VMware vSphere Replication 安全指南

vSphere Replication 8.2

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

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

威睿信息技术（中国）有限公司
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

1 关于《VMware vSphere Replication 安全指南》 4

2 vSphere Replication 安全参考 5

vSphere Replication 虚拟设备使用的服务、端口和外部接口 5

vSphere Replication 配置文件 8

vSphere Replication 专用密钥、证书和密钥库 8

vSphere Replication 许可证和 EULA 文件 8

vSphere Replication 日志文件 9

vSphere Replication 用户帐户 10

vSphere Replication 的安全更新和修补程序 11

关于《VMware vSphere Replication 安全指南》

1

《VMware vSphere Replication 安全指南》提供有关 vSphere Replication 的安全功能的简明参考。

为了帮助保护 vSphere Replication 安装，本指南介绍了 vSphere Replication 中内置的安全功能以及为保护它不受攻击而可以采取的措施。

- vSphere Replication 正常运行所需的外部接口、端口和服务
- 具有安全影响的配置选项和设置
- 日志文件的位置及其用途
- 所需系统帐户
- 有关获取最新安全修补程序的信息

目标读者

本指南旨在为 IT 决策制定者、架构师、管理员以及必须熟悉 vSphere Replication 的安全组件的其他人员提供相关信息。

vSphere Replication 安全参考

2

可以使用该安全参考了解 vSphere Replication 的安全功能以及为保护该环境不受攻击而可以采取的措施。

本章讨论了以下主题：

- vSphere Replication 虚拟设备使用的服务、端口和外部接口
- vSphere Replication 配置文件
- vSphere Replication 专用密钥、证书和密钥库
- vSphere Replication 许可证和 EULA 文件
- vSphere Replication 日志文件
- vSphere Replication 用户帐户
- vSphere Replication 的安全更新和修补程序

vSphere Replication 虚拟设备使用的服务、端口和外部接口

vSphere Replication 的操作取决于某些服务、端口和外部接口。

vSphere Replication 服务

vSphere Replication 的操作取决于在 vSphere Replication 虚拟设备上运行的几项服务。

表 2-1. vSphere Replication 服务

服务名称	启动类型	描述
hms	对于 vSphere Replication 设备：自动。对于 vSphere Replication 附加设备：禁用。	vSphere Replication 管理服务
hbrsrv	自动	vSphere Replication 服务
sshd	默认值：禁用。	SSH 服务

表 2-1. vSphere Replication 服务 （续）

服务名称	启动类型	描述
ntp	自动	时间服务，用于通过网络时间协议与 Internet 时间服务器同步。 注 安装或升级 vSphere Replication 虚拟设备后，必须将设备与时间服务器进行同步。
vaos	自动	客户机操作系统初始化，用于驱动网络设置、主机名设置、ssh 密钥创建、EULA 接受、引导脚本执行和 VAMI 初始化。

通信端口

vSphere Replication 使用多个通信端口和协议。

vSphere Replication 设备需要某些端口处于打开状态。

注 vSphere Replication 服务器必须对目标 ESXi 主机具有 NFC 流量访问权限。

表 2-2. 由 vSphere Replication 设备使用的端口

源	目标	端口	协议	描述
vSphere Replication 设备	本地 vCenter Server	80	TCP	所有传输到本地 vCenter Server 代理系统的管理流量。vSphere Replication 将打开一个 SSL 隧道以连接到 vCenter Server 服务。
vSphere Replication 设备	远程查找服务	443	TCP	对远程查找服务的所有调用。
vSphere Replication 设备中的 vSphere Replication 服务器	ESXi 主机（站点内）	80	HTTP	用于在初始复制开始之前建立连接。
vSphere Replication 设备	本地和远程 vCenter Server	443	TCP	流向 vSphere Replication 设备的所有管理流量。
vSphere Replication 设备中的 vSphere Replication 服务器	辅助站点上的 ESXi 主机（仅限站点内）	902	TCP 和 UDP	由 vSphere Replication 服务器用于向目标 ESXi 主机发送复制流量。
浏览器	vSphere Replication 设备	5480	HTTPS	vSphere Replication 虚拟设备管理界面 (VAMI) Web UI。
vCenter Server 代理	vSphere Replication 设备	8043	SOAP	来自源站点和目标站点的 vSphere Replication 管理服务器的站点内部通信。
vSphere Replication 设备	vSphere Replication 服务器	8123	SOAP	环境中从 vSphere Replication 管理服务器到其他 vSphere Replication 服务器的站点内部管理流量。

表 2-2. 由 vSphere Replication 设备使用的端口 （续）

源	目标	端口	协议	描述
源站点上的 ESXi 主机	目标站点上的 vSphere Replication 服务器	31031	TCP	从源站点上的 ESXi 主机到目标站点上的 vSphere Replication 设备或 vSphere Replication 服务器的初始和出站复制流量，且不对复制流量使用网络加密。
源站点上的 ESXi 主机	目标站点上的 vSphere Replication 服务器	32032	TCP	从源站点上的 ESXi 主机到目标站点上的 vSphere Replication 设备或 vSphere Replication 服务器的初始和出站复制流量，并对复制流量使用网络加密。

如果部署其他 vSphere Replication 服务器，必须在这些服务器上打开 vSphere Replication 需要的端口。

表 2-3. 由 vSphere Replication 服务器使用的端口

源	目标	端口	协议	描述
vSphere Replication 设备中的 vSphere Replication 服务器	辅助站点上的 ESXi 主机（仅限站点内）	902	TCP 和 UDP	同一站点上的 vSphere Replication 服务器和 ESXi 主机之间的流量。尤其是 NFC 服务到目标 ESXi 服务器的流量。
浏览器	vSphere Replication 服务器	5480	HTTPS	管理员的 Web 浏览器。
vSphere Replication 管理服务器	vSphere Replication 服务器	8123	SOAP	从 vSphere Replication 设备或 vSphere Replication 管理服务器到 vSphere Replication 服务器的站点内部管理流量。
源站点上的 ESXi 主机	vSphere Replication 服务器	31031	TCP	从源站点上的 ESXi 主机到目标站点上的 vSphere Replication 设备或 vSphere Replication 服务器的初始和正向复制流量。
源站点上的 ESXi 主机	目标站点上的 vSphere Replication 服务器	32032	TCP	从源站点上的 ESXi 主机到目标站点上的 vSphere Replication 设备或 vSphere Replication 服务器的初始和正向复制流量（使用网络加密）。

在与云建立连接时，vSphere Replication 设备中的 vCloud Tunneling Agent 会创建通道，以确保向云组织传输复制数据时的安全。

表 2-4. 云复制所需的端口

源	目标	端口	协议	描述
源站点上的 ESXi 主机	源站点上的 vCenter Server	80	TCP	vCenter Server 反向代理将 VIB（vCloud Availability 防火墙规则）下载请求转发到 vSphere Replication 设备。
源站点上的 vSphere Replication 设备	vCloud API	443	HTTPS 上的 REST	vSphere Replication 设备连接到此端口以便将复制数据发送到云组织。
源站点上的 ESXi 主机	源站点上的 vSphere Replication 设备	10000 – 10010	TCP	vCloud Tunneling Agent 打开 vSphere Replication 设备上的这些端口之一。ESXi 主机连接到此端口以便将复制数据发送到云组织。

开源和第三方组件

有关开源许可证的完整文本、所有开源和第三方组件的列表以及 vSphere Replication 中使用的开源代码，可以访问 http://www.vmware.com/download/open_source.html 并查看 VMware vSphere 开源链接下的 VMware vSphere Replication 开源和许可证部分。如果某个开源许可证需要它，则可以通过 vSphere Replication 开源公开数据包 (ODP) 获取包含如何构建和替换软件库说明的文本文件。

vSphere Replication 配置文件

某些配置文件包含的设置影响 vSphere Replication 的安全性。

注 与安全有关的所有资源都通过正确的权限和所有权进行保护。请勿更改这些文件的所有权或权限。

文件位置	描述
/opt/vmware/hms/conf/hms-configuration.xml	vSphere Replication 管理服务器的默认系统配置。
/opt/vmware/hms/conf/embedded_db.cfg	嵌入式数据库的配置文件。

vSphere Replication 专用密钥、证书和密钥库

vSphere Replication 的专用密钥、证书和密钥库位于 vSphere Replication 虚拟设备上。

注 与安全有关的所有资源都通过正确的权限和所有权进行保护。请勿更改这些文件的所有权或权限。

- /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 许可证和 EULA 文件

最终用户许可协议 (EULA) 和开源许可证文件位于 vSphere Replication 虚拟设备中。

文件	位置
开源许可证	/usr/share/doc/vmware-vspherereplication/OPEN_SOURCE_LICENSE
VMware Postgres 许可证	/usr/share/doc/vmware-vspherereplication/ VMware_Postgres_9.5.16.0_open_source_licenses.txt
最终用户许可协议	/opt/vmware/etc/isv/EULA/*language_code*/0

vSphere Replication 日志文件

包含系统消息的文件位于 vSphere Replication 虚拟设备中。

文件位置	描述
/opt/vmware/hms/logs/hms-configtool.log	用于记录在虚拟设备管理界面 (VAMI) 配置期间发生的错误。
/opt/vmware/hms/logs/hms.*n*.log	用于跟踪 vSphere Replication 管理服务器的运行时信息。最新日志文件标记为 hms.log 和 hms。*n*.log 文件包含较旧的日志消息。带有最高 *n* 值的文件包含最旧消息。
/opt/vmware/var/log/lighttpd/error.log	VAMI 错误日志文件。用于跟踪 VAMI 操作中的错误。
/var/log/vmware/	此文件夹包含 vSphere Replication 服务器日志文件。用于跟踪复制问题。
/var/opt/apache-tomcat/logs/dr.log	Site Recovery 用户界面日志。
/opt/vmware/hms/logs/hms-audit.log	vSphere Replication 审核日志。

与安全有关的日志消息

/opt/vmware/hms/logs/hms.log 文件包含登录和注销事件消息、授权错误消息以及证书验证错误消息，其格式如下所示。

- 登录消息

  ```
  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

  ]
  ```

- 注销消息

```
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
```

- 授权消息

```
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

}
```

- 证书验证错误消息

```
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 用户帐户

您必须为 vSphere Replication 设置一个 root 帐户。root 帐户用于访问虚拟设备控制台和虚拟设备管理界面 (Virtual Appliance Management Interface, VAMI)。

vSphere Replication 当前使用 root 帐户作为 VAMI 的管理员。未创建其他用户。

当您部署 vSphere Replication 虚拟设备时，会在 OVF 部署向导中设置 root 帐户的密码。

root 帐户密码的长度必须不少于 8 个字符。

分配给默认用户角色的特权

vSphere Replication 包含一组角色。每一角色包含一组特权，拥有这些角色的用户可以完成不同操作。

请参见《VMware vSphere Replication 安装和配置》指南中的“vSphere Replication 角色和权限”主题。

vSphere Replication 的安全更新和修补程序

vSphere Replication 虚拟设备使用 VMware Photon OS 2.0 作为客户机操作系统。

可以使用相应的 ISO 文件来应用最新的安全更新或修补程序。

在对客户机操作系统应用更新或修补程序之前，请考虑依赖关系。请参见 vSphere Replication 虚拟设备使用的服务、端口和外部接口。

要接收最新的安全公告，可以在 http://lists.vmware.com/ 上订阅 VMware 安全公告邮件列表。