Site Recovery Manager Security

Site Recovery Manager 8.4

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

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

Contents

About VMware Site Recovery Manager Security

Site Recovery Manager Security provides a concise reference to the security features of Site Recovery Manager.

To help you protect your Site Recovery Manager installation, this guide describes security features built into Site Recovery Manager and the measures that you can take to safeguard it from attack.

- External interfaces, ports, and services that are necessary for the proper operation of Site Recovery Manager
- Configuration options and settings that have security implications
- Location of log files and their purpose
- Required system accounts
- Information on obtaining the latest security patches

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of Site Recovery Manager.

Site Recovery Manager Security Reference

1

Use the Security Reference to learn about the security features of your Site Recovery Manager installation and the measures that you can take to safeguard your environment from attack.

- Site Recovery Manager Services

  The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

- Site Recovery Manager Network Ports

  Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

- Site Recovery Manager Configuration Files

  Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

- Site Recovery Manager Certificates and Keys

  Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

- Site Recovery Manager Stored Credentials

  Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in encrypted format.

- Site Recovery Manager License and EULA Files

  The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

- Site Recovery Manager Log Files

  Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

- Site Recovery Manager Accounts

  Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

- Site Recovery Manager Security Updates and Patches

  You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

- Best Practices for Securing Site Recovery Manager Server

  Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Site Recovery Manager Services

The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Table 1-1. Services that Site Recovery Manager Requires

Service Name	Startup Time	Description
srm-server	Automatic	Provides the core Site Recovery Manager functions.
srm-postgress	Automatic	The vPostgres server for the Site Recovery Manager embedded database.
dr-client	Automatic	Provides VMware vCenter Site Recovery Manager Client (Tomcat, HTML5 user interface) functionality.

Site Recovery Manager Network Ports

Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

All Site Recovery Manager Virtual Appliance services run behind a reverse HTTP proxy on port 443. The Site Recovery Manager Appliance Management Interface requires port 5480.

Site Recovery Manager Server communicates with Platform Services Controller, vCenter Server, ESXi hosts, and Arrays at the local site. You must verify that the network firewall policies enable the traffic to network ports of all components at the local site. For the list of the default ports that all VMware products use, see http://kb.vmware.com/kb/1012382.

The connection between the local and the remote site of a Site Recovery Manager pair must be private such as VPN. The local Site Recovery Manager Server communicates with Site Recovery Manager Server, Platform Services Controller, and vCenter Server on the remote site, and your network provider must ensure the appropriate network policies to enable the traffic.

For a list of all the ports that must be open for Site Recovery Manager, see the Network Ports for Site Recovery Manager topic in the *Site Recovery Manager Installation and Configuration* documentation.

Site Recovery Manager Configuration Files

Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Virtual Appliance Configuration Files

Note Do not move, or delete the configuration files.

File or Directory Location	Description
`/opt/vmware/srm/conf/vmware-dr.xml`	Defines system configuration of Site Recovery Manager Server. You can safely change the system settings of a Site Recovery Manager instance by using the **Advanced Settings** on the Site Pair tab in the Site Recovery Manager user interface.
`/opt/vmware/srm/conf/drconfig.xml`	Defines configuration of the `dr-configurator` service.
`/opt/vmware/dr-client/lib/h5dr.properties`	Defines configuration of the Site Recovery Manager HTML 5 user interface. You can safely change the telemetry settings of the Site Recovery Manager HTML 5 user interface by changing the *phonehomeEnabled* value from true to false and the reverse. You can change the session timeout setting of the Site Recovery Manager HTML 5 user interface by changing the *sessionTimeout* value in seconds. By default, the session timeout is set to 7200 seconds. Changing the values in the `h5dr.properties` file requires restart of the `dr-client` service.
`/opt/vmware/srm/conf/extension.xml`	Defines configuration of Site Recovery Manager Server Extension. The `extension.xml` file contains definitions of default user roles and their privileges. **Note** Do not modify the `extension.xml` file.
`/var/lib/srmdb`	Contains the embedded database configuration files. **Note** Do not modify the configuration files.

Site Recovery Manager Certificates and Keys

Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Virtual Appliance Certificates and Keys

All Site Recovery Manager Virtual Appliance services run behind a reverse HTTP proxy and do not use SSL for the communication path to the proxy. There is only one certificate for the proxy service. The certificate files are stored in `/opt/vmware/srm/conf/keys/vmware-dr/My/`.

CA certificate or private key or both	Location
TLS certificate and key for **solution** user created during the Site Recovery Manager Appliance deployment	In the `/opt/vmware/srm/conf/keys/vmware-dr/su-`*`Site Recovery Manager UUID`* folder.
TLS certificate and key for **solution** user on the remote site	In the `/opt/vmware/srm/conf/keys/vmware-dr/remote-su-`*`Site Recovery Manager UUID`* folder.
TLS certificate and key for the HTML5 user interface **solution** user created during the Site Recovery Manager Appliance deployment	In the `/opt/vmware/dr-client/lib/h5dr.keystore` file.

For more information about the Site Recovery Manager authentication mechanisms, see the *Site Recovery Manager Authentication* topic in the *Site Recovery Manager Installation and Configuration Guide*.

Site Recovery Manager Stored Credentials

Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in encrypted format.

Site Recovery Manager Virtual Appliance Credentials

File Path	Description
`/opt/vmware/srm/conf/db:`*`datastore name`*	Credentials to access Site Recovery Manager Virtual Appliance database using *datastore name* System Datastore.
`/opt/vmware/srm/conf/prefix-keyname-username`	User name that must be used by the SRA when connecting to the array manager identified by manager id.
`/opt/vmware/srm/conf/prefix-keyname-password`	Password that must be used by the SRA when connecting to the array manager identified by *manager id*.

The credentials for the java keystore `h5dr.keystore` are stored in the `h5dr.properties` file located in the `/opt/vmware/dr-client/lib/` folder.

Site Recovery Manager License and EULA Files

The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Table 1-2. Site Recovery Manager Virtual Appliance License and EULA Files

File or Directory	Description
`/opt/vmware/etc/isv/EULA`	Directory containing the Site Recovery Manager End-user license agreement files.
`/opt/vmware/srm/open_source_license.txt`	Site Recovery Manager Open Source License file.

Site Recovery Manager Log Files

Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Virtual Appliance Server Logs

The Site Recovery Manager Virtual Appliance stores the system log files in the `/var/log/vmware/srm` directory. The latest messages from Site Recovery Manager Server are placed in the `vmware-dr-`*`number`*`.log` file.

The support bundle is located in the `/var/log/vmware/srm/Support` folder.

Log Levels for Server Logs

Level	Description
error	Displays only error log entries.
info	Displays information, error, and warning log entries.
trivia	Displays information, error, warning, verbose, and trivia log entries.
verbose	Displays information, error, warning, and verbose log entries.
warning	Displays warning and error log entries.

Site Recovery Manager supports components such as:

- Default
- Replication
- Recovery
- Storage
- StorageProvider
- Vdb
- Persistence

The `vmware-dr-number.log` file does not contain security messages concerning the authentication process and connections with the remote side.

Site Recovery Manager Virtual Appliance User Interface Logs

The Site Recovery Manager Virtual Appliance stores the Site Recovery user interface log files in the `/var/log/vmware/dr-client/` folder. The latest messages are placed in the `dr.log` file.

You can modify the log level of each component by updating the level value element in the `log4j2.xml` file in the `/opt/vmware/dr-client/webapps/dr/WEB-INF/classes` directory. The default level of all components is info.

The Site Recovery Manager Virtual Appliance Management Interface logs are located in the `/var/log/vmware/drconfigui/` folder. The latest messages are placed in the `drconfigui.log` file.

You can modify the log level of each component by updating the level value element in the `log4j2.xml` file in the `/opt/vmware/drconfigui/webapps/configure/WEB-INF/classes/` folder. The default level of all components is info.

Log Levels for User Interface Logs

Level	Description
error	Displays only error log entries.
warn	Displays warning and error log entries.
info	Displays information, error, and warning log entries.
debug	Displays debug, information, error, and warning log entries.
trace	Displays the most detailed information.

The tomcat server used by the Site Recovery user interface supports components such as:

- Http Async I/O
- Per handler call time
- VC L10N catalogs
- SRM
- VR
- Common

Site Recovery Manager Accounts

Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

User Accounts

The vCenter Server administrators have administration access to Site Recovery Manager in the default configuration. You must use administrator credentials when you try to log in to Site Recovery Manager for the first time after the installation.

If you have administrator credentials, you can grant access to Site Recovery Manager to other users by using the vSphere Web Client.

For more information about Site Recovery Manager roles, privileges, and permissions, see the *Site Recovery Manager Privileges, Roles, and Permissions* in the *Site Recovery Manager Administration* documentation.

Solution User Account

Site Recovery Manager creates a `solution` user during the installation and uses it during the authentication with vCenter Server . The `solution` user is unique for each Site Recovery Manager instance and is for internal use by Site Recovery Manager, vCenter Server, and Platform Services Controller.

Site Recovery Manager creates an additional `solution` user on each remote site during the pairing process of sites that do not use Enhanced Linked Mode. Site Recovery Manager uses the `solution` user to perform necessary operations on the remote site.

Site Recovery Manager creates a `solution` user for the HTML5 user interface during the installation and uses it by the HTML5 UI during the authentication with vCenter Server. The solution user is unique for each Site Recovery Manager instance and is for internal use by Site Recovery Manager HTML5 UI client, vCenter Server, and Platform Services Controller.

Note You must not delete and modify the roles and privileges associated with the `solution` user accounts.

For more information about the `solution` users and authentication between the local and remote site, see the *Site Recovery Manager Authentication* topic in the *Site Recovery Manager Installation and Configuration* documentation.

Site Recovery Manager Security Updates and Patches

You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Applying Site Recovery Manager Patches and Security Updates to the Site Recovery Manager Virtual Appliance

You apply Site Recovery Manager security patches and updates by performing an update of your existing Site Recovery Manager Virtual Appliance installation. For information about updating the Site Recovery Manager Virtual Appliance, see the *Update the Site Recovery Manager Virtual Appliance* topic in *Site Recovery Manager Installation and Configuration*.

Best Practices for Securing Site Recovery Manager Server

Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

The secure operation of Site Recovery Manager depends on the proper configuration and maintenance of the Site Recovery Manager Server.

- Apply the latest Site Recovery Manager updates and patches to address any known issues with Site Recovery Manager.
- Ensure the integrity of your Site Recovery Manager deployment when you run Site Recovery Manager as a VM. See the *Virtual Machine Security Best Practices* topic in the *vSphere Security* documentation.
- Allow only administrators to access the server. To limit the number of accounts that an attacker can use, limit the number of accounts that can access the server.
- Check the network ports that Site Recovery Manager uses and configure a firewall to protect your server.