Site Recovery Manager Installation and Configuration

Site Recovery Manager 5.8

vmware®

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

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

About VMware vCenter Site Recovery Manager Installation and Configuration

Site Recovery Manager Installation and Configuration provides information about how to install, upgrade, and configure VMware vCenter Site Recovery Manager.

This information also provides a general overview of Site Recovery Manager.

For information about how to perform day-to-day administration of Site Recovery Manager, see *Site Recovery Manager Administration*.

Intended Audience

This information is intended for anyone who wants to install, upgrade, or configure Site Recovery Manager. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Updated Information

Site Recovery Manager Installation and Configuration is updated with each release of the product or when necessary.

This table provides the update history of *Site Recovery Manager Installation and Configuration*.

Revision	Description
EN-001399-08	Updated the information about the embedded vPostgreSQL database in Chapter 3 Creating the Site Recovery Manager Database.
EN-001399-07	Updated Requirements When Using Trusted SSL Certificates with Site Recovery Manager with new requirements for public authority certificates with internal server names.
EN-001399-06	■ Added that you install patches by following the procedure for in-place upgrade in In-Place Upgrade of Site Recovery Manager Server and Upgrade Site Recovery Manager Server with Migration. ■ Added that you cannot map individual hosts from clusters to other objects in Select Inventory Mappings.
EN-001399-05	■ Added Uninstall and Reinstall the Same Version of Site Recovery Manager. ■ Added that advanced settings are not retained during upgrade in Information That Site Recovery Manager Upgrade Preserves. ■ Expanded the upgrade prerequisites in Prepare for Site Recovery Manager Upgrade. ■ Added that only in-place upgrade is possible to upgrade to an update release in In-Place Upgrade of Site Recovery Manager Server and Upgrade Site Recovery Manager Server with Migration. ■ Added instruction to check build numbers after upgrade in In-Place Upgrade of Site Recovery Manager Server. ■ Clarified that SRA credentials must be reentered in all cases in Configure and Verify the Upgraded Site Recovery Manager Installation. ■ Corrected the path to SRA downloads on myvmware.com and clarified that you can download certified SRAs from third party sites in Configure and Verify the Upgraded Site Recovery Manager Installation. ■ Added additional setting to configure for large shared recovery site setups in Timeout Errors when Powering on Virtual Machines on a Shared Recovery Site.

Revision	Description
EN-001399-04	■ Expanded Chapter 8 Installing Site Recovery Manager to Use with a Shared Recovery Site to state that converting a one-to-one configuration into a shared recovery site configuration is possible. Removed the statement from Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration that stated that such a conversion is not possible. ■ Added that shared protected site and multiple-to-multiple site configurations are supported in Chapter 8 Installing Site Recovery Manager to Use with a Shared Recovery Site. Removed the recommendation against implementing shared protected site configurations from Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration. ■ Added that Site Recovery Manager does not support replication to multiple targets in Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration. ■ Added information about what happens to the Site Recovery Manager extension ID during upgrade in a shared recovery site configuration in Upgrade Site Recovery Manager in a Shared Recovery Site Configuration.
EN-001399-03	Added note about installations with custom permissions requiring upgrade with migration in In-Place Upgrade of Site Recovery Manager Server.
EN-001399-02	■ Added topic Back Up and Restore the Embedded vPostgres Database. ■ Added that you might need to clear the browser cache after upgrade in In-Place Upgrade of Site Recovery Manager Server and Upgrade Site Recovery Manager Server with Migration.
EN-001399-01	■ Clarified that the vSphere Client for Windows is not supported in Chapter 5 Installing Site Recovery Manager, Chapter 6 Upgrading Site Recovery Manager, and Prepare for Site Recovery Manager Upgrade. ■ Corrected information about Subject Name requirements in Requirements When Using Trusted SSL Certificates with Site Recovery Manager. ■ Clarified that you must upgrade all components of vCenter Server before upgrading Site Recovery Manager in Prepare for Site Recovery Manager Upgrade.
EN-001399-00	Initial release.

Overview of VMware vCenter Site Recovery Manager

1

VMware vCenter Site Recovery Manager is a business continuity and disaster recovery solution that helps you to plan, test, and run the recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site.

You can configure Site Recovery Manager to work with several third-party disk replication mechanisms by configuring array-based replication. Array-based replication surfaces replicated datastores to recover virtual machine workloads. You can also use host-based replication by configuring Site Recovery Manager to use VMware vSphere Replication to protect virtual machine workloads.

You can use Site Recovery Manager to implement different types of recovery from the protected site to the recovery site.

Planned Migration	The orderly evacuation of virtual machines from the protected site to the recovery site. Planned migration prevents data loss when migrating workloads in an orderly fashion. For planned migration to succeed, both sites must be running and fully functioning.
Disaster Recovery	Similar to planned migration except that disaster recovery does not require that both sites be up and running, for example if the protected site goes offline unexpectedly. During a disaster recovery operation, failure of operations on the protected site are reported but otherwise ignored.

Site Recovery Manager orchestrates the recovery process with the replication mechanisms, to minimize data loss and system down time.

- At the protected site, Site Recovery Manager shuts down virtual machines cleanly and synchronizes storage, if the protected site is still running.
- Site Recovery Manager powers on the replicated virtual machines at the recovery site according to a recovery plan.

A recovery plan specifies the order in which virtual machines start up on the recovery site. A recovery plan specifies network parameters, such as IP addresses, and can contain user-specified scripts that Site Recovery Manager can run to perform custom recovery actions on virtual machines.

Site Recovery Manager lets you test recovery plans. You conduct tests by using a temporary copy of the replicated data in a way that does not disrupt ongoing operations at either site.

- About Protected Sites and Recovery Sites

  In a typical Site Recovery Manager installation, the protected site provides business-critical datacenter services. The recovery site is an alternative infrastructure to which Site Recovery Manager can migrate these services.

- Bidirectional Protection

  You can use a single set of paired Site Recovery Manager sites to protect virtual machines in both directions. Each site can simultaneously be a protected site and a recovery site, but for a different set of virtual machines.

- Heterogeneous Configurations on the Protected and Recovery Sites

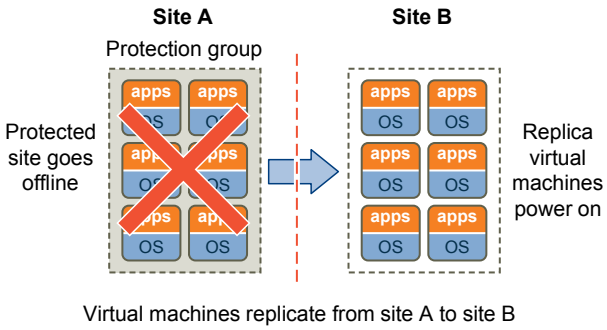
  Some components in the Site Recovery Manager and vCenter Server installations must be identical on each site. Because the protected and recovery sites are often in different physical locations, some components on the protected site can be of a different type to their counterparts on the recovery site.

About Protected Sites and Recovery Sites

In a typical Site Recovery Manager installation, the protected site provides business-critical datacenter services. The recovery site is an alternative infrastructure to which Site Recovery Manager can migrate these services.

The protected site can be any site where vCenter Server supports a critical business need. The recovery site can be located thousands of miles away from the protected site. Conversely, the recovery site can be in the same room as a way of establishing redundancy. The recovery site is usually located in a facility that is unlikely to be affected by environmental, infrastructure, or other disturbances that affect the protected site. You can establish bidirectional protection in which each site serves as the recovery site for the other. See Bidirectional Protection.

Figure 1-1. Site Recovery Manager Protected and Recovery Sites



The vSphere configurations at each site must meet requirements for Site Recovery Manager.

- You must run the same version of Site Recovery Manager on both sites.
- You must run the same version of vCenter Server on both sites.

- The version of vCenter Server must be compatible with the version of Site Recovery Manager. For information about compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.
- Each site must have at least one datacenter.
- If you are using array-based replication, the same replication technology must be available at both sites, and the arrays must be paired.
- If you are using vSphere Replication, you require a vSphere Replication appliance on both sites. The vSphere Replication appliances must be connected to each other.
- The vSphere Replication appliances must be of the same version.
- The vSphere Replication version must be compatible with the version of Site Recovery Manager. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.
- The recovery site must have hardware, network, and storage resources that can support the same virtual machines and workloads as the protected site. You can oversubscribe the recovery site by running additional virtual machines there that are not protected. In this case, during a recovery you must suspend noncritical virtual machines on the recovery site.
- The sites must be connected by a reliable IP network. If you are using array-based replication, ensure that your network connectivity meets the arrays' network requirements.
- The recovery site should have access to comparable public and private networks as the protected site, although not necessarily the same range of network addresses.

Bidirectional Protection

You can use a single set of paired Site Recovery Manager sites to protect virtual machines in both directions. Each site can simultaneously be a protected site and a recovery site, but for a different set of virtual machines.

You can implement bidirectional protection by using either array-based replication or vSphere Replication. If you are using array-based replication, each of the array’s LUNs replicates in only one direction. Two LUNs in paired arrays can replicate in different directions from each other.

Heterogeneous Configurations on the Protected and Recovery Sites

Some components in the Site Recovery Manager and vCenter Server installations must be identical on each site. Because the protected and recovery sites are often in different physical locations, some components on the protected site can be of a different type to their counterparts on the recovery site.

Although components can be different on each site, you must use the types and versions of these components that Site Recovery Manager supports. See the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html for information.

Table 1-1. Heterogeneity of Site Recovery Manager Components Between Sites

Component	Heterogeneous or Identical Installations
Site Recovery Manager Server	Must be the same version on both sites.
vCenter Server	Must be the same version on both sites. The Site Recovery Manager version must be compatible with the vCenter Server version.
vSphere Replication	Must be the same version on both sites. The vSphere Replication version must be compatible with the Site Recovery Manager version and the vCenter Server version.
Authentication method	Must be the same on both sites. If you use autogenerated certificates to authenticate between the Site Recovery Manager Server instances on each site, you must use autogenerated certificates on both sites. If you use custom certificates that are signed by a certificate authentication service, you must use such certificates on both sites. Similarly, the authentication method that you use between Site Recovery Manager Server and vCenter Server must be the same on both sites. If you use different authentication methods on each site, site pairing fails.
vCenter Server Appliance or standard vCenter Server instance	Can be different on each site. You can run a vCenter Server Appliance on one site and a standard vCenter Server instance on the other site.
Storage arrays for array-based replication	Can be different versions on each site. You can use different versions of the same type of storage array on each site. The Site Recovery Manager Server instance on each site requires the appropriate storage replication adapter (SRA) for each version of storage array for that site. Check SRA compatibility with all versions of your storage arrays to ensure compatibility.
Site Recovery Manager database	Can be different on each site. You can use different versions of the same type of database on each site, or different types of database on each site.
Host operating system of the Site Recovery Manager Server installation	Can be different on each site. You can run different versions of the host operating system and the host operating system can run in different locales on each site.
Host operating system of the vCenter Server installation	Can be different on each site. You can run different versions of the host operating system and the host operating system can run in different locales on each site.

Example: Heterogenous Configurations on the Protected and Recovery Sites

The Site Recovery Manager and vCenter Server installations might be in different countries, with different setups.

- Site A in Japan:
  - Site Recovery Manager Server runs on Windows Server 2008 in the Japanese locale
  - Site Recovery Manager extends a vCenter Server Appliance instance
  - Site Recovery Manager Server uses the embedded Site Recovery Manager database
- Site B in the United States:
  - Site Recovery Manager Server runs on Windows Server 2012 in the English locale
  - Site Recovery Manager extends a standard vCenter Server instance that runs on Windows Server 2008 in the English locale
  - Site Recovery Manager Server uses an Oracle Server database

Site Recovery Manager System Requirements

2

The system on which you install vCenter Site Recovery Manager must meet specific hardware requirements.

Table 2-1. Site Recovery Manager System Requirements

Component	Requirement
Processor	2.0GHz or higher Intel or AMD x86 processor
Memory	2GB minimum. You might require more memory if you use the embedded database, as the content of the database grows.
Disk Storage	5GB minimum. If you install Site Recovery Manager on a different drive to the C: drive, the Site Recovery Manager installer still requires at least 1GB of free space on the C: drive. This space is required for extracting and caching the installation package. You might require more disk storage if you use the embedded database, as the content of the database grows.
Networking	1 Gigabit recommended for communication between Site Recovery Manager sites. Use a trusted network for the management of ESXi hosts.

For information about supported platforms and databases, see the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.

- Site Recovery Manager Licensing

  After you install Site Recovery Manager, it remains in evaluation mode until you install a Site Recovery Manager license key.

- Site Recovery Manager Network Ports

  Site Recovery Manager Server instances use several network ports to communicate with each other, with client plug-ins, and with vCenter Server. If any of these ports are in use by other applications or are blocked on your network, you must reconfigure Site Recovery Manager to use different ports.

- Operational Limits of Site Recovery Manager

  Each Site Recovery Manager server can support a certain number of protected virtual machines, protection groups, datastore groups, recovery plans, and concurrent recoveries.

Site Recovery Manager Licensing

After you install Site Recovery Manager, it remains in evaluation mode until you install a Site Recovery Manager license key.

After the evaluation license expires, existing protection groups remain protected and you can recover them, but you cannot create new protection groups or add virtual machines to an existing protection group until you obtain and assign a valid Site Recovery Manager license key. Obtain and assign Site Recovery Manager license keys as soon as possible after installing Site Recovery Manager.

Site Recovery Manager licenses allow you to protect a set number of virtual machines. To obtain Site Recovery Manager license keys, go to the Site Recovery Manager Product Licensing Center at http://www.vmware.com/products/site-recovery-manager/buy.html, or contact your VMware sales representative.

Site Recovery Manager License Keys and vCenter Server Instances in Linked Mode

If your vCenter Server instances are connected with vCenter Server instances in linked mode, you install the same Site Recovery Manager license on both vCenter Server instances.

Site Recovery Manager License Keys and Protected and Recovery Sites

Site Recovery Manager requires a license key on any site on which you protect virtual machines.

- Install a Site Recovery Manager license key at the protected site to enable protection in one direction from the protected site to the recovery site.
- Install the same Site Recovery Manager license keys at both sites to enable bidirectional protection, including reprotect.

Site Recovery Manager checks for a valid license whenever you add a virtual machine to or remove a virtual machine from a protection group. If licenses are not in compliance, vSphere triggers a licensing alarm and Site Recovery Manager prevents you from protecting further virtual machines. Configure alerts for triggered licensing events so that licensing administrators receive a notification by email.

Site Recovery Manager and vCloud Suite Licensing

You can license Site Recovery Manager 5.8 individually or as part of vCloud Suite 5.8. You should consider the licensing and integration options that are available to you.

When products are part of vCloud Suite, they are licensed on a per-CPU basis. You can run unlimited number of virtual machines on CPUs that are licensed with vCloud Suite.

You can combine the features of Site Recovery Manager 5.8 with other components of vCloud Suite to leverage the full capabilities of the software-defined data center. For more information, see *vCloud Suite Architecture Overview and Use Cases*.

Not all features and capabilities of vSphere are available in all editions. For a comparison of feature sets in each edition, see http://www.vmware.com/products/vsphere/.

Example: Site Recovery Manager Licenses Required for Recovery and Reprotect

You have a site that contains 25 virtual machines for Site Recovery Manager to protect.

- For recovery, you require a license for at least 25 virtual machines, that you install on the protected site to allow one-way protection from the protected site to the recovery site.
- For reprotect, you require a license for at least 25 virtual machines, that you install on both the protected and the recovery site to allow bidirectional protection between the sites.

Site Recovery Manager Network Ports

Site Recovery Manager Server instances use several network ports to communicate with each other, with client plug-ins, and with vCenter Server. If any of these ports are in use by other applications or are blocked on your network, you must reconfigure Site Recovery Manager to use different ports.

Site Recovery Manager uses default network ports for intrasite communication between hosts at a single site and intersite communication between hosts at the protected and recovery sites. You can change these defaults when you install Site Recovery Manager. Beyond these standard ports, you must also meet network requirements of your particular array-based replication provider.

You can change the network ports from the defaults when you first install Site Recovery Manager. You cannot change the network ports after you have installed Site Recovery Manager.

For a list of all the ports that must be open for Site Recovery Manager, see http://kb.vmware.com/kb/2081159.

For the list of default ports that all VMware products use, see http://kb.vmware.com/kb/1012382.

Operational Limits of Site Recovery Manager

Each Site Recovery Manager server can support a certain number of protected virtual machines, protection groups, datastore groups, recovery plans, and concurrent recoveries.

For details about the operational limits of Site Recovery Manager 5.8 see http://kb.vmware.com/kb/2081158.

Creating the Site Recovery Manager Database

3

The Site Recovery Manager Server requires its own database, which it uses to store data such as recovery plans and inventory information.

Site Recovery Manager provides an embedded vPostgreSQL database that requires fewer steps to configure than an external database. The embedded vPostgreSQL database can support a full-scale Site Recovery Manager environment. You can select the option to use the embedded database when you install Site Recovery Manager. The Site Recovery Manager installer creates the embedded database and a database user account according to the information that you specify during installation.

You can also use an external database. If you use an external database, you must create the database and establish a database connection before you can install Site Recovery Manager.

Site Recovery Manager cannot use the vCenter Server database because it has different database schema requirements. You can use the vCenter Server database server to create and support the Site Recovery Manager database.

Each Site Recovery Manager site requires its own instance of the Site Recovery Manager database. Use a different database server instance to run the individual Site Recovery Manager databases for each site. If you use the same database server instance to run the databases for both sites, and if the database server experiences a problem, neither Site Recovery Manager site will work and you will not be able to perform a recovery.

Site Recovery Manager does not require the databases on each site to be identical. You can run different versions of a supported database from the same vendor on each site, or you can run databases from different vendors on each site. For example, you can run different versions of Oracle Server on each site, or you can have an Oracle Server database on one site and the embedded database on the other.

If you are updating Site Recovery Manager to a new version, you can use the existing database. Before you attempt an upgrade, make sure that both Site Recovery Manager Server databases are backed up. Doing so helps ensure that you can revert back to the previous version after the upgrade, if necessary.

For the list of database software that Site Recovery Manager supports, see the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.

- Requirements when Using Microsoft SQL Server with Site Recovery Manager

  When you create a Microsoft SQL Server database, you must configure it correctly to support Site Recovery Manager.

- Requirements for Using Oracle Server with Site Recovery Manager

  When you create a Oracle Server database, you must configure it correctly to support Site Recovery Manager.

- Back Up and Restore the Embedded vPostgres Database

  If you select the option to use an embedded database for Site Recovery Manager, the Site Recovery Manager installer creates a vPostgres database during the installation process. You can back up and restore the embedded vPostgres database by using PostgreSQL commands.

- Create an ODBC System DSN for Site Recovery Manager

  You must provide Site Recovery Manager with a system database source name (DSN) for a 64-bit open database connectivity (ODBC) connector. The ODBC connector allows Site Recovery Manager to connect to the Site Recovery Manager database.

Requirements when Using Microsoft SQL Server with Site Recovery Manager

When you create a Microsoft SQL Server database, you must configure it correctly to support Site Recovery Manager.

This information provides the requirements for an SQL Server database for use with Site Recovery Manager. For specific instructions about creating an SQL Server database, see the SQL Server documentation.

- Database user account:
  - If you use Integrated Windows Authentication to connect to SQL Server and SQL Server runs on the same machine as Site Recovery Manager Server, use a local or domain account that has administrative privileges on the Site Recovery Manager Server machine. Use the same account or an account with the same privileges when you install Site Recovery Manager Server. When the Site Recovery Manager installer detects an SQL Server data source name (DSN) that uses Integrated Windows Authentication, it configures Site Recovery Manager Server to run under the same account as you use for the installer, to guarantee that Site Recovery Manager can connect to the database.
  - If you use Integrated Windows Authentication to connect to SQL Server and SQL Server runs on a different machine from Site Recovery Manager Server, use a domain account with administrative privileges on the Site Recovery Manager Server machine. Use the same account or an account with the same privileges when you install Site Recovery Manager Server. When the Site Recovery Manager installer detects an SQL Server data source name (DSN) that uses Integrated Windows Authentication, it configures Site Recovery Manager Server to run under the same account as you use for the installer, to guarantee that Site Recovery Manager can connect to the database.
  - If you use SQL authentication, you can run the Site Recovery Manager service under the Windows Local System account, even if SQL Server is running on a different machine to Site Recovery Manager Server. The Site Recovery Manager installer configures the Site Recovery Manager service to run under the Windows Local System account by default.

    - Make sure that the Site Recovery Manager database user account has the **ADMINISTER BULK OPERATIONS**, **CONNECT**, and **CREATE TABLE** permissions.
- Database schema:
    - The Site Recovery Manager database schema must have the same name as the database user account.
    - The Site Recovery Manager database user must be the owner of the Site Recovery Manager database schema.
    - The Site Recovery Manager database schema must be the default schema for the Site Recovery Manager database user.
- The Site Recovery Manager database must be the default database for all SQL connections that Site Recovery Manager makes. You can set the default database either in the user account configuration in SQL Server or in the DSN.
- Map the database user account to the database login.

For information about database sizing, see the *Sizing calculator for vCenter Site Recovery Manager databases - MSSQL* at http://www.vmware.com/products/site-recovery-manager/resource.html.

Requirements for Using Oracle Server with Site Recovery Manager

When you create a Oracle Server database, you must configure it correctly to support Site Recovery Manager.

You create and configure an Oracle Server database for Site Recovery Manager by using the tools that Oracle Server provides.

This information provides the general steps that you must perform to configure an Oracle Server database for Site Recovery Manager. For instructions about how to perform the relevant steps, see the Oracle documentation.

- When creating the database instance, specify UTF-8 encoding.
- Grant the Site Recovery Manager database user account the **connect**, **resource**, **create session** privileges and permissions.

For information about database sizing, see the *Sizing calculator for vCenter Site Recovery Manager databases - Oracle* at http://www.vmware.com/products/site-recovery-manager/resource.html.

Back Up and Restore the Embedded vPostgres Database

If you select the option to use an embedded database for Site Recovery Manager, the Site Recovery Manager installer creates a vPostgres database during the installation process. You can back up and restore the embedded vPostgres database by using PostgreSQL commands.

Always back up the Site Recovery Manager database before updating or upgrading Site Recovery Manager. You also might need to back up and restore the embedded vPostgres database if you need to uninstall then reinstall Site Recovery Manager and retain data from the previous installation, migrate Site Recovery Manager Server to another host machine, or revert the database to a clean state in the event that it becomes corrupted.

Prerequisites

For information about the commands that you use to back up and restore the embedded vPostgres database, see the pg_dump and pg_restore commands in the PostgreSQL documentation at http://www.postgresql.org/docs/9.3/static/index.html.

Procedure

1. Log into the system on which you installed Site Recovery Manager Server.
2. Stop the Site Recovery Manager service.
3. Navigate to the folder that contains the vPostgres commands.

   If you installed Site Recovery Manager Server in the default location, you find the vPostgres commands in `C:\Program Files\VMware\VMware vCenter Site Recovery Manager Embedded Database\bin`.
4. Create a backup of the embedded vPostgres database by using the `pg_dump` command.

   `pg_dump –Fc ––host 127.0.0.1 ––port` *`port_number`* `––username=`*`db_username`* `srm_db > srm_backup_name`

   You set the port number, username, and password for the embedded vPostgres database when you installed Site Recovery Manager. The default port number is 5678. The database name is `srm_db` and cannot be changed.
5. Perform the actions that necessitate the backup of the embedded vPostgres database.

   For example, update or upgrade Site Recovery Manager, uninstall and reinstall Site Recovery Manager, or migrate Site Recovery Manager Server.
6. (Optional) Restore the database from the backup that you created in Step 4 by using the `pg_restore` command.

   `pg_restore –Fc ––host 127.0.0.1 ––port` *`port_number`* `––username=`*`db_username`* `–– dbname=srm_db` *`srm_backup_name`*
7. Start the Site Recovery Manager service.

Create an ODBC System DSN for Site Recovery Manager

You must provide Site Recovery Manager with a system database source name (DSN) for a 64-bit open database connectivity (ODBC) connector. The ODBC connector allows Site Recovery Manager to connect to the Site Recovery Manager database.

You can create the ODBC system DSN before you run the Site Recovery Manager installer by running `Odbcad32.exe`, the 64-bit Windows ODBC Administrator tool.

Alternatively, you can create an ODBC system DSN by running the Windows ODBC Administrator tool during the Site Recovery Manager installation process.

Note If you use the embedded Site Recovery Manager database, the Site Recovery Manager installer creates the ODBC system DSN according to the information that you provide during installation. If you uninstall the embedded database, the uninstaller does not remove the DSN for the embedded database. The DSN remains available for use with a future reinstallation of the embedded database.

Prerequisites

You created the database instance to connect to Site Recovery Manager.

Procedure

1 Double-click the `Odbcad32.exe` file at `C:\Windows\System32` to open the 64-bit ODBC Administrator tool.

Important Do not confuse the 64-bit Windows ODBC Administrator tool with the 32-bit ODBC Administrator tool located in `C:\Windows\SysWoW64`. Do not use the 32-bit ODBC Administrator tool.

2 Click the **System DSN** tab and click **Add**.

3 Select the appropriate ODBC driver for your database software and click **Finish**.

Option	Action
SQL Server	Select **SQL Server Native Client 10.0**, **SQL Server Native Client 11.0**, or **ODBC Driver 11 for SQL Server**.
Oracle Server	Select **Microsoft ODBC for Oracle**.

4 (Optional) Create an SQL Server data source for the database.

a Provide the details for the data source.

Option	Action
Name	Enter a name for this data source, for example **SRM**.
Description	Enter a description of the data source, for example **SRM**.
Server	Select the running database instance to which to connect or enter the address of the database server.

b Select the authentication method that corresponds to the type of database user account that you created and click **Next**.

If you select Integrated Windows Authentication, you must use the same user account, or an account with the same privileges on the Site Recovery Manager Server host machine, when you run the Site Recovery Manager.

c Select the **Change the default database to** check box and select the Site Recovery Manager database.

d Click **Next** to retain the default settings for this database connection and click **Finish**.

5 (Optional) Create an Oracle Server data source for the database and click **Next**.

Option	Action
Data Source Name	Enter a name for this data source, for example `SRM`.
Description	Enter a description of the data source, for example `SRM`.
TNS Service Name	Enter the address of the database server in the format *`database_server_address`*`:1521/`*`database_name`*.
User ID	Enter the database user name.

6 Click **Test Data Source** to test the connection and click **OK** if the test succeeds.

If the test does not succeed, check the configuration information and try again.

7 Click **OK** to exit the Windows ODBC Administrator tool.

The ODBC driver for your database is ready to use.

Site Recovery Manager Authentication

4

All communications between Site Recovery Manager and vCenter Server instances take place over SSL connections and are authenticated by public key certificates or stored credentials.

When you install Site Recovery Manager Server, you must choose either credential-based authentication or custom certificate-based authentication. By default, Site Recovery Manager uses credential-based authentication, but custom certificate-based authentication can alternatively be selected. The authentication method you choose when installing the Site Recovery Manager Server is used to authenticate connections between the Site Recovery Manager Server instances at the protected and recovery sites, and between Site Recovery Manager and vCenter Server.

Important You cannot mix authentication methods between Site Recovery Manager Server instances at different sites and between Site Recovery Manager and vCenter Server.

Credential-Based Authentication

This is the default authentication method that Site Recovery Manager uses. If you are using credential-based authentication, Site Recovery Manager stores a user name and password that you specify during installation, and then uses those credentials when connecting to vCenter Server. Site Recovery Manager also creates a special-purpose certificate for its own use. This certificate includes additional information that you supply during installation.

Note Even though Site Recovery Manager creates and uses this special-purpose certificate when you choose credential-based authentication, credential-based authentication is not equivalent to certificate-based authentication in either security or operational simplicity.

Custom Certificate-Based Authentication

If you have or can acquire a PKCS#12 certificate signed by a trusted certificate authority (CA), use custom certificate-based authentication. Public key certificates signed by a trusted CA streamline many Site Recovery Manager operations and provide the highest level of security. Custom certificates that Site Recovery Manager uses have special requirements. See Requirements When Using Trusted SSL Certificates with Site Recovery Manager.

If you use custom certificate-based authentication, you must use certificates signed by a CA that both the vCenter Server and Site Recovery Manager Server instances trust, on both the protected site and the recovery site. You can use a certificate that is signed by a different CA on each site if both CAs are installed as trusted Root CAs on both sites.

If a certificate has expired and you attempt to start or restart Site Recovery Manager Server, the Site Recovery Manager service starts and then stops. If a certificate expires while Site Recovery Manager is running, Site Recovery Manager cannot establish a session with vCenter Server and appears in the disconnected state.

Certificate Warnings

If you are using credential-based authentication, inital attempts by the Site Recovery Manager Server to connect to vCenter Server produce a certificate warning because the trust relationship asserted by the special-purpose certificates created by Site Recovery Manager and vCenter Server cannot be verified by SSL. A warning allows you to verify the thumbprint of the certificate used by the other server and confirm its identity. To avoid these warnings, use certificate-based authentication and obtain your certificate from a trusted certificate authority.

This chapter includes the following topics:

Requirements When Using Trusted SSL Certificates with Site Recovery Manager

If you installed SSL certificates issued by a trusted certificate authority (CA) on the vCenter Server that supports Site Recovery Manager, the certificates you create for use by Site Recovery Manager must meet specific criteria.

Important Public CAs stopped issuing SSL/TLS certificates that contain internal server names or reserved IP addresses in November 2015. CAs will revoke SSL/TLS certificates that contain internal server names or reserved IP addresses on 1st October 2016. To minimize future disruption, if you use SSL/TLS certificates that contain internal server names or reserved IP addresses, obtain new, compliant certificates from a private CA before 1st October 2016.

- For information about the deprecation of internal server names and reserved IP addresses, see https://cabforum.org/internal-names/.
- For information about how the deprecation of internal server names and reserved IP addresses affects VMware products, see http://kb.vmware.com/kb/2134735.

While Site Recovery Manager uses standard PKCS#12 certificate for authentication, it places a few specific requirements on the contents of certain fields of those certificates. These requirements apply to the certificates used by both members of a Site Recovery Manager Server pair.

- The certificates must have a Subject Name value that must be the same for both members of the Site Recovery Manager pair. The Subject Name value can be constructed from the following components.
  - A Common Name (CN) attribute. A string such as **SRM** is appropriate here. The CN attribute is obligatory.
  - An Organization (O) attribute and an Organizational Unit (OU) attribute. The O and OU attributes are obligatory.
  - Other attributes, for example, the L (locality), S (state), and C (country) attributes, among others, are permitted but are not obligatory. If you specify any of these attributes, the values must be the same for both members of the Site Recovery Manager pair.
- The certificate used by each member of a Site Recovery Manager Server pair must include a Subject Alternative Name attribute the value of which is the fully-qualified domain name of the Site Recovery Manager Server host. This value will be different for each member of the Site Recovery Manager Server pair. Because this name is subject to a case-sensitive comparison, use lowercase letters when specifying the name during Site Recovery Manager installation.
  - If you are using an openssl CA, modify the openssl configuration file to include a line like the following if the Site Recovery Manager Server host's fully-qualified domain name is srm1.example.com:

    ```
    subjectAltName = DNS: srm1.example.com
    ```

  - If you are using a Microsoft CA, refer to http://support.microsoft.com/kb/931351 for information on how to set the Subject Alternative Name.
- If both Site Recovery Manager Server and vCenter Server run on the same host machine, you must provide two certificates, one for Site Recovery Manager and one for vCenter Server. Each certificate must have the Subject Alternative Name attribute set to the fully-qualified domain name of the host machine. Consequently, from a security perspective, it is better to run Site Recovery Manager Server and vCenter Server on different host machines.
- The certificate used by each member of a Site Recovery Manager Server pair must include an `extendedKeyUsage` or `enhancedKeyUsage` attribute the value of which is `serverAuth, clientAuth`. If you are using an openssl CA, modify the openssl configuration file to include a line like the following:

  ```
  extendedKeyUsage = serverAuth, clientAuth
  ```

- The Site Recovery Manager certificate password must not exceed 31 characters.
- The Site Recovery Manager certificate key length must be a minimum of 2048-bits.

- Site Recovery Manager accepts certificates with MD5RSA and SHA1RSA signature algorithms, but these are not recommended. Use SHA256RSA or stronger signature algorithms.

Provide Trusted CA Certificates to vSphere Web Client

If you use custom certificates that a certificate authority (CA) signed to authenticate between vCenter Server and Site Recovery Manager, you must copy the certificates of the signing CA to the host machine on which the vSphere Web Client service is running.

The vSphere Web Client service for each site requires the certificate of the signing CA for vCenter Server on the remote site. If you use a different CA to sign the certificates for Site Recovery Manager, the vSphere Web Client service for each site requires the certificate of the signing CA for Site Recovery Manager on both sites so that it can authenticate the client connection to the remote site. If you do not provide the certificates of the signing CA to the vSphere Web Client service on each site, installation and upgrade of Site Recovery Manager succeeds, but site pairing fails.

Prerequisites

Verify that you have custom certificates that a CA signed to authenticate between vCenter Server and Site Recovery Manager. If you use auto-generated certificates, you do not need to copy a certificate to the host machine on which the vSphere Web Client service is running.

Procedure

1. Log in to the host machine on which the vSphere Web Client service for a site is running.
2. Copy the certificate of the signing CA for the remote vCenter Server to the SSL trust store on the vSphere Web Client host machine.

   For example, if you are logged in to the vSphere Web Client host machine for site A, copy the certificate of the signing CA for the vCenter Server on site B to the SSL trust store on site A.

Type of Setup	SSL Trust Store Location
vCenter Server and vSphere Web Client running on Windows	`%ALLUSERSPROFILE%\VMware\SSL`
vCenter Server Virtual Appliance running on Linux	`/etc/ssl/certs`

3 (Optional) If you use a different CA to sign the certificates for Site Recovery Manager, copy the certificates of the signing CA for the local and remote Site Recovery Manager instances to the SSL trust store on the vSphere Web Client host machine.

   For example, if you are logged in to the vSphere Web Client host machine for site A, copy the certificates of the signing CA for the Site Recovery Manager instances on both sites A and B to the SSL trust store on site A.

Type of Setup	SSL Trust Store Location
vCenter Server and vSphere Web Client running on Windows	`%ALLUSERSPROFILE%\VMware\SSL`
vCenter Server Virtual Appliance running on Linux	`/etc/ssl/certs`

4 Restart the vSphere Web Client service.

5 Repeat Step 1 to Step 4 on the other site in the site pair.

   For example, copy the certificates of the signing CA for the vCenter Server on site A and optionally copy the certificates of the signing CA for the Site Recovery Manager instances on both sites A and B to the SSL trust store on site B.

Installing Site Recovery Manager

5

You must install a Site Recovery Manager Server instance at the protected site and also at the recovery site.

Site Recovery Manager requires a vCenter Server instance of the appropriate version at each site before you install Site Recovery Manager Server. The Site Recovery Manager installer must be able to connect to this vCenter Server instance during installation. For information about compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.

After you install the Site Recovery Manager Server instances, the Site Recovery Manager plug-in appears in the vSphere Web Client. You use the Site Recovery Manager plug-in in the vSphere Web Client for the vCenter Server instances on the protected and recovery sites to configure and manage Site Recovery Manager. Site Recovery Manager 5.8 does not support the vSphere Client for Windows.

Procedure

1 Prerequisites for Site Recovery Manager Server Installation

   Before you install Site Recovery Manager Server, you must perform several tasks and verify that you have certain information.

2 Install Site Recovery Manager Server

   You must install Site Recovery Manager Server at the protected site and at the recovery site.

3 Connect the Site Recovery Manager Server Instances on the Protected and Recovery Sites

   Before you can use Site Recovery Manager, you must connect the Site Recovery Manager Server instances on the protected and recovery sites. The sites must authenticate with each other. This is known as site pairing.

4 Establish a Client Connection to the Remote Site Recovery Manager Server Instance

   After you connect the Site Recovery Manager Server instances, you must establish a connection from the Site Recovery Manager interface in the vSphere Web Client to the remote Site Recovery Manager Server.

5 Install the Site Recovery Manager License Key

   Site Recovery Manager Server requires a license key to operate. Install a Site Recovery Manager license key as soon as possible after you install Site Recovery Manager.

6 (Optional) Modify a Site Recovery Manager Server Installation

To change some of the information that you supplied when you installed Site Recovery Manager Server, you can run the Site Recovery Manager installer in modify mode.

7 (Optional) Repair a Site Recovery Manager Server Installation

You can run the Site Recovery Manager installer in repair mode to repair a Site Recovery Manager Server installation.

8 Site Recovery Manager Server Does Not Start

Site Recovery Manager depends on other services. If one of those services is not running, the Site Recovery Manager Server does not start.

9 Uninstall and Reinstall the Same Version of Site Recovery Manager

If you uninstall then reinstall the same version of Site Recovery Manager, you must perform certain actions to reconfigure your Site Recovery Manager installation. You must perform these actions even if you retained the database contents when you uninstalled Site Recovery Manager, then connected the new installation to the existing database.

10 Unregister an Incompatible Version of vSphere Replication

Site Recovery Manager 5.8 requires vSphere Replication 5.8. The Site Recovery Manager installer stops if it detects an incompatible version of vSphere Replication.

Prerequisites for Site Recovery Manager Server Installation

Before you install Site Recovery Manager Server, you must perform several tasks and verify that you have certain information.

- Install the appropriate version of vCenter Server. This release of Site Recovery Manager requires the vSphere Web Client. For information about compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.
- If you do not use the embedded Site Recovery Manager database, configure and start the Site Recovery Manager database service before you install the Site Recovery Manager Server. See Chapter 3 Creating the Site Recovery Manager Database.
- If you do not use the embedded Site Recovery Manager database, Site Recovery Manager requires a database source name (DSN) for 64-bit open database connectivity (ODBC). You can create the ODBC system DSN before you run the Site Recovery Manager installer, or you can create the DSN during the installation process. For details about creating the ODBC system DSN, see Create an ODBC System DSN for Site Recovery Manager. If you use the embedded Site Recovery Manager database, the Site Recovery Manager installer creates the necessary DSN.
- Download the Site Recovery Manager installation file to a folder on the machine on which to install Site Recovery Manager.

- Verify that no reboot is pending on the Windows machine on which to install Site Recovery Manager Server. Verify that no other installation is running, including the silent installation of Windows updates. Pending reboots or running installations can cause the installation of Site Recovery Manager Server or the embedded Site Recovery Manager database to fail.
- To use Site Recovery Manager with vSphere Replication, deploy the appropriate version of vSphere Replication on both of the protected and recovery sites before you install Site Recovery Manager Server. The Site Recovery Manager installer verifies the version of vSphere Replication during installation and stops if it detects an incompatible version. This verification is not performed if you install vSphere Replication after you install Site Recovery Manager Server, which might lead to incompatible versions. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Web Client to stop working. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.
- If you have existing vSphere Replication appliances on the sites, you must either upgrade them to the correct version or unregister them from both vCenter Server instances before you install Site Recovery Manager. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Web Client to stop working. See Unregister an Incompatible Version of vSphere Replication.
- The user account that you use to install and run Site Recovery Manager must be a member of the local Administrators group. You can configure the Site Recovery Manager service to run under a specified user account. This account can be a local user or a domain user that is a member of the Administrators group on the machine on which you are installing Site Recovery Manager.
- If you are using certificate-based authentication, you must obtain appropriate certificate file. You must use the same type of authentication on both sites. See Chapter 4 Site Recovery Manager Authentication and Requirements When Using Trusted SSL Certificates with Site Recovery Manager.
- If you are using certificate-based authentication, provide the certificate for the remote site to the vSphere Web Client service on each site. See Provide Trusted CA Certificates to vSphere Web Client.
- Verify that you have the following information:
  - The fully qualified domain name (FQDN) or IP address of the site's vCenter Server instance. The server must be running and accessible during Site Recovery Manager installation. You must use the address format that you use to connect Site Recovery Manager to vCenter Server when you later pair the Site Recovery Manager sites. Using FQDNs is preferred, but if that is not universally possible, use IP addresses for all cases.
  - The user name and password of the vCenter Server administrator account.
  - A user name and password for the Site Recovery Manager database, if you are not using the embedded database.

Install Site Recovery Manager Server

You must install Site Recovery Manager Server at the protected site and at the recovery site.

You must install the same version of Site Recovery Manager Server and vCenter Server on both sites. You cannot mix Site Recovery Manager or vCenter Server versions across sites.

For environments with a small number of virtual machines to protect, you can run Site Recovery Manager Server and vCenter Server on the same system. For environments that approach the maximum limits of Site Recovery Manager and vCenter Server, install Site Recovery Manager Server on a system that is different from the system on which vCenter Server is installed. If Site Recovery Manager Server and vCenter Server are installed on the same system, administrative tasks might become more difficult to perform in large environments.

If you are upgrading an existing Site Recovery Manager installation, see Chapter 6 Upgrading Site Recovery Manager.

If you are installing Site Recovery Manager in a shared recovery site configuration, see Chapter 8 Installing Site Recovery Manager to Use with a Shared Recovery Site.

Prerequisites

- Site Recovery Manager requires the appropriate version of vCenter Server. For information about compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.
- Perform the tasks and verify that you have the required information listed in Prerequisites for Site Recovery Manager Server Installation.
- If you use an SQL Server database with Integrated Windows Authentication as the Site Recovery Manager database, you must use the same user account or an account with the same privileges when you install Site Recovery Manager Server as you used when you created the Integrated Windows Authentication data source name (DSN) for SQL Server.

Procedure

1. Double-click the Site Recovery Manager installer, select an installation language, and click **OK**.
2. Follow the installer prompts to accept the license agreement, and verify that you satisfied the installation prerequisites.
3. Choose where to install Site Recovery Manager Server, and click **Next**.
   - Keep the default destination folder.
   - Click **Change** to change the destination folder, and select a target volume.

   The default installation folder for Site Recovery Manager is `C:\Program Files\VMware\VMware vCenter Site Recovery Manager`. If you use a different folder, the pathname cannot be longer than 120 characters including the end slash, and cannot include non-ASCII characters.

4 Enter information about the vCenter Server instance at the site where you are installing Site Recovery Manager and click **Next**.

Option	Action
vCenter Server Address	Enter the host name or IP address of vCenter Server. Enter the host name in lowercase letters. After installation is complete and you are configuring the connection between the protected and recovery sites, supply this host name or IP address exactly as you enter it here, because it is subject to case-sensitive comparisons. **Important** Note the address format that you use to connect Site Recovery Manager to vCenter Server. You must use the same address format when you later pair the Site Recovery Manager sites. If you use an IP address to connect Site Recovery Manager to vCenter Server, you must use this IP address when pairing the Site Recovery Manager sites. If you use certificate-based authentication, the address of Site Recovery Manager Server must be the same as the Subject Alternative Name (SAN) value of the Site Recovery Manager certificate. This is usually the fully qualified domain name of the Site Recovery Manager Server host.
vCenter Server Port	Accept the default or enter a new value if vCenter Server uses a different port.
vCenter Server Username	Enter the user name of an administrator of the specified vCenter Server instance. If you use auto-generated certificates, Site Recovery Manager Server uses the username and password that you specify here to authenticate with vCenter Server whenever you connect to Site Recovery Manager. If you use custom certificates, only the Site Recovery Manager installer uses this account to register Site Recovery Manager with vCenter Server during installation.
vCenter Server Password	Enter the password for the specified user name. The password text box cannot be empty.

5 (Optional) If you are using credential-based authentication, verify the vCenter Server certificate and click **Yes** to accept it.

If you are using certificate-based authentication, you do not receive a prompt to accept the certificate.

6 Enter information with which to register the Site Recovery Manager with vCenter Server, and click **Next**.

Option	Description
Local Site Name	A name for this Site Recovery Manager site, that appears in the Site Recovery Manager interface. A suggested name is generated, but you can enter any name. It cannot be the same name that you use for another Site Recovery Manager installation with which this one will be paired.
Administrator E-mail	Email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.

Option	Description
Local Host	Name or IP address of the local host. The Site Recovery Manager installer obtains this value. Only change it if it is incorrect. For example, the local host might have more than one network interface and the one that the Site Recovery Manager installer detects is not the interface you want to use. If you use certificate-based authentication, the **Local Host** value must be the same as the SAN value of the supplied certificate. This is usually the fully qualified domain name of the Site Recovery Manager Server host.
Listener Ports	SOAP and HTTP port numbers to use.
API Listener Port	SOAP port number for API clients to use.

The Site Recovery Manager installer supplies default values for the listener ports. Do not change them unless the defaults would cause port conflicts.

7 Select the default Site Recovery Manager plug-in identifier, or create a plug-in identifier for this Site Recovery Manager Server pair, and click **Next**.

You can install Site Recovery Manager in a shared recovery site configuration, in which multiple protected sites recover to a single recovery site.

Option	Description	
Default SRM Plug-in Identifier	Installs Site Recovery Manager in a standard configuration with one protected site and one recovery site.	
Custom SRM Plug-in Identifier	Installs Site Recovery Manager in a shared recovery site configuration, with multiple protected sites and one recovery site. Enter the details of the plug-in identifier.	
	Plug-in ID	A unique identifier. Assign the same identifier to the Site Recovery Manager Server instances on the protected site and the shared recovery site.
	Organization	The name of the organization to which this Site Recovery Manager Server pair belongs. This name helps to identify to Site Recovery Manager Server pairs in a shared recovery site configuration, especially when multiple organizations use the shared recovery site.
	Description	An optional description of this Site Recovery Manager Server pair.

8 Select an authentication method and click **Next**.

Important You must use the same authentication method on both sites. If you attempt to use credential-based authentication on one site and certificate-based authentication on the other, site pairing fails.

Option	Description
Authenticate with vCenter Server by using credential-based authentication with an automatically generated certificate	a Select **Automatically generate certificate** and click **Next**. b Enter text values for your organization and organization unit, typically your company name and the name of your group in the company. c Click **Next**.
Authenticate with vCenter Server by using a custom certificate	a Select **Load a certificate file** and click **Next**. b Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. c Enter the certificate password. d Click **Next**.

9 Select whether to use the embedded database or a custom database, and click **Next**.

Option	Description
Use the embedded database server	Site Recovery Manager provides a built-in vPostgres database that you can use with minimal configuration.
Use a custom database server	Select an existing 64-bit DSN from the drop-down menu. You can also click **DSN Setup** to start the Windows 64-bit ODBC Administrator tool, to view the existing DSNs, or to create a new 64-bit system DSN for the Site Recovery Manager database.

10 Provide the Site Recovery Manager database configuration information and click **Next**.

Option	Action
Data Source Name	■ Enter a name for the DSN that the Site Recovery Manager installer creates when it creates the embedded database. The embedded database DSN can only contain alphanumeric characters and underscores. ■ If you use a custom database, select the DSN for your database.
Database Username	■ Enter a user name for the database user account that the Site Recovery Manager installer creates when it creates the embedded database. The embedded database username can only contain lower case alphanumeric characters and underscores. ■ Enter the user name for an existing database user account to use with a custom database. This option is disabled if you use SQL Server with Integrated Windows Authentication. In this case, the credentials of the user account running the Site Recovery Manager installer are used to authenticate with SQL Server. This account is also used to run the Site Recovery Manager service, to guarantee that Site Recovery Manager can connect to the database.

Option	Action
Database Password	■ Enter a password for the database user account that the Site Recovery Manager installer creates when it creates the embedded database. The password cannot contain any white spaces, quotation marks, backslashes, or Extended ASCII characters. ■ Enter the password for an existing database user account to use with a custom database.
Database Port	This option is only visible if you selected **Use the embedded database server**. Leave the default port number or enter a new port number if the default port is already in use.
Connection Count	Enter the initial connection pool size. If all connections are in use and a new one is needed, a connection is created as long as it does not exceed the maximum number of connections allowed. It is faster for Site Recovery Manager to use a connection from the pool than to create one. In most cases, it is not necessary to change this setting. Before changing this setting, consult with your database administrator.
Max Connections	Enter the maximum number of database connections that can be open simultaneously. If the database administrator restricted the number of connections that the database can have open, this value cannot exceed that number. In most cases, it is not necessary to change this setting. Before you change this setting, consult with your database administrator.

11 Select the user account under which to run the Site Recovery Manager Server service.

- Select **Use Local System Account** to run the Site Recovery Manager Server service under the Local System account.
- Enter the username and password of an existing LDAP user account to run the Site Recovery Manager Server service under a different user account. This can be any user account, including local users, that is a member of the built-in Administrators group.

This option is not available if you use an SQL Server database with Integrated Windows Authentication. In this case, the Site Recovery Manager Server service runs under the account that you use to install Site Recovery Manager.

12 Click **Install**.

13 When the installation is finished, click **Finish**.

14 Repeat steps Step 1 through Step 13 on the recovery site.

Connect the Site Recovery Manager Server Instances on the Protected and Recovery Sites

Before you can use Site Recovery Manager, you must connect the Site Recovery Manager Server instances on the protected and recovery sites. The sites must authenticate with each other. This is known as site pairing.

Important You must use the same authentication method on both sites. If you attempt to use credential-based authentication on one site and certificate-based authentication on the other, site pairing fails.

Prerequisites

- Verify that you installed Site Recovery Manager Server instances at the protected and recovery sites.
- If you did not select the default plug-in ID when you installed Site Recovery Manager Server, you must have assigned the same custom plug-in ID to the Site Recovery Manager Server instances on each of the sites.
- If you are using certificate-based authentication, provide the certificate for the remote site to the vSphere Web Client service on each site. See Provide Trusted CA Certificates to vSphere Web Client.

Procedure

1. Connect to vSphere Web Client on one of the sites, and select **Site Recovery > Sites**.
2. On the **Objects** tab, right-click a site and select **Pair Site**.
3. Enter the details for the vCenter Server instance on the remote site, and click **OK**.

Option	Action
vCenter Server	Enter the IP address or hostname of the vCenter Server instance on the remote site. You must use the same vCenter Server address format that you used when you installed Site Recovery Manager Server on that site. If you used an IP address when installing Site Recovery Manager Server, use an IP address for the remote site to pair the Site Recovery Manager sites. If you entered a hostname when installing Site Recovery Manager Server, use the same hostname to pair the sites.
Port	Port 80 is used for the initial connection to the remote site. After the initial HTTP connection is made, the two sites establish an SSL connection for subsequent connections. Change this setting only if vCenter Server uses a different port.
Username	Enter the user name of an administrator of the specified vCenter Server instance. This information is only required if you use auto-generated certificates for authentication.
Password	Enter the password for the specified user name. This information is only required if you use auto-generated certificates for authentication.

   The remote site appears on the **Objects** tab.

The protected and recovery sites are connected.

Establish a Client Connection to the Remote Site Recovery Manager Server Instance

After you connect the Site Recovery Manager Server instances, you must establish a connection from the Site Recovery Manager interface in the vSphere Web Client to the remote Site Recovery Manager Server.

You require a client connection to the remote Site Recovery Manager Server to perform operations that affect both sites, such as configuring inventory mappings and creating protection groups. If you do not establish the client connection, Site Recovery Manager prompts you to log in to the remote site when you attempt operations that affect both sites.

Prerequisites

You connected the Site Recovery Manager Server instances on the protected and recovery sites.

Procedure

1. Connect to vSphere Web Client on one of the sites, and select **Site Recovery > Sites**.
2. Right-click the remote site, select **Login Site**, enter the username and password for vCenter Server at the remote site, and click **OK**.

Install the Site Recovery Manager License Key

Site Recovery Manager Server requires a license key to operate. Install a Site Recovery Manager license key as soon as possible after you install Site Recovery Manager.

Prerequisites

Site Recovery Manager uses the vSphere licensing infrastructure for license management. Ensure that you have sufficient vSphere licenses for Site Recovery Manager to protect and recover virtual machines on both sites.

Procedure

1. Connect vSphere Web Client to a vCenter Server instance on which Site Recovery Manager is installed.
2. On the vSphere Web Client **Home** tab, click **Licensing**.
3. Click the plus sign on the **License Keys** tab.
4. Enter the Site Recovery Manager license key in the **Add License Keys** text box and click **Next**.
5. Review the details of the Site Recovery Manager license and click **Finish**.
6. Click the **Solutions** tab.
7. Select the Site Recovery Manager site and click **Assign License Key**.
8. Select the Site Recovery Manager license key from the list of available licenses, and click **OK**.
9. Repeat step Step 1 through Step 8 to assign Site Recovery Manager license keys to all appropriate vCenter Server instances.

(Optional) Modify a Site Recovery Manager Server Installation

To change some of the information that you supplied when you installed Site Recovery Manager Server, you can run the Site Recovery Manager installer in modify mode.

Installing Site Recovery Manager Server binds the installation to a number of values that you supply, including the vCenter Server instance to extend, the Site Recovery Manager database type, DSN and credentials, the type of authentication, and so on. The Site Recovery Manager installer supports a modify mode that allows you to change certain values that you configured when you installed Site Recovery Manager Server.

- The user name and password of the vCenter Server administrator, if they changed since you installed Site Recovery Manager
- The type of authentication (certificate-based or credential-based), the authentication details, or both.
- The user name, password, and connection numbers for the Site Recovery Manager database
- The user account under which the Site Recovery Manager Server service runs

The installer's modify mode presents modified versions of some of the pages that are part of the Site Recovery Manager Server installer. You cannot modify the host and administrator configuration information, including the local site name, Site Recovery Manager administrator email address, local host address, or the listener ports. This page is omitted when you run the installer in modify mode. Site Recovery Manager does not use the administrator email address that you provided during installation, so if the Site Recovery Manager administrator changes after you installed Site Recovery Manager Server, Site Recovery Manager operation is not affected.

Caution Updating the certificate affects the thumbprint, which can affect the connection between the protected site and the recovery site. Check the connection between the protected site and the recovery site after you run the installer in modify mode. For information about how to configure the connection between the protected site and the recovery site, see Connect the Site Recovery Manager Server Instances on the Protected and Recovery Sites.

If you selected the embedded database when you installed Site Recovery Manager, you cannot modify the installation to use an external database, and the reverse.

Prerequisites

- Verify that you have administrator privileges on Site Recovery Manager Server or that you are a member of the Administrators group. Disable Windows User Account Control (UAC) before you attempt the change operation or select **Run as administrator** when you start the Site Recovery Manager installer
- If you change the Site Recovery Manager installation to use certificate-based authentication instead of credential-based authentication, or if you upload a new custom certificate, you must provide the certificate for the remote site to the vSphere Web Client service on each site. See Provide Trusted CA Certificates to vSphere Web Client.

Procedure

1. Log in to the Site Recovery Manager Server host.
2. Open **Programs and Features** from the Windows Control Panel.
3. Select the entry for **VMware vCenter Site Recovery Manager** and click **Change**.

4 Click **Next**.

5 Select **Modify** and click **Next**.

6 Enter the username and password for the vCenter Server instance that Site Recovery Manager extends.

If you use auto-generated certificates, Site Recovery Manager Server uses the username and password that you specify here to authenticate with vCenter Server whenever you connect to Site Recovery Manager. If you use custom certificates, only the Site Recovery Manager installer uses this account to register Site Recovery Manager with vCenter Server during installation.

You cannot use the installer's modify mode to change the vCenter Server address or port. When you click **Next**, the installer contacts the specified vCenter Server instance and validates the information you supplied.

7 Select an authentication method and click **Next**.

Option	Description
Leave the current authentication method unchanged	Select **Use existing certificate**. If the installed certificate is not valid, this option is unavailable.
Use credential-based authentication	Select **Automatically generate a certificate** to generate a new certificate.
Use certificate-based authentication	Select **Use a PKCS #12 certificate file** to upload a new certificate.

If you do not select **Use existing certificate**, you are prompted to supply additional authentication details such as certificate location or strings to use for Organization and Organizational Unit.

8 Provide or change the database configuration information and click **Next**.

Option	Description
Username	A user ID valid for the specified database.
Password	The password for the specified user ID.
Connection Count	The initial connection pool size.
Max Connections	The maximum number of database connections open simultaneously.

9 Choose whether to keep or discard the database contents and click **Next**.

Option	Description
Use existing data	Preserves the contents of the existing database.
Recreate the database	Overwrites the existing database and deletes its contents.

10 Select or deselect the **Use Local System account** check box to change the user account under which the Site Recovery Manager Server service runs, and click **Next**.

- If you deselect **Use Local System account**, you must provide a username and password for a valid user account.
- If you are using SQL Server with Integrated Windows Authentication, the username text box shows the username of the account that is running the installer and cannot be modified.

11 Click **Install** to modify the installation.

   The installer makes the requested modifications and restarts the Site Recovery Manager Server.

12 When the modification operation is finished and the Site Recovery Manager Server restarts, log in to the vSphere Web Client to check the status of the connection between the protected site and the recovery site.

13 (Optional) If the connection between the protected site and the recovery site is broken, reconfigure the connection, starting from the Site Recovery Manager Server that you updated.

(Optional) Repair a Site Recovery Manager Server Installation

You can run the Site Recovery Manager installer in repair mode to repair a Site Recovery Manager Server installation.

Running the installer in repair mode fixes missing or corrupted files, shortcuts, and registry entries in the Site Recovery Manager Server installation.

Caution Do not run the Site Recovery Manager installer in repair mode on the protected site and on the recovery site simultaneously.

Prerequisites

Verify that you have administrator privileges on Site Recovery Manager Server or that you are a member of the Administrators group. Disable Windows User Account Control (UAC) before you attempt the change operation or select **Run as administrator** when you start the Site Recovery Manager installer

Procedure

1 Log in to the Site Recovery Manager Server host.

2 Open **Programs and Features** from the Windows Control Panel.

3 Select the entry for **VMware vCenter Site Recovery Manager** and click **Change**.

4 Click **Next**.

5 Select **Repair** and click **Next**.

6 Click **Install** to repair the installation.

   The installer makes any necessary repairs and restarts Site Recovery Manager Server.

Site Recovery Manager Server Does Not Start

Site Recovery Manager depends on other services. If one of those services is not running, the Site Recovery Manager Server does not start.

Problem

After you install, repair, or modify Site Recovery Manager by running the Site Recovery Manager installer, or after you reboot the Site Recovery Manager Server, the Site Recovery Manager Server does not start, or else starts and then stops.

Cause

The Site Recovery Manager Server might not start if vCenter Server is not running, if it cannot connect to the Site Recovery Manager database, or if other services that Site Recovery Manager requires are not running.

Solution

1. Check the latest Site Recovery Manager Server log file and the Windows Event Viewer for errors.

   Most errors appear in the Site Recovery Manager Server log file. Other errors can appear in the Windows Event Viewer. For example, the Site Recovery Manager database initializes before the Site Recovery Manager logging service starts. If errors occur during database initialization, they appear in the Windows Event Viewer. Errors related to certificate validity also appear in the Windows Event Viewer.

2. Verify that the vCenter Server instance that Site Recovery Manager extends is running.

   If the vCenter Server service is running on a different host to the Site Recovery Manager Server and the vCenter Server service stops, the Site Recovery Manager Server will start succesfully and then stop after a short period.

3. Verify that the Site Recovery Manager database service is running.

   If you use the embedded database, check that the VMware Postgres service is running. If you use an external database, check that the appropriate SQL Server or Oracle Server service is running.

4. Log in to the machine on which you installed the Site Recovery Manager Server.

5. Verify that Site Recovery Manager can connect to vCenter Server.

   a. Open **Programs and Features** from the Windows Control Panel.

   b. Select the entry for **VMware vCenter Site Recovery Manager** and click **Change**.

   c. Click **Next**.

   d. Select **Modify**.

   e. Check that the address for vCenter Server is correct.

      If the vCenter Server address has changed since you installed Site Recovery Manager, for example if the vCenter Server machine uses DHCP instead of a static address, remove, reinstall, and reconfigure Site Recovery Manager.

   f. Enter the vCenter Server password and click **Next**.

      If the vCenter Server password has changed since you installed Site Recovery Manager, enter the new password.

g Select **Use existing certificate** and click **Next**.

h Check that the credentials for the Site Recovery Manager database are correct.

i Verify that the Site Recovery Manager database permits sufficient connections.

If the Site Recovery Manager logs contain the message `GetConnection: Still waiting for available connections`, increase the maximum number of database connections. Consult with your database administrator before changing these settings.

j Click **Next**.

If the connection to the database fails, close the Site Recovery Manager installer and go to Step 6.

k Select **Use existing data** and click **Next**.

l Check that the user account for the Site Recovery Manager service is correct, and click **Next**.

If you use an account other than the Local System account, check that the username and password are correct.

m Click **Install** to update the Site Recovery Manager configuration, or click **Cancel** if you made no changes.

6 Verify that Site Recovery Manager can connect to the Site Recovery Manager database.

a Open the Windows ODBC Data Source Administrator utility, `C:\Windows\System32\Odbcad32.exe`.

b Select the system DSN for Site Recovery Manager and click **Configure**.

c Check the database settings.

- Check that Site Recovery Manager is attempting to connect to the correct database server.
- Check that the login credentials for the Site Recovery Manager database are correct.
- Check that the authentication method is correct.

d Click **Test Data Source**.

If the connection is configured correctly, the **ODBC Data Source Test** window shows a positive result.

e If the connection test fails, reconfigure the Site Recovery Manager database by using the administration software from your database provider.

7 Open the Windows Server Manager utility and select **Configuration > Services**.

8 Verify that the services that Site Recovery Manager requires are running.

- Windows Server
- Windows Workstation
- Protected Storage

9 Select the **VMware vCenter Site Recovery Manager Server** service in the Windows Server Manager utility and click **Start** or **Restart**.

Uninstall and Reinstall the Same Version of Site Recovery Manager

If you uninstall then reinstall the same version of Site Recovery Manager, you must perform certain actions to reconfigure your Site Recovery Manager installation. You must perform these actions even if you retained the database contents when you uninstalled Site Recovery Manager, then connected the new installation to the existing database.

If you configured advanced settings in the previous installation, these advanced settings are not retained if you uninstall and then reinstall the same version of Site Recovery Manager. This is by design.

Procedure

1 (Optional) If you configured advanced settings in the existing installation, take a note of the advanced settings.

   You configure advanced settings in **Site Recovery > Sites > *Site* > Manage > Advanced Settings** in the vSphere Web Client

2 Uninstall Site Recovery Manager, without deleting its data.

3 Reinstall Site Recovery Manager.

   During reinstallation, connect Site Recovery Manager to the same vCenter Server instance and the same database as the previous installation.

4 Reconfigure the connection between the sites.

5 Reconfigure Storage Array Managers (SRAs) to enter the SRA credentials.

6 Reconfigure any advanced settings.

Unregister an Incompatible Version of vSphere Replication

Site Recovery Manager 5.8 requires vSphere Replication 5.8. The Site Recovery Manager installer stops if it detects an incompatible version of vSphere Replication.

Problem

If you install an incompatible version of vSphere Replication after you installed Site Recovery Manager 5.8, the verification of the vSphere Replication version is not performed and vSphere Web Client stops working.

Cause

Running incompatible versions of Site Recovery Manager and vSphere Replication causes vSphere Web Client to stop working. If the Site Recovery Manager installer detects an incompatible version of vSphere Replication or if you installed an incompatible version of vSphere Replication after you installed Site Recovery Manager 5.8, you must either upgrade vSphere Replication or unregister it from vCenter Server.

Solution

If you cannot upgrade vSphere Replication to the correct version, unregister vSphere Replication from vCenter Server. For information about how to unregister vSphere Replication from vCenter Server, see Uninstall vSphere Replication and Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted in *vSphere Replication Administration*.

Upgrading Site Recovery Manager

6

You can upgrade existing Site Recovery Manager installations. The Site Recovery Manager upgrade process preserves existing information about Site Recovery Manager configurations.

Because of update release schedules, upgrading to certain Site Recovery Manager 5.8.x update releases is not supported for all 5.1.x and 5.5.x releases. For information about supported upgrade paths, see **Solution Upgrade Path > VMware vCenter Site Recovery Manager** in the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php? before you upgrade.

Important Upgrading from Site Recovery Manager 5.0.x to Site Recovery Manager 5.8 is not supported. Upgrade Site Recovery Manager 5.0.x to a Site Recovery Manager 5.5.x release before you upgrade to Site Recovery Manager 5.8. See Upgrading Site Recovery Manager in the Site Recovery Manager 5.5 documentation for information about upgrading from 5.0.x to 5.5.x.

After you upgrade the Site Recovery Manager Server instances, the Site Recovery Manager plug-in appears in the vSphere Web Client. You use the Site Recovery Manager plug-in in the vSphere Web Client for the vCenter Server instances on the protected and recovery sites to configure and manage Site Recovery Manager. Site Recovery Manager 5.8 does not support the vSphere Client for Windows.

For the supported upgrade paths for other Site Recovery Manager releases, see the release notes for those releases. Alternatively, see the Solution Upgrade Path section of the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

To revert to Site Recovery Manager 5.1.x or 5.5.x after upgrading to Site Recovery Manager 5.8, see Revert to a Previous Release of Site Recovery Manager.

- Information That Site Recovery Manager Upgrade Preserves

  The Site Recovery Manager upgrade procedure preserves information from existing installations.

- Types of Upgrade that Site Recovery Manager Supports

  Upgrading Site Recovery Manager requires that you upgrade vCenter Server. Site Recovery Manager supports different upgrade configurations.

- Order of Upgrading vSphere and Site Recovery Manager Components

  You must upgrade certain components of your vSphere environment before you upgrade Site Recovery Manager.

- Upgrade Site Recovery Manager

  You perform several tasks to upgrade Site Recovery Manager.

Information That Site Recovery Manager Upgrade Preserves

The Site Recovery Manager upgrade procedure preserves information from existing installations.

Site Recovery Manager preserves settings and configurations that you created for the previous release.

- Datastore groups
- Protection groups
- Inventory mappings
- Recovery plans
- IP customizations for individual virtual machines
- Custom roles and their memberships
- Site Recovery Manager object permissions in vSphere
- Custom alarms and alarm actions
- Test plan histories
- Security certificates
- Mass IP customization files (CSVs)

Important During an upgrade, Site Recovery Manager does not retain any advanced settings that you configured in the previous installation. This is by design. Due to changes in default values or improvements in performance, advanced settings that you set in a previous version of Site Recovery Manager might not be required by or compatible with the new version.

Important During an upgrade, Site Recovery Manager preserves only protection groups and recovery plans that are in a valid state. Site Recovery Manager discards protection groups or recovery plans that are in an invalid state.

Types of Upgrade that Site Recovery Manager Supports

Upgrading Site Recovery Manager requires that you upgrade vCenter Server. Site Recovery Manager supports different upgrade configurations.

Table 6-1. Types of vCenter Server and Site Recovery Manager Upgrades

Upgrade Type	Description	Supported
In-place upgrade of Site Recovery Manager	The simplest upgrade path. This path involves upgrading the vCenter Server instances associated with Site Recovery Manager before upgrading Site Recovery Manager Server. Run the new version of the Site Recovery Manager installer on the existing Site Recovery Manager Server host machine, connecting to the existing database.	Yes
Upgrade Site Recovery Manager with migration	This path involves upgrading the vCenter Server instances associated with Site Recovery Manager before upgrading Site Recovery Manager Server. To migrate Site Recovery Manager to a different host or virtual machine as part of the Site Recovery Manager upgrade, stop the existing Site Recovery Manager Server. Do not uninstall the previous release of Site Recovery Manager Server and make sure that you retain the database contents. Run the new version of the Site Recovery Manager installer on the new host or virtual machine, connecting to the existing database.	Yes
New vCenter Server installation with migration of Site Recovery Manager	Create new installations of vCenter Server and migrate Site Recovery Manager Server to these new vCenter Server instances.	No. You cannot migrate Site Recovery Manager Server to a new installation of vCenter Server. Site Recovery Manager requires unique object identifiers on the vCenter Server that are not available if you use a new vCenter Server installation. To use a new vCenter Server installation you must create a new Site Recovery Manager Server installation.

Order of Upgrading vSphere and Site Recovery Manager Components

You must upgrade certain components of your vSphere environment before you upgrade Site Recovery Manager.

Upgrade the components on the protected site before you upgrade the components on the recovery site. Upgrading the protected site first allows you to perform a disaster recovery on the recovery site if you encounter problems during the upgrade that render the protected site unusable. The exception is the ESXi hosts, which you can upgrade after you finish upgrading the other components on the protected and recovery sites.

Important If you configured bidirectional protection, in which each site acts as the recovery site for the virtual machines on the other site, upgrade the most critical of the sites first.

1 Upgrade vCenter Server and vSphere Web Client on the protected site.

2 If you use vSphere Replication, upgrade the vSphere Replication deployment on the protected site.

3 Upgrade Site Recovery Manager Server on the protected site.

4 If you use array-based replication, upgrade the storage replication adapters (SRA) on the protected site.

5 Upgrade vCenter Server and vSphere Web Client on the recovery site.

6 If you use vSphere Replication, upgrade the vSphere Replication deployment on the recovery site.

7 Upgrade Site Recovery Manager Server on the recovery site.

8 If you use array-based replication, upgrade the storage replication adapters (SRA) on the recovery site.

9 Verify the connection between the Site Recovery Manager sites.

10 Verify that your protection groups and recovery plans are still valid.

11 Upgrade ESXi Server on the recovery site.

12 Upgrade ESXi Server on the protected site.

13 Upgrade the virtual hardware and VMware Tools on the virtual machines on the ESXi hosts.

Upgrade Site Recovery Manager

You perform several tasks to upgrade Site Recovery Manager.

You must perform the upgrade tasks in order. Complete all of the upgrade tasks on the protected site first, then complete the tasks on the recovery site.

Prerequisites

Because of update release schedules, upgrading to certain Site Recovery Manager 5.8.x update releases is not supported for all 5.1.x and 5.5.x releases. For information about supported upgrade paths, see **Solution Upgrade Path > VMware vCenter Site Recovery Manager** in the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php? before you upgrade.

Important Upgrading from Site Recovery Manager 5.0.x to Site Recovery Manager 5.8 is not supported. Upgrade Site Recovery Manager 5.0.x to a Site Recovery Manager 5.5.x release before you upgrade to Site Recovery Manager 5.8. See Upgrading Site Recovery Manager in the Site Recovery Manager 5.5 documentation for information about upgrading from 5.0.x to 5.5.x.

- Prepare for Site Recovery Manager Upgrade

  Before you can upgrade Site Recovery Manager, you must perform preparatory tasks on both Site Recovery Manager sites.

- In-Place Upgrade of Site Recovery Manager Server

  An in-place upgrade provides a quick way to upgrade Site Recovery Manager Server to a new release without changing any of the information that you provided for the current installation. You can upgrade Site Recovery Manager Server on the same host machine as an existing Site Recovery Manager Server installation.

- Upgrade Site Recovery Manager Server with Migration

  You can upgrade Site Recovery Manager and migrate Site Recovery Manager Server to a different host than the previous Site Recovery Manager Server installation.

- Configure and Verify the Upgraded Site Recovery Manager Installation

  You must configure the upgraded components to establish a working Site Recovery Manager installation.

- Revert to a Previous Release of Site Recovery Manager

  To revert to a previous release of Site Recovery Manager, you must uninstall Site Recovery Manager from the protected and recovery sites. You can then reinstall the previous release.

Prepare for Site Recovery Manager Upgrade

Before you can upgrade Site Recovery Manager, you must perform preparatory tasks on both Site Recovery Manager sites.

Prerequisites

- Because of update release schedules, upgrading to certain Site Recovery Manager 5.8.x update releases is not supported for all 5.1.x and 5.5.x releases. For information about supported upgrade paths, see **Solution Upgrade Path > VMware vCenter Site Recovery Manager** in the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php? before you upgrade.

  Important Upgrading from Site Recovery Manager 5.0.x to Site Recovery Manager 5.8 is not supported. Upgrade Site Recovery Manager 5.0.x to a Site Recovery Manager 5.5.x release before you upgrade to Site Recovery Manager 5.8. See Upgrading Site Recovery Manager in the Site Recovery Manager 5.5 documentation for information about upgrading from 5.0.x to 5.5.x.

- If you are using certificate-based authentication, provide the certificate for the remote site to the vSphere Web Client service on each site. See Provide Trusted CA Certificates to vSphere Web Client.
- To use Site Recovery Manager with vSphere Replication, deploy the appropriate version of vSphere Replication on both of the protected and recovery sites before you upgrade Site Recovery Manager Server. The Site Recovery Manager installer verifies the version of vSphere Replication during installation and stops if it detects an incompatible version. This verification is not performed if you install vSphere Replication after you upgrade Site Recovery Manager Server, which might lead to incompatible versions. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Web Client to stop working. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.
- If you have existing vSphere Replication appliances on the sites, you must either upgrade them to the correct version or unregister them from both vCenter Server instances before you upgrade Site Recovery Manager. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Web Client to stop working. See Unregister an Incompatible Version of vSphere Replication.
- Migration of data from an external database to the embedded database is not supported. For information about how to back up the embedded database, see Back Up and Restore the Embedded vPostgres Database.
- **Important** Verify that there are no pending cleanup operations on recovery plans and that there are no configuration issues for the virtual machines that Site Recovery Manager protects.
  - All recovery plans are in the Ready state.
  - The protection status of all of the protection groups is OK.
  - The protection status of all of the individual virtual machines in the protection groups is OK.
  - The recovery status of all of the protection groups is Ready.

- If you configured advanced settings in the existing installation, take a note of the settings that you configured before upgrading.
- The local and remote vCenter Server instances must be running when you upgrade Site Recovery Manager.
- Upgrade all of the vCenter Server components and Site Recovery Manager on one site before you upgrade vCenter Server and Site Recovery Manager on the other site.
- Download the Site Recovery Manager installation file to a folder on the machines on which to upgrade Site Recovery Manager.
- Verify that no reboot is pending on the Windows machine on which to install Site Recovery Manager Server. Verify that no other installation is running, including the silent installation of Windows updates. Pending reboots or running installations can cause the installation of Site Recovery Manager Server to fail.

Procedure

1. Back up the Site Recovery Manager database by using the tools that the database software provides.
2. Upgrade vCenter Server.

   Site Recovery Manager 5.8.0 requires vCenter Server 5.5 update 2. For information about compatibility between vCenter Server and Site Recovery Manager 5.8 update releases, see *vCenter Server Requirements* in the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.

   Important You must upgrade all components of vCenter Server, including the Inventory Service as well as vCenter Server itself.
3. Upgrade the vSphere Web Client server.

   Site Recovery Manager 5.8 requires the appropriate version of the vSphere Web Client. Site Recovery Manager 5.8 does not support the vSphere Client for Windows.
4. Upgrade vSphere Replication.

   Site Recovery Manager 5.8.0 requires vSphere Replication 5.8.0. If you cannot upgrade vSphere Replication, you must unregister the vSphere Replication appliance from vCenter Server.

In-Place Upgrade of Site Recovery Manager Server

An in-place upgrade provides a quick way to upgrade Site Recovery Manager Server to a new release without changing any of the information that you provided for the current installation. You can upgrade Site Recovery Manager Server on the same host machine as an existing Site Recovery Manager Server installation.

To upgrade Site Recovery Manager and migrate the Site Recovery Manager Server to a different host machine, see Upgrade Site Recovery Manager Server with Migration.

Important If you are updating Site Recovery Manager 5.8 to a 5.8.x update release or to a 5.8.x.x patch release, you must perform in-place upgrade. You cannot perform upgrade with migration if you are updating Site Recovery Manager 5.8 to a 5.8.x update release or to a 5.8.x.x patch release.

When you upgrade an existing version of Site Recovery Manager Server, the Site Recovery Manager installer reuses information about vCenter Server connections, certificates, and database configuration from the existing installation. The installer populates the text boxes in the installation wizard with the values from the previous installation.

To change installation information, for example, database connections, the authentication method, certificate location, or administrator credentials, you must run the installer in modify mode after you upgrade an existing Site Recovery Manager Server.

If existing configuration information is invalid for the upgrade, the upgrade fails. For example, the upgrade fails if the database is not accessible at the same DSN, or if vCenter Server is not accessible at the same port.

You cannot change the vCenter Server instance to which Site Recovery Manager connects. To connect to a different vCenter Server instance, you must install a new Site Recovery Manager Server.

If you are using credential-based authentication, you receive prompts to accept the vCenter Server certificate during the installation. If you are using certificate-based authentication, you do not receive a prompt to accept the certificate.

If you are updating an existing Site Recovery Manager 5.8 release to a 5.8.x update release or to a 5.8.x.x patch release, not all of the steps in the procedure apply.

Important If you created custom permissions that you assigned to the previous Site Recovery Manager instance, you must upgrade the Site Recovery Manager Server with migration. If you upgrade the Site Recovery Manager Server without migration, custom permissions are lost. See Upgrade Site Recovery Manager Server with Migration.

Prerequisites

- You completed the tasks in Prepare for Site Recovery Manager Upgrade.
- Log in to the Site Recovery Manager host machine to upgrade. Log in using an account with sufficient privileges. This is often an Active Directory domain administrator, but can also be a local administrator.
- Download the Site Recovery Manager installation file to a folder on the Site Recovery Manager Server host.
- If you use an SQL Server database with Integrated Windows Authentication as the Site Recovery Manager database, use the same user account or an account with the same privileges when you upgrade Site Recovery Manager Server as you used when you created the Integrated Windows Authentication data source name (DSN) for SQL Server.

Procedure

1. Double-click the Site Recovery Manager installer, select an installation language, and click **OK**.
2. Follow the installer prompts to accept the license agreement, and verify that you satisfied the installation prerequisites.
3. Choose where to install Site Recovery Manager Server, and click **Next**.
   - Keep the default destination folder.
   - Click **Change** to change the destination folder, and select a target volume.

   The default installation folder for Site Recovery Manager is `C:\Program Files\VMware\VMware vCenter Site Recovery Manager`. If you use a different folder, the pathname cannot be longer than 120 characters including the end slash, and cannot include non-ASCII characters.
4. Provide the user name and password for vCenter Server and click **Next**.
5. Verify the Administrator E-mail and Local Host values and click **Next**.
6. Select an authentication method and click **Next**.

   Important You must use the same authentication method on both sites. If you attempt to use credential-based authentication on one site and certificate-based authentication on the other, site pairing fails.

Option	Description
Authenticate with vCenter Server by using credential-based authentication with an automatically generated certificate	a Select **Automatically generate certificate** and click **Next**. b Enter text values for your organization and organization unit, typically your company name and the name of your group in the company. c Click **Next**.
Authenticate with vCenter Server by using a custom certificate	a Select **Load a certificate file** and click **Next**. b Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. c Enter the certificate password. d Click **Next**.

7. Enter the user name and password for the database, and click **Next**.
8. Select **Use existing database** and click **Next**.

   Caution If you select **Recreate the database**, the installer overwrites the existing database and you lose all configuration information from the previous installation.

9 Select the user account under which to run the Site Recovery Manager Server service.

- Select **Use Local System Account** to run the Site Recovery Manager Server service under the Local System account.
- Enter the username and password of an existing LDAP user account to run the Site Recovery Manager Server service under a different user account. This can be any user account, including local users, that is a member of the built-in Administrators group.

This option is not available if you use an SQL Server database with Integrated Windows Authentication. In this case, the Site Recovery Manager Server service runs under the account that you use to install Site Recovery Manager.

10 Click **Install**.

11 When the installation is finished, click **Finish**.

What to do next

Repeat the procedure to upgrade the Site Recovery Manager Server on the other Site Recovery Manager site.

Log in to vSphere Web Client, or if you are already connected to vSphere Web Client, log out of vSphere Web Client and log in again. The Site Recovery Manager extension appears in vSphere Web Client.

Note If you are updating an existing Site Recovery Manager 5.8.x installation, you might need to clear the browser cache for the update to appear in vSphere Web Client. You might also see RPC fault errors when you log into vSphere Web Client for the first time after the update. Logging out of vSphere Web Client and logging in again removes the errors.

Select **Site Recovery > Sites > *Site* > Summary** in the vSphere Web Client to verify that the build numbers for Site Recovery Manager Server and the Site Recovery Manager plugin reflect the upgrade.

Upgrade Site Recovery Manager Server with Migration

You can upgrade Site Recovery Manager and migrate Site Recovery Manager Server to a different host than the previous Site Recovery Manager Server installation.

To upgrade Site Recovery Manager and keep Site Recovery Manager Server on the same host as the previous installation, see In-Place Upgrade of Site Recovery Manager Server.

To upgrade Site Recovery Manager and migrate Site Recovery Manager Server to a different host, you create a new Site Recovery Manager Server installation on the new host, and connect it to the Site Recovery Manager database from the previous installation. You can uninstall the old Site Recovery Manager Server installation.

If you are using credential-based authentication, you receive prompts to accept the vCenter Server certificate during the installation. If you are using certificate-based authentication, you do not receive a prompt to accept the certificate.

Note You cannot perform upgrade with migration if you are updating Site Recovery Manager 5.8 to a 5.8.x update release or to a 5.8.x.x patch release. To upgrade Site Recovery Manager 5.8 to a 5.8.x update release or to a 5.8.x.x patch release, see In-Place Upgrade of Site Recovery Manager Server.

Prerequisites

- You completed the tasks in Prepare for Site Recovery Manager Upgrade.
- Log in to the Site Recovery Manager host machine to upgrade. Log in using an account with sufficient privileges. This is often an Active Directory domain administrator, but can also be a local administrator.
- Log in to the host machine on which to install the new version of Site Recovery Manager Server.
- Create a 64-bit ODBC system data source name (DSN) on the new host machine to connect to the existing Site Recovery Manager database that you used with the previous version. For information about creating an ODBC DSN, see Create an ODBC System DSN for Site Recovery Manager.
- If you use an SQL Server database with Integrated Windows Authentication as the Site Recovery Manager database, you must use the same user account or an account with the same privileges when you upgrade Site Recovery Manager Server as you used when you created the Integrated Windows Authentication DSN for SQL Server.
- Download the Site Recovery Manager installation file to a folder on the new Site Recovery Manager Server host.

Procedure

1. Stop the Site Recovery Manager Server service on the old Site Recovery Manager Server host.
2. On the host on which to install the new version of Site Recovery Manager Server, double-click the Site Recovery Manager installer icon, select an installation language, and click **OK**.
3. Follow the installer prompts to accept the license agreement, and verify that you satisfied the installation prerequisites.
4. Choose where to install Site Recovery Manager Server, and click **Next**.
   - Keep the default destination folder.
   - Click **Change** to change the destination folder, and select a target volume.

   The default installation folder for Site Recovery Manager is `C:\Program Files\VMware\VMware vCenter Site Recovery Manager`. If you use a different folder, the pathname cannot be longer than 120 characters including the end slash, and cannot include non-ASCII characters.

5 Enter information about the upgraded vCenter Server instance that you used with the previous Site Recovery Manager Server installation and click **Next**.

Option	Action
vCenter Server Address	Enter the host name or IP address of vCenter Server. Enter the host name in lowercase letters. After installation is complete and you are configuring the connection between the protected and recovery sites, supply this host name or IP address exactly as you enter it here, because it is subject to case-sensitive comparisons. **Important** Note the address format that you use to connect Site Recovery Manager to vCenter Server. You must use the same address format when you later pair the Site Recovery Manager sites. If you use an IP address to connect Site Recovery Manager to vCenter Server, you must use this IP address when pairing the Site Recovery Manager sites. If you use certificate-based authentication, the address of Site Recovery Manager Server must be the same as the Subject Alternative Name (SAN) value of the Site Recovery Manager certificate. This is usually the fully qualified domain name of the Site Recovery Manager Server host.
vCenter Server Port	Accept the default or enter a new value if vCenter Server uses a different port.
vCenter Server Username	Enter the user name of an administrator of the specified vCenter Server instance. If you use auto-generated certificates, Site Recovery Manager Server uses the username and password that you specify here to authenticate with vCenter Server whenever you connect to Site Recovery Manager. If you use custom certificates, only the Site Recovery Manager installer uses this account to register Site Recovery Manager with vCenter Server during installation.
vCenter Server Password	Enter the password for the specified user name. The password text box cannot be empty.

6 Enter information with which to register the Site Recovery Manager with vCenter Server, and click **Next**.

Option	Description
Local Site Name	A name for this Site Recovery Manager site, that appears in the Site Recovery Manager interface. A suggested name is generated, but you can enter any name. It cannot be the same name that you use for another Site Recovery Manager installation with which this one will be paired.
Administrator E-mail	Email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.
Local Host	Name or IP address of the local host. The Site Recovery Manager installer obtains this value. Only change it if it is incorrect. For example, the local host might have more than one network interface and the one that the Site Recovery Manager installer detects is not the interface you want to use. If you use certificate-based authentication, the **Local Host** value must be the same as the SAN value of the supplied certificate. This is usually the fully qualified domain name of the Site Recovery Manager Server host.

Option	Description
Listener Ports	SOAP and HTTP port numbers to use.
API Listener Port	SOAP port number for API clients to use.

The Site Recovery Manager installer supplies default values for the listener ports. Do not change them unless the defaults would cause port conflicts.

7 Select the default Site Recovery Manager plug-in identifier, or create a plug-in identifier for this Site Recovery Manager Server pair, and click **Next**.

You can install Site Recovery Manager in a shared recovery site configuration, in which multiple protected sites recover to a single recovery site.

Option	Description	
Default SRM Plug-in Identifier	Installs Site Recovery Manager in a standard configuration with one protected site and one recovery site.	
Custom SRM Plug-in Identifier	Installs Site Recovery Manager in a shared recovery site configuration, with multiple protected sites and one recovery site. Enter the details of the plug-in identifier.	
	Plug-in ID	A unique identifier. Assign the same identifier to the Site Recovery Manager Server instances on the protected site and the shared recovery site.
	Organization	The name of the organization to which this Site Recovery Manager Server pair belongs. This name helps to identify to Site Recovery Manager Server pairs in a shared recovery site configuration, especially when multiple organizations use the shared recovery site.
	Description	An optional description of this Site Recovery Manager Server pair.

8 Click **Yes** to confirm that you want to overwrite the existing Site Recovery Manager extension on this vCenter Server instance.

9 Select an authentication method and click **Next**.

Important You must use the same authentication method on both sites. If you attempt to use credential-based authentication on one site and certificate-based authentication on the other, site pairing fails.

Option	Description
Authenticate with vCenter Server by using credential-based authentication with an automatically generated certificate	a Select **Automatically generate certificate** and click **Next**. b Enter text values for your organization and organization unit, typically your company name and the name of your group in the company. c Click **Next**.
Authenticate with vCenter Server by using a custom certificate	a Select **Load a certificate file** and click **Next**. b Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. c Enter the certificate password. d Click **Next**.

10 Select **Use a custom database server**, select a 64-bit DSN that connects to the Site Recovery Manager database that you used with the previous installation, click **Next**, and provide the database connection information.

Option	Action
Username	Enter a valid user name for the specified database. If you use Integrated Windows Authentication, this option is not available.
Password	Enter the password for the specified user name. If you use Integrated Windows Authentication, this option is not available.
Connection Count	Enter the initial connection pool size. In most cases, it is not necessary to change this setting. Before changing this setting, consult with your database administrator.
Max Connections	Enter the maximum number of database connections that can be open simultaneously. In most cases, it is not necessary to change this setting. Before changing this setting consult with your database administrator.

11 Select **Use existing database** and click **Next**.

Caution If you select **Recreate the database**, the installer overwrites the existing database and you lose all configuration information from the previous installation.

12 Select the user account under which to run the Site Recovery Manager Server service.

- Select **Use Local System Account** to run the Site Recovery Manager Server service under the Local System account.
- Enter the username and password of an existing LDAP user account to run the Site Recovery Manager Server service under a different user account. This can be any user account, including local users, that is a member of the built-in Administrators group.

This option is not available if you use an SQL Server database with Integrated Windows Authentication. In this case, the Site Recovery Manager Server service runs under the account that you use to install Site Recovery Manager.

13 Click **Install**.

14 When the installation is finished, click **Finish**.

What to do next

Repeat the procedure to upgrade the Site Recovery Manager Server on the other Site Recovery Manager site.

Log in to vSphere Web Client, or if you are already connected to vSphere Web Client, log out of vSphere Web Client and log in again. The Site Recovery Manager extension appears in vSphere Web Client.

Note If you are updating an existing Site Recovery Manager 5.8.x installation, you might need to clear the browser cache for the update to appear in vSphere Web Client. You might also see RPC fault errors when you log into vSphere Web Client for the first time after the update. Logging out of vSphere Web Client and logging in again removes the errors.

Configure and Verify the Upgraded Site Recovery Manager Installation

You must configure the upgraded components to establish a working Site Recovery Manager installation.

If you use array-based replication, you must check that your storage replication adapters (SRAs) are compatible with this version of Site Recovery Manager. Depending on the type of storage that you use, you might need to reinstall the SRAs.

If you use vSphere Replication and you upgraded vSphere Replication to the correct version, no additional configuration is required other than verifying your connections, protection groups, and recovery plans.

Prerequisites

- You upgraded vCenter Server and Site Recovery Manager.
- If you use array-based replication, check the availability of an SRA for your type of storage by consulting the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.

- Download the SRA by going to https://my.vmware.com/web/vmware/downloads, selecting **VMware vCenter Site Recovery Manager > Download Product**, then selecting **Drivers & Tools > Storage Replication Adapters > Go to Downloads**.
- If you obtain an SRA from a different vendor site, verify that it has been certified for the Site Recovery Manager release you are using by checking the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.
- Connect to the vSphere Web Client on both of the sites.

Procedure

1. In the vSphere Web Client client, select **Site Recovery > Sites**, right-click a site and select **Reconfigure Pairing** to reconfigure the connection between the Site Recovery Manager sites.
2. If you use array-based replication, select **Site Recovery > Array Based Replication** and check the status of the array pairs.
3. If array managers are in the `Error` state, uninstall the SRAs, install the new version, and rescan the SRAs on the Site Recovery Manager Server hosts that you upgraded.

   You must perform these tasks on both sites.

   a. Log in to the Site Recovery Manager Server host machine on each site.

   b. Uninstall the SRAs that are in the `Error` state.

   c. Reinstall the SRAs with the SRA version that corresponds to this version of Site Recovery Manager.

   d. In the vSphere Web Client client for each site, select **Site Recovery > Sites**, right-click a site and select **Rescan SRAs**.
4. If you use array-based replication, reenter the login credentials for the array managers.

   a. Select **Site Recovery > Array Based Replication**, right-click an array manager and select **Edit Array Manager**.

   b. Follow the prompts to the Configure array manager page, and enter the username and password for the array.

   c. Follow the prompts to complete the reconfiguration of the array manager.
5. Select **Site Recovery > Protection Groups** and **Site Recovery > Recovery Plans** and verify that your protection groups and recovery plans from the previous version are present.
6. In **Site Recovery > Recovery Plans**, run a test on each of your recovery plans.

Revert to a Previous Release of Site Recovery Manager

To revert to a previous release of Site Recovery Manager, you must uninstall Site Recovery Manager from the protected and recovery sites. You can then reinstall the previous release.

Prerequisites

- Verify that your installation of vCenter Server supports the Site Recovery Manager release that you are reverting to. For information about the vCenter Server releases that support other versions of Site Recovery Manager, see the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html. For information about reverting a vCenter Server installation, see the vSphere documentation.
- Verify that you made a backup of the Site Recovery Manager database before you upgraded Site Recovery Manager from a previous release to this release.

Procedure

1. Use the Windows Control Panel options to uninstall Site Recovery Manager at the protected and recovery sites.

   If you connected the Site Recovery Manager Server instances at the protected and recovery sites, you must uninstall Site Recovery Manager at both sites. If you uninstall Site Recovery Manager from one side of a site pairing but not the other, the database on the remaining site becomes inconsistent.
2. Restore the Site Recovery Manager database from the backup that you made when you upgraded Site Recovery Manager from the previous release.

   You must restore the database on both sites so they are synchronized. For instructions about how to restore a database from a backup, see the documentation from your database vendor.
3. Install the previous release of Site Recovery Manager Server on the protected and recovery sites.
4. Install the corresponding release of the Site Recovery Manager client plug-in on any vSphere Client instances that you use to connect to Site Recovery Manager.
5. Reestablish the connection between the Site Recovery Manager Server instances on the protected and recovery sites.

If you restored a backup of the Site Recovery Manager database from the previous version, any configurations or protection plans that you created before you upgraded Site Recovery Manager are retained.

Creating Site Recovery Manager Placeholders and Mappings

7

When you use Site Recovery Manager to configure the protection for virtual machines, you reserve resources on the recovery site by creating placeholders. You map the resources of the protected virtual machines to resources on the recovery site.

- About Placeholder Virtual Machines

  When you add a virtual machine or template to a protection group, Site Recovery Manager creates a placeholder virtual machine at the recovery site.

- About Inventory Mappings

  You must create inventory mappings so that Site Recovery Manager can create placeholder virtual machines.

- About Placeholder Datastores

  For every virtual machine in a protection group, Site Recovery Manager creates a placeholder virtual machine at the recovery site. You must identify a datastore on the recovery site in which Site Recovery Manager can store the placeholder virtual machines.

About Placeholder Virtual Machines

When you add a virtual machine or template to a protection group, Site Recovery Manager creates a placeholder virtual machine at the recovery site.

Site Recovery Manager reserves a place for protected virtual machines in the inventory of the recovery site by creating a subset of virtual machine files. Site Recovery Manager uses that subset of files as a placeholder to register a virtual machine with vCenter Server on the recovery site. The presence of placeholder in the recovery site inventory provides a visual indication to Site Recovery Manager administrators that the virtual machines are protected. The placeholders also indicate to vCenter Server administrators that the virtual machines can power on and start consuming local resources when Site Recovery Manager tests or runs a recovery plan.

When you recover a protected virtual machine by testing or running a recovery plan, Site Recovery Manager replaces its placeholder with the recovered virtual machine and powers it on according to the settings of the recovery plan. After a recovery plan test finishes, Site Recovery Manager restores the placeholders and powers off the virtual machines as part of the cleanup process.

About Placeholder Virtual Machine Templates

When you protect a template on the protected site, Site Recovery Manager creates the placeholder template by creating a virtual machine in the default resource pool of a compute resource and then by marking that virtual machine as a template. Site Recovery Manager selects the compute resource from the set of available compute resources in the datacenter on the recovery site to which the folder of the virtual machine on the protected site is mapped. All the hosts in the selected compute resource must have access to at least one placeholder datastore. At least one host in the compute resource must support the hardware version of the protected virtual machine template.

About Inventory Mappings

You must create inventory mappings so that Site Recovery Manager can create placeholder virtual machines.

Inventory mappings provide a convenient way to specify how Site Recovery Manager maps virtual machine resources at the protected site to resources at the recovery site. Site Recovery Manager applies these mappings to all members of a protection group when you create the group. You can reapply mappings whenever necessary, for example when you add new members to a group.

Site Recovery Manager does not enforce an inventory mapping requirement. If you create a protection group without defining inventory mappings, you must configure each protected virtual machine individually or use the Configure All option. Site Recovery Manager cannot protect a virtual machine unless it has valid inventory mappings for key virtual machine resources.

- Networks
- Folders
- Compute resources
- Placeholder datastores

After you configure mappings at the protected site when you configure protection, configure inventory mappings at the recovery site to enable reprotect.

When Site Recovery Manager creates a placeholder virtual machine, Site Recovery Manager derives its folder and compute resource assignments from inventory mappings that you establish at the protected site. A vCenter Server administrator at the recovery site can modify folder and compute resource assignments as necessary.

Configuring Inventory Mappings for Individual Virtual Machines

You can configure mappings for individual virtual machines in a protection group. If you create inventory mappings for a site, you can override them by configuring the protection of individual virtual machines. If you must override inventory mappings for some members of a protection group, use the vSphere Client to connect to the recovery site, and edit the settings of the placeholder virtual machines or move them to a different folder or resource pool.

Changing Inventory Mappings

If you change existing inventory mappings for a site, the changes do not affect virtual machines that Site Recovery Manager already protects. Site Recovery Manager only applies the new mappings to newly added virtual machines or if you repair a lost placeholder for a particular virtual machine.

Because placeholder virtual machines do not support NICs, you cannot change the network configurations of placeholder virtual machines. You can only change the network for a placeholder virtual machine in the inventory mappings. If no mapping for a network exists, you can specify a network when you configure protection for an individual virtual machine. Changes that you make to the placeholder virtual machine override the settings that you establish when you configure the protection of the virtual machine. Site Recovery Manager preserves these changes at the recovery site during the test and recovery.

How Site Recovery Manager Applies Mappings During Reprotect

During reprotect, Site Recovery Manager converts the virtual machines from the original protected site into placeholders, to protect the recovered virtual machines that were formerly the placeholder virtual machines on the recovery site. In most cases, the previously protected virtual machines and their devices are used during reprotect. If you add devices to a virtual machine after the virtual machine is recovered, or if original protected virtual machines are deleted, Site Recovery Manager uses mappings during reprotect.

Select Inventory Mappings

Inventory mappings provide default resources, folders, and networks for virtual machines to use when Site Recovery Manager creates placeholder virtual machines on the recovery site.

Unless you intend to configure mappings individually for each virtual machine in a protection group, configure inventory mappings for a site before you create protection groups.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.

2 On the **Manage** tab, select the type of resource to configure.

Option	Action
Network Mappings	Map networks on the protected site to networks on the recovery site.
Folder Mappings	Map datacenters or virtual machine folders on the protected site to datacenters or virtual machine folders on the recovery site.
Resource Mappings	Map resource pools, standalone hosts, vApps, or clusters on the protected site to resource pools, standalone hosts, vApps, or clusters on the recovery site. You can map any type of resource on one site to any type of resource on the other site. **Note** You cannot map individual hosts that are part of clusters to other resource objects.

3 Click the icon to create a new mapping.

4 Expand the inventory items on the left to select a resource on the local site.

5 Expand the inventory items on the right to select a resource on the remote site to which to map the resource that you selected on the local site.

   You can map multiple items on the local site to a single item on the remote site. You can select only one item at a time on the remote site.

6 Click **Add mappings**.

7 (Optional) Repeat Step 4 through Step 6 to map other resources of the same type from the local site to the remote site.

8 (Optional) Select the **Create reverse mappings** check box for each mapping.

   Selecting this option creates corresponding mappings from the item on the remote site to the item on the local site. You require reverse mappings to establish bidirectional protection and to run reprotect operations. You cannot select this option if two or more mappings have the same target on the remote site.

9 Click **OK** to create the mappings.

10 Repeat Step 2 through Step 9 to establish mappings for the remaining resource types.

About Placeholder Datastores

For every virtual machine in a protection group, Site Recovery Manager creates a placeholder virtual machine at the recovery site. You must identify a datastore on the recovery site in which Site Recovery Manager can store the placeholder virtual machines.

After you select the datastore to contain the placeholder virtual machines, Site Recovery Manager reserves a place for protected virtual machines in the inventory on the recovery site. Site Recovery Manager creates a set of virtual machine files on the specified datastore at the recovery site and uses that subset to register the placeholder virtual machine with vCenter Server on the recovery site.

To enable planned migration and reprotect, you must select placeholder datastores at both sites.

Placeholder datastores must meet certain criteria.

- For clusters, the placeholder datastores must be visible to all of the hosts in the cluster.
- You cannot select replicated datastores as placeholder datastores.

Configure a Placeholder Datastore

You must specify a placeholder datastore for Site Recovery Manager to use to store placeholder virtual machines on the recovery site.

You must configure a placeholder datastore on both sites in the pair to establish bidirectional protection and reprotect.

Prerequisites

Verify that you connected and paired the protected and recovery sites.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.
2. On the **Manage** tab, click **Placeholder Datastores**.
3. Click the icon to configure a placeholder datastore.
4. Select a datastore to designate as the location for placeholder virtual machines on the local site, and click **OK**.

   Previously configured datastores appear but you cannot select them. If a datastore is replicated, but Site Recovery Manager does not have an array manager for that datastore, the option to select the replicated datastore might be available. Do not select replicated datastores that Site Recovery Manager does not manage.

   Important If you use vSphere Replication, do not select a placeholder datastore that you already use as the target datastore for replications. Selecting the same datastore for placeholder virtual machines as you use to contain the replica virtual machines that vSphere Replication creates can cause problems when you run reprotect.
5. Select the other site in the pair.
6. Repeat Step 2 to Step 4 to configure a placeholder datastore on the other site.

Installing Site Recovery Manager to Use with a Shared Recovery Site

8

With Site Recovery Manager, you can connect multiple protected sites to a single recovery site. The virtual machines on the protected sites all recover to the same recovery site. This configuration is known as a shared recovery site, a many-to-one, or an N:1 configuration.

In the standard one-to-one Site Recovery Manager configuration, you use Site Recovery Manager to protect a specific instance of vCenter Server by pairing it with another vCenter Server instance. The first vCenter Server instance, the protected site, recovers virtual machines to the second vCenter Server instance, the recovery site.

Another example is to have multiple protected sites that you configure to recover to a single, shared recovery site. For example, an organization can provide a single recovery site with which multiple protected sites for remote field offices can connect. Another example for a shared recovery site is for a service provider that offers business continuity services to multiple customers.

In a shared recovery site configuration, you install one Site Recovery Manager Server instance on each protected site, each of which connects to a different vCenter Server instance. On the recovery site, you install multiple Site Recovery Manager Server instances to pair with each Site Recovery Manager Server instance on the protected sites. All of the Site Recovery Manager Server instances on the shared recovery site connect to a single vCenter Server instance. Each Site Recovery Manager Server instance in a pair must have the same Site Recovery Manager extension ID, which you can set when you install Site Recovery Manager Server. You can consider the owner of a Site Recovery Manager Server pair to be a customer of the shared recovery site.

You can convert an existing one-to-one configuration of Site Recovery Manager into a shared recovery site configuration. To convert a one-to-one configuration to a shared recovery site configuration, you deploy additional Site Recovery Manager Server and vCenter Server instances as protected sites, and pair them with additional Site Recovery Manager Server instances that all connect to the existing vCenter Server instance on the recovery site. Each pair of Site Recovery Manager Server instances in the shared recovery site configuration must use a different Site Recovery Manager extension ID. For example, if you installed a one-to-one configuration that uses the default Site Recovery Manager extension ID, you must deploy all subsequent Site Recovery Manager Server pairs with different custom extension IDs.

You can use either array-based replication or vSphere Replication or a combination of both when you configure Site Recovery Manager Server to use a shared recovery site.

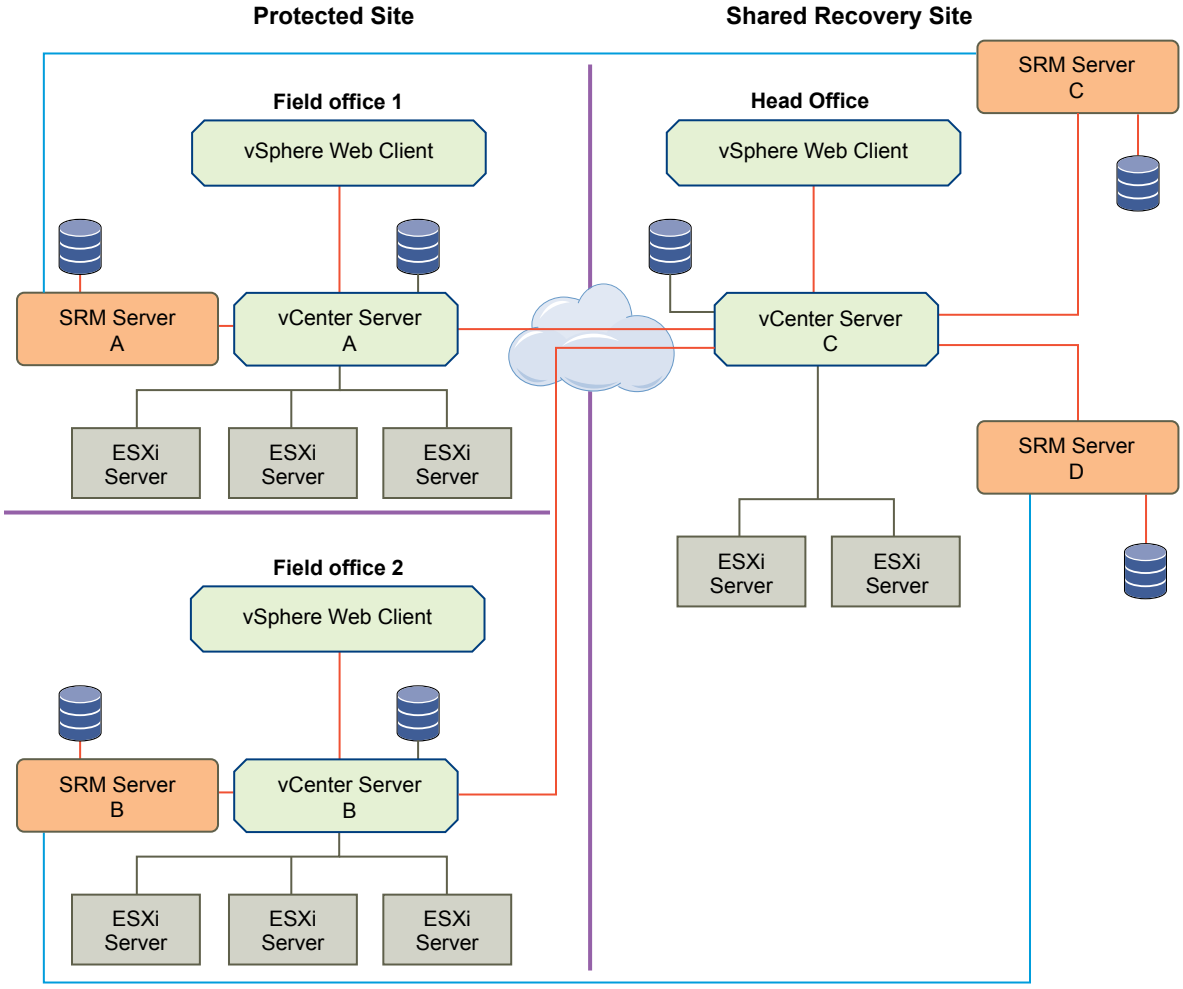
In addition to the shared recovery site configuration, Site Recovery Manager also allows and supports shared protected site (1:N) and many-to-many (N:N) configurations.

Example: Using Site Recovery Manager with Multiple Protected Sites and a Shared Recovery Site

An organization has two field offices and a head office. Each of the field offices is a protected site. The head office acts as the recovery site for both of the field offices. Each field office has a Site Recovery Manager Server instance and a vCenter Server instance. The head office has two Site Recovery Manager Server instances, each of which is paired with a Site Recovery Manager Server instance in one of the field offices. Both of the Site Recovery Manager Server instances at the head office extend a single vCenter Server instance.

- Field office 1
  - Site Recovery Manager Server A
  - vCenter Server A
- Field office 2
  - Site Recovery Manager Server B
  - vCenter Server B
- Head office
  - Site Recovery Manager Server C, that is paired with Site Recovery Manager Server A
  - Site Recovery Manager Server D, that is paired with Site Recovery Manager Server B
  - vCenter Server C, that is extended by Site Recovery Manager Server C and Site Recovery Manager Server D

Figure 8-1. Example of Using Site Recovery Manager in a Shared Recovery Site Configuration



- Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration

  When you configure Site Recovery Manager to use a shared recovery site, Site Recovery Manager supports the same operations as it does in a standard one-to-one configuration. Using Site Recovery Manager with a shared recovery site is subject to some limitations.

- Site Recovery Manager Licenses in a Shared Recovery Site Configuration

  If you configure Site Recovery Manager to use with a shared recovery site, you can assign licenses individually on the shared recovery site. You can also share a license between all Site Recovery Manager Server instances on the shared recovery site.

- Install Site Recovery Manager In a Shared Recovery Site Configuration

  To install Site Recovery Manager in a shared recovery site configuration, you deploy Site Recovery Manager Server on one or more protected sites, and deploy a corresponding number of Site Recovery Manager Server instances on the shared recovery site.

- Upgrade Site Recovery Manager in a Shared Recovery Site Configuration

  You can upgrade existing Site Recovery Manager installations that use a shared recovery site.

Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration

When you configure Site Recovery Manager to use a shared recovery site, Site Recovery Manager supports the same operations as it does in a standard one-to-one configuration. Using Site Recovery Manager with a shared recovery site is subject to some limitations.

- Site Recovery Manager supports point-to-point replication. Site Recovery Manager does not support replication to multiple targets, even in a multi-site configuration.
- For each shared recovery site customer, you must install Site Recovery Manager Server once at the customer site and again at the recovery site.
- You must specify the same Site Recovery Manager extension ID when you install the Site Recovery Manager Server instances on the protected site and on the shared recovery site. For example, you can install the first pair of sites with the default Site Recovery Manager extension ID, then install subsequent pairs of sites with custom extension IDs.
- You must install each Site Recovery Manager Server instance at the shared recovery site on its own host machine. You cannot install multiple instances of Site Recovery Manager Server on the same host machine.
- Each Site Recovery Manager Server instance on the protected site and on the shared recovery site requires its own database.
- Both sites must use the same authentication method. For information about authentication methods, see Chapter 4 Site Recovery Manager Authentication.
- A single shared recovery site can support a maximum of ten protected sites. You can run concurrent recoveries from multiple sites. See http://kb.vmware.com/kb/2081866 for the number of concurrent recoveries that you can run with array-based replication and with vSphere Replication.
- In a large Site Recovery Manager environment, you might experience timeout errors when powering on virtual machines on a shared recovery site. See Timeout Errors when Powering on Virtual Machines on a Shared Recovery Site.
- When connecting to Site Recovery Manager on the shared recovery site, every customer can see all of the Site Recovery Manager extensions that are registered with the shared recovery site, including company names and descriptions. All customers of a shared recovery site can have access to other customers' folders and potentially to other information at the shared recovery site.

Timeout Errors when Powering on Virtual Machines on a Shared Recovery Site

In a large Site Recovery Manager environment, you might encounter timeout errors when powering on virtual machines on a shared recovery site.

Problem

When you power on virtual machines on a shared recovery site, you see the error message `Error:Operation timed out:900 seconds`.

Cause

This problem can occur if a single vCenter Server instance manages a large number of virtual machines on the shared recovery site, for example 1000 or more.

Solution

1. Go to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` on the Site Recovery Manager Server host machine on the recovery site.
2. Open `vmware-dr.xml` in a text editor.
3. Increase the default `RemoteManager` timeout value.

   The default timeout value is 900 seconds (15 minutes). Increase the timeout to, for example, 1800 seconds (30 minutes).

   ```
   <RemoteManager>
     <DefaultTimeout>1800</DefaultTimeout>
   </RemoteManager>
   ```

4. Set the timeout for reading from the vSphere Web Client.

   Set the timeout to 900 seconds (15 minutes) by adding a line to the `<vmacore><http>` element.

   ```
   <vmacore>
     <http>
       <defaultClientReadTimeoutSeconds>900</defaultClientReadTimeoutSeconds>
     </http>
   </vmacore>
   ```

5. Restart the Site Recovery Manager Server service.

What to do next

If you still experience timeouts after increasing the `RemoteManager` timeout value, experiment with progressively longer timeout settings. Do not increase the timeout period excessively. Setting the timeout to an unrealistically long period can hide other problems, for example problems related to communication between Site Recovery Manager Server and vCenter Server or other services that Site Recovery Manager requires.

Site Recovery Manager Licenses in a Shared Recovery Site Configuration

If you configure Site Recovery Manager to use with a shared recovery site, you can assign licenses individually on the shared recovery site. You can also share a license between all Site Recovery Manager Server instances on the shared recovery site.

In a shared recovery site configuration, you install Site Recovery Manager license keys on each of the protected sites to enable recovery. You can install the same license key on the shared recovery site and assign it to the partner Site Recovery Manager Server instance to enable bidirectional operation, including reprotect. You can use the same license key for both Site Recovery Manager Server instances in the Site Recovery Manager pair, in the same way as for a one-to-one configuration.

Alternatively, you can install one Site Recovery Manager license key on the shared recovery site. All Site Recovery Manager Server instances on the shared recovery site share this license. In this configuration, you must ensure that you have sufficient licenses for the total number of virtual machines that you protect on the shared recovery site, for all protected sites.

Example: Sharing Site Recovery Manager Licenses on a Shared Recovery Site

You connect two protected sites to a shared recovery site. You install a single Site Recovery Manager license on the shared recovery site.

- If you protect 20 virtual machines on protected site A, you require a license for 20 virtual machines on protected site A to recover these virtual machines to the shared recovery site.
- If you protect 10 virtual machines on protected site B, you require a license for 10 virtual machines on protected site B to recover these virtual machines to the shared recovery site.
- You share a Site Recovery Manager license for 25 virtual machines between two Site Recovery Manager Server instances, C and D, on the shared recovery site. The Site Recovery Manager Server instances on sites A and B connect to Site Recovery Manager Server instances C and D respectively.

Because you have a license for 25 virtual machines on the shared recovery site, the total number of virtual machines for which you can perform reprotect after a recovery is 25. If you recover all of the virtual machines from sites A and B to the shared recovery site and attempt to perform reprotect, you have sufficient licenses to reprotect only 25 of the 30 virtual machines that you recovered. You can reprotect all 20 of the virtual machines from site A to reverse protection from Site Recovery Manager Server C to site A. You can reprotect only 5 of the virtual machines to reverse protection from Site Recovery Manager Server D to site B.

In this situation, you can purchase licenses for more virtual machines for the shared recovery site. Alternatively, you can add the license keys from sites A and B to vCenter Server on the shared recovery site, and assign the license from site A to Site Recovery Manager Server C and the license from site B to Site Recovery Manager Server D.

Install Site Recovery Manager In a Shared Recovery Site Configuration

To install Site Recovery Manager in a shared recovery site configuration, you deploy Site Recovery Manager Server on one or more protected sites, and deploy a corresponding number of Site Recovery Manager Server instances on the shared recovery site.

You can only pair protected and recovery sites that have the same Site Recovery Manager extension ID.

Procedure

1 Use vSphere Replication in a Shared Recovery Site Configuration

You can use vSphere Replication with Site Recovery Manager in a shared recovery site configuration in the same way that you do in a standard one-to-one configuration.

2 Install Site Recovery Manager Server on Multiple Protected Sites to Use with a Shared Recovery Site

You install Site Recovery Manager Server to use with a shared recovery site by running the Site Recovery Manager installer and specifying a Site Recovery Manager ID for the site pair.

3 Install Multiple Site Recovery Manager Server Instances on a Shared Recovery Site

In a shared recovery site configuration, you can install multiple Site Recovery Manager Server instances that all extend the same vCenter Server instance on the shared recovery site.

4 Connect the Site Recovery Manager Sites in a Shared Recovery Site Configuration

In a shared recovery site configuration, you connect the Site Recovery Manager sites in the same way as for a standard one-to-one configuration.

5 Use Array-Based Replication in a Shared Recovery Site Configuration

You can use array-based replication with Site Recovery Manager in a shared recovery site configuration in the same way as you do in a standard one-to-one configuration.

6 Configure Placeholders and Mappings in a Shared Recovery Site Configuration

When you configure placeholders and mappings in a shared recovery site configuration, the customers of the shared recovery site can share the resources on the recovery site. Alternatively, you can assign isolated resources to each customer.

Use vSphere Replication in a Shared Recovery Site Configuration

You can use vSphere Replication with Site Recovery Manager in a shared recovery site configuration in the same way that you do in a standard one-to-one configuration.

You deploy one vSphere Replication appliance on each protected site. You deploy only one vSphere Replication appliance on the shared recovery site. All of the vSphere Replication appliances on the protected sites connect to this single vSphere Replication appliance on the recovery site. You deploy the vSphere Replication appliances in the same way as for a standard one-to-one configuration.

Important Deploy only one vSphere Replication appliance on the shared recovery site. If you deploy multiple vSphere Replication appliances on the shared recovery site, each new vSphere Replication appliance overwrites the registration of the previous vSphere Replication appliance with vCenter Server. This overwrites all existing replications and configurations.

You can deploy multiple additional vSphere Replication servers on the shared recovery site to distribute the replication load. For example, you can deploy on the shared recovery site a vSphere Replication server for each of the protected sites that connects to the shared recovery site. For information about protection and recovery limits when using vSphere Replication with Site Recovery Manager in a shared recovery site configuration, see KB 2081866.

Prerequisites

- To use Site Recovery Manager with vSphere Replication, deploy the appropriate version of vSphere Replication on both of the protected and recovery sites before you install Site Recovery Manager Server. The Site Recovery Manager installer verifies the version of vSphere Replication during installation and stops if it detects an incompatible version. This verification is not performed if you install vSphere Replication after you install Site Recovery Manager Server, which might lead to incompatible versions. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Web Client to stop working. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrixes for vCenter Site Recovery Manager 5.8* at https://www.vmware.com/support/srm/srm-compat-matrix-5-8.html.
- If you have existing vSphere Replication appliances on the sites, you must either upgrade them to the correct version or unregister them from both vCenter Server instances before you install Site Recovery Manager. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Web Client to stop working. See Unregister an Incompatible Version of vSphere Replication.

Procedure

1. Deploy a vSphere Replication appliance on each of the protected sites.
2. Deploy one vSphere Replication appliance on the shared recovery site.
3. (Optional) Deploy additional vSphere Replication servers on the shared recovery site.
4. (Optional) Register the additional vSphere Replication servers with the vSphere Replication appliance on the shared recovery site.

   The vSphere Replication servers become available to all Site Recovery Manager instances on the shared recovery site.

The shared recovery site is ready to receive replicated virtual machines that you recover from the protected sites by using vSphere Replication.

Install Site Recovery Manager Server on Multiple Protected Sites to Use with a Shared Recovery Site

You install Site Recovery Manager Server to use with a shared recovery site by running the Site Recovery Manager installer and specifying a Site Recovery Manager ID for the site pair.

For each protected site, you must install one instance of Site Recovery Manager Server at the protected site and one instance of Site Recovery Manager Server at the recovery site. You can only pair Site Recovery Manager Server instances that have the same Site Recovery Manager extension ID. Each protected site must include its own vCenter Server instance.

Prerequisites

- Download the Site Recovery Manager installation file to a folder on the Site Recovery Manager Server host.

- This information presumes knowledge of the standard procedure for installing Site Recovery Manager. See Install Site Recovery Manager Server for information about a standard Site Recovery Manager installation.

Procedure

1. Double-click the Site Recovery Manager installer, select an installation language, and click **OK**.
2. Follow the prompts to begin the Site Recovery Manager installation.
3. At the SRM Plug-in ID page, select **Custom SRM Plug-in Identifier**, provide information to identify this custom Site Recovery Manager extension, and click **Next**.

Option	Description
SRM ID	Enter a unique identifier for this pair of Site Recovery Manager Server instances. The Site Recovery Manager ID can be a string of up to 29 ASCII characters from the set of ASCII upper- lower-case characters, digits, the underscore, the period, and the hyphen. You cannot use the underscore, period, and hyphen as the first or last characters of the Site Recovery Manager ID, and they cannot appear adjacent to one another.
Organization	Enter a string of up to 50 ASCII characters to specify the organization that created the extension.
Description	Enter a string of up to 50 ASCII characters to provide a description of the extension.

4. Follow the prompts to complete the remainder of the installation.
5. Repeat the procedure on each of the sites to protect.

   Connect each Site Recovery Manager Server to its own vCenter Server instance. Assign a unique Site Recovery Manager ID to each Site Recovery Manager Server.

What to do next

For each Site Recovery Manager Server that you installed on a protected site, install a corresponding Site Recovery Manager Server instance on the shared recovery site.

Install Multiple Site Recovery Manager Server Instances on a Shared Recovery Site

In a shared recovery site configuration, you can install multiple Site Recovery Manager Server instances that all extend the same vCenter Server instance on the shared recovery site.

The Site Recovery Manager Server instances that you install on a shared recovery site each correspond to a Site Recovery Manager Server on a protected site.

Prerequisites

- You created one or more protected sites, each with a Site Recovery Manager Server instance for which you configured a unique Site Recovery Manager ID. Click **Site Recovery > Sites**, select a site and click **Summary** to check the Site Recovery Manager ID of the Site Recovery Manager instance to which you are connecting this instance.

- Download the Site Recovery Manager installation file to a folder on the Site Recovery Manager Server host.
- This information presumes knowledge of the standard procedure for installing Site Recovery Manager. See Install Site Recovery Manager Server for information about a standard Site Recovery Manager installation.

Procedure

1. Double-click the Site Recovery Manager installer, select an installation language, and click **OK**.
2. Follow the prompts to begin the Site Recovery Manager installation.
3. At the **VMware vCenter Site Recovery Manager Plugin Identifier** page of the installer, select **Custom SRM Plugin Identifier** and click **Next**.
4. At the SRM Plug-in ID page, select **Custom SRM Plug-in Identifier**, provide information to identify this Site Recovery Manager extension as the partner of a Site Recovery Manager Server instance on a protected site , and click **Next**.

Option	Description
SRM ID	Enter the same Site Recovery Manager ID as you provided for the corresponding Site Recovery Manager Server instance on the protected site. For example, if you set the Site Recovery Manager ID of the Site Recovery Manager Server instance on the protected site to **`SRM-01`**, set the Site Recovery Manager ID to **`SRM-01`**.
Organization	Enter a string of up to 50 ASCII characters to specify the organization that created the extension.
Description	Enter a string of up to 50 ASCII characters to provide a description of the extension.

5. Follow the prompts to complete the remainder of the installation.

What to do next

Repeat the procedure to install further Site Recovery Manager Server instances on the shared recovery site, each with a Site Recovery Manager ID that matches a Site Recovery Manager Server instance on another protected site. Each additional Site Recovery Manager Server instance that you install on the recovery site connects to the vCenter Server instance.

Connect the Site Recovery Manager Sites in a Shared Recovery Site Configuration

In a shared recovery site configuration, you connect the Site Recovery Manager sites in the same way as for a standard one-to-one configuration.

If you start the site connection from one of the protected sites, Site Recovery Manager uses the Site Recovery Manager ID that you set during installation to connect to the correct Site Recovery Manager Server instance on the recovery site.

If you start the site connection from one of the Site Recovery Manager Server instances on the shared recovery site, and you try to connect to a protected site that has a Site Recovery Manager Server extension with a different Site Recovery Manager ID, the connection fails with an error.

Prerequisites

- You installed Site Recovery Manager Server on one or more protected sites.
- You installed one or more Site Recovery Manager Server instances on a shared recovery site.
- You assigned the same Site Recovery Manager extension ID to a Site Recovery Manager Server instance on a protected site and to a Site Recovery Manager Server instance on the shared recovery site.

Procedure

1. Connect to the vSphere Web Client for a site, click **Site Recovery > Sites**, and select a site.
2. Right-click the site and select **Pair Site**.
3. Enter the address of the vCenter Server on the remote site, enter the vCenter Server username and password, and click **OK**.
   - If you logged in to Site Recovery Manager on a protected site, enter the address of vCenter Server on the shared recovery site.
   - If you logged in to Site Recovery Manager on the shared recovery site, enter the address of vCenter Server on the corresponding protected site. The Site Recovery Manager extension of this vCenter Server instance must have a Site Recovery Manager ID that matches the Site Recovery Manager ID of the Site Recovery Manager instance from which you are connecting.
4. Repeat Step 1 to Step 3 to configure the site pairing for all of the sites that use the shared recovery site.
5. (Optional) In the vSphere Web Client for the shared recovery site, click **Site Recovery > Sites**.

   All of the Site Recovery Manager Server instances that connect to vCenter Server on the shared recovery site appear in the list. All of the Site Recovery Manager Server instances on the protected sites that are paired with instances on the shared recovery site also appear.
6. (Optional) Select a site in the list and click the **Summary** tab to see information about the remote site that this site is paired with.

Use Array-Based Replication in a Shared Recovery Site Configuration

You can use array-based replication with Site Recovery Manager in a shared recovery site configuration in the same way as you do in a standard one-to-one configuration.

To use array-based replication with Site Recovery Manager in a shared recovery site configuration, you must install storage arrays and storage replication adapters (SRA) on each of the protected sites. Each protected site can use a different type of storage array.

Each protected site can either share the same storage on the shared recovery site, or you can allocate storage individually for each protected site. You can use storage from multiple vendors on the shared recovery site, as long as they correspond to storage that you use on the respective protected sites. You must install the appropriate SRA for each type of storage that you use on the shared recovery site.

For information about protection and recovery limits when you use array-based replication with Site Recovery Manager in a shared recovery site configuration, see KB 2081866.

Prerequisites

- You installed Site Recovery Manager in a shared recovery site configuration.
- You connected the protected sites with the shared recovery site.

Procedure

1. Set up storage arrays on the protected sites following the instructions that your storage array provides.
2. Install the appropriate SRAs on Site Recovery Manager Server systems on the protected sites.
3. Install the appropriate SRAs on Site Recovery Manager Server systems on the shared recovery site.
4. Configure the array managers on the protected sites and on the shared recovery sites.
5. Configure the mappings from the resources on the protected sites to resources on the shared recovery site and configure the placeholder datastores.

The shared recovery site is ready to receive replicated virtual machines that you recover from the protected sites by using array-based replication.

Configure Placeholders and Mappings in a Shared Recovery Site Configuration

When you configure placeholders and mappings in a shared recovery site configuration, the customers of the shared recovery site can share the resources on the recovery site. Alternatively, you can assign isolated resources to each customer.

On a shared recovery site, multiple customers share a single vCenter Server instance. In some cases, multiple customers can share a single ESXi host on the recovery site. You can map the resources on the protected sites to shared resources on the shared recovery site. You might share resources on the recovery site if you do not need to keep all of the customers' virtual machines separate, for example if all of the customers belong to the same organization.

You can also create isolated resources on the shared recovery site and map the resources on the protected sites to their own dedicated resources on the shared recovery site. You might use this configuration if you must keep all of the customers' virtual machines separate from each other, for example if all of the customers belong to different organizations.

For information about how to assign permissions to allow users to access the resources on a shared recovery site, see *Site Recovery Manager Administration*.

Prerequisites

- You installed Site Recovery Manager in a shared recovery site configuration.
- You connected the protected sites with the shared recovery site.
- Familiarize yourself with the procedure for configuring placeholders and mappings. For information about configuring placeholders and mappings in a standard configuration, see Chapter 7 Creating Site Recovery Manager Placeholders and Mappings.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Sites**, and select a site.
2. In the **Manage** tab, use the **Network Mappings**, **Folder Mappings**, **Resource Mappings**, and **Placeholder Datastores** tabs to configure the mappings.

Option	Action
Share customer resources	Map the resources, networks, and datastores on the protected sites to a common datacenter, network, and placeholder datastore on the shared recovery site. You can create individual folders for each customer on the recovery site and map the folders on the protected sites to the individual folders.
Isolate customer resources	Map the resources, networks, folders, and datastores on the protected sites to separate datacenters, networks, folders, and placeholder datastores on the shared recovery site.

3. (Optional) If you use vSphere Replication, select the appropriate target datastores for the replica virtual machines when you configure replication.

Option	Action
Share customer resources	Select a common target datastore on the shared recovery site. You can create individual folders in the target datastore for each customer on the recovery site.
Isolate customer resources	Select a different datastore for each customer on the shared recovery site.

Upgrade Site Recovery Manager in a Shared Recovery Site Configuration

You can upgrade existing Site Recovery Manager installations that use a shared recovery site.

When you upgrade a Site Recovery Manager installation that uses a shared recovery site, the same recommendations apply as for upgrading a standard one-to-one installation of Site Recovery Manager. See Chapter 6 Upgrading Site Recovery Manager.

Upgrade all of the protected sites before you upgrade the shared recovery site. When you upgrade all of the protected sites before you upgrade the shared recovery site, you can run recoveries on the shared recovery site if failures occur on a protected site during the upgrade process. If you upgrade vCenter Server on the shared recovery site before you upgrade all of the protected sites, you cannot perform recovery until you complete all of the upgrades.

Upgrade the protected sites in order of importance, upgrading the most important sites first and the least important sites last. For example, upgrade protected sites that run business-critical applications before you upgrade sites that are less vital to your operations.

Prerequisites

- Verify that you know the standard procedure for upgrading Site Recovery Manager. For information about a standard Site Recovery Manager upgrade, see Chapter 6 Upgrading Site Recovery Manager.
- Evaluate the importance of each protected site, and prioritize the upgrade of the sites accordingly.

Procedure

1. Upgrade vCenter Server on the most critical of the protected sites.
2. (Optional) If you use vSphere Replication, upgrade the vSphere Replication appliance that connects to the vCenter Server instance that you upgraded in Step 1.
3. Upgrade the Site Recovery Manager Server instance that connects to the vCenter Server instance that you upgraded in Step 1.
   - If you upgrade Site Recovery Manager Server without migration, the installer obtains from the registry the Site Recovery Manager extension ID that you set during the previous installation. There is no option to modify the Site Recovery Manager extension ID during upgrade.
   - If you upgrade Site Recovery Manager Server with migration, you must specify the same Site Recovery Manager extension ID as you used for the previous installation.
4. (Optional) If you use array-based replication, upgrade the storage replication adapters (SRA) on the Site Recovery Manager Server host machine that you upgraded in Step 3.
5. Repeat Step 1 to Step 4 for each of the protected sites that connect to the shared recovery site.
6. Upgrade vCenter Server on the shared recovery site.
7. (Optional) If you use vSphere Replication, upgrade the vSphere Replication appliance on the shared recovery site.
8. Upgrade the Site Recovery Manager Server instance on the shared recovery site that is paired with the first protected site that you upgraded.
   - If you upgrade Site Recovery Manager Server without migration, the installer obtains from the registry the Site Recovery Manager extension ID that you set during the previous installation. There is no option to modify the Site Recovery Manager extension ID during upgrade.
   - If you upgrade Site Recovery Manager Server with migration, you must specify the same Site Recovery Manager extension ID as you used for the previous installation.
9. (Optional) If you use array-based replication, upgrade the SRAs for this Site Recovery Manager Server instance on the shared recovery site.
10. Repeat Step 8 and Step 9 for each of the remaining Site Recovery Manager Server instances on the shared recovery site.
11. Upgrade the ESXi Server instances on the shared recovery sites and each of the protected sites.

12 Upgrade the virtual hardware and VMware Tools on the virtual machines on the ESXi Server instances.