VMware vSphere Replication 보안 가이드

vSphere Replication 8.2

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

https://docs.vmware.com/kr/

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

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화:+82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

목차

VMware vSphere Replication 보안 가이드 정보

1

"VMware vSphere Replication 보안 가이드" 는 vSphere Replication의 보안 기능에 대한 간결한 참조를 제공합니다.

이 설명서에서는 설치된 vSphere Replication을 보호할 수 있도록 vSphere Replication에 포함되어 있는 보안 기능 및 공격을 방지하는 방법에 대해 설명합니다.

- vSphere Replication의 적절한 작동을 위해 필요한 외부 인터페이스, 포트 및 서비스
- 보안에 영향을 미치는 구성 옵션 및 설정
- 로그 파일의 위치 및 해당 파일의 용도
- 필수 시스템 계정
- 최신 보안 패치 가져오기에 대한 정보

대상 사용자

이 정보는 IT 의사결정권자, 설계자, 관리자 및 vSphere Replication의 보안 구성 요소를 숙지해야 하는 기타 사용자를 위한 것입니다.

vSphere Replication 보안 참조 2

보안 참조를 사용하여 vSphere Replication의 보안 기능 및 공격으로부터 환경을 보호하는 방법에 대해 알아볼 수 있습니다.

본 장은 다음 항목을 포함합니다.

- vSphere Replication 가상 장치에 사용되는 서비스, 포트 및 외부 인터페이스
- vSphere Replication 구성 파일
- vSphere Replication 개인 키, 인증서 및 Keystore
- vSphere Replication 라이센스 및 EULA 파일
- vSphere Replication 로그 파일
- vSphere Replication 사용자 계정
- vSphere Replication용 보안 업데이트 및 패치

vSphere Replication 가상 장치에 사용되는 서비스, 포트 및 외부 인터페이스

vSphere Replication의 작동은 특정 서비스, 포트 및 외부 인터페이스에 따라 다릅니다.

vSphere Replication 서비스

vSphere Replication의 작동은 vSphere Replication 가상 장치에서 실행되는 여러 서비스에 따라 다릅니다.

표 2-1. vSphere Replication 서비스

서비스 이름	시작 유형	설명
hms	vSphere Replication 장치에 대해 자동입니다. vSphere Replication 추가 기능 장치에 대해 사용하지 않도록 설정되어 있습니다.	vSphere Replication 관리 서비스
hbrsrv	자동	vSphere Replication 서비스
sshd	기본적으로 사용하지 않도록 설정되어 있습니다.	SSH 서비스

표 2-1. vSphere Replication 서비스 (계속)

서비스 이름	시작 유형	설명
ntp	자동	NTP(Network Time Protocol)를 통해 인터넷 시간 서버와 동기화하기 위한 시간 서비스입니다. **참고** vSphere Replication 가상 장치를 설치하거나 업그레이드한 후 장치를 시간 서버와 동기화해야 합니다.
vaos	자동	네트워크 설정, 호스트 이름 설정, ssh 키 생성, EULA 수락, 부팅 스크립트 실행 및 VAMI 초기화를 제공하는 게스트 OS 초기화입니다.

통신 포트

vSphere Replication은 여러 통신 포트 및 프로토콜을 사용합니다.

vSphere Replication 장치를 사용하려면 특정 포트가 열려 있어야 합니다.

참고 vSphere Replication 서버에는 대상 ESXi 호스트에 대한 NFC 트래픽 액세스 권한이 있어야 합니다.

표 2-2. vSphere Replication 장치에 사용되는 포트

소스	대상	포트	프로토콜	설명
vSphere Replication 장치	로컬 vCenter Server	80	TCP	로컬 vCenter Server 프록시 시스템으로의 모든 관리 트래픽. vSphere Replication 은 vCenter Server 서비스에 연결하는 SSL 터널을 엽니다.
vSphere Replication 장치	원격 조회 서비스	443	TCP	원격 조회 서비스에 대한 모든 호출.
vSphere Replication 장치의 vSphere Replication 서버	ESXi 호스트(사이트 내)	80	HTTP	초기 복제가 시작되기 전에 연결을 설정하는 데 사용됩니다.
vSphere Replication 장치	로컬 및 원격 vCenter Server	443	TCP	vSphere Replication 장치에 대한 모든 관리 트래픽
vSphere Replication 장치의 vSphere Replication 서버	보조 사이트의 ESXi 호스트(사이트 내만)	902	TCP 및 UDP	vSphere Replication 서버가 복제 트래픽을 대상 ESXi 호스트로 보내는 데 사용됩니다.
브라우저	vSphere Replication 장치	5480	HTTPS	vSphere Replication VAMI(가상 장치 관리 인터페이스) 웹 UI입니다.
vCenter Server 프록시	vSphere Replication 장치	8043	SOAP	소스 사이트와 대상 사이트의 vSphere Replication 관리 서버의 사이트 간 통신입니다.
vSphere Replication 장치	vSphere Replication 서버	8123	SOAP	vSphere Replication 관리 서버에서 환경의 추가적인 vSphere Replication 서버로의 사이트 내 관리 트래픽입니다.

표 2-2. vSphere Replication 장치에 사용되는 포트 (계속)

소스	대상	포트	프로토콜	설명
소스 사이트의 ESXi 호스트	대상 사이트의 vSphere Replication 서버	31031	TCP	소스 사이트의 ESXi 호스트에서 대상 사이트의 vSphere Replication 장치 또는 vSphere Replication 서버로의 초기 복제 트래픽 및 나가는 복제 트래픽입니다(네트워크 암호화가 없는 복제 트래픽).
소스 사이트의 ESXi 호스트	대상 사이트의 vSphere Replication 서버	32032	TCP	소스 사이트의 ESXi 호스트에서 대상 사이트의 vSphere Replication 장치 또는 vSphere Replication 서버로의 초기 복제 트래픽 및 나가는 복제 트래픽입니다(네트워크 암호화가 있는 복제 트래픽).

vSphere Replication 서버를 추가로 배포하는 경우 사용자는 해당 서버에서 vSphere Replication에 필요한 포트를 열어야 합니다.

표 2-3. vSphere Replication 서버에 사용되는 포트

소스	대상	포트	프로토콜	설명
vSphere Replication 장치의 vSphere Replication 서버	보조 사이트의 ESXi 호스트(사이트 내만)	902	TCP 및 UDP	동일한 사이트에 있는 vSphere Replication 서버와 ESXi 호스트 간 트래픽입니다. 특히 대상 ESXi 서버로 이동하는 NFC 서비스 트래픽입니다.
브라우저	vSphere Replication 서버	5480	HTTPS	관리자의 웹 브라우저입니다.
vSphere Replication 관리 서버	vSphere Replication 서버	8123	SOAP	vSphere Replication 장치 또는 vSphere Replication 관리 서버에서 vSphere Replication 서버로의 사이트 내 관리 트래픽입니다.
소스 사이트의 ESXi 호스트	vSphere Replication 서버	31031	TCP	소스 사이트의 ESXi 호스트에서 대상 사이트의 vSphere Replication 장치 또는 vSphere Replication 서버로의 초기 복제 트래픽 및 정방향 복제 트래픽입니다.
소스 사이트의 ESXi 호스트	대상 사이트의 vSphere Replication 서버	32032	TCP	소스 사이트의 ESXi 호스트에서 대상 사이트의 vSphere Replication 장치 또는 vSphere Replication 서버로의 네트워크 암호화가 있는 초기 복제 트래픽 및 정방향 복제 트래픽입니다.

클라우드에 대한 연결을 생성하는 경우 vSphere Replication 장치의 vCloud Tunneling Agent가 사용자 클라우드 조직으로의 복제 데이터 전송을 보호하기 위해 터널을 생성합니다.

표 2-4. 클라우드 복제에 필요한 포트

소스	대상	포트	프로토콜	설명
소스 사이트의 ESXi 호스트	소스 사이트의 vCenter Server	80	TCP	vCenter Server 역방향 프록시에서 VIB (vCloud Availability 방화벽 규칙) 다운로드 요청을 vSphere Replication 장치에 전달합니다.
소스 사이트의 vSphere Replication 장치	vCloud API	443	HTTPS를 통한 REST	vSphere Replication 장치는 이 포트에 연결하여 클라우드 조직에 복제 데이터를 보냅니다.
소스 사이트의 ESXi 호스트	소스 사이트의 vSphere Replication 장치	10000–10010	TCP	vCloud Tunneling Agent는 vSphere Replication 장치에서 이러한 포트 중 하나를 엽니다. ESXi 호스트는 해당 포트에 연결하여 클라우드 조직에 복제 데이터를 보냅니다.

오픈 소스 및 타사 구성 요소

오픈 소스 라이센스의 완전한 텍스트, 모든 오픈 소스 및 타사 구성 요소 목록 그리고 vSphere Replication에서 사용된 오픈 소스 코드를 보려면 http://www.vmware.com/download/open_source.html 주소로 이동하여 "VMware vSphere 오픈 소스" 링크 아래의 "VMware vSphere Replication 오픈 소스 및 라이센스" 섹션을 참조하십시오. 특정 오픈 소스 라이센스에 필요한 경우, vSphere Replication ODP(오픈 소스 공개 패키지)에 소프트웨어 라이브러리를 구축하고 교체하는 방법을 설명하는 텍스트 파일이 포함되어 있습니다.

vSphere Replication 구성 파일

일부 구성 파일에는 vSphere Replication의 보안에 영향을 미치는 설정이 포함되어 있습니다.

참고 모든 보안 관련 리소스는 올바른 사용 권한 및 소유권으로 보호됩니다. 해당 파일의 소유권이나 사용 권한을 변경하지 마십시오.

파일 위치	설명
`/opt/vmware/hms/conf/hms-configuration.xml`	vSphere Replication 관리 서버의 기본 시스템 구성입니다.
`/opt/vmware/hms/conf/embedded_db.cfg`	포함된 데이터베이스의 구성 파일입니다.

vSphere Replication 개인 키, 인증서 및 Keystore

vSphere Replication의 개인 키, 인증서 및 keystore는 vSphere Replication 가상 장치에 있습니다.

참고 모든 보안 관련 리소스는 올바른 사용 권한 및 소유권으로 보호됩니다. 해당 파일의 소유권이나 사용 권한을 변경하지 마십시오.

- `/etc/vmware/ssl/hbrsrv.crt`
- `/etc/vmware/ssl/hbrsrv.key`

- /opt/vmware/hms/security/hms-keystore.jks
- /opt/vmware/hms/security/hms-truststore.jks

vSphere Replication 라이센스 및 EULA 파일

EULA(최종 사용자 라이센스 계약) 및 오픈 소스 라이센스 파일은 vSphere Replication 가상 장치에 있습니다.

파일	위치
오픈 소스 라이센스	/usr/share/doc/vmware-vspherereplication/OPEN_SOURCE_LICENSE
VMware Postgres 라이센스	/usr/share/doc/vmware-vspherereplication/VMware_Postgres_9.5.16.0_open_source_licenses.txt
최종 사용자 라이센스 계약	/opt/vmware/etc/isv/EULA/*language_code*/0

vSphere Replication 로그 파일

시스템 메시지가 포함된 파일은 vSphere Replication 가상 장치에 있습니다.

파일 위치	설명
/opt/vmware/hms/logs/hms-configtool.log	VAMI(가상 장치 관리 인터페이스) 구성 중에 발생한 오류를 기록하는 데 사용됩니다.
/opt/vmware/hms/logs/hms.*n*.log	vSphere Replication 관리 서버의 런타임 정보를 추적하는 데 사용됩니다. 최신 로그 파일에는 hms.log로 레이블이 지정되며, hms.*n*.log 파일에는 이전 로그 메시지가 포함되어 있습니다. 가장 큰 *n* 값이 있는 파일에 가장 오래된 메시지가 포함되어 있습니다.
/opt/vmware/var/log/lighttpd/error.log	VAMI 오류 로그 파일입니다. VAMI 작업에서 오류를 추적하는 데 사용됩니다.
/var/log/vmware/	이 폴더에는 vSphere Replication 서버 로그 파일이 포함되어 있습니다. 복제 문제를 추적하는 데 사용됩니다.
/var/opt/apache-tomcat/logs/dr.log	Site Recovery 사용자 인터페이스 로그입니다.
/opt/vmware/hms/logs/hms-audit.log	vSphere Replication 감사 로그입니다.

보안과 관련된 로그 메시지

/opt/vmware/hms/logs/hms.log 파일에는 다음과 같은 형식으로 로그인과 로그아웃 이벤트 메시지, 인증 오류 메시지 및 인증서 확인 오류 메시지가 포함되어 있습니다.

- 로그인 메시지

  ```
  2015-03-23 15:54:05.558 DEBUG jvsl.security.authentication.sessionmap [tcweb-5]
  (..security.authentication.SessionMap) operationID=087657ec-ef0f-494c-9739-
  a4af62a5c049-HMS-1033 | Adding new session to the session
  map:com.vmware.hms.security.authentication.HmsUserSession@234f4bed:[
  ```

```
com.vmware.vim.binding.hms.UserSession:
key = site_...1b034,
userName = root,
fullName = root ,
loginTime = ...,
lastActiveTime = ...,
hmsServers = null,
locale = en,
messageLocale = en
]
```

- 로그아웃 메시지

```
15-03-23 15:54:05.585 INFO jvsl.security.authorization [tcweb-8]
(..security.authorization.SessionAuthorizer) |
HmsSessionManager.HmsSessionManagerLogout called on session-manager by root@/
10.26.233.124:50776 with opId 43263a64-1681-4459-a921-1d9406308dc8-HMS-1036
```

- 인증 메시지

```
2015-06-25 16:10:35.994 INFO jvsl.security.authorization [tcweb-5]
(..security.authorization.SessionAuthorizer) | Authorization for method
"HmsRemoteSiteManager.HmsRemoteSiteManagerFindHmsServer" failed.
(vim.fault.NoPermission) {
faultCause = null,
faultMessage = null,
object = MoRef: type = HmsRemoteSiteManager, value = site-manager, serverGuid =
18327b1a-dac2-44d9-972e-fa9dd99fce47,
privilegeId = HmsRemote.com.vmware.vcHms.Hms.View
}
```

- 인증서 확인 오류 메시지

```
2015-06-25 16:19:13.794 WARN jvsl.sessions [hms-main-thread-1]
(..hms.net.ServerRegistryHms) | Can not start HMS connection to remote site
'some-address.com'
java.util.concurrent.ExecutionException:
com.vmware.vim.vmomi.client.exception.SslException:
javax.net.ssl.SSLHandshakeException:
com.vmware.vim.vmomi.client.exception.VlsiCertificateException: Server
certificate chain is not trusted and thumbprint doesn't match
```

vSphere Replication 사용자 계정

vSphere Replication에 대한 루트 계정을 설정해야 합니다. 루트 계정을 사용하여 가상 장치 콘솔 및 VAMI(가상 장치 관리 인터페이스) 모두에 액세스합니다.

현재 vSphere Replication은 루트 계정을 VAMI의 관리자로 사용합니다. 다른 사용자는 생성되지 않습니다.

vSphere Replication 가상 장치를 배포하는 경우 OVF 배포 마법사에서 루트 계정에 대한 암호를 설정합니다.

루트 암호는 8자 이상이어야 합니다.

기본 사용자 역할에 할당된 권한

vSphere Replication에는 역할 집합이 포함되어 있습니다. 각 역할에는 해당 역할을 가진 사용자가 서로 다른 작업을 수행할 수 있도록 하는 권한 집합이 포함되어 있습니다.

자세한 내용은 "VMware vSphere Replication 설치 및 구성" 가이드의 "vSphere Replication 역할 및 사용 권한" 항목을 참조하십시오.

vSphere Replication용 보안 업데이트 및 패치

vSphere Replication 가상 장치는 VMware Photon OS 2.0을 게스트 운영 체제로 사용합니다.

해당 ISO 파일을 사용하여 최신 보안 업데이트 또는 패치를 적용할 수 있습니다.

게스트 운영 체제에 업데이트나 패치를 적용하기 전에 종속성을 고려하십시오. vSphere Replication 가상 장치에 사용되는 서비스, 포트 및 외부 인터페이스를 참조하십시오.

최신 보안 공지 사항을 받으려면 http://lists.vmware.com/에서 VMware 보안 공지 사항 메일 그룹을 구독할 수 있습니다.