Site Recovery Manager 보안

Site Recovery Manager 6.5

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/kr/support/pubs를 참조하십시오.

KO-002309-00

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.com으로 사용자 의견을 보내주십시오.

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

목차

VMware Site Recovery Manager 보안 정보

Site Recovery Manager 보안은 Site Recovery Manager의 보안 기능에 대한 간략한 참조를 제공합니다.

이 가이드에서는 설치된 Site Recovery Manager를 보호할 수 있도록 Site Recovery Manager에 포함되어 있는 보안 기능 및 공격을 방지하는 방법에 대해 설명합니다.

- Site Recovery Manager의 정상 작동에 필요한 외부 인터페이스, 포트 및 서비스
- 보안에 영향을 미치는 구성 옵션 및 설정
- 로그 파일 위치 및 그 용도
- 필요한 시스템 계정
- 최신 보안 패치 가져오기에 관한 정보

대상 사용자

이 정보는 IT 의사결정권자, 설계자, 관리자를 비롯하여 Site Recovery Manager의 보안 구성 요소를 숙지해야 하는 기타 사용자들을 위한 것입니다.

Site Recovery Manager 보안 참조 1

Site Recovery Manager 설치의 보안 기능 및 사용자 환경을 공격으로부터 보호하기 위해 수행할 수 있는 조치에 대해 알아보려면 보안 참조를 사용하십시오.

- Site Recovery Manager 서비스(8 페이지)

  Site Recovery Manager Server 호스트 시스템에서 실행되는 여러 서비스는 Site Recovery Manager의 작동에 중요한 역할을 합니다.

- Site Recovery Manager 네트워크 포트(8 페이지)

  Site Recovery Manager는 사용자가 구성 가능한 네트워크 포트를 사용하여 클라이언트 및 다른 서버와 통신합니다. Site Recovery Manager가 사용하는 포트를 방화벽이 차단하지 않는지 확인해야 합니다.

- Site Recovery Manager 구성 파일(9 페이지)

  일부 Site Recovery Manager 구성 파일에는 환경의 보안에 영향을 미칠 수 있는 설정이 포함되어 있습니다. 또한 부적절한 설정은 Site Recovery Manager 환경의 적절한 작동에 영향을 미칠 수도 있습니다.

- Site Recovery Manager 인증서 및 키(9 페이지)

  Site Recovery Manager는 TLS 인증서 및 개인 키를 사용하여 네트워크 통신을 보호하고 다른 서버와의 인증을 안전하게 설정합니다.

- Site Recovery Manager 저장된 자격 증명(10 페이지)

  Site Recovery Manager는 SRA(스토리지 복제 어댑터)와 데이터베이스의 자격 증명을 Windows 레지스트리에 암호화된 형식으로 저장합니다.

- Site Recovery Manager 라이센스 및 EULA 파일(10 페이지)

  Site Recovery Manager 라이센스 및 EULA 파일은 Site Recovery Manager Server 호스트 시스템에 있습니다.

- Site Recovery Manager 로그 파일(10 페이지)

  Site Recovery Manager는 작동 정보를 로그 파일에 기록합니다. 로그 파일에는 개인 키나 암호와 같은 민감한 정보가 포함되지 않습니다.

- Site Recovery Manager 계정(11 페이지)

  Site Recovery Manager에서는 SSO(Single Sign-On)를 사용하여 vCenter Server 및 Platform Services Controller에 액세스합니다.

- Site Recovery Manager 보안 업데이트 및 패치(12 페이지)

  VMware에서 Site Recovery Manager 보안 업데이트 및 패치를 제공할 경우 이를 적용할 수 있습니다. 호스트 운영 체제의 벤더가 호스트 운영 체제의 보안 업데이트 및 패치를 제공할 경우 이를 적용할 수 있습니다.

- Site Recovery Manager Server 보안 모범 사례(12 페이지)
  Site Recovery Manager Server 보안 모범 사례를 통해 발생 가능한 보안 문제로부터 환경을 보호할 수 있습니다.

Site Recovery Manager 서비스

Site Recovery Manager Server 호스트 시스템에서 실행되는 여러 서비스는 Site Recovery Manager의 작동에 중요한 역할을 합니다.

표 1-1. Site Recovery Manager 에 필요한 서비스

서비스 이름	시작 시간	설명
VMware vCenter Site Recovery Manager Server	자동	핵심 Site Recovery Manager 기능을 제공합니다.
VMware vCenter Site Recovery Manager 내장형 데이터베이스	내장형 데이터베이스를 사용하는 경우 자동	Site Recovery Manager 내장형 데이터베이스용 vPostgres 서버입니다.
서버	자동	네트워크를 통한 파일 공유를 지원하는 Windows 서비스입니다.
Workstation	자동	원격 서버에 대한 연결을 만들고 유지하는 Windows 서비스입니다.
보호된 스토리지	자동	민감한 데이터를 저장하는 Windows 서비스입니다.

Site Recovery Manager 네트워크 포트

Site Recovery Manager는 사용자가 구성 가능한 네트워크 포트를 사용하여 클라이언트 및 다른 서버와 통신합니다. Site Recovery Manager가 사용하는 포트를 방화벽이 차단하지 않는지 확인해야 합니다.

Site Recovery Manager Server는 들어오는 모든 트래픽을 하나의 네트워크 포트에서 수신합니다. 기본 포트는 9086입니다. 내장형 데이터베이스를 사용하도록 Site Recovery Manager를 구성하면 Site Recovery Manager 내장형 데이터베이스는 로컬 루프백 인터페이스에서 localhost 네트워크 트래픽을 수신합니다. 기본 포트는 5678입니다.

기본 포트가 차단되었거나 다른 애플리케이션이 해당 포트를 사용하는 경우에는 설치 프로세스 도중 Site Recovery Manager 및 내장형 데이터베이스용으로 다른 포트를 선택할 수 있습니다. 수신 포트의 트래픽을 허용하도록 네트워크 정책을 구성해야 합니다. 설치 후 변경할 수 있는 포트에 대한 자세한 내용은 Site Recovery Manager 설치 및 구성 설명서에서 Site Recovery Manager Server 설치 수정 항목을 참조하십시오.

Site Recovery Manager Server는 로컬 사이트의 Platform Services Controller, vCenter Server, ESXi 호스트 및 어레이와 통신합니다. 로컬 사이트에 있는 모든 구성 요소의 네트워크 포트로 가는 트래픽을 네트워크 방화벽 정책이 허용하는지 확인해야 합니다. 모든 VMware 제품이 사용하는 기본 포트의 목록은 http://kb.vmware.com/kb/1012382를 참조하십시오.

Site Recovery Manager 쌍에 속하는 로컬 사이트와 원격 사이트 간 연결은 VPN처럼 전용이어야 합니다. 로컬 Site Recovery Manager Server는 원격 사이트의 Site Recovery Manager Server, Platform Services Controller 및 vCenter Server와 통신하며 네트워크 공급자는 네트워크 정책이 트래픽을 허용하는지 확인해야 합니다.

Site Recovery Manager에 대해 열려 있어야 하는 모든 포트의 목록은 http://kb.vmware.com/kb/2147112를 참조하십시오.

Site Recovery Manager 구성 파일

일부 Site Recovery Manager 구성 파일에는 환경의 보안에 영향을 미칠 수 있는 설정이 포함되어 있습니다. 또한 부적절한 설정은 Site Recovery Manager 환경의 적절한 작동에 영향을 미칠 수도 있습니다.

표 1-2. Site Recovery Manager 구성 파일

파일 또는 디렉토리 위치	설명
installation_folder₩VMware₩VMware vCenter Site Recovery Manager₩config₩vmware-dr.xml	Site Recovery Manager Server의 시스템 구성을 정의합니다. **참고** 구성 파일을 이동하거나 삭제하지 마십시오. vSphere Web Client 사용자 인터페이스의 [관리] 페이지에서 **고급 설정** 탭을 사용하여 Site Recovery Manager 인스턴스의 시스템 설정을 안전하게 변경할 수 있습니다.
installation_folder₩VMware₩VMware vCenter Site Recovery Manager Embedded Database₩bin₩vmw_vpg_config₩	내장형 데이터베이스 구성 파일이 포함되어 있습니다. **참고** 구성 파일을 수정, 이동 또는 삭제하지 마십시오.
installation_folder₩VMware₩VMware vCenter Site Recovery Manager₩config₩extension.xml	Site Recovery Manager Server 확장의 구성을 정의합니다. extension.xml 파일에는 기본 사용자 역할과 그 권한에 대한 정의가 포함되어 있습니다. **참고** 구성 파일을 수정, 이동 또는 삭제하지 마십시오.

Site Recovery Manager 인증서 및 키

Site Recovery Manager는 TLS 인증서 및 개인 키를 사용하여 네트워크 통신을 보호하고 다른 서버와의 인증을 안전하게 설정합니다.

CA 인증서나 개인 키 또는 둘 모두	위치 및 설명
Site Recovery Manager Server 끝점용 TLS 인증서 및 키	Windows 인증서 저장소의 Certificates₩vmware-dr₩Personal₩Certificates 폴더입니다. 설치 도중 사용자 지정 인증서를 제공하지 않으면 Site Recovery Manager가 인증서를 생성합니다.
Site Recovery Manager 설치 도중 생성되는 solution 사용자용 TLS 인증서 및 키	Windows 인증서 저장소의 Certificates₩vmware-dr₩su-*Site Recovery Manager UUID*₩Certificates 폴더입니다.
원격 사이트의 solution 사용자용 TLS 인증서 및 키	Windows 인증서 저장소의 Certificates₩vmware-dr₩remote-su-*Site Recovery Manager UUID*₩Certificates 폴더입니다. Site Recovery Manager 는 쌍 구성 프로세스 도중 파일을 생성합니다.
Site Recovery Manager Server 용 인증서 및 TLS 인증서	*installation_folder*₩VMware₩VMware vCenter Site Recovery Manager₩bin₩*SRM_Server_IP_addressca*.p7b 파일. 설치 도중 사용자 지정 인증서를 제공하지 않으면 Site Recovery Manager가 인증서를 생성합니다. 인증서를 클라이언트 신뢰 Keystore로 가져와서 사용자가 Site Recovery Manager Server 인증서를 명시적으로 신뢰하도록 허용할 수 있습니다.

참고 Site Recovery Manager 인스턴스를 보호하기 위해, 개인 키 정보를 추출하거나 공유하지 마십시오.

Site Recovery Manager 인증 메커니즘에 대한 자세한 내용은 Site Recovery Manager 설치 및 구성 가이드에서 Site Recovery Manager 인증 항목을 참조하십시오.

Site Recovery Manager 저장된 자격 증명

Site Recovery Manager는 SRA(스토리지 복제 어댑터)와 데이터베이스의 자격 증명을 Windows 레지스트리에 암호화된 형식으로 저장합니다.

관리자 그룹의 구성원인 경우 자격 증명에 액세스할 수 있습니다.

레지스트리 경로	설명
HKEY_LOCAL_MACHINE₩System₩CurrentControlSet₩services₩Vmware DR₩Creds₩db:*datastore name*	datastore name 시스템 데이터스토어를 사용하여 Site Recovery Manager 데이터베이스에 액세스하기 위한 자격 증명입니다.
HKEY_LOCAL_MACHINE₩System₩CurrentControlSet₩services₩Vmware DR₩Creds₩storage-arraymanager *manager id*-username	SRA에서 어레이 관리자(manager id로 식별)에 연결하는 데 사용해야 하는 사용자 이름입니다.
HKEY_LOCAL_MACHINE₩System₩CurrentControlSet₩services₩ Vmware DR₩Creds₩storage-arraymanager-*manager id*-password	SRA에서 어레이 관리자(manager id로 식별)에 연결하는 데 사용해야 하는 암호입니다.

Site Recovery Manager 라이센스 및 EULA 파일

Site Recovery Manager 라이센스 및 EULA 파일은 Site Recovery Manager Server 호스트 시스템에 있습니다.

표 1-3. Site Recovery Manager 라이센스 및 EULA 파일

파일 또는 디렉토리	설명
installation_folder₩VMware₩VMware vCenter Site Recovery Manager₩en₩	Site Recovery Manager 최종 사용자 계약 파일이 들어 있는 디렉토리입니다.
installation_folder₩VMware₩VMware vCenter Site Recovery Manager₩en₩open_source_license.txt	Site Recovery Manager 오픈 소스 라이센스 파일입니다.
installation_folder ₩VMware₩VMware vCenter Site Recovery Manager₩en₩ open_source_license_vix.txt	Virtual Infrastructure Extension API 오픈 소스 라이센스 파일입니다.
installation_folder₩VMware₩VMware vCenter Site Recovery Manager Embedded Database₩share₩EULA-en.doc	Site Recovery Manager 내장형 데이터베이스 최종 사용자 라이센스 계약 파일입니다.
installation_folder₩VMware₩VMware vCenter Site Recovery Manager Embedded Database₩share₩open_source_license.txt	Site Recovery Manager 내장형 데이터베이스 오픈 소스 라이센스 파일입니다.

Site Recovery Manager 로그 파일

Site Recovery Manager는 작동 정보를 로그 파일에 기록합니다. 로그 파일에는 개인 키나 암호와 같은 민감한 정보가 포함되지 않습니다.

Site Recovery Manager는 C:₩ProgramData₩VMware₩VMware vCenter Site Recovery Manager₩Logs 디렉토리에 시스템 로그 파일을 저장합니다. Site Recovery Manager Server의 최신 메시지는 vmware-dr-*number*.log 파일에 기록됩니다.

Site Recovery Manager Server를 다시 시작하거나 현재 파일이 설정된 파일 크기 제한을 초과하는 경우 Site Recovery Manager는 현재 로그 파일을 보관하고 새 로그 파일을 생성합니다.

로그 파일 디렉토리를 변경하려면 *installation_directory*₩VMware₩VMware vCenter Site Recovery Manager₩config₩vmware-dr.xml 구성 파일의 directory XML 요소에 사용자 지정 디렉토리 이름을 입력하십시오. 또한 vmware-dr.xml 파일의 logLevel XML 요소를 업데이트하여 각 구성 요소의 로그 수준을 변경할 수도 있습니다. 모든 구성 요소의 기본 수준은 세부 정보 표시입니다.

중요 액세스 제어 목록을 구성하여 로그 파일에 대한 액세스를 제한하십시오.

표 1-4. 로그 수준

수준	설명
오류	오류 로그 항목만 표시
정보	정보, 오류 및 경고 로그 항목 표시
기타 정보	정보, 오류, 경고, 세부 로그 항목 및 기타 로그 항목 표시
세부 정보 표시	정보, 오류, 경고 및 세부 로그 항목 표시
주의	경고 및 오류 로그 항목 표시

Site Recovery Manager에서는 다음과 같은 구성 요소를 지원합니다.

- 기본값
- 복제
- 복구
- 스토리지
- StorageProvider
- Vdb
- 지속성

vmware-dr-*number*.log 파일에는 인증 프로세스 및 원격 측과의 연결에 대한 보안 메시지가 포함되지 않습니다.

Site Recovery Manager 계정

Site Recovery Manager에서는 SSO(Single Sign-On)를 사용하여 vCenter Server 및 Platform Services Controller에 액세스합니다.

사용자 계정

vCenter Server 관리자는 기본 구성에서 Site Recovery Manager에 대한 관리 액세스 권한을 갖습니다. 설치 후 Site Recovery Manager에 처음 로그인할 때는 관리자 자격 증명을 사용해야 합니다.

관리자 자격 증명이 있는 경우에는 vSphere Web Client를 사용하여 다른 사용자에게 Site Recovery Manager 액세스 권한을 부여할 수 있습니다.

Site Recovery Manager 역할, 권한 및 사용 권한에 대한 자세한 내용은 Site Recovery Manager 관리 설명서의 Site Recovery Manager 권한, 역할 및 사용 권한을 참조하십시오.

Solution 사용자 계정

Site Recovery Manager는 설치 도중 solution 사용자를 생성하고 vCenter Server에 인증할 때 이를 사용합니다. solution 사용자는 각 Site Recovery Manager 인스턴스마다 고유하며 Site Recovery Manager, vCenter Server 및 Platform Services Controller가 내부적으로 사용하기 위한 용도입니다.

Site Recovery Manager는 고급 연결 모드를 사용하지 않는 사이트의 쌍 구성 프로세스 도중에 각 원격 사이트에 추가적인 solution 사용자를 생성합니다. Site Recovery Manager는 원격 사이트에서 필요한 작업을 수행할 때 solution 사용자를 사용합니다.

참고 solution 사용자 계정과 연결된 역할 및 권한을 삭제 및 수정하면 안 됩니다.

solution 사용자 및 로컬 사이트와 원격 사이트 간의 인증에 대한 자세한 내용은 Site Recovery Manager 설치 및 구성 설명서의 Site Recovery Manager 인증 항목을 참조하십시오.

Site Recovery Manager 보안 업데이트 및 패치

VMware에서 Site Recovery Manager 보안 업데이트 및 패치를 제공할 경우 이를 적용할 수 있습니다. 호스트 운영 체제의 벤더가 호스트 운영 체제의 보안 업데이트 및 패치를 제공할 경우 이를 적용할 수 있습니다.

Site Recovery Manager 호스트 운영 체제 버전

Site Recovery Manager Server에서 지원하는 호스트 운영 체제에 대한 자세한 내용은 Site Recovery Manager 6.5 호환성 매트릭스(https://www.vmware.com/support/srm/srm-compat-matrix-6-5.html)를 참조하십시오.

Site Recovery Manager 패치 및 보안 업데이트 적용

Site Recovery Manager 보안 패치 및 업그레이드는 기존 Site Recovery Manager 설치에 인플레이스 업그레이드를 수행하여 적용합니다. Site Recovery Manager 업그레이드에 대한 자세한 내용은 Site Recovery Manager 설치 및 구성의 Site Recovery Manager Server 인플레이스 업그레이드 항목을 참조하십시오.

Site Recovery Manager Server 보안 모범 사례

Site Recovery Manager Server 보안 모범 사례를 통해 발생 가능한 보안 문제로부터 환경을 보호할 수 있습니다.

Site Recovery Manager Server 운영 체제가 적절하게 구성 및 유지 보수되어야 Site Recovery Manager의 안전한 작동이 보장됩니다.

- Site Recovery Manager는 지원되는 호스트 운영 체제, 데이터베이스 및 하드웨어에서만 실행합니다. Site Recovery Manager가 지원되는 호스트 운영 체제에서 실행 중이지 않은 경우 Site Recovery Manager가 제대로 실행되지 않을 수 있습니다.
- 호스트 운영 체제를 악의적 공격으로부터 보호하기 위해 최신 운영 체제 업데이트 및 패치를 적용합니다. 최신 Site Recovery Manager 업데이트 및 패치를 적용하여 Site Recovery Manager의 알려진 문제를 해결합니다.
- Site Recovery Manager를 VM으로 실행할 때 Site Recovery Manager 배포의 무결성을 확인합니다. vSphere 보안 설명서의 가상 시스템 보안 모범 사례 항목을 참조하십시오.
- 소프트웨어 설치를 제한하고 Site Recovery Manager가 사용하지 않는 서비스를 사용하지 않도록 설정하여 리소스를 확보하고 서버 공격의 가능성을 줄입니다. 불필요한 소프트웨어 및 서비스는 CPU, 스토리지, 메모리 및 대역폭 리소스를 소비하며 서버 공격의 기회를 높입니다.
- 관리자만 서버에 액세스하도록 허용합니다. 공격자가 사용할 수 있는 계정의 수를 제한하기 위해 서버에 액세스할 수 있는 계정의 수를 제한합니다.
- Site Recovery Manager가 사용하는 네트워크 포트를 확인하고 서버를 보호하도록 방화벽을 구성합니다.

색인