다음 참고 사항을 읽으십시오! View 5.1 설치가 보다 편리해집니다!

참고 사항은 해당 언어로 읽으실 수 있습니다:
Français Deutsch 简体中文 日本語 한국어

View 5.1은 View 구성 요소를 이전과 약간 다르게 구성하도록 변경되었습니다. 이러한 참고 사항은 View 5.1 설치 또는 업그레이드 시 발생할 수 있는 잠재적 위험을 피하는 데 도움을 줍니다.

1) View 5.1 연결 서버를 이전 버전으로 다운그레이드할 수 없습니다.

View 5.1에서는 View LDAP 구성이 암호화되어 있고 View 이전 버전에서 사용할 수 없습니다.

- View 연결 서버 인스턴스를 View 5.1로 업그레이드하면 이전 버전으로 인스턴스를 다운그레이드할 수 없습니다.
- 복제된 그룹에 있는 모든 View 연결 서버 인스턴스를 업그레이드하면 이전 버전의 View에서 실행되는 다른 인스턴스를 추가할 수 없습니다.

참고: 다운그레이드가 지원되지 않았지만, 이전 릴리스에서는 작동되었습니다. 하지만 이제 서비스가 지원되지 않습니다.

2) vCenter Server 및 View Composer 호스트에 유효한 SSL 인증서가 필요합니다.

- *최적의 선택*: vCenter Server 및 View Composer에 인증 기관(CA: Certificate Authority)이 제공하는 인증서가 있는지 확인합니다.
  - vCenter Server가 설치되어 있는 Windows 서버에 인증 기관이 서명한 SSL 인증서를 설치합니다.
  - View Composer도 동일하게 설치합니다. View Composer 및 vCenter Server를 같은 호스트에 설치하는 경우, 동일한 인증서를 사용할 수 있지만 각 구성 요소에 대해서는 개별적으로 인증서를 구성해야 합니다.

    * View Composer를 설치하기 전에 인증서를 설치하는 경우, View Composer 설치 중에 인증서를 선택할 수 있습니다.

    * 나중에 기본 인증서를 대체할 경우, *SviConfig ReplaceCertificate* 명령을 실행하여 View Composer가 사용하는 포트에 새 인증서를 연결합니다.
  - View 연결 서버 인스턴스가 설치된 각 Windows 서버가 새 인증서의 인증 기관 및 모든 상위 인증 기관을 신뢰하는지 확인합니다.
- *대안*: vCenter Server와 View Composer를 View에 추가한 후, View Administrator에서 **확인**을 클릭하여 View Composer에 대한 기본 인증서의 지문 인식을 허용합니다. vCenter Server도 같은 과정을 따릅니다.

추가 정보: *View 설치* 가이드에서 "View Server용 SSL 인증서 구성"을 참조하십시오.

3) 보안 서버와 View 연결 서버 호스트에 유효한 SSL 인증서가 필요합니다.

- *최적의 선택*: Windows Server 호스트에 View 연결 서버 인스턴스 또는 보안 서버를 설치한 후, Windows Server 인증서 저장소를 열고 다음 단계를 따릅니다.
  - 인증 기관이 서명하고 클라이언트가 검증할 수 있는 SSL 인증서를 가져옵니다.
  - 중간 인증서 및 루트 인증서를 포함하여 전체 인증서 체인이 설치되어 있는지 확인합니다.
  - 인증서에 개인 키가 있는지 확인하고 키를 내보내기 가능으로 표시합니다.
  - 인증서 이름을 *vdm*으로 구성합니다.
- *대안*: View Server 설치 관리자가 Windows Server 인증서 저장소에 기본 인증서를 만들 수 있도록 지원합니다. 인증서는 자체 서명되어 있으며 View Administrator에서 유효하지 않은 인증서로 표시됩니다.
- *View 5.1로 업그레이드*: 기존 View Server에 인증 기관이 서명한 SSL 인증서가 이미 있는 경우, 추가 작업이 필요하지 않습니다. 업그레이드 중, View가 인증서를 Windows Server 인증서 저장소로 가져옵니다.

기존 View Server에 기본 인증서가 있는 경우, View Server를 업그레이드하고 위의 *최적의 선택* 단계를 따릅니다.

추가 정보: *View 설치* 가이드에서 "View Server용 SSL 인증서 구성"을 참조하십시오.

4) vCenter Server, View Composer 및 View Server용 인증서에는 인증서 해지 목록(CRL: Certificate Revocation List)이 포함되어 있어야 합니다.

View는 CRL이 없는 인증서를 검증하지 않습니다.

- *최적의 선택*: 필요에 따라 다음 단계를 따릅니다.
  - 인증서에 CRL을 추가합니다.
  - 업데이트된 인증서를 vCenter Server, View Composer 및 View Server 호스트에 있는 Windows 인증서 저장소로 가져옵니다.
- *대안*: CRL 확인을 제어하는 레지스트리 설정을 변경합니다.

추가 정보: *View 설치* 가이드에서 "서버 인증서에 대한 인증서 해지 확인 구성"을 참조하십시오.

5) 보안 서버와 View 연결 서버 호스트에서 고급 보안이 포함된 Windows 방화벽을 사용하도록 설정해야 합니다.

기본적으로, IPsec 규칙은 View 보안 서버와 View 연결 서버 간의 연결을 관리하고 고급 보안이 포함된 Windows 방화벽의 사용이 필요합니다.

- *최적의 선택*: View Server를 설치하기 전에 고급 보안이 포함된 Windows 방화벽을 **켜기**로 설정합니다. 모든 활성 프로필에서 **켜기** 상태인지 확인합니다. *모든* 프로필을 **켜기** 상태로 설정하는 것이 좋습니다.

- *대안*: 보안 서버를 설치하기 전에 View Administrator를 열고 전역 설정 *보안 서버 연결용 IPSec 사용*을 **아니요**로 설정하여 비활성화합니다. (권장하지 않음)

6) IPsec을 지원하기 위해 백엔드 방화벽을 설정해야 합니다.

보안 서버와 View 연결 서버 인스턴스 사이에 백엔드 방화벽이 있는 경우, 연결을 위해 방화벽 규칙을 구성해야 합니다.

추가 정보: *View 설치* 가이드에서 "IPsec 지원을 위한 백엔드 방화벽 구성"을 참조하십시오.

7) View Client는 View에 연결하기 위해 HTTPS를 사용해야 합니다.

View 연결 서버 인스턴스 및 보안 서버는 SSL을 사용하여 클라이언트에 연결됩니다.

- View Client가 SSL 오프로딩 중간 장치를 통해 연결되는 경우, View 연결 서버 또는 보안 서버에 중간 장치의 SSL 인증서를 설치해야 합니다.

- View Client가 부하 분산 장치와 같은 중간 장치를 통해 연결되는지 여부에 관계없이, 연결은 HTTPS여야 합니다. 중간 장치를 사용하고 있고 중간 장치와 View Server 간의 연결을 HTTP(SSL 오프로딩) 경유로 설정하려면, View Server에서 *locked.properties* 파일을 구성합니다.

- HTTPS를 사용하지 않도록 선택할 수 있는 기존의 View Client에서 HTTP를 선택하면 오류가 발생합니다. 이전에는 자동으로 HTTPS로 리디렉션되었습니다. SSL에 연결되지 않은 클라이언트는 View에 연결될 수 없습니다.

추가 정보: *View 관리* 가이드에서 "SSL 연결을 중간 서버에 오프로딩"을 참조하십시오.

8) 암호화 및 클리닝 View 백업에 새 복원 단계가 필요합니다.

기본적으로, View 5.1 백업은 암호화되어 있습니다. View 백업을 클리닝하거나(백업 데이터에서 암호 및 기타 중요 정보 제거) 일반 텍스트로 백업할 수도 있습니다(권장하지 않음).

- 암호화된 백업을 복원하려면 먼저 데이터의 암호화를 해제해야 합니다. View 연결 서버를 설치했을 때 입력한 데이터 복구 암호를 사용해야 합니다.
- 클리닝 백업을 복원하지 마십시오. View LDAP 구성에서 암호 등의 데이터가 손실됩니다. View 구성 요소는 이 데이터가 없으면 올바르게 작동하지 않습니다. 일반 기능을 복원하려면, View Administrator를 사용하여 모든 암호 및 기타 누락된 데이터 항목을 수동으로 재설정해야 합니다.

추가 정보: *View 관리* 가이드에서 "View 구성 데이터 백업 및 복원"을 참조하십시오.

9) View 5.1 보안 서버를 업그레이드하거나 재설치하기 전에, 관련 IPsec 규칙을 연결된 View 연결 서버 인스턴스에서 제거해야 새로운 규칙을 설정할 수 있습니다.

- View Administrator에서 보안 서버를 선택하고 **추가 명령 > 업그레이드 또는 다시 설치 준비**를 클릭합니다.

  참고: 서버를 업그레이드하거나 재설치하기 전에 View에서 보안 서버를 제거할 필요는 없습니다.

추가 정보: *View 설치* 가이드에서 "보안 서버 업그레이드 또는 재설치 준비"를 참조하십시오.