Site Recovery Manager 安全

Site Recovery Manager 8.1

vmware®

最新的技术文档可以从 VMware 网站下载：

https://docs.vmware.com/cn/

您如果对本文档有任何意见或建议，请把反馈信息提交至：

docfeedback@vmware.com

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

北京办公室
北京市海淀区科学院南路 2 号
融科资讯中心 C 座南 8 层
www.vmware.com/cn

上海办公室
上海市浦东新区浦东南路 999 号
新梅联合广场 23 楼
www.vmware.com/cn

广州办公室
广州市天河北路 233 号
中信广场 7401 室
www.vmware.com/cn

目录

关于 VMware Site Recovery Manager 安全

*Site Recovery Manager 安全*提供了对 Site Recovery Manager 的安全功能的简明参考。

为了帮助保护 Site Recovery Manager 安装，本指南介绍了 Site Recovery Manager 中内置的安全功能以及为使其免受攻击而可以采取的措施。

- Site Recovery Manager 正常运行所需的外部接口、端口和服务
- 具有安全意义的配置选项和设置
- 日志文件的位置及其用途
- 所需的系统帐户
- 关于获取最新安全修补程序的信息

目标受众

本信息专供 IT 决策者、架构师、管理员以及必须熟悉 Site Recovery Manager 的安全组件的人员使用。

Site Recovery Manager 安全参考

1

通过安全参考，可以了解 Site Recovery Manager 安装的安全功能以及为使环境免受攻击而可以采取的措施。

- Site Recovery Manager 服务

  Site Recovery Manager 的操作取决于 Site Recovery Manager Server 主机上运行的几项服务。

- Site Recovery Manager 网络端口

  Site Recovery Manager 使用可配置的网络端口与客户端及其他服务器进行通信。必须确保防火墙不会阻止 Site Recovery Manager 使用的端口。

- Site Recovery Manager 配置文件

  某些 Site Recovery Manager 配置文件包含的设置可能会影响环境安全。错误设置还会影响您 Site Recovery Manager 环境的正常运行。

- Site Recovery Manager 证书和密钥

  Site Recovery Manager 使用 TLS 证书和专用密钥保护网络通信并安全建立针对其他服务器的身份验证。

- Site Recovery Manager 存储的凭据

  Site Recovery Manager 以加密格式将存储复制适配器 (storage replication adapter, SRA) 和数据库的凭据存储在 Windows 注册表中。

- Site Recovery Manager 许可证和 EULA 文件

  Site Recovery Manager 许可证和 EULA 文件位于 Site Recovery Manager Server 主机上。

- Site Recovery Manager 日志文件

  Site Recovery Manager 将操作信息记录到日志文件中。日志文件不包含专用密钥和密码等敏感信息。

- Site Recovery Manager 帐户

  Site Recovery Manager 使用单点登录 (Single Sign-On, SSO) 来访问 vCenter Server 和 Platform Services Controller。

- Site Recovery Manager 安全更新和修补程序

  您可以在 VMware 提供 Site Recovery Manager 安全更新和修补程序时进行应用。您可以在主机操作系统供应商提供主机操作系统安全更新和修补程序时进行应用。

- 确保 Site Recovery Manager Server 安全的最佳做法

  确保 Site Recovery Manager Server 安全的最佳做法可防止您的环境出现潜在安全问题。

Site Recovery Manager 服务

Site Recovery Manager 的操作取决于 Site Recovery Manager Server 主机上运行的几项服务。

表 1-1 Site Recovery Manager 要求的服务

服务名称	启动时间	描述
VMware vCenter Site Recovery Manager Server	自动	提供核心 Site Recovery Manager 功能。
VMware vCenter Site Recovery Manager 嵌入式数据库	自动（如果使用嵌入式数据库）。	Site Recovery Manager 嵌入式数据库的 vPostgres 服务器。
VMware vCenter Site Recovery Manager 客户端	自动	提供 VMware vCenter Site Recovery Manager 客户端（Tomcat，HTML5 用户界面）功能。
服务器	自动	支持通过网络共享文件的 Windows 服务。
工作站	自动	创建并维护到远程服务器连接的 Windows 服务。
受保护的存储	自动	存储敏感数据的 Windows 服务。

Site Recovery Manager 网络端口

Site Recovery Manager 使用可配置的网络端口与客户端及其他服务器进行通信。必须确保防火墙不会阻止 Site Recovery Manager 使用的端口。

Site Recovery Manager Server 接收一个网络端口上的所有入站流量。默认端口为 9086。如果您将 Site Recovery Manager 配置为使用嵌入式数据库，Site Recovery Manager 嵌入式数据库将接收本地环回接口上的 localhost 网络流量。默认端口为 5678。

如果默认端口被阻止或者由其他应用程序所使用，则可以在安装过程中为 Site Recovery Manager 和嵌入式数据库流量选择其他端口。您必须配置网络策略以启用入站端口上的流量。有关安装后可以更改的端口的信息，请参见 *Site Recovery Manager 的安装和配置* 文档中的 *“修改 Site Recovery Manager 服务器安装”* 主题。

Site Recovery Manager Server 与本地站点的 Platform Services Controller、vCenter Server、ESXi 主机以及阵列进行通信。您必须验证网络防火墙策略是否启用到本地站点中所有组件网络端口的流量。有关所有 VMware 产品使用的默认端口列表，请参见 http://kb.vmware.com/kb/1012382。

Site Recovery Manager 对中的本地站点和远程站点之间的连接必须是专用的，例如 VPN。本地 Site Recovery Manager Server 与远程站点上的 Site Recovery Manager Server、Platform Services Controller 和 vCenter Server 进行通信，您的网络提供商必须确保相应的网络策略启用该流量。

有关必须针对 Site Recovery Manager 打开的所有端口列表，请参见 *Site Recovery Manager 的安装和配置* 文档中的 Site Recovery Manager 的网络端口主题。

Site Recovery Manager 配置文件

某些 Site Recovery Manager 配置文件包含的设置可能会影响环境安全。错误设置还会影响您 Site Recovery Manager 环境的正常运行。

表 1-2 Site Recovery Manager 配置文件

文件或目录位置	描述
installation_folder\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml	定义 Site Recovery Manager Server 的系统配置。 **注意** 请勿移动或删除配置文件。 在 Site Recovery Manager 用户界面中，使用“站点对”选项卡上的**高级设置**可以安全地更改 Site Recovery Manager 实例的系统设置。
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\bin\vmw_vpg_config\	包含嵌入式数据库配置文件。 **注意** 请勿修改、移动或删除配置文件。
installation_folder\VMware\VMware vCenter Site Recovery Manager\config\extension.xml	定义 Site Recovery Manager Server 扩展的配置。extension.xml 文件包含默认用户角色及其权限的定义。 **注意** 请勿修改、移动或删除配置文件。
C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\h5dr.properties	定义 Site Recovery Manager HTML 5 用户界面的配置。 **注意** 请勿移动或删除配置文件。 通过将 *phonehomeEnabled* 值从 true 更改为 false（或从 false 更改为 true），可以安全地更改 Site Recovery Manager HTML 5 用户界面的遥测设置。

Site Recovery Manager 证书和密钥

Site Recovery Manager 使用 TLS 证书和专用密钥保护网络通信并安全建立针对其他服务器的身份验证。

CA 证书或专用密钥或两者	位置与描述
Site Recovery Manager Server 端点的 TLS 证书和密钥	在 Windows 证书存储的 Certificates\vmware-dr\Personal\Certificates 文件夹中。 如果在安装过程中未提供自定义证书，Site Recovery Manager 会生成该证书。
Site Recovery Manager 安装过程中创建的 solution 用户的 TLS 证书和密钥	在 Windows 证书存储的 Certificates\vmware-dr\su-*Site Recovery Manager UUID*\Certificates 文件夹中。
远程站点上的 solution 用户的 TLS 证书和密钥	在 Windows 证书存储的 Certificates\vmware-dr\remote-su-*Site Recovery Manager UUID*\Certificates 文件夹中。 Site Recovery Manager 在配对过程中创建这些文件。
Site Recovery Manager 安装过程中创建的 HTML5 UI solution 用户的 TLS 证书和密钥	在 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\h5dr.keystore 文件中。

CA 证书或专用密钥或两者	位置与描述
Tomcat 服务器端点的 TLS 证书和密钥	在 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\conf\h5dr-server.keystore 文件中。 与 Site Recovery Manager Server 端点的 TLS 证书和密钥相同。
Site Recovery Manager Server 的 CA 证书，以及 TLS 证书	*installation_folder*\VMware\VMware vCenter Site Recovery Manager\bin*SRM_Server_IP_addressca*.p7b 文件。 如果在安装过程中未提供自定义证书，Site Recovery Manager 会生成该证书。 您可以将该证书导入客户端信任密钥库以允许用户隐式信任 Site Recovery Manager Server 证书。

注意 请勿提取或共享专用密钥信息以保护您的 Site Recovery Manager 实例。

有关 Site Recovery Manager 身份验证机制的详细信息，请参见《*Site Recovery Manager 的安装和配置指南*》中的 *"Site Recovery Manager 身份验证"* 主题。

Site Recovery Manager 存储的凭据

Site Recovery Manager 以加密格式将存储复制适配器 (storage replication adapter, SRA) 和数据库的凭据存储在 Windows 注册表中。

如果您是管理员组的成员，则具有访问凭据的权限。

注册表路径	描述
HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Vmware DR\Creds\db:*datastore name*	使用 *datastore name* 系统存储来访问 Site Recovery Manager 数据库的凭据。
HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Vmware DR\Creds\storage-arraymanager *manager id*-username	SRA 在连接由 *manager id* 标识的阵列管理器时必须使用的用户名。
HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ Vmware DR\Creds\storage-arraymanager-*manager id*-password	SRA 连接由 *manager id* 标识的阵列管理器时必须使用的密码。

Java 密钥库 h5dr.keystore 的凭据存储在位于 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm client\lib\ 文件夹的 h5dr.properties 文件中。Java 密钥库 h5dr-server.keystore 的凭据存储在位于 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\conf\ 文件夹的 server.xml 文件中。

Site Recovery Manager 许可证和 EULA 文件

Site Recovery Manager 许可证和 EULA 文件位于 Site Recovery Manager Server 主机上。

表 1-3 Site Recovery Manager 许可证和 EULA 文件

文件或目录	描述
installation_folder\VMware\VMware vCenter Site Recovery Manager\en\	包含 Site Recovery Manager 最终用户许可协议文件的目录。
installation_folder\VMware\VMware vCenter Site Recovery Manager\en\open_source_license.txt	Site Recovery Manager 开源许可证文件。
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\EULA-en.rtf	Site Recovery Manager 嵌入式数据库最终用户许可协议文件。
installation_folder\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\open_source_license.txt	Site Recovery Manager 嵌入式数据库开源许可证文件。

Site Recovery Manager 日志文件

Site Recovery Manager 将操作信息记录到日志文件中。日志文件不包含专用密钥和密码等敏感信息。

Site Recovery Manager Server 日志

Site Recovery Manager 将系统日志文件存储在 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs 目录中。来自 Site Recovery Manager Server 的最新消息放在 vmware-dr-*number*.log 文件中。

如果重新启动 Site Recovery Manager Server 或当前文件将超过设置的文件大小限制，则 Site Recovery Manager 将存档当前日志文件并创建新的日志文件。

要更改日志文件目录，请在 *installation_directory*\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml 配置文件中的目录 XML 元素中输入自定义目录名称。还可以通过更新 vmware-dr.xml 文件中的 logLevel XML 元素来更改每个组件的日志级别。所有组件的默认级别均为“详细”。

重要事项 配置访问控制列表以限制对日志文件的访问。

表 1-4 日志级别

级别	描述
错误	仅显示错误日志条目。
信息	显示信息、错误和警告日志条目。
琐事	显示信息、错误、警告、详细和琐事日志条目。
详细	显示信息、错误、警告和详细日志条目。
警告	显示警告和错误日志条目。

Site Recovery Manager 支持诸如以下组件：

- 默认
- 复制

- 恢复
- 存储
- StorageProvider
- Vdb
- 持久性

vmware-dr-*number*.log 文件不包含有关身份验证进程以及远程端连接的安全消息。

Site Recovery 用户界面日志

Site Recovery Manager 将 Site Recovery 用户界面日志文件存储在 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-clients\logs 目录中。最新的消息位于 dr.log 文件中。

可以通过在 C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm client\webapps\dr\WEB INF\classes 目录下的 log4j.xml 文件中更新级别值元素来修改每个组件的日志级别。所有组件的默认级别均为“信息”。

表 1-5 日志级别

级别	描述
错误	仅显示错误日志条目。
警告	显示警告和错误日志条目。
信息	显示信息、错误和警告日志条目。
调试	显示调试、信息、错误和警告日志条目。
跟踪	显示最详细的信息。

Site Recovery 用户界面使用的 Tomcat 服务器支持以下组件等：

- Http 异步 I/O
- 每个处理程序调用时间
- VC L10N 目录
- SRM
- VR
- 公用

Site Recovery Manager 帐户

Site Recovery Manager 使用单点登录 (Single Sign-On, SSO) 来访问 vCenter Server 和 Platform Services Controller。

用户帐户

在默认配置中，vCenter Server 管理员具有对 Site Recovery Manager 的管理访问权限。安装后首次尝试登录到 Site Recovery Manager 时，必须使用管理员凭据。

如果您拥有管理员凭据，您可以通过使用 vSphere Web Client 授予其他用户对 Site Recovery Manager 的访问权限。

有关 Site Recovery Manager 角色、特权和权限的详细信息，请参见《*Site Recovery Manager 管理*》文档中的 *"Site Recovery Manager 特权、角色和权限"*。

Solution 用户帐户

Site Recovery Manager 会在安装期间创建一个 `solution` 用户，并使用该用户进行 vCenter Server 身份验证。每个 Site Recovery Manager 实例的 `solution` 用户是唯一的，供 Site Recovery Manager、vCenter Server 和 Platform Services Controller 内部使用。

对不使用增强型链接模式的站点进行配对的过程中，Site Recovery Manager 将在每个远程站点上创建另一个 `solution` 用户。Site Recovery Manager 使用 `solution` 用户在远程站点上执行必要操作。

Site Recovery Manager 会在安装期间针对 HTML5 用户界面创建一个 `solution` 用户，HTML5 UI 将使用该用户进行 vCenter Server 身份验证。每个 Site Recovery Manager 实例的 solution 用户是唯一的，供 Site Recovery Manager HTML5 UI 客户端、vCenter Server 和 Platform Services Controller 内部使用。

注意 不得删除和修改与 `solution` 用户帐户关联的角色和特权。

有关 `solution` 用户以及本地站点和远程站点之间的身份验证的详细信息，请参见《*Site Recovery Manager 的安装和配置*》文档中的 *"Site Recovery Manager 身份验证"* 主题。

Site Recovery Manager 安全更新和修补程序

您可以在 VMware 提供 Site Recovery Manager 安全更新和修补程序时进行应用。您可以在主机操作系统供应商提供主机操作系统安全更新和修补程序时进行应用。

Site Recovery Manager 主机操作系统版本

有关 Site Recovery Manager Server 支持的主机操作系统的信息，请参见 https://docs.vmware.com/cn/Site-Recovery-Manager/8.1/rn/srm-compat-matrix-8-1.html 上的 *Site Recovery Manager 8.1 兼容性列表*。

应用 Site Recovery Manager 修补程序和安全更新

您可通过对现有 Site Recovery Manager 安装执行对位升级来应用 Site Recovery Manager 安全修补程序和更新。有关升级 Site Recovery Manager 的信息，请参见 *Site Recovery Manager 的安装和配置*中的 *"Site Recovery Manager Server 的对位升级"* 主题。

确保 Site Recovery Manager Server 安全的最佳做法

确保 Site Recovery Manager Server 安全的最佳做法可防止您的环境出现潜在安全问题。

Site Recovery Manager 的安全操作依赖于 Site Recovery Manager Server 操作系统的正确配置和维护。

- 仅在受支持的主机操作系统、数据库和硬件上运行 Site Recovery Manager。如果 Site Recovery Manager 未在受支持的主机操作系统上运行，Site Recovery Manager 可能无法正常运行。
- 应用最新的操作系统更新和修补程序以保护主机操作系统免受恶意攻击。应用最新的 Site Recovery Manager 更新和修补程序以处理 Site Recovery Manager 的任何已知问题。
- 作为虚拟机运行 Site Recovery Manager 时，确保 Site Recovery Manager 部署的完整性。请参见 *《vSphere 安全性》*文档中的 *“虚拟机安全性最佳做法”*主题。
- 对于 Site Recovery Manager 不使用的软件和服务，限制软件安装并禁用此类服务，以便释放资源并降低遭受服务器攻击的可能性。不需要的软件和服务会消耗 CPU、存储、内存和带宽资源，并增加遭受服务器攻击的可能性。
- 仅允许管理员访问服务器。为了限制攻击者可使用的帐户数目，限制可访问服务器的帐户数目。
- 检查 Site Recovery Manager 使用的网络端口，配置防火墙以保护您的服务器。