VMware View 보안

View 5.0
View Manager 5.0
View Composer 2.7

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-000575-00

vmware®

VMware 웹 사이트(http://www.vmware.com/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

목차

VMware View 보안

*VMware View 보안*에서는 VMware View™의 보안 기능에 대한 간단한 참조를 제공합니다.

- 필수 시스템 및 데이터베이스 로그인 계정.
- 보안과 관련이 있는 구성 옵션 및 설정.
- 보안 관련 구성 파일 및 암호, 그리고 보안 작업을 위해 권장되는 액세스 제어 등 보호해야 할 리소스.
- 로그 파일 위치 및 용도.
- VMware View 의 올바른 작업을 위해 열어두거나 활성화해야 하는 외부 인터페이스, 포트 및 서비스.

대상

본 정보는 IT 의사 결정권자, 설계자, 관리자를 비롯해 기타 VMware View 의 보안 구성 요소를 숙지해야 하는 사용자를 대상으로 합니다. 본 참조 안내서는 *VMware View Hardening Guide(VMware View 강화 안내서)* 및 기타 VMware View 설명서와 함께 사용해야 합니다.

VMware View 보안 참조

안전한 View 환경을 구성할 때 시스템을 보호하기 위해 설정을 변경하고 여러 영역을 조정할 수 있습니다.

- VMware View 계정(8 페이지)

  VMware View 구성 요소를 관리하려면 시스템 및 데이터베이스 계정을 설정해야 합니다.

- VMware View 보안 설정(9 페이지)

  VMware View 에는 구성 보안 조정에 사용할 수 있는 여러 설정이 포함되어 있습니다. 필요 시 View Administrator 를 사용하거나 그룹 프로필을 편집하거나 ADSI Edit 유틸리티를 사용하여 설정에 액세스할 수 있습니다.

- VMware View 리소스(16 페이지)

  VMware View 에는 보호해야 할 유사한 리소스 및 여러 구성 파일이 포함되어 있습니다.

- VMware View 로그 파일(17 페이지)

  VMware View 소프트웨어는 해당 구성 요소의 설치 및 작업을 기록하는 로그 파일을 생성합니다.

- VMware View TCP 및 UDP 포트(18 페이지)

  View 에서는 구성 요소 간 네트워크 액세스에 TCP 및 UDP 포트를 사용합니다. 적절한 포트에 액세스할 수 있도록 방화벽을 다시 구성해야 할 수 있습니다.

- View Connection Server 호스트의 서비스(24 페이지)

  View Manager 의 작업은 View Connection Server 호스트에서 실행할 여러 서비스에 따라 다릅니다. 이러한 서비스의 작업을 조정할 경우 서비스에 먼저 익숙해져야 합니다.

- Security Server 의 서비스(24 페이지)

  View Manager 의 작업은 보안 서버에서 실행할 여러 서비스에 따라 다릅니다. 이러한 서비스의 작업을 조정할 경우 서비스에 먼저 익숙해져야 합니다.

- View Transfer Server 호스트의 서비스(25 페이지)

  로컬 데스크톱의 전송 작업은 View Transfer Server 호스트에서 실행되는 서비스에 따라 다릅니다. 이러한 서비스의 작업을 조정할 경우 서비스에 먼저 익숙해져야 합니다.

VMware View 계정

VMware View 구성 요소를 관리하려면 시스템 및 데이터베이스 계정을 설정해야 합니다.

표 1. VMware View 시스템 계정

VMware View 구성 요소	필수 계정
View Client	View 데스크톱에 액세스할 수 있는 사용자를 위해 Active Directory에 사용자 계정을 구성하십시오. 사용자 계정은 원격 데스크톱 사용자 그룹의 구성원이어야 하지만 이 계정에는 View 관리자 권한이 필요하지 않습니다.
View Client with Local Mode를 사용해야 합니다.	로컬 모드의 View 데스크톱에 액세스할 수 있는 사용자를 위해 Active Directory에 사용자 계정을 구성하십시오. 이 사용자 계정에는 View 관리자 권한이 필요하지 않습니다. 데스크톱의 표준 모범 사례로서, 로컬 모드로 사용할 각 View 데스크톱에서 로컬 관리자 계정의 고유 암호를 생성해야 합니다.
vCenter Server	View Manager를 지원하는 데 필요한 vCenter Server에서 작업을 수행할 권한이 있는 Active Directory에 사용자 계정을 구성하십시오. 필수 권한에 대한 자세한 내용은 *VMware View 설치* 문서를 참조하십시오.
View Composer	View Composer에서 사용할 Active Directory에 사용자 계정을 생성하십시오. 연결된 클론 데스크톱을 Active Directory 도메인에 연결하려면 View Composer에서 이 계정을 사용해야 합니다. 사용자 계정은 View 관리 계정과 달라야 합니다. 특정 Active Directory 컨테이너에서 컴퓨터 개체를 생성 또는 제거하는 데 필요한 최소 권한을 계정에 부여하십시오. 예를 들어 계정에는 도메인 관리자 권한이 필요하지 않습니다. 필수 권한에 대한 자세한 내용은 *VMware View 설치* 문서를 참조하십시오.
View Connection Server, Security Server 또는 View Transfer Server	처음에는 View Connection Server 컴퓨터에서 로컬 관리자 그룹(BUILTIN\Administrators)의 구성원인 모든 사용자가 View Administrator에 로그인할 수 있습니다. View Administrator에서 **View 구성 > 관리자**를 사용해 View 관리자 목록을 변경할 수 있습니다. 필요한 권한에 대한 자세한 내용은 *VMware View 관리* 문서를 참조하십시오.

표 2. VMware View 데이터베이스 계정

VMware View 구성 요소	필수 계정
View Composer 데이터베이스	SQL Server 또는 Oracle 데이터베이스는 View Composer 데이터를 저장합니다. View Composer 사용자 계정과 연결할 수 있는 데이터베이스의 관리 계정을 생성합니다. View Composer 데이터베이스 설정에 대한 자세한 내용은 *VMware View 설치* 문서를 참조하십시오.
View Connection Server에서 사용하는 이벤트 데이터베이스	SQL Server 또는 Oracle 데이터베이스는 View 이벤트 데이터를 저장합니다. View Administrator가 이벤트 데이터에 액세스하는 데 사용할 수 있는 데이터베이스의 관리 계정을 생성합니다. View Composer 데이터베이스 설정에 대한 자세한 내용은 *VMware View 설치* 문서를 참조하십시오.

보안 취약점의 위험을 감소시키려면 다음 작업을 수행하십시오.

- 조직에서 사용하는 기타 데이터베이스 서버와는 별도의 서버에 View 데이터베이스를 구성하십시오.
- 단일 사용자 계정이 여러 데이터베이스에 액세스하지 못하도록 하십시오.
- View Composer 및 이벤트 데이터베이스 액세스를 위한 별도의 계정을 구성하십시오.

VMware View 보안 설정

VMware View 에는 구성 보안 조정에 사용할 수 있는 여러 설정이 포함되어 있습니다. 필요 시 View Administrator 를 사용하거나 그룹 프로필을 편집하거나 ADSI Edit 유틸리티를 사용하여 설정에 액세스할 수 있습니다.

View Administrator 의 보안 관련 전역 설정

클라이언트 세션 및 연결을 위한 보안 관련 전역 설정은 View Administrator 의 **View 구성 > 전역 설정**에서 액세스할 수 있습니다.

표 3. 보안 관련 전역 설정

설정	설명
Local Mode 작업에 단일 로그온 사용 안 함	사용자가 로컬 데스크톱에 로그인할 때 단일 로그인을 사용하도록 설정할지 여부를 결정합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
자동 상태 업데이트 사용	View Manager 에서 View Administrator 의 전역 상태 창 및 대시보드를 정기적으로 업데이트할지 여부를 결정합니다. 이 설정을 사용하면 View Administrator 에 로그인한 모든 사용자의 유휴 세션 시간 제한이 없어집니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
메시지 보안 모드	View Manager 구성 요소 간에 전송되는 JMS 메시지를 서명하고 확인할지 여부를 결정합니다. **사용 안 함**으로 설정된 경우, 메시지 보안 모드를 사용하지 않습니다. **사용**으로 설정된 경우, View 구성 요소는 서명되지 않은 메시지를 거부합니다. **혼합**으로 설정된 경우, 메시지 보안 모드를 사용하도록 설정되지만 View Manager 3.0 이전의 View 구성 요소에는 적용되지 않습니다. 기본 설정은 **사용 안 함**입니다.
네트워크 중단 후 보안 터널 연결 재인증	View 클라이언트에서 보안 터널 연결을 사용해 View 데스크톱에 연결하는 경우 네트워크 중단 이후 사용자 자격 증명을 재인증해야 할지 여부를 결정합니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
클라이언트 연결 및 View Administrator 에 대한 SSL 필요	View Connection Server 와 View 데스크톱 클라이언트 간, View Connection Server 와 View Administrator 에 액세스하는 클라이언트 간에 보안 SSL 통신 채널을 사용할지 여부를 결정합니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
세션 시간 초과	View Connection Server 에 로그인한 후에 사용자가 세션을 열어 놓을 수 있는 시간을 지정합니다. 기본값은 600 분입니다.

이러한 설정 및 보안 영향에 대한 자세한 내용은 *VMware View 관리* 문서를 참조하십시오.

View Administrator 의 보안 관련 서버 설정

보안 관련 서버 설정은 View Administrator 의 **View 구성 > 서버**에서 액세스할 수 있습니다.

표 4. 보안 관련 서버 설정

설정	설명
SSL 을 사용하여 연결	사용하도록 설정된 경우, View 는 SSL 암호화를 사용하여 vCenter Server 와 통신합니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
데스크톱에 대한 PCoIP 연결에 PCoIP 보안 게이트웨이 사용	사용하도록 설정된 경우, 사용자가 PCoIP 디스플레이 프로토콜로 View 데스크톱에 연결할 때 View Client 에서 View Connection Server 또는 보안 서버 호스트에 추가 보안 연결을 생성합니다. 사용하지 않도록 설정된 경우, View Connection Server 또는 보안 서버 호스트를 건너뛰고 클라이언트 시스템과 View 데스크톱 가상 시스템 간에 데스크톱 세션이 바로 구축됩니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
보안 터널을 사용하여 데스크톱에 연결	사용하도록 설정된 경우, 사용자가 View 데스크톱에 연결할 때 View Client 에서 View Connection Server 또는 보안 서버 호스트에 추가 HTTPS 연결을 생성합니다. 사용하지 않도록 설정된 경우, View Connection Server 또는 보안 서버 호스트를 건너뛰고 클라이언트 시스템과 View 데스크톱 가상 시스템 간에 데스크톱 세션이 바로 구축됩니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
Local Mode **작업에 보안 터널 연결 사용**	사용하도록 설정된 경우, 로컬 데스크톱은 터널링된 통신을 사용합니다. 네트워크 트래픽은 구성된 경우 View Connection Server 또는 보안 서버를 통해 라우팅됩니다. 사용하지 않도록 설정된 경우, 데이터가 로컬 데스크톱과 데이터 센터의 해당 원격 데스크톱 간에 직접 전송됩니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Local Mode **작업에 SSL 사용**	사용하도록 설정된 경우, 클라이언트 컴퓨터와 데이터 센터 사이의 통신 및 데이터 전송은 SSL 암호화를 사용합니다. 이러한 작업에는 데스크톱 체크인 및 체크아웃 그리고 데이터 센터로 클라이언트 컴퓨터의 데이터 복제가 포함되지만 View Composer 기본 이미지의 전송은 포함되지 않습니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
Local Mode **에서 데스크톱을 프로비저닝할 때 SSL 사용**	사용하도록 설정된 경우, Transfer Server 저장소의 View Composer 기본 이미지 파일을 클라이언트 컴퓨터로 전송할 때 SSL 암호화를 사용합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.

이러한 설정 및 보안 영향에 대한 자세한 내용은 *VMware View 관리* 문서를 참조하십시오.

View Agent 구성 템플릿의 보안 관련 설정

보안 관련 설정은 View Agent 용 ADM 템플릿 파일(vdm_agent.adm)로 제공됩니다. 다른 설명이 없는 한, 설정에는 컴퓨터 구성 설정만 포함됩니다.

보안 설정은 게스트 시스템 레지스트리의 HKLM₩Software₩Policies₩VMware, Inc.₩VMware VDM₩Agent₩Configuration 에 저장됩니다.

표 5. View Agent 구성 템플릿의 보안 관련 설정

설정	레지스트리 값 이름	설명
AllowDirectRDP	AllowDirectRDP	비 View 클라이언트가 RDP 를 사용하여 View 데스크톱에 직접 연결할 수 없는지 확인합니다. 이 설정이 사용되지 않도록 설정된 경우, View Agent 는 View Client 를 통해 View 에서 관리하는 연결만 허용합니다. **중요** View 가 올바르게 작동하려면 Windows Terminal Services 서비스가 각 데스크톱의 게스트 운영 체제에서 실행 중이어야 합니다. 이 설정을 사용하여 사용자가 데스크톱에 대한 직접 RDP 연결을 설정하지 못하도록 할 수 있습니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
AllowSingleSignon	AllowSingleSignon	단일 로그온(SSO)이 사용자를 View 데스크톱에 연결하는 데 사용되었는지 확인합니다. 이 설정이 사용되도록 설정된 경우, 사용자는 View Client 와 연결할 때 해당 자격 증명만 입력해야 합니다. 사용되지 않도록 설정된 경우, 사용자는 원격 연결이 설정될 때 다시 인증해야 합니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
CommandsToRunOnConnect	CommandsToRunOnConnect	처음 세션이 연결될 때 실행될 명령 스크립트 또는 명령 목록을 지정합니다. 기본적으로 지정되는 목록은 없습니다.
CommandsToRunOnReconnect	CommandsToRunOnReconnect	연결이 끊긴 후 세션이 다시 연결될 때 실행될 명령 스크립트 또는 명령 목록을 지정합니다. 기본적으로 지정되는 목록은 없습니다.
ConnectionTicketTimeout	VdmConnectionTicketTimeout	View 연결 티켓이 유효한 시간을 초로 지정합니다. 이 설정이 구성되지 않을 경우 기본 시간 초과 기간은 120 초입니다.
CredentialFilterExceptions	CredentialFilterExceptions	CredentialFilter 에이전트 로드에 허용되지 않는 실행 파일을 지정합니다. 파일 이름에는 경로 또는 접미사가 포함될 수 없습니다. 세미콜론을 사용하여 여러 파일 이름을 구분합니다. 기본적으로 지정되는 목록은 없습니다.

이러한 설정 및 보안 영향에 대한 자세한 내용은 *VMware View 관리* 문서를 참조하십시오.

View Client 구성 템플릿의 보안 설정

보안 관련 설정은 View Client 용 ADM 템플릿 파일(vdm_client.adm)로 제공됩니다. 다른 설명이 없는 한, 설정에는 컴퓨터 구성 설정만 포함됩니다. 사용자 구성 설정을 사용할 수 있고 그 값을 정의할 경우, 동등한 컴퓨터 구성 설정이 무시됩니다.

보안 설정은 호스트 시스템 레지스트리의 HKLM₩Software₩Policies₩VMware, Inc.₩VMware VDM₩Client₩Security 에 저장됩니다.

표 6. View Client 구성 템플릿의 보안 설정

설정	레지스트리 값 이름	설명
명령줄 자격 증명 허용	AllowCmdLineCredentials	사용자 자격 증명이 View Client 명령줄 옵션과 함께 제공될 수 있는지 확인합니다. 이 설정이 사용되도록 설정된 경우 사용자가 명령줄에서 View Client 를 실행할 때 smartCardPIN 및 password 옵션을 사용할 수 없습니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
위임을 위해 신뢰된 브로커	BrokersTrustedForDelegation	사용자가 **현재 사용자로 로그인** 확인란을 선택할 때 전달된 사용자 ID 및 자격 증명 정보를 허용하는 View Connection Server 인스턴스를 지정합니다. View Connection Server 인스턴스를 지정하지 않을 경우, 모든 View Connection Server 인스턴스는 이 정보를 허용합니다. View Connection Server 인스턴스를 추가하려면 다음 형식 중 하나를 사용하십시오. ■ **domain₩system$** ■ **system$@domain.com** ■ View Connection Server 의 서비스 사용자 이름 (SPN).

표 6. View Client 구성 템플릿의 보안 설정 (계속)

설정	레지스트리 값 이름	설명

인증서 검사 모드	CertCheckMode	View Client 에서 수행되는 인증서 검사 수준을 구성합니다. 다음 모드 중 하나를 선택할 수 있습니다.
		■ 보안 없음. View 는 인증서 검사를 수행하지 않습니다.
		■ 경고와 함께 허용. 다음 서버 인증서 문제가 발생할 때 경고가 표시되지만 사용자는 계속 View Connection Server 에 연결할 수 있습니다.
		  ■ 자체 서명 인증서가 View 에 의해 제공됩니다. 이런 경우, 인증서 이름이 View Client 의 사용자가 제공하는 View Connection Server 이름과 일치하지 않더라도 허용됩니다.
		  ■ 배포에 구성된 확인할 수 있는 인증서가 만료되었거나 아직 유효하지 않습니다.
		  다른 인증서 오류 조건이 발생할 경우, View 에서 오류 대화 상자가 표시되고 사용자가 View Connection Server 에 연결할 수 없게 됩니다.
		  경고와 함께 허용이 기본값입니다.
		■ 전체 보안. 임의의 인증서 오류 유형이 발생할 경우 사용자는 View Connection Server 에 연결할 수 없습니다. View 는 사용자에게 인증서 오류를 표시합니다.
		View Client 가 임의의 인증서 검사를 수행할 수 있도록 하려면 View Administrator 에서 **클라이언트 연결 및 View Administrator 에 대한 SSL 필요** 전역 설정을 선택해야 합니다.
		이 그룹 정책 설정이 구성되면 사용자는 View Client 에서 선택한 인증서 검사 모드를 볼 수 있지만 설정은 구성할 수 없습니다. SSL 구성 대화 상자는 사용자에게 관리자가 설정을 차단했다고 알립니다.
		이 설정이 구성되지 않았거나 사용하지 않도록 설정된 경우, View Client 사용자는 SSL 을 구성하고 인증서 검사 모드를 선택할 수 있습니다.
		또한 Windows 클라이언트에서 이 설정을 그룹 정책으로 구성하지 않을 경우, CertCheckMode 값 이름을 클라이언트 컴퓨터의 다음 레지스트리 키에 추가하여 인증서 검사를 사용하도록 설정할 수 있습니다.
		HKEY_LOCAL_MACHINE₩Software₩VMware, Inc.₩VMware VDM₩Client₩Security
		다음 값을 레지스트리 키에 사용하십시오.
		■ **0** 은 보안 없음을 구현합니다.
		■ **1** 은 경고와 함께 허용을 구현합니다.
		■ **2** 는 전체 보안을 구현합니다.
		레지스트리 키에 그룹 정책 설정 및 CertCheckMode 설정 모두를 구성할 경우 그룹 정책 설정이 레지스트리 키 값보다 우선합니다.

표 6. View Client 구성 템플릿의 보안 설정 (계속)

설정	레지스트리 값 이름	설명
'현재 사용자로 로그인' 확인란의 기본값	LogInAsCurrentUse	View Client 연결 대화 상자에서 **현재 사용자로 로그인** 확인란의 기본값을 지정합니다. 이 설정은 View Client 설치 중 지정된 기본값보다 우선합니다. 사용자가 명령줄에서 View Client를 실행하고 logInAsCurrentUser 옵션을 지정할 경우 해당 값은 이 설정보다 우선합니다. **현재 사용자로 로그인** 확인란이 선택된 경우, 클라이언트 시스템에 로그인할 때 사용자가 제공한 ID 및 자격 증명 정보가 View Connection Server 인스턴스에 전달되고 결국 View 데스크톱에 전달됩니다. 확인란 선택이 해제될 경우 View 데스크톱에 액세스하려면 사용자는 먼저 ID 및 자격 증명 정보를 여러 번 제공해야 합니다. 컴퓨터 구성 설정 외에도 사용자 구성 설정을 사용할 수 있습니다. 이러한 설정은 기본적으로 사용하지 않도록 설정됩니다.
현재 사용자로 로그인할 옵션 표시	LogInAsCurrentUser_Display	**현재 사용자로 로그인** 확인란이 View Client 연결 대화 상자에 나타나는지 확인합니다. 확인란이 보일 경우, 사용자는 선택 또는 선택을 해제할 수 있고 해당 기본값을 무시합니다. 확인란이 숨겨질 경우, 사용자는 View Client 연결 대화 상자에서 해당 기본값을 무시할 수 없습니다. '현재 사용자로 로그인' 확인란의 기본값 정책 설정을 사용하여 **현재 사용자로 로그인** 확인란의 기본값을 지정할 수 있습니다. 컴퓨터 구성 설정 외에도 사용자 구성 설정을 사용할 수 있습니다. 이러한 설정은 기본적으로 사용하도록 설정됩니다.
점프 목록 통합 사용	EnableJumplist	Windows 7 이후 시스템의 작업 표시줄에 있는 View Client 아이콘에 점프 목록이 나타나는지 확인합니다. 점프 목록을 사용하여 사용자는 최근 View Connection Server 인스턴스 및 View 데스크톱에 연결할 수 있습니다. View Client가 공유된 경우, 사용자가 최근 데스크톱의 이름을 보는 것을 원하지 않을 수 있습니다. 이 설정을 사용하지 않도록 설정하여 점프 목록을 사용하지 않도록 설정할 수 있습니다. 이 설정은 기본적으로 사용하도록 설정됩니다.
스마트 카드 인증을 위해 단일 로그온 사용	EnableSmartCardSSO	스마트 카드 인증을 위해 단일 로그온이 사용되도록 설정되었는지 확인합니다. 단일 로그온이 사용되도록 설정된 경우, View Client는 암호화된 스마트 카드 PIN을 View Connection Server로 제출하기 전에 임시 메모리에 저장합니다. 단일 로그온이 사용되지 않도록 설정되면 View Client에는 사용자 지정 PIN 대화 상자가 표시되지 않습니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
서버에서 수신된 불량 SSL 인증서 날짜 무시	IgnoreCertDateInvalid	잘못된 서버 인증서 날짜와 연결된 오류가 무시되었는지 확인합니다. 이러한 오류는 서버에서 경과된 날짜를 가진 인증서를 보낼 때 발생합니다. 이 설정은 기본적으로 사용하도록 설정됩니다. 이 설정은 View 4.6 이전 릴리스에만 적용됩니다.

표 6. View Client 구성 템플릿의 보안 설정 (계속)

설정	레지스트리 값 이름	설명
인증서 해지 문제 무시	IgnoreRevocation	해지된 서버 인증서와 연결된 오류가 무시되었는지 확인합니다. 이러한 오류는 서버에서 해지된 인증서를 보낼 때와 클라이언트가 인증서의 해지 상태를 확인할 수 없을 때 발생합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다. 이 설정은 View 4.6 이전 릴리스에만 적용됩니다.
잘못된 SSL 인증서 일반 이름(호스트 이름 필드) 무시	IgnoreCertCnInvalid	잘못된 서버 인증서 일반 이름과 연결된 오류가 무시되었는지 확인합니다. 이러한 오류는 인증서의 일반 이름이 이름을 보내는 서버의 호스트 이름과 일치하지 않을 때 발생합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다. 이 설정은 View 4.6 이전 릴리스에만 적용됩니다.
잘못된 사용 문제 무시	IgnoreWrongUsage	서버 인증서의 잘못된 사용과 연결된 오류가 무시되었는지 확인합니다. 이러한 오류는 서버에서 전송자의 ID를 확인하고 서버 통신을 암호화하는 것과 다른 용도의 인증서를 보낼 때 발생합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다. 이 설정은 View 4.6 이전 릴리스에만 적용됩니다.
알려지지 않은 인증 기관 문제 무시	IgnoreUnknownCa	서버의 알려지지 않은 인증 기관(CA)과 연결된 오류가 무시되는지 확인합니다. 이러한 오류는 서버에서 신뢰되지 않은 타사 CA로 서명된 인증서를 보낼 때 발생합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다. 이 설정은 View 4.6 이전 릴리스에만 적용됩니다.

이러한 설정 및 보안 영향에 대한 자세한 내용은 *VMware View 관리* 문서를 참조하십시오.

View Client 구성 템플릿 내 스크립팅 정의 섹션의 보안 관련 설정

보안 관련 설정은 View Client용 ADM 템플릿 파일(vdm_client.adm)의 스크립팅 정의 섹션에 제공됩니다. 다른 설명이 없는 한, 설정에는 컴퓨터 구성 설정 및 사용자 구성 설정 모두가 포함됩니다. 사용자 구성 설정을 정의할 경우, 동등한 컴퓨터 구성 설정을 무시합니다.

스크립팅 정의 설정은 호스트 시스템 레지스트리의 HKLM₩Software₩Policies₩VMware, Inc.₩VMware VDM₩Client에 저장됩니다.

표 7. 스크립팅 정의 섹션의 보안 관련 설정

설정	레지스트리 값 이름	설명
시작할 때 모든 USB 디바이스를 데스크톱에 연결	connectUSBOnStartup	클라이언트 시스템에서 사용할 수 있는 모든 USB 디바이스가 데스크톱을 시작할 때 데스크톱에 연결되는지 확인합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
전원 사용 시 모든 USB 디바이스를 데스크톱에 연결	connectUSBOnInsert	클라이언트 시스템에 전원을 공급할 때 USB 디바이스가 데스크톱에 연결되는지 확인합니다. 이 설정은 기본적으로 사용하지 않도록 설정됩니다.
로그온 암호	암호	로그인 중 View Client에서 사용하는 암호를 지정합니다. 암호는 Active Director에 의해 일반 텍스트로 저장됩니다. 이 설정은 기본적으로 정의되어 있지 않습니다.

이러한 설정 및 보안 영향에 대한 자세한 내용은 *VMware View 관리* 문서를 참조하십시오.

View LDAP 의 보안 관련 설정

보안 관련 설정은 View LDAP 의 개체 경로 cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int 에 있습니다. ADSI Edit 유틸리티를 사용하여 View Connection Server 인스턴스에서 이 설정의 값을 변경할 수 있습니다. 변경 사항은 그룹 내의 모든 다른 View Connection Server 인스턴스에 자동으로 전파됩니다.

표 8. View LDAP 의 보안 관련 설정

이름-값 쌍	특성	설명
cs-allowunencryptedstartsession	pae-NameValuePair	SSPI(Security Support Provider Interface) 협상이 지원되는 신뢰된 도메인에 없는 데스크톱으로 단일 로그온에 사용될 정적 키 보호를 허용합니다. 정적 키 보호는 SSPI 에 비해 덜 안전한 것으로 알려져 있습니다. 0 으로 설정하면 정적 키 보호가 허용되지 않습니다. 이 설정은 모든 데스크톱이 신뢰할 수 있는 도메인에 있는 경우에 적합합니다. SSPI 협상이 실패할 경우 세션이 시작되지 않습니다. 1 로 설정된 경우, 정적 키 보호는 SSPI 협상 실패 시 사용될 수 있습니다. 이 설정은 일부 데스크톱이 신뢰할 수 없는 도메인에 있는 경우에 적합합니다. 기본 설정은 1 입니다.
	pae-OVDIKeyCipher	사용자가 로컬 데스크톱을 체크인 및 체크아웃할 때 View Connection Server 가 가상 디스크(.vmdk) 파일을 암호화하는 데 사용하는 암호화 키 암호를 지정합니다. 암호화 키 암호 값을 AES-128, AES-192 또는 AES-256 으로 설정할 수 있습니다. 기본값은 AES-128 입니다.
	pae-SSOCredentialCacheTimeout	특정 시간이 지나면 사용자의 SSO 자격 증명이 유효하지 않게 되도록 SSO 시간 초과 제한을 분 단위로 설정합니다. 기본값은 15 입니다. 값이 -1 이면 SSO 시간 초과 제한이 설정되지 않았음을 의미합니다. 값이 0 이면 SSO 를 사용하지 않도록 설정됩니다.

VMware View 리소스

VMware View 에는 보호해야 할 유사한 리소스 및 여러 구성 파일이 포함되어 있습니다.

표 9. View Connection Server 및 Security Server 리소스

리소스	위치	보호
LDAP 설정	적용할 수 없습니다.	LDAP 데이터는 역할 기반 액세스 제어의 일부로 자동 보호됩니다.
LDAP 백업 파일	*<Drive Letter>*:₩Programdata₩VMWare₩VDM₩backups(Windows Server 2008) *<Drive Letter>*:₩Documents and Settings₩All Users₩Application Data₩VMWare₩VDM₩backups(Windows Server 2003)	액세스 제어로 보호됩니다.
locked.properties (인증서 속성 파일)	*install_directory*₩VMware₩VMware View₩Server₩sslgateway₩conf	액세스 제어로 보호할 수 있습니다. 이 파일은 View 관리자 이외의 모든 사용자 액세스로부터 보호해야 합니다.

표 9. View Connection Server 및 Security Server 리소스 (계속)

리소스	위치	보호
로그 파일	*%ALLUSERSPROFILE%*₩Application Data₩VMware₩VDM₩logs *<Drive Letter>*:₩Documents and Settings₩All Users₩Application Data₩VMware₩VDM₩logs	액세스 제어로 보호됩니다.
web.xml (Tomcat 구성 파일)	*install_directory*₩VMware View₩Server₩broker₩web apps₩ROOT₩Web INF	액세스 제어로 보호됩니다.

표 10. View Transfer Server 리소스

리소스	위치	보호
httpd.conf (Apache 구성 파일)	*install_directory*₩VMware₩VMware View₩Server₩httpd₩conf	액세스 제어로 보호할 수 있습니다. 이 파일은 View 관리자 이외의 모든 사용자 액세스로부터 보호해야 합니다.
로그 파일	*<Drive Letter>*:₩ProgramData₩VMware₩VDM₩logs(Windows Server 2008 R2) *%ALLUSERSPROFILE%*₩Application Data₩VMware₩VDM₩logs(Windows Server 2003 및 Windows Server 2003 R2) *<Drive Letter>*:₩Program Files₩Apache Group₩Apache2₩logs(Apache 서버)	액세스 제어로 보호됩니다.

VMware View 로그 파일

VMware View 소프트웨어는 해당 구성 요소의 설치 및 작업을 기록하는 로그 파일을 생성합니다.

참고 VMware View 로그 파일은 VMware 지원에서 사용하기 위한 것입니다. VMware 에서는 이벤트 데이터베이스를 구성하고 사용하여 View 를 모니터할 것을 권장합니다. 자세한 내용은 *VMware View 설치* 및 *VMware View 통합* 문서를 참조하십시오.

표 11. VMware View 로그 파일

VMware View 구성 요소	파일 경로 및 기타 정보
모든 구성 요소(설치 로그)	*%TEMP%*₩vminst.log_*date_timestamp* *%TEMP%*₩vmmsi.log_*date_timestamp*
View Agent	Windows XP 게스트 OS: *<Drive Letter>*:₩Documents and Settings₩All Users₩Application Data₩VMware₩VDM₩logs Windows Vista 및 Windows 7 게스트 OS: *<Drive Letter>*:₩ProgramData₩VMware₩VDM₩logs 사용자 데이터 디스크(UDD)가 구성되면 *<Drive Letter>*가 UDD 와 일치할 수 있습니다. PCoIP 로그는 pcoip_agent*.log 및 pcoip_server*.log 으로 이름 지정됩니다.
View 애플리케이션	SQL Server 또는 Oracle 데이터베이스 서버에 구성된 View 이벤트 데이터베이스. Windows 애플리케이션 이벤트 로그. 기본적으로 사용하지 않도록 설정됩니다.
View Client with Local Mode	Windows XP 호스트 OS: C:₩Documents and Settings₩*%username%*₩Local Settings₩Application Data₩VMware₩VDM₩Logs₩ Windows Vista 및 Windows 7 호스트 OS: C:₩Users₩*%username%*₩AppData₩VMware₩VDM₩Logs₩

표 11. VMware View 로그 파일 (계속)

VMware View 구성 요소	파일 경로 및 기타 정보
View Composer	연결된 클론 데스크톱의 *%system_drive%*₩Windows₩Temp₩vmware-viewcomposer-ga-new.log. View Composer 로그에는 QuickPrep 및 Sysprep 스크립트 실행에 대한 정보가 포함됩니다. 로그는 스크립트 실행의 시작과 끝 시간을 기록하고 출력 또는 오류 메시지를 로그합니다.
View Connection Server 또는 Security Server	서버의 *%ALLUSERSPROFILE%*₩Application Data₩VMware₩VDM₩logs₩*.txt. 서버의 *<Drive Letter>*:₩Documents and Settings₩All Users₩Application Data₩VMware₩VDM₩logs₩*.txt. 로그 디렉토리는 View 일반 구성 ADM 템플릿 파일(vdm_common.adm)의 로그 구성 설정에서 구성 가능합니다. PCoIP Secure Gateway 로그는 보안 서버에 있는 로그 디렉토리의 PCoIP Secure Gateway 하위 디렉토리에 있는 SecurityGateway_*.log 파일에 작성됩니다.
View 서비스	SQL Server 또는 Oracle 데이터베이스 서버에 구성된 View 이벤트 데이터베이스. Windows 시스템 이벤트 로그.
View Transfer Server	Windows Server 2008 R2: *<Drive Letter>*:₩ProgramData₩VMware₩VDM₩logs₩*.txt Windows Server 2003 및 Windows Server 2003 R2: *%ALLUSERSPROFILE%*₩Application Data₩VMware₩VDM₩logs₩*.txt Apache Server: *<Drive Letter>*:₩Program Files₩Apache Group₩Apache2₩logs₩error.log

VMware View TCP 및 UDP 포트

View 에서는 구성 요소 간 네트워크 액세스에 TCP 및 UDP 포트를 사용합니다. 적절한 포트에 액세스할 수 있도록 방화벽을 다시 구성해야 할 수 있습니다.

표 12. Local Mode 를 제외하고 View 에서 사용되는 TCP 및 UDP 포트

소스	포트	대상	포트	프로토콜	설명
보안 서버	4172	View Agent 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	UDP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
보안 서버	4172	View Agent 4.6 이상	4172	UDP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
보안 서버	4172	View Client 4.5 이하	50002(변경할 수 없음)	UDP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
보안 서버	4172	View Client 4.6 이상	4172	UDP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
보안 서버	*	View Connection Server	4001	TCP	JMS 트래픽입니다.
보안 서버	*	View Connection Server	8009	TCP	AJP13 으로 전달된 웹 트래픽입니다.

표 12. Local Mode 를 제외하고 View 에서 사용되는 TCP 및 UDP 포트 (계속)

소스	포트	대상	포트	프로토콜	설명
보안 서버	*	View 데스크톱	3389	TCP	View 데스크톱에 대한 Microsoft RDP 트래픽입니다.
보안 서버	*	View 데스크톱	9427	TCP	Wyse MMR 리디렉션입니다.
보안 서버	*	View 데스크톱	32111	TCP	USB 리디렉션입니다.
보안 서버	*	View 데스크톱 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	TCP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(HTTPS)입니다.
보안 서버	*	View 데스크톱 4.6 이상	4172	TCP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(HTTPS)입니다.
View Agent 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	View Client 4.5 이하	50002(변경할 수 없음)	UDP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(AES-128-GCM 또는 SALSA20)입니다.
View Agent 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	View Client 4.6 이상	4172	UDP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(AES-128-GCM 또는 SALSA20)입니다.
View Agent 4.6 이상	4172	View Client 4.5 이하	50002(변경할 수 없음)	UDP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(AES-128-GCM 또는 SALSA20)입니다.
View Agent 4.6 이상	4172	View Client 4.6 이상	4172	UDP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(AES-128-GCM 또는 SALSA20)입니다.
View Agent 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	View Connection Server 또는 보안 서버	4172	UDP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
View Agent 4.6 이상	4172	View Connection Server 또는 보안 서버	4172	UDP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
View Client	*	View Connection Server 또는 보안 서버	80	TCP	클라이언트 연결에 SSL 을 사용하지 않도록 설정할 경우 HTTP 액세스입니다.

표 12. Local Mode 를 제외하고 View 에서 사용되는 TCP 및 UDP 포트 (계속)

소스	포트	대상	포트	프로토콜	설명
View Client	*	View Connection Server 또는 보안 서버	443	TCP	클라이언트 연결에 SSL 을 사용하도록 설정할 경우 HTTPS 액세스입니다.
View Client	*	View Connection Server 또는 보안 서버	4172	TCP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(HTTPS)입니다.
View Client	*	View 데스크톱	3389	TCP	터널 연결 대신 직접 연결을 사용할 경우 View 데스크톱에 대한 Microsoft RDP 트래픽입니다.
View Client	*	View 데스크톱	9427	TCP	터널 연결 대신 직접 연결을 사용할 경우 Wyse MMR 리디렉션입니다.
View Client	*	View 데스크톱	32111	TCP	터널 연결 대신 직접 연결을 사용할 경우 USB 리디렉션입니다.
View Client 4.5 이하	*	View Agent 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	TCP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(HTTPS)입니다.
View Client 4.5 이하	50002(변경할 수 없음)	View Agent 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	UDP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(AES-28-GCM 또는 SALSA20)입니다.
View Client 4.5 이하	*	View Agent 4.6 이상	4172	TCP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(HTTPS)입니다.
View Client 4.5 이하	50002(변경할 수 없음)	View Agent 4.6 이상	4172	UDP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(AES-28-GCM 또는 SALSA20)입니다.
View Client 4.5 이하	50002(변경할 수 없음)	View Connection Server 또는 보안 서버	4172	UDP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
View Client 4.6 이상	*	View Agent 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	TCP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(HTTPS)입니다.

표 12. Local Mode 를 제외하고 View 에서 사용되는 TCP 및 UDP 포트 (계속)

소스	포트	대상	포트	프로토콜	설명
View Client 4.6 이상	4172	View Agent 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	UDP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(AES-28-GCM 또는 SALSA20)입니다.
View Client 4.6 이상	*	View Agent 4.6 이상	4172	TCP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(HTTPS)입니다.
View Client 4.6 이상	4172	View Agent 4.6 이상	4172	UDP	PCoIP Secure Gateway 를 사용하지 않을 경우 PCoIP(AES-28-GCM 또는 SALSA20)입니다.
View Client 4.6 이상	4172	View Connection Server 또는 보안 서버	4172	UDP	PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
View Connection Server	*	vCenter Server 또는 View Composer	80	TCP	vCenter Server 또는 View Composer 액세스를 위해 SSL 을 사용하지 않도록 설정된 경우 SOAP 메시지입니다.
View Connection Server	*	vCenter Server 또는 View Composer	443	TCP	vCenter Server 또는 View Composer 액세스에 SSL 을 사용하도록 설정된 경우 SOAP 메시지입니다.
View Connection Server	4172	View Agent 4.5 이하	50002(그룹 정책으로 변경될 수 있음)	UDP	View Connection Server 를 통해 PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
View Connection Server	4172	View Agent 4.6 이상	4172	UDP	View Connection Server 를 통해 PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
View Connection Server	4172	View Client 4.5 이하	50002(변경할 수 없음)	UDP	View Connection Server 를 통해 PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.

표 12. Local Mode 를 제외하고 View 에서 사용되는 TCP 및 UDP 포트 (계속)

소스	포트	대상	포트	프로토콜	설명
View Connection Server	4172	View Client 4.6 이상	4172	UDP	View Connection Server 를 통해 PCoIP Secure Gateway 를 사용할 경우 PCoIP(AES-128-GCM 전용)입니다.
View Connection Server	*	View Connection Server	4100	TCP	JMS inter-router 트래픽입니다.
View Connection Server	*	View 데스크톱	3389	TCP	View Connection Server 를 통해 터널 연결을 사용할 경우 View 데스크톱에 대한 Microsoft RDP 트래픽입니다.
View Connection Server	*	View 데스크톱	4172	TCP	View Connection Server 를 통해 PCoIP Secure Gateway 를 사용할 경우 PCoIP(HTTPS)입니다.
View Connection Server	*	View 데스크톱	9427	TCP	View Connection Server 를 통해 터널 연결을 사용할 경우 Wyse MMR 리디렉션입니다.
View Connection Server	*	View 데스크톱	32111	TCP	View Connection Server 를 통해 터널 연결을 사용할 경우 USB 리디렉션입니다.
View 데스크톱	*	View Connection Server 인스턴스	4001	TCP	JMS 트래픽입니다.
View Composer 서비스	*	ESXi 호스트	902	TCP	View Composer 에서 View Composer 내부 디스크 그리고, 지정된 경우, 영구 디스크와 시스템 임시 디스크를 포함하여 연결된 클론 디스크를 사용자 지정할 때 사용됩니다.

Local Mode 기능이 바르게 작동하려면 포트를 추가로 열어야 합니다.

표 13. Local Mode 에서 사용되는 TCP 및 UDP 포트

소스	포트	대상	포트	프로토콜	설명
보안 서버	*	View Transfer Server	80	TCP	터널 연결을 사용하고 로컬 모드 작업에 SSL 을 사용하지 않도록 설정한 경우, View 데스크톱 다운로드 및 데이터 복제입니다.
보안 서버	*	View Transfer Server	443	TCP	터널 연결을 사용하고 로컬 모드 작업에 SSL 을 사용하도록 설정할 경우 View 데스크톱 다운로드 및 데이터 복제입니다.
View Client with Local Mode	*	View Transfer Server	80	TCP	터널 연결 대신 직접 연결을 사용하고 로컬 모드 작업에 SSL 을 사용하지 않도록 설정할 경우 View 데스크톱 다운로드 및 데이터 복제입니다.
View Client with Local Mode	*	View Transfer Server	443	TCP	터널 연결 대신 직접 연결을 사용하고 로컬 모드 작업에 SSL 을 사용하도록 설정할 경우 View 데스크톱 다운로드 및 데이터 복제입니다.
View Connection Server	*	ESX 호스트	902	TCP	로컬 데스크톱을 체크아웃할 때 사용됩니다.
View Connection Server	*	View Transfer Server	80	TCP	View Connection Server 를 통해 터널 연결을 사용하고 로컬 모드 작업에 SSL 을 사용하지 않도록 설정한 경우 View 데스크톱 다운로드 및 데이터 복제입니다.
View Connection Server	*	View Transfer Server	443	TCP	View Connection Server 를 통해 터널 연결을 사용하고 로컬 모드 작업에 SSL 을 사용하도록 설정한 경우 View 데스크톱 다운로드 및 데이터 복제입니다.
View Connection Server	*	View Transfer Server	4001	TCP	로컬 모드를 지원하는 JMS 트래픽입니다.
View Transfer Server	*	ESX 호스트	902	TCP	로컬 모드를 위한 게시용 View Composer 패키지입니다.

View Connection Server 호스트의 서비스

View Manager 의 작업은 View Connection Server 호스트에서 실행할 여러 서비스에 따라 다릅니다. 이러한 서비스의 작업을 조정할 경우 서비스에 먼저 익숙해져야 합니다.

표 14. View Connection Server 호스트 서비스

서비스 이름	시작 유형	설명
VMware View Connection Server	자동	연결 브로커 서비스를 제공합니다. 이 서비스는 View Manager 의 올바른 작업을 위해 실행 중이어야 합니다. 이 서비스를 시작 또는 중지할 경우 Framework, Message Bus, Security Gateway 및 Web 서비스 또한 시작 또는 중지합니다. 이 서비스는 VMwareVDMDS 또는 VMware View Script Host 서비스를 시작 또는 중지하지 않습니다.
VMware View Framework 구성 요소	수동	View Manager 에 이벤트 로깅, 보안 및 COM+ 프레임워크 서비스를 제공합니다. 이 서비스는 View Manager 의 올바른 작업을 위해 실행 중이어야 합니다.
VMware View Message Bus 구성 요소	수동	View Manager 구성 요소 간 메시지 서비스를 제공합니다. 이 서비스는 View Manager 의 올바른 작업을 위해 실행 중이어야 합니다.
VMware View PCoIP Secure Gateway	수동	PCoIP Secure Gateway 서비스를 제공합니다. 이 서비스는 클라이언트가 PCoIP Secure Gateway 를 통해 View Connection Server 에 연결할 경우 실행 중이어야 합니다.
VMware View Script Host	자동(사용하도록 설정된 경우)	가상 시스템을 삭제할 때 실행된 타사 스크립트의 지원을 제공합니다. 이 서비스가 기본적으로 사용되지 않도록 설정됩니다. 스크립트를 실행할 경우 이 서비스를 사용하도록 설정해야 합니다.
VMware View Security Gateway 구성 요소	수동	View Manager 에 보안 터널 서비스를 제공합니다. 이 서비스는 View Manager 의 올바른 작업을 위해 실행 중이어야 합니다.
VMware View Web 구성 요소	수동	View Manager 에 웹 서비스를 제공합니다. 이 서비스는 View Manager 의 올바른 작업을 위해 실행 중이어야 합니다.
VMwareVDMDS	자동	View Manager 에 LDAP 디렉토리 서비스를 제공합니다. 이 서비스는 View Manager 의 올바른 작업을 위해 실행 중이어야 합니다. 기존 데이터가 올바르게 마이그레이션되었는지 확인하려면 이 서비스가 VMware View 의 업그레이드 중 실행 중이어야 합니다.

Security Server 의 서비스

View Manager 의 작업은 보안 서버에서 실행할 여러 서비스에 따라 다릅니다. 이러한 서비스의 작업을 조정할 경우 서비스에 먼저 익숙해져야 합니다.

표 15. Security Server 서비스

서비스 이름	시작 유형	설명
VMware View Security Server	자동	보안 서버 서비스를 제공합니다. 이 서비스는 보안 서버의 올바른 작업을 위해 실행 중이어야 합니다. 이 서비스를 시작 또는 중지할 경우 Framework 및 Security Gateway 서비스 또한 시작 또는 중지합니다.
VMware View Framework 구성 요소	수동	이벤트 로깅, 보안 및 COM+ 프레임워크 서비스를 제공합니다. 이 서비스는 보안 서버의 올바른 작업을 위해 실행 중이어야 합니다.

표 15. Security Server 서비스 (계속)

서비스 이름	시작 유형	설명
VMware View PCoIP Secure Gateway	수동	PCoIP Secure Gateway 서비스를 제공합니다. 이 서비스는 클라이언트가 PCoIP Secure Gateway 를 통해 보안 서버에 연결할 경우 실행 중이어야 합니다.
VMware View Security Gateway 구성 요소	수동	보안 터널 서비스를 제공합니다. 이 서비스는 보안 서버의 올바른 작업을 위해 실행 중이어야 합니다.

View Transfer Server 호스트의 서비스

로컬 데스크톱의 전송 작업은 View Transfer Server 호스트에서 실행되는 서비스에 따라 다릅니다. 이러한 서비스의 작업을 조정할 경우 서비스에 먼저 익숙해져야 합니다.

View Transfer Server 와 함께 설치된 모든 서비스는 View Manager 에서 로컬 데스크톱의 올바른 작업을 위해 실행 중이어야 합니다.

표 16. View Transfer Server 호스트 서비스

서비스 이름	시작 유형	설명
VMware View Transfer Server	자동	View Transfer Server 관련 서비스를 통합하는 서비스를 제공합니다. 이 서비스를 시작 또는 중지할 경우 View Transfer Server Control Service 및 Framework 서비스 또한 시작 또는 중지합니다.
VMware View Transfer Server Control 서비스	수동	View Transfer Server 에 관리 기능을 제공하고 View Connection Server 와의 통신을 처리합니다.
VMware View Framework 구성 요소	수동	View Manager 에 이벤트 로깅, 보안 및 COM+ 프레임워크 서비스를 제공합니다.
Apache2.2 서비스	자동	로컬 모드에서 View 데스크톱을 실행하는 클라이언트 컴퓨터에 데이터 전송 기능을 제공합니다. Apache2.2 서비스는 View Transfer Server 를 View Manager 에 추가할 때 시작됩니다.

색인