VMware View 설치

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-000730-00

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 설치

*VMware View 설치*에서는 VMware® View™ server 및 클라이언트 구성 요소를 설치하는 방법을 설명합니다.

대상

이 정보는 VMware View 를 설치하려는 모든 사용자를 대상으로 합니다. 이 정보는 가상 컴퓨터 기술과 데이터 센터 운영에 익숙하고 경험 많은 Windows 또는 Linux 시스템 관리자를 대상으로 작성되었습니다.

서버 구성 요소의 시스템 요구 사항 1

VMware View 서버 구성 요소를 실행하는 호스트는 특정 하드웨어 및 소프트웨어 요구 사항을 만족해야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

View Connection Server 요구 사항

View Connection Server는 들어오는 사용자 요청을 인증한 다음 적절한 View 데스크톱으로 지시하여 클라이언트 연결의 브로커 역할을 합니다. View Connection Server에는 특정 하드웨어, 운영 체제, 설치 및 지원하는 소프트웨어 요구 사항이 있습니다.

- View 연결 서버의 하드웨어 요구 사항(8 페이지)

  특정 하드웨어 요구 사항을 충족하는 전용 물리적 시스템 또는 가상 컴퓨터에 표준, 복제 및 보안 서버 설치 등 모든 형태의 View 연결 서버 설치본을 설치해야 합니다.

- View 연결 서버 지원 운영 체제(8 페이지)

  Windows Server 2008 R2 운영 체제에 View 연결 서버를 설치해야 합니다.

- View 연결 서버 가상화 소프트웨어 요구 사항(8 페이지)

  View 연결 서버에는 특정 버전의 VMware 가상화 소프트웨어가 필요합니다.

- 복제된 View Connection Server 인스턴스의 네트워크 요구 사항(9 페이지)

  복제된 View Connection Server 인스턴스를 설치할 경우 동일한 위치에서 인스턴스를 구성하고 고성능 LAN을 통해 연결합니다.

View 연결 서버의 하드웨어 요구 사항

특정 하드웨어 요구 사항을 충족하는 전용 물리적 시스템 또는 가상 컴퓨터에 표준, 복제 및 보안 서버 설치 등 모든 형태의 View 연결 서버 설치본을 설치해야 합니다.

표 1-1. View 연결 서버 하드웨어 요구 사항

하드웨어 구성 요소	필수	권장
프로세서	Pentium IV 2.0GHz 프로세서 이상	CPU 4 대
네트워킹	10/100Mbps NIC(네트워크 인터페이스 카드) 1 개 이상	1Gbps NIC
메모리 Windows Server 2008 64 비트	4GB RAM 이상	View 데스크톱 50 대 이상 배포에 필요한 10GB 이상의 RAM

이러한 요구 사항은 고가용성 또는 외부 액세스에 대해 설치하는 복제본 및 보안 서버 View 연결 서버 인스턴스에도 적용됩니다.

중요 View 연결 서버를 호스팅하는 물리적 또는 가상 컴퓨터는 고정 IP 주소를 사용해야 합니다.

View 연결 서버 지원 운영 체제

Windows Server 2008 R2 운영 체제에 View 연결 서버를 설치해야 합니다.

다음 운영 체제는 표준, 복제 및 보안 서버 설치를 포함한 모든 View 연결 서버 설치 유형을 지원합니다.

표 1-2. View 연결 서버의 운영 체제 지원

운영 체제	버전	버전
Windows Server 2008 R2	64 비트	Standard Enterprise
Windows Server 2008 R2 SP1	64 비트	Standard Enterprise

View 연결 서버 가상화 소프트웨어 요구 사항

View 연결 서버에는 특정 버전의 VMware 가상화 소프트웨어가 필요합니다.

- vSphere 를 사용할 경우, 다음 지원되는 버전 중 하나를 사용해야 합니다.
  - vSphere 4.0 Update 4 이상
  - vSphere 4.1 Update 2 이상
  - vSphere 5.0 Update 1 이상
- ESX 및 ESXi 호스트 모두 지원됩니다.

각 vCenter Server 및 ESX/ESXi 버전과 호환되는 VMware View 버전에 대한 자세한 내용은 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 에서 VMware 제품 상호 호환성 표를 참조하십시오.

복제된 View Connection Server 인스턴스의 네트워크 요구 사항

복제된 View Connection Server 인스턴스를 설치할 경우 동일한 위치에서 인스턴스를 구성하고 고성능 LAN 을 통해 연결합니다.

WAN 을 사용하여 복제된 View Connection Server 인스턴스를 연결하지 마십시오.

평균 지연 시간이 낮고 처리량이 높은 고성능 WAN 이지만 View Connection Server 인스턴스가 일관성을 유지하는 데 필요한 성능 특징을 네트워크로 전달할 수 없는 기간이 있습니다.

View Connection Server 인스턴스의 View LDAP 구성이 일관성이 없는 경우 사용자는 데스크톱에 액세스할 수 없습니다. 구성이 오래된 View Connection Server 인스턴스에 연결할 때 사용자의 액세스가 거부될 수 있습니다.

View Administrator 요구 사항

관리자는 View Administrator 를 사용하여 View 연결 서버를 구성하고 데스크톱을 배포 및 관리하며 사용자 인증을 제어하고 시스템 이벤트를 초기화 및 검토하고 분석 작업을 수행합니다. View Administrator 를 실행하는 클라이언트 시스템은 특정 요구 사항을 만족해야 합니다.

View Administrator 는 View 연결 서버를 설치할 때 설치된 웹 기반 애플리케이션입니다. View Administrator 에 액세스하여 다음 웹 브라우저와 함께 사용할 수 있습니다.

- Internet Explorer 8
- Internet Explorer 9
- Firefox 6
- Firefox 7

웹 브라우저에서 View Administrator 를 사용할 경우, Adobe Flash Player 10 이상을 설치해야 합니다. 클라이언트 시스템은 Adobe Flash Player 가 설치될 수 있도록 인터넷에 액세스할 수 있어야 합니다.

View Administrator 를 실행하는 컴퓨터는 View 연결 서버를 호스팅하는 서버의 루트 및 중간 인증서를 신뢰해야 합니다. 지원되는 브라우저에는 이미 잘 알려진 모든 인증 기관(CA)의 인증서가 포함되어 있습니다. 잘 알려지지 않은 CA 의 인증서를 사용하는 경우, *VMware View 설치* 문서에서 루트 및 중간 인증서 가져오기에 관한 지침을 따르십시오.

텍스트를 올바르게 표시하려면 View Administrator 에 Microsoft 특정 글꼴이 필요합니다. 웹 브라우저가 Linux, UNIX 또는 Mac OS 와 같은 비 Windows 운영 체제에서 실행될 경우 Microsoft 특정 글꼴이 컴퓨터에 설치되어 있어야 합니다.

현재 Microsoft 웹 사이트에서는 Microsoft 글꼴을 배포하지 않지만 독립 웹 사이트에서 다운로드할 수 있습니다.

View Composer 요구 사항

View Manager 는 View Composer 를 사용하여 단일 집중 베이스 이미지에서 여러 연결된 클론 데스크톱을 배포합니다. View Composer 에는 특정 설치 및 스토리지 요구 사항이 있습니다.

- View Composer 지원 운영 체제(10 페이지)

  View Composer 는 특정 요구 사항 및 제한 사항이 있는 64 비트 운영 체제를 지원합니다. View Composer 를 vCenter Server 와 동일한 물리적 또는 가상 컴퓨터에 설치하거나 별도 서버에 설치할 수 있습니다.

- 독립 실행형 View Composer 의 하드웨어 요구 사항(10 페이지)

  View 5.1 이상 릴리스에서는 View Composer 를 더 이상 vCenter Server 와 동일한 물리적 또는 가상 컴퓨터에 설치할 필요가 없습니다. View Composer 를 별도 서버에 설치하는 경우, 특정 하드웨어 요구 사항을 충족하는 전용 물리적 또는 가상 컴퓨터를 사용해야 합니다.

- View Composer 데이터베이스 요구 사항(11 페이지)

  데이터를 저장하려면 View Composer 에 SQL 데이터베이스가 필요합니다. View Composer 데이터베이스는 View Composer 서버 호스트에 있거나 View Composer 서버 호스트에서 사용할 수 있어야 합니다.

View Composer 지원 운영 체제

View Composer 는 특정 요구 사항 및 제한 사항이 있는 64 비트 운영 체제를 지원합니다. View Composer 를 vCenter Server 와 동일한 물리적 또는 가상 컴퓨터에 설치하거나 별도 서버에 설치할 수 있습니다.

표 1-3. View Composer 의 운영 체제 지원

운영 체제	버전	버전
Windows Server 2008 R2	64 비트	Standard Enterprise
Windows Server 2008 R2 SP1	64 비트	Standard Enterprise

vCenter Server 가 아닌 다른 물리적 시스템 또는 가상 컴퓨터에 View Composer 를 설치하려는 경우 "독립 실행형 View Composer 의 하드웨어 요구 사항," (10 페이지)을 참조하십시오.

독립 실행형 View Composer 의 하드웨어 요구 사항

View 5.1 이상 릴리스에서는 View Composer 를 더 이상 vCenter Server 와 동일한 물리적 또는 가상 컴퓨터에 설치할 필요가 없습니다. View Composer 를 별도 서버에 설치하는 경우, 특정 하드웨어 요구 사항을 충족하는 전용 물리적 또는 가상 컴퓨터를 사용해야 합니다.

독립 실행형 View Composer 는 Windows Server 컴퓨터에 설치된 vCenter Server 및 Linux 기반 vCenter Server 어플라이언스에 설치하여 사용할 수 있습니다. 각 View Composer 서비스와 vCenter Server 인스턴스 사이에 일대일 매핑이 존재해야 하는 것이 좋습니다.

표 1-4. View Composer 하드웨어 요구 사항

하드웨어 구성 요소	필수	권장
프로세서	1.4 GHz 64 비트 프로세서 이상 및 2 CPU Itanium 기반 시스템을 위한 Intel Itanium 2 프로세서	2GHz 이상 및 4 CPU
네트워킹	10/100Mbps NIC(네트워크 인터페이스 카드) 1 개 이상	1Gbps NIC
메모리	4GB RAM 이상	50 대 이상의 View 데스크톱 배포에 필요한 8GB 이상 RAM
디스크 공간	40GB	60GB

중요 View Composer 를 호스팅하는 물리적 또는 가상 컴퓨터는 고정 IP 주소를 사용해야 합니다.

View Composer 데이터베이스 요구 사항

데이터를 저장하려면 View Composer에 SQL 데이터베이스가 필요합니다. View Composer 데이터베이스는 View Composer 서버 호스트에 있거나 View Composer 서버 호스트에서 사용할 수 있어야 합니다.

vCenter Server의 데이터베이스 서버가 있고 표 1-5에 있는 버전일 경우 View Composer는 해당 데이터베이스 서버를 사용할 수 있습니다. 예를 들어 View Composer는 vCenter Server와 함께 제공된 Microsoft SQL Server 2005 또는 2008 Express 인스턴스를 사용할 수 있습니다. 데이터베이스 서버가 없으면 설치해야 합니다.

View Composer는 vCenter Server에서 지원하는 데이터베이스 서버의 하위 집합을 지원합니다. View Composer에서 지원하지 않는 데이터베이스 서버로 vCenter Server를 이용하고 있는 경우 vCenter Server용으로 해당 데이터베이스 서버를 계속 사용하고 View Composer 및 View Manager 데이터베이스 이벤트용으로 별도의 데이터베이스 서버를 설치합니다.

중요 vCenter Server와 동일한 SQL Server 인스턴스에 View Composer 데이터베이스를 생성하는 경우, vCenter Server 데이터베이스를 덮어쓰지 마십시오.

표 1-5에 지원되는 데이터베이스 서버 및 버전 목록이 나와 있습니다. vCenter Server로 지원되는 전체 데이터베이스 버전 목록은 VMware vSphere 설명서 웹 사이트의 *VMware vSphere Compatibility Matrixes*(VMware vSphere 호환성 표)를 참조하십시오.

표 1-5. View Composer에서 지원하는 데이터베이스 서버

데이터베이스	vCenter Server 5.0 U1 이상	vCenter Server 4.1 U2 이상	vCenter Server 4.0 U4 이상
Microsoft SQL Server 2005(SP4), Standard, Enterprise 및 Datacenter (32 비트 및 64 비트)	예	예	예
Microsoft SQL Server 2008 Express(R2) (64 비트)	예	아니요	아니요
Microsoft SQL Server 2008(SP2), Standard, Enterprise 및 Datacenter (32 비트 및 64 비트)	예	예	예
Microsoft SQL Server 2008(R2), Standard 및 Enterprise (32 비트 및 64 비트)	예	예	예
Oracle 10g 릴리스 2, Standard, Standard ONE 및 Enterprise[10.2.0.4] (32 비트 및 64 비트)	예	예	예
Oracle 11g 릴리스 2, Standard, Standard ONE 및 Enterprise[11.2.0.1] , 패치 5 포함 (32 비트 및 64 비트)	예	예	예

참고 Oracle 11g R2 데이터베이스를 사용할 경우, Oracle 11.2.0.1 패치 5를 설치해야 합니다. 이 패치 요구 사항은 32 비트 및 64 비트 버전 모두에 적용됩니다.

View Transfer Server 요구 사항

View Transfer Server 는 로컬 모드에서 실행되는 데스크톱의 체크인, 체크아웃 및 복제를 지원하는 View Manager 의 선택적인 구성 요소입니다. View Transfer Server 에는 특정 설치, 운영 체제 및 스토리지 요구 사항이 있습니다.

- View 전송 서버 설치 및 업그레이드 요구 사항(12 페이지)

  특정 요구 사항을 만족하는 가상 컴퓨터에 Windows 애플리케이션으로 View 전송 서버를 설치해야 합니다.

- View 전송 서버 지원 운영 체제(12 페이지)

  최소 필요한 양의 RAM 이 있는 지원된 운영 체제에 View 전송 서버를 설치해야 합니다.

- View Transfer Server 의 스토리지 요구 사항(13 페이지)

  View Transfer Server 는 데이터 센터의 로컬 데스크톱 및 원격 데스크톱 사이에서 정적 컨텐츠를 Transfer Server 저장소 및 동적 컨텐츠로 또는 Transfer Server 저장소 및 동적 컨텐츠에서 전송합니다. View Transfer Server 에는 특정 스토리지 요구 사항이 있습니다.

View 전송 서버 설치 및 업그레이드 요구 사항

특정 요구 사항을 만족하는 가상 컴퓨터에 Windows 애플리케이션으로 View 전송 서버를 설치해야 합니다.

View 전송 서버를 호스팅하는 가상 컴퓨터는 네트워크 연결성에 관하여 여러 요구 사항을 만족해야 합니다.

- 관리할 로컬 데스크톱과 동일한 vCenter Server 인스턴스에서 관리해야 합니다.
- 도메인의 일부일 필요는 없습니다.
- 정적 IP 주소를 사용해야 합니다.

View 전송 서버 소프트웨어는 View 연결 서버를 포함하는 다른 View Manager 소프트웨어 구성 요소와 함께 동일한 가상 컴퓨터에 공존할 수 없습니다.

View 전송 서버를 호스팅하는 가상 컴퓨터에서 PCI 장치를 수동으로 추가하거나 제거하지 마십시오. PCI 장치를 추가하거나 제거하는 경우, View 가 Hot-add 기능으로 추가된 장치를 발견하지 못하여 데이터 전송 작업이 수행되지 않을 수 있습니다.

고가용성 및 확장성을 위해 여러 View 전송 서버 인스턴스를 설치할 수 있습니다.

View 전송 서버 지원 운영 체제

최소 필요한 양의 RAM 이 있는 지원된 운영 체제에 View 전송 서버를 설치해야 합니다.

표 1-6. View 전송 서버의 운영 체제 지원

운영 체제	버전	버전	최소 RAM
Windows Server 2008 R2	64 비트	Standard Enterprise	4GB
Windows Server 2008 R2 SP1	64 비트	Standard Enterprise	4GB

중요 View 전송 서버를 호스팅하는 가상 시스템의 두 개의 가상 CPU 를 구성하십시오.

View Transfer Server 의 스토리지 요구 사항

View Transfer Server 는 데이터 센터의 로컬 데스크톱 및 원격 데스크톱 사이에서 정적 컨텐츠를 Transfer Server 저장소 및 동적 컨텐츠로 또는 Transfer Server 저장소 및 동적 컨텐츠에서 전송합니다. View Transfer Server 에는 특정 스토리지 요구 사항이 있습니다.

- Transfer Server 저장소를 구성할 디스크 드라이브에는 정적 이미지 파일을 저장할 공간이 충분해야 합니다. 이미지 파일은 View Composer 기본 이미지입니다.
- View Transfer Server 는 전송될 데스크톱 디스크를 저장하는 데이터스토어에 액세스할 수 있어야 합니다. 데이터스토어는 View Transfer Server 가상 시스템이 실행 중인 ESX/ESXi 호스트에서 액세스할 수 있어야 합니다.
- View Transfer Server 에서 지원할 수 있는 동시 디스크 전송의 최대 권장 수는 20 입니다.

  전송 작업 중 로컬 데스크톱의 가상 디스크는 View Transfer Server 에 마운트됩니다. View Transfer Server 가상 시스템에는 네 개의 SCSI 컨트롤러가 있습니다. 이 구성으로 많은 디스크가 가상 시스템에 한번에 연결될 수 있습니다.
- 로컬 데스크톱에 민감한 사용자 데이터가 포함될 수 있기 때문에 네트워크를 통한 전송 중에 데이터를 암호화해야 합니다.

  View Administrator 에서 각 View Connection Server 인스턴스의 데이터 전송 보안 옵션을 구성할 수 있습니다. View Administrator 에서 이러한 옵션을 구성하려면 **View 구성 > 서버**를 클릭하고 View Connection Server 인스턴스를 선택한 다음 **편집**을 클릭합니다.
- View Transfer Server 가 View Manager 에 추가된 경우 DRS(Distributed Resource Scheduler) 자동화 정책이 수동으로 설정됩니다(DRS 를 효과적으로 해제함).

  View Transfer Server 인스턴스를 다른 ESX 호스트 또는 데이터스토어로 마이그레이션하려면 마이그레이션을 시작하기 전에 인스턴스를 유지 관리 모드로 지정해야 합니다.

  View Transfer Server 가 View Manager 에서 제거되면 DRS 자동화 정책이 View Transfer Server 가 View Manager 에 추가되기 전의 값으로 재설정됩니다.

클라이언트 구성 요소의 시스템 요구 사항 2

View 클라이언트 구성 요소를 실행 중인 시스템은 특정 하드웨어 및 소프트웨어 요구 사항을 만족해야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

View Agent 지원 운영 체제

View Agent 구성 요소는 세션 관리, 단일 로그온 및 장치 리디렉션을 지원합니다. View Manager 에서 관리할 모든 가상 컴퓨터, 물리적 시스템 및 터미널 서버에 View Agent 를 설치해야 합니다.

표 2-1. View Agent 운영 체제 지원

게스트 운영 체제	버전	버전	서비스 팩
Windows 7	64 비트 및 32 비트	Enterprise 및 Professional	없음 및 SP1
Windows Vista	32 비트	Business 및 Enterprise	SP1 및 SP2
Windows XP	32 비트	Professional	SP3
Windows 2008 R2 Terminal Server	64 비트	Standard	SP1
Windows 2008 Terminal Server	64 비트	Standard	SP2

View Agent 를 포함한 View 개인 설정 관리 설치 옵션을 사용하려면 View Agent 를 Windows 7, Windows Vista 또는 Windows XP 가상 컴퓨터에 설치해야 합니다. 이 옵션은 물리적 컴퓨터 또는 Microsoft 터미널 서버에서 작동하지 않습니다.

View 개인 설정 관리 독립 실행형 버전을 물리적 컴퓨터에 설치할 수 있습니다. "독립 실행형 View 개인 설정 관리의 지원 운영 체제," (16 페이지)의 내용을 참조하십시오.

중요 가상 컴퓨터에서 Windows 7 을 사용할 경우, 호스트는 ESX/ESXi 4.0 Update 4 이상, ESX/ESXi 4.1 Update 2 이상 또는 ESXi 5.0 Update 1 이상이어야 합니다.

독립 실행형 View 개인 설정 관리의 지원 운영 체제

독립 실행형 View 개인 설정 관리 소프트웨어는 View Agent 5.*x*가 설치되지 않은 독립 실행형 물리적 컴퓨터와 가상 시스템에서 개인 관리를 제공합니다. 사용자가 로그인하면 원격 프로파일 저장소에서 독립 실행형 시스템으로 프로파일이 동적으로 다운로드됩니다.

참고 View 데스크톱에 대해 View 개인 설정 관리를 구성하려면 **View 개인 설정 관리** 설정 옵션을 포함시켜 View Agent 를 설치합니다. 독립 실행형 View 개인 설정 관리 소프트웨어는 View 이외 시스템 전용입니다.

표 2-2 에는 독립 실행형 View 개인 설정 관리 소프트웨어에 지원되는 운영 체제가 나와 있습니다.

표 2-2. 독립 실행형 View 개인 설정 관리의 운영 체제 지원

게스트 운영 체제	버전	버전	서비스 팩
Windows 7	64 비트 및 32 비트	Enterprise 및 Professional	없음 및 SP1
Windows Vista	32 비트	Business 및 Enterprise	SP1 및 SP2
Windows XP	32 비트	Professional	SP3

독립 실행형 View 개인 설정 관리 소프트웨어는 Microsoft 터미널 서비스 또는 Microsoft 원격 데스크톱 서비스에서 지원되지 않습니다.

Windows 기반 View Client 및 View Client with Local Mode 지원 운영 체제

사용자는 View Client 를 사용하여 가상 데스크톱에 연결합니다. 지원된 운영 체제에 View Client 또는 View Client with Local Mode 를 설치해야 합니다.

표 2-3 에는 View Client 에서 지원하는 Microsoft Windows 운영 체제가 나열되어 있습니다. Mac 용 View Client 및 iPad 용 View Client 와 같은 기타 View Client 에서 지원하는 운영 체제에 대한 자세한 내용은 해당 클라이언트에 관련된 문서를 참조하십시오.
https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html 로 이동합니다.

표 2-3. Windows 기반 클라이언트의 View Client 운영 체제 지원

운영 체제	버전	버전	서비스 팩
Windows 7	32 비트 및 64 비트	Home, Enterprise, Professional 및 Ultimate	없음 및 SP1
Windows XP	32 비트	Home 및 Professional	SP3
Windows Vista	32 비트	Home, Business, Enterprise 및 Ultimate	SP2

중요 View Client with Local Mode 는 Windows 시스템 및 물리적 컴퓨터에서만 지원됩니다. 또한 이 기능을 사용하려면 VMware 라이센스에 View Client with Local Mode 가 포함되어 있어야 합니다.

View Client with Local Mode 는 이전 릴리스에서 View Client with Offline Desktop 이라는 시범적 기능이었던 전체 지원된 기능입니다.

참고 VMware 파트너에서 VMware View 배포용 씬 클라이언트 디바이스를 제공합니다. 공급업체와 모델, 기업이 사용하기로 결정한 구성에 따라 각 씬 클라이언트 디바이스에서 사용할 수 있는 기능 및 Linux 운영 체제가 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.

Local Mode 데스크톱 하드웨어 요구 사항

View 데스크톱을 체크아웃해 로컬 컴퓨터에서 실행하는 경우 클라이언트 컴퓨터의 하드웨어에서 로컬 시스템과 이를 실행하는 가상 컴퓨터를 모두 지원해야 합니다.

PC 하드웨어

표 2-4 에서는 다양한 View 데스크톱 운영 체제의 하드웨어 요구 사항을 설명합니다.

표 2-4. 프로세서 요구 사항

클라이언트 컴퓨터 요구 사항	설명
PC	x86 64-호환 롱 모드에서 LAHF/SAHF 지원
CPU 수	다중 프로세서 시스템을 지원합니다.
CPU 속도	Windows XP 로컬 데스크톱은 1.3GHz 이상, 1.6GHz 를 권장합니다. Windows 7 데스크톱은 1.3GHz 이상(Aero 사용 시 2.0GHz 이상)을 권장합니다.
Intel 프로세서	Pentium 4, Pentium M(PAE 사용), Core, Core 2, Core i3, Core i5 및 Core i7 프로세서 Windows 7 Aero 사용 시: Intel Dual Core
AMD 프로세서	Athlon, Athlon MP, Athlon XP, Athlon 64, Athlon X2, Duron, Opteron, Turion X2, Turion 64, Sempron, Phenom, Phenom II AMD CPU 는 롱 모드에서 세그먼트 제한을 지원해야 합니다. Windows 7 Aero 사용 시: Athlon 4200+ 이상

표 2-4. 프로세서 요구 사항 (계속)

클라이언트 컴퓨터 요구 사항	설명
View 데스크톱에서 64 비트 운영 체제	EM64T 및 Intel 가상화 기술을 사용하는 Intel Pentium 4 및 Core 2 및 Core i7 프로세서 Intel CPU 는 호스트 시스템 BIOS 에서 VT-x 를 지원하도록 설정해야 합니다. VT-x 를 지원하도록 설정해야 하는 BIOS 설정은 시스템 공급업체에 따라 다릅니다. VT-x 지원이 사용되었는지 확인하는 방법에 대해서는 VMware 기술 자료 문서 http://kb.vmware.com/kb/1003944 를 참조하십시오. 대부분의 AMD64 프로세서(최초의 C Opteron 프로세서 버전 제외)
Windows 7 Aero 용 GPU	nVidia GeForce 8800GT 이상 ATI Radeon HD 2600 이상

클라이언트 컴퓨터의 운영 체제가 32 비트 또는 64 비트일 수 있지만 하드웨어는 64 비트 호환이어야 하며 64 비트 운영 체제에서 View 데스크톱을 실행할 수 있도록 Intel 또는 AMD 가상화 지원 기술이 사용되도록 설정해야 합니다. 이러한 요구 사항이 충족되면 32 비트 또는 64 비트 운영 체제인 클라이언트에서 64 비트 운영 체제의 View 데스크톱을 실행할 수 있습니다.

디스크 공간

View 데스크톱에서 운영 체제 기본 설정을 사용한 경우 물리적 컴퓨터에 운영 체제와 애플리케이션을 설치하고 실행하는 데 필요한 것과 동일한 실제 디스크 공간이 필요합니다.

예를 들어 Microsoft 는 32 비트 Windows 7 운영 체제를 실행하는 시스템의 16GB 의 하드 디스크 공간을 권장합니다. 32 비트 Windows 7 운영 체제에 대해 16GB 의 가상 하드 디스크를 구성하면 로컬 데스크톱을 체크아웃할 때 실제로 사용되는 디스크 공간만 다운로드됩니다. 16GB 가 할당된 데스크톱의 경우 실제 다운로드 크기는 7GB 일 수 있습니다.

데스크톱을 다운로드한 후 16GB 하드 디스크를 구성한 경우 디스크 공간 사용량이 16GB 로 늘어날 수 있습니다. 복제 작업 동안 스냅샷이 생성되기 때문에 동일한 디스크 공간이 추가로 필요합니다. 예를 들어 로컬 데스크톱에서 7GB 의 디스크 공간을 사용하고 있는 경우, 스냅샷이 클라이언트 컴퓨터에서 7GB 를 추가로 사용합니다.

IDE 및 SCSI 하드 드라이브를 지원합니다.

메모리

클라이언트 컴퓨터에서 호스트 운영 체제를 실행하는 경우에는 충분한 메모리가 필요하며, 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. 메모리 요구 사항에 대한 자세한 내용은 게스트 운영 체제와 응용 프로그램 설명서를 참조하십시오.

단일 컴퓨터에서 실행하는 모든 가상 컴퓨터에 할당할 수 있는 전체 메모리 양은 해당 컴퓨터의 RAM 양에 의해서만 제한됩니다. 64 비트 컴퓨터에서 각 View 데스크톱의 최대 메모리는 32GB 입니다.

디스플레이

32 비트 디스플레이 어댑터를 권장합니다. 일부 그래픽 하드웨어에서 Windows Vista 또는 Windows 7 가상 컴퓨터를 실행할 때 3DMark '06 과 같은 3D 벤치마크가 바르게 렌더링되지 않거나 전혀 렌더링되지 않을 수 있습니다.

View Client with Local Mode 는 가용 GPU 가 있는 클라이언트 시스템에서 자동으로 활성화되는 DirecX9c 를 지원합니다. DirecX9c 에는 빌딩 3D 이미지 보기(3D Buildings)가 포함된 Google Earth, Windows 7 Aero 효과, 몇 가지 3D 게임 등의 3D 기능을 지원합니다.

720p 이상의 비디오를 재생하려면 다중 프로세서 시스템이 필요합니다.

Windows 7 Aero 를 지원하는 CPU 및 GPU 요구 사항은 표 2-4 을 참조하십시오.

View Portal 클라이언트 브라우저 요구 사항

클라이언트 시스템에서 브라우저를 열고 View 연결 서버 인스턴스로 이동할 수 있습니다. 나타나는 웹 페이지는 View Portal 이라고 하며 여기에는 View Client 용 설치 관리자 파일을 다운로드하기 위한 링크가 포함되어 있습니다.

다음 웹 브라우저에서만 View Portal 을 사용할 수 있습니다.

- Internet Explorer 8
- Internet Explorer 9
- Firefox 6
- Firefox 7
- Safari 5(Mac)

원격 디스플레이 프로토콜 및 소프트웨어 지원

원격 디스플레이 프로토콜 및 소프트웨어를 사용하여 네트워크 연결된 원격 컴퓨터의 데스크톱에 연결합니다. View Client 는 Microsoft 원격 데스크톱 프로토콜(RDP) 및 VMware 의 PCoIP 를 지원합니다.

- PCoIP 포함 VMware View(19 페이지)

  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.

- Microsoft RDP(21 페이지)

  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.

- MMR(멀티미디어 리디렉션) 사용을 위한 요구 사항(22 페이지)

  MMR(멀티미디어 리디렉션)은 가상 채널을 사용하여 클라이언트 컴퓨터에 멀티미디어 스트림을 직접 전달합니다.

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.
- “View Agent 지원 운영 체제,” (15 페이지)지원됩니다.

- 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.

MMR(멀티미디어 리디렉션) 사용을 위한 요구 사항

MMR(멀티미디어 리디렉션)은 가상 채널을 사용하여 클라이언트 컴퓨터에 멀티미디어 스트림을 직접 전달합니다.

MMR 을 사용하면 멀티미디어 스트림이 처리됩니다. 즉, 클라이언트 시스템에서 인코딩 및 디코딩됩니다. 로컬 하드웨어는 미디어 컨텐츠를 형식 지정하고 재생하여 ESX/ESXi 호스트에 대한 요청 부담을 덜어줍니다.

View Client 및 View Client with Local Mode 는 다음 운영 체제에서 MMR 을 지원합니다.

- Windows XP
- Windows XP Embedded
- Windows Vista

로컬 디코더가 클라이언트에 존재해야 하기 때문에 MMR 기능은 클라이언트 시스템이 지원하는 미디어 파일 형식을 지원합니다. 이러한 파일 형식에는 MPEG2-1, MPEG-2, MPEG-4 Part 2, WMV 7, 8 및 9, WMA, AVI, ACE, MP3 및 WAV 등이 포함됩니다.

Windows Media Player 10 이상을 사용하고 이를 로컬 컴퓨터 또는 클라이언트 액세스 디바이스 및 View 데스크톱 모두에 설치합니다.

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

참고 View Client 비디오 디스플레이 하드웨어에는 MMR 가 올바르게 작동할 수 있도록 오버레이 지원이 있어야 합니다.

Windows 7 클라이언트 및 Windows 7 View 데스크톱에서는 MMR 을 지원하지 않습니다. Windows 7 클라이언트 에이전트의 경우, RDP 7 이 포함된 Windows 미디어 리디렉션을 사용합니다.

Adobe Flash 요구 사항

View 데스크톱 세션에서 실행하는 Adobe Flash 컨텐츠 대역폭 양을 줄일 수 있습니다. 이를 통해 전반적인 검색 경험을 비롯해 데스크톱에서 실행하는 다른 애플리케이션의 응답 속도를 향상할 수 있습니다.

Adobe Flash 대역폭 절감은 Microsoft Windows 의 Internet Explorer 세션과 Adobe Flash 버전 9 및 10 에서만 가능합니다. Adobe Flash 대역폭 절감 설정을 사용하려면 Adobe Flash 를 전체 화면 모드로 실행해서는 안 됩니다.

스마트 카드 인증 요구 사항

사용자 인증에 스마트 카드를 사용하는 클라이언트 시스템은 특정 요구 사항을 만족해야 합니다.

사용자 인증에 스마트 카드를 사용하는 각 클라이언트 시스템에는 다음 소프트웨어 및 하드웨어가 있어야 합니다.

- View Client
- Windows 호환 스마트 카드 판독기
- 스마트 카드 미들웨어
- 제품 특정 애플리케이션 드라이버

또한 View 데스크톱에 제품 특정 애플리케이션 드라이버를 설치해야 합니다.

View 는 PKCS#11 또는 Microsoft CryptoAPI 공급자를 사용하는 스마트 카드 및 스마트 카드 판독기를 지원합니다. 스마트 카드와 상호 작용하기 위한 도구를 제공하는 ActivIdentity ActivClient 소프트웨어 제품군을 선택적으로 설치할 수 있습니다.

스마트 카드를 사용하여 인증하는 사용자는 스마트 카드 또는 USB 스마트 카드 토큰이 있어야 하며 각 스마트 카드에는 사용자 인증서가 포함되어 있어야 합니다.

스마트 카드에 인증서를 설치하려면 등록 스테이션 역할을 하도록 컴퓨터를 설정해야 합니다. 이 컴퓨터에는 사용자에게 스마트 카드 인증서를 발행할 기관이 있어야 하며 이는 인증서를 발행 중인 도메인의 구성원이어야 합니다.

중요 스마트 카드를 등록할 때 결과 인증서의 키 크기를 선택할 수 있습니다. 로컬 데스크톱에서 스마트 카드를 사용하려면 스마트 카드 등록 중에 1024 비트 또는 2048 비트 키 크기를 선택해야 합니다. 512 비트 키를 가진 인증서는 지원되지 않습니다.

Microsoft TechNet 웹 사이트에는 Windows 시스템의 스마트 카드 인증 계획 및 구현에 대한 자세한 정보가 포함되어 있습니다.

View 를 사용하여 스마트 카드 인증을 구현할 때 Active Directory 에서 수행해야 하는 작업에 대한 자세한 내용은 "스마트 카드 인증을 위한 Active Directory 준비," (28 페이지)에 나와 있습니다.

일부 View Client 는 스마트 카드 인증을 지원하지 않습니다. 특정 View Client 유형에서 스마트 카드를 지원하는지 여부를 확인하려면 해당 클라이언트 유형의 *View Client 사용* 문서에 있는 기능 지원 표를 참조하십시오. https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html 로 이동합니다.

3 Active Directory 준비

View 에서는 사용자 인증 및 관리를 위해 기존 Microsoft Active Directory 인프라를 사용합니다. 특정 작업을 수행하여 View 와 함께 사용할 Active Directory 를 준비해야 합니다.

View 는 다음 버전의 Active Directory 를 지원합니다.

- Windows 2003 Active Directory
- Windows 2008 Active Directory

이 장에서는 다음 주제에 대해 설명합니다.

도메인 및 신뢰 관계 구성

Active Directory 도메인에 각 View Connection Server 호스트를 가입시켜야 합니다. 호스트를 도메인 컨트롤러로 사용하면 안 됩니다. View Connection Server 호스트와 같은 도메인 또는 View Connection Server 호스트의 도메인과 양방향 신뢰 관계를 가진 도메인에 View 데스크톱을 배치합니다.

View Connection 호스트 도메인의 사용자 및 그룹에 View 데스크톱 및 풀에 대한 권한을 부여할 수 있습니다. View Connection Server 호스트의 도메인에서 사용자 및 그룹을 선택해 View Administrator 의 관리자 권한을 부여할 수 있습니다. 다른 도메인의 사용자 및 그룹을 선택 또는 권한을 부여하려면 해당 도메인과 View Connection Server 호스트의 도메인 간에 양방향 신뢰 관계를 구축해야 합니다.

사용자는 View Connection Server 호스트의 도메인용 Active Directory 및 신탁 계약이 존재하는 모든 추가 사용자 도메인에 대해 인증 받습니다.

참고 보안 서버는 Active Directory 를 포함한 어떤 인증 저장소에도 액세스하지 않으므로 Active Directory 도메인에 있지 않아도 됩니다.

신뢰 관계 및 도메인 필터링

액세스할 수 있는 도메인을 결정하기 위해 View Connection Server 인스턴스는 도메인부터 시작하여 신뢰 관계를 탐색합니다.

규모가 작고 연결된 도메인 집합의 경우 View Connection Server는 신속하게 도메인 전체 목록을 확인할 수 있지만 도메인 수가 증가하거나 도메인 간의 연결 수가 감소하면 작업 시간이 늘어납니다. 목록에는 사용자가 View 데스크톱에 로그인할 때 사용자에게 제공하기 원하지 않는 도메인이 포함될 수 있습니다.

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

View 데스크톱의 OU 생성

View 데스크톱의 조직 단위(OU)를 생성해야 합니다. OU는 사용자, 그룹, 컴퓨터 또는 OU를 포함하고 있는 Active Directory의 하위 분류 단위입니다.

데스크톱과 동일한 도메인에 있는 다른 Windows 서버 또는 워크스테이션에 그룹 정책 설정을 적용하지 않으려면 View 그룹 정책의 GPO를 생성하고 View 데스크톱을 포함하고 있는 OU에 연결하면 됩니다. 서버 운영자 또는 개인 사용자 등과 같은 종속 그룹에 OU 제어 권한을 위임할 수 있습니다.

View Composer를 사용하면 View 데스크톱의 OU를 기반으로 하는 연결된 클론 데스크톱의 개별 Active Directory 컨테이너를 생성해야 합니다. Active Directory에서 OU 관리자 권한을 가지고 있는 View 관리자는 도메인 관리자 권한 없이 연결된 클론 데스크톱을 프로비저닝할 수 있습니다. Active Directory의 관리자 자격 증명을 변경하면 View Composer의 자격 증명 정보도 업데이트해야 합니다.

키오스크 모드 클라이언트 계정을 위한 OU 및 그룹 생성

키오스크 모드의 클라이언트는 잠금 PC 또는 씬 클라이언트로 View Client를 실행해 View Connection Server 인스턴스에 연결하고 원격 데스크톱 세션을 시작합니다. 키오스크 모드에서 클라이언트를 구성하면 키오스크 모드 클라이언트 계정을 위해 Active Directory에서 전용 OU 및 그룹을 생성해야 합니다.

키오스크 모드 클라이언트 계정의 전용 OU 및 그룹을 생성하면 허가 받지 않은 침입으로부터 클라이언트 시스템을 보호하고, 클라이언트 구성과 관리를 간소화할 수 있습니다.

자세한 내용은 *VMware View 관리* 설명서를 참조하십시오.

View 사용자 그룹 생성

Active Directory의 다른 View 사용자 유형에 대해 그룹을 생성해야 합니다. 예를 들어 View 데스크톱 사용자에 대해 VMware View 사용자, View 데스크톱을 관리할 사용자에 대해 VMware View 관리자 그룹을 생성할 수 있습니다.

vCenter Server의 사용자 계정 생성

vCenter Server에서 사용하기 위해 Active Directory에 사용자 계정을 생성해야 합니다. View Administrator에서 vCenter Server 인스턴스를 추가할 때 이 사용자 계정을 지정합니다.

사용자 계정은 View Connection Server 호스트와 같은 도메인 또는 신뢰할 수 있는 도메인에 있어야 합니다. View Composer를 사용하면 vCenter Server 컴퓨터의 로컬 관리자 그룹에 사용자 계정을 추가해야 합니다.

vCenter Server에서 특정 작업을 수행할 수 있도록 사용자 계정 권한을 부여해야 합니다. View Composer를 사용하면 사용자 계정에 추가 권한을 부여해야 합니다. 이러한 권한 구성에 대한 자세한 내용은 "vCenter Server 및 View Composer의 사용자 계정 구성," (85 페이지)에 나와 있습니다.

View Composer 에 대한 사용자 계정 생성

View Composer 를 사용하는 경우에는 View Composer 에서 사용할 사용자 계정을 Active Directory 에서 생성해야 합니다. 연결된 클론 데스크톱을 Active Directory 도메인에 연결하려면 View Composer 에서 이 계정을 사용해야 합니다.

보안 상의 이유로 View Composer 에서 사용할 사용자 계정을 별도로 생성해야 합니다. 별도 계정을 생성해 다른 용도로 정의된 추가 권한을 가지고 있지 않도록 보장할 수 있습니다. 특정 Active Directory 컨테이너에서 컴퓨터 개체를 생성 또는 제거하는데 필요한 최소 권한을 계정에 부여할 수 있습니다. 예를 들어 View Composer 계정에는 도메인 관리자 권한이 필요하지 않습니다.

프로시저

1 Active Director 에서 View Connection Server 호스트와 동일한 도메인 또는 신뢰할 수 있는 도메인에서 사용자 계정을 생성하십시오.

2 연결된 클론 컴퓨터 계정을 생성하거나 연결된 클론 컴퓨터 계정을 이동한 Active Directory 컨테이너에 **컴퓨터 개체 생성**, **컴퓨터 개체 삭제** 및 **모든 속성 쓰기** 사용 권한을 추가하십시오.

   다음 목록은 기본으로 할당된 사용 권한을 포함해 사용자 계정에 필요한 모든 사용 권한을 보여줍니다.

   - 목록 내용
   - 모든 속성 읽기
   - 모든 속성 쓰기
   - 사용 권한 읽기
   - 컴퓨터 개체 생성
   - 컴퓨터 개체 삭제

3 Active Directory 컨테이너 및 컨테이너의 모든 하위 개체에 사용자 계정의 사용 권한을 적용했는지 확인하십시오.

후속 작업

vCenter Server 에 대한 View Composer 를 구성하고 연결된 클론 데스크톱 풀을 배포할 때 View Administrator 에서 계정을 지정하십시오.

제한된 그룹 정책 구성

View 데스크톱의 로컬 원격 데스크톱 사용자 그룹에 속해 있는 사용자만 View 데스크톱에 로그인할 수 있습니다. 도메인에 가입되어 있는 모든 View 데스크톱의 로컬 원격 데스크톱 사용자 그룹에 Active Directory 의 제한된 그룹 정책을 사용해 사용자 또는 그룹을 추가할 수 있습니다.

제한된 그룹 정책은 도메인에 있는 컴퓨터의 로컬 그룹 구성원 자격을 제한된 그룹 정책에 정의된 구성원 자격 목록 설정과 일치하도록 설정합니다. View 데스크톱 사용자 그룹의 구성원은 도메인에 가입된 모든 View 데스크톱의 로컬 원격 데스크톱 사용자 그룹에 항상 추가됩니다. 새 사용자를 추가할 때는 View 데스크톱 사용자 그룹에만 추가해야 합니다.

필수 조건

Active Directory 의 도메인에 View 데스크톱 사용자 그룹을 생성하십시오.

프로시저

1 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동합니다.

AD 버전	탐색 경로
Windows 2003	a **시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터**. b 도메인을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 클릭합니다. c 그룹 정책 관리 플러그인을 열려면 **그룹 정책** 탭에서 **열기**를 클릭하십시오. d **기본 도메인 정책**을 마우스 오른쪽 버튼으로 클릭하고 **편집**을 클릭합니다.
Windows 2008	a **시작 > 관리 도구 > 그룹 정책 관리**. b 도메인을 확장하고 **기본 도메인 정책**을 마우스 오른쪽 버튼으로 클릭한 다음 **편집**을 클릭합니다.

2 **컴퓨터 구성** 섹션을 확장하고 Windows Settings\Security Settings 을 여십시오.

3 마우스 오른쪽 버튼으로 **제한된 그룹**을 클릭하고 **그룹 추가**를 선택한 다음 원격 데스크톱 사용자 그룹을 추가하십시오.

4 마우스 오른쪽 버튼으로 새로 제한된 원격 데스크톱 사용자 그룹을 클릭하고 그룹 구성원 자격 목록에 View 데스크톱 사용자 그룹을 추가하십시오.

5 변경 사항을 저장하려면 **확인**을 클릭합니다.

View 그룹 정책 관리 템플릿 파일 사용

View 에는 여러 구성 요소 특정 그룹 정책 관리(ADM) 템플릿 파일이 있습니다.

View Connection Server 설치 중 View ADM 템플릿 파일은 View Connection Server 호스트의 *install_directory*₩VMware₩VMware View₩Server₩Extras₩GroupPolicyFiles 디렉토리에 설치됩니다. 이러한 파일을 Active Directory 서버에 복사해야 합니다.

이러한 파일의 정책 설정을 Active Directory 의 다음 또는 기존 GPO 에 추가한 다음 해당 GPO 를 View 데스크톱이 포함된 OU 에 연결하여 View 데스크톱을 최적화하고 보호할 수 있습니다.

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

스마트 카드 인증을 위한 Active Directory 준비

스마트 카드 인증을 구현할 때 Active Directory 에서 특정 작업을 수행해야 할 수 있습니다.

- 스마트 카드 사용자의 UPN 추가(29 페이지)

  스마트 카드 로그인이 UPN(사용자 이름)에 기반하기 때문에 스마트 카드를 사용해 View 에 인증하는 사용자의 Active Directory 계정에 UPN 이 올바르게 구성되어 있어야 합니다.

- 신뢰할 수 있는 루트 인증 기관에 루트 인증서 추가(29 페이지)

  인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory 의 신뢰할 수 있는 루트 인증 기관 그룹 정책에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA 로 사용하면 이 절차를 수행할 필요가 없습니다.

- 중간 인증 기관에 중간 인증서 추가(30 페이지)

  중간 인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory 의 중간 인증 기관 그룹 정책에 중간 인증서를 추가해야 합니다.

- Enterprise NTAuth 저장소에 루트 인증서 추가(30 페이지)

  CA 를 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory 의 Enterprise NTAuth 저장소에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA 로 사용하면 이 절차를 수행할 필요가 없습니다.

스마트 카드 사용자의 UPN 추가

스마트 카드 로그인이 UPN(사용자 이름)에 기반하기 때문에 스마트 카드를 사용해 View 에 인증하는 사용자의 Active Directory 계정에 UPN 이 올바르게 구성되어 있어야 합니다.

스마트 카드 사용자가 위치한 도메인이 루트 인증서를 발급한 도메인과 다르면 사용자의 UPN 을 신뢰할 수 있는 CA 의 루트 인증서에 포함된 SAN(주체 대체 이름)으로 설정해야 합니다. 스마트 카드 사용자의 현재 도메인에 있는 서버에서 루트 인증서를 발급한 경우 사용자의 UPN 을 수정할 필요가 없습니다.

참고 같은 도메인에서 인증서를 발급한 경우에도 기본 Active Directory 계정에 대한 UPN 을 설정해야 할 수 있습니다. Administrator 를 포함해 기본 계정에는 UPN 이 기본적으로 설정되지 않습니다.

필수 조건

- 인증서 속성을 확인해 신뢰할 수 있는 CA 의 루트 인증서에 포함된 SAN 을 가져오십시오.
- Active Directory 서버에 ADSI 편집 유틸리티가 없으면 Microsoft 웹 사이트에서 적절한 Windows 지원 도구를 다운로드하여 설치하십시오.

프로시저

1 Active Directory 서버에서 ADSI 편집 유틸리티를 시작하십시오.

2 왼쪽 창에서 사용자가 위치한 도메인을 확장하고 `CN=Users` 를 두 번 클릭합니다.

3 오른쪽 창에서 마우스 오른쪽 단추로 사용자를 클릭한 다음 **속성**을 클릭합니다.

4 `userPrincipalName` 특성을 두 번 클릭하고 신뢰할 수 있는 CA 인증서의 SAN 값을 입력하십시오.

5 특성 설정을 저장하려면 **확인**을 클릭합니다.

신뢰할 수 있는 루트 인증 기관에 루트 인증서 추가

인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory 의 신뢰할 수 있는 루트 인증 기관 그룹 정책에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA 로 사용하면 이 절차를 수행할 필요가 없습니다.

프로시저

1 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동합니다.

AD 버전	탐색 경로
Windows 2003	a **시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터**. b 도메인을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 클릭합니다. c 그룹 정책 관리 플러그인을 열려면 **그룹 정책** 탭에서 **열기**를 클릭하십시오. d **기본 도메인 정책**을 마우스 오른쪽 버튼으로 클릭하고 **편집**을 클릭합니다.
Windows 2008	a **시작 > 관리 도구 > 그룹 정책 관리**. b 도메인을 확장하고 **기본 도메인 정책**을 마우스 오른쪽 버튼으로 클릭한 다음 **편집**을 클릭합니다.

2 **컴퓨터 구성** 섹션을 확장하고 **Windows 설정\보안 설정\공개 키**를 여십시오.

3 **신뢰할 수 있는 루트 인증 기관**을 마우스 오른쪽 버튼으로 클릭하고 **가져오기**를 선택합니다.

4 마법사에 표시된 메시지에 따라 루트 인증서(예: rootCA.cer)를 가져오고 **확인**을 클릭합니다.

5 그룹 정책 창을 닫습니다.

이제 도메인의 모든 시스템에서 신뢰할 수 있는 루트 저장소의 루트 인증서 복사본을 가지고 있습니다.

후속 작업

중간 인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory 의 중간 인증 기관 그룹 정책에 중간 인증서를 추가하십시오. "중간 인증 기관에 중간 인증서 추가," (30 페이지)의 내용을 참조하십시오.

중간 인증 기관에 중간 인증서 추가

중간 인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory 의 중간 인증 기관 그룹 정책에 중간 인증서를 추가해야 합니다.

프로시저

1 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동합니다.

AD 버전	탐색 경로
Windows 2003	a **시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터**. b 도메인을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 클릭합니다. c 그룹 정책 관리 플러그인을 열려면 **그룹 정책** 탭에서 **열기**를 클릭하십시오. d **기본 도메인 정책**을 마우스 오른쪽 버튼으로 클릭하고 **편집**을 클릭합니다.
Windows 2008	a **시작 > 관리 도구 > 그룹 정책 관리**. b 도메인을 확장하고 **기본 도메인 정책**을 마우스 오른쪽 버튼으로 클릭한 다음 **편집**을 클릭합니다.

2 **컴퓨터 구성** 섹션을 확장하고 Windows **설정\보안 설정\공개 키**에 대한 정책을 엽니다.

3 **중간 인증 기관**을 마우스 오른쪽 버튼으로 클릭하고 **가져오기**를 선택합니다.

4 마법사에 표시된 메시지에 따라 중간 인증서(예: intermediateCA.cer)를 가져오고 **확인**을 클릭합니다.

5 그룹 정책 창을 닫습니다.

이제 도메인의 모든 시스템에서 중간 인증 기관 저장소의 중간 인증서 복사본을 가지고 있습니다.

Enterprise NTAuth 저장소에 루트 인증서 추가

CA 를 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory 의 Enterprise NTAuth 저장소에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA 로 사용하면 이 절차를 수행할 필요가 없습니다.

프로시저

◆ Enterprise NTAuth 저장소에 인증서를 게시하려면 Active Directory 서버에서 certutil 명령을 사용하십시오.

예: **certutil -dspublish -f** ***path_to_root_CA_cert*** **NTAuthCA**

이제 해당 CA 에서 이러한 유형의 인증서를 신뢰하고 발급할 수 있습니다.

View Composer 설치 4

View Composer 를 사용하려면 View Composer 데이터베이스를 생성하고 View Composer 서비스를 설치하고 View 인프라를 최적화하여 View Composer 를 지원합니다. vCenter Server 와 동일한 호스트 또는 별도 호스트에 View Composer 서비스를 설치할 수 있습니다.

View Composer 는 선택 기능입니다. 연결된 클론 데스크톱 풀을 배포하려면 View Composer 를 설치합니다.

View Composer 기능을 설치하고 사용하려면 라이센스가 있어야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

View Composer 데이터베이스 준비

데이터베이스 및 데이터 소스 이름(DSN)을 생성하여 View Composer 데이터를 저장해야 합니다.

View Composer 서비스에는 데이터베이스가 포함되지 않습니다. 네트워크 환경에 데이터베이스 인스턴스가 없으면 설치해야 합니다. 데이터베이스 인스턴스를 설치한 후 View Composer 데이터베이스를 인스턴스에 추가합니다.

View Composer 데이터베이스를 vCenter Server 데이터베이스가 지정된 인스턴스에 추가할 수 있습니다. 데이터베이스를 로컬로, 또는 네트워크 연결된 Linux, UNIX 또는 Windows Server 컴퓨터에서 원격으로 구성할 수 있습니다.

View Composer 데이터베이스는 View Composer 에서 사용하는 연결 및 구성 요소에 대한 정보를 저장합니다.

- vCenter Server 연결
- Active Directory 연결
- View Composer 에서 배포한 연결된 클론 데스크톱
- View Composer 에서 생성된 복제본

View Composer 서비스의 각 인스턴스에는 고유의 View Composer 데이터베이스가 있어야 합니다. 여러 View Composer 서비스는 View Composer 데이터베이스를 공유할 수 없습니다.

지원되는 데이터베이스 버전 목록은 "View Composer 데이터베이스 요구 사항," (11 페이지)을 참조하십시오.

View Composer 데이터베이스를 설치된 데이터베이스 인스턴스에 추가하려면 이러한 절차 중 하나를 선택합니다.

- View Composer 용 SQL Server 데이터베이스 생성(32 페이지)

  View Composer 는 연결된 클론 데스크톱 정보를 SQL Server 데이터베이스에 저장할 수 있습니다. SQL Server 에 View Composer 데이터베이스를 추가하고 ODBC 데이터 소스를 구성하여 이를 생성합니다.

- View Composer 용 Oracle 데이터베이스 생성(34 페이지)

  View Composer 는 연결된 클론 데스크톱 정보를 Oracle 11g 또는 10g 데이터베이스에 저장할 수 있습니다. 기존 Oracle 인스턴스에 View Composer 데이터베이스를 추가하고 ODBC 데이터 소스를 구성하여 생성합니다. Oracle 데이터베이스 구성 도우미를 사용하거나 SQL 문을 실행해 새 View Composer 데이터베이스를 추가할 수 있습니다.

View Composer 용 SQL Server 데이터베이스 생성

View Composer 는 연결된 클론 데스크톱 정보를 SQL Server 데이터베이스에 저장할 수 있습니다. SQL Server 에 View Composer 데이터베이스를 추가하고 ODBC 데이터 소스를 구성하여 이를 생성합니다.

SQL Server 에 View Composer 데이터베이스 추가

기존 Microsoft SQL Server 인스턴스에 새 View Composer 데이터베이스를 추가해 View Composer 의 연결된 클론 데이터를 저장할 수 있습니다.

데이터베이스가 로컬에 있는 경우, View Composer 가 설치될 시스템에서 통합 Windows 인증 보안 모델을 사용할 수 있습니다. 데이터베이스가 원격 시스템에 있으면 이 인증 방법을 사용할 수 없습니다.

필수 조건

- View Composer 를 설치하려는 컴퓨터 또는 네트워크 환경에 지원되는 SQL Server 버전이 설치되어 있는지 확인하십시오. 자세한 내용은 "View Composer 데이터베이스 요구 사항," (11 페이지).
- 데이터 소스를 생성하고 관리할 수 있는 SQL Server Management Studio 또는 SQL Server Management Studio Express 를 사용하는지 확인하십시오. 다음 웹 사이트에서 SQL Server Management Studio Express 를 다운로드하고 설치할 수 있습니다.

  http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796

프로시저

1 View Composer 컴퓨터에서 **시작 > 모든 프로그램 >** Microsoft SQL Server 2008 또는 Microsoft SQL Server 2005 를 선택하십시오.

2 SQL Server Management Studio Express 를 선택하고 vSphere Management 의 기존 SQL Server 인스턴스에 연결하십시오.

3 개체 탐색기 패널에서 마우스 오른쪽 단추로 데이터베이스 항목을 클릭하고 **새 데이터베이스**를 선택하십시오.

4 새 데이터베이스 대화 상자의 데이터베이스 이름 텍스트 상자에 이름을 입력하십시오.

  예: **viewComposer**

5 **확인**을 클릭합니다.

  SQL Server Management Studio Express 에서 개체 탐색기 패널의 데이터베이스 항목에 데이터베이스를 추가합니다.

6 Microsoft SQL Server Management Studio Express 를 종료하십시오.

후속 작업

"SQL Server 에 ODBC 데이터 소스 추가," (33 페이지).

SQL Server 에 ODBC 데이터 소스 추가

SQL Server 에 View Composer 데이터베이스를 추가한 후에 View Composer 서비스에서 이 데이터 소스를 볼 수 있도록 새 데이터베이스에 대한 ODBC 연결을 구성해야 합니다.

View Composer 에 대해 ODBC DSN 을 구성하는 경우, 기본적 데이터베이스 연결의 보안 수준을 해당 환경에 적합하게 지정하십시오. 데이터베이스 연결의 보안 지정에 대한 내용은 SQL Server 설명서를 참조하십시오.

기본 데이터베이스 연결에 SSL 암호화가 사용되는 경우 신뢰할 수 있는 CA 에서 서명한 SSL 인증서로 데이터베이스 서버를 구성하는 것이 좋습니다. 자체 서명된 인증서를 사용하는 경우, 데이터베이스 연결이 외부 공격에 민감할 수 있습니다.

필수 조건

"SQL Server 에 View Composer 데이터베이스 추가," (32 페이지).

프로시저

1 View Composer 가 설치되는 컴퓨터에서 **시작 > 관리 도구 > 데이터 소스(ODBC)**를 선택합니다.

2 **시스템 DSN** 탭을 선택하십시오.

3 **추가**를 클릭하고 목록에서 SQL Native Client 를 선택하십시오.

4 **마침**을 클릭하십시오.

5 SQL Server 설치에 새 데이터 원본 만들기 마법사에서 View Composer 데이터베이스 이름과 설명을 입력하십시오.

   예: **ViewComposer**

6 서버 텍스트 상자에 SQL Server 데이터베이스 이름을 입력하십시오.

   *host_name**server_name* 형식을 사용하십시오. *host_name* 은 컴퓨터 이름, *server_name* 은 SQL Server 인스턴스입니다.

   예: **VCHOST1WVIM_SQLEXP**

7 **다음**을 클릭하십시오.

8 **추가 구성 옵션의 기본 설정을 얻기 위해 SQL Server 에 연결** 확인란을 선택했는지 확인하고 인증 옵션을 선택하십시오.

옵션	설명
Windows NT 인증	SQL Server 의 로컬 인스턴스를 사용하는 경우 이 옵션을 선택합니다. 신뢰할 수 있는 인증이라고도 합니다. 로컬 컴퓨터에서 SQL Server 를 실행하는 경우에만 Windows NT 인증을 지원합니다.
SQL Server 인증	SQL Server 의 원격 인스턴스를 사용하는 경우 이 옵션을 선택합니다. 원격 SQL Server 에서는 Windows NT 인증을 지원하지 않습니다.

9 **다음**을 클릭하십시오.

10 **기본 데이터베이스를 다음으로 변경:** 확인란을 선택하고 목록에서 View Composer 데이터베이스 이름을 선택하십시오.

   예: **ViewComposer**

11 SSL 이 활성화된 상태로 SQL Server 연결이 구성된 경우 Microsoft SQL Server DSN 구성 페이지로 이동한 다음 **데이터에 강력한 암호 사용**을 선택합니다.

12 Microsoft ODBC 데이터 원본 관리자 마법사를 종료하고 닫으십시오.

후속 작업

새 View Composer 서비스를 설치합니다. "View Composer 서비스 설치," (37 페이지)를 참조하십시오.

View Composer 용 Oracle 데이터베이스 생성

View Composer 는 연결된 클론 데스크톱 정보를 Oracle 11g 또는 10g 데이터베이스에 저장할 수 있습니다. 기존 Oracle 인스턴스에 View Composer 데이터베이스를 추가하고 ODBC 데이터 소스를 구성하여 생성합니다. Oracle 데이터베이스 구성 도우미를 사용하거나 SQL 문을 실행해 새 View Composer 데이터베이스를 추가할 수 있습니다.

- Oracle 11g 또는 10g 에 View Composer 데이터베이스 추가(34 페이지)

  Oracle 데이터베이스 구성 도우미를 사용해 기존 Oracle 11g 또는 10g 인스턴스에 새로운 View Composer 데이터베이스를 추가할 수 있습니다.

- SQL 문을 사용하여 Oracle 인스턴스에 View Composer 데이터베이스 추가(35 페이지)

  View Composer 데이터베이스에는 특정 테이블 공간 및 권한이 있어야 합니다. SQL 문을 사용하여 Oracle 11g 또는 10g 데이터베이스 인스턴스에 View Composer 데이터베이스를 생성할 수 있습니다.

- View Composer 의 Oracle 데이터베이스 사용자 구성(36 페이지)

  기본적으로 View Composer 데이터베이스를 실행하는 데이터베이스 사용자는 Oracle 시스템 관리자 사용 권한을 가지고 있습니다. View Composer 데이터베이스를 실행하는 사용자의 보안 권한을 제한하려면 특정 사용 권한을 가진 Oracle 데이터베이스 사용자를 구성해야 합니다.

- Oracle 11g 또는 10g 에 ODBC 데이터 소스 추가(36 페이지)

  Oracle 11g 또는 10g 인스턴스에 View Composer 데이터베이스를 추가한 후에 View Composer 서비스에서 데이터 소스를 볼 수 있도록 새 데이터베이스에 대한 ODBC 연결을 구성해야 합니다.

Oracle 11g 또는 10g 에 View Composer 데이터베이스 추가

Oracle 데이터베이스 구성 도우미를 사용해 기존 Oracle 11g 또는 10g 인스턴스에 새로운 View Composer 데이터베이스를 추가할 수 있습니다.

필수 조건

로컬 또는 원격 컴퓨터에 지원되는 Oracle 11g 또는 10g 버전이 설치되어 있는지 확인하십시오. 다음을 참조: "View Composer 데이터베이스 요구 사항," (11 페이지).

프로시저

1 View Composer 데이터베이스를 추가하는 컴퓨터에서 **데이터베이스 구성 도우미**를 시작합니다.

데이터베이스 버전	조치
Oracle 11g	**시작 > 모든 프로그램 > Oracle-OraDb11g_home > 구성 및 마이그레이션 도구 > 데이터베이스 구성 도우미**.
Oracle 10g	**시작 > 모든 프로그램 > Oracle-OraDb10g_home > 구성 및 마이그레이션 도구 > 데이터베이스 구성 도우미**.

2 작업 페이지에서 **데이터베이스 만들기**를 선택하십시오.

3 데이터베이스 템플릿 페이지에서 **범용 또는 트랜잭션 처리** 템플릿을 선택하십시오.

4 데이터베이스 ID 페이지에서 전역 데이터베이스 이름 및 Oracle SID(시스템 식별자) 접두사를 입력하십시오.

양쪽 항목에 동일한 값을 사용하면 간단하게 작업할 수 있습니다.

5 관리 옵션 페이지에서 **다음**을 클릭해 기본 설정을 적용하십시오.

6 데이터베이스 자격 증명 페이지에서 **모든 계정에 동일한 관리 암호 사용**을 선택하고 암호를 입력하십시오.

7 나머지 구성 페이지에서 **다음**을 클릭해 기본 설정을 적용하십시오.

8 생성 옵션 페이지에서 **데이터베이스 생성**을 선택했는지 확인하고 **마침**을 클릭하십시오.

9 확인 페이지에서 옵션을 검토하고 **확인**을 클릭하십시오.

구성 도구가 데이터베이스를 생성합니다.

10 데이터베이스 생성 완료 페이지에서 **확인**을 클릭하십시오.

후속 작업

"Oracle 11g 또는 10g 에 ODBC 데이터 소스 추가," (36 페이지).

SQL 문을 사용하여 Oracle 인스턴스에 View Composer 데이터베이스 추가

View Composer 데이터베이스에는 특정 테이블 공간 및 권한이 있어야 합니다. SQL 문을 사용하여 Oracle 11g 또는 10g 데이터베이스 인스턴스에 View Composer 데이터베이스를 생성할 수 있습니다.

데이터베이스를 생성할 때 데이터 및 로그 파일의 위치를 사용자 지정할 수 있습니다.

필수 조건

로컬 또는 원격 컴퓨터에 지원되는 Oracle 11g 또는 10g 버전이 설치되어 있는지 확인하십시오. 자세한 내용은 "View Composer 데이터베이스 요구 사항," (11 페이지).

프로시저

1 시스템 계정으로 SQL*Plus 세션에 로그인하십시오.

2 다음 SQL 문을 실행하여 데이터베이스를 생성합니다.

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

이 예에서, `VCMP` 는 View Composer 데이터베이스의 샘플 이름이고 `vcmp01.dbf` 는 데이터베이스 파일의 이름입니다.

Windows 설치의 경우 `vcmp01.dbf` 파일에 대한 디렉토리 경로에 Windows 규칙을 사용합니다.

후속 작업

특정 보안 권한을 사용하여 View Composer 데이터베이스를 실행할 경우 "View Composer 의 Oracle 데이터베이스 사용자 구성," (36 페이지).

"Oracle 11g 또는 10g 에 ODBC 데이터 소스 추가," (36 페이지)

View Composer의 Oracle 데이터베이스 사용자 구성

기본적으로 View Composer 데이터베이스를 실행하는 데이터베이스 사용자는 Oracle 시스템 관리자 사용 권한을 가지고 있습니다. View Composer 데이터베이스를 실행하는 사용자의 보안 권한을 제한하려면 특정 사용 권한을 가진 Oracle 데이터베이스 사용자를 구성해야 합니다.

필수 조건

Oracle 11g 또는 10g 인스턴스에 View Composer 데이터베이스가 생성됐는지 확인하십시오.

프로시저

1 시스템 계정으로 SQL*Plus 세션에 로그인하십시오.

2 올바른 사용 권한을 가진 View Composer 데이터베이스 사용자를 생성하려면 다음 SQL 명령을 실행하십시오.

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
   grant connect to VCMPADMIN;
   grant resource to VCMPADMIN;
   grant create view to VCMPADMIN;
   grant create sequence to VCMPADMIN;
   grant create table to VCMPADMIN;
   grant create materialized view to VCMPADMIN;
   grant execute on dbms_lock to VCMPADMIN;
   grant execute on dbms_job to VCMPADMIN;
   grant unlimited tablespace to VCMPADMIN;
```

이 예에서 사용자 이름은 VCMPADMIN이고 View Composer 데이터베이스 이름은 VCMP입니다.

기본적으로 리소스 역할은 프로시저 생성, 테이블 생성 및 시퀀스 생성 권한을 가지고 있습니다. 리소스 역할에 이런 권한이 없으면 View Composer 데이터베이스 사용자에 명시적으로 이들 권한을 부여하십시오.

Oracle 11g 또는 10g에 ODBC 데이터 소스 추가

Oracle 11g 또는 10g 인스턴스에 View Composer 데이터베이스를 추가한 후에 View Composer 서비스에서 데이터 소스를 볼 수 있도록 새 데이터베이스에 대한 ODBC 연결을 구성해야 합니다.

View Composer에 대해 ODBC DSN을 구성하는 경우, 기본적 데이터베이스 연결의 보안 수준을 해당 환경에 적합하게 지정하십시오. 데이터베이스 연결의 보안 지정에 대한 내용은 Oracle 데이터베이스 설명서를 참조하십시오.

기본 데이터베이스 연결에 SSL 암호화가 사용되는 경우 신뢰할 수 있는 CA에서 서명한 SSL 인증서로 데이터베이스 서버를 구성하는 것이 좋습니다. 자체 서명된 인증서를 사용하는 경우, 데이터베이스 연결이 외부 공격에 민감할 수 있습니다.

필수 조건

"Oracle 11g 또는 10g에 View Composer 데이터베이스 추가," (34 페이지) 또는 "SQL 문을 사용하여 Oracle 인스턴스에 View Composer 데이터베이스 추가," (35 페이지).

프로시저

1 View Composer 데이터베이스 컴퓨터에서 **시작 > 관리 도구 > 데이터 소스(ODBC)**를 선택합니다.

2 Microsoft ODBC 데이터 원본 관리자 마법사에서 **시스템 DSN** 탭을 선택하십시오.

3 **추가**를 클릭하고 목록에서 적절한 Oracle 드라이버를 선택하십시오.

예: OraDb11g_home

4 **마침**을 클릭하십시오.

5 Oracle ODBC 드라이버 구성 대화 상자에서 View Composer 와 함께 사용할 DSN, 데이터 소스 설명, 데이터베이스에 연결할 사용자 ID 를 입력하십시오.

특정 보안 권한을 가진 Oracle 데이터베이스 사용자 ID 를 구성한 경우 해당 사용자 ID 를 지정하십시오.

참고 View Composer 서비스를 설치할 때 DSN 을 사용합니다.

6 드롭다운 메뉴에서 전역 데이터베이스 이름을 선택하여 **TNS 서비스 이름**을 지정하십시오.

Oracle 데이터베이스 구성 도우미가 전역 데이터베이스 이름을 지정합니다.

7 데이터 소스를 확인하려면 **연결 테스트**를 클릭하고 **확인**을 클릭하십시오.

후속 작업

새 View Composer 서비스를 설치합니다. "View Composer 서비스 설치," (37 페이지)를 참조하십시오.

View Composer 에 대한 SSL 인증서 구성

기본적으로, 자체 서명된 인증서는 View Composer 와 함께 설치됩니다. 테스트 목적으로 기본 인증서를 사용할 수 있지만 운영 목적을 위해서는 이 인증서를 인증 기관(CA)에서 서명한 인증서로 대체해야 합니다.

View Composer 를 설치하기 전이나 후에 인증서를 구성할 수 있습니다. View 5.1 이상 릴리스에서는 View Composer 가 설치되었거나 설치될 Windows Server 컴퓨터의 Windows 로컬 컴퓨터 인증서 저장소로 인증서를 가져오는 식으로 인증서를 구성합니다.

- View Composer 를 설치하기 전에 CA 서명 인증서를 가져오는 경우, View Composer 설치 중에 서명된 인증서를 선택할 수 있습니다. 이 방법을 이용하면 설치 후 기본 인증서를 수작업으로 대체할 필요가 없습니다.
- View Composer 설치 후 기존 인증서 또는 자체 서명된 기본 인증서를 새 인증서로 대체하려는 경우, 새 인증서를 가져온 후 SviConfig ReplaceCertificate 유틸리티를 실행하여 새 인증서를 View Composer 에서 사용하는 포트에 바인딩시켜야 합니다.

SSL 인증서 구성 및 SviConfig ReplaceCertificate 유틸리티 사용에 대한 자세한 내용은 View Server 를 위한 SSL 인증서 구성을 참조하십시오.

동일 Windows Server 컴퓨터에 vCenter Server 와 View Composer 를 설치하는 경우, 동일 SSL 인증서의 사용이 가능하지만 각 구성 요소에 대해 개별적으로 인증서를 구성해야 합니다.

View Composer 서비스 설치

View Composer 를 사용하려면 View Composer 서비스를 설치해야 합니다. View Manager 는 View Composer 를 사용해 vCenter Server 에 연결된 클론 데스크톱을 생성하고 배포합니다.

vCenter Server 가 설치된 Windows Server 컴퓨터 또는 별도 Windows Server 컴퓨터에 View Composer 서비스를 설치할 수 있습니다. 독립 실행형 View Composer 는 Windows Server 컴퓨터에 설치된 vCenter Server 및 Linux 기반 vCenter Server 어플라이언스에 설치하여 사용할 수 있습니다.

View Composer 소프트웨어는 replica server, 보안 서버, View 연결 서버, View Agent, View Client 또는 View 전송 서버 등 다른 View Manager 소프트웨어 구성 요소가 있는 동일 가상 또는 물리적 시스템에 함께 있을 수 없습니다.

필수 조건

- "View Composer 요구 사항," (9 페이지)의 View Composer 요구 사항에 따라 설치했는지 확인하십시오.
- View Composer 를 설치 및 사용할 수 있는 라이센스를 가지고 있는지 확인하십시오.
- ODBC 데이터 원본 관리자 마법사에서 제공한 DSN, 도메인 관리자 사용자 이름, 암호를 가지고 있는지 확인하십시오. View Composer 서비스를 설치할 때 해당 정보를 입력합니다.
- 설치 과정에서 View Composer 에 대해 CA 에서 서명한 SSL 인증서를 구성하려는 경우, Windows 로컬 컴퓨터의 인증서 저장소에 인증서를 가져왔는지 확인하십시오. View Server 를 위한 SSL 인증서 구성의 내용을 참조하십시오.
- View Composer 컴퓨터에서 실행되는 어떤 애플리케이션도 Microsoft 보안 채널(Schannel) 보안 패키지를 통해 제공되는 SSL 버전 2(SSLv2)가 필요한 Windows SSL 라이브러리를 사용하지 않는지 확인합니다. View Composer 설치 관리자는 Microsoft Schannel 에서 SSLv2 의 사용을 해제합니다. Java SSL 을 사용하는 Tomcat 또는 OpenSSL 을 사용하는 Apache 등의 애플리케이션은 이 제약의 영향을 받지 않습니다.
- View Composer 설치 관리자를 실행하려면 시스템에서 관리자 권한을 가진 도메인 사용자 자격이 필요합니다.

프로시저

1 http://www.vmware.com/products/의 VMware 제품 페이지에서 VMware View Composer 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드하십시오.

   설치 관리자 파일 이름은 `VMware-viewcomposer-`*y.y.y*`-`*xxxxxx*`.exe` 입니다. 여기서 *xxxxxx* 는 빌드 번호이며 *y.y.y* 는 버전 번호입니다. 이 설치 관리자 파일로 64 비트 Windows Server 운영 체제에 View Composer 서비스를 설치할 수 있습니다.

2 View Composer 설치 프로그램을 시작하려면 설치 관리자 파일을 마우스 오른쪽 버튼으로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

3 VMware 사용 약관에 동의하십시오.

4 대상 폴더를 허용 또는 변경하십시오.

5 Microsoft 또는 Oracle ODBC 데이터 원본 관리자 마법사에 제공된 View Composer 데이터베이스의 DSN 을 입력하십시오.

   예: **VMware View Composer**

   참고 View Composer 데이터베이스의 DSN 을 구성하지 않은 경우 지금 이름을 구성하려면 ODBC DSN **설치**를 클릭하십시오.

6 ODBC 데이터 원본 관리자 마법사에 제공된 도메인 관리자 사용자 이름과 암호를 입력하십시오.

   특정 보안 권한을 가진 Oracle 데이터베이스 사용자를 구성한 경우 해당 사용자 이름을 지정하십시오.

7 포트 번호를 입력하거나 기본값을 허용하십시오.

   View 연결 서버는 해당 포트를 사용해 View Composer 서비스와 통신합니다.

8 SSL 인증서를 지정하십시오.

옵션	조치
기본 SSL 인증서 생성	View Composer 서비스에 대한 기본 SSL 인증서를 생성하려면 이 라디오 버튼을 선택합니다. 설치 후, 기본 인증서를 CA 에서 서명한 SSL 인증서로 대체할 수 있습니다.
기존 SSL 인증서 사용	View Composer 서비스에 대해 사용할 서명된 SSL 인증서를 설치한 경우, 이 라디오 버튼을 선택합니다. 목록에서 SSL 인증서를 선택합니다.

9 View Composer 서비스 설치를 완료하려면 **설치**와 **마침**을 클릭하십시오.

VMware View Composer 서비스가 시작됩니다.

View Composer 는 Windows Server 운영 체제가 제공하는 암호화 암호 집합을 사용합니다. Windows Server 시스템에서 암호 집합을 관리하기 위한 해당 조직의 가이드라인을 따라야 합니다. 조직에서 가이드라인을 제공하지 않는 경우, View Composer 서버에서 약한 암호화 암호 집합의 사용을 해제하여 View 환경의 보안을 강화하는 것이 좋습니다. 암호화 암호 집합을 관리하기 위한 자세한 내용은 Microsoft 문서를 참조하십시오.

View Composer 를 위한 인프라 구축

vSphere, vCenter Server, Active Directory 및 인프라의 다른 구성 요소에 있는 기능을 사용해 View Composer 성능, 가용성, 신뢰성을 최적화할 수 있습니다.

View Composer 를 위한 vSphere 환경 구성

View Composer 를 지원하려면 특정 모범 사례에 따라 vCenter Server, ESX/ESXi 및 기타 vSphere 구성 요소를 설치하고 구성해야 합니다.

이러한 모범 사례를 통해 vSphere 환경에서 View Composer 가 더욱 효율적으로 작동할 수 있습니다.

- 연결된 클론 가상 컴퓨터의 경로 및 폴더 정보를 생성한 후에는 vCenter Server 에서 해당 정보를 변경하지 마십시오. 대신 View Administrator 를 사용해 폴더 정보를 변경하십시오.

  vCenter Server 에서 이 정보를 변경할 경우 View Manager 가 vCenter Server 에서 가상 컴퓨터를 찾을 수 없습니다.

- ESX/ESXi 호스트에서 실행되는 연결된 클론 가상 컴퓨터에 구성되어 있는 총 가상 NIC 수를 지원하기에 충분한 포트가 구성되었는지 ESX/ESXi 호스트의 vSwitch 설정을 확인하십시오.
- 연결된 클론 데스크톱을 리소스 풀에 배포할 때 vSphere 환경에 필요한 데스크톱 수를 호스팅하기에 충분한 CPU 와 메모리가 준비되어 있는지 확인하십시오. 리소스 풀의 CPU 와 메모리 사용량을 모니터링하려면 vSphere Client 를 사용하십시오.
- View Composer 연결된 클론에 사용되는 클러스터는 8 대 이상의 ESX/ESXi 호스트를 포함할 수 있지만 NFS 데이터스토어에 복제 디스크를 저장해야 합니다. VMFS 데이터스토어에서 최대 8 대의 ESX/ESXi 호스트를 포함하는 클러스터를 사용해서만 복제 디스크를 저장할 수 있습니다.
- vSphere DRS 를 사용하십시오. DRS 는 호스트에서 연결된 클론 가상 컴퓨터를 효율적으로 분산시킵니다.

참고 연결된 클론 데스크톱은 Storage vMotion 을 지원하지 않습니다.

View Composer의 추가 모범 사례

View Composer가 효율적으로 작동하는지 확인하려면 DNS(Dynamic Name Service)가 제대로 작동하는지 확인하고 바이러스 백신 소프트웨어 검사를 여러 차례로 나눠 실시합니다.

DNS 확인 작업을 올바르게 수행하면 DNS 오류로 인해 간혹 발생하는 문제를 해결할 수 있습니다. View Composer 서비스는 동적 이름 확인을 통해 다른 컴퓨터와 통신합니다. DNS 작업을 테스트하려면 Active Directory 및 View Connection Server 컴퓨터를 이름으로 Ping 합니다.

바이러스 백신 소프트웨어 실행 시간을 분산하면 연결된 클론 데스크톱 성능에 영향을 미치지 않습니다. 모든 연결된 클론에서 바이러스 백신 소프트웨어를 동시에 실행하면 스토리지 하위 시스템에서 초당 I/O 작업(IOPS)이 과도하게 발생합니다. 이러한 과도한 활동은 연결된 클론 데스크톱 성능에 영향을 미칠 수 있습니다.

View Connection Server 설치 5

View Connection Server를 사용하려면 지원된 컴퓨터에 소프트웨어를 설치하고 필요한 구성 요소를 구성하며 선택적으로 구성 요소를 최적화합니다.

이 장에서는 다음 주제에 대해 설명합니다.

View Connection Server 소프트웨어 설치

View 배포의 성능, 가용성 및 보안 요구에 따라 View Connection Server의 단일 인스턴스, View Connection Server의 복제된 인스턴스 및 보안 서버를 설치할 수 있습니다. View Connection Server 인스턴스를 하나 이상 설치해야 합니다.

View Connection Server를 설치할 때 설치 유형을 선택합니다.

표준 설치	새 View LDAP 구성을 사용하여 View Connection Server 인스턴스를 생성합니다.
복제 설치	기존 인스턴스에서 복사된 View LDAP 구성을 사용하여 View Connection Server 인스턴스를 생성합니다.
보안 서버 설치	인터넷 및 내부 네트워크 사이에 추가 보안 계층을 추가하는 View Connection Server 인스턴스를 생성합니다.

View 연결 서버의 설치 전제 조건

View 연결 서버를 설치하기 전에 설치 환경이 특정 전제 조건을 만족해야 합니다.

- View 연결 서버에는 View Manager의 유효한 라이센스 키가 필요합니다. 다음 라이센스 키를 사용할 수 있습니다.
  - View Manager
  - View Composer 및 Local Mode 포함 View Manager
- View 연결 서버 호스트를 Active Directory 도메인에 결합시켜야 합니다. View 연결 서버는 다음 버전의 Active Directory를 지원합니다.
  - Windows 2003 Active Directory
  - Windows 2008 Active Directory

  View 연결 서버 호스트는 도메인 컨트롤러가 될 수 없습니다.

  참고 View 연결 서버에서는 Active Directory에 대해 스키마 또는 구성을 업데이트하지 않고 업데이트가 필요하지도 않습니다.
- Windows Terminal Server 역할이 설치된 시스템에 View 연결 서버를 설치하지 마십시오. View 연결 서버를 설치할 임의의 시스템에서 Windows Terminal Server 역할을 제거해야 합니다.
- 다른 기능 또는 역할을 수행하는 시스템에 View 연결 서버를 설치하지 마십시오. 예를 들어 동일한 시스템을 사용하여 vCenter Server를 호스팅하지 마십시오.
- View 연결 서버를 설치할 시스템에 정적 IP 주소가 있어야 합니다.
- View 연결 서버 설치 관리자를 실행하려면 시스템에서 관리자 권한을 가진 도메인 사용자 계정을 사용해야 합니다.
- View 연결 서버를 설치할 때 View Administrators 계정을 인증합니다. 로컬 Administrators 그룹, 도메인 사용자 또는 그룹 계정을 지정할 수 있습니다. View에서는 복제된 View 연결 서버 인스턴스를 설치할 수 있는 권한을 포함하여 전체 View 관리 권한을 이 계정에만 할당합니다. 도메인 사용자 또는 그룹을 지정할 경우, 설치 관리자를 실행하기 전에 Active Directory에 계정을 생성해야 합니다.

새 구성을 사용하여 View 연결 서버 설치

복제된 View 연결 서버 인스턴스 그룹의 단일 서버 또는 첫 번째 인스턴스로 View 연결 서버를 설치하려면 표준 설치 옵션을 사용합니다.

표준 설치 옵션을 선택하면 설치 중 새 로컬 View LDAP 구성이 생성됩니다. 설치 중 스키마 정의, Directory Information Tree(DIT) 정의 및 ACL이 로드되고 데이터가 초기화됩니다.

설치 후 View Administrator를 사용하여 대부분의 View LDAP 구성 데이터를 관리합니다. View 연결 서버는 일부 View LDAP 항목을 자동으로 관리합니다.

View 연결 서버 소프트웨어는 replica server, 보안 서버, View Composer, View Agent, View Client 또는 View 전송 서버 등 다른 View Manager 소프트웨어 구성 요소가 있는 동일 가상 또는 물리적 시스템에 함께 있을 수 없습니다.

새로운 구성을 적용하여 View 연결 서버를 설치할 때 고객 경험 개선 프로그램에 참여할 수 있습니다. VMware 는 사용자의 요구에 대한 VMware 의 응답을 개선하기 위해 사용자의 배포 상황에 대한 익명 데이터를 수집합니다. 조직을 식별할 수 있는 데이터는 수집되지 않습니다. 설치 중 이 옵션을 선택 취소하여 참여를 선택하지 않을 수 있습니다. 설치 후 참여에 대한 생각이 바뀌는 경우, View Administrator 에서 제품 라이센싱과 사용 페이지를 편집하여 프로그램에 참여하거나 탈퇴할 수 있습니다. 익명 필드를 포함하여 데이터가 수집되는 필드 목록을 검토하려면 *VMware View 관리* 문서에서 "고객 경험 개선 프로그램에서 수집되는 정보"를 참조하십시오.

필수 조건

- View 연결 서버를 설치할 Windows Server 컴퓨터에 관리자 권한을 가진 도메인 사용자로 로그인할 수 있는지 확인합니다.
- "View Connection Server 요구 사항," (7 페이지)에 설명된 설치 요구 사항을 충족하는지 확인하십시오.
- 설치 환경을 준비하십시오. "View 연결 서버의 설치 전제 조건," (42 페이지)의 내용을 참조하십시오.
- View Administrators 계정으로 도메인 사용자 또는 그룹을 인증할 경우, Active Directory 에 도메인 계정을 생성했는지 확인하십시오.
- 데이터 복구 암호를 준비합니다. View 연결 서버를 백업하는 경우, View LDAP 구성이 암호화된 LDIF 데이터로 내보내집니다. 암호화된 백업 View 구성을 복원하려면 데이터 복구 암호를 제공해야 합니다. 암호에는 1 ~ 128 문자를 포함시켜야 합니다. 안전한 암호 생성에 권장되는 조직의 모범 사례를 따르십시오.

  중요 BCDR(Business Continuity and Disaster Recovery) 시나리오에서 View 작동을 유지하고 운영 중단을 방지하기 위해 데이터 복구 암호가 필요합니다. View 연결 서버를 설치할 때 암호와 함께 암호 알림을 제공할 수 있습니다.

- View 연결 서버 인스턴스의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. "View 연결 서버의 방화벽 규칙," (58 페이지)의 내용을 참조하십시오.
- 보안 서버를 이 View 연결 서버 인스턴스와 쌍으로 구성하려는 경우, 활성 프로파일에서 고급 보안을 포함한 Windows 방화벽이 **켜기**로 설정되었는지 확인합니다. 모든 프로파일에 대해 이 설정을 **켜기**로 설정하는 것이 좋습니다. 기본적으로, IPsec 규칙은 보안 서버와 View 연결 서버 사이의 연결을 관리하고 고급 보안을 포함한 Windows 방화벽의 사용을 요구합니다.
- 해당 네트워크 토폴로지에 보안 서버와 View 연결 서버 인스턴스 사이의 백엔드 방화벽이 포함된 경우, IPsec 을 지원하도록 방화벽을 구성해야 합니다. "IPsec 을 지원하도록 백엔드 방화벽 구성," (58 페이지)의 내용을 참조하십시오.

프로시저

1 http://www.vmware.com/products/의 VMware 제품 페이지에서 View 연결 서버 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드합니다.

  설치 관리자 파일 이름은 `VMware-viewconnectionserver-x86_64-`*y.y.y*`-`*xxxxxx*`.exe` 입니다. 여기서 *xxxxxx* 는 빌드 번호이며 *y.y.y* 는 버전 번호입니다.

2 View 연결 서버 설치 프로그램을 시작하려면 설치 관리자 파일을 두 번 클릭합니다.

3 VMware 사용 약관에 동의하십시오.

4 대상 폴더를 허용 또는 변경하십시오.

5 View Standard Server 설치 옵션을 선택합니다.

6 데이터 복구 암호를 입력하고, 필요에 따라 암호 알림을 지정합니다.

7 Windows 방화벽 서비스의 구성 방법을 선택합니다.

옵션	조치
자동으로 Windows 방화벽 구성	설치 관리자에서 Windows 방화벽을 구성해 필요한 네트워크 연결을 허용합니다.
Windows 방화벽 구성 안 함	Windows 방화벽 규칙을 수동으로 구성합니다. 해당 조직이 Windows 방화벽 구성에 고유한 사전 정의 규칙을 사용하는 경우에만 이 옵션을 선택합니다.

8 View Administrator 계정을 인증하십시오.

이 계정의 구성원만 View Administrator에 로그인하고 전체 View 관리 권한을 실행하고, 복제된 View 연결 서버 인스턴스 및 기타 View servers를 설치할 수 있습니다.

옵션	설명
로컬 Administrators 그룹 인증	로컬 Administrators 그룹의 사용자가 View를 관리할 수 있도록 허용합니다.
특정 도메인 사용자 또는 도메인 그룹 인증	지정된 도메인 사용자 또는 그룹이 View를 관리할 수 있도록 허용합니다.

9 도메인 View Administrator 계정을 지정했고 도메인 계정에 액세스하지 않고 로컬 관리자 또는 다른 사용자로 설치 관리자를 실행 중인 경우, 인증된 사용자 이름 및 암호를 사용하여 도메인에 로그인할 수 있도록 자격 증명을 제공하십시오.

domain name₩*user name* 또는 UPN 형식을 사용하십시오. UPN은 *user@domain.com*의 형식으로 되어 있습니다.

10 고객 경험 개선 프로그램에 참여할지 여부를 선택합니다.

참여하는 경우, 본인의 의사에 따라 해당 조직의 유형, 규모 및 위치를 선택할 수 있습니다.

11 설치 마법사를 완료하여 View 연결 서버 설치를 마칩니다.

12 Windows Server 컴퓨터에서 새 패치가 있는지 확인하고 필요에 따라 Windows 업데이트를 실행합니다.

View 연결 서버를 설치하기 전에 Windows Server 컴퓨터에 완벽하게 패치를 적용했더라도 설치 시에 운영 체제 기능이 처음으로 활성화되었을 수 있습니다. 따라서 현재 추가 패치가 필요할 수도 있습니다.

Windows Server 컴퓨터에 VMware View 서비스가 설치되었습니다.

- VMware View 연결 서버
- VMware View Framework 구성 요소
- VMware View Message Bus 구성 요소
- VMware View Script Host
- VMware View Security Gateway 구성 요소
- VMware View PCoIP Secure Gateway
- VMware View Web 구성 요소
- View LDAP 디렉터리 서비스를 제공하는 VMware VDMDS

이러한 서비스에 대한 자세한 내용을 보려면 *VMware View 관리* 문서를 참조하십시오.

후속 작업

View 연결 서버를 위한 SSL 서버 인증서를 구성하십시오. 7 장, "View Servers 를 위한 SSL 인증서 구성," (71 페이지)의 내용을 참조하십시오.

View 연결 서버에서 초기 구성을 수행합니다. 8 장, "처음으로 View 구성," (85 페이지)의 내용을 참조하십시오.

View 연결 서버 인스턴스 및 보안 서버를 배포할 경우 View 연결 서버 설치 관리자 파일을 실행하여 각 서버 인스턴스를 설치해야 합니다.

Windows Server 2008 운영 체제에 View 연결 서버를 다시 설치할 것이고 성능 데이터를 모니터하도록 데이터 수집기 세트를 구성한 경우 데이터 수집기 세트를 중지했다가 다시 시작합니다.

View 연결 서버 자동 설치

Microsoft Windows Installer 의 자동 설치(MSI) 기능을 사용하여 여러 Windows 컴퓨터에 View 연결 서버 표준 설치를 수행할 수 있습니다. 자동 설치 시에는 명령줄을 사용하고 마법사 메시지에 응답할 필요가 없습니다.

자동 설치를 통해 대기업에서 효율적으로 View 구성 요소를 배포할 수 있습니다.

필수 조건

- View 연결 서버를 설치할 Windows Server 컴퓨터에 관리자 권한을 가진 도메인 사용자로 로그인할 수 있는지 확인합니다.
- "View Connection Server 요구 사항," (7 페이지).
- 설치 환경을 준비하십시오. "View 연결 서버의 설치 전제 조건," (42 페이지)을 참조하십시오.
- View Administrators 계정으로 도메인 사용자 또는 그룹을 인증할 경우, Active Directory 에 도메인 계정을 생성했는지 확인하십시오.
- View 연결 서버 인스턴스의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. "View 연결 서버의 방화벽 규칙," (58 페이지)을 참조하십시오.
- 보안 서버를 이 View 연결 서버 인스턴스와 쌍으로 구성하려는 경우, 활성 프로파일에서 고급 보안을 포함한 Windows 방화벽이 **켜짐**으로 설정되었는지 확인합니다. 모든 프로파일에 대해 이 설정을 **켜짐**으로 설정하는 것이 좋습니다. 기본적으로, IPsec 규칙은 보안 서버와 View 연결 서버 사이의 연결을 관리하고 고급 보안을 포함한 Windows 방화벽의 사용을 요구합니다.
- 해당 네트워크 토폴로지에 보안 서버와 View 연결 서버 인스턴스 사이의 백엔드 방화벽이 포함된 경우, IPsec 을 지원하도록 방화벽을 구성해야 합니다. "IPsec 을 지원하도록 백엔드 방화벽 구성," (58 페이지)을 참조하십시오.
- View 연결 서버를 설치할 Windows 컴퓨터에는 MSI 런타임 엔진 버전 2.0 이상이 있어야 합니다. 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.
- MSI 설치 관리자 명령줄 옵션을 숙지하십시오. "Microsoft Windows Installer 명령줄 옵션," (59 페이지)을 참조하십시오.
- View 연결 서버의 표준 설치에 사용할 수 있는 자동 설치 속성에 익숙해지십시오. "View 연결 서버 표준 설치의 자동 설치 속성," (46 페이지)을 참조하십시오.

프로시저

1 http://www.vmware.com/products/의 VMware 제품 페이지에서 View 연결 서버 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드합니다.

   설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-*y.y.y-xxxxxx*.exe 입니다. 여기서 *xxxxxx* 는 빌드 번호이며 *y.y.y* 는 버전 번호입니다.

2 Windows Server 컴퓨터에서 명령 프롬프트를 엽니다.

3 설치 명령을 한 줄에 입력하십시오.

```
예: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1
VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini
VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""
```

중요 자동 설치를 수행하는 경우, 데이터 복구 암호를 포함한 전체 명령줄이 설치 관리자의 vminst.log 파일에 기록됩니다. 설치가 완료되면 View Administrator 를 사용하여 이 로그 파일을 삭제하거나 데이터 복구 암호를 변경합니다.

4 Windows Server 컴퓨터에서 새 패치가 있는지 확인하고 필요에 따라 Windows 업데이트를 실행합니다.

View 연결 서버를 설치하기 전에 Windows Server 컴퓨터에 완벽하게 패치를 적용했더라도 설치 시에 운영 체제 기능이 처음으로 활성화되었을 수 있습니다. 따라서 현재 추가 패치가 필요할 수도 있습니다.

Windows Server 컴퓨터에 VMware View 서비스가 설치되었습니다. 자세한 내용은 "새 구성을 사용하여 View 연결 서버 설치," (42 페이지)를 참조하십시오.

후속 작업

View 연결 서버를 위한 SSL 서버 인증서를 구성하십시오. 7 장, "View Servers 를 위한 SSL 인증서 구성," (71 페이지)을 참조하십시오.

View 를 처음으로 구성하는 경우, View 연결 서버에서 초기 구성을 수행합니다. 8 장, "처음으로 View 구성," (85 페이지)을 참조하십시오.

View 연결 서버 표준 설치의 자동 설치 속성

명령줄에서 자동 설치를 수행할 때 특정 View 연결 서버 속성이 포함될 수 있습니다. Microsoft Windows Installer(MSI)에서 속성 및 값을 해석할 수 있도록 하려면 *PROPERTY=value* 형식을 사용해야 합니다.

표 5-1. 표준 설치에서 View 연결 서버를 자동 설치하기 위한 MSI 속성

MSI 속성	설명	기본값
INSTALLDIR	View 연결 서버 소프트웨어가 설치된 경로 및 폴더입니다. 예: INSTALLDIR=""D:₩abc₩my folder"" 경로를 둘러싼 큰 따옴표 두 개 세트를 사용하면 MSI 설치 관리자에서 공백을 유효한 경로 부분으로 해석합니다.	%ProgramFiles%₩VMware₩VMware View₩Server
VDM_SERVER_INSTANCE_TYPE	View server 설치 유형: ■ **1**. 표준 설치 ■ **2**. 복제 설치 ■ **3**. 보안 서버 설치 ■ **4**. View 전송 서버 설치 예를 들어, 표준 설치를 수행하려면 VDM_SERVER_INSTANCE_TYPE=1 을 정의합니다.	1
FWCHOICE	View 연결 서버 인스턴스의 방화벽을 구성할지 여부를 결정하는 MSI 속성입니다. 1 의 값은 방화벽을 구성합니다. 2 의 값은 방화벽을 구성하지 않습니다. 예: FWCHOICE=1	1

표 5-1. 표준 설치에서 View 연결 서버를 자동 설치하기 위한 MSI 속성 (계속)

MSI 속성	설명	기본값
VDM_INITIAL_ADMIN_SID	View 의 전체 관리 권한으로 인증된 초기 View Administrators 사용자 또는 그룹의 SID 입니다. 기본값은 View 연결 서버 컴퓨터에 있는 로컬 Administrators 그룹의 SID 입니다. 도메인 사용자 또는 그룹 계정의 SID 를 지정할 수 있습니다.	S-1-5-32-544
VDM_SERVER_RECOVERY_PWD	데이터 복구 암호. View LDAP 에서 데이터 복구 암호가 설정되지 않은 경우, 이 속성은 필수입니다. 암호에는 1 ~ 128 자가 포함되어야 합니다. 안전한 암호 생성에 권장되는 조직의 모범 사례를 따르십시오.	없음
VDM_SERVER_RECOVERY_PWD_REMINDER	데이터 복구 암호 알림입니다. 이 속성은 선택 사항입니다.	없음

View 연결 서버의 복제된 인스턴스 설치

기존 View 연결 서버 인스턴스를 복제한 View 연결 서버 인스턴스를 1 개 이상 추가 설치해 가용성을 향상하고 로드 밸런싱을 제공할 수 있습니다. 복제본을 설치한 다음에는 기존 및 새로 설치된 View 연결 서버 인스턴스가 동일합니다.

복제된 인스턴스를 설치할 때 View Manager 가 기존 View 연결 서버 인스턴스에서 View LDAP 구성 데이터를 복제합니다.

설치 이후에는 View Manager 소프트웨어가 복제된 그룹에 있는 모든 View 연결 서버 인스턴스에서 동일한 View LDAP 구성 데이터를 유지 관리합니다. 인스턴스 1 개에서 내용을 변경하면 다른 인스턴스에 업데이트 정보가 복사됩니다.

복제된 인스턴스가 잘못된 경우 그룹의 다른 인스턴스에서 작업을 계속합니다. 잘못된 인스턴스가 다시 작업을 시작하면 운영을 중단했던 동안 변경된 구성이 업데이트됩니다.

참고 Active Directory 와 동일한 복제 기술을 사용하는 View LDAP 에서 복제 기능을 제공합니다.

Replica Server 소프트웨어는 보안 서버, View 연결 서버, View Composer, View Agent, View Client 또는 View 전송 서버 등 다른 View Manager 소프트웨어 구성 요소가 있는 동일 가상 또는 물리적 시스템에 함께 있을 수 없습니다.

필수 조건

- 네트워크에 View 연결 서버 인스턴스가 1 개 이상 설치 및 구성되어 있는지 확인하십시오.
- 복제된 인스턴스를 설치하려면 View Administrator 역할을 가진 사용자로 로그인해야 합니다. View 연결 서버의 첫 번째 인스턴스를 설치할 때 View Administrator 역할을 가진 계정 또는 그룹을 지정합니다. 이 역할은 로컬 Administrators 그룹, 도메인 사용자 또는 그룹에 할당될 수 있습니다. "새 구성을 사용하여 View 연결 서버 설치," (42 페이지)의 내용을 참조하십시오.
- 기존 View 연결 서버 인스턴스가 복제된 인스턴스가 아닌 다른 도메인에 있는 경우, 도메인 사용자는 기존 인스턴스가 설치된 Windows Server 컴퓨터에 대해서도 View Administrator 권한을 가지고 있어야 합니다.
- "View Connection Server 요구 사항," (7 페이지)에 설명된 설치 요구 사항을 충족하는지 확인하십시오.
- 복제된 View 연결 서버 인스턴스가 설치된 컴퓨터와 고성능 LAN 을 통해 연결되어 있는지 확인하십시오. "복제된 View Connection Server 인스턴스의 네트워크 요구 사항," (9 페이지)의 내용을 참조하십시오.

- 설치 환경을 준비하십시오. "View 연결 서버의 설치 전제 조건," (42 페이지)의 내용을 참조하십시오.
- View 5.1 이상인 복제된 View 연결 서버 인스턴스를 설치하면서 복제하는 기존 View 연결 서버 인스턴스가 View 5.0.*x* 이전인 경우, 데이터 복구 암호를 준비하십시오. "새 구성을 사용하여 View 연결 서버 설치," (42 페이지)의 내용을 참조하십시오.
- View 연결 서버 인스턴스의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. "View 연결 서버의 방화벽 규칙," (58 페이지)의 내용을 참조하십시오.
- 보안 서버를 이 View 연결 서버 인스턴스와 쌍으로 구성하려는 경우, 활성 프로파일에서 고급 보안을 포함한 Windows 방화벽이 **켜기**로 설정되었는지 확인합니다. 모든 프로파일에 대해 이 설정을 **켜기**로 설정하는 것이 좋습니다. 기본적으로, IPsec 규칙은 보안 서버와 View 연결 서버 사이의 연결을 관리하고 고급 보안을 포함한 Windows 방화벽의 사용을 요구합니다.
- 해당 네트워크 토폴로지에 보안 서버와 View 연결 서버 인스턴스 사이의 백엔드 방화벽이 포함된 경우, IPsec 을 지원하도록 방화벽을 구성해야 합니다. "IPsec 을 지원하도록 백엔드 방화벽 구성," (58 페이지)의 내용을 참조하십시오.

프로시저

1 http://www.vmware.com/products/의 VMware 제품 페이지에서 View 연결 서버 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드합니다.

   설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-*y.y.y-xxxxxx*.exe 입니다. 여기서 *xxxxxx* 는 빌드 번호이며 *y.y.y* 는 버전 번호입니다.

2 View 연결 서버 설치 프로그램을 시작하려면 설치 관리자 파일을 두 번 클릭합니다.

3 VMware 사용 약관에 동의하십시오.

4 대상 폴더를 허용 또는 변경하십시오.

5 View Replica Server 설치 옵션을 선택하십시오.

6 복제한 기존 View 연결 서버 인스턴스의 호스트 이름 또는 IP 주소를 입력하십시오.

7 데이터 복구 암호를 입력하고, 필요에 따라 암호 알림을 지정합니다.

   복제 중인 기존 View 연결 서버 인스턴스가 View 5.0.*x* 이전인 경우에만 데이터 복구 암호를 묻는 메시지가 표시됩니다.

8 Windows 방화벽 서비스의 구성 방법을 선택합니다.

옵션	조치
자동으로 Windows 방화벽 구성	설치 관리자에서 Windows 방화벽을 구성해 필요한 네트워크 연결을 허용합니다.
Windows 방화벽 구성 안 함	Windows 방화벽 규칙을 수동으로 구성합니다. 해당 조직이 Windows 방화벽 구성에 고유한 사전 정의 규칙을 사용하는 경우에만 이 옵션을 선택합니다.

9 복제된 인스턴스 설치를 종료하려면 설치 마법사를 완료하십시오.

10 Windows Server 컴퓨터에서 새 패치가 있는지 확인하고 필요에 따라 Windows 업데이트를 실행합니다.

   View 연결 서버를 설치하기 전에 Windows Server 컴퓨터에 완벽하게 패치를 적용했더라도 설치 시에 운영 체제 기능이 처음으로 활성화되었을 수 있습니다. 따라서 현재 추가 패치가 필요할 수도 있습니다.

Windows Server 컴퓨터에 VMware View 서비스가 설치되었습니다.

- VMware View 연결 서버
- VMware View Framework 구성 요소
- VMware View Message Bus 구성 요소
- VMware View Script Host
- VMware View Security Gateway 구성 요소
- VMware View PCoIP Secure Gateway
- VMware View Web 구성 요소
- View LDAP 디렉터리 서비스를 제공하는 VMware VDMDS

이러한 서비스에 대한 자세한 내용을 보려면 *VMware View 관리* 문서를 참조하십시오.

후속 작업

View 연결 서버 인스턴스에 대해 SSL 서버 인증서를 구성합니다. 7 장, "View Servers 를 위한 SSL 인증서 구성," (71 페이지)의 내용을 참조하십시오.

View 연결 서버의 복제된 인스턴스에서 초기 View 구성을 수행할 필요가 없습니다. 복제된 인스턴스는 기존 View 연결 서버 인스턴스의 구성을 상속합니다.

그러나, 이 View 연결 서버 인스턴스에 대한 클라이언트 연결 설정을 구성해야 할 수 있으며 대규모 배포를 지원하도록 Windows Server 설정을 조정할 수 있습니다. "View Client 연결 구성," (97 페이지) 및 Windows Server 설정을 크기 조정하여 배포 지원을 참조하십시오.

Windows Server 2008 운영 체제에 View 연결 서버를 다시 설치할 것이고 성능 데이터를 모니터하도록 데이터 수집기 세트를 구성한 경우 데이터 수집기 세트를 중지했다가 다시 시작합니다.

View 연결 서버의 복제된 인스턴스 자동 설치

MSI(Microsoft Windows Installer)의 자동 설치 기능을 사용해 여러 Windows 컴퓨터에 View 연결 서버의 복제된 인스턴스를 설치할 수 있습니다. 자동 설치 시에는 명령줄을 사용하고 마법사 메시지에 응답할 필요가 없습니다.

자동 설치를 통해 대기업에서 효율적으로 View 구성 요소를 배포할 수 있습니다.

필수 조건

- 네트워크에 View 연결 서버 인스턴스가 1 개 이상 설치 및 구성되어 있는지 확인하십시오.
- 복제된 인스턴스를 설치하려면 View Administrator 계정에 액세스할 수 있는 자격 증명을 가진 사용자로 로그인해야 합니다. View 연결 서버의 첫 번째 인스턴스를 설치할 때 View Administrator 계정을 지정합니다. 이 계정은 로컬 Administrators 그룹, 도메인 사용자 또는 그룹 계정이 될 수 있습니다. "새 구성을 사용하여 View 연결 서버 설치," (42 페이지)를 참조하십시오.
- 기존 View 연결 서버 인스턴스가 복제된 인스턴스가 아닌 다른 도메인에 있는 경우, 도메인 사용자는 기존 인스턴스가 설치된 Windows Server 컴퓨터에 대해서도 View Administrator 권한을 가지고 있어야 합니다.
- "View Connection Server 요구 사항," (7 페이지).
- 복제된 View 연결 서버 인스턴스가 설치된 컴퓨터와 고성능 LAN 을 통해 연결되어 있는지 확인하십시오. 자세한 내용은 "복제된 View Connection Server 인스턴스의 네트워크 요구 사항," (9 페이지).
- 설치 환경을 준비하십시오. 자세한 내용은 "View 연결 서버의 설치 전제 조건," (42 페이지).

- View 연결 서버 인스턴스의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. 자세한 내용은 "View 연결 서버의 방화벽 규칙," (58 페이지).
- 보안 서버를 이 View 연결 서버 인스턴스와 쌍으로 구성하려는 경우, 활성 프로파일에서 고급 보안을 포함한 Windows 방화벽이 **켜짐**으로 설정되었는지 확인합니다. 모든 프로파일에 대해 이 설정을 **켜짐**으로 설정하는 것이 좋습니다. 기본적으로, IPsec 규칙은 보안 서버와 View 연결 서버 사이의 연결을 관리하고 고급 보안을 포함한 Windows 방화벽의 사용을 요구합니다.
- 해당 네트워크 토폴로지에 보안 서버와 View 연결 서버인스턴스 사이의 백엔드 방화벽이 포함된 경우, IPsec 을 지원하도록 방화벽을 구성해야 합니다. "IPsec 을 지원하도록 백엔드 방화벽 구성," (58 페이지)을 참조하십시오.
- MSI 설치 관리자 명령줄 옵션을 숙지하십시오. 자세한 내용은 "Microsoft Windows Installer 명령줄 옵션," (59 페이지).
- View 연결 서버의 복제본 설치에서 사용할 수 있는 자동 설치 속성을 숙지하십시오. 자세한 내용은 "View 연결 서버의 복제된 인스턴스 자동 설치 속성," (51 페이지).

프로시저

1 http://www.vmware.com/products/의 VMware 제품 페이지에서 View 연결 서버 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드합니다.

   설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-*y.y.y-xxxxxx*.exe 입니다. 여기서 *xxxxxx* 는 빌드 번호이며 *y.y.y* 는 버전 번호입니다.

2 Windows Server 컴퓨터에서 명령 프롬프트를 엽니다.

3 설치 명령을 한 줄에 입력하십시오.

   예: VMware-viewconnectionserver-*y.y.y-xxxxxx*.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544"

   View 5.1 이상인 복제된 View 연결 서버 인스턴스를 설치하면서 복제하는 기존 View 연결 서버 인스턴스가 View 5.0.*x* 이전인 경우, 데이터 복구 암호를 지정해야 하며 암호 알림을 추가할 수 있습니다. 예: VMware-viewconnectionserver-*y.y.y-xxxxxx*.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car""

   중요 자동 설치를 수행하는 경우, 데이터 복구 암호를 포함한 전체 명령줄이 설치 관리자의 vminst.log 파일에 기록됩니다. 설치가 완료되면 View Administrator 를 사용하여 이 로그 파일을 삭제하거나 데이터 복구 암호를 변경합니다.

4 Windows Server 컴퓨터에서 새 패치가 있는지 확인하고 필요에 따라 Windows 업데이트를 실행합니다.

   View 연결 서버를 설치하기 전에 Windows Server 컴퓨터에 완벽하게 패치를 적용했더라도 설치 시에 운영 체제 기능이 처음으로 활성화되었을 수 있습니다. 따라서 현재 추가 패치가 필요할 수도 있습니다.

Windows Server 컴퓨터에 VMware View 서비스가 설치되었습니다. 자세한 내용은 "View 연결 서버의 복제된 인스턴스 설치," (47 페이지).

후속 작업

View 연결 서버 인스턴스에 대해 SSL 서버 인증서를 구성합니다. 7 장, "View Servers 를 위한 SSL 인증서 구성," (71 페이지)을 참조하십시오.

View 연결 서버의 복제된 인스턴스에서 초기 View 구성을 수행할 필요가 없습니다. 복제된 인스턴스는 기존 View 연결 서버 인스턴스의 구성을 상속합니다.

그러나, 이 View 연결 서버 인스턴스에 대한 클라이언트 연결 설정을 구성해야 할 수 있으며 대규모 배포를 지원하도록 Windows Server 설정을 조정할 수 있습니다. "View Client 연결 구성," (97 페이지) 및 Windows Server 설정을 크기 조정하여 배포 지원을 참조하십시오.

View 연결 서버의 복제된 인스턴스 자동 설치 속성

명령줄에서 복제된 View 연결 서버 인스턴스를 자동 설치할 때 특정 속성이 포함될 수 있습니다. Microsoft Windows Installer(MSI)에서 속성 및 값을 해석할 수 있도록 하려면 *PROPERTY=value* 형식을 사용해야 합니다.

표 5-2. View 연결 서버의 복제된 인스턴스 자동 설치를 위한 MSI 속성

MSI 속성	설명	기본값
INSTALLDIR	View 연결 서버 소프트웨어가 설치된 경로 및 폴더입니다. 예: INSTALLDIR=""D:₩abc₩my folder"" 경로를 둘러싼 큰 따옴표 두 개 세트를 사용하면 MSI 설치 관리자에서 공백을 유효한 경로 부분으로 해석합니다. 이 MSI 속성은 선택 사항입니다.	%ProgramFiles%₩VMware₩VMware View₩Server
VDM_SERVER_INSTANCE_TYPE	View server 설치 유형: ■ **1**. 표준 설치 ■ **2**. 복제 설치 ■ **3**. 보안 서버 설치 ■ **4**. View 전송 서버 설치 복제된 인스턴스를 설치하려면 VDM_SERVER_INSTANCE_TYPE=2 를 정의하십시오. 이 MSI 속성은 복제본 설치 시 필수입니다.	1
ADAM_PRIMARY_NAME	복제 중인 기존 View 연결 서버 인스턴스의 호스트 이름이나 IP 주소입니다. 예: ADAM_PRIMARY_NAME=cs1.companydomain.com 이 MSI 속성은 필수입니다.	없음
ADAM_PRIMARY_PORT	복제 중인 기존 View 연결 서버 인스턴스의 View LDAP 포트입니다. 예: ADAM_PRIMARY_PORT=cs1.companydomain.com 이 MSI 속성은 선택 사항입니다.	없음
FWCHOICE	View 연결 서버 인스턴스의 방화벽을 구성할지 여부를 결정하는 MSI 속성입니다. 1 의 값은 방화벽을 구성합니다. 2 의 값은 방화벽을 구성하지 않습니다. 예: FWCHOICE=1 이 MSI 속성은 선택 사항입니다.	1
VDM_SERVER_RECOVERY_PWD	데이터 복구 암호. View LDAP 에서 데이터 복구 암호가 설정되지 않은 경우, 이 속성은 필수입니다. **참고** 복제 중인 표준 View 연결 서버 인스턴스가 View 5.0 이전인 경우, View LDAP 에서 데이터 복구 암호가 설정되지 않습니다. 복제 중인 View 연결 서버 인스턴스가 View 5.1 이상인 경우에는 이 속성을 제공할 필요가 없습니다. 암호에는 1 ~ 128 자가 포함되어야 합니다. 안전한 암호 생성에 권장되는 조직의 모범 사례를 따르십시오.	없음
VDM_SERVER_RECOVERY_PWD_REMINDER	데이터 복구 암호 알림입니다. 이 속성은 선택 사항입니다.	없음

보안 서버 연결 암호 구성

보안 서버를 설치하기 전에 보안 서버 연결 암호를 구성해야 합니다. 설치하는 동안 View 연결 서버 설치 프로그램에서 사용자에게 암호를 묻습니다.

보안 서버 연결 암호는 보안 서버와 View 연결 서버 인스턴스를 연결하는 일회성 암호입니다. View 연결 서버 설치 프로그램에 암호를 입력하면 해당 암호는 더 이상 사용할 수 없습니다.

참고 이전 버전의 보안 서버와 현재 버전의 View 연결 서버를 쌍으로 구성할 수 없습니다. 현재 버전의 View 연결 서버에서 연결 암호를 구성하고 이전 버전의 보안 서버를 설치하려고 하면 연결 암호가 유효하지 않게 됩니다.

프로시저

1 View Administrator 에서 **View 구성 > 서버**.

2 View Servers 창에서 보안 서버와 연결할 View 연결 서버 인스턴스를 선택하십시오.

3 **추가 명령** 드롭다운 메뉴에서 **보안 서버 연결 암호 지정**을 선택하십시오.

4 연결 암호와 암호 확인 텍스트 상자에 암호를 입력하고 암호 시간 초과 값을 지정하십시오.

지정된 제한 시간 내에 암호를 사용해야 합니다.

5 암호를 구성하려면 **확인**을 클릭합니다.

후속 작업

보안 서버를 설치합니다. 다음을 참조: "보안 서버 설치," (52 페이지).

중요 암호 제한 시간 내에 View 연결 서버 설치 프로그램에 보안 서버 연결 암호를 입력하지 않으면 암호는 더 이상 유효하지 않으므로 새 암호를 구성해야 합니다.

보안 서버 설치

보안 서버는 인터넷과 내부 네트워크 사이에 보안 계층을 추가하는 View 연결 서버 인스턴스입니다. View 연결 서버 인스턴스에 연결될 수 있도록 보안 서버를 1 개 이상 설치할 수 있습니다.

보안 서버 소프트웨어는 replica server, View 연결 서버, View Composer, View Agent, View Client 또는 View 전송 서버 등 다른 View Manager 소프트웨어 구성 요소가 있는 동일 가상 또는 물리적 시스템에 함께 있을 수 없습니다.

필수 조건

- 사용할 토폴로지 유형을 지정하십시오. 예를 들어 사용할 로드 밸런싱 솔루션을 지정하십시오. 보안 서버에 연결한 View 연결 서버 인스턴스를 외부 네트워크 사용자 전용으로 사용할 것인지 결정하십시오. 자세한 내용은 *VMware View 아키텍처 계획* 설명서를 참조하십시오.

  중요 로드 밸런서를 사용할 경우, 로드 밸런서 및 각 보안 서버에 정적 IP 주소가 있어야 합니다. 예를 들어, 보안 서버가 2 대인 로드 밸런서를 사용할 경우 3 개의 정적 IP 주소가 필요합니다.

- "View Connection Server 요구 사항," (7 페이지)에 설명된 설치 요구 사항을 충족하는지 확인하십시오.
- 설치 환경을 준비하십시오. "View 연결 서버의 설치 전제 조건," (42 페이지)의 내용을 참조하십시오.

- 보안 서버에 연결할 View 연결 서버 인스턴스가 View 연결 서버 4.6 이상에 설치되고 구성 및 실행되고 있는지 확인하십시오. View 4.6 이상 보안 서버에 이전 버전의 View 연결 서버를 연결할 수 없습니다.
- 보안 서버에 연결할 View 연결 서버 인스턴스에서 보안 서버를 설치할 컴퓨터에 액세스할 수 있는지 확인하십시오.
- 보안 서버 연결 암호를 구성하십시오. "보안 서버 연결 암호 구성," (52 페이지)의 내용을 참조하십시오.
- 외부 URL 형식을 숙지하십시오. "PCoIP 보안 게이트웨이 및 터널 연결용 외부 URL 구성," (99 페이지)의 내용을 참조하십시오.
- 활성 프로파일에서 고급 보안을 포함한 Windows 방화벽이 **켜기**로 설정되었는지 확인합니다. 모든 프로파일에 대해 이 설정을 **켜기**로 설정하는 것이 좋습니다. 기본적으로, IPsec 규칙은 보안 서버와 View 연결 서버 사이의 연결을 관리하고 고급 보안을 포함한 Windows 방화벽의 사용을 요구합니다.
- 보안 서버의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. "View 연결 서버의 방화벽 규칙," (58 페이지)의 내용을 참조하십시오.
- 해당 네트워크 토폴로지에 보안 서버와 View 연결 서버 사이에 백엔드 방화벽이 포함된 경우, IPsec을 지원하도록 방화벽을 구성해야 합니다. "IPsec 을 지원하도록 백엔드 방화벽 구성," (58 페이지)의 내용을 참조하십시오.
- 보안 서버를 업그레이드 또는 다시 설치하는 경우, 보안 서버의 기존 IPsec 규칙이 제거되었는지 확인하십시오. "보안 서버 업그레이드 또는 재설치 준비," (57 페이지)의 내용을 참조하십시오.

프로시저

1 http://www.vmware.com/products/의 VMware 제품 페이지에서 View 연결 서버 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드합니다.

   설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-*y.y.y-xxxxxx*.exe 입니다. 여기서 *xxxxxx*는 빌드 번호이며 *y.y.y*는 버전 번호입니다.

2 View 연결 서버 설치 프로그램을 시작하려면 설치 관리자 파일을 두 번 클릭합니다.

3 VMware 사용 약관에 동의하십시오.

4 대상 폴더를 허용 또는 변경하십시오.

5 **View 보안 서버** 설치 옵션을 선택하십시오.

6 보안 서버에 연결할 View 연결 서버 인스턴스의 정규화된 도메인 이름 또는 IP 주소를 **서버** 텍스트 상자에 입력하십시오.

   보안 서버에서 이 View 연결 서버 인스턴스에 네트워크 트래픽을 전송합니다.

7 암호 텍스트 상자에 보안 서버 연결 암호를 입력하십시오.

   암호가 만료된 경우 View Administrator 를 사용해 새 암호를 구성하고 설치 프로그램에 새 암호를 입력할 수 있습니다.

8 RDP 또는 PCoIP 디스플레이 프로토콜을 사용하는 View Client 보안 서버의 외부 URL 을 **외부 URL** 텍스트 상자에 입력하십시오.

   URL 에는 프로토콜, 클라이언트 확인 가능한 보안 서버 이름 및 포트 번호가 포함되어야 합니다. 네트워크 외부에서 실행하는 터널 클라이언트는 이 URL 을 사용해 보안 서버에 연결합니다.

   예: `https://view.example.com:443`

9 PCoIP 디스플레이 프로토콜을 사용하는 View Client 보안 서버의 외부 URL 을 **PCoIP 외부 URL** 텍스트 상자에 입력하십시오.

포트 번호 4172 를 가진 IP 주소로 PCoIP 외부 URL 을 지정합니다. 프로토콜 이름은 포함시키지 마십시오.

예: 10.20.30.40:4172

URL 에는 클라이언트 시스템에서 보안 서버에 연결할 때 사용하는 IP 주소와 포트 번호가 포함되어 있어야 합니다. PCoIP 보안 게이트웨이가 보안 서버에 설치된 경우에만 텍스트 상자에 입력할 수 있습니다.

10 Windows 방화벽 서비스의 구성 방법을 선택합니다.

옵션	조치
자동으로 Windows 방화벽 구성	설치 관리자에서 Windows 방화벽을 구성해 필요한 네트워크 연결을 허용합니다.
Windows 방화벽 구성 안 함	Windows 방화벽 규칙을 수동으로 구성합니다. 해당 조직이 Windows 방화벽 구성에 고유한 사전 정의 규칙을 사용하는 경우에만 이 옵션을 선택합니다.

11 보안 서버 설치를 종료하려면 설치 마법사를 완료하십시오.

Windows Server 컴퓨터에 보안 서버 서비스가 설치됩니다.

- VMware View 보안 서버
- VMware View Framework 구성 요소
- VMware View Security Gateway 구성 요소
- VMware View PCoIP Secure Gateway

이들 서비스에 대한 자세한 내용은 *VMware View 관리*를 참조하십시오.

View Administrator 의 보안 서버 창에 보안 서버가 나타납니다.

참고 설치가 취소 또는 중단되는 경우, 설치를 다시 시작하기 위해 먼저 보안 서버에 대한 IPsec 규칙을 제거해야 할 수 있습니다. 보안 서버를 다시 설치하거나 업그레이드하기 전에 이미 IPsec 규칙을 제거한 경우에도 이 단계를 따르십시오. IPsec 규칙의 제거에 대한 내용은 "보안 서버 업그레이드 또는 재설치 준비," (57 페이지)를 참조하십시오. .

후속 작업

보안 서버를 위한 SSL 서버 인증서를 구성합니다. 7 장, "View Servers 를 위한 SSL 인증서 구성," (71 페이지)의 내용을 참조하십시오.

보안 서버에 대한 클라이언트 연결 설정을 구성해야 할 수 있으며 대규모 배포를 지원하도록 Windows Server 설정을 조정할 수 있습니다. "View Client 연결 구성," (97 페이지) 및 Windows Server 설정을 크기 조정하여 배포 지원을 참조하십시오.

Windows Server 2008 운영 체제에 보안 서버를 다시 설치하고 성능 데이터를 모니터링하도록 데이터 수집기를 구성한 경우 데이터 수집기 설정을 중지하고 다시 시작합니다.

보안 서버 자동 설치

MSI(Microsoft Windows Installer)의 자동 설치 기능을 사용해 여러 Windows 컴퓨터에 보안 서버를 설치할 수 있습니다. 자동 설치 시에는 명령줄을 사용하고 마법사 메시지에 응답할 필요가 없습니다.

자동 설치를 통해 대기업에서 효율적으로 View 구성 요소를 배포할 수 있습니다.

필수 조건

- 사용할 토폴로지 유형을 지정하십시오. 예를 들어 사용할 로드 밸런싱 솔루션을 지정하십시오. 보안 서버에 연결한 View 연결 서버 인스턴스를 외부 네트워크 사용자 전용으로 사용할 것인지 결정하십시오. 자세한 내용은 *VMware View 아키텍처 계획* 설명서를 참조하십시오.

  중요 로드 밸런서를 사용할 경우, 로드 밸런서 및 각 보안 서버에 정적 IP 주소가 있어야 합니다. 예를 들어, 보안 서버가 2 대인 로드 밸런서를 사용할 경우 3 개의 정적 IP 주소가 필요합니다.

- "View Connection Server 요구 사항," (7 페이지).
- 설치 환경을 준비하십시오. "View 연결 서버의 설치 전제 조건," (42 페이지)을 참조하십시오.
- 보안 서버에 연결할 View 연결 서버 인스턴스가 View 연결 서버 4.6 이상에 설치되고 구성 및 실행되고 있는지 확인하십시오. View 4.6 이상 보안 서버에 이전 버전의 View 연결 서버를 연결할 수 없습니다.
- 보안 서버에 연결할 View 연결 서버 인스턴스에서 보안 서버를 설치할 컴퓨터에 액세스할 수 있는지 확인하십시오.
- 보안 서버 연결 암호를 구성하십시오. "보안 서버 연결 암호 구성," (52 페이지)을 참조하십시오.
- 외부 URL 형식을 숙지하십시오. "PCoIP 보안 게이트웨이 및 터널 연결용 외부 URL 구성," (99 페이지)을 참조하십시오.
- 활성 프로파일에서 고급 보안을 포함한 Windows 방화벽이 **켜짐**으로 설정되었는지 확인합니다. 모든 프로파일에 대해 이 설정을 **켜짐**으로 설정하는 것이 좋습니다. 기본적으로, IPsec 규칙은 보안 서버와 View 연결 서버 사이의 연결을 관리하고 고급 보안을 포함한 Windows 방화벽의 사용을 요구합니다.
- 보안 서버의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. "View 연결 서버의 방화벽 규칙," (58 페이지)을 참조하십시오.
- 해당 네트워크 토폴로지에 보안 서버와 View 연결 서버 사이의 백엔드 방화벽이 포함된 경우, IPsec을 지원하도록 방화벽을 구성해야 합니다. "IPsec 을 지원하도록 백엔드 방화벽 구성," (58 페이지)을 참조하십시오.
- 보안 서버를 업그레이드 또는 다시 설치하는 경우, 보안 서버의 기존 IPsec 규칙이 제거되었는지 확인하십시오. "보안 서버 업그레이드 또는 재설치 준비," (57 페이지)를 참조하십시오.
- MSI 설치 관리자 명령줄 옵션을 숙지하십시오. "Microsoft Windows Installer 명령줄 옵션," (59 페이지)을 참조하십시오.
- 보안 서버에서 사용할 수 있는 자동 설치 속성을 숙지하십시오. "보안 서버 자동 설치 속성," (56 페이지)을 참조하십시오.

프로시저

1 http://www.vmware.com/products/의 VMware 제품 페이지에서 View 연결 서버 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드합니다.

  설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-*y.y.y-xxxxxx*.exe 입니다. 여기서 *xxxxxx*는 빌드 번호이며 *y.y.y*는 버전 번호입니다.

2 Windows Server 컴퓨터에서 명령 프롬프트를 엽니다.

3 설치 명령을 한 줄에 입력하십시오.

```
예: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3
VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443
VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 VDM_SERVER_SS_PCOIP_TCPPORT=4172
VDM_SERVER_SS_PCOIP_UDPPORT=4172 VDM_SERVER_SS_PWD=secret"
```

Windows Server 컴퓨터에 VMware View 서비스가 설치되었습니다. 자세한 내용은 "보안 서버 설치," (52 페이지).

참고 설치가 취소 또는 중단되는 경우, 설치를 다시 시작하기 전에 보안 서버의 IPsec 규칙을 설치 제거해야 할 수도 있습니다. 보안 서버를 다시 설치하거나 업그레이드하기 전에 이미 IPsec 규칙을 제거한 경우에도 이 단계를 따르십시오. IPsec 규칙 제거에 대한 설명은 "보안 서버 업그레이드 또는 재설치 준비," (57 페이지)를 참조하십시오.

후속 작업

보안 서버를 위한 SSL 서버 인증서를 구성합니다. 7 장, "View Servers 를 위한 SSL 인증서 구성," (71 페이지)을 참조하십시오.

보안 서버에 대한 클라이언트 연결 설정을 구성해야 할 수 있으며 대규모 배포를 지원하도록 Windows Server 설정을 조정할 수 있습니다. "View Client 연결 구성," (97 페이지) 및 Windows Server 설정을 크기 조정하여 배포 지원을 참조하십시오.

보안 서버 자동 설치 속성

명령줄에서 보안 서버를 자동 설치할 때 특정 속성이 포함될 수 있습니다. Microsoft Windows Installer(MSI)에서 속성 및 값을 해석할 수 있도록 하려면 *PROPERTY=value* 형식을 사용해야 합니다.

표 5-3. 보안 서버 자동 설치를 위한 MSI 속성

MSI 속성	설명	기본값
INSTALLDIR	View Connection Server 소프트웨어가 설치된 경로 및 폴더입니다. 예: INSTALLDIR=""D:₩abc₩my folder"" 경로를 둘러싼 큰 따옴표 두 개 세트를 사용하면 MSI 설치 관리자에서 공백을 유효한 경로 부분으로 해석합니다. 이 MSI 속성은 선택 사항입니다.	%ProgramFiles%₩VMware₩VMware View₩Server
VDM_SERVER_INSTANCE_TYPE	View Server 설치 유형: ■ 1. 표준 설치 ■ 2. 복제 설치 ■ 3. 보안 서버 설치 ■ 4. View Transfer Server 설치 보안 서버를 설치하려면 VDM_SERVER_INSTANCE_TYPE=3 을 정의하십시오. 이 MSI 속성은 보안 서버 설치 시 필수입니다.	1
VDM_SERVER_NAME	보안 서버와 연결할 기존 View Connection Server 인스턴스의 호스트 이름이나 IP 주소입니다. 예: VDM_SERVER_NAME=cs1.internaldomain.com 이 MSI 속성은 필수입니다.	없음
VDM_SERVER_SS_EXTURL	보안 서버의 외부 URL 입니다. URL 에는 프로토콜, 외부에서 확인 가능한 보안 서버 이름 및 포트 번호가 포함되어야 합니다. 예: VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443 이 MSI 속성은 필수입니다.	없음
VDM_SERVER_SS_PWD	보안 서버 연결 암호입니다. 예: VDM_SERVER_SS_PWD=secret 이 MSI 속성은 필수입니다.	없음
FWCHOICE	View Connection Server 인스턴스의 방화벽을 구성할지 여부를 결정하는 MSI 속성입니다. 1 의 값은 방화벽을 구성합니다. 2 의 값은 방화벽을 구성하지 않습니다. 예: FWCHOICE=1 이 MSI 속성은 선택 사항입니다.	1

표 5-3. 보안 서버 자동 설치를 위한 MSI 속성 (계속)

MSI 속성	설명	기본값
VDM_SERVER_SS_PCOIP_IPADDR	PCoIP 보안 게이트웨이 외부 IP 주소입니다. 이 속성은 보안 서버가 Windows Server 2008 R2 이상에 설치될 경우에만 지원됩니다. 예: VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 이 속성은 PCoIP Secure Gateway 구성 요소를 사용할 계획인 경우 필수입니다.	없음
VDM_SERVER_SS_PCOIP_TCPPORT	PCoIP 보안 게이트웨이 외부 TCP 포트 번호입니다. 이 속성은 보안 서버가 Windows Server 2008 R2 이상에 설치될 경우에만 지원됩니다. 예: VDM_SERVER_SS_PCOIP_TCPPORT=4172 이 속성은 PCoIP Secure Gateway 구성 요소를 사용할 계획인 경우 필수입니다.	없음
VDM_SERVER_SS_PCOIP_UDPPORT	PCoIP 보안 게이트웨이 외부 UDP 포트 번호입니다. 이 속성은 보안 서버가 Windows Server 2008 R2 이상에 설치될 경우에만 지원됩니다. 예: VDM_SERVER_SS_PCOIP_UDPPORT=4172 이 속성은 PCoIP Secure Gateway 구성 요소를 사용할 계획인 경우 필수입니다.	없음

보안 서버 업그레이드 또는 재설치 준비

View 5.1 보안 서버 인스턴스를 업그레이드하거나 다시 설치하려면 우선 보안 서버 및 함께 구성된 View 연결 서버 인스턴스 사이의 통신을 관리하는 현재 IPsec 규칙을 제거해야 합니다. 이 단계를 거치지 않으면 업그레이드 또는 재설치가 되지 않습니다.

중요 이 작업은 View 5.1 이후의 보안 서버에 해당하며 View 5.0.x 이전의 보안 서버에는 적용되지 않습니다.

기본적으로, 보안 서버 및 함께 구성된 View 연결 서버 인스턴스 사이의 통신은 IPsec 규칙으로 관리됩니다. 보안 서버를 업그레이드하거나 다시 설치하고 이를 View 연결 서버 인스턴스와 다시 연결하는 경우, 새 IPsec 규칙 집합을 구성해야 합니다. 업그레이드나 재설치 전에 기존 IPsec 규칙을 제거하지 않으면 서로 연결이 구성되지 않습니다.

보안 서버를 업그레이드 또는 재설치하고 IPsec 를 사용하여 보안 서버와 View 연결 서버 사이의 통신을 보호하려면 이 단계를 수행해야 합니다.

IPsec 규칙을 사용하지 않고 초기 보안 서버 연결을 구성할 수 있습니다. 보안 서버를 설치하기 전에 View Administrator 를 열고 기본적으로 선택된 **보안 서버 연결에 IPsec 사용** 전역 설정의 선택을 취소할 수 있습니다. IPsec 규칙이 적용되지 않는 경우에는 업그레이드나 재설치 전에 이를 제거할 필요가 없습니다.

참고 보안 서버를 업그레이드하거나 재설치하기 전에 View 에서 보안 서버를 제거할 필요가 없습니다. View 환경에서 영구적으로 보안 서버를 제거하려는 경우에만 이 단계를 수행합니다.

View 5.1 이전에는 View Administrator 에서, 혹은 `vdmadmin -S` 명령을 사용하여 보안 서버를 제거할 수 있었습니다. View 5.1 이상 릴리스에서는 `vdmadmin -S` 만 사용할 수 있습니다. *VMware View 관리* 문서에서 "-S 옵션을 사용하여 View 연결 서버 인스턴스 또는 보안 서버의 항목 제거"를 참조하십시오.

주의 활성 보안 서버에 대한 IPsec 규칙을 제거하는 경우, 보안 서버를 업그레이드하거나 다시 설치할 때까지 보안 서버와의 모든 통신이 끊어집니다.

프로시저

1 View Administrator 에서 **View 구성 > 서버**를 클릭합니다.

2 '보안 서버' 탭에서 **추가 명령 > 업그레이드 또는 다시 설치 준비**를 클릭합니다.

보안 서버를 설치하기 전에 IPsec 규칙 사용을 해제한 경우, 이 설정은 비활성 상태가 됩니다. 이 경우, 재설치 또는 업그레이드 전에 IPsec 규칙을 제거할 필요가 없습니다.

3 **확인**을 클릭합니다.

IPsec 규칙이 제거되고 **업그레이드 또는 다시 설치 준비** 설정이 비활성 상태가 되어 보안 서버를 재설치하거나 업그레이드할 수 있음을 나타냅니다.

후속 작업

보안 서버를 업그레이드하거나 다시 설치합니다.

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

IPsec 을 지원하도록 백엔드 방화벽 구성

해당 네트워크 토폴로지에서 보안 서버와 View 연결 서버 인스턴스 사이에 백엔드 방화벽이 포함된 경우, IPsec 을 지원하도록 방화벽에서 특정 프로토콜 및 포트를 구성해야 합니다. 적합하게 구성하지 않으면 보안 서버와 View 연결 서버 인스턴스 사이에서 보내지는 데이터가 방화벽을 통과하지 못합니다.

기본적으로, IPsec 규칙은 보안 서버와 View 연결 서버 인스턴스 사이의 연결을 관리합니다. IPsec 을 지원하기 위해 View 연결 서버 설치 관리자가 View servers 가 설치된 Windows Server 호스트에서 Windows 방화벽 규칙을 구성할 수 있습니다. 백엔드 방화벽의 경우, 사용자가 규칙을 직접 구성해야 합니다.

참고 IPsec 의 사용이 강력히 권장됩니다. 또 다른 방법으로, View Administrator 전역 설정인 **보안 서버 연결에 IPsec 사용**을 해제할 수 있습니다.

다음 규칙이 양방향 트래픽을 허용해야 합니다. 방화벽에서 인바운드 및 아웃바운드 트래픽에 개별 규칙을 지정해야 할 수도 있습니다.

네트워크 주소 변환(NAT)을 사용하는 방화벽과 NAT 를 사용하지 않는 방화벽에 서로 다른 규칙이 적용됩니다.

표 5-5. NAT 이외 방화벽의 IPsec 규칙 지원 요구 사항

소스	프로토콜	포트	대상	참고
보안 서버	ISAKMP	UDP 500	View 연결 서버	보안 서버는 UDP 포트 500 을 사용하여 IPsec 보안을 협상합니다.
보안 서버	ESP	해당 없음	View 연결 서버	ESP 프로토콜은 IPsec 암호화된 트래픽을 캡슐화합니다. 규칙의 일부로 ESP 에 대한 포트를 지정할 필요는 없습니다. 필요한 경우, 소스 및 대상 IP 주소를 지정하여 규칙의 범위를 줄일 수 있습니다.

다음 규칙은 NAT 를 사용하는 방화벽에 적용됩니다.

표 5-6. NAT 방화벽의 IPsec 규칙 지원 요구 사항

소스	프로토콜	포트	대상	참고
보안 서버	ISAKMP	UDP 500	View 연결 서버	보안 서버는 UDP 포트 500 을 사용하여 IPsec 보안 협상을 실행합니다.
보안 서버	NAT-T ISAKMP	UDP 4500	View 연결 서버	보안 서버는 UDP 포트 4500 을 사용하여 NAT 를 탐색하고 IPsec 보안을 협상합니다.

Microsoft Windows Installer 명령줄 옵션

View 구성 요소를 자동으로 설치하려면 Microsoft Windows Installer(MSI) 명령줄 옵션 및 속성을 사용해야 합니다. View 구성 요소 설치 관리자는 MSI 프로그램이며 표준 MSI 기능을 사용합니다. 또한 MSI 명령줄 옵션을 사용하여 View 구성 요소를 자동으로 제거할 수 있습니다.

MSI 에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오. MSI 명령줄 옵션은 Microsoft Developer Network(MSDN) Library 웹 사이트를 참조하여 MSI 명령줄 옵션을 검색합니다. MSI 명령줄 사용을 보려면 View 구성 요소 컴퓨터에서 명령 프롬프트를 열어 `msiexec /?`를 입력할 수 있습니다.

View 구성 요소 설치 관리자를 자동으로 실행하려면 설치 관리자를 임시 디렉토리로 추출하고 대화식 설치를 시작하는 부트스트랩 프로그램을 해제하여 시작합니다.

표 5-7 에는 설치 관리자의 부트스트랩 프로그램을 제어하는 명령줄 옵션이 표시됩니다.

표 5-7. View 구성 요소의 부트스트랩 프로그램의 명령줄 옵션

옵션	설명
/s	대화식 대화 상자를 디스플레이할 수 없는 부트스트랩 스플래시 화면 및 추출 대화 상자를 해제합니다. 예: VMware-viewconnectionserver-*y.y.y-xxxxxx*.exe /s 자동 설치를 실행하기 위해 /s 옵션이 필요합니다. 이 예에서 *xxxxxx*는 빌드 번호이고 *y.y.y*는 버전 번호입니다.
/v" *MSI_command_line_options*"	설치 관리자가 해석할 MSI의 옵션 집합으로 명령줄에 입력할 큰 따옴표로 닫힌 문자열을 전달하도록 지시합니다. 큰 따옴표 사이에 명령줄 항목을 넣어야 합니다. /v 뒤에 그리고 명령줄 끝에 큰 따옴표를 지정합니다. 예: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"*command_line_options*" MSI 설치 관리자가 공백을 포함하는 문자열을 해석하도록 지시하려면 두 세트의 큰 따옴표에 문자열을 지정합니다. 예를 들어 공백을 포함한 설치 경로 이름에 View 구성 요소를 설치할 수 있습니다. 예: VMware-viewconnectionserver-*y.y.y-xxxxxx*.exe /s /v"*command_line_options* INSTALLDIR=""d:\abc\my folder""" 이 예에서 MSI 설치 관리자는 설치 디렉토리 경로에서 전달하며 문자열을 두 개의 명령줄 옵션으로 해석하지 않습니다. 전체 명령줄을 둘러싼 마지막 큰 따옴표에 유의하십시오. 자동 설치를 실행하기 위해 /v"*command_line_options*" 옵션이 필요합니다.

MSI 설치 관리자 msiexec.exe에 명령줄 옵션 및 MSI 속성값을 전달하여 나머지 자동 설치를 제어합니다. MSI 설치 관리자에는 View 구성 요소의 설치 코드가 포함됩니다. 설치 관리자는 명령줄에 입력하는 값과 옵션을 사용하여 View 구성 요소에 특정한 설치 선택 사항 및 설치 옵션을 해석합니다.

표 5-8에는 MSI 설치 관리자에 전달된 명령줄 옵션 및 MSI 등록값이 표시됩니다.

표 5-8. MSI 명령줄 옵션 및 MSI 속성

MSI 옵션 또는 속성	설명
/qn	MSI 설치 관리자가 설치 관리자 마법사 페이지를 표시하지 않도록 지시합니다. 예를 들어 View Agent를 자동 설치하고 기본 설치 옵션 및 기능만 사용할 수 있습니다. VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn" 이 예에서 *xxxxxx*는 빌드 번호이고 *y.y.y*는 버전 번호입니다. 또는 /qb 옵션을 사용하여 자동화된 비대화식 설치에서 마법사 페이지를 표시할 수 있습니다. 설치가 진행될 때 마법사 페이지가 표시되지만 그에 응답할 수 없습니다. 자동 설치를 실행하기 위해 /qn 또는 /qb 옵션이 필요합니다.
INSTALLDIR	View 구성 요소의 다른 설치 경로를 지정합니다. *INSTALLDIR=path* 형식을 사용하여 설치 경로를 지정합니다. 기본 경로에 View 구성 요소를 설치할 경우 이 MSI 속성을 무시할 수 있습니다. 이 MSI 속성은 선택 사항입니다.
ADDLOCAL	설치할 구성 요소 특정 기능을 결정합니다. 대화식 설치에서 View 설치 관리자는 선택할 사용자 지정 설치 옵션을 표시합니다. MSI 속성 ADDLOCAL을 사용하여 이러한 설치 옵션을 명령줄에 지정할 수 있습니다. 사용할 수 있는 모든 사용자 지정 설치 옵션을 설치하려면 ADDLOCAL=ALL을 입력합니다. 예: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" MSI 속성 ADDLOCAL을 사용하지 않는 경우 기본 설치 옵션이 설치됩니다. 개별 설치 옵션을 지정하려면 쉼표로 구분된 설치 옵션 이름 목록을 입력합니다. 이름 사이에 공백을 사용하지 마십시오. *ADDLOCAL=value,value,value...* 형식을 사용하십시오. 예를 들어 View Composer Agent 및 PCoIP 기능을 사용하여 게스트 운영 체제에 View Agent를 설치할 수 있습니다. VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" **참고** View Agent에 Core 기능이 필요합니다. 이 MSI 속성은 선택 사항입니다.

표 5-8. MSI 명령줄 옵션 및 MSI 속성 (계속)

MSI 옵션 또는 속성	설명
REBOOT	REBOOT=ReallySuppress 옵션을 사용하여 시스템을 다시 부팅하기 전에 시스템 구성 작업을 완료할 수 있습니다. 이 MSI 속성은 선택 사항입니다.
/l*v *log_file*	자세한 출력으로 지정된 로그 파일에 로깅 정보를 작성합니다. 예: /l*v ""%TEMP%₩vmmsi.log"" 이 예는 대화식 설치 중 생성된 로그와 유사한 자세한 로그 파일을 생성합니다. 이 옵션을 사용하여 설치에 고유하게 적용할 수 있는 사용자 지정 기능을 기록할 수 있습니다. 기록된 정보를 사용하여 나중에 자동 설치 시 설치 기능을 지정할 수 있습니다. /l*v 옵션은 선택 사항입니다.

MSI 명령줄 옵션을 사용하여 View 제품 자동 제거

Microsoft Windows Installer(MSI) 명령줄 옵션을 사용하여 View 구성 요소를 제거할 수 있습니다.

구문

```
msiexec.exe
/qb
/x
product_code
```

옵션

/qb 옵션은 제거 진행 표시줄을 표시합니다. 제거 진행 표시줄을 표시하지 않으려면 /qb 옵션을 /qn 옵션으로 교체하십시오.

/x 옵션은 View 구성 요소를 제거합니다.

product_code 문자열은 MSI 제거 프로그램에 대해 View 구성 요소 제품 파일을 식별합니다. 설치 중 생성된 %TEMP%₩vmmsi.log 파일에서 ProductCode 를 검색하여 *product_code* 문자열을 찾을 수 있습니다.

MSI 명령줄 옵션에 대한 자세한 내용은 "Microsoft Windows Installer 명령줄 옵션," (59 페이지)에 나와 있습니다.

예

View Connection Server 인스턴스를 제거하십시오.

```
msiexec.exe /qb /x {D6184123-57B7-26E2-809B-090435A8C16A}
```

View Transfer Server 설치 6

View Transfer Server는 체크인, 체크아웃 및 복제 중 로컬 데스크톱 및 데이터 센터 사이에서 데이터를 전송합니다. View Transfer Server를 설치하려면 Windows Server 가상 시스템에 소프트웨어를 설치하고 View Manager 배포에 View Transfer Server를 추가하며 Transfer Server 저장소를 구성합니다.

클라이언트 컴퓨터에 View Client with Local Mode를 배포할 경우 View Transfer Server를 설치 및 구성해야 합니다.

View Transfer Server를 설치하고 로컬 데스크톱을 사용하려면 라이센스가 있어야 합니다.

1 View 전송 서버 설치(63 페이지)

   View 전송 서버는 시스템 이미지 파일을 다운로드하고 로컬 데스크톱과 데이터 센터의 해당 원격 데스크톱 사이에서 데이터를 동기화하며 사용자가 로컬 데스크톱을 체크인 및 체크아웃할 때 데이터를 전송합니다. Windows Server를 실행하는 가상 시스템에 View 전송 서버를 설치합니다.

2 View Manager에 View 전송 서버 추가(65 페이지)

   View 전송 서버와 View 연결 서버를 함께 사용해 로컬 데스크톱과 데이터 센터 간에 파일과 데이터를 전송합니다. View 전송 서버에서 이들 작업을 수행하기 전에 View Manager 배포에 View 전송 서버를 추가해야 합니다.

3 전송 서버 저장소 구성(66 페이지)

   전송 서버 저장소는 로컬 모드로 실행하는 연결된 클론 데스크톱에 대한 View Composer 기본 이미지를 저장합니다. View 전송 서버에 전송 서버 저장소에 대한 액세스 권한을 부여하려면 View Manager에서 이를 구성해야 합니다. View Composer 연결된 클론을 로컬 모드로 사용하지 않는 경우, 전송 서버 저장소를 구성할 필요가 없습니다.

4 View 전송 서버의 방화벽 규칙(67 페이지)

   View 전송 서버 인스턴스의 방화벽에 대해 특정 들어오는 TCP 포트를 열어야 합니다.

5 View Transfer Server 자동 설치(67 페이지)

   명령줄에 설치 관리자 파일 이름 및 설치 옵션을 입력하여 View Transfer Server를 자동으로 설치할 수 있습니다. 자동 설치를 사용하면 대기업에 View 구성 요소를 효과적으로 배포할 수 있습니다.

View 전송 서버 설치

View 전송 서버는 시스템 이미지 파일을 다운로드하고 로컬 데스크톱과 데이터 센터의 해당 원격 데스크톱 사이에서 데이터를 동기화하며 사용자가 로컬 데스크톱을 체크인 및 체크아웃할 때 데이터를 전송합니다. Windows Server를 실행하는 가상 시스템에 View 전송 서버를 설치합니다.

런타임에 View 전송 서버가 Apache Web Server에 배포됩니다. View 전송 서버를 설치할 경우 설치 관리자에서 Apache Web Server가 가상 시스템의 서비스로 구성됩니다. Apache 서비스는 80 및 443 포트를 사용합니다.

필수 조건

- View 전송 서버를 설치할 Windows Server 에서 로컬 관리자 권한을 갖고 있어야 합니다.
- "View Transfer Server 요구 사항," (12 페이지).
- View 전송 서버를 설치하려는 가상 시스템에서 PCI 디바이스를 수동으로 추가 또는 제거하지 않았는지 확인합니다. PCI 디바이스를 추가하거나 제거하는 경우, View 가 Hot-add 기능으로 추가된 디바이스를 발견하지 못하여 데이터 전송 작업이 수행되지 않을 수 있습니다.
- View 전송 서버를 설치하고 로컬 데스크톱을 사용하려면 라이센스가 있어야 합니다.
- View 연결 서버 인스턴스의 Windows 방화벽에 대해 열어야 하는 네트워크 포트를 숙지하십시오. 다음을 참조: "View 전송 서버의 방화벽 규칙," (67 페이지).

프로시저

1 http://www.vmware.com/products/의 VMware 제품 페이지에서 View 연결 서버 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드합니다.

   설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-*y.y.y-xxxxxx*.exe 입니다. 여기서 *xxxxxx* 는 빌드 번호이며 *y.y.y* 는 버전 번호입니다.

2 설치 프로그램을 시작하려면 설치 관리자 파일을 두 번 클릭합니다.

3 VMware 사용 약관에 동의하십시오.

4 대상 폴더를 허용 또는 변경하십시오.

5 **View 전송 서버**를 선택합니다.

6 View 전송 서버가 배포된 Apache Web Server 를 구성합니다.

   설치 관리자에서 제공하는 네트워크 도메인의 기본값, Apache Server 이름 및 관리자의 이메일 주소를 허용할 수 있습니다.

7 Windows 방화벽 서비스의 구성 방법을 선택합니다.

옵션	조치
자동으로 Windows 방화벽 구성	설치 관리자에서 Windows 방화벽을 구성해 필요한 네트워크 연결을 허용합니다.
Windows 방화벽 구성 안 함	Windows 방화벽 규칙을 수동으로 구성합니다.

8 설치 프로그램을 완료하여 View 전송 서버를 설치합니다.

VMware View 전송 서버, View 전송 서버 Control Service 및 VMware View Framework Component 서비스가 가상 시스템에 설치되어 시작됩니다.

후속 작업

View Administrator 에서 View 전송 서버를 View Manager 배포에 추가합니다.

View Manager 에 View 전송 서버 추가

View 전송 서버와 View 연결 서버를 함께 사용해 로컬 데스크톱과 데이터 센터 간에 파일과 데이터를 전송합니다. View 전송 서버에서 이들 작업을 수행하기 전에 View Manager 배포에 View 전송 서버를 추가해야 합니다.

View Manager 에 View 전송 서버 인스턴스를 여러 개 추가할 수 있습니다. 전송 서버 인스턴스는 하나의 공통 전송 서버 저장소에 액세스합니다. View 연결 서버 인스턴스 또는 복제된 View 연결 서버 인스턴스 그룹에서 관리하는 로컬 데스크톱의 전송 워크로드를 공유합니다.

참고 View 전송 서버가 View Manager 에 추가된 경우 DRS(Distributed Resource Scheduler) 자동화 정책이 수동으로 설정됩니다(DRS 를 효과적으로 해제함).

필수 조건

- Windows Server 가상 시스템에 View 전송 서버가 설치되어 있는지 확인하십시오.
- View Manager 에 vCenter Server 가 추가되었는지 확인하십시오. View Administrator 의 **View 구성 > 서버** 페이지에 View Manager 에 추가한 vCenter Server 인스턴스가 표시됩니다.
- View 전송 서버가 버전 5.1 이상이고 로컬 모드에서 연결된 클론 데스크톱을 사용하려는 경우, View 구성에서 복제된 모든 View 연결 서버 인스턴스가 버전 5.1 이상인지 확인하십시오. 이전 버전의 View 연결 서버가 전송 서버 저장소로 기본 이미지 게시 요청을 보내는 경우, View 전송 서버가 게시 작업을 수행할 수 없습니다.

프로시저

1 View Administrator 에서 **View 구성 > 서버**.

2 '전송 서버' 탭을 클릭하고 **추가**를 클릭합니다.

3 전송 서버 추가 마법사에서 View 전송 서버 가상 시스템을 관리하는 vCenter Server 인스턴스를 선택하고 **다음**을 클릭합니다.

4 View 전송 서버가 설치된 가상 시스템을 선택하고 **마침**을 클릭합니다.

   View 연결 서버에서 SCSI 컨트롤러 4 개로 가상 시스템을 재구성합니다. SCSI 컨트롤러를 여러 개 사용하면 View 전송 서버에서 보다 많은 디스크를 동시에 전송할 수 있습니다.

View Administrator 의 전송 서버 패널에 View 전송 서버 인스턴스가 나타납니다. 전송 서버 저장소를 구성하지 않은 경우에는 View 전송 서버 상태가 **보류 중**에서 **구성된 전송 서버 저장소가 없음**으로 변경됩니다. 전송 서버 저장소를 구성한 경우에는 상태가 **보류 중**에서 **전송 서버 저장소 초기화 중**을 거쳐 **준비**로 변경됩니다.

이 작업은 몇 분 정도 걸릴 수 있습니다. View Administrator 에서 새로 고침 단추를 클릭하면 현재 상태를 확인할 수 있습니다.

View Manager 에 View 전송 서버 인스턴스를 추가하는 경우 View 전송 서버 가상 시스템에서 Apache 서비스가 시작됩니다.

주의 View 전송 서버 가상 시스템이 하드웨어 7 이전 버전이면 View Manager 에 View 전송 서버를 추가한 후에 View 전송 서버 가상 시스템에 고정 IP 를 구성해야 합니다.

View 전송 서버 가상 시스템에 SCSI 컨트롤러를 여러 개 추가하는 경우에는 Windows 가 고정 IP 주소를 제거하고 DHCP 을 사용하는 가상 시스템을 재구성합니다. 가상 시스템을 다시 시작한 이후에 가상 시스템에 고정 IP 주소를 다시 입력해야 합니다.

전송 서버 저장소 구성

전송 서버 저장소는 로컬 모드로 실행하는 연결된 클론 데스크톱에 대한 View Composer 기본 이미지를 저장합니다. View 전송 서버에 전송 서버 저장소에 대한 액세스 권한을 부여하려면 View Manager 에서 이를 구성해야 합니다. View Composer 연결된 클론을 로컬 모드로 사용하지 않는 경우, 전송 서버 저장소를 구성할 필요가 없습니다.

전송 서버 저장소를 구성하기 전에 View Manager 에 View 전송 서버가 구성되면 구성 작업을 진행하는 동안 View 전송 서버에서 전송 서버 저장소 위치를 검사합니다.

이 View Manager 배포에 View 전송 서버 인스턴스를 여러 개 추가하려면 네트워크 공유에 전송 서버 저장소를 구성하십시오. 다른 View 전송 서버 인스턴스는 단일 View 전송 서버 인스턴스의 로컬 드라이브에 구성된 전송 서버 저장소에 액세스할 수 없습니다.

전송 서버 저장소 크기가 View Composer 에서 생성한 기본 이미지를 저장할 수 있을 정도로 큰지 확인하십시오. 기본 이미지 크기는 몇 기가바이트에 달할 수 있습니다.

네트워크 공유에 원격 전송 서버 저장소를 구성하는 경우에는 네트워크 공유에 액세스할 수 있도록 자격 증명을 가진 사용자 ID 을 제공해야 합니다. 전송 서버 저장소에 대한 액세스 보안을 강화하려면 네트워크 액세스를 View 관리자로 제한하는 것이 좋습니다.

필수 조건

- Windows Server 가상 시스템에 View 전송 서버가 설치되어 있는지 확인하십시오.
- View Manager 에 View 전송 서버가 추가되었는지 확인하십시오. 다음을 참조: "View Manager 에 View 전송 서버 추가," (65 페이지).

참고 전송 서버 저장소를 구성하기 전에 View Manager 에 View 전송 서버를 추가하는 것이 모범 사례이지만 필수 조건은 아닙니다.

프로시저

1 전송 서버 저장소에 대한 경로와 폴더를 구성하십시오.

전송 서버 저장소는 로컬 드라이브 또는 네트워크 공유에 위치할 수 있습니다.

옵션	조치
로컬 전송 서버 저장소	View 전송 서버가 설치된 가상 시스템에서 전송 서버 저장소에 대한 경로와 폴더를 생성하십시오. 예: C:₩TransferRepository₩
원격 전송 서버 저장소	네트워크 공유에 대한 UNC 경로를 구성하십시오. 예: ₩₩server.domain.com₩TransferRepository₩ View Manager 배포에 추가한 모든 View 전송 서버 인스턴스에서 공유 드라이브에 대한 네트워크 액세스 권한을 가지고 있어야 합니다.

2 View Administrator 에서 **View 구성 > 서버**.

3 모든 View 전송 서버 인스턴스를 유지 관리 모드로 설정하십시오.

a 전송 서버 패널에서 View 전송 서버 인스턴스를 선택합니다.

b **유지 관리 모드 설정**을 클릭하고 **확인**을 클릭합니다.

View 전송 서버 상태가 **유지 관리 모드**로 바뀝니다.

c 각 인스턴스에 대해 단계 3a 및 단계 3b 를 반복하십시오.

모든 View 전송 서버 인스턴스가 유지 관리 모드로 설정되면 현재 전송 작업이 중지됩니다.

4 전송 서버 저장소 페이지의 일반 패널에서 **편집**을 클릭합니다.

5 전송 서버 저장소 위치와 기타 정보를 입력하십시오.

옵션	설명
네트워크 공유	■ **경로** 구성한 UNC 경로를 입력하십시오. ■ **사용자 이름**. 네트워크 공유에 대한 액세스 자격 증명을 가진 관리자의 사용자 ID 를 입력하십시오. ■ **암호** 관리자 암호를 입력하십시오. ■ **도메인** 네트워크 공유의 도메인 이름을 NetBIOS 형식으로 입력하십시오. .com 접미사를 사용하지 마십시오.
로컬 파일 시스템	로컬 View 전송 서버 가상 시스템에서 구성한 경로를 입력하십시오.

6 **확인**을 클릭합니다.

저장소 네트워크 경로 또는 로컬 드라이브가 잘못된 경우에는 전송 서버 저장소 편집 대화 상자에 오류 메시지가 표시되고 위치 구성 작업을 진행할 수 없습니다. 유효한 위치를 입력해야 합니다.

7 **View 구성 > 서버** 페이지에서 View 전송 서버 인스턴스를 선택하고 **유지 관리 모드 종료**를 클릭합니다.

View 전송 서버 상태가 **준비**로 바뀝니다.

View 전송 서버의 방화벽 규칙

View 전송 서버 인스턴스의 방화벽에 대해 특정 들어오는 TCP 포트를 열어야 합니다.

설치 프로그램에서 사용자에게 필요한 Windows 방화벽 규칙을 선택적으로 구성할 수 있습니다.

표 6-1 에는 View 전송 서버 인스턴스의 방화벽에 대해 열어야 하는 들어오는 TCP 포트 목록이 나와 있습니다.

표 6-1. 전송 서버 인스턴스의 TCP 포트

프로토콜	포트
HTTP	80
HTTPS	443

View Transfer Server 자동 설치

명령줄에 설치 관리자 파일 이름 및 설치 옵션을 입력하여 View Transfer Server 를 자동으로 설치할 수 있습니다. 자동 설치를 사용하면 대기업에 View 구성 요소를 효과적으로 배포할 수 있습니다.

View 전송 서버를 자동 설치하도록 그룹 정책 설정

View 전송 서버를 자동으로 설치하려면 상승된 권한으로 설치할 수 있도록 Microsoft Windows 그룹 정책을 구성해야 합니다.

로컬 컴퓨터의 컴퓨터 및 사용자를 위한 Windows Installer 그룹 정책을 설정해야 합니다.

필수 조건

View 전송 서버를 설치할 Windows Server 컴퓨터에서 로컬 관리자 권한을 갖고 있어야 합니다.

프로시저

1 Windows Server 컴퓨터에 로그인하고 **시작 > 실행을 클릭합니다.**.

2 **gpedit.msc** 를 입력하고 **확인**을 클릭합니다.

3 그룹 정책 개체 편집기에서 **로컬 컴퓨터 정책 > 컴퓨터 구성**.

4 **관리 템플릿**을 확장하고 Windows **구성 요소**를 확장한 다음 Windows Installer 폴더를 열고 **항상 상승된 권한으로 설치**를 두 번 클릭합니다.

5 **항상 상승된 권한으로 설치 속성** 창에서 **사용**을 클릭하고 **확인**을 클릭합니다.

6 왼쪽 창에서 **사용자 구성**을 클릭합니다.

7 **관리 템플릿**을 확장하고 Windows **구성 요소**를 확장한 다음 Windows Installer 폴더를 열고 **항상 상승된 권한으로 설치**를 두 번 클릭합니다.

8 **항상 상승된 권한으로 설치 속성** 창에서 **사용**을 클릭하고 **확인**을 클릭합니다.

후속 작업

View 전송 서버를 자동으로 설치합니다.

View 전송 서버 자동 설치

Microsoft Windows Installer의 자동 설치(MSI) 기능을 사용하여 여러 Windows 컴퓨터에 View 전송 서버를 설치할 수 있습니다. 자동 설치 시에는 명령줄을 사용하고 마법사 메시지에 응답할 필요가 없습니다.

필수 조건

- View 전송 서버를 설치할 Windows Server에서 로컬 관리자 권한을 갖고 있어야 합니다.
- "View Transfer Server 요구 사항," (12 페이지).
- View 전송 서버를 설치하고 로컬 데스크톱을 사용하려면 라이센스가 있어야 합니다.
- View 전송 서버를 설치할 가상 시스템에는 MSI 런타임 엔진 버전 2.0 이상이 있어야 합니다. 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.
- MSI 설치 관리자 명령줄 옵션을 숙지하십시오. 다음을 참조: "Microsoft Windows Installer 명령줄 옵션," (59 페이지).
- View 전송 서버와 사용할 수 있는 자동 설치 속성에 익숙해지십시오. 다음을 참조: "View Transfer Server 자동 설치 속성," (69 페이지).
- 자동 설치에 필요한 Windows Installer 그룹 정책이 Windows Server 컴퓨터에 구성되어 있어야 합니다. 다음을 참조: "View 전송 서버를 자동 설치하도록 그룹 정책 설정," (67 페이지).

프로시저

1 http://www.vmware.com/products/의 VMware 제품 페이지에서 View 연결 서버 설치 관리자 파일을 Windows Server 컴퓨터에 다운로드합니다.

   설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-*y.y.y*-*xxxxxx*.exe 입니다. 여기서 *xxxxxx*는 빌드 번호이며 *y.y.y*는 버전 번호입니다.

2 Windows Server 컴퓨터에서 명령 프롬프트를 엽니다.

3 설치 명령을 한 줄에 입력하십시오.

   예: VMware-viewconnectionserver-*y.y.y*-*xxxxxx*.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=4"

VMware View 전송 서버, View 전송 서버 Control Service 및 VMware View Framework Component 서비스가 가상 시스템에 설치되어 시작됩니다.

후속 작업

View Administrator에서 View 전송 서버를 View Manager 배포에 추가합니다.

View Transfer Server 자동 설치 속성

명령줄에서 View Transfer Server 를 자동 설치할 때 특정 속성이 포함될 수 있습니다. Microsoft Windows Installer(MSI)에서 속성 및 값을 해석할 수 있도록 하려면 *PROPERTY=value* 형식을 사용해야 합니다.

표 6-2. View Transfer Server 를 자동 설치하기 위한 MSI 속성

MSI 속성	설명	기본값
INSTALLDIR	View Connection Server 소프트웨어가 설치된 경로 및 폴더입니다. 예: INSTALLDIR=""D:₩abc₩my folder"" 경로를 둘러싼 큰 따옴표 두 개 세트를 사용하면 MSI 설치 관리자에서 공백을 유효한 경로 부분으로 해석합니다. 이 MSI 속성은 선택 사항입니다.	%ProgramFiles%₩VMware₩VMware View₩Server
VDM_SERVER_INSTANCE_TYPE	View Server 설치 유형: ■ **1**. 표준 설치 ■ **2**. 복제 설치 ■ **3**. 보안 서버 설치 ■ **4**. View Transfer Server 설치 View Transfer Server 를 설치하려면 VDM_SERVER_INSTANCE_TYPE=4 를 정의하십시오. 이 MSI 속성은 표준 설치의 선택 사항입니다. 다른 모든 유형의 설치에 필요합니다.	1
SERVERDOMAIN	View Transfer Server 를 설치할 가상 시스템의 네트워크 도메인입니다. 이 값은 대화식 설치 중 구성되는 Apache Web Server 네트워크 도메인과 일치합니다. 예: SERVERDOMAIN=companydomain.com MSI 속성 SERVERDOMAIN 을 사용하여 사용자 지정 Apache Web Server 도메인을 지정할 경우 사용자 지정 SERVERNAME 및 SERVERADMIN 속성도 지정해야 합니다. 이 MSI 속성은 선택 사항입니다.	없음
SERVERNAME	View Transfer Server 를 설치할 가상 시스템의 호스트 이름입니다. 이 값은 대화식 설치 중 구성되는 Apache Web Server 호스트 이름과 일치합니다. 예: SERVERNAME=ts1.companydomain.com MSI 속성 SERVERNAME 을 사용하여 사용자 지정 Apache Web Server 도메인을 지정할 경우 사용자 지정 SERVERDOMAIN 및 SERVERADMIN 속성도 지정해야 합니다. 이 MSI 속성은 선택 사항입니다.	없음
SERVERADMIN	View Transfer Server 와 함께 구성되는 Apache Web Server 의 관리자 이메일 주소입니다. 예: SERVERADMIN=admin@companydomain.com MSI 속성 SERVERADMIN 을 사용하여 사용자 지정 Apache Web Server 관리자를 지정할 경우 사용자 지정 SERVERDOMAIN 및 SERVERNAME 속성도 지정해야 합니다. 이 MSI 속성은 선택 사항입니다.	없음
FWCHOICE	View Connection Server 인스턴스의 방화벽을 구성할지 여부를 결정하는 MSI 속성입니다. 1 의 값은 방화벽을 구성합니다. 2 의 값은 방화벽을 구성하지 않습니다. 예: FWCHOICE=1 이 MSI 속성은 선택 사항입니다.	1

View Servers 를 위한 SSL 인증서 구성 7

VMware 는 View 연결 서버 인스턴스, 보안 서버 및 View Composer 서비스 인스턴스의 인증을 위한 SSL 인증서 구성을 강력히 권장합니다.

기본 SSL 서버 인증서는 View 연결 서버 인스턴스, 보안 서버 또는 View Composer 인스턴스를 설치할 때 생성됩니다. 테스트 용도로 기본 인증서를 사용할 수 있습니다.

중요 가능한 한 빨리 기본 인증서를 교체합니다. 기본 인증서는 인증 기관(CA)에 의해 서명되지 않습니다. CA 에서 서명하지 않은 인증서를 사용하여 신뢰할 수 없는 사용자가 서버로 가장하여 트래픽을 인터셉트할 수 있습니다

이 장에서는 다음 주제에 대해 설명합니다.

View Servers 를 위한 SSL 인증서 이해

View servers 및 관련 구성 요소에 대해 SSL 인증서를 구성하기 위한 특정 가이드라인을 따라야 합니다.

View 연결 서버 및 보안 서버

SSL 은 View Client 에서 View 에 연결하기 위해 필요합니다. SSL 연결을 종료시키는 클라이언트 쪽 View 연결 서버 인스턴스, 보안 서버 및 중간 서버에 SSL 서버 인증서가 필요합니다.

기본적으로, View 연결 서버 또는 보안 서버를 설치할 때 설치 과정에서 View server 에 자체 서명된 인증서가 생성됩니다. 그러나, 다음의 경우에는 설치 과정에서 기존 인증서가 사용됩니다.

- Windows 인증서 저장소에 `vdm` 의 이름을 가진 유효한 인증서가 이미 있는 경우
- 이전 릴리스에서 View 5.1 이상으로 업그레이드하고 Windows Server 컴퓨터에서 유효한 keystore 파일이 구성된 경우 설치 과정에서 키와 인증서를 추출하여 Windows 인증서 저장소로 가져옵니다.

vCenter Server 및 View Composer

운영 환경에서 View Manager 에 vCenter Server 및 View Composer 를 추가하기 전에 vCenter Server 와 View Composer 가 CA 에서 서명한 인증서를 사용하는지 확인합니다.

vCenter Server 에 대한 기본 인증서를 교체하기 위한 내용은 *vSphere 예제 및 시나리오* 문서를 참조하십시오.

동일 Windows Server 호스트에 vCenter Server 와 View Composer 를 설치하는 경우, 동일 SSL 인증서의 사용이 가능하지만 각 구성 요소에 대해 개별적으로 인증서를 구성해야 합니다.

View 전송 서버

View 5.1 이상을 설치하는 경우에는 View 전송 서버에 대해 SSL 인증서를 구성할 필요가 없습니다.

View Client 와의 보조 연결을 처리하기 위해 View 연결 서버가 사용하는 View 전송 서버에는 자체 서명된 기본 인증서가 설치됩니다. "View 전송 서버 및 SSL 인증서," (83 페이지)의 내용을 참조하십시오.

추가 가이드라인

CA 에서 서명한 SSL 인증서의 요청 및 사용에 관한 일반 정보는 "CA 에서 서명한 SSL 인증서를 사용할 때의 이점," (83 페이지)을 참조하십시오.

View Client 가 View 연결 서버 인스턴스나 보안 서버에 연결하는 경우, View server 의 SSL 서버 인증서 및 신뢰 체인에 있는 모든 중간 인증서가 제공됩니다. 서버 인증서를 신뢰하려면 클라이언트 시스템에 서명 CA 의 루트 인증서가 설치되어 있어야 합니다.

View 연결 서버가 vCenter Server 및 View Composer 와 통신하는 경우, View 연결 서버에 SSL 서버 인증서와 이러한 서버의 중간 인증서가 제공됩니다. vCenter Server 및 View Composer 서버를 신뢰하려면 View 연결 서버 컴퓨터에 서명 CA 의 루트 인증서가 설치되어 있어야 합니다.

SSL 인증서 설정 작업 개요

View servers 에 대한 SSL 서버 인증서를 설정하려면 몇 가지 중요한 작업을 수행해야 합니다.

이러한 작업 수행을 위한 절차는 본 개요 이후에 나오는 항목에서 설명합니다.

1 CA 에서 새로운 서명 SSL 인증서를 가져와야 하는지 확인합니다.

조직에 이미 유효한 SSL 서버 인증서가 있는 경우 해당 인증서를 사용하여 View 연결 서버, 보안 서버 또는 View Composer 에서 제공하는 기본 SSL 서버 인증서를 교체할 수 있습니다. 기존 인증서를 사용하려면 동봉된 개인 키도 필요합니다.

시작 위치	조치
조직에서 유효한 SSL 서버 인증서를 제공했습니다.	2 단계로 바로 이동합니다.
SSL 서버 인증서가 없습니다.	CA 를 통해 서명된 SSL 서버 인증서를 구하십시오.

2 View server 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 SSL 인증서를 가져옵니다.

3 View 연결 서버 인스턴스와 보안 서버의 경우 인증서 이름을 **vdm** 으로 수정합니다.

이름 **vdm** 을 각 View server 호스트에 있는 하나의 인증서에만 할당합니다.

4 View 연결 서버 컴퓨터에서, Windows Server 호스트가 루트 인증서를 신뢰하지 않는 경우 루트 인증서를 Windows 로컬 컴퓨터의 인증서 저장소로 가져옵니다.

View 연결 서버 인스턴스에 대해서만 이 단계를 수행합니다. View Composer, vCenter Server 또는 보안 서버 호스트로 루트 인증서를 가져올 필요가 없습니다.

5 중간 CA 가 서버 인증서에 서명한 경우, 중간 인증서를 Windows 로컬 컴퓨터의 인증서 저장소로 가져옵니다.

클라이언트 구성을 단순화하기 위해 전체 인증서 체인을 Windows 로컬 컴퓨터의 인증서 저장소로 가져옵니다. View server 에서 중간 인증서가 누락된 경우, View Administrator 를 실행하는 컴퓨터 및 View Client 에 대해 이 인증서를 구성해야 합니다.

6 View Composer 인스턴스의 경우, 다음 단계 중 하나만 수행합니다.

- View Composer 를 설치하기 전에 인증서를 Windows 로컬 컴퓨터의 인증서 저장소로 가져오는 경우, View Composer 설치 과정에서 해당 인증서를 선택할 수 있습니다.
- View Composer 설치 후 기존 인증서 또는 자체 서명된 기본 인증서를 새 인증서로 대체하려는 경우, `SviConfig ReplaceCertificate` 유틸리티를 실행하여 새 인증서를 View Composer 에서 사용하는 포트에 바인딩합니다.

7 해당 CA 가 잘 알려지지 않은 경우, 루트 및 중간 인증서를 신뢰하도록 View Client 를 구성합니다.

또한 View Administrator 를 실행하는 컴퓨터도 루트 및 중간 인증서를 신뢰하도록 합니다.

8 인증서 해지 확인을 재구성할지 여부를 결정합니다.

View 연결 서버가 View servers, View Composer 및 vCenter Server 에서 인증서 해지 확인을 수행합니다. CA 에서 서명한 대부분의 인증서에 인증서 해지 정보가 포함되어 있습니다. 해당 CA 에 이 정보가 포함되지 않은 경우, 인증서의 해지를 확인하지 않도록 서버를 구성할 수 있습니다.

CA 로부터 서명된 SSL 인증서 얻기

조직에서 SSL 서버 인증서를 제공하지 않는 경우, CA 에서 서명한 새 인증서를 요청해야 합니다.

서명된 새 인증서를 얻기 위한 몇 가지 방법을 사용할 수 있습니다. 예를 들어, Microsoft Internet Information Services(IIS) Manager 를 사용하여 CA 로부터 SSL 서버 인증서를 요청할 수 있습니다. 신뢰할 수 없는 루트를 기반으로 한 무료 임시 인증서를 많은 CA 에서 테스트 용도로 구할 수 있습니다.

컴퓨터에서 인증서 요청을 생성할 때는 개인 키가 생성되는지도 확인하십시오. SSL 서버 인증서를 얻고 이를 Windows 로컬 컴퓨터의 인증서 저장소로 가져오는 경우, 인증서에 대응하는 개인 키도 함께 있어야 합니다.

중요 Windows Server 2008 엔터프라이즈 CA 이상과만 호환되는 인증서 템플릿을 사용하여 View servers 인증서를 만들지 마십시오.

인증서 얻기에 관한 일반 정보는 MMC 의 인증서 스냅인에 제공되는 Microsoft 온라인 도움말을 참조하십시오. 컴퓨터에 인증서 스냅인이 아직 설치되지 않은 경우 "MMC 에 인증서 스냅인 추가," (75 페이지)를 참조하십시오.

Windows 도메인 또는 Enterprise CA 로부터 서명된 인증서 얻기

Windows 도메인 또는 Enterprise CA 로부터 서명된 인증서를 얻으려면 Windows 인증서 저장소의 Windows 인증서 등록 마법사를 사용할 수 있습니다.

이 인증서 요청 방법은 컴퓨터 사이의 통신이 내부 도메인 내에서 유지되는 경우에 적합합니다. 예를 들어, 서버 사이의 통신에는 Windows 도메인 CA 로부터 서명된 인증서를 얻는 것이 적합할 수 있습니다.

View Client 가 외부 네트워크에서 View servers 에 연결하는 경우, 신뢰할 수 있는 타사 CA 에서 서명한 SSL 서버 인증서를 요청하십시오.

필수 조건

- 클라이언트 컴퓨터가 호스트에 연결하기 위해 사용하는 완전히 검증된 도메인 이름(FQDN)을 결정합니다.
- 인증서 스냅인이 MMC 에 추가되었는지 확인합니다. "MMC 에 인증서 스냅인 추가," (75 페이지)의 내용을 참조하십시오.
- 컴퓨터나 서비스에 발행할 수 있는 인증서를 요청하기 위해 적합한 자격 증명이 준비되어 있는지 확인합니다.

프로시저

1 Windows Server 호스트의 MMC 창에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **개인** 폴더를 선택합니다.

2 **작업** 메뉴에서 **모든 작업 > 새 인증서 요청**으로 이동하여 인증서 등록 마법사를 표시합니다.

3 인증서 등록 정책을 선택합니다.

4 요청하려는 인증서의 종류를 선택하고 **등록**을 클릭합니다.

5 **마침**을 클릭하십시오.

서명된 새 인증서가 Windows 인증서 저장소의 **개인 > 인증서** 폴더에 추가됩니다.

후속 작업

- 서버 인증서와 인증서 체인을 Windows 인증서 저장소로 가져왔는지 확인합니다.
- View 연결 서버 인스턴스 또는 보안 서버의 경우 인증서 이름을 `vdm` 으로 수정합니다. "인증서 이름 수정," (77 페이지)의 내용을 참조하십시오.
- View Composer 서버의 경우, 새 인증서를 View Composer 에서 사용하는 포트에 바인딩합니다. "View Composer 가 사용하는 포트에 새 SSL 인증서 바인딩," (78 페이지)의 내용을 참조하십시오.

새로운 SSL 인증서를 사용하도록 View 연결 서버, 보안 서버 또는 View Composer 구성

SSL 인증서를 사용하도록 View 연결 서버 인스턴스, 보안 서버 또는 View Composer 인스턴스를 구성하려면 서버 인증서와 전체 인증서 체인을 View 연결 서버, 보안 서버 또는 View Composer 호스트에 있는 Windows 로컬 컴퓨터의 인증서 저장소로 가져와야 합니다.

중요 인증서를 사용하도록 View 연결 서버 또는 보안 서버를 구성하려면 인증서 이름을 **vdm** 으로 변경해야 합니다. 또한, 인증서에 부속 개인 키가 있어야 합니다.

View Composer 설치 후 기존 인증서 또는 자체 서명된 기본 인증서를 새 인증서로 대체하려는 경우, `SviConfig ReplaceCertificate` 유틸리티를 실행하여 새 인증서를 View Composer 에서 사용하는 포트에 바인딩시켜야 합니다.

프로시저

1 MMC 에 인증서 스냅인 추가(75 페이지)

Windows 인증서 저장소에 인증서를 추가하려면 먼저 View server 가 설치된 Windows Server 호스트에서 Microsoft Management Console(MMC)에 인증서 스냅인을 추가해야 합니다.

2 Windows 인증서 저장소로 서명된 서버 인증서 가져오기(76 페이지)

View 연결 서버 인스턴스, 보안 서버 또는 View Composer 서비스가 설치된 Windows Server 호스트에 있는 Windows 로컬 컴퓨터 인증서 저장소로 SSL 서버 인증서를 가져와야 합니다.

3 인증서 이름 수정(77 페이지)

SSL 인증서를 인식 및 사용하도록 View 연결 서버 인스턴스나 보안 서버를 구성하려면 인증서 이름을 `vdm` 으로 수정해야 합니다.

4 Windows 인증서 저장소로 루트 인증서 및 중간 인증서 가져오기(77 페이지)

View 연결 서버가 설치된 Windows Server 호스트가 서명된 SSL 서버 인증서의 루트 인증서를 신뢰하지 않는 경우, 루트 인증서를 Windows 로컬 컴퓨터의 인증서 저장소로 가져와야 합니다. 또한, View 연결 서버 호스트가 보안 서버, View Composer 및 vCenter Server 호스트에 대해 구성된 SSL 서버 인증서의 루트 인증서를 신뢰하지 않는 경우에도 이러한 루트 인증서를 가져와야 합니다.

5 View Composer 가 사용하는 포트에 새 SSL 인증서 바인딩(78 페이지)

View Composer 를 설치한 후 새 SSL 인증서를 구성하는 경우, `SviConfig ReplaceCertificate` 유틸리티를 실행하여 View Composer 가 사용하는 포트에 바인딩되는 인증서를 대체해야 합니다. 이 유틸리티는 기존 인증서의 바인딩을 해제하고 새 인증서를 포트에 바인딩합니다.

MMC 에 인증서 스냅인 추가

Windows 인증서 저장소에 인증서를 추가하려면 먼저 View server 가 설치된 Windows Server 호스트에서 Microsoft Management Console(MMC)에 인증서 스냅인을 추가해야 합니다.

필수 조건

View server 가 설치된 Windows Server 컴퓨터에서 MMC 와 인증서 스냅인을 사용할 수 있는지 확인합니다.

프로시저

1 Windows Server 컴퓨터에서 **시작**을 클릭하고 **mmc.exe** 를 입력합니다.

2 MMC 창에서 **파일 > 스냅인 추가/제거**로 이동합니다.

3 스냅인 추가 또는 제거 창에서 **인증서**를 선택하고 **추가**를 클릭합니다.

4 인증서 스냅인 창에서 **컴퓨터 계정**을 선택하고 **다음**을 클릭한 다음 **로컬 컴퓨터**를 선택하고 **마침**을 클릭합니다.

5 스냅인 추가 또는 제거 창에서 **확인**을 클릭합니다.

후속 작업

Windows 인증서 저장소로 SSL 서버 인증서를 가져옵니다.

Windows 인증서 저장소로 서명된 서버 인증서 가져오기

View 연결 서버 인스턴스, 보안 서버 또는 View Composer 서비스가 설치된 Windows Server 호스트에 있는 Windows 로컬 컴퓨터 인증서 저장소로 SSL 서버 인증서를 가져와야 합니다.

인증서 파일 형식에 따라 keystore 파일에 포함된 전체 인증서 체인을 Windows 로컬 컴퓨터 인증서 저장소로 가져올 수도 있습니다. 예를 들어 서버 인증서, 중간 인증서 및 루트 인증서를 가져올 수도 있습니다.

다른 인증서 파일 유형의 경우, 서버 인증서만 Windows 로컬 컴퓨터 인증서 저장소로 가져옵니다. 이 경우, 인증서 체인에 있는 루트 인증서와 모든 중간 인증서를 가져오기 위한 별도의 단계를 거쳐야 합니다.

인증서에 대한 자세한 내용은 MMC 의 인증서 스냅인에 제공되는 Microsoft 온라인 도움말을 참조하십시오.

참고 중간 서버와의 SSL 연결을 오프로드하는 경우, 동일한 SSL 서버 인증서를 중간 서버와 오프로드한 View server 모두로 가져와야 합니다. 자세한 내용은 *VMware View 관리* 문서에서 "중간 서버와의 SSL 연결 오프로드"를 참조하십시오.

필수 조건

인증서 스냅인이 MMC 에 추가되었는지 확인합니다. "MMC 에 인증서 스냅인 추가," (75 페이지)의 내용을 참조하십시오.

프로시저

1 Windows Server 호스트의 MMC 창에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **개인** 폴더를 선택합니다.

2 작업 창에서 **추가 작업 > 모든 작업 > 가져오기**로 이동합니다.

3 인증서 가져오기 마법사에서 **다음**을 클릭하고 인증서가 저장된 위치로 이동합니다.

4 인증서 파일을 선택하고 **열기**를 클릭합니다.

인증서 파일 유형을 표시하려면 **파일 이름** 드롭다운 메뉴에서 파일 형식을 선택할 수 있습니다.

5 인증서 파일에 포함된 개인 키의 암호를 입력합니다.

6 **내보내기 가능 키로 표시**를 선택합니다.

7 **확장할 수 있는 모든 속성 포함**을 선택합니다.

8 **다음**을 클릭하고 **마침**을 클릭합니다.

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

9 새 인증서에 개인 키가 포함되어 있는지 확인합니다.

a **인증서(로컬 컴퓨터) > 개인 > 인증서** 폴더에서 새 인증서를 두 번 클릭합니다.

b '인증서 정보' 대화 상자의 '일반' 탭에서 다음 메시지가 나타나는지 확인합니다. 이 인증서에 해당하는 개인 키가 있습니다.

후속 작업

인증서 이름을 **vdm** 으로 수정하십시오.

인증서 이름 수정

SSL 인증서를 인식 및 사용하도록 View 연결 서버 인스턴스나 보안 서버를 구성하려면 인증서 이름을 vdm 으로 수정해야 합니다.

View Composer 에서 사용하는 SSL 인증서 이름을 수정할 필요는 없습니다.

필수 조건

서버 인증서를 Windows 인증서 저장소의 **인증서(로컬 컴퓨터) > 개인 > 인증서** 폴더로 가져왔는지 확인합니다. "Windows 인증서 저장소로 서명된 서버 인증서 가져오기," (76 페이지)의 내용을 참조하십시오.

프로시저

1 Windows Server 호스트의 MMC 창에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **개인 > 인증서** 폴더를 선택합니다.

2 View server 호스트에 발행된 인증서를 마우스 오른쪽 버튼으로 클릭하고 **속성**을 클릭합니다.

3 '일반' 탭에서 **이름** 텍스트를 삭제하고 **vdm** 을 입력합니다.

4 **적용**을 클릭하고 **확인**을 클릭합니다.

후속 작업

Windows 로컬 컴퓨터의 인증서 저장소로 루트 인증서와 중간 인증서를 가져옵니다.

체인에 있는 모든 인증서를 가져온 후 변경 내용이 적용되도록 View 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작해야 합니다.

Windows 인증서 저장소로 루트 인증서 및 중간 인증서 가져오기

View 연결 서버가 설치된 Windows Server 호스트가 서명된 SSL 서버 인증서의 루트 인증서를 신뢰하지 않는 경우, 루트 인증서를 Windows 로컬 컴퓨터의 인증서 저장소로 가져와야 합니다. 또한, View 연결 서버 호스트가 보안 서버, View Composer 및 vCenter Server 호스트에 대해 구성된 SSL 서버 인증서의 루트 인증서를 신뢰하지 않는 경우에도 이러한 루트 인증서를 가져와야 합니다.

View 연결 서버, 보안 서버, View Composer 및 vCenter Server 인증서를 View 연결 서버 호스트에서 신뢰하고 알려져 있는 루트 CA 가 서명하였고 인증서 체인에 다른 중간 인증서가 없는 경우, 이 작업을 건너뛸 수 있습니다. 일반적으로 사용되는 인증 기관은 대체적으로 호스트에서 신뢰합니다.

참고 View Composer, vCenter Server 또는 보안 서버 호스트로 루트 인증서를 가져올 필요가 없습니다.

서버 인증서를 중간 CA 에서 서명한 경우, 인증 체인에 있는 각 중간 인증서도 가져와야 합니다. 클라이언트 구성을 단순화하려면 전체 중간 체인을 보안 서버, View Composer 및 vCenter Server 호스트뿐만 아니라 View 연결 서버 호스트로도 가져오십시오. View 연결 서버 또는 보안 서버 호스트에서 중간 인증서가 누락된 경우, View Administrator 를 실행하는 컴퓨터 및 View Client 에 대해 이 인증서를 구성해야 합니다. View Composer 또는 vCenter Server 호스트에서 중간 인증서가 누락된 경우, 각 View 연결 서버 인스턴스에 대해 이 인증서를 구성해야 합니다.

Windows 로컬 컴퓨터의 인증서 저장소로 전체 인증서 체인을 가져왔음을 이미 확인한 경우, 이 작업을 건너뛸 수 있습니다.

프로시저

1 Windows Server 호스트의 MMC 콘솔에서 **인증서(로컬 컴퓨터)** 노드를 확장하고 **신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더로 이동합니다.

   - 루트 인증서가 이 폴더에 있고 인증서 체인에 중간 인증서가 없는 경우, 7 단계를 건너뛰십시오.
   - 루트 인증서가 이 폴더에 없으면 2 단계로 진행하십시오.

2 **신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더를 마우스 오른쪽 단추로 클릭하고 **모든 작업 > 가져오기**를 클릭합니다.

3 인증서 가져오기 마법사에서 **다음**을 클릭하고 루트 CA 인증서가 저장된 위치로 이동합니다.

4 루트 CA 인증서 파일을 선택하고 **열기**를 클릭합니다.

5 **다음**, **다음**, **마침**을 차례로 클릭합니다.

6 중간 CA가 서버 인증서에 서명한 경우, 인증 체인에 있는 모든 중간 인증서를 Windows 로컬 컴퓨터의 인증서 저장소로 가져옵니다.

   a **인증서(로컬 컴퓨터) > 중간 인증 기관 > 인증서** 폴더로 이동합니다.

   b 가져와야 하는 각 중간 인증서에 대해 3 ~ 6 단계를 반복합니다.

7 View 연결 서버 서비스, 보안 서버 서비스, View Composer 서비스 또는 vCenter Server 서비스를 다시 시작하여 변경 내용을 적용합니다.

View Composer가 사용하는 포트에 새 SSL 인증서 바인딩

View Composer를 설치한 후 새 SSL 인증서를 구성하는 경우, SviConfig ReplaceCertificate 유틸리티를 실행하여 View Composer가 사용하는 포트에 바인딩되는 인증서를 대체해야 합니다. 이 유틸리티는 기존 인증서의 바인딩을 해제하고 새 인증서를 포트에 바인딩합니다.

View Composer를 설치하기 전에 Windows Server 컴퓨터에 새 인증서를 설치하는 경우, SviConfig ReplaceCertificate 유틸리티를 실행할 필요가 없습니다. View Composer 설치 관리자를 실행하는 경우, 자체 서명된 기본 인증서 대신 CA에서 서명한 인증서를 선택할 수 있습니다. 설치 과정에서 선택된 인증서가 View Composer에서 사용하는 포트에 바인딩됩니다.

기존 인증서 또는 자체 서명된 기본 인증서를 새 인증서로 대체하려는 경우, SviConfig ReplaceCertificate 유틸리티를 사용해야 합니다.

필수 조건

View Composer가 설치된 Windows Server 컴퓨터의 Windows 로컬 컴퓨터 인증서 저장소로 새 인증서를 가져왔는지 확인합니다.

프로시저

1 View Composer 서비스를 중지하십시오.

2 View Composer가 설치된 Windows Server 호스트에서 명령 프롬프트를 엽니다.

3 SviConfig ReplaceCertificate 명령을 입력합니다.

예:

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

여기서 -delete 는 대체되는 인증서에 적용되는 필수 매개 변수입니다. Windows 로컬 컴퓨터 인증서 저장소에서 이전 인증서를 삭제하려면 -delete=true 를 지정하거나 Windows 인증서 저장소에 이전 인증서를 유지하려면 -delete=false 를 지정해야 합니다.

유틸리티가 Windows 로컬 컴퓨터 인증서 저장소에서 사용할 수 있는 SSL 인증서 번호 목록을 표시합니다.

4 인증서를 선택하려면 인증서 번호를 입력하고 Enter 를 누릅니다.

5 변경 내용을 적용하려면 View Composer 서비스를 다시 시작하십시오.

예: SviConfig ReplaceCertificate

다음 예제는 View Composer 포트에 바인딩된 인증서를 대체합니다.

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

루트 및 중간 인증서를 신뢰하도록 View Client 구성

View server 인증서가 View Client 컴퓨터 및 View Administrator 에 액세스하는 클라이언트 컴퓨터에서 신뢰하지 않는 CA 에 의해 서명된 경우, 루트 및 중간 인증서를 신뢰하도록 도메인의 모든 Windows 클라이언트 시스템을 구성할 수 있습니다. 이를 위해서는 루트 인증서에 대한 공용 키를 Active Directory 의 신뢰할 수 있는 루트 인증 기관 그룹 정책에 추가하고 루트 인증서를 Enterprise NTAuth 저장소에 추가해야 합니다.

예를 들어, 조직에서 내부 인증서 서비스를 사용할 경우 이러한 단계를 적용해야 할 수도 있습니다.

Windows 도메인 컨트롤러가 루트 CA 역할을 하거나 인증서가 잘 알려진 CA 에 의해 서명된 경우에는 이러한 단계를 거치지 않아도 됩니다. 잘 알려진 CA 의 경우, 운영 체제 공급 업체는 클라이언트 시스템에 루트 인증서를 미리 설치합니다.

잘 알려지지 않은 중간 CA 에서 View server 인증서를 서명할 경우, 중간 인증서를 Active Directory 의 중간 인증 기관 그룹 정책에 추가해야 합니다.

다른 운영 체제 및 장치에서 실행되는 View Client 의 경우, 사용자가 설치할 수 있는 루트 및 중간 인증서 배포를 위한 다음 지침을 참조하십시오.

- Mac OS X 용 View Client 의 경우, "루트 및 중간 인증서를 신뢰하도록 Mac OS X 용 View Client 구성," (80 페이지)을 참조하십시오.
- iPad 용 View Client 의 경우, "루트 및 중간 인증서를 신뢰하도록 iPad 용 View Client 구성," (81 페이지)을 참조하십시오.
- Android 용 View Client 의 경우, Google 웹 사이트에서 *Android 3.0 사용자 설명서* 등의 문서를 참조하십시오.
- Linux 용 View Client 의 경우, Ubuntu 설명서를 참조하십시오.

프로시저

1 Enterprise NTAuth 저장소에 인증서를 게시하려면 Active Directory 서버에서 certutil 명령을 사용하십시오.

예: **certutil -dspublish -f *path_to_root_CA_cert* NTAuthCA**

2 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동합니다.

AD 버전	탐색 경로
Windows 2003	a **시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터**. b 도메인을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 클릭합니다. c 그룹 정책 관리 플러그인을 열려면 **그룹 정책** 탭에서 **열기**를 클릭하십시오. d **기본 도메인 정책**을 마우스 오른쪽 버튼으로 클릭하고 **편집**을 클릭합니다.
Windows 2008	a **시작 > 관리 도구 > 그룹 정책 관리**. b 도메인을 확장하고 **기본 도메인 정책**을 마우스 오른쪽 버튼으로 클릭한 다음 **편집**을 클릭합니다.

3 **컴퓨터 구성** 섹션을 확장하고 Windows **설정 > 보안 설정 > 공용 키 정책**으로 이동하십시오.

4 인증서를 가져 오십시오.

옵션	설명
루트 인증서	a **신뢰할 수 있는 루트 인증 기관**을 마우스 오른쪽 버튼으로 클릭하고 **가져오기**를 선택합니다. b 마법사에 표시된 메시지에 따라 루트 인증서(예: rootCA.cer)를 가져오고 **확인**을 클릭합니다.
중간 인증서	a **중간 인증 기관**을 마우스 오른쪽 버튼으로 클릭하고 **가져오기**를 선택합니다. b 마법사에 표시된 메시지에 따라 중간 인증서(예: intermediateCA.cer)를 가져오고 **확인**을 클릭합니다.

5 그룹 정책 창을 닫습니다.

이제 도메인에 있는 모든 시스템이 신뢰할 수 있는 루트 인증서 저장소와 중간 인증서 저장소에서 인증서 정보를 확인할 수 있어 루트 및 중간 인증서를 신뢰하도록 허용할 수 있습니다.

루트 및 중간 인증서를 신뢰하도록 Mac OS X 용 View Client 구성

View server 인증서가 Mac OS X 용 View Client 를 실행하는 컴퓨터가 신뢰하지 않는 CA 에 의해 서명된 경우, 루트 및 중간 인증서를 신뢰하도록 이러한 컴퓨터를 구성할 수 있습니다. 신뢰 체인에 있는 루트 인증서와 모든 중간 인증서를 클라이언트 컴퓨터에 배포해야 합니다.

프로시저

1 Mac OS X 용 View Client 를 실행하는 컴퓨터로 루트 인증서 및 중간 인증서를 보냅니다.

2 Mac OS X 컴퓨터에서 루트 인증서를 엽니다.

인증서가 다음 메시지를 표시합니다. 지금부터 컴퓨터가 *CA 이름*에 의해 서명된 인증서를 신뢰하도록 하시겠습니까?

3 **항상 신뢰**를 클릭합니다.

4 사용자 암호를 입력합니다.

5 신뢰 체인에 있는 모든 중간 인증서에 대해 2 ~ 4 단계를 반복합니다.

루트 및 중간 인증서를 신뢰하도록 iPad 용 View Client 구성

View server 인증서가 iPad 용 View Client 를 실행하는 iPad 가 신뢰하지 않는 CA 에 의해 서명된 경우, 루트 및 중간 인증서를 신뢰하도록 iPad 를 구성할 수 있습니다. 신뢰 체인에 있는 루트 인증서와 모든 중간 인증서를 iPad 에 배포해야 합니다.

프로시저

1 루트 인증서와 중간 인증서를 이메일 첨부 파일로 iPad 로 보냅니다.

2 루트 인증서에 대한 이메일 첨부 파일을 열고 **설치**를 선택합니다.

인증서가 다음 메시지를 표시합니다.

확인할 수 없는 프로파일. *인증서 이름*의 신뢰성을 확인할 수 없습니다. 이 프로파일을 설치하면 iPad 의 설정이 변경됩니다.

루트 인증서. *인증서 이름* 인증서를 설치하면 iPad 의 신뢰할 수 있는 인증서 목록에 이 인증서가 추가됩니다.

3 **설치**를 다시 선택합니다.

4 신뢰 체인에 있는 모든 중간 인증서에 대해 2 단계 및 3 단계를 반복합니다.

서버 인증서에 대한 인증서 해지 확인 구성

각 View 연결 서버 인스턴스는 자체 인증서 및 쌍으로 구성된 보안 서버의 인증서에 대해 인증서 해지 확인을 수행합니다. 각 인스턴스는 또한 연결을 구성할 때마다 vCenter 및 View Composer 서버의 인증서를 검사합니다. 기본적으로, 루트 인증서를 제외하고 체인에 있는 모든 인증서가 검사됩니다. 그러나 이 기본값은 변경이 가능합니다.

View 는 인증서 해지 목록(CRL) 및 온라인 인증서 상태 프로토콜(OCSP) 등의 다양한 인증서 해지 확인 방법을 지원합니다. CRL 은 인증서를 발행한 CA 에서 게시한 해지된 인증서 목록입니다. OCSP 는 X.509 인증서의 해지 상태를 얻는 데 사용되는 인증서 유효성 검사 프로토콜입니다.

CRL 의 경우, 해지되는 인증서 목록은 종종 인증서에 지정되는 인증서 배포 지점(DP)에서 다운로드됩니다. View server 는 주기적으로 인증서에 지정된 CRL DP URL 로 이동하여 목록을 다운로드하고 이를 검사하여 서버 인증서가 해지되었는지 여부를 확인합니다. OCSP 의 경우, View server 는 OCSP 응답자로 요청을 보내어 인증서의 해지 상태를 확인합니다.

타사 인증 기관(CA)으로부터 서버 인증서를 얻는 경우, 인증서에 CRL DP URL 또는 OCSP 응답자의 URL 등 인증서의 해지 상태를 확인할 수 있는 한 가지 이상의 방법이 포함됩니다. 자체 CA 를 가지고 있고 인증서를 생성하지만 인증서에 해지 정보가 포함되지 않는 경우, 인증서 해지 확인을 통과하지 못합니다. 이러한 인증서에 대한 해지 정보의 예로는 CRL 을 호스팅하는 서버의 웹 기반 CRL DP URL 등이 포함될 수 있습니다.

자체 CA 를 가지고 있지만 인증서에 인증서 해지 정보를 포함시키지 않거나 포함시킬 수 없는 경우, 인증서의 해지 검사를 선택하지 않거나 체인의 특정 인증서만 검사하도록 선택할 수 있습니다. View server 에서 Windows 레지스트리 편집기를 사용하여 HKLM₩Software₩VMware, Inc.₩VMware VDM₩Security 에서 문자열(REG_SZ) 값 CertificateRevocationCheckType 을 생성하고 이 값을 다음 데이터 값 중 하나로 설정할 수 있습니다.

값	설명
1	인증서 해지 확인을 수행하지 않습니다.
2	서버 인증서만 검사합니다. 체인에 있는 다른 어떤 인증서도 검사하지 않습니다.

값	설명
3	체인에 있는 모든 인증서를 검사합니다.
4	(기본값) 루트 인증서를 제외한 모든 인증서를 검사합니다.

이 레지스트리 값을 설정하지 않거나 설정 값이 유효하지 않으면(즉, 값이 1, 2, 3 또는 4 가 아닌 경우), 루트 인증서를 제외한 모든 인증서가 검사됩니다. 해지 확인을 수정하려는 각 View server 에서 이 레지스트리 값을 설정합니다. 이 값을 설정한 후 시스템을 다시 시작할 필요는 없습니다.

Windows 용 View Client 에서 인증서 검사 구성

View Client 구성 ADM 템플릿 파일(vdm_client.adm)의 보안 관련 그룹 정책 설정을 사용하면 Windows 기반 View Client 에 SSL 서버 인증서 검사를 구성할 수 있습니다.

인증서 검사는 View 연결 서버와 View Client 간에 SSL 연결이 있을 때 수행됩니다. 인증서 검사에는 다음 확인 사항이 포함됩니다.

- 인증서가 해지되었습니까? 인증서가 해지되었는지 확인할 수 있습니까?
- 해당 인증서는 전송자 ID 확인 및 서버 통신 암호화 이외의 용도입니까? 즉, 올바른 유형의 인증서입니까?
- 인증서가 만료되었거나 나중에만 유효합니까? 즉, 컴퓨터 시계에 따라 인증서가 유효합니까?
- 인증서의 공통 이름이 이름을 보내는 서버의 호스트 이름과 일치합니까? 로드 밸런서가 사용자가 입력한 호스트 이름과 일치하지 않는 인증서를 사용하여 View Client 를 서버로 리디렉션할 경우, 불일치가 발생할 수 있습니다. 사용자가 클라이언트에 호스트 이름이 아닌 IP 주소를 입력하는 경우에도 불일치가 발생할 수 있습니다.
- 알 수 없거나 신뢰할 수 없는 인증 기관(CA)에서 서명된 인증서입니까? 자체 서명된 인증서는 신뢰할 수 없는 CA 유형 중 하나입니다.

  이 검사를 통과하려면 인증서의 신뢰 체인이 장치의 로컬 인증서 저장소의 루트 위치에 있어야 합니다.

처음 View 환경을 설정할 때에는 기본 자체 서명 인증서가 사용됩니다. 기본적으로, **경고와 함께 허용**은 인증서 검사 모드입니다. 이 모드에서는 다음 서버 인증서 문제 중 하나가 발생할 때 경고가 표시되지만 사용자가 경고를 무시하고 계속 진행할 수 있습니다.

- 자체 서명 인증서가 View server 에 의해 제공됩니다. 이런 경우, 인증서 이름이 View Client 의 사용자가 제공하는 View 연결 서버 이름과 일치하지 않더라도 허용됩니다.
- 배포에 구성된 확인할 수 있는 인증서가 만료되었거나 아직 유효하지 않습니다.

기본 인증서 검사 모드를 변경할 수 있습니다. 모드를 **보안 없음**으로 설정하여 인증서 검사가 수행되지 않도록 하거나 모드를 **전체 보안**으로 설정하여 어느 한 검사라도 통과하지 못할 경우 사용자의 서버 연결을 거부할 수 있습니다. 또한 최종 사용자가 직접 모드를 설정하도록 허용할 수 있습니다.

클라이언트 구성 ADM 템플릿 파일에서 인증서 검사 모드 그룹 정책 설정을 사용하여 검사 모드를 변경합니다. 이 그룹 정책 설정이 구성되면 설정이 View Client 에서 잠깁니다. 사용자는 View Client 에서 선택한 검사 모드를 볼 수는 있지만 설정을 구성할 수 없습니다. 이 그룹 정책 설정이 구성되지 않거나 비활성화된 경우, View Client 사용자가 검사 모드를 선택할 수 있습니다.

View 구성 요소의 ADM 템플릿 파일은 View 연결 서버 호스트의 *install_directory*₩VMware₩VMware View₩Server₩Extras₩GroupPolicyFiles 디렉터리에 설치됩니다. 이러한 템플릿을 사용한 GPO 설정 제어에 대한 자세한 내용은 *VMware View 관리* 문서를 참조하십시오.

View 전송 서버 및 SSL 인증서

View 5.1 이상을 설치하는 경우에는 View 전송 서버에 대해 SSL 인증서를 구성할 필요가 없습니다.

View Client 와의 보조 연결을 처리하기 위해 View 연결 서버가 사용하는 View 전송 서버에는 자체 서명된 기본 인증서가 설치됩니다.

View 에 View 전송 서버를 추가하면 View 연결 서버가 View 전송 서버와 신뢰 관계를 수립합니다. View 연결 서버와 View 전송 서버 사이의 통신에는 JMS(Java Message Service)가 사용됩니다. 중요한 데이터를 포함한 메시지는 암호화됩니다.

View Client 가 View 전송 서버에 연결이 필요한 데이터 전송 작업을 요청하면 View 연결 서버가 View 전송 서버 인증서의 지문을 클라이언트로 보냅니다. 클라이언트가 View 전송 서버와 연결된 Apache 서버에 연결하면 View Client 는 View 연결 서버에서 전달된 지문이 Apache 서버의 인증서 지문과 일치하는지 확인합니다.

View 전송 서버의 기본 인증서를 CA 에서 서명한 인증서로 교체해도 View 전송 서버, View 연결 서버 및 View Client 사이의 보안 통신에는 큰 영향을 미치지 않습니다.

View 5.0.*x* 이전 버전에서는 View 전송 서버에 SSL 인증서를 구성해야 했습니다.

View 5.0.*x* 이전 버전을 View 5.1 이상 버전으로 업그레이드하면서 View 전송 서버의 업그레이드 버전에서 CA 에 의해 서명된 인증서를 계속 사용하려면 인증서를 백업하고 View 전송 서버를 업그레이드하고 새 View 전송 서버 버전에 적합하게 서명 인증서를 구성해야 합니다.

이전 View 전송 서버에 대해 자체 서명한 인증서를 구성했거나 업그레이드된 서버에서 기존의 CA 서명 인증서를 사용하지 않으려는 경우에는 인증서를 다시 구성할 필요가 없습니다. 업그레이드 과정에서 View 전송 서버에 자체 서명된 유효한 인증서가 설치됩니다.

자세한 내용은 *VMware View 업그레이드* 문서를 참조하십시오.

vCenter Server 또는 View Composer 인증서를 신뢰하도록 View Administrator 설정

View Administrator 대시보드에서 신뢰할 수 없는 vCenter Server 또는 View Composer 인증서를 신뢰하도록 View 를 구성할 수 있습니다.

CA 에서 서명한 SSL 인증서를 사용하도록 vCenter Server 및 View Composer 를 구성하는 것이 매우 중요합니다. 혹은, vCenter Server 또는 View Composer 에 대한 기본 인증서의 지문을 수락할 수 있습니다.

CA 에서 서명한 SSL 인증서를 사용할 때의 이점

CA 는 인증서와 작성자의 ID 를 보증하는 신뢰할 수 있는 엔터티입니다. 신뢰할 수 있는 CA 에서 인증서에 서명한 경우, 사용자에게 인증서 확인을 묻는 메시지가 더 이상 표시되지 않으며, 추가 구성 없이 씬 클라이언트 디바이스에 연결할 수 있습니다.

`www.mycorp.com` 과 같은 웹 도메인에 특정한 SSL 서버 인증서를 요청하거나 `*.mycorp.com` 과 같이 도메인 전반에 사용할 수 있는 와일드카드 SSL 서버 인증서를 요청할 수 있습니다. 여러 서버 또는 여러 하위 도메인에 인증서를 설치할 경우, 관리를 간소화하기 위해 와일드카드 인증서를 요청할 수 있습니다. 보안 설치에서는 도메인에 특정한 인증서를 사용하는 것이 일반적이고 CA 는 와일드카드 인증서보다 도메인에 특정한 인증서의 손실을 추가적으로 보호합니다. 와일드카드 인증서를 사용할 경우, 서버 간 개인 키가 전송 가능한지 확인해야 합니다.

기본 인증서를 자신의 인증서와 교체할 경우 클라이언트는 인증서를 사용하여 서버를 인증합니다. 인증서가 CA 에서 서명되지 않은 경우 CA 의 인증서는 기본적으로 브라우저에 내장되어 있거나 클라이언트가 액세스할 수 있는 신뢰된 데이터베이스에 있습니다. 클라이언트가 인증서에 동의한 후 인증서에 포함된 공용 키로 암호화된 비밀 키를 사용하여 응답합니다. 비밀 키는 클라이언트 및 서버 사이의 트래픽을 암호화하기 위해 사용됩니다.

8 처음으로 View 구성

View server 소프트웨어를 설치하고 서버의 SSL 인증서를 구성한 후, 운영 View 환경을 설정하기 위한 몇 가지 추가 단계를 거쳐야 합니다.

vCenter Server 및 View Composer 의 사용자 계정을 구성하고, View 라이센스 키를 설치하고, View 환경에 vCenter Server 및 View Composer 를 추가하고, PCoIP 보안 게이트웨이와 보안 터널을 구성하고, 필요할 경우 View 환경을 지원하도록 Windows Server 설정의 크기를 지정할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

vCenter Server 및 View Composer 의 사용자 계정 구성

vCenter Server 를 View Manager 와 함께 사용하려면 vCenter Server 에서 작업을 수행할 수 있는 사용 권한을 가진 사용자 계정을 구성해야 합니다. View Composer 를 사용하려면 vCenter Server 사용자에게 추가 권한을 부여해야 합니다. 로컬 모드로 사용하는 데스크톱을 관리하려면 View Manager 및 View Composer 에 필요한 권한 외에 이 사용자 권한을 부여해야 합니다.

그리고 Active Directory 에 View Composer 를 위한 도메인 사용자를 생성해야 합니다. 자세한 내용은 "View Composer 에 대한 사용자 계정 생성," (27 페이지)에 나와 있습니다.

View Composer 의 vCenter Server 사용자 및 도메인 사용자 사용 위치

이러한 두 개의 사용자 계정을 생성하여 구성한 다음 View Administrator 의 사용자 이름을 지정합니다.

- vCenter Server 를 View Manager 에 추가할 때 vCenter Server 사용자를 지정합니다.
- vCenter Server 의 View Composer 를 구성할 때 View Composer 의 도메인 사용자를 지정합니다.
- 연결된 클론 풀을 생성할 때 View Composer 의 도메인 사용자를 지정합니다.

View Manager, View Composer 및 Local Mode 를 위한 vCenter Server 사용자 구성

vCenter Server 에서 작업할 수 있도록 View Manager 사용 권한을 가진 사용자 계정을 구성하려면 해당 사용자에게 적절한 권한을 가진 역할을 할당해야 합니다. vCenter Server 에서 View Composer 서비스를 사용하려면 사용자 계정에 추가 권한을 부여해야 합니다. 로컬 모드로 사용되는 데스크톱을 관리하려면 사용자 계정에 View Manager, View Composer 및 로컬 모드 권한 등을 포함한 권한을 부여해야 합니다.

그리고 View Composer 를 지원하려면 해당 사용자에게 vCenter Server 컴퓨터의 로컬 시스템 관리자 권한을 부여해야 합니다.

필수 조건

- Active Directory 에서 View Connection Server 도메인 또는 신뢰할 수 있는 도메인에 사용자를 생성하십시오. 자세한 내용은 "vCenter Server 의 사용자 계정 생성," (26 페이지)에 나와 있습니다.
- 사용자 계정에 필요한 권한을 숙지하십시오. 자세한 내용은 "vCenter Server 사용자에게 필요한 View Manager 권한," (87 페이지)에 나와 있습니다.
- View Composer 를 사용하는 경우, 필요한 추가 권한을 숙지하십시오. 자세한 내용은 "vCenter Server 사용자에게 필요한 View Composer 권한," (88 페이지)에 나와 있습니다.
- 로컬 데스크톱을 관리하는 경우, 필요한 추가 권한을 숙지하십시오. 자세한 내용은 "vCenter Server 사용자에게 필요한 Local Mode 권한," (88 페이지)에 나와 있습니다.

프로시저

1 vCenter Server 에서 사용자에 대해 필요한 권한을 가진 역할을 준비하십시오.

   - vCenter Server 의 미리 정의된 관리자 역할을 사용할 수 있습니다. 이 역할을 사용하면 vCenter Server 에서 모든 작업을 수행할 수 있습니다.
   - View Composer 를 사용하는 경우, vCenter Server 작업을 수행하기 위해 View Manager 및 View Composer 에 필요한 최소 권한을 가진 제한된 역할을 생성할 수 있습니다.

     vSphere Client 에서 **홈 > 역할 > 역할 추가**를 클릭하고 **View Composer Administrator** 와 같은 역할 이름을 입력한 다음 역할에 대한 권한을 선택하십시오.

     이 역할은 View Manager 및 View Composer 가 vCenter Server 에서 작업하는 데 필요한 모든 권한을 가지고 있어야 합니다.
   - 로컬 데스크톱을 관리하는 경우, vCenter Server 작업을 수행하기 위해 View Manager, View Composer 및 로컬 모드 기능에 필요한 최소 권한을 가진 제한된 역할을 생성할 수 있습니다.

     vSphere Client 에서 **홈 > 역할 > 역할 추가**를 클릭하고 **Local Mode Administrator** 와 같은 역할 이름을 입력한 다음 역할에 대한 권한을 선택하십시오.

     이 역할은 View Manager, View Composer 를 비롯해 로컬 모드 기능으로 vCenter Server 에서 작업하는 데 필요한 모든 권한을 가지고 있어야 합니다.
   - View Composer 없이 View Manager 를 사용하며 로컬 데스크톱을 관리하지 않는 경우, vCenter Server 작업을 수행하기 위해 View Manager 에 필요한 최소 권한을 가지고 있으면서 더욱 제한된 역할을 생성할 수 있습니다.

     vSphere Client 에서 **홈 > 역할 > 역할 추가**를 클릭하고 **View Manager Administrator** 와 같은 역할 이름을 입력한 다음 역할에 대한 권한을 선택하십시오.

2 vSphere Client의 인벤토리 최상위 수준에서 마우스 오른쪽 단추로 vCenter Server를 클릭하고 **사용 권한 추가**를 클릭한 다음 vCenter Server 사용자를 추가하십시오.

참고 vCenter Server 수준의 vCenter Server 사용자를 정의해야 합니다.

3 드롭다운 메뉴에서 관리자 역할 또는 생성한 View Composer나 View Manager 역할을 선택한 다음 vCenter Server 사용자에 할당합니다.

4 View Composer를 사용하는 경우, vCenter Server 컴퓨터에서 vCenter Server 사용자 계정을 로컬 시스템 관리자 그룹 구성원으로 추가하십시오.

View Composer에서는 vCenter Server 사용자가 vCenter Server 컴퓨터의 시스템 관리자여야 합니다.

후속 작업

View Administrator에서 View Manager에 vCenter Server를 추가할 때 vCenter Server 사용자를 지정하십시오. 자세한 내용은 "View Manager에 vCenter Server 인스턴스 추가," (90 페이지)에 나와 있습니다.

vCenter Server 사용자에게 필요한 View Manager 권한

vCenter Server 사용자는 View Manager가 vCenter Server에서 사용하도록 설정할 수 있는 충분한 권한이 있어야 합니다. 필요한 권한을 사용하여 vCenter Server 사용자의 View Manager 역할을 생성합니다.

표 8-1. View Manager 권한

권한 그룹	사용하도록 설정할 권한
폴더	**폴더 생성** **폴더 삭제**
가상 시스템	**구성**에서 ■ **디바이스 추가 또는 제거** ■ **고급** ■ **디바이스 설정 수정** **상호 작용**에서 ■ **전원 끄기** ■ **전원 켜기** ■ **재설정** ■ **일시 중단** **인벤토리**에서 ■ **새로 만들기** ■ **제거** **프로비저닝**에서 ■ **사용자 지정** ■ **템플릿 배포** ■ **읽기 사용자 지정 규격**
리소스	**리소스 풀에 가상 시스템 할당**
전역	다음 권한은 View에서 ESXi 호스트 캐싱을 구현하는 데 필요합니다. 호스트 캐싱을 사용하지 않을 경우에는 vCenter Server 사용자에게 이 권한이 필요하지 않습니다. **vCenter Server 역할**

vCenter Server 사용자에게 필요한 View Composer 권한

View Composer를 지원하려면 vCenter Server 사용자에게 View Manager를 지원하는 데 필요한 것 이외의 권한이 있어야 합니다. View Manager 권한 및 이러한 추가 권한을 사용하여 vCenter Server 사용자의 View Composer 역할을 생성하십시오.

표 8-2. View Composer 권한

권한 그룹	사용하도록 설정할 권한
데이터스토어	**공간 할당** **데이터스토어 찾아보기** **낮은 수준의 파일 작업**
가상 시스템	**인벤토리**(모두) **구성**(모두) **상태**(모두) **프로비저닝**에서 ■ **클론 가상 시스템** ■ **디스크 액세스 허용**
리소스	**리소스 풀에 가상 시스템 할당**
전역	**사용하도록 설정하는 방법** **사용하지 않도록 설정하는 방법** **시스템 태그** 다음 권한은 View에서 ESXi 호스트 캐싱을 구현하는 데 필요합니다. 호스트 캐싱을 사용하지 않을 경우에는 vCenter Server 사용자에게 이 권한이 필요하지 않습니다. **vCenter Server 역할**
네트워크	(모두)

vCenter Server 사용자에게 필요한 Local Mode 권한

로컬 모드에서 사용된 데스크톱을 관리하려면 vCenter Server 사용자는 View Manager 및 View Composer를 지원하기 위해 사용된 것 외에 권한을 가져야 합니다. View Manager 권한, View Composer 권한 및 로컬 모드 권한을 겸하는 vCenter Server 사용자의 Local Mode Administrator 역할을 생성합니다.

표 8-3. 로컬 모드 권한

권한 그룹	사용하도록 설정할 권한
전역	**사용자 지정 특성 설정**
호스트	**구성**에서 **시스템 관리**

처음으로 View 연결 서버 구성

View 연결 서버를 설치한 후, 제품 라이센스를 설치하고 vCenter Server 및 View Composer 서비스를 View Manager에 추가해야 합니다. 가상 시스템 디스크 데이터를 캐시하도록 ESXi 호스트를 구성할 수도 있습니다.

보안 서버를 설치하는 경우, 이 서버는 View Manager에 추가되고 View Administrator에 자동으로 표시됩니다.

View Administrator 및 View Connection Server

View Administrator 는 View Manager 에 관리 인터페이스를 제공합니다.

View 배포에 따라 하나 이상의 View Administrator 인터페이스를 사용합니다.

- 하나의 View Administrator 인터페이스를 사용하여 단일 독립 실행형 View Connection Server 인스턴스 또는 복제된 View Connection Server 인스턴스 그룹과 관련된 View 구성 요소를 관리합니다.

  임의의 복제된 인스턴스의 IP 주소를 사용하여 View Administrator 에 로그인할 수 있습니다.

- 개별 View Administrator 인터페이스를 사용하여 각 단일 독립 실행형 View Connection Server 인스턴스 또는 복제된 View Connection Server 인스턴스의 각 그룹을 위한 View 구성 요소를 관리합니다.

또한 View Administrator 를 사용하여 View Connection Server 와 연결된 View Transfer Server 인스턴스 및 보안 서버를 관리합니다.

- 각 보안 서버는 하나의 View Connection Server 인스턴스와 연결됩니다.
- 각 View Transfer Server 인스턴스는 복제된 인스턴스 그룹에서 임의의 View Connection Server 인스턴스와 통신할 수 있습니다.

View Administrator 에 로그인

초기 구성 작업을 수행하려면 View Administrator 에 로그인해야 합니다.

필수 조건

View Administrator 에서 지원하는 웹 브라우저를 사용하는지 확인하십시오. "View Administrator 요구 사항," (9 페이지)의 내용을 참조하십시오.

프로시저

1 웹 브라우저를 열고 다음 URL 을 입력하십시오. 여기서 *server* 는 View 연결 서버 인스턴스의 호스트 이름입니다.

```
https://server/admin
```

참고 호스트 이름을 확인할 수 없을 때 View 연결 서버 인스턴스에 액세스해야 하는 경우 IP 주소를 사용할 수 있습니다. 그러나 연결하는 호스트가 해당 View 연결 서버 인스턴스에 대해 구성된 SSL 인증서와 일치하지 않아 액세스가 차단되거나 약화된 보안 수준으로 액세스하게 됩니다.

View Administrator 에 대한 액세스는 View 연결 서버 컴퓨터에 구성된 인증서의 유형에 따라 결정됩니다.

옵션	설명
View 연결 서버에 대해 CA 에서 서명한 인증서를 구성했습니다.	처음 연결하면 웹 브라우저에 View Administrator 가 표시됩니다.
View 연결 서버에 제공된 자체 서명된 기본 인증서가 구성되었습니다.	처음 연결할 때 신뢰할 수 있는 인증서 기관에서 해당 주소와 연결된 보안 인증서를 발행하지 않았다는 내용의 경고 페이지가 웹 브라우저에 나타날 수 있습니다. 현재 SSL 인증서를 계속 사용하려면 **무시**를 클릭합니다.

2 자격 증명을 가진 사용자로 로그인하여 View Administrators 계정에 액세스합니다.

복제된 그룹에 독립 실행형 View 연결 서버 인스턴스 또는 첫 번째 View 연결 서버 인스턴스를 설치할 때 View Administrators 계정을 지정합니다. View Administrators 계정은 View 연결 서버 컴퓨터 또는 도메인 사용자 또는 그룹 계정의 로컬 관리자 그룹(BUILTIN\Administrators)이 될 수 있습니다.

View Administrator에 로그인한 후에 **View 구성 > 인스턴스에**를 사용하여 View Administrator 역할을 가진 사용자 및 그룹 목록을 변경할 수 있습니다.

View Connection Server 라이센스 키 설치

View Connection Server를 사용하기 전에 제품 라이센스 키를 입력해야 합니다.

처음 로그인하면 View Administrator에 제품 라이센싱 및 사용 페이지가 나타납니다.

라이센스 키를 설치한 다음 로그인할 때 View Administrator에 대시보드 페이지가 나타납니다.

복제된 View Connection Server 인스턴스 또는 보안 서버를 설치할 때는 라이센스 키를 구성하지 않아도 됩니다. 복제된 인스턴스 및 보안 서버는 View LDAP 구성에 저장된 일반 라이센스 키를 사용합니다.

참고 View Connection Server는 유효한 View 5.0 라이센스 키가 필요합니다. VMware View 4.0 릴리스부터, VMware View 라이센스 키는 25자 키입니다.

프로시저

1 View Configuration 보기가 나타나지 않으면 왼쪽 탐색 창에서 **View 구성**을 클릭하십시오.

2 **제품 라이센싱 및 사용**을 클릭하십시오.

3 제품 라이센싱 테이블에서 **라이센스 편집**을 클릭하고 View Manager 라이센스 일련 번호를 입력하십시오.

4 **확인**을 클릭합니다.

5 라이센스 만료 날짜를 확인하십시오.

View Manager에 vCenter Server 인스턴스 추가

View 배포의 vCenter Server 인스턴스에 연결할 View Manager를 구성해야 합니다. vCenter Server는 View Manager에서 데스크톱 소스로 사용하는 가상 컴퓨터를 만들고 관리합니다.

Linked Mode 그룹에서 vCenter Server 인스턴스를 실행하려면 각 vCenter Server 인스턴스를 View Manager에 따로 추가해야 합니다.

View Manager는 보안 채널(SSL)을 사용하여 vCenter Server 인스턴스에 연결합니다.

필수 조건

- View 연결 서버 제품 라이센스 키를 설치하십시오.
- View Manager 지원에 필요한 vCenter Server에서 작업을 수행할 수 있는 사용 권한을 가진 vCenter Server 사용자를 준비하십시오. View Composer를 사용하려면 사용자에게 추가 권한을 부여해야 합니다. 로컬 모드로 사용하는 데스크톱을 관리하려면 View Manager 및 View Composer에 필요한 권한 외에 다른 권한을 사용자에게 부여해야 합니다.

  "View Manager, View Composer 및 Local Mode를 위한 vCenter Server 사용자 구성," (86페이지)의 내용을 참조하십시오.

- vCenter Server 호스트에 SSL 서버 인증서가 설치되어 있는지 확인합니다. 운영 환경에서는 신뢰할 수 있는 인증 기관(CA)에서 서명한 유효한 SSL 인증서를 설치하십시오.

  테스트 환경에서는 vCenter Server 와 함께 설치된 기본 인증서를 사용할 수 있지만 vCenter Server 를 View 에 추가할 때 인증서 지문을 허용해야 합니다.

- 복제된 그룹의 모든 View 연결 서버 인스턴스가 vCenter Server 호스트에 설치된 서버 인증서의 루트 CA 인증서를 신뢰하는지 확인합니다. View 연결 서버 호스트의 Windows 로컬 컴퓨터 인증서 저장소에 있는 Trusted Root Certification Authorities > Certificates 폴더에 루트 CA 인증서가 있는지 확인합니다. 없는 경우, Windows 로컬 컴퓨터 인증서 저장소로 루트 CA 인증서를 가져오십시오.

  VMware View 설치 문서에서 "Windows 인증서 저장소로 루트 인증서 및 중간 인증서 가져오기"를 참조하십시오.

- vCenter Server 및 View Composer 에 대한 최대 작업 수를 결정하는 설정에 익숙해지십시오. "vCenter Server 및 View Composer 의 최대 동시 작업 수," (95 페이지) 및 "View 데스크톱 로그온 스톰을 지원하기 위한 동시 전원 작업 속도 설정," (95 페이지)의 내용을 참조하십시오.

프로시저

1 View Administrator 에서 **View 구성 > 서버**.

2 vCenter Servers 탭에서 **추가**를 클릭합니다.

3 vCenter Server 설정의 서버 주소 텍스트 상자에 vCenter Server 인스턴스의 정규화된 도메인 이름(FQDN)을 입력합니다.

  FQDN 에는 호스트 이름과 도메인 이름이 포함되어 있습니다. 예를 들어 FQDN *myserverhost.companydomain.com* 에서 *myserverhost* 는 호스트 이름이고 *companydomain.com* 은 도메인입니다.

  참고 DNS 이름 또는 URL 을 사용해 서버를 입력한 경우에는 View Manager 에서 DNS 조회를 통해 이전에 관리자가 IP 주소를 사용하여 View Manager 에 이 서버를 추가했는지 여부를 확인하지 않습니다. DNS 이름과 IP 주소를 모두 사용해 vCenter Server 를 추가하면 충돌이 발생합니다.

4 vCenter Server 사용자 이름을 입력하십시오.

5 vCenter Server 사용자 암호를 입력하십시오.

6 (선택 사항) 이 vCenter Server 인스턴스에 대한 설명을 입력하십시오.

7 TCP 포트 번호를 입력하십시오.

  기본 포트는 443 입니다.

8 '고급 설정'에서 vCenter Server 및 View Composer 작업에 대한 최대 동시 작업 수를 설정합니다.

9 **다음**을 클릭하여 'View Composer 설정' 페이지를 표시합니다.

후속 작업

View Composer 설정을 구성합니다.

- vCenter Server 인스턴스가 서명된 SSL 인증서로 구성되었고 View 연결 서버가 루트 인증서를 신뢰하는 경우, 'vCenter Server 추가' 마법사가 'View Composer 설정' 페이지를 표시합니다.
- vCenter Server 인스턴스가 기본 인증서로 구성된 경우, 우선 기존 인증서의 지문을 허용할 것인지 결정해야 합니다. "기본 SSL 인증서 지문 허용," (96 페이지)의 내용을 참조하십시오.

View Manager 가 다수의 vCenter Server 인스턴스를 사용하는 경우, 이 절차를 반복하여 다른 vCenter Server 인스턴스를 추가합니다.

View Composer 설정 구성

View Composer 를 사용하려면 View Manager 가 View Composer 서비스에 연결할 수 있도록 설정을 구성해야 합니다. View Composer 는 별도의 고유 호스트 또는 vCenter Server 와 동일한 호스트에 설치할 수 있습니다.

각 View Composer 서비스와 vCenter Server 인스턴스 사이에 일대일 매핑이 존재해야 합니다. View Composer 서비스는 단 하나의 vCenter Server 인스턴스에서 사용될 수 있습니다. vCenter Server 인스턴스는 단 하나의 View Composer 서비스와만 연결할 수 있습니다.

필수 조건

- 연결된 클론을 포함하고 있는 Active Directory 도메인에서 가상 컴퓨터를 추가 및 제거하려면 Active Directory 관리자가 사용 권한을 가진 도메인 사용자를 생성해야 합니다. Active Directory 에서 연결된 클론 시스템 계정을 관리하려면 도메인 사용자에게 **컴퓨터 개체 생성**, **컴퓨터 개체 삭제**및 **모든 속성 쓰기** 권한이 있어야 합니다.

  "View Composer 에 대한 사용자 계정 생성," (27 페이지)의 내용을 참조하십시오.

- vCenter Server 에 연결할 View Manager 를 구성했는지 확인하십시오. 이를 위해, 'vCenter Server 추가' 마법사의 'vCenter Server 정보' 페이지를 완료해야 합니다. "View Manager 에 vCenter Server 인스턴스 추가," (90 페이지)의 내용을 참조하십시오.

- 이 View Composer 서비스가 다른 vCenter Server 인스턴스에 연결하도록 이미 구성되어 있지 않은지 확인합니다.

프로시저

1 View Administrator 에서 'vCenter Server 추가' 마법사의 'vCenter Server 정보' 페이지를 완료합니다.

   a **View 구성 > 서버**.

   b vCenter Servers 탭에서 **추가**를 클릭하고 vCenter Server 설정을 제공합니다.

2 'View Composer 설정' 페이지에서 View Composer 를 사용하지 않는 경우 **View Composer 사용 안 함**을 선택합니다.

   View Composer 사용 안 함을 선택하는 경우, 다른 View Composer 설정이 비활성화됩니다. **다음**을 클릭하면 'vCenter Server 추가' 마법사가 '호스트 캐시 설정' 페이지를 표시합니다. 'View Composer 도메인' 페이지는 표시되지 않습니다.

3 View Composer 를 사용하는 경우, View Composer 호스트의 위치를 선택합니다.

옵션	설명
View Composer 는 vCenter Server 와 동일한 호스트에 설치됩니다.	a **vCenter Server 와 함께 설치된 View Composer** 를 선택합니다. b 포트 번호가 vCenter Server 에 View Composer 서비스를 설치할 때 지정한 포트 번호와 동일한지 확인합니다. 기본 포트 번호는 18443 입니다.
View Composer 가 별도의 고유 호스트에 설치됩니다.	a **독립 실행형 View Composer 서버**를 선택합니다. b View Composer 서버 주소 텍스트 상자에 View Composer 호스트의 FQDN(정규화된 도메인 이름)을 입력합니다. c View Composer 사용자 이름을 입력합니다. d View Composer 사용자 암호를 입력합니다. e 포트 번호가 View Composer 서비스를 설치할 때 지정한 포트 번호와 동일한지 확인합니다. 기본 포트 번호는 18443 입니다.

4 **다음**을 클릭하여 'View Composer 도메인' 페이지를 표시합니다.

후속 작업

View Composer 도메인을 구성합니다.

- View Composer 인스턴스가 서명된 SSL 인증서로 구성되었고 View 연결 서버가 루트 인증서를 신뢰하는 경우, 'vCenter Server 추가' 마법사가 'View Composer 도메인' 페이지를 표시합니다.
- View Composer 인스턴스가 기본 인증서로 구성된 경우, 우선 기존 인증서의 지문을 허용할 것인지 결정해야 합니다. "기본 SSL 인증서 지문 허용," (96 페이지)의 내용을 참조하십시오.

View Composer 도메인 구성

View Composer 가 연결된 클론 데스크톱을 배포하는 Active Directory 도메인을 구성해야 합니다. View Composer 에 대해 여러 도메인을 구성할 수 있습니다. 우선 View 에 vCenter Server 와 View Composer 설정을 추가한 후, View Administrator 에서 vCenter Server 인스턴스를 편집하여 View Composer 도메인을 추가할 수 있습니다.

필수 조건

View Administrator 에서 'vCenter Server 추가' 마법사의 'vCenter Server 정보' 및 'View Composer 설정' 페이지를 완료했는지 확인합니다.

프로시저

1 'View Composer 도메인' 페이지에서 **추가**를 클릭하여 View Composer 계정 정보에 대한 도메인 사용자를 추가합니다.

2 Active Directory 도메인의 도메인 이름을 입력하십시오.

예: **domain.com**

3 도메인 이름을 포함한 도메인 사용자 이름을 입력하십시오.

예: **domain.com₩admin**

4 계정 암호를 입력하십시오.

5 **확인**을 클릭합니다.

6 연결된 클론 풀을 배포한 다른 Active Directory 도메인에 권한을 가진 도메인 사용자 계정을 추가하려면 앞의 단계를 반복하십시오.

7 **다음**을 클릭하여 '호스트 캐시 설정' 페이지를 표시합니다.

후속 작업

View 에 대한 호스트 캐시 설정을 구성합니다.

vCenter Server 에 View Storage Accelerator(호스트 캐싱) 구성

vSphere 5.0 이상 버전의 경우, ESXi 호스트를 구성하여 가상 컴퓨터 디스크 데이터를 캐시할 수 있습니다. View Storage Accelerator 라고 하는 이 기능은 ESXi 호스트의 CBRC(Content Based Read Cache) 기능을 사용합니다. 호스트 캐싱은 여러 데스크톱이 한꺼번에 시작하거나 바이러스 백신을 실행할 때 발생할 수 있는 I/O 스톰 중 View 성능을 향상시킵니다. 스토리지 시스템에서 전체 OS 를 반복해서 읽는 대신, 호스트는 캐시에서 공통 데이터 블록을 읽을 수 있습니다.

부트 스톰 중 IOPS 수가 감소되면 호스트 캐싱이 스토리지 어레이의 요구를 감소시키게 되고, 따라서 View 배포를 지원하는 스토리지 I/O 대역폭을 덜 사용하게 됩니다.

vCenter Server 에 View 인터페이스를 사용하여 ESXi 호스트에서 캐싱을 사용하도록 설정합니다.

이 기능을 사용하도록 설정하려면 개별 데스크톱 풀의 호스트 캐싱도 구성해야 합니다. 호스트 캐싱은 명시적으로 사용하도록 설정할 때까지 풀에 대해 활성화되지 않습니다. 풀을 생성 또는 편집할 때 호스트 캐싱을 사용하도록 설정할 수 없습니다. 기존 풀을 편집하여 호스트 캐싱을 사용하지 않도록 설정할 수 있습니다.

전체 가상 컴퓨터를 포함하는 연결된 클론 및 풀이 있는 풀에서 호스트 캐싱을 사용하도록 설정할 수 있습니다.

호스트 캐싱은 로컬 모드에서도 지원됩니다. 사용자는 호스트 캐싱에 활성화된 풀의 데스크톱을 체크아웃할 수 있습니다. 데스크톱이 체크아웃되었을 때는 호스트 캐싱이 사용되지 않고 데스크톱이 체크인하면 다시 사용됩니다.

View Composer 어레이 통합은 호스트 캐싱의 사용이 지정된 풀에서 지원되지 않습니다. View Composer 어레이 통합은 VAAI(vStorage APIs for Array Integration) 기본 NFS 스냅샷 기술을 사용하여 가상 컴퓨터를 복제합니다.

필수 조건

- vCenter Server 및 ESXi 호스트 버전이 5.0 이상인지 확인하십시오.

  ESXi 클러스터에서 모든 호스트가 버전 5.0 이상인지 확인합니다.

- vCenter Server 사용자가 vCenter Server의 **전역 > vCenter Server 역할** 권한을 할당 받았는지 확인하십시오. vCenter Server 사용자에게 필요한 View Manager 및 View Composer 권한에 대해 설명하는 *VMware View 설치* 설명서의 항목을 참조하십시오.

프로시저

1 View Administrator에서 '호스트 캐시 설정' 페이지 이전에 표시되는 'vCenter Server 추가' 마법사 페이지를 완료합니다.

   a **구성 보기 > 서버**를 선택합니다.

   b vCenter Servers 탭에서 **추가**를 클릭합니다.

   c 'vCenter Server 정보', 'View Composer 설정' 및 'View Composer 도메인' 페이지를 완료합니다.

2 '호스트 캐시 설정' 페이지에서 **View에 대한 호스트 캐싱 사용** 확인란을 선택합니다.

3 기본 호스트 캐시 크기를 지정합니다.

   기본 캐시 크기는 이 vCenter Server 인스턴스에서 관리하는 모든 ESXi 호스트에 적용됩니다.

   기본값은 1,024MB 입니다. 캐시 크기는 100MB 와 2,048MB 사이여야 합니다.

4 개별 ESXi 호스트에 다른 캐시 크기를 지정하려면 ESXi 호스트를 선택하고 **캐시 크기 편집**을 클릭하십시오.

   a 호스트 캐시 대화 상자에서 **기본 호스트 캐시 크기 재정의**를 선택합니다.

   b 100MB 와 2,048MB 사이의 **호스트 캐시 크기**를 입력하고 **확인**을 클릭합니다.

5 '호스트 캐시 설정' 페이지에서 **다음**을 클릭합니다.

6 **마침**을 클릭하여 vCenter Server, View Composer 및 호스트 캐시 설정을 View에 추가합니다.

후속 작업

클라이언트 연결에 대한 PCoIP 보안 게이트웨이, 보안 터널 및 외부 URL을 구성하려면 "View Client 연결 구성," (97 페이지)을 참조하십시오.

View에서 호스트 캐시 설정을 지정하려면 데스크톱 풀에 호스트 캐싱을 구성하십시오. *VMware View 관리* 문서에서 "데스크톱 풀에 호스트 캐싱 구성"을 참조하십시오.

vCenter Server 및 View Composer 의 최대 동시 작업 수

vCenter Server 를 View 에 추가하거나 vCenter Server 설정을 편집하는 경우, vCenter Server 및 View Composer 가 수행하는 최대 동시 작업 수를 설정하는 몇 가지 옵션을 구성할 수 있습니다.

'vCenter Server 정보' 페이지의 '고급 설정' 패널에서 이 옵션을 구성합니다.

표 8-4. vCenter Server 및 View Composer 의 최대 동시 작업 수

설정	설명
최대 동시 vCenter 프로비저닝 작업 수	이 vCenter Server 인스턴스에서 전체 가상 컴퓨터를 프로비저닝하고 삭제하기 위해 View Manager 에 허용되는 최대 동시 요청 수를 결정합니다. 기본값은 20 입니다. 이 설정은 전체 가상 컴퓨터에만 적용됩니다.
최대 동시 전원 작업 수	이 vCenter Server 인스턴스에서 View Manager 가 관리하는 가상 컴퓨터에 수행될 수 있는 최대 동시 전원 작업 수를 결정합니다(시작, 종료, 일시 중단 등). 기본값은 50 입니다. 이 설정에 대한 값을 계산하기 위한 내용은 "View 데스크톱 로그온 스톰을 지원하기 위한 동시 전원 작업 속도 설정," (95 페이지)을 참조하십시오. 이 설정은 전체 가상 컴퓨터 및 연결된 클론에 적용됩니다.
최대 동시 View Composer 유지 관리 작업 수	이 View Composer 인스턴스에 의해 관리되는 연결된 클론에서 수행될 수 있는 최대 동시 View Composer 새로 고침, 재구성 및 재조정 작업 수를 결정합니다. 기본값은 12 입니다. 유지 관리 작업을 시작하려면 먼저 활성 세션이 있는 데스크톱을 로그오프해야 합니다. 유지 관리 작업을 시작하는 즉시 사용자를 강제로 로그오프시키는 경우, 로그오프가 필요한 데스크톱에서 가능한 최대 동시 작업의 수는 구성된 값의 절반입니다. 예를 들어, 이 설정을 24 로 구성하고 사용자를 강제로 로그오프시키는 경우, 로그오프가 필요한 데스크톱에서 가능한 최대 동시 작업의 수는 12 입니다. 이 설정은 연결된 클론에만 적용됩니다.
최대 동시 View Composer 프로비저닝 작업 수	이 View Composer 인스턴스에 의해 관리되는 연결된 클론에서 수행될 수 있는 최대 동시 생성 및 삭제 작업 수를 결정합니다. 기본값은 8 입니다. 이 설정은 연결된 클론에만 적용됩니다.

View 데스크톱 로그온 스톰을 지원하기 위한 동시 전원 작업 속도 설정

최대 동시 전원 작업 수 설정은 vCenter Server 인스턴스의 View 데스크톱 가상 컴퓨터에서 이루어질 수 있는 최대 동시 전원 작업의 수를 관리합니다. View 5.0 부터 이 제한은 기본적으로 50 으로 설정됩니다. 많은 사용자가 데스크톱에 동시에 로그온할 때 최대 전원 켜기 속도를 지원하도록 이 값을 변경할 수 있습니다.

가장 모범적인 방법으로 이 설정에 적합한 값을 결정하기 위한 예비 단계를 수행할 수 있습니다. 계획 가이드라인에 대해서는 *VMware View 아키텍처 계획* 문서에서 "아키텍처 설계 요소 및 계획 가이드라인"을 참조하십시오.

필요한 동시 전원 작업 수는 데스크톱의 전원이 켜지는 최대 속도 및 데스크톱이 켜지고 부팅되어 연결 가능한 상태가 되기까지 걸리는 시간에 따라 결정됩니다. 일반적으로, 권장되는 전원 작업 제한은 데스크톱이 시작되는 데 걸리는 총 시간에 최대 전원 켜기 속도를 곱한 값입니다.

예를 들어, 데스크톱이 시작되는 데 평균 2, 3 분이 걸립니다. 따라서, 동시 전원 작업 제한은 최대 전원 켜기 속도에 3 을 곱한 값이 됩니다. 50 의 기본 설정에서 분당 16 데스크톱의 최대 전원 켜기 속도가 지원됩니다.

View 는 최대 5 분 동안 데스크톱이 켜지기를 기다립니다. 시작 시간이 더 오래 걸리면 다른 오류가 발생할 가능성이 큽니다. 동시 전원 작업 제한을 최대 전원 켜기 속도의 5 배로 설정하면 보다 넉넉합니다. 넉넉한 설정에서 50 의 기본 설정은 분당 10 데스크톱의 최대 전원 켜기 속도를 지원합니다.

로그온, 따라서 데스크톱 전원 켜기 작업은 일반적으로 특정 시간 범위에 걸쳐 정규 분포 형태로 발생합니다. 전원 켜기 작업의 약 40%가 시간 범위의 1/6 에서 발생하는 시간 범위의 중간에서 최대 전원 켜기 속도가 발생한다고 가정하고 이 속도의 근사치를 구할 수 있습니다. 예를 들어, 사용자가 오전 8:00 ~ 오전 9:00 시 사이에 로그온하는 경우, 시간 범위는 1 시간이고 로그온의 40%가 오전 8:25 ~ 오전 8:35 의 10 분 사이에 이루어집니다. 2,000 명의 사용자가 있다고 했을 때 이들 중 20%의 데스크톱 전원이 꺼져 있고 400 데스크톱 전원 켜기 작업의 40%는 이 10 분 동안 이루어집니다. 최대 전원 켜기 속도는 분당 16 데스크톱입니다.

기본 SSL 인증서 지문 허용

View 에 vCenter Server 및 View Composer 인스턴스를 추가하는 경우, vCenter Server 및 View Composer 인스턴스에 사용되는 SSL 인증서가 유효하고 View 연결 서버에서 신뢰하는지 확인해야 합니다. vCenter Server 및 View Composer 와 함께 설치된 기본 인증서가 아직 사용되고 있는 경우, 이 인증서의 지문을 허용할 것인지 여부를 결정해야 합니다.

vCenter Server 또는 View Composer 인스턴스가 CA 에서 서명한 인증서로 구성되었고 루트 인증서를 View 연결 서버에서 신뢰하는 경우, 인증서 지문을 허용할 필요가 없습니다. 어떤 조치도 필요하지 않습니다.

기본 인증서를 CA 에서 서명한 인증서로 대체하지만 View 연결 서버가 루트 인증서를 신뢰하지 않는 경우, 인증서 지문을 허용할지 여부를 결정해야 합니다. 지문은 인증서의 암호화된 해시입니다. 지문은 제공된 인증서가 이전에 수용된 인증서와 같이 다른 인증서와 동일한지 여부를 빠르게 확인하는 목적으로 이용됩니다.

참고 동일 Windows Server 호스트에 vCenter Server 와 View Composer 를 설치하는 경우, 동일 SSL 인증서의 사용이 가능하지만 각 구성 요소에 대해 개별적으로 인증서를 구성해야 합니다.

SSL 인증서 구성에 대한 자세한 내용은 View Server 를 위한 SSL 인증서 구성을 참조하십시오.

우선 View Administrator 의 'vCenter Server 추가' 마법사에서 vCenter Server 와 View Composer 를 View 에 추가합니다. 인증서를 신뢰할 수 없고 사용자가 지문을 허용하지 않으면 vCenter Server 와 View Composer 를 View 에 추가할 수 없습니다.

이러한 서버가 View 에 추가되면 'vCenter Server 편집' 대화 상자에서 이를 다시 구성할 수 있습니다.

참고 이전 View 버전을 View 5.1 이상 버전으로 업그레이드하고 vCenter Server 또는 View Composer 인증서를 신뢰할 수 없는 경우, 혹은 신뢰할 수 있는 인증서를 신뢰할 수 없는 인증서로 대체하는 경우에도 인증서 지문을 허용해야 합니다.

View Administrator 대시보드에서 vCenter Server 또는 View Composer 아이콘이 빨간색으로 바뀌고 '유효하지 않은 인증서 탐지됨' 대화 상자가 나타납니다. **확인**을 클릭하고 여기에 나타난 절차를 따라야 합니다.

프로시저

1 View Administrator 에 '유효하지 않은 인증서 탐지됨' 대화 상자가 표시되면 **인증서 보기**를 클릭합니다.

2 '인증서 정보' 창에서 인증서 지문을 검사합니다.

3 vCenter Server 또는 View Composer 인스턴스에 대해 구성된 인증서 지문을 검사합니다.

   a vCenter Server 또는 View Composer 호스트에서 MMC 스냅인을 시작하고 Windows 인증서 저장소를 엽니다.

   b vCenter Server 또는 View Composer 인증서로 이동합니다.

   c '인증서 세부 내용' 탭을 클릭하여 인증서 지문을 표시합니다.

4 '인증서 정보' 창의 지문이 vCenter Server 또는 View Composer 인스턴스에 대한 지문과 일치하는지 확인합니다.

5 인증서 지문을 허용할 것인지 결정합니다.

옵션	설명
지문이 일치합니다.	기본 인증서를 사용하려면 **허용**을 클릭합니다.
지문이 일치하지 않습니다.	**거부**를 클릭합니다. 일치하지 않는 인증서 문제를 해결합니다. 예를 들어, vCenter Server 또는 View Composer에 잘못된 IP 주소를 제공했을 수도 있습니다.

View Client 연결 구성

View 클라이언트는 보안 연결을 통해 View 연결 서버 또는 보안 서버 호스트와 통신합니다.

사용자가 View Client에 도메인 이름을 제공할 때 HTTPS를 통해 사용자 인증 및 View 데스크톱 선택에 사용되는 초기 View Client 연결이 생성됩니다. 네트워크 환경에 방화벽과 로드 밸런싱 소프트웨어를 제대로 구성한 경우 이 요청이 View 연결 서버 또는 보안 서버 호스트에 전달됩니다. 이 연결로 사용자는 인증을 받고 데스크톱을 선택하지만 View 데스크톱에는 아직 연결되지 않은 상태입니다.

사용자가 View 데스크톱에 연결할 때 기본적으로 View Client에서 View 연결 서버 또는 보안 서버 호스트에 대한 두 번째 연결을 생성합니다. 이 연결은 HTTPS를 통해 RDP 및 다른 데이터를 전송하는 보안 터널을 제공하므로 터널 연결이라고 부릅니다.

사용자가 PCoIP 디스플레이 프로토콜로 View 데스크톱에 연결할 때 View Client는 View 연결 서버 또는 보안 서버 호스트에서 PCoIP 보안 게이트웨이에 대한 추가 연결을 생성할 수 있습니다. PCoIP 보안 게이트웨이는 인증된 사용자만 PCoIP를 통해 View 데스크톱과 통신하도록 허용합니다.

보안 터널 또는 PCoIP 보안 게이트웨이를 사용하지 않도록 설정되어 있으면 View 연결 서버 또는 보안 서버 호스트를 건너뛰고 클라이언트 시스템과 View 데스크톱 가상 컴퓨터 사이에 View 데스크톱 세션이 직접 구축됩니다. 이러한 연결 유형을 직접 연결이라 합니다.

View 연결 서버가 더 이상 실행되지 않아도 직접 연결을 사용하는 데스크톱 세션은 연결 상태를 유지합니다.

일반적으로 WAN을 통해 보안 서버 또는 View 연결 서버 호스트에 연결하는 외부 클라이언트에게 보안 연결을 제공하려면 보안 터널과 PCoIP 보안 게이트웨이를 모두 사용하도록 설정해야 합니다. 보안 터널과 PCoIP 보안 게이트웨이를 사용하지 않도록 설정하면 내부 LAN 연결 클라이언트가 View 데스크톱에 직접 연결을 구축하도록 허용할 수 있습니다.

씬 클라이언트와 같은 특정 View Client 끝점은 터널 연결을 지원하지 않고 RDP 데이터용 직접 연결을 사용하지만 PCoIP 데이터를 위해 PCoIP 보안 게이트웨이를 지원합니다.

SSL은 View 연결 서버 및 보안 서버 호스트에 대한 모든 클라이언트 연결에 필요합니다.

PCoIP 보안 게이트웨이 및 보안 터널 연결 구성

View Administrator를 사용해 보안 터널 및 PCoIP 보안 게이트웨이 사용을 구성합니다. 이들 구성 요소를 통해 인증 받은 사용자만 View 데스크톱과 통신할 수 있습니다.

PCoIP 디스플레이 프로토콜을 사용하는 클라이언트는 PCoIP 보안 게이트웨이를 사용할 수 있습니다. RDP 디스플레이 프로토콜을 사용하는 클라이언트는 보안 터널을 사용할 수 있습니다.

중요 외부 클라이언트에 보안 연결을 제공하는 기존 네트워크 구성에는 보안 서버가 포함되어 있습니다. 보안 서버의 보안 터널 및 PCoIP Secure Gateway를 사용 또는 사용하지 않도록 설정하려면 보안 서버에 연결되어 있는 View Connection Server 인스턴스를 편집해야 합니다.

외부 클라이언트를 View Connection Server 호스트에 직접 연결하는 네트워크 구성의 경우, View Administrator의 View Connection Server 인스턴스를 편집하여 보안 터널과 PCoIP 보안 게이트웨이를 사용 또는 사용하지 않도록 설정할 수 있습니다.

필수 조건

- PCoIP Secure Gateway를 사용하도록 설정할 경우, View Connection Server 인스턴스 및 연결된 보안 서버가 View 4.6 이상인지 확인하십시오.
- PCoIP Secure Gateway를 이미 사용하도록 설정한 View Connection Server 인스턴스와 보안 서버를 연결할 경우, 보안 서버가 View 4.6 이상인지 확인하십시오.

프로시저

1 View Administrator에서 **View 구성 > 서버**를 선택합니다.

2 View Connection Server 패널에서 View Connection Server 인스턴스를 선택하고 **편집**을 클릭하십시오.

3 보안 터널 사용을 구성하십시오.

옵션	설명
보안 터널 사용 안 함	**보안 터널을 사용하여 데스크톱에 연결**을 선택 해제합니다.
보안 터널 사용	**보안 터널을 사용하여 데스크톱에 연결**을 선택합니다.

기본적으로 보안 터널을 사용하도록 설정되어 있습니다.

4 PCoIP 보안 게이트웨이 사용을 구성하십시오.

옵션	설명
PCoIP 보안 게이트웨이 사용	**데스크톱에 대한 PCoIP 연결에 PCoIP 보안 게이트웨이 사용**을 선택합니다.
PCoIP 보안 게이트웨이 사용 안 함	**데스크톱에 대한 PCoIP 연결에 PCoIP 보안 게이트웨이 사용**을 선택 해제합니다.

기본적으로 PCoIP 보안 게이트웨이를 사용하지 않도록 설정되어 있습니다.

5 변경 사항을 저장하려면 **확인**을 클릭하십시오.

PCoIP 보안 게이트웨이 및 터널 연결용 외부 URL 구성

보안 터널을 사용하려면 클라이언트 시스템에서 클라이언트가 View 연결 서버 또는 보안 서버 호스트에 연결하는 데 사용하는 IP 주소를 확인할 수 있는 FQDN(정규화된 도메인 이름) 또는 IP 주소에 액세스할 수 있어야 합니다. PCoIP 보안 게이트웨이를 사용하려면 클라이언트 시스템에서 클라이언트가 View 연결 서버 또는 보안 서버 호스트에 연결하는 데 사용하는 IP 주소에 액세스할 수 있어야 합니다.

외부 위치에서 터널 연결 사용

기본적으로 View 연결 서버 또는 보안 서버 호스트는 동일 네트워크에 위치한 터널 클라이언트로만 연결할 수 있으므로 요청한 호스트를 찾을 수 있습니다.

많은 조직의 경우, 특정 IP 주소 또는 클라이언트가 확인할 수 있는 도메인 이름 및 특정 포트를 사용해 사용자가 외부 위치에서 연결할 것을 요구하고 있습니다. 이 정보는 View 연결 서버 또는 보안 서버 호스트의 실제 주소 및 포트 번호와 유사하거나 다를 수 있습니다. 이 정보는 클라이언트 시스템에 URL 형태로 제공됩니다. 예:

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://10.20.30.40:443`

View Manager 에서 이러한 주소를 사용하려면 호스트의 FQDN 이 아닌 외부 URL 로 반환되도록 View 연결 서버 또는 보안 서버 호스트를 구성해야 합니다.

외부 URL 구성

외부 URL 을 2 개 구성합니다. 하나는 클라이언트 시스템에서 터널 연결할 수 있는 URL 입니다. 다른 하나는 PCoIP 를 사용하는 클라이언트 시스템이 PCoIP 보안 게이트웨이를 통해 보안 연결할 수 있는 URL 입니다. 클라이언트 시스템이 외부 위치에서 연결할 수 있는 IP 주소로 PCoIP 외부 URL 을 지정해야 합니다.

네트워크 구성에 보안 서버가 포함된 경우 보안 서버용 외부 URL 을 제공하십시오. 보안 서버에 연결되는 View 연결 서버 인스턴스에는 외부 URL 이 필요하지 않습니다.

외부 URL 을 구성하는 프로세스는 View 연결 서버 인스턴스 및 보안 서버와 다릅니다.

- View 연결 서버 인스턴스의 경우 View Administrator 의 View 연결 서버 설정을 편집하여 외부 URL 을 설정합니다.
- 보안 서버의 경우 View 연결 서버 설치 프로그램을 실행할 때 외부 URL 을 설정합니다. View Administrator 를 사용해 보안 서버용 외부 URL 을 수정할 수 있습니다.

View 연결 서버 인스턴스의 외부 URL 설정

View Administrator 를 사용하여 View 연결 서버 인스턴스의 외부 URL 을 구성합니다.

보안 터널 외부 URL 및 PCoIP 외부 URL 모두 클라이언트 시스템에서 이 View 연결 서버 인스턴스에 도달하기 위해 사용하는 주소여야 합니다. 예를 들어 이 인스턴스의 보안 터널 외부 URL 및 연결된 보안 서버의 PCoIP 외부 URL 을 지정하지 마십시오.

프로시저

1 View Administrator 에서 **View 구성 > 서버**.

2 View 연결 서버 패널에서 View 연결 서버 인스턴스를 선택하고 **편집**을 클릭하십시오.

3 **외부 URL** 텍스트 상자에 보안 터널 외부 URL 을 입력합니다.

URL 에는 프로토콜, 클라이언트에서 확인 가능한 호스트 이름 및 포트 번호가 포함되어야 합니다.

예: **https://view.example.com:443**

참고 호스트 이름을 확인할 수 없을 때 View 연결 서버 인스턴스에 액세스해야 하는 경우 IP 주소를 사용할 수 있습니다. 그러나 연결하는 호스트가 해당 View 연결 서버 인스턴스에 대해 구성된 SSL 인증서와 일치하지 않아 액세스가 차단되거나 약화된 보안 수준으로 액세스하게 됩니다.

4 **PCoIP 외부 URL** 텍스트 상자에 PCoIP 보안 게이트웨이 외부 URL 을 입력합니다.

포트 번호 4172 를 가진 IP 주소로 PCoIP 외부 URL 을 지정합니다. 프로토콜 이름은 포함시키지 마십시오.

예: 10.20.30.40:4172

URL 에는 클라이언트 시스템에서 이 View 연결 서버 호스트에 도달하기 위해 사용할 수 있는 IP 주소 및 포트 번호가 포함되어야 합니다. PCoIP 보안 게이트웨이가 View 연결 서버 인스턴스에 설치된 경우에만 텍스트 상자에 입력할 수 있습니다.

5 **확인**을 클릭합니다.

보안 서버의 외부 URL 수정

View Administrator 를 사용하여 보안 서버의 외부 URL 을 수정합니다.

View 연결 서버 설치 프로그램의 보안 서버 외부 URL 을 처음으로 구성합니다.

보안 터널 외부 URL 및 PCoIP 외부 URL 모두 클라이언트 시스템에서 이 보안 서버에 도달하기 위해 사용하는 주소여야 합니다. 예를 들어 이 보안 서버의 보안 터널 외부 URL 및 연결된 View 연결 서버 인스턴스의 PCoIP 외부 URL 을 지정하지 마십시오.

필수 조건

보안 서버 버전이 View 연결 서버 4.6 이상인지 확인하십시오.

프로시저

1 View Administrator 에서 **View 구성 > 서버**.

2 보안 서버 패널에서 보안 서버를 선택하고 **편집**을 클릭합니다.

편집 버튼은 보안 서버가 View 연결 서버 4.6 이상으로 업그레이드되지 않은 경우 사용할 수 없습니다.

3 **외부 URL** 텍스트 상자에 보안 터널 외부 URL 을 입력합니다.

URL 에는 프로토콜, 클라이언트에서 확인 가능한 보안 서버 호스트 이름 및 포트 번호가 포함되어야 합니다.

예: https://view.example.com:443

참고 호스트 이름을 확인할 수 없을 때 보안 서버에 액세스해야 하는 경우 IP 주소를 사용할 수 있습니다. 그러나 연결하는 호스트가 보안 서버에 대해 구성된 SSL 인증서와 일치하지 않아 액세스가 차단되거나 약화된 보안 수준으로 액세스하게 됩니다.

4 **PCoIP 외부 URL** 텍스트 상자에 PCoIP 보안 게이트웨이 외부 URL 을 입력합니다.

포트 번호 4172 를 가진 IP 주소로 PCoIP 외부 URL 을 지정합니다. 프로토콜 이름은 포함시키지 마십시오.

예: 10.20.30.40:4172

URL 에는 클라이언트 시스템에서 이 보안 서버에 도달하기 위해 사용할 수 있는 IP 주소 및 포트 번호가 포함되어야 합니다. PCoIP 보안 게이트웨이가 보안 서버에 설치된 경우에만 텍스트 상자에 입력할 수 있습니다.

5 변경 사항을 저장하려면 **확인**을 클릭합니다.

View Administrator 는 보안 서버에 업데이트된 외부 URL 을 보냅니다. 변경 내용이 적용되도록 보안 서버 서비스를 다시 시작할 필요가 없습니다.

Windows Server 설정을 크기 조정하여 배포 지원

View Manager 데스크톱을 크게 배포하기 위해 View Connection Server 를 설치할 Windows Server 컴퓨터를 구성할 수 있습니다. 각 컴퓨터에서 Windows 페이지 파일을 크기 조정할 수 있습니다.

64 비트 Windows Server 2008 컴퓨터에서 임시 포트, TCB 해시 테이블 및 Java 가상 시스템 설정이 기본적으로 크기 조정됩니다. 이렇게 조정하면 컴퓨터에는 예상된 사용자 로드와 함께 올바르게 실행할 적절한 리소스가 생깁니다.

기본적으로 시스템은 Windows Server 2008 에서 동시에 실행되는 약 16,000 개(최대값)의 임시 포트를 생성할 수 있습니다. 약 16,000 개의 임시 포트는 2,000 개 이상의 동시 클라이언트 연결(최고로 지원된 View Connection Server 인스턴스 수)를 지원할 수 있습니다.

Windows Server 2008 컴퓨터에서는 TCB 해시 테이블의 최대 크기를 늘리지 않아도 됩니다. 기본적으로 Windows Server 2008 은 이 값을 완전히 조정합니다.

View Connection Server 의 하드웨어 및 메모리 요구 사항을 보려면 "View 연결 서버의 하드웨어 요구 사항," (8 페이지)의 내용을 참조하십시오.

큰 View 배포에서 View Connection Server 를 사용하기 위한 하드웨어 및 메모리 권장 사항은 *VMware View 아키텍처 계획*의 "View Connection Server 최대값 및 가상 시스템 구성"을 참조하십시오.

Java 가상 시스템 크기 조정

View Connection Server 설치 관리자는 View Connection Server 컴퓨터의 Java 가상 시스템(JVM) 힙 메모리를 크기 조정하여 많은 수의 동시 View 데스크톱 세션을 지원합니다.

10GB 이상의 메모리를 가진 64 비트 Windows Server 컴퓨터에서 설치 관리자는 View Secure Gateway Server 구성 요소의 JVM 힙 크기 2GB 를 구성합니다. 이 구성은 View Connection Server 가 지원할 수 있는 최대값 약 2,000 개의 동시 터널 세션을 지원합니다. 10GB 메모리를 가진 64 비트 컴퓨터의 JVM 힙 크기 증가에는 이점이 없습니다.

참고 64 비트 View Connection Server 컴퓨터에서 50 개 이상의 View 데스크톱 배포에는 10GB 메모리가 권장됩니다. 작은 개념 증명 방식의 배포에는 10GB 미만의 메모리만 구성합니다.

64 비트 컴퓨터의 메모리가 10GB 미만인 경우 설치 관리자는 View Secure Gateway Server 구성 요소의 JVM 힙 크기 512MB 를 구성합니다. 컴퓨터의 메모리가 최소 요구량인 4GB 인 경우 이 구성은 약 500 개의 동시 터널 세션을 지원합니다. 이 구성은 작은 개념 증명 방식 배포를 지원하기에 충분합니다.

더 큰 배포를 지원하기 위해 64 비트 컴퓨터의 메모리를 10GB 까지 늘릴 경우 View Connection Server 는 JVM 힙 크기를 늘리지 않습니다. JVM 힙 크기를 권장하는 값으로 조정하려면 View Connection Server 를 다시 설치합니다.

중요 64 비트 Windows Server 컴퓨터에서 JVM 힙 크기를 변경하지 마십시오. 이 값을 변경하면 View Connection Server 동작이 불안정해질 수 있습니다. 64 비트 컴퓨터에서 View Connection Server 설치 관리자는 물리적 메모리에 맞춰 JVM 힙 크기를 설정합니다. 64 비트 View Connection Server 컴퓨터의 물리적 메모리를 변경할 경우 View Connection Server 를 다시 설치하여 JVM 힙 크기를 재설정합니다.

시스템 페이지 파일 설정 구성

시스템 페이지 파일 설정을 변경해 View Connection Server 인스턴스가 설치된 Windows Server 컴퓨터의 가상 메모리를 최적화할 수 있습니다.

Windows Server 를 설치한 경우 Windows 는 컴퓨터에 설치된 물리적 메모리에 기초해 초기 및 최대 페이지 파일 크기를 계산합니다. 이러한 기본 설정은 컴퓨터를 다시 시작한 후에도 그대로 유지됩니다.

Windows Server 컴퓨터가 가상 시스템인 경우, vCenter Server 를 통해 메모리 크기를 변경할 수 있습니다. 그러나 Windows 에서 기본 설정을 사용하면 새 메모리 크기에 맞춰 시스템 페이지 파일 크기가 조정되지 않습니다.

프로시저

1 View Connection Server 가 설치된 Windows Server 컴퓨터에서 Virtual Memory 대화 상자로 이동하십시오.

   기본적으로 **사용자 지정 크기**가 선택됩니다. 초기 및 최대 페이지 파일 크기가 표시됩니다.

2 **시스템이 관리하는 크기**를 클릭하십시오.

Windows 에서 현재 메모리 사용과 사용 가능한 메모리에 기초해 시스템 페이지 파일 크기를 계속해서 다시 계산합니다.

9 이벤트 데이터베이스 생성

View Manager 이벤트에 대한 정보를 기록하려면 이벤트 데이터베이스를 생성합니다. 이벤트 데이터베이스를 구성하지 않으면 로그 파일에서 이벤트 정보를 확인해야 하지만, 로그 파일에는 매우 제한된 정보만 담겨 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

View 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가

기존 데이터베이스 서버에 추가하는 방식을 사용해 이벤트 데이터베이스를 생성할 수 있습니다. 그런 다음 엔터프라이즈 보고 소프트웨어를 사용해 데이터베이스의 이벤트를 분석할 수 있습니다.

이벤트 데이터베이스의 데이터베이스 서버는 View Connection Server 호스트 자체 또는 전용 서버에 배치할 수 있습니다. 또는 View Composer 데이터베이스를 호스팅하는 서버와 같은 적절한 기존 데이터베이스 서버를 사용할 수 있습니다.

참고 이 데이터베이스에 대해 ODBC 데이터 소스를 생성할 필요가 없습니다.

필수 조건

- View Connection Server 인스턴스에서 액세스할 수 있는 시스템에 지원되는 Microsoft SQL Server 또는 Oracle 데이터베이스 서버가 있는지 확인하십시오. 지원되는 데이터베이스 버전 목록은 "View Composer 데이터베이스 요구 사항," (11 페이지)에 나와 있습니다.
- 데이터베이스 서버에 데이터베이스와 사용자를 생성하는 데 필요한 데이터베이스 권한이 있는지 확인하십시오.
- Microsoft SQL Server 데이터베이스 서버에서 데이터베이스를 생성하는 절차는 "SQL Server에 View Composer 데이터베이스 추가," (32 페이지)에 나와 있습니다.
- Oracle 데이터베이스 서버에서 데이터베이스를 생성하는 절차는 "Oracle 11g 또는 10g에 View Composer 데이터베이스 추가," (34 페이지)에 나와 있습니다.

프로시저

1 서버에 새 데이터베이스를 추가하고 ViewEvents와 같이 설명이 포함된 이름을 지정하십시오.

2 이 데이터베이스에 대해 테이블과 보기를 생성할 수 있는 권한을 가진 사용자를 추가하십시오. Oracle의 경우, 트리거와 시퀀스를 생성하는 권한을 비롯해 이들 개체를 읽고 쓰는 사용 권한을 가진 사용자를 추가하십시오.

Microsoft SQL Server 데이터베이스의 경우 인증 방법으로 통합 Windows 인증 보안 모델을 사용하지 마십시오. SQL Server 인증 방법을 사용해야 합니다.

데이터베이스는 생성되지만 View Administrator에 데이터베이스를 구성하기 전까지는 스키마가 설치되지 않습니다.

후속 작업

"이벤트 데이터베이스 구성," (105 페이지)의 지침을 따르십시오.

이벤트 보고용 SQL Server 데이터베이스 준비

View Administrator를 사용하여 Microsoft SQL Server에서 이벤트 데이터베이스를 구성하려면 올바른 TCP/IP 속성을 구성하고 서버에서 SQL Server Authentication을 사용해야 합니다.

필수 조건

- 이벤트 보고를 위해 SQL Server 데이터베이스를 생성합니다. 자세한 내용은 "View 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가," (103 페이지)에 나와 있습니다.
- 데이터베이스를 구성하기 위해 필요한 데이터베이스 권한이 있는지 확인합니다.
- 데이터베이스 서버는 인증 방법으로 SQL Server Authentication을 사용해야 합니다. Windows Authentication을 사용하지 마십시오.

프로시저

1 SQL Server Configuration Manager를 열고 **SQL Server*YYYY* 네트워크 구성**을 확장합니다.

2 ***server_name*의 프로토콜**을 선택합니다.

3 프로토콜 목록에서 TCP/IP를 마우스 오른쪽 단추로 클릭하고 **속성**을 선택합니다.

4 **사용** 속성을 **예**로 설정합니다.

5 포트가 할당되었는지 확인하거나 필요한 경우 포트를 할당합니다.

정적 및 동적 포트와 그 할당 방법에 대한 자세한 내용은 SQL Server Configuration Manager의 온라인 도움말을 참조하십시오.

6 이 포트가 방화벽으로 차단되는지 확인합니다.

후속 작업

View Administrator를 사용하여 데이터베이스를 View Connection Server에 연결합니다. "이벤트 데이터베이스 구성," (105 페이지)의 지침을 따르십시오.

이벤트 데이터베이스 구성

이벤트 데이터베이스는 로그 파일이 아닌 데이터베이스에 View 이벤트에 대한 정보를 저장합니다.

View 연결 서버 인스턴스를 설치한 후에 이벤트 데이터베이스를 구성합니다. View 연결 서버 그룹에서 호스트를 1 개만 구성하면 됩니다. 그룹의 나머지 호스트는 자동으로 구성됩니다.

참고 이벤트 트래픽이 View 환경의 상태 정보로 제한되기는 하지만 View 연결 서버 인스턴스와 외부 데이터베이스 사이의 데이터베이스 연결 보안은 관리자의 책임입니다. 보다 철저한 주의 조치를 위해서는 IPSec 등의 수단으로 이 채널의 보안을 강화하거나 View 연결 서버 컴퓨터에서 로컬로 데이터베이스를 배포할 수 있습니다.

Microsoft SQL Server 또는 Oracle 데이터베이스 보고 도구를 사용해 데이터베이스 테이블의 이벤트를 검토할 수 있습니다. 자세한 내용은 *VMware View Integration*(VMware View 통합) 설명서를 참조하십시오.

타사 분석 소프트웨어에서 이벤트 데이터에 액세스할 수 있도록 View 이벤트를 Syslog 형식으로 생성할 수도 있습니다. -l 옵션과 함께 vdmadmin 명령을 사용하여 이벤트 로그 파일에 Syslog 형식으로 View 이벤트 메시지를 기록합니다. *VMware View 관리* 문서에서 "-l 옵션을 사용하여 Syslog 형식으로 View 이벤트 로그 메시지 생성"을 참조하십시오.

필수 조건

이벤트 데이터베이스를 구성하려면 다음 정보가 필요합니다.

- 데이터베이스 서버의 DNS 이름 또는 IP 주소.
- 데이터베이스 서버 유형: Microsoft SQL Server 또는 Oracle
- 데이터베이스 서버 액세스 시 사용하는 포트 번호. Oracle 의 기본 포트 번호는 1521 이고 SQL Server 는 1433 입니다. SQL Server 의 경우 데이터베이스 서버가 명명된 인스턴스이거나 SQL Server Express 를 사용하면 포트 번호를 지정해야 할 수도 있습니다. SQL Server 의 명명된 인스턴스 연결에 대한 자세한 내용은 http://support.microsoft.com/kb/265808 의 Microsoft 기술 자료(KB) 문서를 참조하십시오.
- 데이터베이스 서버에 생성한 이벤트 데이터베이스 이름. "View 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가," (103 페이지)의 내용을 참조하십시오.
- 이 데이터베이스용으로 생성한 사용자의 사용자 이름과 암호. "View 이벤트에 대한 데이터베이스 및 데이터베이스 사용자 추가," (103 페이지)의 내용을 참조하십시오.

  이 사용자에 대해 SQL Server 인증을 사용하십시오. 통합 Windows 인증 보안 모델을 사용하지 마십시오.
- 이벤트 데이터베이스의 테이블 접두사(예: VE_). 접두사를 사용해 View 설치 간에 데이터베이스를 공유할 수 있습니다.

  참고 사용하는 데이터베이스 소프트웨어에 유효한 문자를 입력해야 합니다. 대화 상자를 완료할 때 접두사 구문을 검사하지 않습니다. 사용하는 데이터베이스 소프트웨어에 유효하지 않는 문자를 입력하면 View 연결 서버에서 데이터베이스 서버에 연결할 때 오류가 발생합니다. 로그 파일에는 이러한 오류와 데이터베이스 이름이 유효하지 않을 때 데이터베이스 서버에서 반환되는 다른 오류를 포함한 모든 오류가 기록됩니다.

프로시저

1 View Administrator 에서 **View 구성 > 이벤트 구성**.

2 **이벤트 데이터베이스** 섹션에서 **편집**을 클릭하고 필드에 정보를 입력한 다음 **확인**을 클릭하십시오.

3 (선택 사항) 이벤트 설정 창에서 **편집**을 클릭하고 이벤트를 표시할 시간, 이벤트를 새 이벤트로 분류할 일 수를 변경하고 **확인**을 클릭하십시오.

이 설정은 이벤트가 View Administrator 인터페이스에 표시되는 시간에 대한 설정입니다. 이 시점 이후에는 내역 데이터베이스 테이블에서만 이벤트를 볼 수 있습니다.

데이터베이스 구성 창에는 이벤트 데이터베이스의 현재 구성이 표시됩니다.

4 **모니터링 > 이벤트**를 선택하십시오.

연결이 실패한 경우 오류 메시지가 나타납니다. SQL Express 를 사용하거나 SQL Server 의 명명된 인스턴스를 사용하는 경우, 준비 단계에서 언급했듯이 올바른 포트 번호를 지정해야 합니다.

View Administrator 대시보드의 시스템 구성 요소 상태에 보고 데이터베이스 머리글 아래 이벤트 데이터베이스 서버가 표시됩니다.

10 View Client 설치 및 시작

VMware 웹 사이트 또는 View Connection Server에서 제공한 웹 액세스 페이지인 View Portal에서 Windows 기반 View Client 설치 관리자를 구할 수 있습니다. View Client를 설치한 후 최종 사용자를 위해 다양한 시작 옵션을 설정할 수 있습니다.

Mac용 View Client 및 iPad용 View Client와 같은 기타 View Client 설치 및 사용에 대한 자세한 내용은 특정 클라이언트에 관련된 문서를 참조하십시오. 자세한 내용은 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html에 나와 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

View Client용 View 연결 서버 준비

최종 사용자가 View 데스크톱에 연결할 수 있도록 하려면 관리자가 특정 작업을 수행해야 합니다.

최종 사용자가 View 연결 서버 또는 보안 서버에 연결하고 View 데스크톱에 액세스할 수 있으려면 특정 풀 설정 및 보안 설정을 구성해야 합니다.

- 보안 서버를 사용할 경우, View 연결 서버 4.6.1 및 View 보안 서버 4.6.1 이상을 사용 중이어야 합니다. View 4.6 이상에 대한 *VMware View 설치* 설명서를 참조하십시오.
- 클라이언트 장치를 위해 보안 연결을 사용하고, 보안 연결이 View 연결 서버 또는 보안 서버의 DNS 호스트 이름으로 구성될 경우, 클라이언트 장치가 DNS 이름을 확인할 수 있는지 확인하십시오.

  보안 터널을 사용하도록 또는 사용하지 않도록 설정하려면 View Administrator에서 View 연결 서버 설정 편집 대화 상자로 이동하여 **보안 터널을 사용하여 데스크톱에 연결** 확인란을 선택합니다.
- 가상 데스크톱 풀이 생성되었고 사용할 사용자 계정이 이 View 데스크톱에 액세스할 권한이 있는지 확인합니다. *VMware View 관리* 설명서의 데스크톱 풀 생성에 대한 항목을 참조하십시오.
- RSA SecurID 또는 RADIUS 인증과 같은 2요소 인증을 View Client에 사용하려면 View 연결 서버에서 이 기능을 사용하도록 설정해야 합니다. RADIUS 인증은 View 5.1 이상의 View 연결 서버에서 제공됩니다. 자세한 내용은 *VMware View 관리* 문서에서 2요소 인증 항목을 참조하십시오.

Windows 기반 View Client 또는 View Client with Local Mode 설치

최종 사용자가 물리적 시스템에서 가상 데스크톱에 연결하려면 View Client 를 엽니다. Windows 기반 설치 관리자 파일을 실행해 View Client 의 모든 구성 요소를 설치할 수 있습니다.

최종 사용자는 View Client with Local Mode 를 사용해 가상 데스크톱 복사본을 로컬 컴퓨터에 다운로드합니다. 그러면 최종 사용자는 네트워크 연결이 없어도 가상 데스크톱을 사용할 수 있습니다. 레거시는 최소화되고 성능은 향상됩니다.

View Client with Local Mode 는 이전 릴리스에서 View Client with Offline Desktop 이라는 시범적 기능이었던 전체 지원된 기능입니다.

이 절차는 대화식 설치 마법사를 사용하여 View Client 를 설치하는 방법에 대해 설명합니다. 이 방법 대신 명령줄을 사용하는 Microsoft Windows Installer(MSI)의 자동 설치 기능을 사용하려면 "View Client 자동 설치," (116 페이지)를 참조하십시오.

필수 조건

- 클라이언트 시스템에서 지원되는 운영 체제를 사용하는지 확인하십시오. 다음을 참조: "Windows 기반 View Client 및 View Client with Local Mode 지원 운영 체제," (16 페이지).
- 클라이언트 시스템에 관리자로 로그인할 수 있는지 확인하십시오.
- View Agent 가 설치되지 않았는지 확인하십시오.
- 로컬 모드 요구 사항:
  - 라이센스에 View Client with Local Mode 가 포함되어 있는지 확인하십시오.
  - 다음 제품 중 어느 것도 설치되지 않은 것을 확인합니다. View Client with Local Mode 를 설치할 수 없습니다.
- USB 리디렉션을 위한 요구 사항:
  - 클라이언트 장치 사용자가 가상 데스크톱에서 로컬로 연결된 USB 장치에 액세스할 수 있도록 허용할지 결정하십시오. 허용하지 않을 경우, 마법사에서 제공하는 **USB 리디렉션** 구성 요소를 선택 해제하거나 구성 요소를 설치하되 GPO 를 사용하여 해당 구성 요소를 사용하지 않도록 설정하십시오.

    하지만 **USB 리디렉션** 구성 요소를 설치하고 GPO 를 사용하여 USB 액세스를 제어하는 것이 좋습니다. 이렇게 하면 나중에 특정 클라이언트에 대해 USB 리디렉션을 사용하고 싶을 경우 View Client 를 다시 설치하지 않아도 됩니다. 자세한 내용은 *VMware View 관리* 문서의 구성 정책 관련 장에서 'View Client 구성 ADM 템플릿 설정' 항목을 참조하십시오.
  - **USB 리디렉션** 구성 요소를 설치하려면 클라이언트 컴퓨터에서 Windows 자동 업데이트 기능이 해제되어 있는지 확인하십시오.
- 최종 사용자가 현재 로그인한 사용자로서 View Client 와 가상 데스크톱에 로그인할 수 있도록 허용하는 기능을 사용할지 여부를 결정하십시오. 사용자가 클라이언트 시스템에 로그인할 때 입력한 자격 증명 정보가 View 연결 서버 인스턴스 그리고 최종적으로 가상 데스크톱에 전달됩니다. 일부 클라이언트 운영 체제에서는 이 기능을 지원하지 않습니다.
- 최종 사용자에게 가상 컴퓨터를 호스팅하는 View 연결 서버 인스턴스의 FQDN(정규화된 도메인 이름)을 지정하도록 요청하지 않으려면 설치하는 동안 지정할 수 있도록 FQDN 을 확인하십시오.

프로시저

1 관리자 권한을 가진 사용자로 클라이언트 시스템에 로그인하십시오.

2 클라이언트 시스템에서 http://www.vmware.com/products/의 VMware 제품 페이지에서 View Client 설치 관리자 파일을 다운로드하십시오.

적절한 설치 관리자 파일을 선택하십시오. *xxxxxx*는 빌드 번호이고 *y.y.y*는 버전 번호입니다.

옵션	조치
64 비트 운영 체제의 View Client	View Client 를 설치하려면 VMware-viewclient-x86_64-*y.y.y-xxxxxx*.exe 를 선택하십시오. View Client with Local Mode 를 설치하려면 VMware-viewclientwithlocalmode-x86_64-*y.y.y-xxxxxx*.exe 를 선택하십시오.
32 비트 운영 체제의 View Client	View Client 를 설치하려면 VMware-viewclient-*y.y.y-xxxxxx*.exe 를 선택하십시오. View Client with Local Mode 를 설치하려면 VMware-viewclientwithlocalmode-*y.y.y-xxxxxx*.exe 를 선택하십시오.

3 View Client 설치 프로그램을 시작하려면 설치 관리자 파일을 두 번 클릭하십시오.

4 필요한 구성 요소를 설치하려면 표시된 메시지를 따르십시오.

Windows 클라이언트 컴퓨터에 VMware View Client 서비스가 설치됩니다. View Client 의 서비스 이름은 wsnm.exe 입니다. USB 구성 요소에 대한 서비스 이름은 vmware-usbarbitrator.exe 및 vmware-view-usbd.exe 입니다.

후속 작업

View Client 를 시작하고 올바른 가상 데스크톱에 로그인할 수 있는지 확인합니다. 다음을 참조: "View 데스크톱에 로그인," (112 페이지) 또는 "View Portal 을 사용한 View Client 설치," (109 페이지).

View Portal 을 사용한 View Client 설치

View Client 또는 View Client with Local Mode 애플리케이션을 간단하게 다운로드하여 설치할 수 있는 방법은 브라우저를 열고 View Portal 웹 페이지를 검색하는 것입니다. View Portal 을 사용해 Windows 및 Mac 클라이언트 컴퓨터용 전체 View Client 설치 관리자를 다운로드할 수 있습니다.

View Client 를 다운로드하기 위한 VMware 다운로드 페이지로 이동하는 또 다른 방법으로 View 연결 서버 URL 로 이동할 수 있습니다. View Portal 의 링크가 VMware 다운로드 페이지가 아닌 다른 위치를 가리키도록 설정을 구성할 수도 있습니다.

필수 조건

- View Portal 의 링크가 VMware 다운로드 페이지가 아닌 다른 위치를 가리켜야 하는 경우, "View Portal 에 표시되는 View Client 다운로드 링크 구성," (110 페이지)을 참조하십시오.
- View 연결 서버 인스턴스에 대한 URL 이 있는지 확인하십시오.
- 클라이언트 시스템에 관리자로 로그인할 수 있는지 확인하십시오.
- 가상 데스크톱이 생성되었고 사용자 계정에 이 데스크톱에 액세스할 자격이 있는지 확인하십시오.
- 클라이언트 시스템에서 지원되는 운영 체제를 사용하는지 확인하십시오. 다음을 참조: "Windows 기반 View Client 및 View Client with Local Mode 지원 운영 체제," (16 페이지).
- View Agent 가 설치되지 않았는지 확인하십시오.
- 로컬 모드 요구 사항:
  - 라이센스에 View Client with Local Mode 가 포함되어 있는지 확인하십시오.
  - 다음 제품 중 어느 것도 설치되지 않은 것을 확인합니다. View Client with Local Mode 를 설치할 수 없습니다.

- USB 리디렉션을 위한 요구 사항:
  - 클라이언트 장치 사용자가 가상 데스크톱에서 로컬로 연결된 USB 장치에 액세스할 수 있도록 허용할지 결정하십시오. 허용하지 않을 경우, 마법사에서 제공하는 **USB 리디렉션** 구성 요소를 선택 해제하거나 구성 요소를 설치하되 GPO 를 사용하여 해당 구성 요소를 사용하지 않도록 설정하십시오.

    하지만 **USB 리디렉션** 구성 요소를 설치하고 GPO 를 사용하여 USB 액세스를 제어하는 것이 좋습니다. 이렇게 하면 나중에 특정 클라이언트에 대해 USB 리디렉션을 사용하고 싶을 경우 View Client 를 다시 설치하지 않아도 됩니다. 자세한 내용은 *VMware View 관리* 문서의 구성 정책 관련 장에서 'View Client 구성 ADM 템플릿 설정' 항목을 참조하십시오.
  - **USB 리디렉션** 구성 요소를 설치하려면 클라이언트 컴퓨터에서 Windows 자동 업데이트 기능이 해제되어 있는지 확인하십시오.

프로시저

1 관리자 권한을 가진 사용자로 클라이언트 시스템에 로그인하십시오.

2 브라우저를 열고 가상 데스크톱에 대한 액세스를 제공하는 View 연결 서버 인스턴스의 URL 을 입력하십시오.

  URL 에서 http 가 아닌 https 를 사용해야 합니다.

3 가지고 있는 운영 체제 유형(32 비트 또는 64 비트) 및 설치할 View Client 의 유형(로컬 모드가 있거나 없음)에 맞는 링크를 클릭합니다.

4 메시지가 표시되면 설치 관리자 파일을 클라이언트 시스템에 저장합니다.

5 View Client 설치 프로그램을 시작하려면 설치 관리자 파일을 두 번 클릭하십시오.

6 필요한 구성 요소를 설치하려면 표시된 메시지를 따르십시오.

후속 작업

View 데스크톱에 연결하십시오. 다음을 참조: "View 데스크톱에 로그인," (112 페이지).

View Portal 에 표시되는 View Client 다운로드 링크 구성

기본적으로, 브라우저를 열고 View 연결 서버 인스턴스의 URL 을 입력하면, 표시되는 View Portal 페이지에 View Client 를 다운로드하기 위한 VMware 다운로드 사이트 링크가 포함되어 있습니다. 기본값은 변경할 수 있습니다.

View Portal 의 기본 View Client 링크를 통해 호환되는 최신 View Client 설치 프로그램를 얻을 수 있습니다. 그러나 경우에 따라 내부 웹 서버를 가리키는 링크가 필요하거나 고유 View 연결 서버에서 특정한 클라이언트 버전을 사용할 수 있어야 할 수도 있습니다. 다른 URL 을 가리키도록 페이지를 재구성할 수 있습니다.

필수 조건

- 해당 환경에서 사용할 View Client 의 종류에 맞는 설치 관리자 파일을 다운로드합니다. View Client 다운로드 페이지 URL 은 https://www.vmware.com/go/viewclients 입니다.
- 설치 관리자 파일을 호스팅할 HTTP 서버를 결정합니다. 이 파일은 View 연결 서버 인스턴스 또는 다른 HTTP 서버에 있을 수 있습니다.

프로시저

1 설치 관리자 파일이 있는 HTTP 서버에서 설치 프로그램 파일이 들어갈 폴더를 만듭니다.

예를 들어, View 연결 서버 호스트의 downloads 폴더에 파일을 놓으려면 기본 설치 디렉토리에서 다음 경로를 사용합니다.

C:₩Program Files₩VMware₩VMware View₩Server₩broker₩webapps₩downloads

그러면 파일 링크에 https://*server-name*/downloads/*client-installer-file-name* 형식의 URL 이 사용됩니다. 예를 들어, view.mycompany.com 이름을 가진 서버는 Windows 용 View Client 에 다음 URL 을 사용합니다. https://view.mycompany.com/downloads/VMware-viewclient.exe. 이 예에서는 webapps 루트 폴더에 downloads 라는 폴더가 있습니다.

2 View Client 설치 관리자 파일을 폴더에 복사합니다.

폴더가 View 연결 서버에 있는 경우, VMware View 연결 서버 서비스를 다시 시작할 필요 없이 이 폴더의 모든 파일을 대체할 수 있습니다.

3 View 연결 서버 시스템에서 *install-path*₩Server₩Extras₩PortalExamples 에 있는 portal-links.properties 파일과 portal.properties 파일을 복사합니다.

4 C:₩ProgramData₩VMware₩VDM 디렉토리에 portal 폴더를 만들고 portal-links.properties 및 portal.properties 파일을 portal 폴더에 복사합니다.

5 설치 관리자 파일의 새 위치를 가리키도록 C:₩ProgramData₩VMware₩VDM₩portal₩portal-links.properties 파일을 편집합니다.

필요에 따라 이 파일의 라인을 편집하고 내용을 추가하여 추가 링크를 만들 수 있습니다. 라인을 삭제할 수도 있습니다.

다음 예는 Windows 용 View Client 를 위한 두 개의 링크 및 Linux 용 View Client 를 위한 두 개의 링크를 만드는 속성을 보여줍니다.

link.win=https://*server-name*/downloads/VMware-viewclient-x86_64-*y.y.y-XXXX*.exe#win
link.win.1=https://*server-name*/downloads/VMware-viewclient-*y.y.y-XXXX*.exe#win
link.linux=https://*server-name*/downloads/VMware-viewclient-x86_64-*y.y.y-XXXX*.rpm#linux
link.linux.1=https://*server-name*/downloads/VMware-viewclient-*y.y.y-XXXX*.tar.gz#linux

이 예에서 *y.y.y-XXXX* 는 버전 및 빌드 번호를 나타냅니다. 라인 끝에 있는 win 텍스트는 클라이언트에 Windows 운영 체제가 사용된 경우 이 링크가 브라우저에 나타난다는 것을 의미합니다. Windows 에는 win, Linux 에는 linux, 그리고 Mac OS X 에는 mac 을 사용합니다.

6 C:₩ProgramData₩VMware₩VDM₩portal₩portal.properties 파일을 편집하여 링크에 표시할 텍스트를 지정합니다.

이 라인은 # keys based on key names in portal-links.properties 라고 하는 파일 섹션에 나타납니다.

다음 예는 link.win 및 link.win.1 에 대해 지정된 링크에 해당하는 텍스트를 나타냅니다.

text.win=View Client for Windows 32 bit Client users text.win.1=View Client for Windows 64 bit Client users

7 VMware View 연결 서버 서비스를 다시 시작하십시오.

최종 사용자가 View 연결 서버에 대한 URL 을 입력하면 지정한 텍스트가 있는 링크가 표시됩니다. 이 링크는 지정된 위치를 가리킵니다.

View 데스크톱에 로그인

최종 사용자가 가상 데스크톱에 액세스하려면 클라이언트 디바이스에서 가상 데스크톱으로 로그인할 수 있는지 테스트하십시오. **시작** 메뉴 또는 클라이언트 시스템의 데스크톱 바로 가기에서 View Client 를 시작할 수 있습니다.

네트워크 연결을 사용할 수 있는 환경에서 사용자 세션은 View 연결 서버에서 인증됩니다.

필수 조건

- 사용자 이름/암호, RSA SecurID 사용자 이름/암호, RADIUS 인증 사용자 이름/암호 또는 스마트 카드 개인 ID 번호(PIN)와 같이 로그인에 필요한 자격 증명을 얻습니다.
- 로그인을 위한 도메인 이름을 얻습니다.
- "View Client 용 View 연결 서버 준비," (107 페이지).
- 회사 네트워크 외부에 있고 가상 데스크톱에 액세스하기 위해 보안 서버를 사용하지 않는 경우, 클라이언트 장치가 VPN 연결을 사용하도록 설정되어 있고 해당 연결을 켰는지 확인합니다.

  중요 VPN 이 아닌 보안 서버를 사용하는 것이 좋습니다.

- 가상 데스크톱에 액세스하는 서버의 정규화된 도메인 이름(FQDN)이 있는지 확인합니다. 포트가 443 이 아닌 경우 포트 번호도 필요합니다.
- RDP 디스플레이 프로토콜을 사용하여 View 데스크톱에 연결하려는 경우에는 AllowDirectRDP View Agent 그룹 정책 설정을 사용하도록 설정했는지 확인합니다.
- 관리자가 허용한 경우 View 연결 서버에서 제시한 SSL 인증서에 대한 인증서 검사 모드를 구성할 수 있습니다.

  어떤 모드를 사용할지 결정하려면 "Windows 용 View Client 에서 인증서 검사 구성," (82 페이지)을 참조하십시오.

프로시저

1 VMware View Client 데스크톱 바로 가기를 두 번 클릭하거나 **시작 > 프로그램** > VMware > VMware View Client.

2 **연결 서버** 드롭다운 메뉴에서 View 연결 서버 또는 보안 서버의 호스트 이름을 입력합니다.

3 대화 상자의 다른 선택적인 설정이 구성한 대로 나타나는지 확인합니다.

옵션	설명
현재 사용자로 로그인	이 확인란은 View Administrator 의 전역 설정에 따라 표시되거나 숨겨집니다. 로컬 모드에서 사용할 View 데스크톱을 체크아웃할 경우에는 이 확인란을 선택하지 마십시오.
포트	이 필드를 비워 두면 기본 포트 443 이 사용됩니다.
자동 연결	이 확인란을 선택할 경우 다음에 View Client 를 시작할 때 **연결 서버** 필드를 사용할 수 없으며 Autoconnect 확인란을 선택할 때 지정된 서버에 연결됩니다. 이 확인란을 해제하려면 표시되는 다음 대화 상자를 취소하고 **옵션**을 클릭하여 이 설정을 표시하고 변경합니다.
SSL 구성	View 관리자가 허용한 경우, 이 절차의 요구 사항에서 설명된 대로 이 링크를 클릭하여 인증서 검사 모드를 설정할 수 있습니다.

4 **연결**을 클릭합니다.

로그인 대화 상자가 나타나기 전에 확인 메시지가 표시될 수도 있습니다.

5 RSA SecurID 자격 증명 또는 RADIUS 인증 자격 증명을 묻는 메시지가 표시되면 사용자 이름과 암호를 입력하고 **계속**을 클릭합니다.

6 하나 이상의 데스크톱 풀을 사용할 권한이 있는 사용자의 자격 증명을 입력하고 도메인을 선택하여 **로그인**을 클릭합니다.

`user@domain` 형식을 사용하여 사용자 이름을 입력할 경우, 이름은 @ 기호로 인해 UPN 으로 처리되므로, 도메인 드롭다운 메뉴를 사용할 수 없습니다.

데스크톱 풀 생성 및 풀에 대한 사용자 권한 부여에 대한 자세한 내용은 *VMware View 관리* 문서를 참조하십시오.

7 데스크톱 목록이 나타나면 데스크톱을 선택합니다.

a (선택 사항) **디스플레이** 드롭다운 메뉴에서 View 데스크톱 표시를 위해 창 크기를 선택합니다.

다음 번에 데스크톱을 열면 기본으로 디스플레이 설정이 유지됩니다.

b (선택 사항) 디스플레이 프로토콜을 선택하려면 목록에서 데스크톱 옆에 있는 아래쪽 화살표를 클릭하고 **디스플레이 프로토콜**을 클릭하여 프로토콜을 선택합니다.

이 선택 사항은 View 관리자가 사용하도록 설정한 경우에만 사용할 수 있습니다. PCoIP 는 LAN 또는 WAN 을 통한 이미지, 오디오 및 비디오 컨텐츠 전송을 위한 최적화된 PC 환경을 제공합니다.

참고 로그인에 스마트 카드 자격 증명을 사용하고 있고 프로토콜을 전환하려는 경우, 로그오프했다가 다시 로그인해야 합니다.

다음 번에 데스크톱을 열면 기본으로 프로토콜 설정이 유지됩니다.

8 **연결**을 클릭합니다.

데스크톱에 연결됩니다.

연결되고 나면 클라이언트 창이 나타납니다.

View 연결 서버에 대한 인증이 실패하거나 View Client 가 데스크톱에 연결할 수 없는 경우 다음 작업을 수행하십시오.

- View 연결 서버가 SSL 을 사용하지 않도록 구성되어 있는지 확인합니다. View Client 를 사용하려면 SSL 연결이 필요합니다. View Administrator 의 전역 설정에서 **클라이언트 연결에 SSL 사용** 확인란이 선택 해제되어 있는지 확인합니다. 선택 해제되어 있다면 확인란을 선택하여 SSL 이 사용되도록 하거나 클라이언트가 HTTPS 지원 로드 밸런서 또는 View 연결 서버에 HTTP 로 연결하도록 구성된 다른 중간 디바이스에 연결할 수 있도록 환경을 설정해야 합니다.
- View 연결 서버의 보안 인증서가 올바르게 작동하는지 확인합니다. 올바르게 작동하지 않는 경우, View Administrator 에서 데스크톱의 View Agent 를 연결할 수 없고 전송 서버 상태가 준비되지 않은 것으로 표시될 수도 있습니다. 이는 인증서 문제로 발생한 추가 연결 문제의 증상입니다.
- View 연결 서버 인스턴스에 설정된 태그가 이 사용자의 연결을 허용하는지 확인합니다. *VMware View 관리* 문서를 참조하십시오.
- 사용자에게 이 데스크톱에 액세스할 권한이 있는지 확인합니다. *VMware View 관리* 문서를 참조하십시오.
- RDP 디스플레이 프로토콜을 사용하여 View 데스크톱에 연결하는 경우 클라이언트 컴퓨터가 원격 데스크톱 연결을 허용하는지 확인합니다.

후속 작업

- 시작 옵션을 구성하십시오.

View 연결 서버의 호스트 이름을 제공할 최종 사용자가 필요하지 않거나 다른 시작 옵션을 구성할 경우 View Client 명령줄 옵션을 사용하여 데스크톱 바로 가기를 생성하십시오.

VMware View 관리 문서를 참조하십시오.

- 로컬 모드에서 사용할 수 있는 데스크톱을 체크아웃하십시오.

  최종 사용자는 View Client with Local Mode 에서 제공한 목록에서 데스크톱 옆에 있는 아래 방향 화살표를 클릭하여 데스크톱이 체크아웃에 적합한지 결정할 수 있습니다. 데스크톱을 로컬 모드에서 사용할 수 있는 경우 컨텍스트 메뉴에 **체크아웃** 옵션이 나타납니다. 그룹에 데스크톱 액세스 권한이 있더라도 데스크톱을 체크아웃하는 사용자만 데스크톱에 액세스할 수 있습니다.

Windows 클라이언트에서 가상 프린터 기능의 인쇄 환경설정 설정

가상 인쇄 기능을 사용하면 최종 사용자가 추가 인쇄 드라이버를 View 데스크톱에 설치할 필요 없이 View 데스크톱에서 로컬 또는 네트워크 프린터를 사용할 수 있습니다. 이 기능을 통해 사용할 수 있는 각 프린터의 경우 데이터 압축, 인쇄 품질, 양면 인쇄, 색상 등의 환경을 설정할 수 있습니다.

프린터가 로컬 Windows 컴퓨터에 추가되고 나면 View 는 View 데스크톱에서 사용할 수 있는 프린터 목록에 해당 프린터를 추가합니다. 추가 구성은 필요하지 않습니다. 관리자 권한을 가진 사용자는 가상 프린터 구성 요소와의 충돌 없이 View 데스크톱에 프린터 드라이버를 계속 설치할 수 있습니다.

중요 이 기능은 다음 유형의 프린터에서 사용할 수 없습니다.

- View 데스크톱의 가상 USB 포트에 연결하기 위해 USB 리디렉션 기능을 사용 중인 USB 프린터

  가상 인쇄 기능을 함께 사용하기 위해 View 데스크톱에서 USB 프린터 연결을 끊어야 합니다.

- 파일로 인쇄하기 위한 Windows 기능

  인쇄 대화 상자에서 **파일로 인쇄** 확인란을 선택할 수 없습니다. 파일을 생성하는 프린터 드라이버를 사용할 수 있습니다. 예를 들어 PDF 작성 프로그램을 사용하여 PDF 파일로 인쇄할 수 있습니다.

필수 조건

View Agent 의 가상 인쇄 구성 요소가 View 데스크톱에 설치되어 있는지 확인합니다. View 데스크톱 파일 시스템의 드라이버는 C:₩Program Files₩Common Files₩VMware₩Drivers₩Virtual Printer 에 있습니다.

View Agent 설치는 View 데스크톱으로 사용할 가상 시스템을 준비하기 위해 필요한 작업 중 하나입니다. 자세한 내용은 *VMware View 관리* 설명서를 참조하십시오.

프로시저

1 View 데스크톱에서 **시작 > 설정 > 프린터 및 팩스**를 클릭합니다.

2 프린터 및 팩스 창에서 로컬로 사용할 수 있는 프린터 중 임의의 프린터를 마우스 오른쪽 단추로 클릭하고 **속성**을 선택합니다.

  Windows 7 데스크톱에서 다른 프린터를 사용할 수 있는데도 기본 프린터만 나타날 수 있습니다. 다른 프린터를 보려면 기본 프린터를 마우스 오른쪽 단추로 클릭하고 **프린터 속성**을 가리킵니다.

  View 데스크톱에서는 가상 프린터가 *<printer_name>#:<number>*로 나타납니다.

3 인쇄 속성 창에서 ThinPrint **디바이스 설치** 탭을 클릭하고 사용할 설정을 지정합니다.

4 **일반** 탭에서 **인쇄 환경설정**을 클릭하고 페이지 및 색상 설정을 편집합니다.

5 **고급** 탭에서 양면 인쇄 및 세로 방향(긴 쪽) 또는 가로 방향(짧은 쪽) 인쇄를 위해 환경설정을 설정합니다.

6 호스트에서 각 인쇄물을 미리 보려면 **인쇄하기 전에 클라이언트에서 미리 보기**를 사용하도록 설정합니다.

이 미리 보기에서 사용 가능한 모든 속성과 함께 임의의 프린터를 사용할 수 있습니다.

7 **조정** 탭에서 자동 인쇄 조정을 위해 설정을 검토합니다.

기본 설정을 유지하는 것이 좋습니다.

8 **확인**을 클릭합니다.

USB 프린터 사용

View 환경에서 가상 프린터 및 복제된 USB 프린터가 충돌 없이 함께 작동할 수 있습니다.

USB 프린터는 로컬 클라이언트 시스템의 USB 포트에 연결된 프린터입니다. USB 프린터에 인쇄 작업을 보내기 위해 USB 리디렉션 기능을 사용하거나 가상 인쇄 기능을 사용할 수 있습니다. USB 인쇄는 네트워크 상태에 따라 가상 인쇄보다 빠를 수도 있습니다.

- 필요한 드라이버를 View 데스크톱에 설치했기 때문에 USB 리디렉션 기능을 사용하여 USB 프린터를 View 데스크톱의 가상 USB 포트에 연결할 수 있습니다.

  이 리디렉션 기능을 사용할 경우 프린터는 클라이언트의 물리적 USB 포트에 더 이상 연결되지 않으며 이는 USB 프린터가 가상 인쇄 기능에서 표시하는 로컬 프린터 목록에 나타나지 않기 때문입니다. 또한 이는 View 데스크톱에서 USB 프린터로 인쇄할 수 있지만 로컬 클라이언트 시스템에서는 인쇄할 수 없다는 뜻입니다.

  View 데스크톱에서는 USB 프린터가 *<printer_name>*으로 나타납니다.

- 또는 Windows 클라이언트에서 가상 인쇄 기능을 사용하여 인쇄 작업을 USB 프린터로 보낼 수 있습니다. 가상 인쇄 기능을 사용할 경우 View 데스크톱 및 로컬 클라이언트에서 USB 프린터로 인쇄할 수 있으며 View 데스크톱에 프린터 드라이버를 설치할 필요가 없습니다.

View Client 자동 설치

명령줄에 설치 관리자 파일 이름 및 설치 옵션을 입력하여 View Client 를 자동으로 설치할 수 있습니다. 자동 설치를 사용하면 대기업에 View 구성 요소를 효과적으로 배포할 수 있습니다.

View Client with Local Mode 를 자동 설치하도록 그룹 정책 설정

View Client with Local Mode 를 자동으로 설치하려면 상승된 권한으로 설치할 수 있도록 Microsoft Windows 그룹 정책을 구성해야 합니다.

View Client 를 자동으로 설치하기 위해 이러한 그룹 정책을 설정할 필요가 없습니다. 이러한 정책은 View Client with Local Mode 에만 필요합니다.

클라이언트 컴퓨터의 컴퓨터 및 사용자를 위한 Windows Installer 그룹 정책을 설정해야 합니다.

필수 조건

View Client with Local Mode 를 설치할 Windows 클라이언트 컴퓨터에 대해 관리자 권한을 가지고 있어야 합니다.

프로시저

1 클라이언트 컴퓨터에 로그인하고 **시작 > 실행을 클릭합니다.**.

2 `gpedit.msc` 를 입력하고 **확인**을 클릭합니다.

3 그룹 정책 개체 편집기에서 **로컬 컴퓨터 정책 > 컴퓨터 구성**.

4 **관리 템플릿**을 확장하고 Windows **구성 요소**를 확장한 다음 Windows Installer 폴더를 열고 **항상 상승된 권한으로 설치**를 두 번 클릭합니다.

5 **항상 상승된 권한으로 설치 속성** 창에서 **사용**을 클릭하고 **확인**을 클릭합니다.

6 왼쪽 창에서 **사용자 구성**을 클릭합니다.

7 **관리 템플릿**을 확장하고 Windows **구성 요소**를 확장한 다음 Windows Installer 폴더를 열고 **항상 상승된 권한으로 설치**를 두 번 클릭합니다.

8 **항상 상승된 권한으로 설치 속성** 창에서 **사용**을 클릭하고 **확인**을 클릭합니다.

후속 작업

View Client with Local Mode 를 자동으로 설치합니다.

View Client 자동 설치

Microsoft Windows Installer 의 자동 설치(MSI) 기능을 사용하여 여러 Windows 컴퓨터에 View Client 또는 View Client with Local Mode 를 설치할 수 있습니다. 자동 설치 시에는 명령줄을 사용하고 마법사 메시지에 응답할 필요가 없습니다.

필수 조건

- 클라이언트 시스템에서 지원되는 운영 체제를 사용하는지 확인하십시오. "Windows 기반 View Client 및 View Client with Local Mode 지원 운영 체제," (16 페이지)의 내용을 참조하십시오.
- 클라이언트 시스템에 관리자로 로그인할 수 있는지 확인하십시오.
- View Agent 가 설치되지 않았는지 확인하십시오.
- 로컬 모드 요구 사항:
  - 자동 설치에 필요한 Windows Installer 그룹 정책이 클라이언트 컴퓨터에 구성되어 있어야 합니다. "View Client with Local Mode 를 자동 설치하도록 그룹 정책 설정," (115 페이지)의 내용을 참조하십시오.
  - 라이센스에 View Client with Local Mode 가 포함되어 있는지 확인하십시오.
  - 다음 제품 중 어느 것도 설치되지 않은 것을 확인합니다. View Client with Local Mode 를 설치할 수 없습니다.
- 최종 사용자가 현재 로그인한 사용자로서 View Client 와 가상 데스크톱에 로그인할 수 있도록 허용하는 기능을 사용할지 여부를 결정하십시오. 사용자가 클라이언트 시스템에 로그인할 때 입력한 자격 증명 정보가 View 연결 서버 인스턴스 그리고 최종적으로 가상 데스크톱에 전달됩니다. 일부 클라이언트 운영 체제에서는 이 기능을 지원하지 않습니다.
- MSI 설치 관리자 명령줄 옵션을 숙지하십시오. "Microsoft Windows Installer 명령줄 옵션," (59 페이지)의 내용을 참조하십시오.
- View Client 와 사용할 수 있는 MSI 속성에 익숙해지십시오. "View Client 의 자동 설치 속성," (117 페이지)의 내용을 참조하십시오.
- 최종 사용자가 가상 데스크톱에서 로컬로 연결된 USB 디바이스에 액세스할 수 있는지 확인합니다. 아닌 경우, MSI 속성 `ADDLOCAL` 을 사용할 기능 목록으로 설정하고 USB 기능을 생략합니다. 자세한 내용은 "View Client 의 자동 설치 속성," (117 페이지)에 나와 있습니다.
- 최종 사용자에게 가상 컴퓨터를 호스팅하는 View 연결 서버 인스턴스의 FQDN(정규화된 도메인 이름)을 지정하도록 요청하지 않으려면 설치하는 동안 지정할 수 있도록 FQDN 을 확인하십시오.

프로시저

1 클라이언트 시스템에서 http://www.vmware.com/products/의 VMware 제품 페이지에서 View Client 설치 관리자 파일을 다운로드하십시오.

적절한 설치 관리자 파일을 선택하십시오. *xxxxxx*는 빌드 번호이고 *y.y.y*는 버전 번호입니다.

옵션	조치
64 비트 운영 체제의 View Client	View Client 를 설치하려면 VMware-viewclient-x86_64-*y.y.y-xxxxxx*.exe 를 선택하십시오. View Client with Local Mode 를 설치하려면 VMware-viewclientwithlocalmode-x86_64-*y.y.y-xxxxxx*.exe 를 선택하십시오.
32 비트 운영 체제의 View Client	View Client 를 설치하려면 VMware-viewclient-*y.y.y-xxxxxx*.exe 를 선택하십시오. View Client with Local Mode 를 설치하려면 VMware-viewclientwithlocalmode-*y.y.y-xxxxxx*.exe 를 선택하십시오.

2 Windows 클라이언트 컴퓨터에서 명령 프롬프트를 엽니다.

3 설치 명령을 한 줄에 입력하십시오.

이 예는 단일 로그온 및 USB 리디렉션 기능이 있는 View Client 를 설치합니다. 기본 View Connection Server 인스턴스는 View Client 사용자를 위해 구성됩니다. `VMware-viewclient-y.y.y-xxxxxx.exe /s /v"/qn REBOOT=ReallySuppress VDM_SERVER=cs1.companydomain.com ADDLOCAL=Core,TSSO,USB"`

이 예는 View Client with Local Mode 를 설치합니다. `VMware-viewclientwithlocal-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,MVDI"`

참고 Core 기능이 필수입니다.

Windows 클라이언트 컴퓨터에 VMware View Client 서비스가 설치됩니다.

후속 작업

View Client 를 시작하고 올바른 가상 데스크톱에 로그인할 수 있는지 확인합니다. 자세한 내용은 "View 데스크톱에 로그인," (112 페이지) 또는 "View Portal 을 사용한 View Client 설치," (109 페이지)에 나와 있습니다.

View Client 의 자동 설치 속성

명령줄에서 View Client 를 자동 설치할 때 특정 속성이 포함될 수 있습니다. Microsoft Windows Installer(MSI)에서 속성 및 값을 해석할 수 있도록 하려면 *PROPERTY=value* 형식을 사용해야 합니다.

표 10-1 에는 명령줄에서 사용할 수 있는 View Client 자동 설치 속성이 나와 있습니다.

표 10-1. View Client 를 자동 설치하기 위한 MSI 속성

MSI 속성	설명	기본값
INSTALLDIR	View Client 소프트웨어가 설치된 경로 및 폴더입니다. 예: INSTALLDIR=""D:₩abc₩my folder"" 경로를 둘러싼 큰 따옴표 두 개 세트를 사용하면 MSI 설치 관리자에서 공백을 유효한 경로 부분으로 해석합니다. 이 MSI 속성은 선택 사항입니다.	%ProgramFiles%₩VMware₩VMware View₩Client
VDM_SERVER	View Client 사용자가 기본적으로 연결하는 View 연결 서버 인스턴스의 FQDN(정규화된 도메인 이름)입니다. 이 속성을 구성할 때 View Client 사용자는 이 FQDN 을 제공할 필요가 없습니다. 예: VDM_SERVER=cs1.companydomain.com 이 MSI 속성은 선택 사항입니다.	없음

표 10-1. View Client 를 자동 설치하기 위한 MSI 속성 (계속)

MSI 속성	설명	기본값
DESKTOP_SHORTCUT	View Client 의 데스크톱 바로 가기 아이콘을 구성합니다. 1 의 값은 바로 가기를 설치합니다. 0 의 값은 바로 가기를 설치하지 않습니다. 이 MSI 속성은 선택 사항입니다.	1
QUICKLAUNCH_SHORTCUT	View Client 의 빠른 실행 트레이에 바로 가기 아이콘을 구성합니다. 1 의 값은 바로 가기를 설치합니다. 0 의 값은 바로 가기를 설치하지 않습니다. 이 MSI 속성은 선택 사항입니다.	1
STARTMENU_SHORTCUT	시작 메뉴에 View Client 의 바로 가기를 구성합니다. 1 의 값은 바로 가기를 설치합니다. 0 의 값은 바로 가기를 설치하지 않습니다. 이 MSI 속성은 선택 사항입니다.	1

자동 설치 명령에 MSI 속성 ADDLOCAL=을 사용하여 View Client 설치 관리자에서 구성할 기능을 지정할 수 있습니다. 각 자동 설치 기능은 대화식 설치 중 선택할 수 있는 설치 옵션과 일치합니다.

표 10-2 에는 명령줄 및 해당 대화식 설치 옵션에 입력할 수 있는 View Client 기능이 나와 있습니다.

표 10-2. View Client 자동 설치 기능 및 대화식 사용자 지정 설치 옵션

자동 설치 기능	대화식 설치의 사용자 지정 설치 옵션
코어 MSI 속성 ADDLOCAL=을 사용하여 개별 기능을 지정할 경우 **Core** 를 포함시켜야 합니다. ADDLOCAL=ALL 을 지정할 경우 Core 를 포함하여 모든 View Client 및 View Client with Local Mode 기능이 설치됩니다.	없음. 대화식 설치 중 코어 View Client 기능이 기본적으로 설치됩니다.
MVDI View Client with Local Mode 를 설치할 때 이 기능을 사용하고 ADDLOCAL=을 사용하여 개별 기능을 지정하십시오. ADDLOCAL=ALL 을 지정할 경우 MVDI 를 포함하여 모든 View Client with Local Mode 기능이 설치됩니다.	없음. View Client with Local Mode 를 대화식으로 설치할 때 MVDI 기능이 기본적으로 설치됩니다. View Client 를 대화식으로 설치할 때 MVDI 기능을 사용할 수 없습니다.
ThinPrint	가상 인쇄
TSSO	단일 로그온(SSO)
USB	USB 리디렉션

색인

ㅎ