스토어에 링크드 클론을 저장할 수 있습니다. 이러한 디스크는 성능은 낮지만 비용이 높지 않고 스토리지 용량은 더 높아 큰 풀에 링크드 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 View 를 위한 스토리지 고려 사항* 모범 사례 안내를 참조하십시오.

페이징 및 임시 파일의 삭제 가능한 디스크

또한 링크드 클론 풀을 생성할 경우 삭제 가능한 개별 가상 디스크를 선택적으로 구성하여 사용자 세션 중 생성된 게스트 운영 체제의 페이징 및 임시 파일을 저장할 수 있습니다. 가상 시스템의 전원이 꺼진 경우 View Manager 가 삭제 가능한 디스크를 삭제합니다. 삭제 가능한 디스크를 사용하면 링크드 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 Composer 는 각 가상 데스크톱의 개별적인 영구 가상 디스크를 선택적으로 생성할 수 있습니다. 최종 사용자의 Windows 프로파일 및 애플리케이션 데이터는 영구 디스크에 저장됩니다. 링크드 클론을 새로 고치거나 재구성되거나 재조정되더라도 영구 가상 디스크의 컨텐츠가 보존됩니다. VMware 에서는 개별 데이터스토어에 View Composer 영구 디스크를 보관할 것을 권장합니다. 그런 다음 영구 디스크를 보관하는 전체 LUN 을 백업할 수 있습니다.

부동, 상태 비저장 데스크톱용 로컬 데이터스토어

링크드 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 View 환경에서는 유용하지만 다른 환경에서는 적절하지 않습니다.

사용자 환경의 View 데스크톱이 상태를 저장하지 않는 경우, 로컬 데이터스토어를 사용하면 잘 작동됩니다. 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 복제 및 링크드 클론을 저장할 수 없고 실제로 VMware 에서는 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, 링크드 클론을 로컬 데이터스토어에 성공적으로 배포할 수 있습니다.

자세한 내용은 *VMware View 관리* 문서의 데스크톱 풀 생성에 대한 장을 참조하십시오.

애플리케이션 프로비저닝

VMware View 는 여러 가지 애플리케이션 프로비저닝 방법을 제공합니다. 기존 애플리케이션 프로비저닝 기법을 사용하거나, VMware ThinApp 으로 생성된 애플리케이션 패키지를 배포하고, View Composer 기본 이미지의 일부로 애플리케이션을 배포할 수 있습니다.

- View Composer 로 애플리케이션 및 시스템 업데이트 배포(32 페이지)

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

- View Administrator 에서 VMware ThinApp 애플리케이션 관리(33 페이지)

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

- 기존 프로세스를 사용한 애플리케이션 프로비저닝(33 페이지)

  VMware View 를 사용하면 회사에서 현재 사용하는 애플리케이션 프로비저닝 기술을 계속 사용할 수 있습니다. 서버 CPU 사용 및 스토리지 I/O 를 관리하고 사용자가 애플리케이션을 설치하도록 허용되는지 여부를 결정하는 두 가지 추가 고려 사항이 있습니다.

View Composer 로 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)

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.

View Administrator 에서 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.

ThinApp 은 기본 운영 체제와 라이브러리, 프레임워크에서 애플리케이션을 분리하고 해당 애플리케이션을 단일 실행 파일로 묶어 애플리케이션 패키지를 생성함으로써 애플리케이션을 가상화합니다. View 4.5 에서는 View Administrator 를 사용해 데스크톱과 풀에 ThinApp 애플리케이션을 배포할 수 있습니다.

ThinApp 으로 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 가상 데스크톱에 설치된 ThinApp 패키지 모두 애플리케이션 저장소용 스토리지를 고려하여 구성합니다.

참고 로컬 모드에 다운로드하여 사용하는 View 데스크톱의 경우, VMware ThinApp 으로 생성한 애플리케이션 패키지 할당을 지원하지 않습니다. 데스크톱 롤백으로 인해 View Connection Server 가 롤백된 데스크톱의 ThinApp 에 대해 잘못된 정보를 갖게 될 수 있습니다.

기존 프로세스를 사용한 애플리케이션 프로비저닝

VMware View 를 사용하면 회사에서 현재 사용하는 애플리케이션 프로비저닝 기술을 계속 사용할 수 있습니다. 서버 CPU 사용 및 스토리지 I/O 를 관리하고 사용자가 애플리케이션을 설치하도록 허용되는지 여부를 결정하는 두 가지 추가 고려 사항이 있습니다.

동시에 많은 가상 데스크톱으로 애플리케이션을 푸시(push)할 경우 CPU 사용 및 스토리지 I/O 에서 사용량이 많아지는 것을 볼 수 있습니다. 이러한 피크 워크로드는 데스크톱 성능에 적지 않은 영향을 미칩니다. 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.

사용자에게 사용자 자신의 애플리케이션을 설치하고 가상 데스크톱의 수명 기간 동안 해당 애플리케이션을 지속시키기 위한 확실한 요구 사항이 있는 경우, 애플리케이션 프로비저닝에 View Composer를 사용하는 대신 전체 영구 데스크톱을 생성하고 사용자에게 애플리케이션을 설치하도록 허용할 수 있습니다.

Active Directory GPO를 사용한 사용자 및 데스크톱 관리

VMware View에는 View 구성 요소 및 View 데스크톱의 관리 및 구성을 집중시키기 위한 그룹 정책 관리(ADM) 템플릿이 많습니다.

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
- View Connection Server 구성
- View Client 구성
- View Agent 구성

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

GPO를 사용하여 View Administrator 사용자 인터페이스(UI)에서 사용할 수 있는 모든 정책을 설정할 수 있습니다. 또한 GPO를 사용하여 UI에서 사용할 수 없는 정책을 설정할 수 있습니다. ADM 템플릿을 통해 사용할 수 있는 전체 설정 목록 및 설명은 *VMware View 관리* 설명서에 나와 있습니다.

4 아키텍처 설계 요소 및 계획 지침

일반적인 VMware View 아키텍처 설계는 vSphere 4.1 이상의 인프라를 사용해 가상 데스크톱을 최대 10,000 대까지 지원하는 구성 요소로 이루어진 팟 전략을 사용합니다. 팟 정의는 하드웨어 구성, 사용한 View 및 vSphere 소프트웨어 버전, 기타 환경별 설계 요소에 따라 다를 수 있습니다.

이 아키텍처는 확장 가능한 표준 설계를 제공하므로 기업 환경 및 별도의 요구 사항에 적용할 수 있습니다. 본 장에서는 IT 설계자와 기획자가 VMware View 솔루션 배포에 실질적으로 필요한 사항을 이해할 수 있도록 메모리, CPU, 스토리지 용량, 네트워크 구성 요소, 하드웨어 요구 사항에 대해 자세히 설명합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- "가상 시스템 요구 사항," (35 페이지)
- "VMware View ESX/ESXi 노드," (40 페이지)
- "특정 작업자 유형의 데스크톱 풀," (41 페이지)
- "데스크톱 가상 시스템 구성," (45 페이지)
- "vCenter 및 View Composer 가상 시스템 구성과 데스크톱 풀 최대값," (46 페이지)
- "View Connection Server 최대값 및 가상 시스템 구성," (47 페이지)
- "View 전송 서버 가상 시스템 구성 및 스토리지," (48 페이지)
- "vSphere 클러스터," (49 페이지)
- "VMware View 빌드 블록," (50 페이지)
- "VMware View 팟," (54 페이지)

가상 시스템 요구 사항

View 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(36 페이지)

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

- 가상 데스크톱의 메모리 요구 사항 계산(37 페이지)

  RAM 은 PC 용보다 서버용이 더 비쌉니다. RAM 이 전체 서버 하드웨어 비용에서 차지하는 비율이 높고 총 스토리지 용량이 필요하므로 데스크톱 배포 계획에서 메모리 할당량을 올바르게 결정하는 것이 중요합니다.

- 가상 데스크톱의 CPU 요구 사항 계산(39 페이지)

  CPU 를 계산하려면 회사 내 다양한 작업자 유형의 평균 CPU 사용률 정보를 수집해야 합니다. 그리고 가상화 오버헤드와 가장 많이 사용하는 기간에 대비하기 위해 처리 능력의 10-25%을 추가로 계산해야 합니다.

- 적절한 시스템 디스크 크기 선택(40 페이지)

  디스크 공간을 할당할 때는 운영 체제와 애플리케이션을 비롯해 사용자가 설치 또는 생성할 수 있는 추가 컨텐츠에 대한 공간만 충분히 제공하십시오. 일반적으로 이 공간은 물리적 PC 의 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 CPU 와 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.

로컬 모드로만 데스크톱을 사용하는 직원

로컬 시스템에서만 View 데스크톱을 다운로드하고 실행하는 사용자로 대역폭, 메모리, CPU 리소스와 관련된 데이터 센터 비용을 절감합니다. 예정된 복제 작업을 통해 시스템과 데이터를 백업합니다. 관리자는 최종 사용자의 시스템이 잠기는 것을 방지하기 위해 View Manager 에 접속해야 하는 빈도를 구성합니다.

키오스크 사용자

이들 사용자는 공용 위치에 있는 데스크톱을 공유해야 합니다. 키오스크 사용자에는 교실이나 간호사 실에서 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 데스크톱의 메모리 요구 사항 계산

RAM 은 PC 용보다 서버용이 더 비쌉니다. RAM 이 전체 서버 하드웨어 비용에서 차지하는 비율이 높고 총 스토리지 용량이 필요하므로 데스크톱 배포 계획에서 메모리 할당량을 올바르게 결정하는 것이 중요합니다.

RAM 을 너무 낮게 할당하면 메모리 스와핑이 너무 많이 발생하여 스토리지 입출력에 악영향을 미칠 수 있습니다. RAM 을 너무 높게 할당하면 각 가상 시스템에 대한 게스트 운영 체제의 페이징 파일과 스왑 및 일시 중단 파일이 너무 커져 스토리지 용량에 악영향을 미칠 수 있습니다.

참고 본 항목에서는 View 데스크톱에 대한 원격 액세스의 메모리 할당과 관련된 문제를 해결합니다. 사용자가 클라이언트 시스템에서 로컬 모드로 View 데스크톱을 실행하면 클라이언트 디바이스에서 사용할 수 있는 메모리 가운데 일부를 사용합니다.

클라이언트 컴퓨터에서 호스트 운영 체제를 실행하는 경우에는 클라이언트 컴퓨터와 View 데스크톱의 애플리케이션과 View 데스크톱의 운영 체제에도 메모리가 필요합니다. VMware 는 Windows XP 및 Windows Vista 의 경우 2GB 이상, Windows 7 의 경우 3GB 이상을 권장합니다.

vCenter Server 에 구성되어 있는 데스크톱을 체크아웃해 로컬 클라이언트 시스템에서 수용할 수 있는 양보다 많은 메모리를 요청하는 경우에는 Windows 레지스트리 설정을 변경해야만 체크아웃할 수 있습니다. 자세한 내용은 *VMware View 관리* 설명서를 참조하십시오.

RAM 크기가 성능에 미치는 영향

RAM 을 할당할 때는 지나치게 보수적인 설정을 선택하지 마십시오. 다음을 고려하십시오.

- RAM 할당이 부족하면 게스트 스와핑이 과도하게 발생해 성능 저하와 스토리지 입출력 로드 증가를 유발하는 입출력이 생성될 수 있습니다.
- VMware ESX/ESXi 는 투명한 메모리 공유, 메모리 조정과 같은 정교한 메모리 리소스 관리 알고리즘을 지원하여, 지정된 게스트 RAM 할당 지원에 필요한 물리적 RAM 을 크게 줄일 수 있습니다. 예를 들어 가상 데스크톱에 2GB 를 할당하더라도 물리적 RAM 에서는 이 가운데 일부만 사용합니다.
- 가상 데스크톱 성능은 응답 시간에 민감하므로 ESX/ESXi 호스트에서는 RAM 예약 설정 값을 0 이외의 값으로 설정하십시오. 작업이 없지만 사용 중인 데스크톱에 일부 RAM 을 예약하면 디스크에 완전히 스와핑되지 않습니다. 이는 또한 ESX/ESXi 스왑 파일에서 사용하는 스토리지 공간을 줄일 수 있습니다. 그러나 예약 설정이 높으면 ESX/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 페이지와 최대 절전 모드 파일을 찾고 ESX/ESXi 호스트의 파일 시스템을 사용해 ESX/ESXi 스왑 및 일시 중단 파일을 찾습니다.

Windows 페이지 파일 기본적으로 파일 크기는 게스트 RAM 의 150%에 해당합니다. 기본적으로 C:₩pagefile.sys 에 위치한 이 파일에 빈번하게 액세스하기 때문에 씬 프로비저닝된 스토리지 용량이 커집니다. 링크드 클론 가상 시스템에서 가상 시스템 전원이 꺼지면 삭제되는 개별 가상 디스크에 페이지 파일과 임시 파일이

	리디렉션될 수 있습니다. 삭제 가능한 페이지 파일 리디렉션은 스토리지를 절약하고 링크드 클론 증가 속도를 낮춰 성능을 향상할 수 있습니다. Windows 에서 이 크기를 조정할 수 있지만 이는 애플리케이션 성능에 악영향을 미칠 수 있습니다.
랩톱용 Windows 최대 절전 모드 파일	파일 크기는 게스트 RAM 의 100%와 동일합니다. View Client with Local Mode 를 사용해도 이 파일은 View 배포에 불필요하기 때문에 안전하게 삭제할 수 있습니다.
ESX/ESXi 스왑 파일	확장명은 .vswp 이며 가상 시스템 RAM 의 100% 미만을 예약하는 경우 생성됩니다. 이 스왑 파일의 크기는 게스트 RAM 에서 예약되지 않은 부분과 동일합니다. 예를 들어 게스트 RAM 의 50%가 예약되어 있고 게스트 RAM 이 2GB 이면 ESX/ESXi 스왑 파일은 1GB 입니다. ESX/ESXi 호스트 또는 클러스터의 로컬 데이터스토어에 이 파일을 저장할 수 있습니다.
ESX/ESXi 일시 중단 파일	확장명이 .vmss 인 이 파일은 데스크톱 풀 로그오프 정책을 설정해 최종 사용자의 로그오프로 가상 데스크톱이 일시 중단될 때 생성됩니다. 파일 크기는 게스트 RAM 크기와 동일합니다.

PCoIP 사용 시 특정 모니터 구성을 위한 RAM 크기

VMware 의 디스플레이 프로토콜인 PCoIP 를 사용하면 최종 사용자용으로 구성한 모니터 수와 화면 해상도에 따라 ESX/ESXi 호스트에 필요한 추가 RAM 양이 다릅니다. 표 4-1 은 다양한 구성에 필요한 오버헤드 RAM 양을 나타냅니다. 열에 표시된 메모리 양은 다른 PCoIP 기능에 필요한 메모리 양을 더한 값입니다.

표 4-1. PCoIP 클라이언트 디스플레이 오버헤드

화면 해상도 표준	너비(픽셀)	높이(픽셀)	1-모니터 오버헤드	2-모니터 오버헤드	4-모니터 오버헤드
VGA	640	480	2.34MB	4.69MB	9.38MB
SVGA	800	600	3.66MB	7.32MB	14.65MB
720p	1280	720	7.03MB	14.65MB	28.13MB
UXGA	1600	1200	14.65MB	29.30MB	58.59MB
1080p	1920	1080	15.82MB	31.64MB	63.28MB
WUXGA	1920	1200	17.58MB	35.16MB	70.31MB
QXGA	2048	1536	24.00MB	48.00MB	96.00MB
WQXGA	2560	1600	31.25MB	62.50MB	125.00MB

이들 요구 사항을 고려하는 경우에는 할당된 RAM 의 가상 시스템 구성은 변경되지 않는다는 점에 유의하십시오. 즉, 애플리케이션용으로 RAM 1GB 를 할당하고 이중 1080p 모니터용으로 31MB 를 할당할 필요가 없습니다. 대신, 오버헤드 RAM 을 고려해 각 ESX/ESXi 호스트에 필요한 전체 물리적 RAM 을 계산하십시오. 오버헤드 RAM 에 게스트 운영 체제 RAM 을 더하고 가상 시스템 수를 곱하십시오.

참고 View 5.0 이상에서 제공하는 3D 렌더링 기능을 사용하려면 각 Windows 7 View 데스크톱에 대해 64MB ~ 128MB 사이의 VRAM 을 할당해야 합니다. 이 비 하드웨어 가속 그래픽 기능을 통해 Windows Aero 테마 또는 Google Earth 와 같은 3D 애플리케이션을 사용할 수 있습니다. 3D 렌더링이 활성화될 때 최대 모니터 수는 2 대입니다.

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 Windows XP 데스크톱, 32 비트 Windows Vista 와 Windows 7 데스크톱에 1GB, 64 비트 Windows 7 데스크톱에 2GB 를 할당하는 것이 좋습니다. 시험 단계에서는 다양한 작업자 유형이 사용하는 디스크 공간과 성능을 모니터링하고 각 작업자 풀에 가장 적합한 설정을 찾을 때까지 조정하십시오.

가상 데스크톱의 CPU 요구 사항 계산

CPU 를 계산하려면 회사 내 다양한 작업자 유형의 평균 CPU 사용률 정보를 수집해야 합니다. 그리고 가상화 오버헤드와 가장 많이 사용하는 기간에 대비하기 위해 처리 능력의 10-25%을 추가로 계산해야 합니다.

참고 본 항목에서는 원격으로 View 데스크톱에 액세스할 경우의 CPU 요구 사항과 관련된 문제를 해결합니다. 사용자가 클라이언트 시스템에서 로컬 모드로 View 데스크톱을 실행하는 경우 View 데스크톱은 클라이언트 디바이스에서 사용 가능한 CPU 를 최대 2 개까지 사용합니다.

작업자 유형에 따라 CPU 요구 사항이 다릅니다. 시험 단계에서는 가상 시스템의 Perfmon, ESX/ESXi 의 esxtop, 또는 vCenter 성능 모니터링 툴과 같은 성능 모니터링 툴을 사용해 이들 작업자 그룹의 평균 및 최고 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. PCoIP 디스플레이 프로토콜을 사용해 Windows 7 데스크톱에서 720p 비디오를 재생해야 하는 등 계산 집약적 작업의 경우에는 이중 가상 CPU 를 사용하는 것이 좋습니다.
- 다른 경우에는 일반적으로 단일 가상 CPU 를 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 View Composer 로 이미지를 업데이트합니다.
- 소수의 사용자가 로그인해 사용량이 적을 시간에 바이러스 백신 및 소프트웨어 업데이트를 예약합니다.
- 업데이트 시간을 분산 또는 무작위로 설정합니다.

비공식적 방법으로 처음 크기를 계산하려면 각 가상 시스템당 최소 계산 능력으로 CPU 코어의 1/8~1/10 이 필요하다고 가정합니다. 즉 코어당 가상 시스템 8~10 대를 사용하는 시험 단계를 계획하십시오. 예를 들어 코어당 가상 시스템 8 대를 예상하고 2 소켓 8 코어 ESX/ESXi 호스트를 보유하고 있는 경우에는 시험 기간 동안 가상 시스템 128 대를 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 컨텐츠에 대한 공간만 충분히 제공하십시오. 일반적으로 이 공간은 물리적 PC 의 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.
- 앞으로의 확장에 대비하면서도 과도하지 않은 가상 디스크 크기를 선택하십시오.
- 사용자 생성 컨텐츠 및 사용자 설치 애플리케이션에 대해 중앙 집중화된 파일 공유 또는 View Composer 영구 디스크를 사용하십시오.

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

- ESX/ESXi 일시 중단 파일은 가상 시스템에 할당된 RAM 용량과 같습니다.
- Windows 페이지 파일은 RAM 의 150%와 동일합니다.
- 로그 파일은 각 가상 시스템마다 약 100MB 의 공간을 차지합니다.
- 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 Composer 를 사용하면 `.vmdk` 파일 크기가 점차 늘어나지만 View Composer 새로 고침 작업을 예약하고, View 데스크톱 풀의 스토리지 오버 커밋을 설정하고, 별도의 비영구 디스크로 Windows 페이지와 임시 파일을 리디렉션해 증가량을 제어할 수 있습니다.

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

VMware View ESX/ESXi 노드

노드는 VMware View 배포에서 가상 시스템 데스크톱을 호스트하는 단일 VMware ESX/ESXi 호스트입니다.

VMware View 는 통합 비율(ESX/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 8 대~10 대의 가상 데스크톱 식으로 계산 용량을 고려합니다. 각 가상 시스템의 CPU 요구 사항 계산에 대한 자세한 내용은 "가상 데스크톱의 CPU 요구 사항 계산," (39 페이지)에 나와 있습니다.
- 가상 데스크톱 RAM, 호스트 RAM 및 오버커밋 비율의 식으로 메모리 용량을 생각해 봅니다. CPU 코어 당 8 대에서 10 대 사이의 가상 데스크톱이 있을 수 있지만 물리적 RAM 요구 사항도 신중하게 고려해야 합니다. 가상 시스템 당 필요한 RAM 양 계산에 대한 자세한 내용은 "가상 데스크톱의 메모리 요구 사항 계산," (37 페이지)에 나와 있습니다.

  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 나을 수 있습니다.

- 끝으로 클러스터 요구 사항 및 모든 페일오버 요구 사항을 고려합니다. 자세한 내용은 "고가용성 요구 사항 확인," (49 페이지)에 나와 있습니다.

vSphere 의 ESX/ESXi 호스트 규격에 대한 자세한 내용은 *VMware vSphere Configuration Maximums*(VMware vSphere 구성 최대값) 문서에 나와 있습니다.

특정 작업자 유형의 데스크톱 풀

VMware View 는 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 상태 비저장 아키텍처는 보다 간편한 지원, 스토리지 비용 절감 등 다양한 장점을 제공합니다. 그 외에도 연결된 클론 가상 시스템 백업 필요성을 줄이고, 보다 간단하고 저렴하게 재난 복구 및 무중단 업무 운영 옵션 등을 제공합니다.

상태 저장 데스크톱 이미지 이들 이미지에는 기존의 이미지 관리 기술이 필요할 수 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 Consolidated Backup 및 VMware Site Recovery Manager 와 같은 백업 및 복구 방법이 중요합니다.

View Composer 를 사용해 연결된 클론 가상 시스템의 부동 할당 풀을 생성함으로써 상태 비저장 데스크톱 이미지를 생성합니다. 연결된 클론 가상 시스템 또는 전체 가상 시스템의 전용 할당 풀을 생성해 상태 저장 데스크톱 이미지를 생성합니다. 연결된 클록 가상 시스템을 사용하는 경우 View Composer 영구 디스크 및 폴더 리디렉션을 구성할 수 있습니다. 일부 스토리지 공급업체는 상태 저장 데스크톱 이미지에 대해 비용 효율적인 스토리지 솔루션을 제공합니다. 이러한 공급업체들은 고유한 모범 사례와 프로비저닝 유틸리티를 보유하고 있는 경우도 있습니다. 이들 공급업체와 작업하면 수동 전용 할당 풀을 생성해야 하는 경우도 있습니다.

- 일반 작업자 풀(42 페이지)

  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(42 페이지)

  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.

- 모바일 사용자용 풀(43 페이지)

  이러한 사용자는 View 데스크톱을 체크아웃할 수 있고 네트워크 연결 없이도 노트북이나 데스크톱에서 로컬로 실행할 수 있습니다.

- 키오스크 사용자 풀(44 페이지)

  키오스크 사용자는 항공사 체크인 스테이션 고객, 교실이나 도서관을 사용하는 학생, 의료 데이터 입력 사무실의 의료 관계자 또는 셀프 서비스 장소 고객 등이 있습니다. 사용자는 로그인하지 않고 클라이언트 디바이스나 View 데스크톱을 사용해야 하기 때문에 사용자가 아닌 클라이언트 디바이스 관련 계정에 데스크톱 풀의 사용 권한이 있습니다. 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. 다음 풀 설정을 사용하십시오.

- 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 View Composer 링크드 클론 데스크톱을 생성합니다.
- 사용자가 로그 오프할 때 수행할 작업을 결정합니다. 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.
- 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," (32 페이지)에 나와 있습니다.
- 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 View 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 View 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. View 개인 설정 관리를 사용하면 부동 할당 데스크톱의 최종 사용자가 해당 세션 및 전용 할당 데스크톱의 세션 간의 차이점을 구분할 수 없습니다.

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.

회계사, 영업 관리자, 마케팅 조사 분석가와 같은 지식 작업자 및 고급 사용자는 문서 및 설정을 작성하고 유지할 수 있어야 하기 때문에 그들을 위한 전용 할당 데스크톱을 생성합니다. 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. 다음 풀 설정을 사용하십시오.

- 각 지식 작업자 또는 고급 사용자가 매번 동일한 데스크톱에 로그인할 수 있도록 전용 할당 풀을 사용합니다.
- Windows 사용자 프로파일처럼, 사용자가 선호하는 데스크톱 모양 및 애플리케이션 설정을 항상 유지할 수 있도록 개인 설정 관리 기능을 사용합니다.

- 처음에는 각 데스크톱이 초기 작업에 필요한 디스크 스토리지 공간 만큼만 사용할 수 있도록 vStorage 씬 프로비저닝을 사용합니다.
- 고유 애플리케이션을 설치해야 하는 고급 사용자 및 지식 작업자의 경우(운영 체제 디스크에 데이터를 추가) 전체 가상 시스템 데스크톱을 생성하십시오.
- 임시 사용인 경우는 제외하고, 지식 작업자가 사용자 설치 애플리케이션이 필요하지 않은 경우 View Composer 연결된 클론 데스크톱을 생성할 수 있습니다. 데스크톱 이미지는 동일한 기본 이미지를 공유하며 전체 가상 시스템보다 스토리지 공간을 덜 사용합니다.
- View Composer 연결된 클론 데스크톱을 사용하는 경우 View 개인 설정 관리, 로밍 프로파일 또는 다른 프로파일 관리 솔루션을 구현합니다.

  연결된 클론 OS 디스크를 새로 고치고 재구성하는 동시에 영구 디스크에 각 사용자 프로파일의 복사본을 보관할 수 있도록 영구 디스크를 구성합니다.

모바일 사용자용 풀

이러한 사용자는 View 데스크톱을 체크아웃할 수 있고 네트워크 연결 없이도 노트북이나 데스크톱에서 로컬로 실행할 수 있습니다.

View Client with Local Mode 는 최종 사용자 및 IT 관리자 모두에게 이점을 제공합니다. 관리자의 경우 로컬 모드를 사용하여 이전에 관리하지 않았던 노트북에 View 보안 정책을 확장시킬 수 있습니다. 관리자는 View 데스크톱에서 실행하는 애플리케이션에 대한 제어권을 그대로 보유할 수 있으며 원격 View 데스크톱을 관리하듯 데스크톱을 중앙에서 관리할 수 있습니다. 로컬 모드의 경우 모든 VMware View 이점이 네트워크가 느리거나 신뢰할 수 없는 원격 사무실 또는 지점까지 확장될 수 있습니다.

최종 사용자에 대한 이점에는 온라인 또는 오프라인으로 본인 컴퓨터를 계속 사용할 수 있는 유연성이 포함됩니다. View 데스크톱은 자동으로 암호화되며 재해 복구를 위해 데이터 센터의 이미지와 쉽게 동기화할 수 있습니다.

일반 권장사항

로컬 모드 사용자는 네트워크 연결을 사용할 수 없을 때 노트북에서 데스크톱 데이터 및 애플리케이션에 액세스해야 할 수 있습니다. 또한 노트북이 분실되거나 손상되거나 도난당할 경우에 대비해 데이터 센터로 이 데이터를 정기적으로 자동 백업해야 할 수 있습니다. 이러한 기능을 위해 사용할 수 있는 풀 설정은 다음과 같습니다.

- 풀을 기본으로 하는 가상 시스템을 생성할 경우 게스트 운영 체제에 필요한 최소량의 RAM 및 가상 CPU 를 구성합니다. 로컬 모드에서 실행하는 데스크톱은 클라이언트 컴퓨터에서 사용 가능한 사항을 기반으로 사용하는 메모리 및 처리 능력을 조정합니다.
- 데스크톱이 풀 생성 시 생성되거나 풀 사용을 기반으로 요구 시 생성될 수 있도록 자동화된 풀을 생성합니다.
- 로컬 모드 사용자는 동일한 데스크톱에 매번 로그인해야 하기 때문에 전용 할당을 사용합니다.
- 데스크톱이 동일한 기본 이미지를 공유하며 전체 가상 시스템보다 데이터 센터의 스토리지 공간을 덜 사용하도록 View Composer 링크드 클론 데스크톱을 생성합니다.
- 프로비저닝 프로세스에서 풀의 각 연결된 클론에 대한 고유 로컬 컴퓨터 SID 및 GUID 를 생성할 경우 풀을 생성할 때 Sysprep 사용자 지정 규격을 선택합니다. 초기 프로비저닝 동안과 재구성 작업 후 Sysprep 은 새 SID 및 GUID 를 생성합니다. 로컬 모드 풀은 거의 재구성하지 않기 때문에 SID 및 GUID 는 변경되지 않습니다.
- 로컬 모드에 사용할 데스크톱만 풀에 포함시킵니다. 로컬 모드 가상 시스템은 많은 원격 View 데스크톱을 지원하는 스토리지보다 IOPS 요구 사항이 더 낮은 데이터스토어에 지정될 수 있습니다.

자본 지출 최소화를 위한 추가 권장 사항

ESX/ESXi 호스트 당 가상 시스템 수를 늘릴 경우 로컬 모드 풀에 필요한 ESX/ESXi 호스트 수를 줄일 수 있습니다. 로컬 모드 풀에서 자주 있는 경우처럼 대부분의 전원이 동시에 켜지지 않을 경우 ESX/ESXi 4.1 호스트는 최고 500 대의 가상 시스템을 수용할 수 있습니다.

다음 권장 사항을 실행하여 각 가상 시스템에 필요한 대역폭 및 I/O 작업량을 줄이고 ESX/ESXi 호스트의 가상 시스템 수를 최대화합니다.

- 최종 사용자들이 로컬 모드에서만 View 데스크톱을 사용하도록 View 정책을 설정하십시오. 이렇게 설정할 경우 데이터 센터의 가상 시스템은 잠기고 전원이 꺼진 채로 유지됩니다.
- 최종 사용자가 데스크톱 롤백, 데이터 백업 또는 데이터 센터에 대한 체크인을 초기화할 수 없도록 로컬 모드 정책을 설정하십시오.
- 자동 백업을 예약하지 마십시오.
- 로컬 모드 데스크톱 프로비저닝 또는 다운로드에 대해 SSL 을 켜지 마십시오.
- View Connection Server 성능이 로컬 데스크톱의 수에 따라 영향을 받을 경우 하트비트 간격을 넓게 설정합니다. View Connection Server 에서는 하트비트를 통해 로컬 데스크톱에 네트워크가 연결되어 있는지 확인합니다. 기본 간격은 5 분입니다.

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 로그인하지 않고 클라이언트 디바이스나 View 데스크톱을 사용해야 하기 때문에 사용자가 아닌 클라이언트 디바이스 관련 계정에 데스크톱 풀의 사용 권한이 있습니다. 일부 애플리케이션은 사용자가 인증 자격 증명을 제공해야 사용할 수 있습니다.

키오스크 모드에서 실행되도록 설치된 View 데스크톱은 운영 체제 디스크에 사용자 데이터를 저장할 필요가 없기 때문에 상태 비저장 데스크톱 이미지를 사용합니다. 키오스크 모드 데스크톱은 씬 클라이언트 디바이스 또는 잠긴 PC 와 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.

전용 View 연결 서버 인스턴스를 모범 사례로 사용해 키오스크 모드에서 클라이언트를 처리하고 Active Directory 에서 이들 클라이언트 계정에 대한 전용 조직 단위 및 그룹을 생성하십시오. 이 프랙티스는 시스템을 분할해 허가 받지 않은 침입에 대비할 뿐 아니라 클라이언트를 보다 쉽게 구성 및 관리하도록 지원합니다.

키오스크 모드를 설정하려면 `vdmadmin` 명령줄 인터페이스를 사용하고 *VMware View 관리* 설명서의 키오스크 모드 항목에서 설명한 몇 가지 절차를 수행해야 합니다. 다음과 같은 풀 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 View Composer 링크드 클론 데스크톱을 생성합니다.
- 새로 고침 정책을 시행해 데스크톱을 자주 새로 고치십시오(예: 사용자가 로그인할 때마다).
- 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," (32 페이지)에 나와 있습니다.

- 데스크톱에서 가장 가까운 프린터를 사용할 수 있도록 Active Directory GPO(그룹 정책 개체)를 사용해 위치 기반 인쇄를 구성하십시오. ADM(Group Policy 관리) 템플릿으로 사용할 수 있는 전체 설정 목록 및 설명은 *VMware View 관리* 설명서를 참조하십시오.
- 데스크톱을 시작하거나 클라이언트 컴퓨터에 USB 디바이스를 연결할 때 데스크톱에 로컬 USB 디바이스를 연결하는 기본 정책을 무시하려면 GPO 를 사용하십시오.

데스크톱 가상 시스템 구성

게스트 운영 체제에 따라 가상 시스템에 필요한 RAM, CPU, 디스크 공간이 다르기 때문에 Windows XP, Windows Vista, Windows 7 가상 데스크톱에 대해 개별적인 구성 예를 제공합니다.

메모리, 가상 프로세서 수, 디스크 공간과 같은 가상 시스템을 위한 설정의 예는 VMware View 에만 적용됩니다.

표 4-2 의 지침은 원격 모드로 실행되는 표준 Windows XP 가상 데스크톱에 해당하는 내용입니다.

표 4-2. Windows XP 용 데스크톱 가상 시스템의 예

항목	예
운영 체제	32 비트 Windows XP(최신 서비스 팩 필요)
RAM	1GB(최소 512MB, 최고 2GB)
가상 CPU	1
시스템 디스크 용량	16GB(최소 8GB, 최고 40GB)
사용자 데이터 용량(영구 디스크)	5GB(시작 용량)
가상 SCSI 어댑터 유형	LSI Logic Parallel(기본 아님)
가상 네트워크 어댑터	Flexible(기본)

기본 이미지에 필요한 애플리케이션 수에 따라 필요한 시스템 디스크 공간이 다릅니다. VMware 는 8GB 의 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 Composer 를 사용하면 영구 디스크에 이 데이터가 보관됩니다.

표 4-3 의 지침은 원격 모드로 실행되는 표준 Windows Vista 가상 데스크톱용입니다.

표 4-3. Windows Vista 용 데스크톱 가상 시스템의 예

항목	예
운영 체제	32 비트 Windows Vista(최신 서비스 팩 필요)
RAM	1GB
가상 CPU	1
시스템 디스크 용량	20GB(표준)
사용자 데이터 용량(영구 디스크)	5GB(시작 용량)
가상 SCSI 어댑터 유형	LSI Logic Parallel(기본)
가상 네트워크 어댑터	VMXNET 3

표 4-4 의 지침은 원격 모드로 실행되는 표준 Windows 7 가상 데스크톱용입니다.

표 4-4. ESX/ESXi 4.1 이상 호스트에서 Windows 7 용 데스크톱 가상 시스템의 예

항목	예
운영 체제	32 비트 Windows 7(최신 서비스 팩 필요)
RAM	1GB
가상 CPU	1
시스템 디스크 용량	20GB(표준보다 다소 적음)
사용자 데이터 용량(영구 디스크)	5GB(시작 용량)
가상 SCSI 어댑터 유형	LSI Logic SAS(기본)
가상 네트워크 어댑터	VMXNET 3 (이 어댑터를 사용하려면 Windows 7 SP1 의 경우 Microsoft 핫픽스 패치 http://support.microsoft.com/kb/2550978, 이전 버전의 경우 http://support.microsoft.com/kb/2344941 설치가 필요합니다.)

vCenter 및 View Composer 가상 시스템 구성과 데스크톱 풀 최대값

동일한 가상 시스템 또는 개별 호스트에 vCenter Server 및 View Composer 를 설치할 수 있습니다. vCenter Server 에는 데스크톱 가상 시스템보다 훨씬 더 많은 메모리 및 처리 능력이 필요합니다.

vSphere 4.1 이상을 사용하는 경우 View Composer 에서 풀당 최대 1,000 개의 데스크톱을 생성하고 프로비저닝할 수 있습니다. 또한 View Composer 는 한 번에 최대 1,000 개의 데스크톱에서 재구성 작업을 수행할 수 있습니다. 데스크톱 풀 크기는 다음 요소에 의해 제한됩니다.

- 각 데스크톱 풀에는 하나의 ESX/ESXi 클러스터만 포함될 수 있습니다.
- View 5.1 이상 및 vSphere 5.0 이상이 있는 경우, ESXi 클러스터에는 8 대 이상의 ESXi 호스트(최대 32 대)가 포함될 수 있지만 NFS 데이터스토어에 링크드 클론 복제 디스크를 저장해야 합니다.
- 각 CPU 코어는 가상 데스크톱 8 대 ~ 10 대에 해당하는 계산 용량을 제공합니다.
- 서브넷에 대해 사용 가능한 IP 주소 수에 따라 풀의 데스크톱 수가 제한됩니다. 예를 들어 풀의 서브넷에 256 개의 사용 가능한 IP 주소만 포함되도록 네트워크를 설정한 경우 풀 크기가 256 개의 데스크톱으로 제한됩니다.

물리적 시스템에 vCenter Server 및 View Composer 를 설치할 수 있지만 이 예제는 표 4-5 에 나열된 규격의 가상 시스템을 사용합니다. 이 가상 시스템의 ESX/ESXi 호스트는 물리적 서버 실패에 대해 보호하는 VMware HA 클러스터의 일부일 수 있습니다.

이 예에서는 vSphere 4.1 이상 및 vCenter Server 4.1 이상과 함께 VMware View 를 사용 중이라고 가정합니다.

표 4-5. vCenter Server 가상 시스템의 예 및 풀 크기 최대값

항목	예
운영 체제	64 비트 Windows Server 2008 R2 Enterprise
RAM	4GB
가상 CPU	2
시스템 디스크 용량	40GB
가상 SCSI 어댑터 유형	LSI Logic SAS(Windows Server 2008 의 기본값)

표 4-5. vCenter Server 가상 시스템의 예 및 풀 크기 최대값 (계속)

항목	예
가상 네트워크 어댑터	E1000(기본)
최대 View Composer 풀 크기	1,000 개의 데스크톱

vCenter Server 에서 개별 서버에 설치된 독립 실행형 View Composer 인스턴스의 시스템 요구 사항의 경우, *VMware View 설치* 문서의 시스템 요구 사항 항목을 참조하십시오.

중요 개별 가상 시스템에 vCenter 및 View Composer 가 연결할 데이터베이스를 배치하는 것이 좋습니다.

View Connection Server 최대값 및 가상 시스템 구성

View Connection Server 를 설치할 때 View Administrator 사용자 인터페이스도 설치됩니다. 이 서버에는 vCenter Server 인스턴스보다 더 많은 메모리 및 처리 리소스가 필요합니다.

View Connection Server 구성

물리적 시스템에 View Connection Server 를 설치할 수 있지만 이 예제는 표 4-6 에 나열된 규격의 가상 시스템을 사용합니다. 이 가상 시스템의 ESX/ESXi 호스트는 물리적 서버 실패에 대해 보호하는 VMware HA 클러스터의 일부일 수 있습니다.

표 4-6. Connection Server 가상 시스템의 예

항목	예
운영 체제	64 비트 Windows Server 2008 R2
RAM	10GB
가상 CPU	4
시스템 디스크 용량	40GB
가상 SCSI 어댑터 유형	LSI Logic SAS(Windows Server 2008 의 기본값)
가상 네트워크 어댑터	E1000(기본값)
1 NIC	1 기가비트

View Connection Server 클러스터 디자인 고려 사항

여러 복제된 View Connection Server 인스턴스를 한 그룹에 배포하여 로드 밸런싱 및 고가용성을 지원할 수 있습니다. 복제된 인스턴스 그룹은 LAN 연결 단일 데이터 센터 환경에서 클러스터링을 지원하도록 디자인되었습니다. 그룹화된 인스턴스 사이에 통신 트래픽이 필요하기 때문에 VMware 는 WAN 에 대해 복제된 View Connection Server 인스턴스 그룹 사용을 권장하지 않습니다. 여러 데이터 센터에 View 배포를 실시해야 하는 시나리오에서 각 데이터 센터에 대해 개별 View 배포를 생성합니다.

View Connection Server 의 최대 연결의 수

표 4-7 에는 VMware View 배포에서 수용할 수 있는 동시 연결의 수에 관하여 테스트한 범위에 대한 정보가 나와 있습니다.

이 예에서는 vSphere 4.1 이상 및 vCenter Server 4.1 이상과 함께 VMware View 를 사용 중이라고 가정합니다. 또한 View Connection Server 는 64 비트 Windows Server 2008 R2 Enterprise 운영 체제에서 실행 중이라고 가정합니다.

표 4-7. View 데스크톱 연결

배포 당 연결 서버	연결 유형	최대 동시 연결 수
1 대의 Connection Server	직접 연결, RDP 또는 PCoIP; 터널링된 연결, RDP, PCoIP 보안 게이트웨이 연결	2,000
7 대의 Connection Server(5 + 2 대의 예비 연결 서버)	직접 연결, RDP 또는 PCoIP	10,000
1 대의 Connection Server	물리적 PC 에 대한 통일된 액세스	100
1 대의 Connection Server	터미널 서버에 대한 통일된 액세스	200

PCoIP 보안 게이트웨이 연결은 회사 네트워크 외부에서 PCoIP 연결을 위해 보안 서버를 사용할 경우 필요합니다. 회사 네트워크 외부에서 RDP 연결을 위해 보안 서버를 사용하고 PCoIP 보안 게이트웨이 연결과 함께 USB 및 MMR(멀티미디어 리디렉션) 가속을 위해 보안 서버를 사용할 경우에는 터널링된 연결이 필요합니다. 연결 서버 하나에 여러 보안 서버를 연결할 수 있습니다.

View 전송 서버 가상 시스템 구성 및 스토리지

View 전송 서버는 View Client with Local Mode(이전에는 Offline Desktop 이라고 불렀음)를 실행하는 데스크톱을 지원합니다. 이 서버는 View 연결 서버보다 비용이 덜 듭니다.

View 전송 서버 구성

물리적 시스템이 아니라 가상 시스템에 View 전송 서버를 설치해야 하며 가상 시스템은 관리할 로컬 데스크톱과 동일한 vCenter Server 인스턴스로 관리되어야 합니다. 표 4-8 에는 View 전송 서버 인스턴스에 대한 가상 시스템 규격이 나열되어 있습니다.

표 4-8. View 전송 서버 가상 시스템의 예

항목	예
운영 체제	64 비트 Windows Server 2008 R2
RAM	4GB
가상 CPU	2
시스템 디스크 용량	20GB
가상 SCSI 어댑터 유형	LSI Logic Parallel 또는 SAS
가상 네트워크 어댑터	E1000(기본)
1 NIC	1 기가비트

View 전송 서버의 스토리지 및 대역폭 요구 사항

여러 작업에서 View 전송 서버를 사용하여 vCenter Server 의 View 데스크톱 및 클라이언트 시스템의 해당 로컬 데스크톱 사이에서 데이터를 전송합니다. 사용자가 데스크톱을 체크인 또는 체크아웃할 때 View 전송 서버는 데이터 센터 및 로컬 데스크톱 사이에서 파일을 전송합니다. 또한 View 전송 서버는 데이터 센터에 사용자 변경 내용을 복제하여 데이터 센터의 해당 데스크톱과 로컬 데스크톱을 동기화합니다.

로컬 데스크톱에 View Composer 링크드 클론을 사용할 경우 전송 서버 저장소를 구성하는 디스크 드라이브에 정적 이미지 파일을 저장할 공간이 충분해야 합니다. 이미지 파일은 View Composer 기본 이미지입니다. 네트워크 스토리지 디스크가 빠를수록 성능이 향상됩니다. 기본 이미지 파일 크기 확인에 대한 자세한 내용은 *VMware View 관리* 문서에 나와 있습니다.

네트워크 대역폭이 포화 상태가 되는 수치는 더 낮겠지만 각 전송 서버 인스턴스는 이론적으로 60 개의 동시 디스크 작업을 수용할 수 있습니다. VMware 에서는 초당 1GB 네트워크 연결에 대해 20 개의 동시 디스크 작업(예: 동시에 20 대의 클라이언트에서 로컬 데스크톱 다운로드)을 테스트했습니다.

vSphere 클러스터

VMware View 배포에서는 VMware HA 클러스터를 사용하여 물리적 서버 실패에 대해 보호할 수 있습니다. View 5.1 이상 및 vSphere 5 이상이 있다면 View Composer 를 사용하고 NFS 데이터스토어에 복제 디스크를 저장하는 경우, 클러스터에 최대 32 대의 서버 또는 노드가 포함될 수 있습니다.

VMware vSphere 및 vCenter 는 View 데스크톱을 호스트하는 서버의 클러스터를 관리하기 위해 고급 기능 집합을 제공합니다. 또한 각 View 데스크톱 풀이 vCenter 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 VMware View 배포에서 vCenter 성능 및 응답은 데이터 센터 개체 당 클러스터 개체를 하나만 지정하여 향상될 수 있습니다(기본 동작은 아님). 기본적으로 VMware vCenter 는 동일한 데이터 센터 개체에 새 클러스터를 생성합니다.

고가용성 요구 사항 확인

효율성 및 리소스 관리를 통해 VMware vSphere 를 사용하면 업계 최고 수준의 서버 당 가상 시스템이 될 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 HA 를 적절하게 구성해야 합니다. VMware HA 를 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 128 대의 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 8 대 호스트 모두에서 데스크톱의 밸런싱을 도울 수 있습니다. 모든 핫스페어 리소스를 유휴 상태로 두지 않고 임시 서버 용량을 모두 사용합니다. 또한 DRS 는 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 IOPS 는 서버 실패 시 데스크톱을 빨리 복구하는 방법에 가장 큰 영향을 줍니다.

예: 클러스터 구성의 예

표 4-9 에 나열된 설정은 VMware View 에 특정합니다. vSphere 의 HA 클러스터 제한에 대한 자세한 내용은 *VMware vSphere Configuration Maximums*(VMware vSphere 구성 최대값) 문서에 나와 있습니다.

표 4-9. HA 클러스터 예

항목	예
노드(ESX/ESXi 호스트)	8(1 개의 핫 스페어 포함)
클러스터 유형	DRS(Distributed Resource Scheduler)/HA
네트워킹 구성 요소	표준 ESXi 5.0 클러스터 네트워크
스위치 포트	80

참고 View 5.1 이상 및 vSphere 5 이상이 있다면 View Composer 를 사용하고 NFS 데이터스토어에 복제 디스크를 저장하는 경우, 클러스터에 최대 32 대의 ESXi 호스트가 포함될 수 있습니다. 자세한 내용은 *VMware View 관리* 문서의 데스크톱 풀 생성에 대한 장을 참조하십시오.

네트워킹 요구 사항은 서버 유형, 네트워크 어댑터 수 및 vMotion 구성 방식에 따라 다릅니다.

VMware View 빌드 블록

2,000 사용자 빌드 블록은 물리적 서버, VMware vSphere 인프라, VMware View 서버, 공유 스토리지 및 2,000 대의 가상 시스템 데스크톱으로 구성됩니다. View 팟에 최고 다섯 개의 빌드 블록이 포함될 수 있습니다.

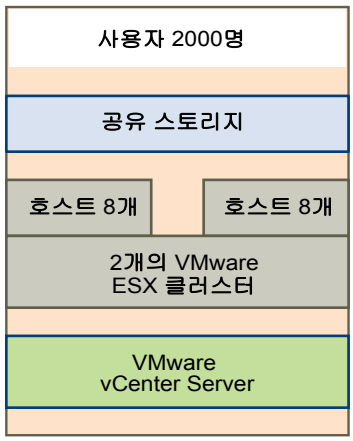
표 4-10. LAN 기반 View 빌드 블록의 예

항목	예
vSphere 클러스터	2 이상
80 포트 네트워크 스위치	1
공유 스토리지 시스템	1
View Composer 포함 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)

vCenter 4.1 및 5.0 이 있는 경우, 각 vCenter Server 는 최대 10,000 대의 가상 시스템을 지원할 수 있습니다. 이 지원을 사용하여 2,000 대 이상의 View 데스크톱을 포함하는 빌드 블록을 보유할 수 있습니다. 그러나 실제 블록 크기 또한 다른 View 별 제한 사항에 속합니다.

팟에 빌드 블록이 하나 뿐인 경우 이중화를 위해 두 개의 View 연결 서버 인스턴스를 사용합니다.

그림 4-1. VMware View 빌드 블록의 구성 요소



View 아키텍처의 공유 스토리지

스토리지 디자인 고려 사항은 성공적인 View 아키텍처의 가장 중요한 요소 중 하나입니다. 아키텍처에 미치는 영향이 가장 큰 결정은 연결된 클론 기술을 사용하는 View Composer 데스크톱의 사용 여부입니다.

VMware vSphere 에서 사용하는 외부 스토리지 시스템은 Fibre Channel 또는 iSCSI SAN(Storage Area Network) 또는 NFS(Network File System) NAS(네트워크 연결 스토리지)가 될 수 있습니다. ESX/ESXi 바이너리, 가상 시스템 스왑 파일 및 상위 가상 시스템의 View Composer 복제본은 이 시스템에 저장됩니다.

아키텍처 관점에서 볼 때, View Composer 는 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 사용된 공간을 이용하는 새로 고침 정책을 설정하여 스토리지 요구 사항을 더 감소시킬 수 있습니다.

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 Composer 를 사용하여 운영 체제에서 개별 사용자 데이터를 분리할 수 있기 때문에 영구 디스크만 백업하거나 복제하면 스토리지 요구 사항이 더 감소합니다. 자세한 내용은 "View Composer 로 스토리지 요구 사항 축소," (31 페이지).

참고 전용 스토리지 구성 요소와 관련한 의사 결정은 시험 단계 중에 수행하는 것이 가장 좋습니다. 기본 고려 사항은 IOPS(초당 입출력)입니다. 계층별 스토리지 전략을 시험하여 성능 및 비용 절약을 최대화할 수 있습니다.

자세한 내용은 *VMware View 를 위한 스토리지 고려 사항* 모범 사례 안내를 참조하십시오.

스토리지 대역폭 고려 사항

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

VMware View 환경에서 모든 가상 시스템이 동시에 작업을 수행하는 동안 가끔 I/O 스톰 로드를 경험할 수 있습니다. I/O 스톰은 안티바이러스 소프트웨어 또는 소프트웨어 업데이트 에이전트와 같은 게스트 기반 에이전트로 인해 발생할 수 있습니다. 또한 I/O 스톰은 아침에 거의 동시에 모든 고용인들이 로그인할 때와 같이 사람의 동작으로 발생할 수도 있습니다.

다른 가상 시스템으로 업데이트를 분산하는 것과 같이 작업 모범 사례를 통해 이러한 스톰 워크로드를 최소할 수 있습니다. 또한 사용자가 로그오프할 때 가상 시스템을 일시 중단할지 또는 전원을 끌지 결정하기 위해 시범 단계 중 다양한 로그오프 정책을 테스트할 수 있습니다. 개별적인 고성능 데이터스토어에 View Composer 복제본을 저장하여 I/O 스톰 로드를 해결하기 위해 많은 동시 읽기 작업 속도를 높일 수 있습니다.

모범 사례를 결정하는 것 외에도 VMware 에서는 평균 대역폭이 10 배 미만일 수 있어도 100 개의 가상 시스템 당 1Gbps 의 대역폭을 제공할 것을 권장합니다. 그러한 보수적인 계획은 피크 로드에 대해 충분한 스토리지 연결성을 보장합니다.

네트워크 대역폭 고려 사항

디스플레이 트래픽의 경우 사용된 프로토콜, 모니터 해상도 및 구성, 워크로드의 멀티미디어 컨텐츠 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 150-200Kbps 의 용량을 계획하십시오.

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

- 두 대의 모니터(1920x1080)
- 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

이 정보는 *PCoIP Display Protocol: Information and Scenario-Based Network Sizing Guide*(PCoIP 디스플레이 프로토콜: 정보 및 시나리오 기반 네트워크 규모 설정 설명서)라는 정보 설명서에서 인용되었습니다.

PCoIP 에서 사용 가능한 최적화 제어

VMware 의 PCoIP 디스플레이 프로토콜을 사용할 경우 대역폭 사용에 영향을 주는 여러 요소를 조정할 수 있습니다.

- Windows 및 Linux 클라이언트 시스템의 경우, 이미지 캐시 크기를 50MB ~ 300MB 사이에서 조정할 수 있습니다. 이미지 캐싱은 재전송해야 할 디스플레이 데이터 양을 줄입니다.
- 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. 이미지의 변경되지 않은 영역은 점차 무손실(완벽한) 품질을 형성합니다. 초당 프레임 수 1 에서 120 까지 프레임 속도를 조정할 수 있습니다.

  이 컨트롤은 업데이트할 필요가 없는 정적 화면 내용 또는 일부분만 새로 고쳐야 하는 경우에 효과가 있습니다.
- 완벽한 품질(무손실)로의 점진적 빌드 대신 인식적 무손실을 선택한 경우에도 무손실 빌드 기능을 끌 수 있습니다.
- 세션 협상 중 PCoIP 끝점에 의해 보급된 암호화 알고리즘을 제어할 수 있습니다. 기본적으로 Salsa20-256round12 및 AES-128-GCM 알고리즘 모두 사용 가능합니다.
- 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 및 컨트롤 PCoIP 트래픽을 포함합니다.

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

WAN 지원 및 PCoIP

광역 네트워크(WAN)의 경우 대역폭 제약 조건 및 지연 문제를 고려해야 합니다. VMware 에서 제공하는 PCoIP 디스플레이 프로토콜은 다양한 지연 및 대역폭 상태에 적응합니다.

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

- 이러한 프로토콜에는 클라이언트 및 서버 간 많은 핸드셰이크가 필요하기 때문에 WAN 최적화는 RDP 와 같은 TCP 기반 프로토콜에 유용합니다. 이러한 핸드셰이크 지연은 매우 커질 수 있습니다. WAN 가속기 스푸핑은 프로토콜의 네트워크 지연이 숨겨지도록 핸드셰이크에 응답합니다. PCoIP 는 UDP 기반이기 때문에 이런 형태의 WAN 가속화는 필요하지 않습니다.
- 또한 WAN 가속기는 클라이언트 및 서버 간 네트워크 트래픽을 압축하지만 이 압축은 대개 2:1 압축 비율로 제한됩니다. PCoIP 는 이미지 및 오디오에 최고 100:1 의 압축 비율을 제공할 수 있습니다.

PCoIP 가 대역폭을 소비하는 방법을 조정하기 위해 사용할 수 있는, View 5 에 적용된 제어에 대한 자세한 내용은 "PCoIP 에서 사용 가능한 최적화 제어," (52 페이지)를 참조하십시오.

다양한 사용자 유형의 대역폭 요구 사항

PCoIP 의 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 VMware View 설정이 없는 일반적인 오피스 애플리케이션.
- 최적화된 오피스 생산성 데스크톱을 위한 50 ~ 100Kbps 평균 대역폭: 비디오, 3D 그래픽은 없고 Windows 데스크톱 설정 및 VMware View 가 최적화되어 있는 일반적인 오피스 애플리케이션.
- 다중 모니터, 3D, Aero 및 Office 2010 을 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 사용자 당 2Mbps 가 필요합니다.

참고 일반적인 사용자 당 50 ~150Kbps 라는 추정치는 모든 사용자가 계속 작업 중이며 하루에 8 ~ 10 시간 넘게 유사한 작업을 수행한다는 가정을 기반으로 합니다. 50Kbps 대역폭 사용 수치는 Build-to-Lossless 기능이 사용되지 않도록 설정된 LAN 의 View Planner 테스팅에서 나왔습니다. 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.
- VMware View 의 일반 오피스 사용자당 필요한 대역폭은 50 ~ 150Kbps 부터입니다.
- T1 네트워크 용량은 1.5Mbps 입니다.
- 대역폭 사용률은 80 퍼센트입니다(사용률 계수 0.8).

지원된 사용자 수 결정 공식

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

결과

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

중요 이 사용자 밀도를 얻으려면 VMware View 및 Windows 데스크톱 설정 모두를 최적화해야 할 수 있습니다.

이 정보는 *VMware View 5 with PCoIP: Network Optimization Guide* 정보 가이드에서 발췌되었습니다.

VMware View 팟

VMware View 팟은 다섯 개의 2,000 사용자 빌드 블록을 하나의 엔터티로 관리할 수 있는 View Manager 설치로 통합합니다.

팟은 VMware View 확장성 제한으로 결정된 조직 단위입니다. 표 4-11 에는 View 팟 구성 요소가 나열되어 있습니다.

표 4-11. VMware View 팟의 예

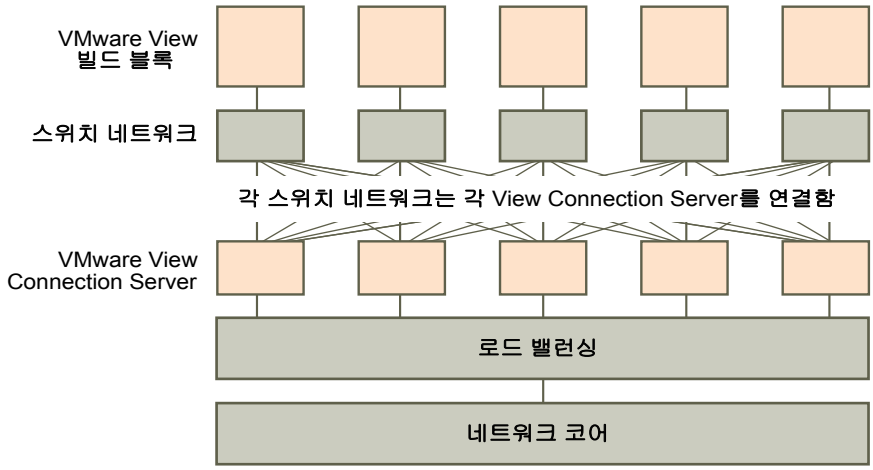
항목	수
View 빌드 블록	5
View Connection Server	7(각 빌드 블록에 1 개 그리고 2 개의 예비)
10Gb 이더넷 모듈	1
모듈식 네트워킹 스위치	1
로드 밸런싱 모듈	1
WAN 용 VPN	1(선택 사항)

네트워크 코어는 View Connection Server 인스턴스에 대해 들어오는 요청을 로드 밸런싱합니다. 이중화 및 페일오버 메커니즘에 대한 지원은 일반적으로 네트워크 수준에서 로드 밸런서가 단일 실패 지점이 되지 않도록 방지합니다. 예를 들어 가상 라우터 중복 프로토콜(VRRP)은 이중화 및 페일오버 기능을 추가하도록 로드 밸런서와 통신합니다.

View Connection Server 인스턴스가 실패하거나 활성 세션 중 응답하지 않을 경우에도 사용자 데이터는 손실되지 않습니다. 사용자가 다른 View Connection Server 인스턴스에 연결할 수 있도록 가상 시스템 데스크톱에서 데스크톱 상태가 유지되며 해당 데스크톱 세션은 실패 발생 시 해당 지점에서 다시 시작됩니다.

그림 4-2 에는 모든 구성 요소를 관리 가능한 하나의 엔터티로 통합할 수 있는 방법이 나와 있습니다.

그림 4-2. 10,000 대의 View 데스크톱의 팟 다이어그램



5 보안 기능 계획

VMware View는 강력한 네트워크 보안을 통해 중요한 기업 데이터를 보호합니다. 보안을 추가한 경우 VMware View에 특정 타사 사용자 인증 솔루션을 통합하고 보안 서버를 사용하고 제한된 권한 기능을 구현할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- "클라이언트 연결 이해," (57 페이지)
- "사용자 인증 방법 선택," (60 페이지)
- "View 데스크톱 액세스 제한," (62 페이지)
- "그룹 정책 설정을 사용한 View 데스크톱 보안," (64 페이지)
- "보안 클라이언트 시스템에 모범 사례 구현," (64 페이지)
- "관리자 역할 할당," (64 페이지)
- "보안 서버 사용 준비," (65 페이지)
- "VMware View 통신 프로토콜 이해," (70 페이지)

클라이언트 연결 이해

View Client 및 View Administrator는 보안 HTTPS 연결을 통해 View 연결 서버 호스트와 통신합니다. View 연결 서버의 서버 인증서에 대한 정보는 클라이언트 및 서버 간 XML 핸드셰이크의 일부로 View Client에 전달됩니다.

사용자 인증 및 View 데스크톱 선택에 사용되는 초기 View Client 연결은 사용자가 View Client를 열고 View 연결 서버 또는 보안 서버 호스트에 정규화된 도메인 이름을 제공할 때 생성됩니다. View Administrator 연결은 관리자가 웹 브라우저에 View Administrator URL을 입력할 때 생성됩니다.

기본 서버 SSL 인증서는 View 연결 서버 설치 중 생성됩니다. 기본적으로 클라이언트는 View Administrator와 같은 보안 페이지를 방문할 때 이 인증서를 제공 받습니다.

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

- PCoIP 보안 게이트웨이를 사용한 클라이언트 연결(58 페이지)

  클라이언트가 VMware에서 PCoIP 디스플레이 프로토콜로 View 데스크톱에 연결하는 경우 View Client는 View 연결 서버 인스턴스 또는 보안 서버의 PCoIP 보안 게이트웨이에 두 번째 연결을 생성할 수 있습니다. 이 연결은 인터넷에서 View 데스크톱에 액세스할 때 필요한 보안 및 연결 수준을 제공합니다.

- Microsoft RDP 로 터널링된 클라이언트 연결(58 페이지)

  사용자가 Microsoft RDP 디스플레이 프로토콜을 사용하여 View 데스크톱에 연결할 때 View Client 는 View Connection Server 호스트에 보조 HTTPS 연결을 설정할 수 있습니다. 이 연결은 RDP 데이터 이동을 위한 터널을 제공하기 때문에 터널 연결이라고 합니다.

- 클라이언트 직접 연결(59 페이지)

  관리자는 View 연결 서버 호스트를 건너뛰고 클라이언트 시스템과 View 데스크톱 가상 시스템 사이에 직접 View 데스크톱 세션을 설정하도록 View 연결 서버 설정을 구성할 수 있습니다. 이러한 연결 유형을 클라이언트 직접 연결이라 부릅니다.

- View Client with Local Mode 클라이언트 연결(59 페이지)

  View Client with Local Mode 는 휴대폰 사용자에게 로컬 컴퓨터에서 View 데스크톱을 체크아웃하는 기능을 제공합니다.

PCoIP 보안 게이트웨이를 사용한 클라이언트 연결

클라이언트가 VMware 에서 PCoIP 디스플레이 프로토콜로 View 데스크톱에 연결하는 경우 View Client 는 View 연결 서버 인스턴스 또는 보안 서버의 PCoIP 보안 게이트웨이에 두 번째 연결을 생성할 수 있습니다. 이 연결은 인터넷에서 View 데스크톱에 액세스할 때 필요한 보안 및 연결 수준을 제공합니다.

View 4.6 부터는 보안 서버에 PCoIP 보안 게이트웨이 구성 요소가 포함되어 있습니다. PCoIP 보안 게이트웨이 연결은 다음과 같은 장점을 제공합니다.

- 인증된 사용자를 대신한 원격 데스크톱 트래픽만 기업 데이터 센터에 들어갈 수 있습니다.
- 사용자는 액세스 권한을 부여 받은 데스크톱 리소스에만 액세스할 수 있습니다.
- 이 연결은 TCP 대신 UDP 에 비디오 디스플레이 패킷을 캡슐화함으로써 네트워크를 더욱 효율적으로 사용하는 고급 원격 데스크톱 프로토콜인 PCoIP 를 지원합니다.
- AES-128 암호화로 PCoIP 를 보호합니다.
- 네트워킹 구성 요소로 인해 PCoIP 가 차단되지 않는 한 VPN 은 필요 없습니다. 예를 들어 호텔 객실에서 View 데스크톱에 액세스하려는 경우 호텔에서 사용하는 프록시 구성이 TCP 포트 4172 에 대한 인바운드 트래픽과 UDP 포트 4172 에 대한 인바운드와 아웃바운드 트래픽을 허용하지 않을 수 있습니다.

  자세한 내용은 "DMZ 기반 보안 서버의 방화벽 규칙,"(68 페이지).

PCoIP 를 지원하는 보안 서버는 Windows Server 2008 R2 에서 실행되며 64 비트 아키텍처를 사용합니다. 이 보안 서버는 또한 AESNI(AES New Instruction)를 지원하는 Intel 프로세서를 사용하여 PCoIP 암호화와 암호 해독 성능을 최적화합니다.

Microsoft RDP 로 터널링된 클라이언트 연결

사용자가 Microsoft RDP 디스플레이 프로토콜을 사용하여 View 데스크톱에 연결할 때 View Client 는 View Connection Server 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 HTTPS 를 통해 터널링되고 SSL 을 사용하여 암호화됩니다. 이 강력한 보안 프로토콜은 다른 보안 웹 사이트에서 제공된 보안(예: 온라인 뱅킹 및 신용 카드 결제에 사용)과 일치합니다.
- 클라이언트는 전체 프로토콜 오버헤드를 줄이는 단일 HTTPS 연결을 통해 여러 데스크톱에 액세스할 수 있습니다.
- VMware View 가 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.

View Connection Server 인스턴스의 표준 배포의 경우 HTTPS 보안 연결은 View Connection Server에서 종료됩니다. DMZ 배포의 경우 HTTPS 보안 연결은 보안 서버에서 종료됩니다. DMZ 배포 및 보안 서버에 대한 자세한 내용은 "보안 서버 사용 준비," (65 페이지)에 나와 있습니다.

PCoIP 디스플레이 프로토콜을 사용하는 클라이언트는 USB 리디렉션 및 MMR(멀티미디어 리디렉션) 가속을 위해 터널 연결을 사용할 수 있지만 다른 모든 데이터의 경우 PCoIP 는 보안 서버에서 PCoIP 보안 게이트웨이를 사용합니다. 자세한 내용은 "PCoIP 보안 게이트웨이를 사용한 클라이언트 연결," (58 페이지).

클라이언트 직접 연결

관리자는 View 연결 서버 호스트를 건너뛰고 클라이언트 시스템과 View 데스크톱 가상 시스템 사이에 직접 View 데스크톱 세션을 설정하도록 View 연결 서버 설정을 구성할 수 있습니다. 이러한 연결 유형을 클라이언트 직접 연결이라 부릅니다.

클라이언트 직접 연결을 사용해 사용자가 View 데스크톱을 인증하고 선택할 수 있도록 클라이언트와 View 연결 서버 호스트 사이에 HTTPS 연결을 생성하지만 두 번째 HTTPS 연결(터널 연결)은 사용하지 않습니다.

직접 PCoIP 연결은 다음과 같은 기본 보안 기능을 제공합니다.

- PCoIP 는 기본적으로 사용되는 AES(Advanced Encryption Standard) 암호화를 지원합니다.
- PCoIP 의 하드웨어 구현은 AES 와 IPsec(IP 보안)를 사용합니다.
- PCoIP 는 타사 VPN 클라이언트에서 작동합니다.

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

View Client with Local Mode 클라이언트 연결

View Client with Local Mode 는 휴대폰 사용자에게 로컬 컴퓨터에서 View 데스크톱을 체크아웃하는 기능을 제공합니다.

View Client with Local Mode 는 LAN 기반 데이터 전송의 터널링 통신 및 비터널링 통신 모두를 지원합니다. View Client 및 View 연결 서버 간 통신이 암호화됩니다. 터널링된 통신의 경우 모든 트래픽은 View 연결 서버 호스트를 통해 라우팅되며 View 연결 서버 및 View 전송 서버 간 데이터 전송을 암호화할지 여부를 지정할 수 있습니다. 터널링되지 않은 통신의 경우 데이터는 클라이언트 시스템의 로컬 데스크톱과 View 전송 서버 사이에서 직접 전송됩니다. 이러한 데이터 전송의 암호화 여부도 지정할 수 있습니다.

로컬 데이터는 터널링된 통신을 구성할지 또는 터널링되지 않은 통신을 구성할지에 상관없이 사용자의 컴퓨터에서 항상 암호화됩니다.

클라이언트 시스템에 로컬로 저장된 데이터 디스크는 AES-128 의 기본 암호화 기능을 사용하여 암호화됩니다. 암호화 키는 사용자의 자격 증명(사용자 이름 및 암호 또는 스마트 카드 및 PIN)의 해시에서 파생된 키를 사용하여 클라이언트 시스템에 암호화되어 저장됩니다. 서버 쪽 키는 View LDAP 에 저장됩니다. 서버의 View LDAP 를 보호하는 데 사용할 보안 측정값은 LDAP 에 저장된 로컬 모드 암호화 키를 보호합니다.

참고 암호화 키 암호를 AES-128 에서 AES-192 또는 AES-256 으로 변경할 수 있습니다.

데스크톱 수명은 정책을 통해 제어됩니다. 클라이언트와 View 연결 서버 간의 연결이 끊어질 경우, 사용자는 서버와 연결되지 않고 사용할 수 있는 최대 시간 동안만 데스크톱을 사용할 수 있으며 그 이후에는 액세스가 거부됩니다. 클라이언트 측에서는 애플리케이션에 내장되어 있는 키로 암호화한 파일에 이 만료 정책을 저장합니다. 이 기본 제공 키는 암호에 액세스할 수 있는 권한이 있는 사용자가 만료 정책을 무시하지 못하도록 합니다.

사용자 인증 방법 선택

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

- Active Directory 인증(60 페이지)

  각 View Connection Server 인스턴스는 Active Directory 도메인에 가입해 있으며 사용자는 가입된 도메인의 Active Directory 에 대해 인증 받습니다. 사용자는 또한 신뢰 계약이 있는 모든 추가 사용자 도메인에 대해서도 인증 받습니다.

- 이중 인증 사용(61 페이지)

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

- 스마트 카드 인증(61 페이지)

  스마트 카드는 컴퓨터 칩이 내장된 소형 플라스틱 카드입니다. 많은 정부 기관 및 대기업에서는 스마트 카드를 사용하여 컴퓨터 네트워크에 액세스하는 사용자를 인증합니다. 또한 스마트 카드는 공동 액세스 카드(CAC)에도 적용됩니다.

- 현재 사용자로 로그인 기능 사용(62 페이지)

  View Client 사용자가 **현재 사용자로 로그인** 확인란을 선택하면 클라이언트 시스템에 로그인할 때 입력했던 자격 증명을 사용해 View Connection Server 인스턴스와 View 데스크톱을 인증합니다. 추가 사용자 인증은 필요하지 않습니다.

Active Directory 인증

각 View Connection Server 인스턴스는 Active Directory 도메인에 가입해 있으며 사용자는 가입된 도메인의 Active Directory 에 대해 인증 받습니다. 사용자는 또한 신뢰 계약이 있는 모든 추가 사용자 도메인에 대해서도 인증 받습니다.

예를 들어 View Connection Server 인스턴스가 도메인 A 의 구성원이고 도메인 A 와 도메인 B 간에 신뢰 계약이 존재하면 도메인 A 와 도메인 B 사용자는 View Client 에서 View Connection Server 인스턴스에 연결할 수 있습니다.

마찬가지로 도메인 A 와 혼합 도메인 환경의 MIT Kerberos 영역 간에 신뢰 계약이 있으면 Kerberos 영역의 사용자는 View Client 에서 View Connection Server 인스턴스에 연결할 때 Kerberos 영역 이름을 선택할 수 있습니다.

View Connection Server 는 호스트가 있는 도메인부터 신뢰 관계를 탐색하여 액세스할 수 있는 도메인을 확인합니다. 규모가 작고 연결된 도메인 집합의 경우 View Connection Server 는 신속하게 도메인 전체 목록을 확인할 수 있지만 도메인 수가 증가하거나 도메인 간의 연결성이 떨어지면 작업 시간이 늘어납니다. 목록에는 사용자가 데스크톱에 로그인할 때 사용자에게 제공하기 원하지 않는 도메인이 포함될 수 있습니다.

관리자는 `vdmadmin` 명령줄 인터페이스를 사용해 도메인 필터링을 구성함으로써 View Connection Server 인스턴스에서 검색하고 사용자에게 표시하는 도메인을 제한할 수 있습니다. 자세한 내용은 *VMware View 관리* 설명서를 참조하십시오.

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

이중 인증 사용

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

View 5.1 이상 버전에서는 VMware View에 포함된 이중 인증 기능에 RADIUS 지원이 추가되었습니다.

- RADIUS 지원은 매우 다양한 대체 이중 토큰 기반 인증 옵션을 제공합니다.
- VMware View는 현재 타사 솔루션 제공자가 View에 고급 인증 확장을 통합할 수 있도록 하는 개방 표준 확장 인터페이스를 제공합니다.

RSA SecurID 및 RADIUS와 같은 이중 인증 솔루션은 인증 관리자와 협력적으로 작동하므로 View 연결 서버 호스트에 적합하게 이러한 서버를 구성하고 액세스 권한을 부여해야 합니다. 예를 들어, RSA SecurID를 사용하는 경우 인증 관리자는 RSA 인증 관리자입니다. RADIUS가 있는 경우, 인증 관리자는 RADIUS 서버입니다.

이중 인증을 사용하려면 각 사용자에게 RSA SecurID 토큰 등 해당 인증 관리자에 등록된 토큰이 있어야 합니다. 이중 인증 토큰은 고정 간격으로 인증 코드를 생성하는 하드웨어 또는 소프트웨어의 일부입니다. 인증을 위해 PIN과 인증 코드에 대한 정보를 모두 알아야 하는 경우도 있습니다.

여러 View 연결 서버 인스턴스가 있는 경우, 일부 인스턴스에 이중 인증을 구성하고 나머지에는 다른 사용자 인증 방법을 구성할 수 있습니다. 예를 들어, 인터넷을 통해 원격으로 View 데스크톱에 액세스하는 사용자 전용으로 이중 인증을 구성할 수 있습니다.

VMware View는 RSA SecurID 준비 프로그램을 통해 인증되며 새 PIN 모드, 다음 토큰코드 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. 또한 스마트 카드는 공동 액세스 카드(CAC)에도 적용됩니다.

스마트 카드 인증은 Windows 기반 View Client 및 View Client with Local Mode에서만 지원됩니다. View Administrator에서는 지원되지 않습니다.

관리자는 스마트 카드 인증을 위해 개별 View Connection Server 인스턴스를 사용할 수 있습니다. 스마트 카드 인증을 사용하기 위해 View Connection Server 인스턴스를 사용하도록 설정하면 truststore 파일에 루트 인증서가 추가된 후 View Connection Server 설정이 수정됩니다.

스마트 카드 인증을 사용하는 클라이언트 연결은 SSL을 사용하도록 설정되어 있어야 합니다. 관리자는 View Administrator의 전역 매개 변수를 설정하여 클라이언트 연결을 위해 SSL을 사용하도록 설정할 수 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.

로컬 데스크톱에서 스마트 카드를 사용하려면 스마트 카드 등록 중에 1024 비트 또는 2048 비트 키 크기를 선택해야 합니다. 512 비트 키를 가진 인증서는 로컬 데스크톱에서 지원되지 않습니다. 기본적으로 View Connection Server는 사용자가 로컬 데스크톱을 체크인하고 체크아웃할 때 AES-128을 사용하여 가상 디스크 파일을 암호화합니다. 암호화 키 암호를 AES-192 또는 AES-256으로 변경할 수 있습니다.

현재 사용자로 로그인 기능 사용

View Client 사용자가 **현재 사용자로 로그인** 확인란을 선택하면 클라이언트 시스템에 로그인할 때 입력했던 자격 증명을 사용해 View Connection Server 인스턴스와 View 데스크톱을 인증합니다. 추가 사용자 인증은 필요하지 않습니다.

이 기능을 사용하려면 View Connection Server 인스턴스와 클라이언트 시스템에 사용자 자격 증명이 저장되어 있어야 합니다.

- View Connection Server 인스턴스에서 사용자 이름, 도메인, 선택적 UPN 과 함께 사용자 자격 증명을 암호화해 사용자 세션에 저장합니다. 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 View LDAP 또는 디스크 파일에 저장되지 않습니다.
- 클라이언트 시스템에서 사용자 자격 증명이 암호화되어 View Client 의 구성 요소인 인증 패키지에 있는 테이블에 저장됩니다. 자격 증명은 사용자가 로그인하면 테이블에 추가되고 사용자가 로그아웃하면 테이블에서 제거됩니다. 테이블은 휘발성 메모리에 상주합니다.

관리자는 View Client 그룹 정책 설정을 사용해 **현재 사용자로 로그인** 확인란의 가용성을 제어하고 기본값을 지정합니다. 관리자는 또한 그룹 정책을 사용해 사용자가 View Client 에서 **현재 사용자로 로그인** 확인란을 선택할 때 전송되는 자격 증명 정보 및 사용자 ID 를 수용할 View Connection Server 인스턴스를 지정합니다.

현재 사용자로 로그인 기능은 다음과 같은 제한 사항이 있습니다.

- View Connection Server 인스턴스에 대해 스마트 카드로 인증하도록 설정한 경우에는 **현재 사용자로 로그인** 확인란을 선택한 스마트 카드 사용자는 View 데스크톱 로그인 시 스마트 카드와 PIN 으로 다시 인증 받아야 합니다.
- 로그인할 때 **현재 사용자로 로그인** 확인란을 선택하면 로컬 모드로 사용하기 위해 데스크톱을 체크아웃할 수 없습니다.
- 클라이언트가 로그인하는 시스템 시간과 View Connection Server 호스트 시간이 동기화되어 있어야 합니다.
- 클라이언트 시스템에서 기본 **네트워크에서 이 컴퓨터 액세스** 사용자 권한 할당을 수정한 경우 VMware 기술 자료(KB) 문서 1025691 에 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 View Connection Server 인스턴스에 연결할 경우, 사용자에게 자격 증명을 묻는 메시지가 나타나며 현재 사용자로 로그인 기능이 작동하지 않습니다.

View 데스크톱 액세스 제한

제한된 권한 기능을 사용하여 사용자가 연결하는 View Connection Server 인스턴스를 기반으로 View 데스크톱 액세스를 제한할 수 있습니다.

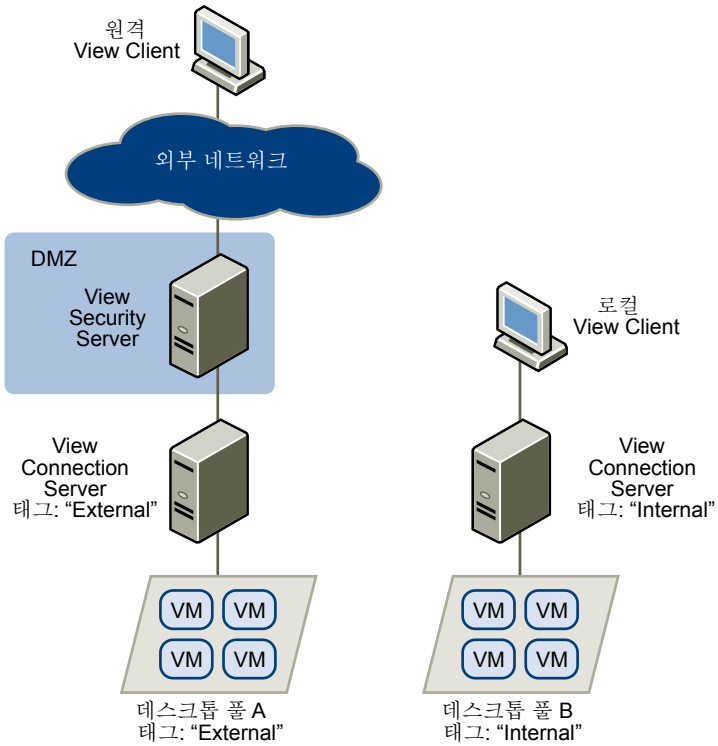
제한된 권한을 사용하여 View Connection Server 인스턴스에 하나 이상의 태그를 할당합니다. 그런 다음 데스크톱 풀을 구성할 때 데스크톱 풀에 액세스하려는 View Connection Server 인스턴스 태그를 선택합니다. 태그가 지정된 View Connection Server 인스턴스를 통해 사용자가 로그인할 경우 일치하는 태그가 최소한 하나이거나 태그가 없는 해당 데스크톱 풀에만 액세스할 수 있습니다.

예를 들어 VMware View 배포에는 두 개의 View Connection Server 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 View Connection Server 인스턴스에 "Internal" 태그를 할당합니다.
- 보안 서버와 연결되고 외부 사용자를 지원하는 View Connection Server 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 External 로 태그가 지정된 View Connection Server 를 통해 로그인하기 때문에 Internal 로 태그가 지정된 데스크톱 풀을 볼 수 없으며 내부 사용자는 Internal 로 태그가 지정된 View Connection Server 를 통해 로그인하기 때문에 External 로 태그가 지정된 데스크톱 풀을 볼 수 없습니다. 그림 5-1 에는 이 구성이 나타나 있습니다.

그림 5-1. 제한된 권한의 예



또한 제한된 권한을 사용하여 특정 View Connection Server 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 View Connection Server 인스턴스를 통해 특정 클라이언트를 강제로 연결해야 합니다.

그룹 정책 설정을 사용한 View 데스크톱 보안

VMware View는 View 데스크톱 보안에 사용할 수 있는 보안 관련 그룹 정책 설정이 포함된 그룹 정책 관리(ADM) 템플릿을 포함합니다.

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

- 사용자가 View Client의 **현재 사용자로 로그인** 확인란을 선택할 때 전달된 사용자 ID 및 자격 증명 정보를 허용할 수 있는 View Connection Server 인스턴스를 지정합니다.
- View Client의 스마트 카드 인증을 위해 단일 로그온을 사용하도록 지정합니다.
- View Client에서 서버 SSL 인증서 확인을 구성합니다.
- 사용자가 View Client 명령줄 옵션을 사용하여 자격 증명 정보를 제공하지 못하도록 합니다.
- 비 View 클라이언트 시스템이 RDP를 사용하여 View 데스크톱에 연결하지 못하도록 합니다. 연결을 View에서 관리하도록 즉, 사용자가 View Client를 사용하여 View 데스크톱에 연결해야 하도록 이 정책을 설정할 수 있습니다.

View Client 그룹 정책 설정 사용에 대한 자세한 내용은 *VMware View 관리* 설명서에 나와 있습니다.

보안 클라이언트 시스템에 모범 사례 구현

보안 클라이언트 시스템에 모범 사례를 구현해야 합니다.

- 일정 기간 사용하지 않으면 절전 상태로 전환되고 사용자가 컴퓨터를 활성화하려면 암호를 입력하도록 클라이언트 시스템을 구성하십시오.
- 사용자가 클라이언트 시스템을 시작할 때 사용자 이름과 암호를 입력하도록 요구하십시오. 자동 로그인을 허용하도록 클라이언트 시스템을 구성하지 마십시오.
- Mac 클라이언트 시스템의 경우 키체인과 사용자 계정의 암호를 다르게 설정하십시오. 암호가 다른 경우에는 시스템에서 사용자 대신 암호를 입력하기 전에 사용자에게 메시지가 표시됩니다. 또한 FileVault 보호 기능 설정을 고려하십시오.
- 로컬 모드 클라이언트 시스템은 원격 및 인터넷에 연결할 때보다 로컬 모드에서 실행할 때 네트워크 액세스 수가 많을 수 있습니다. 로컬 모드 클라이언트 시스템에 대해 인트라넷 네트워크 보안 정책을 강제로 사용하거나, 로컬 모드에서 실행할 때 로컬 모드 클라이언트 시스템에 대해 네트워크 액세스를 사용하지 못하도록 하는 방법을 고려하십시오.

관리자 역할 할당

VMware View 환경에서 주요 관리 작업은 View Administrator를 이용할 수 있는 사용자와 이들 사용자에게 수행 권한을 부여할 작업을 결정하는 것입니다.

View 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 View Administrator에서 볼 수 있는 내용을 제어합니다.

관리자는 폴더를 생성해 데스크톱 풀을 세분화하고 View 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.

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

보안 서버 사용 준비

보안 서버는 View Connection Server 기능의 하위 집합을 실행하는 View Connection Server 의 특별한 인스턴스입니다. 보안 서버를 사용하여 인터넷과 내부 네트워크 사이에 추가 보안 계층을 제공할 수 있습니다.

보안 서버는 DMZ 에 상주하며 신뢰할 수 있는 네트워크 내 연결을 위한 프록시 호스트 역할을 합니다. 각 보안 서버는 View Connection Server 의 인스턴스와 연결되며 모든 트래픽을 해당 인스턴스로 전달합니다. 연결 서버 하나에 여러 보안 서버를 연결할 수 있습니다. 이 디자인은 공용 인터넷에서 View Connection Server 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 View Connection Server 인스턴스 및 보안 서버 간 통신을 위해 포트를 구성해야 합니다. 자세한 내용은 "DMZ 기반 보안 서버의 방화벽 규칙," (68 페이지)에 나와 있습니다.

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

참고 현재 View 4.6 의 보안 서버는 PCoIP 디스플레이 프로토콜을 사용하는 클라이언트가 VPN 이 아니라 보안 서버를 사용할 수 있도록 PCoIP 보안 게이트웨이 구성 요소를 포함합니다.

PCoIP 를 사용하기 위해 VPN 을 설정하는 것에 대한 자세한 내용은 VMware 웹 사이트에서 사용 가능한 다음 솔루션 개요를 참조하십시오.

- *VMware View and Juniper Networks SA Servers SSL VPN Solution(VMware View 및 Juniper Networks SA Servers SSL VPN 솔루션)*
- *VMware View and F5 BIG-IP SSL VPN Solution(VMware View 및 F5 BIG-IP SSL VPN 솔루션)*
- *VMware View and Cisco Adaptive Security Appliances (ASA) SSL VPN Solution(VMware View 및 Cisco Adaptive Security Appliances(ASA) SSL VPN 솔루션)*

보안 서버 배포의 모범 사례

DMZ 에서 보안 서버를 운영할 때는 모범 사례 보안 정책 및 절차를 따라야 합니다.

VMware 인프라로 DMZ 가상화 백서에는 가상화된 DMZ 에 대한 모범 사례의 예가 포함되어 있습니다. 본 백서의 다양한 권장 사항은 물리적 DMZ 에도 적용할 수 있습니다.

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

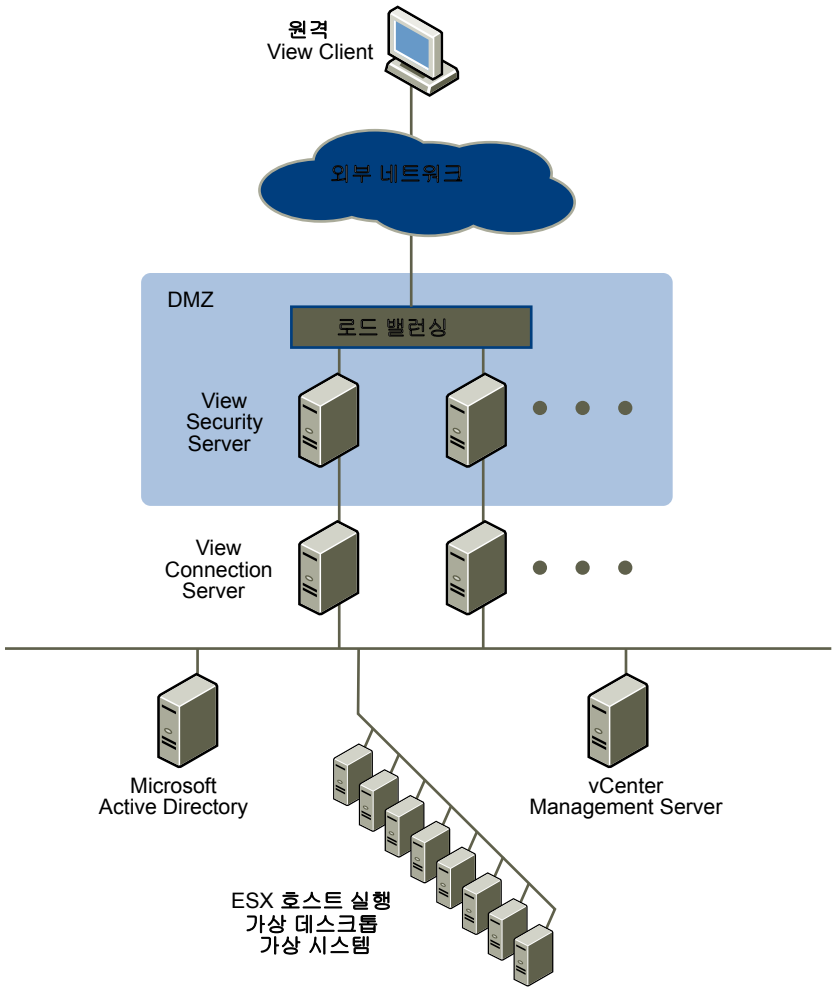
또는 네트워크 스위치의 고급 보안 기능을 사용해 보안 서버와 View Connection Server 통신에 대한 악성 모니터링을 방지하고 ARP Cache Poisoning 등과 같은 모니터링 공격에 대비할 수 있습니다. 네트워크 장비에 대한 자세한 내용은 관리 설명서를 참조하십시오.

보안 서버 토폴로지

여러 가지의 보안 서버 토폴로지를 구현할 수 있습니다.

그림 5-2 에 나타난 토폴로지는 DMZ 에 로드 밸런싱된 보안 서버 두 개가 포함된 고가용성 환경을 보여줍니다. 보안 서버는 내부 네트워크 내 두 개의 View Connection Server 인스턴스와 통신합니다.

그림 5-2. DMZ 의 로드 밸런싱된 보안 서버

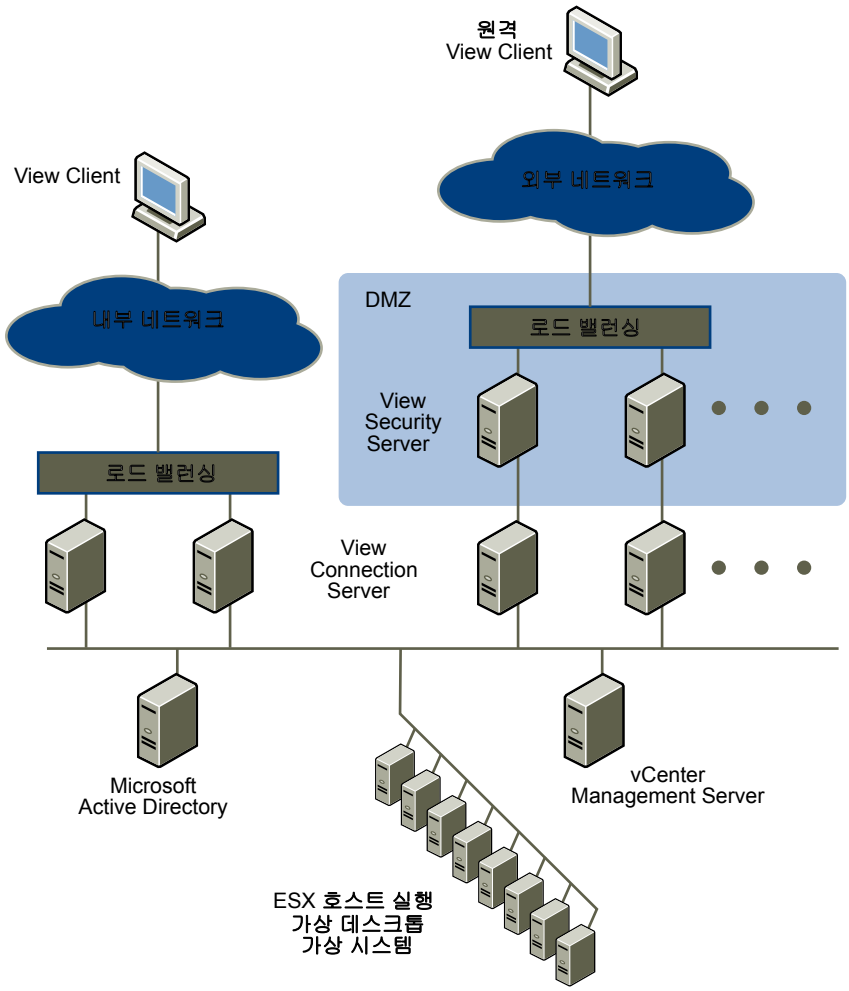


보안 서버에 연결한 원격 사용자는 View 데스크톱에 액세스하기 전에 바르게 인증해야 합니다. DMZ 양쪽에 적절한 방화벽 규칙이 있는 경우 이 토폴로지는 인터넷에 위치한 클라이언트 디바이스에서 View 데스크톱에 액세스하는 데 적합합니다.

View Connection Server 의 각 인스턴스에 여러 보안 서버를 연결할 수 있습니다. 또한 표준 배포와 DMZ 배포를 조합하여 내부 사용자 및 외부 사용자에 대해 액세스를 제공할 수 있습니다.

그림 5-3 에 나타난 토폴로지는 View Connection Server 의 인스턴스 네 개가 하나의 그룹 역할을 하는 환경을 보여줍니다. 내부 네트워크의 인스턴스는 내부 네트워크 사용자 전용이며 외부 네트워크의 인스턴스는 외부 네트워크 사용자 전용입니다. 보안 서버와 연결된 View Connection Server 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. View Connection Server 는 자체의 로드 밸런싱 기능을 제공하지 않습니다. View Connection Server 는 타사 로드 밸런싱 솔루션과 함께 사용할 수 있습니다.

DMZ 기반 보안 서버의 방화벽

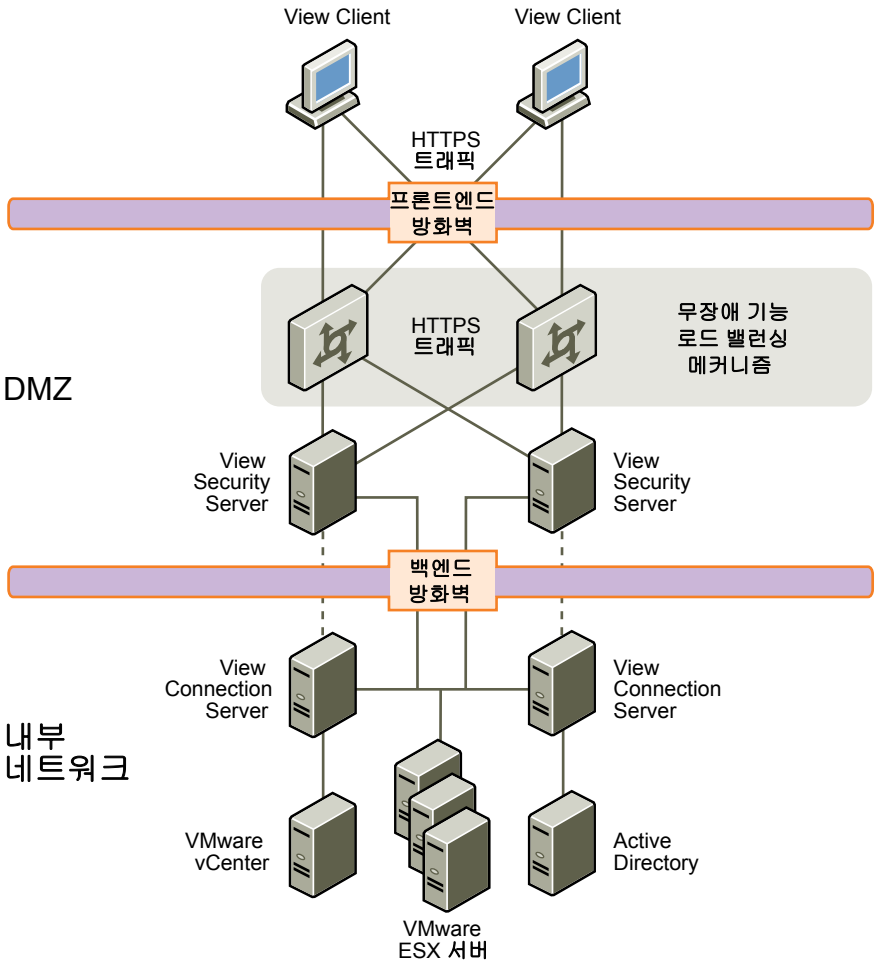
DMZ 기반 보안 서버를 배포할 때는 2 개 방화벽을 포함해야 합니다.

- 외부 네트워크 지향 프론트엔드 방화벽은 DMZ 와 내부 네트워크를 보호해야 합니다. 외부 네트워크 트래픽이 DMZ 에 도달할 수 있도록 방화벽을 구성합니다.
- DMZ 와 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.

그림 5-4 는 프론트엔드와 백엔드 방화벽을 포함하는 구성의 예입니다.

그림 5-4. 이중 방화벽 토폴로지



DMZ 기반 보안 서버의 방화벽 규칙

DMZ 기반 보안 서버는 프론트엔드와 백엔드 방화벽에 대해 특정 방화벽 규칙이 필요합니다.

프론트엔드 방화벽 규칙

외부 클라이언트 디바이스가 DMZ 내에 있는 보안 서버에 연결할 수 있도록 허용하려면 프론트엔드 방화벽에서 특정 TCP 와 UDP 포트에 대한 트래픽을 허용해야 합니다. 표 5-1 은 프론트엔드 방화벽 규칙을 요약 설명합니다.

표 5-1. 프론트엔드 방화벽 규칙

소스	포트	프로토콜	대상	포트	참고
View Client	TCP 임의	HTTPS	보안 서버	TCP 443	외부 클라이언트 디바이스가 TCP 포트 443 의 DMZ 내에 있는 보안 서버에 연결되어 연결 서버 인스턴스 및 View 데스크톱과 통신합니다.
View Client	TCP 임의 UDP 임의	PCoIP	보안 서버	TCP 4172 UDP 4172	외부 클라이언트 디바이스가 TCP 포트 4172 및 UDP 포트 4172 의 DMZ 내에 있는 보안 서버에 연결되어 PCoIP 를 통해 View 데스크톱과 통신합니다.
보안 서버	UDP 4172	PCoIP	View Client	UDP 임의	보안 서버는 UDP 포트 4172 에서 외부 클라이언트 디바이스로 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.

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. View 데스크톱과 View 연결 서버 인스턴스가 서로 통신할 수 있도록 백엔드 방화벽 뒤에 있는 내부 방화벽을 유사하게 구성해야 합니다. 표 5-2 는 백엔드 방화벽 규칙을 요약 설명합니다.

표 5-2. 백엔드 방화벽 규칙

소스	포트	프로토콜	대상	포트	참고
보안 서버	UDP 500	IPSec	연결 서버	UDP 500	보안 서버는 UDP 포트 500 에서 View 연결 서버 인스턴스와 IPSec 를 조정합니다.
연결 서버	UDP 500	IPSec	보안 서버	UDP 500	View 연결 서버 인스턴스는 UDP 포트 500 에서 보안 서버에 응답합니다.
보안 서버	TCP 임의	AJP13	연결 서버	TCP 8009	보안 서버는 TCP 포트 8009 의 View 연결 서버 인스턴스에 연결되어 외부 클라이언트 디바이스에서 웹 트래픽을 전달합니다. IPSec 를 사용하도록 설정하고 단방향 또는 양방향 NAT 가 백엔드 방화벽에 구성되어 있는 경우, UDP 포트 4500 이 보안 서버 및 View 연결 서버 인스턴스 사이 각 방향에서 허용되어야 합니다. 그러면 AJP13 트래픽의 TCP 포트 8009 대신 사용됩니다.
보안 서버	TCP 임의	JMS	연결 서버	TCP 4001	보안 서버가 TCP 포트 4001 의 View 연결 서버 인스턴스에 연결되어 JMS(Java Message Service) 트래픽을 교환합니다.
보안 서버	TCP 임의	RDP	View 데스크톱	TCP 3389	보안 서버가 TCP 포트 3389 의 View 데스크톱에 연결되어 RDP 트래픽을 교환합니다.
보안 서버	TCP 임의	MMR	View 데스크톱	TCP 4927	보안 서버가 TCP 포트 9427 의 View 데스크톱에 연결되어 MMR 트래픽을 수신합니다.
보안 서버	TCP 임의 UDP 임의	PCoIP	View 데스크톱	TCP 4172 UDP 4172	보안 서버가 TCP 포트 4172 및 UDP 포트 4172 의 View 데스크톱에 연결되어 PCoIP 트래픽을 교환합니다.
View 데스크톱	UDP 4172	PCoIP	보안 서버	UDP 임의	View 데스크톱이 UDP 포트 4172 에서 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.

표 5-2. 백엔드 방화벽 규칙 (계속)

소스	포트	프로토콜	대상	포트	참고
보안 서버	TCP 32111	USB-R	View 데스크톱	TCP 4172	보안 서버가 TCP 포트 32111 의 View 데스크톱에 연결되어 외부 클라이언트 디바이스 및 View 데스크톱 사이에서 USB 리디렉션 트래픽을 교환합니다.
보안 서버	TCP 임의	HTTP	전송 서버	TCP 80	보안 서버가 TCP 포트 80 의 View 전송 서버에 연결되어 외부 로컬 클라이언트로 View 데스크톱 데이터를 다운로드하고 복제 데이터를 교환합니다.
보안 서버	TCP 임의	HTTPS	전송 서버	TCP 443	로컬 모드 작업 및 데스크톱 프로비저닝에 SSL 을 사용하도록 View 전송 서버를 구성하는 경우, 보안 서버가 TCP 포트 80 대신 TCP 포트 443 의 View 전송 서버에 연결되어 외부 로컬 모드 클라이언트에 View 데스크톱 데이터를 다운로드하고 복제 데이터를 교환합니다.

View 연결 서버 상호 통신용 TCP 포트

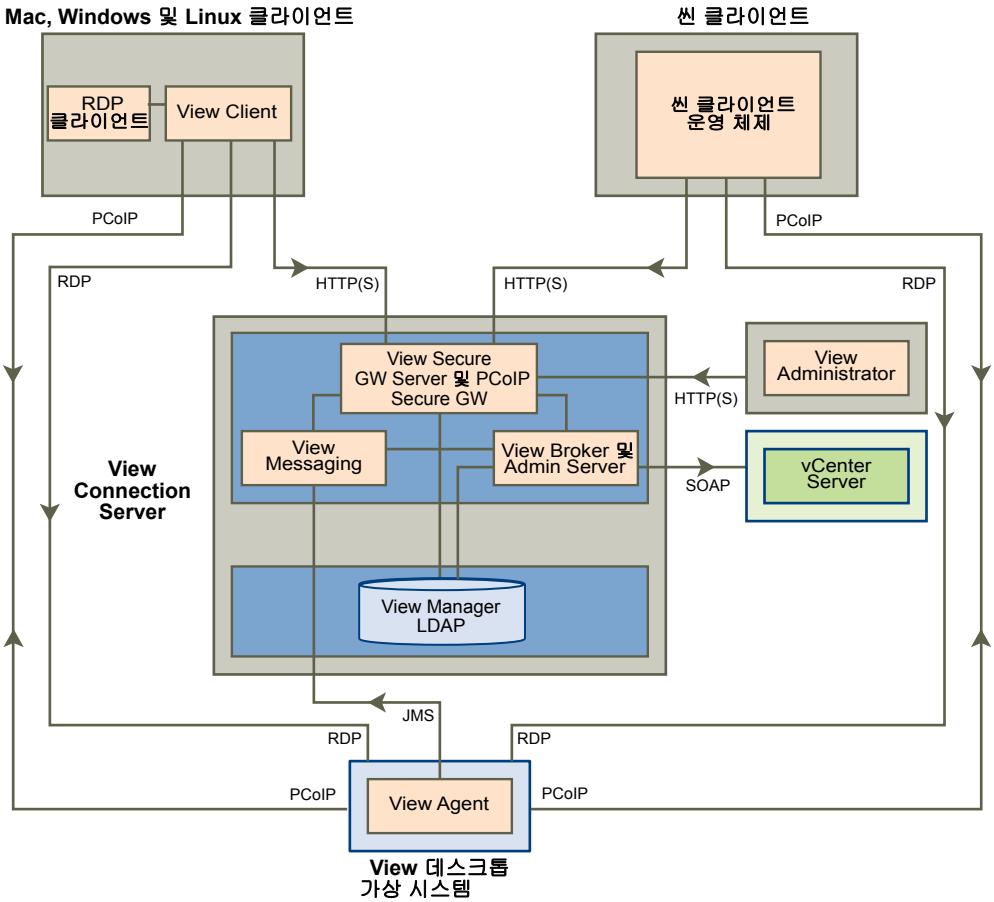
View 연결 서버 인스턴스 그룹은 추가 TCP 포트를 사용해 서로 통신합니다. 예를 들어 View 연결 서버 인스턴스는 포트 4100 을 사용해 서로 JMSIR(JMS inter-router) 트래픽을 전송합니다. 일반적으로 그룹 내 View 연결 서버 인스턴스 간에는 방화벽을 사용하지 않습니다.

VMware View 통신 프로토콜 이해

VMware View 구성 요소는 여러 프로토콜을 사용하여 메시지를 교환합니다.

그림 5-5 에는 보안 서버가 구성되지 않았을 때 각 구성 요소가 통신에 사용하는 프로토콜이 나타나 있습니다. 즉, RDP 를 위한 보안 터널 및 PCoIP 보안 게이트웨이가 꺼져 있습니다. 이 구성은 일반 LAN 배포에 사용될 수 있습니다.

그림 5-5. 보안 서버가 없는 VMware View 구성 요소 및 프로토콜



참고 이 그림은 PCoIP 또는 RDP 를 사용하는 클라이언트의 직접 연결을 보여줍니다. 그러나 기본 설정은 PCoIP 의 직접 연결 및 RDP 의 터널 연결을 설정하는 것입니다.

각 프로토콜에 사용된 기본 포트에 대한 내용은 표 5-3 에 나와 있습니다.

그림 5-6 에는 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 VMware View 구성 요소 및 프로토콜

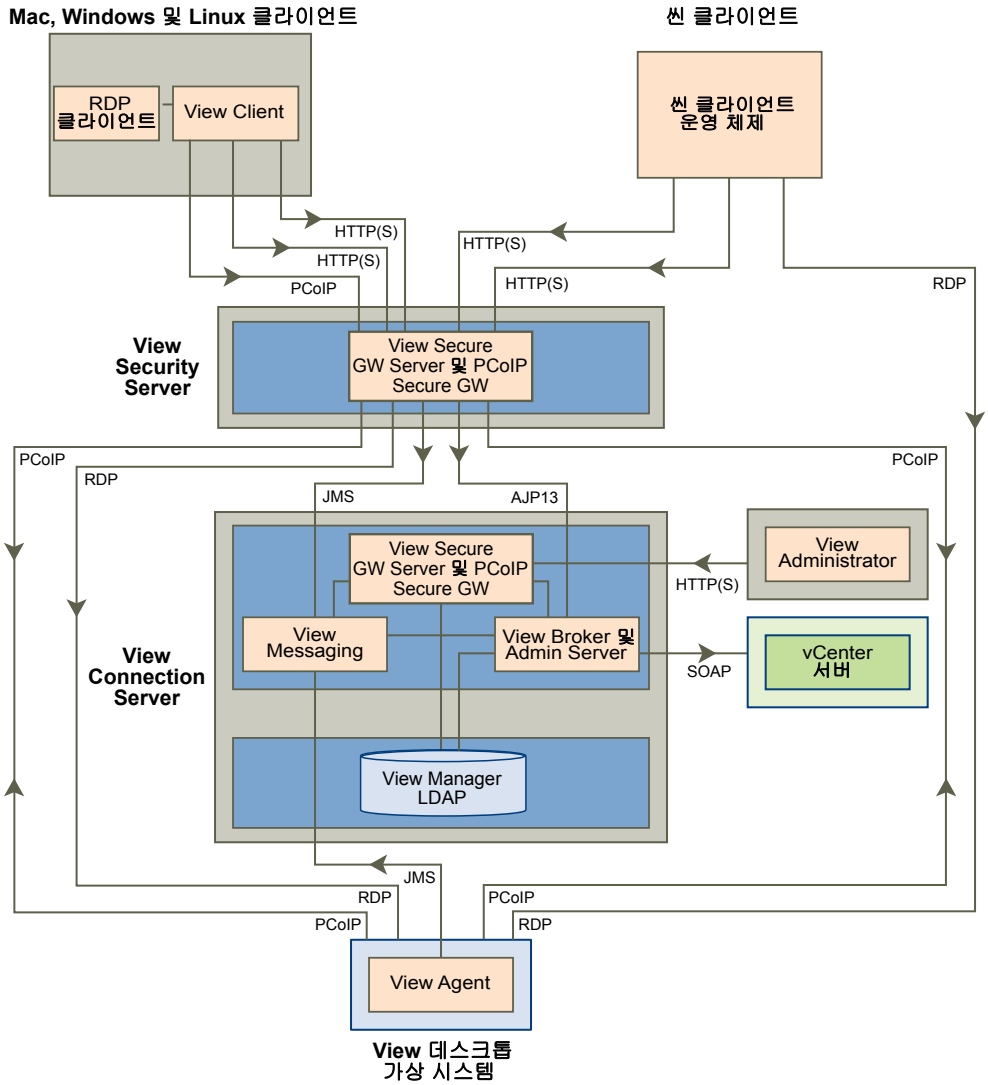


표 5-3 에는 각 프로토콜에서 사용하는 기본 포트가 나열되어 있습니다.

표 5-3. 기본 포트

프로토콜	포트
JMS	TCP 포트 4001
AJP13	TCP 포트 8009 **참고** AJP13 은 보안 서버 구성에만 사용됩니다.
HTTP	TCP 포트 80
HTTPS	TCP 포트 443
RDP	TCP 포트 3389 MMR 의 경우 TCP 포트 9427 과 RDP 를 함께 사용합니다. **참고** View Connection Server 인스턴스가 클라이언트 직접 연결을 위해 구성된 경우 이러한 프로토콜은 클라이언트에서 View 데스크톱으로 바로 연결되며 View Secure GW Server 구성 요소를 통해 터널링되지 않습니다.

표 5-3. 기본 포트 (계속)

프로토콜	포트
SOAP	TCP 포트 80 또는 443
PCoIP	View Client 에서 View 데스크톱까지의 TCP 포트 4172 입니다. 또한 PCoIP 는 양방향으로 UDP 포트 4172 를 사용합니다.
PCoIP 또는 RDP	USB 리디렉션의 경우 클라이언트부터 View 데스크톱까지 TCP 포트 32111 과 PCoIP 또는 RDP 를 함께 사용합니다.

View Broker 및 관리 서버

View Connection Server 의 핵심인 View Broker 구성 요소는 VMware View 클라이언트와 View Connection Server 간 모든 사용자 상호 작용을 책임집니다. 또한 View Broker 에는 View Administrator 웹 클라이언트에서 사용되는 관리 서버가 포함됩니다.

View Broker 는 vCenter Server 와 밀접하게 작동하여 가상 시스템 생성 및 전원 작업을 포함하여 View 데스크톱에 고급 관리를 제공합니다.

View Secure Gateway Server

View Secure Gateway Server 는 VMware View 클라이언트 및 보안 서버 또는 View Connection Server 인스턴스 간 보안 HTTPS 연결을 위한 서버 쪽 구성 요소입니다.

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

참고 PCoIP 디스플레이 프로토콜을 사용하는 클라이언트는 USB 리디렉션 및 MMR(멀티미디어 리디렉션) 가속을 위해 터널 연결을 사용할 수 있지만 다른 모든 데이터의 경우 PCoIP 는 보안 서버에서 PCoIP 보안 게이트웨이를 사용합니다.

또한 View Secure Gateway Server 는 사용자 인증 및 데스크톱 선택 트래픽을 포함하여 VMware View 클라이언트에서 View Broker 구성 요소로 다른 웹 트래픽을 전달하는 책임을 집니다. 또한 View Secure Gateway Server 는 View Administrator 클라이언트 웹 트래픽을 관리 서버 구성 요소로 전달합니다.

PCoIP 보안 게이트웨이

View 4.6 부터는 보안 서버에 PCoIP 보안 게이트웨이 구성 요소가 포함되어 있습니다. PCoIP 보안 게이트웨이를 사용하도록 설정하는 경우 인증 후 PCoIP 를 사용하는 View 클라이언트에서 보안 서버에 다른 보안 연결을 생성할 수 있습니다. 이 연결을 통해 인터넷에서 원격 클라이언트로 View 데스크톱에 액세스할 수 있습니다.

PCoIP 보안 게이트 구성 요소를 사용하도록 설정하면 보안 서버를 사용해 View 데스크톱에 PCoIP 트래픽을 전달합니다. PCoIP 를 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 View 클라이언트에서 View 데스크톱으로 바로 이동합니다.

가정 또는 모바일 작업자와 같은 최종 사용자가 인터넷으로 데스크톱에 액세스하는 경우 필요한 보안 및 연결 수준을 보안 서버에서 제공하기 때문에 VPN 을 연결하지 않아도 됩니다. PCoIP 보안 게이트웨이 구성 요소는 인증된 사용자를 대신한 원격 데스크톱 트래픽만 기업 데이터 센터에 들어갈 수 있도록 보증합니다. 최종 사용자는 액세스 권한을 부여받은 데스크톱 리소스에만 액세스할 수 있습니다.

View LDAP

View LDAP 는 View Connection Server 의 내장된 LDAP 디렉토리이며 모든 VMware View 구성 데이터의 구성 저장소입니다.

View LDAP 에는 각 View 데스크톱, 각 액세스 가능한 View 데스크톱, 함께 관리되는 다중 View 데스크톱 및 View 구성 요소 구성 설정을 나타내는 항목이 포함됩니다.

또한 View LDAP 에는 다른 VMware View 구성 요소의 자동화 및 알림 서비스를 제공하는 View 플러그인 DLL 집합이 포함되어 있습니다.

View 메시징

View 메시징 구성 요소는 View Connection Server 구성 요소 사이 그리고 View Agent 및 View Connection Server 사이의 통신을 위해 메시징 라우터를 제공합니다.

이 구성 요소는 VMware View 의 메시징에 사용되는 JMS(Java Message Service) API 를 지원합니다.

기본적으로 상호 구성 요소 메시지 검사에 사용되는 RSA 키는 512 비트입니다. RSA 키 크기는 더 완벽한 암호를 원할 경우 1024 비트까지 늘릴 수 있습니다.

모든 키를 1024 비트로 만들려면 첫 번째 View Connection Server 인스턴스가 설치된 후와 추가 서버 및 데스크톱이 생성되기 전에 바로 RSA 키 크기를 변경해야 합니다. 자세한 내용은 VMware 기술 자료(KB) 문서 1024431 에 나와 있습니다.

View 연결 서버의 방화벽 규칙

View 연결 서버 인스턴스와 보안 서버의 방화벽에서 특정 포트를 열어야 합니다.

View 연결 서버를 설치할 때 설치 프로그램에서 사용자에게 필요한 Windows 방화벽 규칙을 선택적으로 구성할 수 있습니다.

표 5-4. View 연결 서버 설치 중 열리는 포트

프로토콜	포트	View 연결 서버 인스턴스 유형
JMS	TCP 4001 수신	표준 및 복제
JMSIR	TCP 4100 수신	표준 및 복제
AJP13	TCP 8009 수신	표준 및 복제
HTTP	TCP 80 수신	표준, 복제, 보안 서버
HTTPS	TCP 443 수신	표준, 복제, 보안 서버
PCoIP	TCP 4172 수신, UDP 4172 양방향	표준, 복제, 보안 서버

View Agent 의 방화벽 규칙

View Agent 설치 프로그램은 방화벽에서 특정 TCP 포트를 엽니다. 이러한 포트는 다른 설명이 없는 한 수신용입니다.

표 5-5. View Agent 설치 중에 열리는 TCP 포트

프로토콜	포트
RDP	3389
USB 리디렉션	32111
MMR	9427
PCoIP	4172(TCP 및 UDP)

View Agent 설치 프로그램은 인바운드 RDP 연결에 대해 로컬 방화벽 규칙을 구성해 호스트 운영 체제의 현재 RDP 포트(대부분의 경우 3389)와 일치시킵니다. RDP 포트 번호를 변경하면 관련 방화벽 규칙도 변경해야 합니다.

View Agent 설치 프로그램에 Remote Desktop 지원을 사용하지 않도록 설정하면 포트 3389 와 32111 이 열리지 않으므로 수동으로 열어야 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 875357 에 나와 있습니다.

Active Directory 의 방화벽 규칙

VMware View 환경과 Active Directory 서버 사이에 방화벽이 있으면 필요한 포트가 모두 열렸는지 확인하십시오.

예를 들어 View Connection Server 는 Active Directory Global Catalog 와 LDAP(Lightweight Directory Access Protocol) 서버에 액세스할 수 있어야 합니다. 방화벽 소프트웨어에서 Global Catalog 와 LDAP 포트를 차단하면 관리자는 사용자 권한 구성 시 문제에 부딪칠 수 있습니다.

방화벽을 통해 제대로 작동하기 위해 Active Directory 용으로 열어야 하는 포트 정보는 사용하는 Active Directory 서버 버전의 Microsoft 설명서를 참조하십시오.

View Client with Local Mode 의 방화벽 규칙

View Client with Local Mode 데이터가 TCP 포트 902 를 통해 다운로드 및 업로드됩니다. 또한 View 전송 서버는 TCP 포트 902 를 통해 View Composer 이미지를 게시합니다. View Client with Local Mode 를 사용하려는 경우, TCP 포트 902 는 ESX/ESXi 호스트에 액세스할 수 있어야 하고 UDP 포트 445 는 View 전송 서버 저장소의 네트워크 공유를 사용하는 경우, 네트워크 공유에 액세스할 수 있어야 합니다.

VMware View 환경 설정 단계 개요 6

VMware View 를 설치하고 초기 배포 구성을 수행하려면 다음의 고수준 작업을 완료해야 합니다.

표 6-1. View 설치 및 설정 체크리스트

단계	작업
1	Active Directory 에 필요한 관리자 사용자 및 그룹을 설정하십시오. 지침: *VMware View 설치* 및 vSphere 설명서
2	VMware ESX/ESXi 호스트 및 vCenter Server 를 설치하고 설정하십시오. 지침: vSphere 설명서
3	링크드 클론 데스크톱을 배포하려는 경우, View Composer 를 vCenter Server 시스템 또는 별도의 서버에 설치합니다. View Composer 데이터베이스도 설치합니다. 지침: *VMware View 설치* 설명서
4	View 연결 서버를 설치하고 설정합니다. 이벤트 데이터베이스도 설치합니다. 지침: *VMware View 설치* 설명서
5	로컬 모드에서 데스크톱을 사용하려는 경우 전송 서버를 설치합니다. 지침: *VMware View 설치* 설명서
6	전체 클론 데스크톱 풀의 템플릿 또는 링크드 클론 데스크톱 풀의 상위 풀로 사용할 수 있는 가상 시스템을 하나 이상 만듭니다. 지침: *VMware View 관리* 설명서
7	데스크톱 풀을 만듭니다. 지침: *VMware View 관리* 설명서
8	데스크톱에 대한 사용자 액세스를 제어합니다. 지침: *VMware View 관리* 설명서
9	View Client 를 최종 사용자의 시스템에 설치하고 최종 사용자가 자신의 View 데스크톱에 액세스하도록 합니다. 지침: *VMware View 설치*
10	(선택 사항) 특정 인벤토리 개체 및 설정에 액세스할 수 있는 여러 레벨을 허용할 수 있도록 추가로 관리자를 만들고 구성합니다. 지침: *VMware View 관리* 설명서
11	(선택 사항) View 구성 요소, 데스크톱 풀 및 데스크톱 사용자의 동작을 제어하는 정책을 구성합니다. 지침: *VMware View 관리* 설명서
12	(옵션) 사용자가 데스크톱에 로그인할 때마다 개인 설정 데이터 및 설정에 대한 액세스 권한을 제공하는 View 개인 설정 관리를 구성합니다. 지침: *VMware View 관리* 설명서
13	(선택 사항) 보안 추가를 위해 스마트 카드 인증 또는 RADIUS 2 요소 인증 솔루션을 통합합니다. 지침: *VMware View 관리* 설명서

색인

기호 · 숫자

.vmdk 파일 40

A

Active Directory 9, 34, 60
ADM 템플릿 파일 64
Adobe Flash 29
AJP13 프로토콜 68, 70

C

CPU 계산 39, 45

D

DaaS(관리 서비스로서의 데스크톱) 7
DMZ 12, 65, 67, 73
DRS(Distributed Resource Scheduler) 49

E

ESX/ESXi 호스트 40

F

Fibre Channel SAN 어레이 30

G

GPO, View 데스크톱을 위한 보안 설정 64

H

HA 클러스터 46, 47, 49

I

I/O 스톰 51
iSCSI SAN 어레이 30

J

Java Message Service 74
Java Message Service 프로토콜 68
JMS 프로토콜 68, 70

L

LAN 구성 50
LDAP 구성 데이터 14
LDAP 디렉토리 12, 74
Linux 클라이언트 11, 13
Linux 용 View Client 12
LUN 31

M

Mac 클라이언트 11, 13
Microsoft RDP 17, 26, 59
MMR(멀티미디어 리디렉션) 26

N

NAS 어레이 30

O

Offline Desktop(Local Mode), *참조* 로컬 데스크톱

P

PCoIP, 하드웨어 요구 사항 19
PCoIP 보안 게이트웨이 연결 58, 65, 73

R

RADIUS 인증 61
RDP 21
RSA SecurID 인증, 구성 61
RSA 키 크기, 변경 74

S

SCOM 14
SCSI 어댑터 유형 45
storage, 감소, View Composer 사용 31

T

TCP 포트
  Active Directory 75
  View Agent 75
  View Client with Local Mode 75
  View 연결 서버 74
ThinApp 33

U

UDP 포트 68
USB 디바이스, View 데스크톱에서 사용 9, 17, 25
USB 리디렉션 25

V

vCenter, 구성 46

vCenter Server 13, 14, 29
vdmadmin 명령 14
View Administrator 13, 34
View Agent 13, 34
View Broker 73
View Client 12, 34
View Client with Local Mode, 연결 59
View Composer, 작업 47, 51
View Connection Server
  개요 12
  구성 13, 34, 47
  그룹화 65
  로드 밸런싱 65
  스마트 카드 인증 61
View Open Client 12
View Portal 11, 13
View PowerCLI 14
View Secure Gateway Server 73
View Transfer Server, 로컬 데스크톱 동기화 14
View 노드 구성 40
View 데스크톱 구성 35
View 메시징 74
View 배포 도표 11
View 전송 서버, 구성 48
View 팟 50, 54
vMotion 49
VMware View with Local Mode, *참조* 로컬 데스크톱
VMware View 설정 체크리스트 77
vSphere 7, 9, 30
vSphere 클러스터 49, 50

W
WAN 지원 53
Windows 로밍 프로파일 21
Windows 페이지 파일 40
Wyse MMR 17, 26

ㄱ
가상 개인 네트워크 65
가상 데스크톱의 기본 이미지 30, 31
가상 데스크톱의 디스크 공간 할당 40, 45
가상 시스템 구성
  vCenter 용 46
  View Composer 용 46
  View Connection Server 용 47
  View 데스크톱용 35
  View 전송 서버용 48
가상 시스템을 위한 RAM 할당 37, 45
가상 시스템을 위한 메모리 할당 37, 45
가상 인쇄 기능 9, 17, 25
가상 프로파일 9, 17
개인 설정 관리, 구성 및 관리 21
게이트웨이 서버 73
고급 사용자 36
공유 스토리지 30, 51
관리 서버 73
관리자 역할 64
권한, 제한된 62
기능 지원 표 17
기술 지원 5

ㄴ
네트워크 대역폭 51

ㄷ
다중 모니터 9, 26
단일 로그온(SSO) 13, 26, 62
대역폭 51, 53
데스크톱 소스 29
데스크톱 풀 13, 29, 31, 41
데스크톱 프로비저닝 7
데이터베이스 유형 50
데이터베이스 크기 조정 46
데이터스토어 31
디스플레이 프로토콜
  Microsoft RDP 17, 59
  PCoIP 59, 65
  View PCoIP 9, 17
  정의 19

ㄹ
레거시 PC 11
로드 밸런싱, View Connection Server 54, 65
로드 밸런싱, View 연결 서버 50
로밍 프로파일 21
로컬 데스크톱, View Transfer Server 14
로컬 데스크톱 사용, 장점 23
로컬 모드, *참조* 로컬 데스크톱
로컬 모드 사용자 43
링크드 클론 13, 31

ㅁ
멀티미디어 스트리밍 26
메시징 라우터 74
모바일 클라이언트 11
물리적 PC 47
미디어 파일 형식 지원 26

ㅂ
방화벽
  규칙 68
  백엔드 67
  프론트엔드 67
방화벽 규칙
  Active Directory 75
  View Agent 75
  View Client with Local Mode 75
  View 연결 서버 74
백엔드 방화벽
  구성 67
  규칙 68
보안 기능, 계획 57
보안 서버
  PCoIP 보안 게이트웨이 73
  개요 12
  구현 65
  로드 밸런싱 65
  방화벽 규칙 68
  배포 모범 사례 65
복제본 31
부동 할당 데스크톱 풀 29
비무장 지대 65, 67, 73
비즈니스 인텔리전스 소프트웨어 14

ㅅ
사용자 유형 36
사용자 인증
  Active Directory 60
  방법 60
  스마트 카드 61
사용자 프로파일 21
상위 가상 시스템 31, 32
새로 고침 기능 32, 40
설정, VMware View 77
소프트웨어 프로비저닝 33
스냅샷 32
스마트 카드 인증 61
스마트 카드 판독기 25, 61
스왑 파일 37
스토리지, 감소, View Composer 사용 30
스토리지 구성 51
스토리지 대역폭 51
씬 클라이언트 지원 11, 17

ㅇ
아키텍처 설계 요소 35
암호화, 사용자 자격 증명 62
애플리케이션 가상화 및 프로비저닝 32, 33
애플리케이션 스트리밍 33
에이전트, View 13
연결 유형
  PCoIP 보안 게이트웨이 58, 65, 73
  외부 클라이언트 65
  직접 59
  클라이언트 57
  터널 58
연결된 클론 32, 47, 51
영구 디스크 31
원격 데스크톱, 로컬 데스크톱과 비교 23
원격 디스플레이 프로토콜
  PCoIP 19
  RDP 21
위임된 관리 64
이중 방화벽 토폴로지 67
이중 인증 61
인쇄, 가상 25
일반 작업자 36, 37, 42
일시 중단 파일 37, 40

ㅈ
자격 증명, 사용자 62
작업자 유형 35-37, 39, 41
재구성 기능 32
재조정 기능 31
전문가 서비스 5
전용 할당 데스크톱 풀 29, 31
정책, 데스크톱 34
제한된 권한 62
지식 작업자 36, 37, 42
지연 53

ㅊ
처리 요구 사항 39
코어, 가상 시스템 밀도 39
클라이언트 시스템, 보안 모범 사례 64
클라이언트 연결
  PCoIP 보안 게이트웨이 58, 65, 73
  직접 59
  터널 58
클라이언트 직접 연결 47, 59
클러스터, vSphere 49
클론, 연결된 13, 32
키오스크 모드 44

ㅌ
태블릿 11
터널 연결 47, 58
터널링된 통신 59, 73
터미널 서버 47

템플릿, GPO 34
통신 프로토콜, 이해 70
통일된 액세스 47

ㅍ
풀
  데스크톱 31, 41
  로컬 모드 사용자 43
  일반 작업자 42
  지식 작업자 42
  키오스크 사용자 44
풀, 데스크톱 13, 29
프론트엔드 방화벽
  구성 67
  규칙 68
프린터 17

ㅎ
하드웨어 요구 사항, PCoIP 19
현재 사용자로 로그인 기능 26, 62
확장성, 계획 35