Site Recovery Manager Installation and Configuration

Site Recovery Manager 6.0

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

Copyright © 2008–2017 VMware, Inc. All rights reserved. Copyright and trademark information.

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-001663-05	■ Updated the information about how to use datastores Configure a Placeholder Datastore. ■ Updated the information about the embedded vPostgreSQL database in Chapter 3 Creating the Site Recovery Manager Database. .
EN-001663-04	Updated Requirements When Using Custom SSL/TLS Certificates with Site Recovery Manager with new requirements for public authority certificates with internal server names.
EN-001663-03	Added that you cannot map individual hosts from clusters to other objects in Select Inventory Mappings.
EN-001663-02	■ Added instruction to check build numbers after upgrade in In-Place Upgrade of Site Recovery Manager Server. ■ Added additional setting to configure for large shared recovery site setups in Timeout Errors when Powering on Virtual Machines on a Shared Recovery Site.
EN-001663-01	■ Added that you cannot mix license types in Site Recovery Manager Licensing. ■ 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. ■ Added that you should take a note of the advanced settings before upgrading in Prerequisites and Best Practices for Site Recovery Manager Upgrade. ■ Added that upgrading from 6.0 to a 6.0.x update release is only possible by in-place upgrade in In-Place Upgrade of Site Recovery Manager Server and Upgrade Site Recovery Manager Server with Migration. ■ 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.
EN-001663-00	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

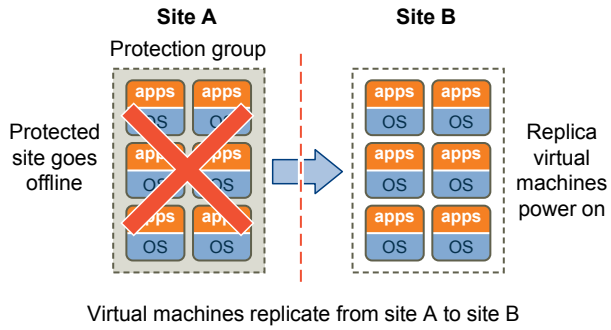
  Some components in the Site Recovery Manager and vCenter Server installations must be identical on each site. Because the protected and recovery sites are often in different physical locations, some components on the protected site can be of a different type to their counterparts on the recovery site.

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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.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 and Platform Services Controller	Must be the same version on both sites. The Site Recovery Manager version must be compatible with the vCenter Server and Platform Services Controller 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.
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. Minimum Site Recovery Manager System Requirements

Component	Requirement
Processor	At least two 2.0GHz or higher Intel or AMD x86 processors. Site Recovery Manager deployments that manage large environments require four 2.0GHz CPUs.
Memory	2GB minimum. You might require more memory if you use the embedded database, as the content of the database grows. The memory requirement increases if Site Recovery Manager manages large environments.
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 deployment and use of Site Recovery Manager and for the management of ESXi hosts.

For information about supported platforms and databases, see the *Compatibility Matrixes for vCenter Site Recovery Manager 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.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, with Platform Services Controller, 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 Shared Platform Services Controller Instances

You can share an external Platform Services Controller across several vCenter Server instances. In this case, you can use the same Site Recovery Manager license on different vCenter Server instances as long as the vCenter Server instances belong to the same Platform Services Controller.

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 6.0 individually or as part of vCloud Suite 6.0. 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 an unlimited number of virtual machines on CPUs that are licensed with vCloud Suite.

Note You cannot mix license types. For example, you cannot protect a certain number of virtual machines by using per-CPU licenses and other virtual machines by using per-VM licenses.

You can combine the features of Site Recovery Manager 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, with Platform Services Controller, 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/2103394.

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 6.0, see http://kb.vmware.com/kb/2105500.

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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.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 an 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 an 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

The Platform Services Controller handles the authentication between Site Recovery Manager and vCenter Server at the vCenter Single Sign-On level.

All communications between Site Recovery Manager and vCenter Server instances take place over transport layer security (TLS) connections. Previous versions of Site Recovery Manager supported both secure sockets layer (SSL) and TLS connections. This version of Site Recovery Manager only supports TLS, due to weaknesses identified in SSL 3.0.

Solution User Authentication

In previous versions of Site Recovery Manager, you used either credential-based authentication or certificate-based authentication to authenticate with vCenter Server. This version of Site Recovery Manager uses solution user authentication to establish secure communication to remote services, such as the Platform Services Controller and vCenter Server. A solution user is a security principal that the Site Recovery Manager installer generates. The installer assigns a private key and a certificate to the solution user and registers it with the vCenter Single Sign-On service. The solution user is tied to a specific Site Recovery Manager instance. You cannot access the solution user private key or certificate. You cannot replace the solution user certificate with a custom certificate.

After installation, you can see the Site Recovery Manager solution user in the Administration view of the vSphere Web Client. Do not attempt to manipulate the Site Recovery Manager solution user. The solution user is for internal use by Site Recovery Manager, vCenter Server, and vCenter Single Sign-On.

During operation, Site Recovery Manager establishes authenticated communication channels to remote services by using certificate-based authentication to acquire a holder-of-key SAML token from vCenter Single Sign-On. Site Recovery Manager sends this token in a cryptographically signed request to the remote service. The remote service validates the token and establishes the identity of the solution user.

Solution Users and Site Recovery Manager Site Pairing

When you pair Site Recovery Manager instances across vCenter Single Sign-On sites that are not federated, Site Recovery Manager creates an additional solution user for the remote site at each site. This solution user for the remote site allows the Site Recovery Manager Server at the remote site to authenticate to services on the local site.

When you pair Site Recovery Manager instances in a federated vCenter Single Sign-On environment, Site Recovery Manager at the remote site uses the same solution user to authenticate to services on the local site.

Site Recovery Manager SSL/TLS Server Endpoint Certificates

Site Recovery Manager requires an SSL/TLS certificate for use as the endpoint certificate for all TLS connections established to Site Recovery Manager. The Site Recovery Manager server endpoint certificate is separate and distinct from the certificate that is generated during the creation and registration of a Site Recovery Manager solution user.

For information about the Site Recovery Manager SSL/TLS endpoint certificate, see Chapter 5 Creating SSL/TLS Server Endpoint Certificates for Site Recovery Manager.

Creating SSL/TLS Server Endpoint Certificates for Site Recovery Manager

5

The Site Recovery Manager server endpoint certificate establishes the identity of Site Recovery Manager Server to clients. The endpoint certificate secures the communication between the client and Site Recovery Manager Server.

During installation of Site Recovery Manager, you can automatically generate an SSL/TLS certificate for use as the Site Recovery Manager endpoint certificate. This is the simpler option that requires minimal user action.

You can also upload a custom SSL/TLS certificate that is signed by a certificate authority. If you use a custom SSL/TLS certificate, the certificate must meet certain requirements to work with Site Recovery Manager.

Note Unlike in previous releases, this version of Site Recovery Manager does not also use custom SSL/TLS certificates to authenticate with vCenter Server. For information about how Site Recovery Manager authenticates with vCenter Server, see Chapter 4 Site Recovery Manager Authentication.

Requirements When Using Custom SSL/TLS Certificates with Site Recovery Manager

If you use custom SSL/TLS certificates for the Site Recovery Manager server endpoint certificate, the certificates must meet specific criteria.

Important Public certificate authorities (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 your public CA before 1st October 2016. Alternatively, use a private CA to issue certificates.

- 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.

Site Recovery Manager uses standard PKCS#12 certificates. Site Recovery Manager places some requirements on the contents of those certificates, but the requirements in this release are less strict than in previous releases of Site Recovery Manager.

- Site Recovery Manager does not accept certificates with MD5 signature algorithms. Use SHA256 or stronger signature algorithms. If you are upgrading an existing Site Recovery Manager installation with which you use MD5 certificates, you must obtain a new certificate with a stronger signature algorithm before you upgrade Site Recovery Manager.
- Site Recovery Manager accepts certificates with SHA1 signature algorithms but these are not recommended and result in a warning during installation. Use SHA256 or stronger signature algorithms.
- The Site Recovery Manager certificate is not the root of a trust chain. It must not be a CA certificate.
- If you use a custom certificate for vCenter Server and Platform Services Controller, you are not obliged to use a custom certificate for Site Recovery Manager, and the reverse.
- The private key in the PKCS #12 file must match the certificate. The minimum length of the private key is 2048-bits.
- The Site Recovery Manager certificate password must not exceed 31 characters.
- The current time must be within the period of validity of the certificate.
- The certificate must be a server certificate, for which the x509v3 Extended Key Usage must indicate TLS Web Server Authentication.
  - The certificate must include an `extendedKeyUsage` or `enhancedKeyUsage` attribute, the value of which is `serverAuth`.
  - Unlike in previous releases, there is no requirement for the certificate to also be a client certificate. The `clientAuth` value is not required.
- The Subject Name must not be empty and must contain fewer than 4096 characters. In this release, the Subject Name does not need to be the same for both members of a Site Recovery Manager Server pair.
- The certificate must identify the Site Recovery Manager Server host.
  - The recommended way to identify the Site Recovery Manager Server host is with the host's fully-qualified domain name (FQDN). If the certificate identifies the Site Recovery Manager Server host with an IP address, this must be an IPv4 address. Using IPv6 addresses to identify the host is not supported.
  - Certificates generally identify the host in the Subject Alternative Name (SAN) attribute. Some CAs issue certificates that identify the host in the Common Name (CN) value of the Subject Name attribute. Site Recovery Manager accepts certificates that identify the host in the CN value, but this is not the best practice. For information about SAN and CN best practices, see the Internet Engineering Task Force (IETF) RFC 6125 at https://tools.ietf.org/html/rfc6125.
  - The host identifier in the certificate must match the Site Recovery Manager Server local host address that you specify when you install Site Recovery Manager.

- If Site Recovery Manager Server, vCenter Server, and Platform Services Controller run on the same host machine, you can use the same certificate for both Site Recovery Manager Server and Platform Services Controller. In this case, you must provide the certificate in two formats:
  - For Site Recovery Manager, the certificate must be a Personal Information Exchange Format (PKCS#12) certificate that contains both of the private and public keys.
  - For vCenter Server and Platform Services Controller, the certificate must be separated into two files, one for the certificate with the public key and one for the private key.
- If you use a custom certificate that is signed by a third-party CA for which the root certificate is not registered by default in Windows, and you want the certificates to be trusted without the need for thumbprint verifications, install the root CA certificate in the Windows certificate store.

Installing Site Recovery Manager

6

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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.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 6.0 does not support the vSphere Client for Windows.

Procedure

1 Site Recovery Manager and vCenter Server Deployment Models

   You can install Site Recovery Manager in any of the deployment models that vCenter Server supports. However, the vCenter Server deployment model that you select can have implications for Site Recovery Manager operation.

2 Prerequisites and Best Practices 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.

3 Install Site Recovery Manager Server

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

4 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. This is known as site pairing.

5 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.

6 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.

7 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.

8 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.

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 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.

Site Recovery Manager and vCenter Server Deployment Models

You can install Site Recovery Manager in any of the deployment models that vCenter Server supports. However, the vCenter Server deployment model that you select can have implications for Site Recovery Manager operation.

You deploy vCenter Server with a Platform Services Controller. You can either embed the Platform Services Controller with vCenter Server or it can be external to vCenter Server. Several vCenter Server instances can share the same external Platform Services Controller.

You can deploy the Platform Services Controller in several different configurations.

- Each Platform Services Controller can have its own vCenter Single Sign-On domain.
- Several Platform Services Controller instances can join the same vCenter Single Sign-On domain.
- You can federate vCenter Single Sign-On domains, which federates all of the Platform Services Controller instances from each of the federated domains.

For information about the deployment models that vCenter Server supports, see vCenter Server Deployment Models in *vSphere Installation and Setup*.

You must take the deployment model of vCenter Server and Platform Services Controller into consideration when you install Site Recovery Manager. During a disaster recovery, Site Recovery Manager, vCenter Server, and the associated Platform Services Controller must be up and running on the recovery site.

Configuring the Platform Services Controller and Selecting the Correct vCenter Server Instance in a Federated Environment

Important Take care when you configure the Platform Services Controller and select the vCenter Server instance with which to register Site Recovery Manager.

When you install Site Recovery Manager Server, you provide the address of the Platform Services Controller that is associated with the vCenter Server instance to protect. You then select the vCenter Server instance with which to register Site Recovery Manager from the list of all of the vCenter Server instances that this Platform Services Controller serves. In a federated environment, that list might include vCenter Server instances from other sites. If you configure the wrong Platform Services Controller or select the wrong vCenter Server instance and complete the Site Recovery Manager installation, you cannot subsequently modify the Site Recovery Manager installation to select the correct Platform Services Controller or vCenter Server instances. In this case, you must uninstall and reinstall Site Recovery Manager to configure the correct Platform Services Controller or select the correct vCenter Server instance.

- When you install Site Recovery Manager Server on the protected site, make sure that you configure the correct Platform Services Controller and select the vCenter Server instance that manages the virtual machines to protect.
- When you install Site Recovery Manager Server on the recovery site, make sure that you configure the correct Platform Services Controller and select the vCenter Server instance to which to recover virtual machines.
- Ensure that the Platform Services Controller, vCenter Server, and Site Recovery Manager Server are all located on the protected site, or all on the recovery site.

Sharing Platform Services Controller Instances Across Site Recovery Manager Sites

A single point of failure is created if you share a Platform Services Controller instance between the protected and recovery sites. If the shared Platform Services Controller goes offline, neither the protected site nor the recovery site will function, making recovery impossible.

Concurrent Installations of Site Recovery Manager in a Federated Environment

In an environment with federated vCenter Single Sign-On domains, do not install Site Recovery Manager under more than one Platform Services Controller at the same time. A conflict can arise in the creation of the solution user that Platform Services Controller creates at the domain level for Site Recovery Manager authentication with vCenter Server if the following conditions exist:

- If the installation of one Site Recovery Manager Server instance overlaps with the installation of another Site Recovery Manager Server instance under two different Platform Services Controller instances.

- Those Platform Services Controller instances are federated.

The conflict does not prevent installation, but it does cause one of the Site Recovery Manager Server instances to fail to start, with the error message `Failed to start service`. The message `Failed to start Authorization Manager` appears in the event log for that Site Recovery Manager Server instance.

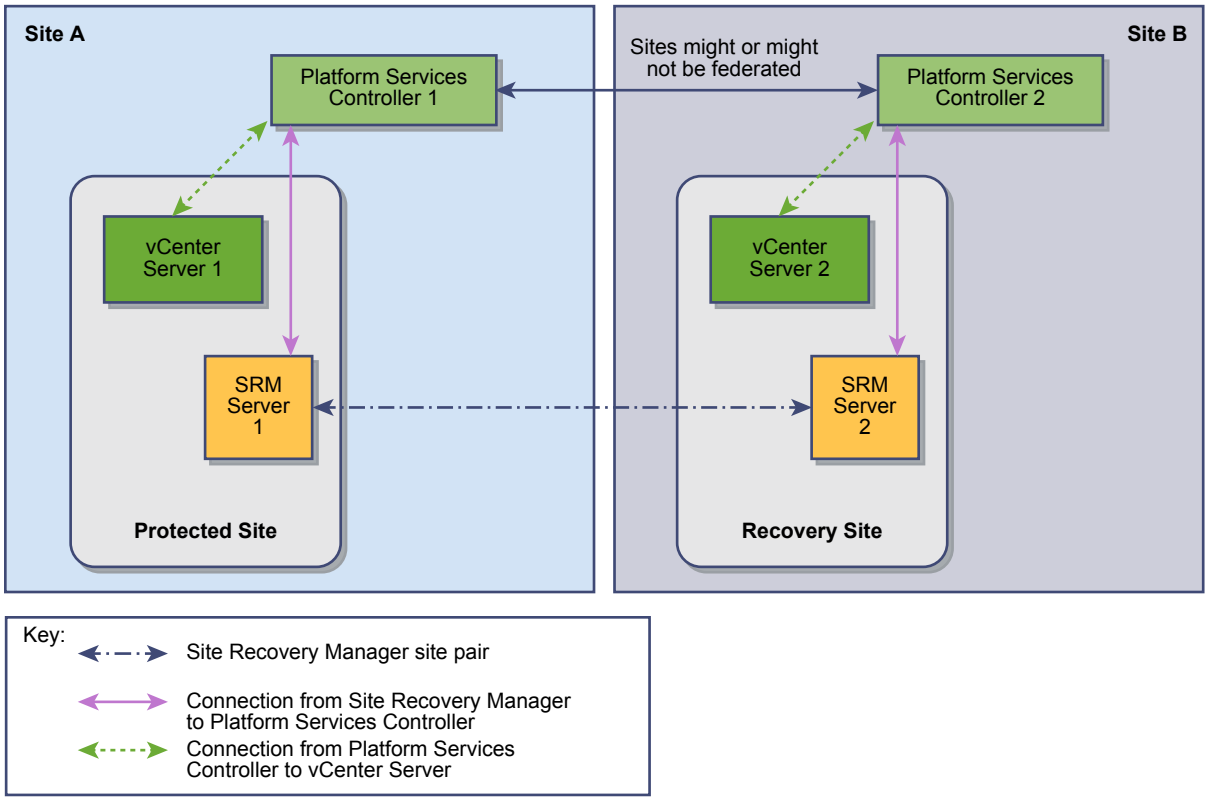
Site Recovery Manager in a Two-Site Topology with One vCenter Server Instance per Platform Services Controller

The most common deployment for Site Recovery Manager is to have two sites with one vCenter Server instance per Platform Services Controller.

In this configuration, the Platform Services Controller instances can be either external to vCenter Server or embedded in the vCenter Server instances.

The Platform Services Controller instances can belong to federated or to unfederated vCenter Single Sign-On domains.

Figure 6-1. Site Recovery Manager in a Two-Site Topology with One vCenter Server Instance per Platform Services Controller



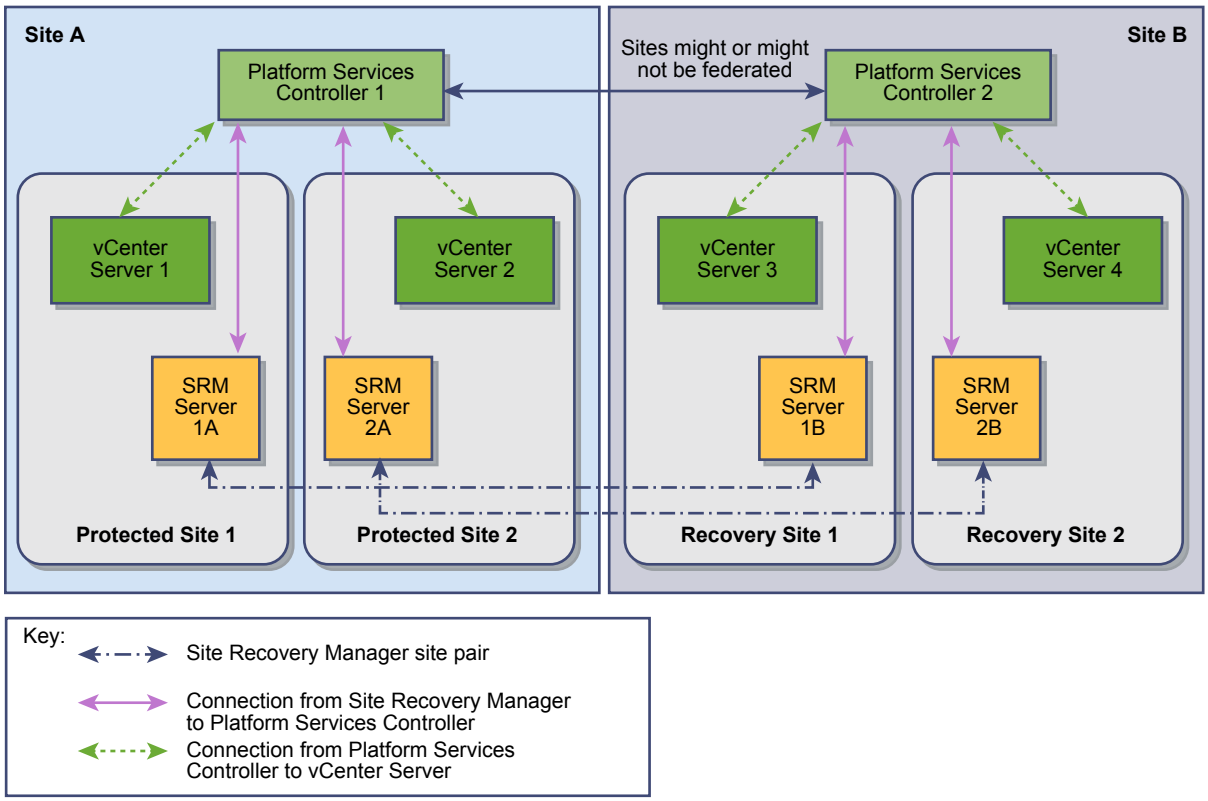
Site Recovery Manager in a Two-Site Topology with Multiple vCenter Server Instances per Platform Services Controller

You can deploy Site Recovery Manager in a topology in which multiple vCenter Server instances share a Platform Services Controller on each site.

In this configuration, the Platform Services Controller instances are external to the vCenter Server instances.

The Platform Services Controller instances can belong to federated or to unfederated vCenter Single Sign-On domains.

Figure 6-2. Site Recovery Manager in a Two-Site Topology with Two vCenter Server Instances per Platform Services Controller



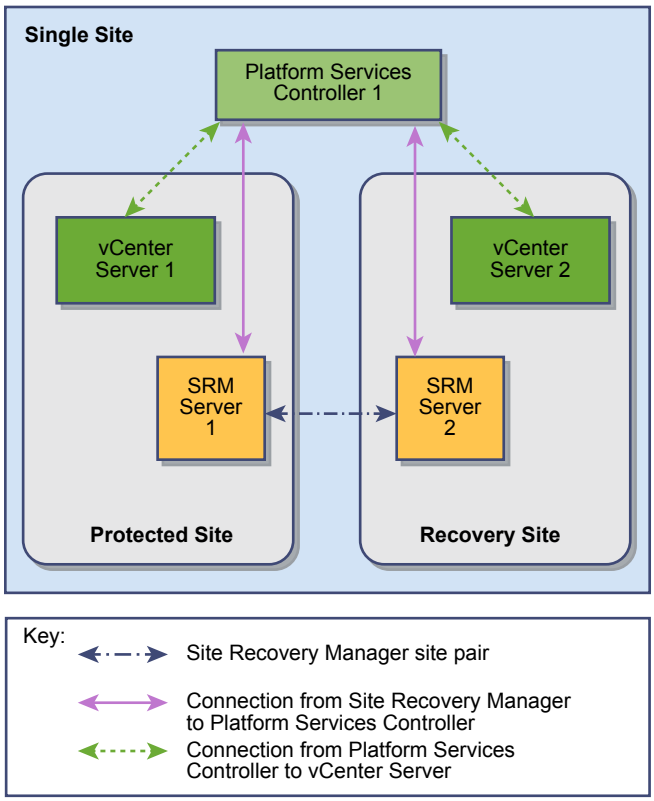
Site Recovery Manager in a Single Site Topology with a Shared Platform Services Controller

You can deploy Site Recovery Manager so that they connect to vCenter Server instances that share a Platform Services Controller.

In this configuration, both vCenter Server instances connect to the same Platform Services Controller within a single site.

Important When the vCenter Server instances on the protected and recovery sites share the same Platform Services Controller, the Platform Services Controller becomes a single point of failure. If the Platform Services Controller goes offline, neither of the protected and recovery sites can function, and recovery is impossible. This configuration is not appropriate for disaster recovery, and is not recommended.

Figure 6-3. Site Recovery Manager in a Single Site Topology with a Shared Platform Services Controller



Prerequisites and Best Practices 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 Platform Services Controller and vCenter Server on both sites. You cannot mix Site Recovery Manager, Platform Services Controller, or vCenter Server versions across sites. 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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.html.
- 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. Furthermore, if you install Site Recovery Manager Server in a virtual machine, and this virtual machine is not the same as the one that runs vCenter Server, you can use vSphere High Availability and VMware Fault Tolerance to protect the Site Recovery Manager Server virtual machine.

- When you install and configure Platform Services Controller, vCenter Server, and vSphere Replication, use fully qualified domain names (FQDN) whenever possible rather than IP addresses. Using FQDN rather than IP addresses allows you to change the vSphere infrastructure, for example by using DHCP, without having to redeploy or reconfigure Site Recovery Manager. You must also use FQDN if you use custom certificates, because most certificate authorities do not accept certificates that use IP addresses for the SAN or CN value.
- The way in which you deploy Platform Services Controller, vCenter Server, and vCenter Single Sign-On on a site affects how you deploy Site Recovery Manager. For information about how the vCenter Server deployment model affects Site Recovery Manager, see Site Recovery Manager and vCenter Server Deployment Models.
- Obtain the address of the Platform Services Controller instance for both sites. The Platform Services Controller must be running and accessible during Site Recovery Manager installation.
- Obtain the vCenter Single Sign-On administrator user name and password for both of the local and remote sites.
- Synchronize the clock settings of the systems on which Platform Services Controller, vCenter Server, and Site Recovery Manager Server run. To avoid conflicts in the time management across these systems, use a persistent synchronization agent such as network time protocol daemon (NTPD), W32Time, or VMware Tools time synchronization. If you run Platform Services Controller, vCenter Server, and Site Recovery Manager Server in virtual machines, set up NTP time synchronization on the ESXi host on which the virtual machines run. For information about timekeeping best practices, see http://kb.vmware.com/kb/1318.
- Obtain a Windows user account with the appropriate privileges on the system on which to install and run Site Recovery Manager Server. You can configure the Site Recovery Manager service to run under a specified user account. The 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. Alternatively, you can configure Site Recovery Manager to run under the Local System account during installation.
- Obtain the user name and password for the Site Recovery Manager database, if you are not using the embedded database.
- If you do not use the embedded Site Recovery Manager database, configure and start the Site Recovery Manager database service on both sites before you install the Site Recovery Manager Server. Each Site Recovery Manager instance requires its own database. 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.

- 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. 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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.html.
- The Site Recovery Manager installer presents the SSL/TLS certificate of the Platform Services Controller for validation when it runs. Obtain the necessary information to allow you validate the certificate.
- If you use custom certificates, obtain an appropriate certificate file. See Requirements When Using Custom SSL/TLS Certificates with Site Recovery Manager.
- 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.
- Optimize the Adobe Flash Player settings in your browser to increase the amount of storage space that the vSphere Web Client can use. Performing a recovery with Site Recovery Manager can sometimes exceed the default amount of storage space that Flash Player is permitted to consume. For information about how to optimize the Flash Player settings for Site Recovery Manager in the vSphere Web Client, see http://kb.vmware.com/kb/2106096.

Install Site Recovery Manager Server

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

If you are upgrading an existing Site Recovery Manager installation, see Chapter 7 Upgrading Site Recovery Manager.

If you are installing Site Recovery Manager in a shared recovery site configuration, see Chapter 9 Installing Site Recovery Manager to Use with a Shared Recovery Site.

Prerequisites

- Perform the tasks and verify that you have the required information listed in Prerequisites and Best Practices 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 Platform Services Controller at the site where you are installing Site Recovery Manager and click **Next**.

Option	Description
Address	The host name or IP address of the Platform Services Controller for the vCenter Server with which to register Site Recovery Manager. 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** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address. **Important** If the Platform Services Controller uses an FQDN rather than an IP address, you must specify the FQDN when you install Site Recovery Manager.
HTTPS Port	Accept the default value of 443 or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS and does not support HTTP connections.
Username	The vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On Administrator group on the Platform Services Controller instance. Only members of the Administrator group have the necessary permissions to create or recreate the Site Recovery Manager solution user.
Password	The password for the specified vCenter Single Sign-On user name. The password text box can be empty.

5. If prompted, verify the Platform Services Controller certificate and click **Accept** to accept it.

6 Select the vCenter Server instance with which to register Site Recovery Manager and click **Next**.

Important The drop-down menu includes all of the vCenter Server instances that are registered with the Platform Services Controller. In a federated environment, it can also include vCenter Server instances from other Platform Services Controller instances. Make sure that you select the correct vCenter Server instance. Once the Site Recovery Manager installation is complete, you cannot modify it to select a different vCenter Server instance.

7 Enter information with which to register the Site Recovery Manager extension 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. The vCenter Server address is used by default, but you can enter any name. You cannot use 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. **Important** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
Listener Port	HTTPS port for all management traffic to Site Recovery Manager Server, including traffic with external API clients for task automation. The port is also used by vSphere Web Client to download the Site Recovery Manager client plugin. This port must be accessible from the vCenter Server proxy system. Do not change the port unless the default of 9086 causes port conflicts.

8 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**.

Both Site Recovery Manager Server instances in a of pair of sites must use the same plug-in identifier.

Option	Description	
Default SRM Plug-in Identifier	Use this option when you install Site Recovery Manager in a standard configuration with one protected site and one recovery site.	
Custom SRM Plug-in Identifier	Use this option when you install 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.

9 Select a certificate type and click **Next**.

Option	Description
Automatically generate certificate	Use 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**.
Load a certificate file	Use 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 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.

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

Option	Action
Data Source Name	This option is only visible if you selected **Use the embedded database server**. 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.
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.
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. This option is disabled if you use SQL Server with Integrated Windows Authentication.
Database Port	This option is only visible if you selected **Use the embedded database server**. You cannot change this value.

Option	Action
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. The maximum value that you can set depends on your database configuration. In most cases, it is not necessary to change this setting. Before changing this setting, consult with your database administrator. Setting the value too high can lead to database errors.
Max Connections	Enter the maximum number of database connections that can be open simultaneously. The maximum value that you can set depends on your database configuration. 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. Setting the value too high can lead to database errors.

12 Select the user account under which to run the Site Recovery Manager Server service and click **Next**.

- 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**.

15 Repeat steps Step 1 through Step 14 on the other 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. This is known as site pairing.

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.

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 address of the Platform Services Controller for the Site Recovery Manager Server on the remote site, and click **Next**.

   The address that you provide for the Platform Services Controller must be an exact match of the of address that you provided when you installed Site Recovery Manager Server on the remote site.

   Important To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

4 Select the vCenter Server instance with which Site Recovery Manager Server is registered on the remote site, provide the vCenter Single Sign-On username and password, and click **Finish**.

The protected and recovery sites are connected. The remote site appears under **Sites** in the Site Recovery Manager interface.

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 vCenter Single Sign-On username and password for 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 **Licenses** tab.
4. Enter the Site Recovery Manager license key in the **License Keys** text box and click **Next**.
5. Update the license name, review the details of the license, and click **Finish**.
6. Click the **Assets** tab and click **Solutions**.
7. Right-click the Site Recovery Manager site and select **Assign License**.
8. Select the license 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.

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 Platform Services Controller and vCenter Server instances to extend, the Site Recovery Manager database type, DSN and credentials, the certificate, and so on. The Site Recovery Manager installer provides a modify mode that allows you to change some of the values that you configured when you installed Site Recovery Manager Server:

- The vCenter Single Sign-On user name and password, if they changed since you installed Site Recovery Manager
- The information with which you register Site Recovery Manager with vCenter Server
- Upload or generate a new certificate
- 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

Note If you change the certificate that vCenter Server or Platform Services Controller uses, you must run the Site Recovery Manager installer in modify mode. Running the Site Recovery Manager installer in modify mode updates the Site Recovery Manager certificate thumbprints to reflect the new vCenter Server or Platform Services Controller certificate.

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 **Modify** and click **Next**.
6. Verify or modify the information with which to register the Site Recovery Manager extension with Platform Services Controller, and click **Next**.

Option	Description
Address	You cannot use the installer's modify mode to change the Platform Services Controller instance with which to register Site Recovery Manager after the initial installation.
HTTPS Port	You cannot use the installer's modify mode to change the Platform Services Controller port after the initial installation.
Username	Modify the vCenter Single Sign-On user name, if it has changed since the initial installation.
Password	Enter the vCenter Single Sign-On password.

7. If prompted, verify the Platform Services Controller certificate and click **Accept** to accept it.
8. Verify the vCenter Server instance that Site Recovery Manager extends, and click **Next**.

   You cannot use the installer's modify mode to change the vCenter Server instance that Site Recovery Manager extends.
9. Verify or modify the information with which to register the Site Recovery Manager extension with vCenter Server, and click **Next**.

Option	Description
Local Site Name	You cannot change this value.
Administrator E-mail	Modify this value if the Site Recovery Manager administrator has changed after you installed Site Recovery Manager Server.
Local Host	The address of the host on which Site Recovery Manager Server runs. If you change this value, you must either regenerate the certificate or provide a new certificate that includes the new address in Step 10. **Important** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
Listener Port	The port for all HTTPS traffic between Site Recovery Manager Server and vCenter Server.

10 Select a certificate type and click **Next**.

Option	Description
Automatically generate a certificate	Select this option to generate a new auto-generated certificate.
Use a PKCS #12 certificate file	Select this option to upload a new custom certificate.
Use existing certificate	Select this option to retain the current certificate. If the installed certificate is not valid, this option is unavailable.

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

Important If you modified the **Local Host** value for Site Recovery Manager Server in Step 9, you must select **Automatically generate a certificate** to regenerate the certificate or **Use a PKCS #12 certificate file** to upload a certificate that includes the new Site Recovery Manager Server address. If you select **Use existing certificate**, the installation modification succeeds, but attempts to log in to Site Recovery Manager fail because the certificate contains an incorrect address for the Site Recovery Manager Server host.

11 Verifiy or modify the database configuration information and click **Next**.

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

Option	Description
Data Source Name	The DSN for the Site Recovery Manager database. You cannot change this value if you use the embedded database.
Database User Name	A user ID valid for the specified database. Modify this value if the database user account has changed after you installed Site Recovery Manager Server.
Database Password	The password for the specified user ID. Modify this value if the password for the database user account has changed after you installed Site Recovery Manager Server. You must enter this value in all cases.
Database Port	You cannot change this value if you use the embedded database.
Connection Count	Modify 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. The maximum value that you can set depends on your database configuration. In most cases, it is not necessary to change this setting. Before changing this setting, consult with your database administrator. Setting the value too high can lead to database errors.
Max Connections	Modify the maximum number of database connections that can be open simultaneously. The maximum value that you can set depends on your database configuration. 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. Setting the value too high can lead to database errors.

12 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.

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

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

14 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.

15 (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.

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.

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.

Migrating a Site Recovery Manager Server to Run on a Different Host

To migrate a Site Recovery Manager server to a new host, you must install Site Recovery Manager on the new host and supply database connection information used by the old installation.

You use this workflow to migrate a Site Recovery Manager server from one host to another and retain data from the previous installation, which is stored in the Site Recovery Manager database.

Prerequisites

- Backup the Site Recovery Manager database.
- Uninstall the old Site Recovery Manager preserving the database.

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 Platform Services Controller at the site where you are installing Site Recovery Manager and click **Next**.

Option	Description
Address	The host name or IP address of the Platform Services Controller for the vCenter Server with which to register Site Recovery Manager. 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** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address. **Important** If the Platform Services Controller uses an FQDN rather than an IP address, you must specify the FQDN when you install Site Recovery Manager.
HTTPS Port	Accept the default value of 443 or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS and does not support HTTP connections.
Username	The vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On Administrator group on the Platform Services Controller instance. Only members of the Administrator group have the necessary permissions to create or recreate the Site Recovery Manager solution user.
Password	The password for the specified vCenter Single Sign-On user name. The password text box can be empty.

5 If prompted, verify the Platform Services Controller certificate and click **Accept** to accept it.

6 Select the vCenter Server instance with which to register Site Recovery Manager and click **Next**.

Important The drop-down menu includes all of the vCenter Server instances that are registered with the Platform Services Controller. In a federated environment, it can also include vCenter Server instances from other Platform Services Controller instances. Make sure that you select the correct vCenter Server instance. Once the Site Recovery Manager installation is complete, you cannot modify it to select a different vCenter Server instance.

7 Enter information with which to register the Site Recovery Manager extension 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. The vCenter Server address is used by default, but you can enter any name. You cannot use 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. **Important** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
Listener Port	HTTPS port for all management traffic to Site Recovery Manager Server, including traffic with external API clients for task automation. The port is also used by vSphere Web Client to download the Site Recovery Manager client plugin. This port must be accessible from the vCenter Server proxy system. Do not change the port unless the default of 9086 causes port conflicts.

8 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**.

Both Site Recovery Manager Server instances in a of pair of sites must use the same plug-in identifier.

Option	Description	
Default SRM Plug-in Identifier	Use this option when you install Site Recovery Manager in a standard configuration with one protected site and one recovery site.	
Custom SRM Plug-in Identifier	Use this option when you install 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.

9 Select a certificate type and click **Next**.

Option	Description
Automatically generate certificate	Use 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**.
Load a certificate file	Use 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 to use a custom database, and click **Next**.

Select the 64-bit DSN of the old database 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.

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

Option	Description
Database Username	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.
Database Password	Enter the password 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.
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. The maximum value that you can set depends on your database configuration. In most cases, it is not necessary to change this setting. Before changing this setting, consult with your database administrator. Setting the value too high can lead to database errors.
Max Connections	Enter the maximum number of database connections that can be open simultaneously. The maximum value that you can set depends on your database configuration. 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. Setting the value too high can lead to database errors.

12 Select to use existing data, and click **Next**.

13 Select the user account under which to run the Site Recovery Manager Server service and click **Next**.

- 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.

14 Click **Install**.

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

Site Recovery Manager server is migrated on a different host.

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 Run the Site Recovery Manager installer in modify mode to check that the installation is configured correctly.

To facilitate IP address changes in your infrastructure, provide fully qualified domain name (FQDN) whenever possible, rather than IP addresses.

- Check that the address for Platform Services Controller is correct.
- If the vCenter Single Sign-On password has changed since you installed Site Recovery Manager, enter the new password.
- Check that the vCenter Server address is correct. If the vCenter Server address has changed since you installed Site Recovery Manager, for example if the Site Recovery Manager machine uses DHCP instead of a static address, remove, reinstall, and reconfigure Site Recovery Manager.
- Check that the local host address for Site Recovery Manager Server is correct.
- Check that the credentials for the Site Recovery Manager database are correct.
- 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.
- Check that the user account for the Site Recovery Manager service is correct. If you use an account other than the Local System account, check that the username and password are correct.

To facilitate IP address changes in your infrastructure, provide fully qualified domain name (FQDN) whenever possible, rather than IP addresses.

6 Run the Windows ODBC Data Source Administrator utility to check that Site Recovery Manager can connect to the Site Recovery Manager database.

a Open, `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**.

Upgrading Site Recovery Manager

7

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 6.0.x update releases is not supported for all 5.5.x and 5.8.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 and 5.1.x to Site Recovery Manager 6.0 is not supported. Upgrade Site Recovery Manager 5.0.x and 5.1.x to a Site Recovery Manager 5.5.x or 5.8.x release before you upgrade to Site Recovery Manager 6.0.

- See Upgrading Site Recovery Manager in the Site Recovery Manager 5.5 documentation for information about upgrading to 5.5.x.
- See Upgrading Site Recovery Manager in the Site Recovery Manager 5.8 documentation for information about upgrading to 5.8.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 6.0 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 5.5.x or 5.8.x after upgrading to Site Recovery Manager 6.0, 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.

- 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 7-1. 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.

Upgrade Site Recovery Manager

You perform several tasks to upgrade Site Recovery Manager.

Because of update release schedules, upgrading to certain Site Recovery Manager 6.0.x update releases is not supported for all 5.5.x and 5.8.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 and 5.1.x to Site Recovery Manager 6.0 is not supported. Upgrade Site Recovery Manager 5.0.x and 5.1.x to a Site Recovery Manager 5.5.x or 5.8.x release before you upgrade to Site Recovery Manager 6.0.

- See Upgrading Site Recovery Manager in the Site Recovery Manager 5.5 documentation for information about upgrading to 5.5.x.
- See Upgrading Site Recovery Manager in the Site Recovery Manager 5.8 documentation for information about upgrading to 5.8.x.

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.

Procedure

1 Order of Upgrading vSphere and Site Recovery Manager Components

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

2 Prerequisites and Best Practices for Site Recovery Manager Upgrade

Before you upgrade Site Recovery Manager, you must perform preparatory tasks on both Site Recovery Manager sites and verify that you have certain information.

3 In-Place Upgrade of Site Recovery Manager Server

An in-place upgrade provides a quick way to upgrade Site Recovery Manager Server without changing the information that you provided for the previous installation.

4 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.

5 Configure and Verify the Upgraded Site Recovery Manager Installation

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

6 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.

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 all components of vCenter Server 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 all components of vCenter Server 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.

Prerequisites and Best Practices for Site Recovery Manager Upgrade

Before you upgrade Site Recovery Manager, you must perform preparatory tasks on both Site Recovery Manager sites and verify that you have certain information.

- Make a full backup of the Site Recovery Manager database by using the tools that the database software provides. For information about how to back up the embedded database, see Back Up and Restore the Embedded vPostgres Database. Migration of data from an external database to the embedded database is not supported. Failure to back up the database results in the loss of all Site Recovery Manager data if the upgrade fails.
- If you configured advanced settings in the existing installation, take a note of the settings that you configured in **Site Recovery > Sites > Site > Manage > Advanced Settings** in the vSphere Web Client.
- Because of update release schedules, upgrading to certain Site Recovery Manager 6.0.x update releases is not supported for all 5.5.x and 5.8.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 and 5.1.x to Site Recovery Manager 6.0 is not supported. Upgrade Site Recovery Manager 5.0.x and 5.1.x to a Site Recovery Manager 5.5.x or 5.8.x release before you upgrade to Site Recovery Manager 6.0.

  - See Upgrading Site Recovery Manager in the Site Recovery Manager 5.5 documentation for information about upgrading to 5.5.x.
  - See Upgrading Site Recovery Manager in the Site Recovery Manager 5.8 documentation for information about upgrading to 5.8.x.

- The local and remote vCenter Server instances must be running when you upgrade Site Recovery Manager.
- Upgrade vCenter Server and install the appropriate version of Platform Services Controller on the site on which you are upgrading Site Recovery Manager.
  - For information about how to upgrade vCenter Server and its components, see vSphere Upgrade in the *VMware vSphere ESXi and vCenter Server 6.0 Documentation*.
  - 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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.html.
  - For information about the order in which to upgrade the components on each site, see Order of Upgrading vSphere and Site Recovery Manager Components.
- 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.

- 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. Furthermore, if you install Site Recovery Manager Server in a virtual machine, and this virtual machine is not the same as the one that runs vCenter Server, you can use vSphere High Availability and VMware Fault Tolerance to protect the Site Recovery Manager Server virtual machine.
- When you install and configure Platform Services Controller, vCenter Server, and vSphere Replication, use fully qualified domain names (FQDN) whenever possible rather than IP addresses. Using FQDN rather than IP addresses allows you to change the vSphere infrastructure, for example by using DHCP, without having to redeploy or reconfigure Site Recovery Manager. You must also use FQDN if you use custom certificates, because most certificate authorities do not accept certificates that use IP addresses for the SAN or CN value.
- The way in which you deploy Platform Services Controller, vCenter Server, and vCenter Single Sign-On on a site affects how you deploy Site Recovery Manager. For information about how the vCenter Server deployment model affects Site Recovery Manager, see Site Recovery Manager and vCenter Server Deployment Models.
- Obtain the address of the Platform Services Controller instance for both sites. The Platform Services Controller must be running and accessible during Site Recovery Manager installation.
- Obtain the vCenter Single Sign-On administrator user name and password for both of the local and remote sites.
- Synchronize the clock settings of the systems on which Platform Services Controller, vCenter Server, and Site Recovery Manager Server run. To avoid conflicts in the time management across these systems, use a persistent synchronization agent such as network time protocol daemon (NTPD), W32Time, or VMware Tools time synchronization. If you run Platform Services Controller, vCenter Server, and Site Recovery Manager Server in virtual machines, set up NTP time synchronization on the ESXi host on which the virtual machines run. For information about timekeeping best practices, see http://kb.vmware.com/kb/1318.
- Obtain the user name and password for the Site Recovery Manager database, if you are not using the embedded database.
- If you use Site Recovery Manager with vSphere Replication, upgrade vSphere Replication 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.
  - For information about how to upgrade vSphere Replication, see Upgrading vSphere Replication in *vSphere Replication Administration*.
  - 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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.html.

- The Site Recovery Manager installer presents the SSL/TLS certificates of the vCenter Server components for validation when it runs. Obtain the necessary information to allow you validate the certificates for the Platform Services Controller instance on the local site and the Platform Services Controller and vCenter Server instances on the remote site.
- If you use custom certificates, obtain an appropriate certificate file. Custom certificates must use at least the SHA1, or preferably SHA256, thumbprint algorithm. This release of Site Recovery Manager does not support certificates that use the MD5 thumbprint algorithm. If you use MD5 certificates with a previous installation of Site Recovery Manager, you must obtain a new certificate with a stronger signature algorithm before you upgrade Site Recovery Manager. See Requirements When Using Custom SSL/TLS Certificates with Site Recovery Manager.
- 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 or the embedded Site Recovery Manager database to fail.
- **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.
- Optimize the Adobe Flash Player settings in your browser to increase the amount of storage space that the vSphere Web Client can use. Performing a recovery with Site Recovery Manager can sometimes exceed the default amount of storage space that Flash Player is permitted to consume. For information about how to optimize the Flash Player settings for Site Recovery Manager in the vSphere Web Client, see http://kb.vmware.com/kb/2106096.

In-Place Upgrade of Site Recovery Manager Server

An in-place upgrade provides a quick way to upgrade Site Recovery Manager Server without changing the information that you provided for the previous installation.

With an in-place upgrade, you 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.

Note If you are updating Site Recovery Manager 6.0 to a 6.0.x update release or to a 6.0.0.x patch release, you must perform in-place upgrade. You cannot perform upgrade with migration if you are updating Site Recovery Manager 6.0 to a 6.0.x update release or to a 6.0.0.x patch release.

When you upgrade an existing 5.5.x or 5.8.x version of Site Recovery Manager Server to 6.0, you must provide the address of the Platform Services Controller that the upgraded vCenter Server instance uses. For the subsequent steps of the upgrade, the Site Recovery Manager installer reuses information about vCenter Server connections, certificates, and database configuration from the previous Site Recovery Manager 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, 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 updating an existing Site Recovery Manager 6.0 release to a 6.0.x update release, not all of the steps in the procedure apply.

Prerequisites

- You completed the tasks and obtained the information described in Prerequisites and Best Practices 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.
- 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 Enter information about the Platform Services Controller at the site where you are upgrading Site Recovery Manager Server and click **Next**.

Option	Description
Address	The host name or IP address of the Platform Services Controller for the vCenter Server with which to register Site Recovery Manager. 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** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address. **Important** If the Platform Services Controller uses an FQDN rather than an IP address, you must specify the FQDN when you install Site Recovery Manager.
HTTPS Port	Accept the default value of 443 or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS and does not support HTTP connections.
Username	The vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On Administrator group on the Platform Services Controller instance. Only members of the Administrator group have the necessary permissions to create or recreate the Site Recovery Manager solution user.
Password	The password for the specified vCenter Single Sign-On user name. The password text box can be empty.

5 If prompted, verify the Platform Services Controller certificate and click **Accept** to accept it.

6 Verify the vCenter Server instance with which the Site Recovery Manager Server instance to upgrade is registered, and click **Next**.

You cannot change the vCenter Server instance that Site Recovery Manager extends during upgrade.

7 Verify the Administrator E-mail, Local Host, and Listener Port values and click **Next**.

8 Select a certificate type and click **Next**.

Option	Description
Automatically generate certificate	Use 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**.
Load a certificate file	Use 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 Enter the password for the Site Recovery Manager database, and click **Next**.

10 Select the user account under which to run the Site Recovery Manager Server service and click **Next**.

- 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.

11 Enter the address and port number of the vCenter Server instance on the remote site, and click **Next**.

If the Site Recovery Manager Server instance that you are upgrading is not paired, you can leave these values empty.

Important The installer uses the address and port of the vCenter Server instance on the remote site to update many pieces of information in the Site Recovery Manager database. If you provide the address of the incorrect vCenter Server instance, or if you leave the text boxes empty when Site Recovery Manager is paired, you risk corrupting the data in the Site Recovery Manager database.

If you have not upgraded vCenter Server on the remote site to 6.0, the default port is 80 (HTTP). If you have upgraded vCenter Server on the remote site to 6.0, the default port is 443 (HTTPS). You can check the port number for vCenter Server on the remote site in the vSphere Web Client.

a Connect to vCenter Server on the remote site in the vSphere Web Client.

b Select the vCenter Server instance.

c Click the **Manage** tab, click **Settings**, and click **General**.

12 Click **Install**.

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

What to do next

- If you upgraded Site Recovery Manager from 5.5.x or 5.8.x to 6.0.x, 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 upgraded Site Recovery Manager extension appears in vSphere Web Client. You might need to clear the browser cache for the upgrade to appear in vSphere Web Client. If the upgrade still does not appear, restart the vSphere Web Client service.
- If you upgraded Site Recovery Manager from 6.0 to a 6.0.x update release or to a 6.0.0.x patch release, log into vSphere Web Client then restart the vSphere Web Client service. The upgraded Site Recovery Manager extension appears in vSphere Web Client.
- 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.
- Repeat the procedure to upgrade the Site Recovery Manager Server on the other Site Recovery Manager site.
- When you have upgraded both sites, perform the post-upgrade tasks in Configure and Verify the Upgraded Site Recovery Manager 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.

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.

You can only upgrade Site Recovery Manager with migration if you use an external database with the previous installation. You cannot migrate the contents of the embedded database.

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.

Important You cannot perform upgrade with migration if you are updating Site Recovery Manager 6.0 to a 6.0.x update release or to a 6.0.0.x patch release. To upgrade Site Recovery Manager 6.0 to a 6.0.x update release or to a 6.0.0.x patch release, see In-Place Upgrade of Site Recovery Manager Server.

Prerequisites

- You completed the tasks and obtained the information described in Prerequisites and Best Practices for Site Recovery Manager Upgrade.

- Log in to the host machine on which the previous version of Site Recovery Manager Server is running. Log in using an account with sufficient privileges. This is often an Active Directory domain administrator, but can also be local administrator.
- Log in to the host machine on which to install the new version of Site Recovery Manager Server. Log in using an account with sufficient privileges. This is often an Active Directory domain administrator, but can also be local administrator.
- 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.

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, 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 Platform Services Controller at the site where you are upgrading Site Recovery Manager Server and click **Next.**

Option	Description
Address	The host name or IP address of the Platform Services Controller for the vCenter Server with which to register Site Recovery Manager. 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** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address. **Important** If the Platform Services Controller uses an FQDN rather than an IP address, you must specify the FQDN when you install Site Recovery Manager.
HTTPS Port	Accept the default value of 443 or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS and does not support HTTP connections.
Username	The vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On Administrator group on the Platform Services Controller instance. Only members of the Administrator group have the necessary permissions to create or recreate the Site Recovery Manager solution user.
Password	The password for the specified vCenter Single Sign-On user name. The password text box can be empty.

6 If prompted, verify the Platform Services Controller certificate and click **Accept** to accept it.

7 Select the vCenter Server instance with which to register Site Recovery Manager and click **Next**.

Important The drop-down menu includes all of the vCenter Server instances that are registered with the Platform Services Controller. In a federated environment, it can also include vCenter Server instances from other Platform Services Controller instances. Make sure that you select the correct vCenter Server instance. Once the Site Recovery Manager installation is complete, you cannot modify it to select a different vCenter Server instance.

8 Enter information with which to register the Site Recovery Manager extension 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. The vCenter Server address is used by default, but you can enter any name. You cannot use 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. **Important** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
Listener Port	HTTPS port for all management traffic to Site Recovery Manager Server, including traffic with external API clients for task automation. The port is also used by vSphere Web Client to download the Site Recovery Manager client plugin. This port must be accessible from the vCenter Server proxy system. Do not change the port unless the default of 9086 causes port conflicts.

9 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**.

Both Site Recovery Manager Server instances in a of pair of sites must use the same plug-in identifier.

Option	Description	
Default SRM Plug-in Identifier	Use this option when you install Site Recovery Manager in a standard configuration with one protected site and one recovery site.	
Custom SRM Plug-in Identifier	Use this option when you install 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.

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

11 Select a certificate type and click **Next**.

Option	Description
Automatically generate certificate	Use 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**.
Load a certificate file	Use 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**.

12 Select **Use a custom database server**, select the 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.

13 Select the user account under which to run the Site Recovery Manager Server service and click **Next**.

- 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.

14 Enter the address and port number of the vCenter Server instance on the remote site, and click **Next**.

If the Site Recovery Manager Server instance that you are upgrading is not paired, you can leave these values empty.

Important The installer uses the address and port of the vCenter Server instance on the remote site to update many pieces of information in the Site Recovery Manager database. If you provide the address of the incorrect vCenter Server instance, or if you leave the text boxes empty when Site Recovery Manager is paired, you risk corrupting the data in the Site Recovery Manager database.

If you have not upgraded vCenter Server on the remote site to 6.0, the default port is 80 (HTTP). If you have upgraded vCenter Server on the remote site to 6.0, the default port is 443 (HTTPS). You can check the port number for vCenter Server on the remote site in the vSphere Web Client.

a Connect to vCenter Server on the remote site in the vSphere Web Client.

b Select the vCenter Server instance.

c Click the **Manage** tab, click **Settings**, and click **General**.

15 Click **Install**.

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

What to do next

- 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 upgraded Site Recovery Manager extension appears in vSphere Web Client. You might need to clear the browser cache for the upgrade to appear in vSphere Web Client. If the upgrade still does not appear, restart the vSphere Web Client service.
- Repeat the procedure to upgrade the Site Recovery Manager Server on the other Site Recovery Manager site.
- When you have upgraded both sites, perform the post-upgrade tasks in Configure and Verify the Upgraded Site Recovery Manager Installation.

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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.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. (Optional) If you reverted to Site Recovery Manager 5.5.x or earlier, 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

8

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

  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.

- 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

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 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 by using 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, connect the vSphere Web Client 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 Select whether to create the mapping automatically or manually and click **Next**.

Option	Description
Automatically	Site Recovery Manager automatically maps networks and folders on the protected site to networks and folders on the recovery site that have the same name. Automatic mapping is only available for network and folder mappings. You must configure resource mappings manually.
Manually	To map specific networks, folders, and resources on the protected site to specific networks, folders, and resources on the recovery site.

5 Select the items on the protected site to map to items on the recovery site.

- If you selected automatic mapping, expand the inventory items on the left to select a parent node on the local site, for example a datacenter or a folder, then expand the inventory items on the right to select a parent node on the remote site.
- If you selected manual mapping, expand the inventory items on the left to select a specific resource on the local site, then expand the inventory items on the right to select the resource on the remote site to which to map this resource.

If you select manual mapping, 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**.

The mappings appear at the bottom of the page. If you selected automatic mapping, Site Recovery Manager automatically maps all of the items under the node that you selected on the protected site to items that have the same name under the node that you selected on the recovery site.

7 (Optional) Repeat Step 5 through Step 6 to map other resources of the same type from the local site to the remote site.

8 (Optional) Click **Next**, and on the **Prepare reverse mappings** page, select the check box for a 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 **Finish** 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, you can select a placeholder datastore that you already use as the target datastore for replications. If you use the same datastore, Site Recovery Manager creates placeholder VMs by using the names of the replication targets and adding the suffix(1). For information about the vSphere Replication protection groups, see the *vSphere Replication Protection Groups* topic in the *Site Recovery Manager Administration*. Selecting the same datastore might lead to confusion when differentiating the replication targets from the placeholder VMs .To avoid confusion, the best practice is to use different datastores.

   Make sure placeholder datastores are not in the same Storage DRS cluster as the vSphere Replication replica target datastores.

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

9

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.

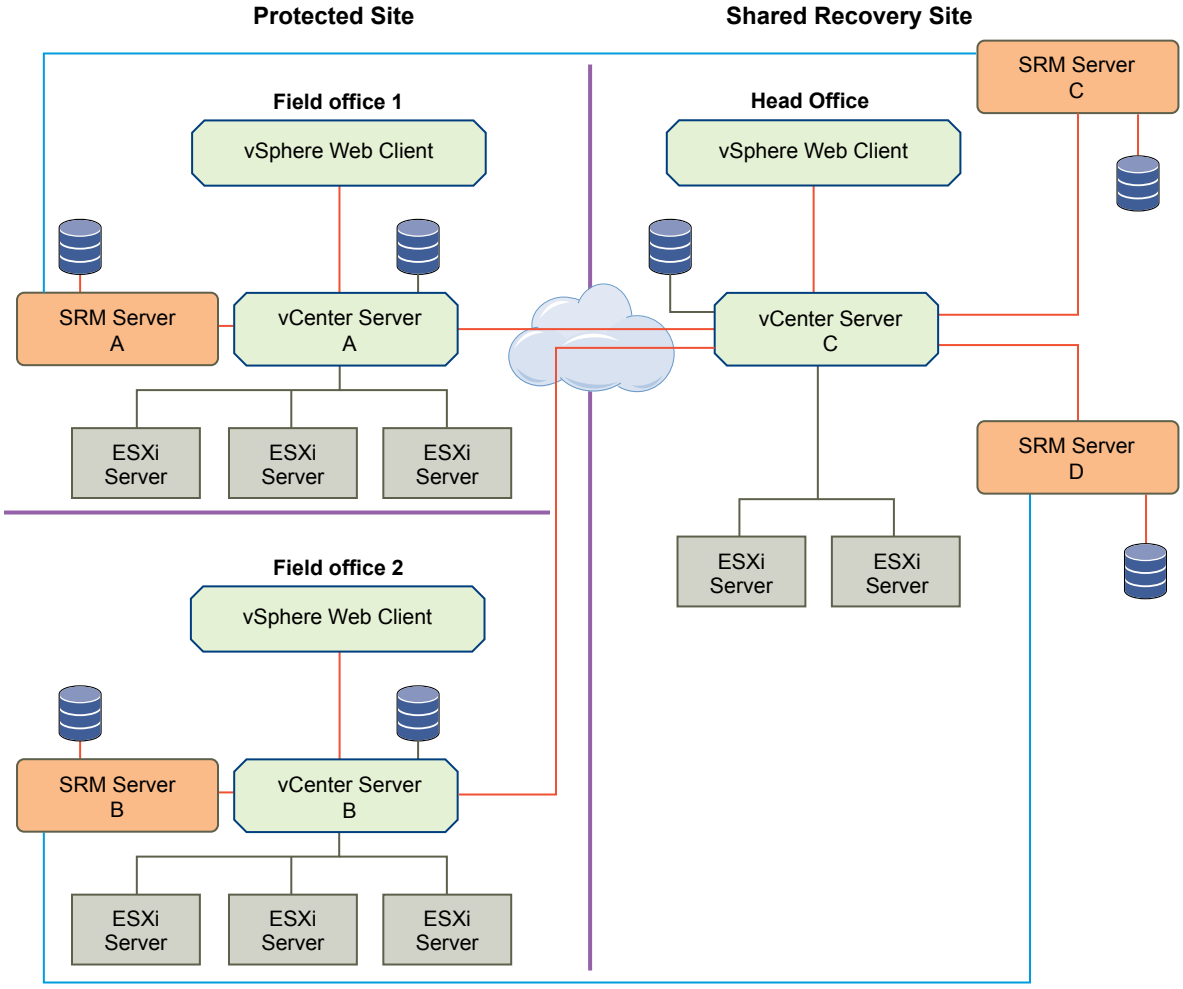
In addition to the shared recovery site configuration, Site Recovery Manager also allows and supports shared protected site (1:N) and many-to-many (N:N) configurations.

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 9-1. Example of Using Site Recovery Manager in a Shared Recovery Site Configuration



- Shared Recovery Sites and vCenter Server Deployment Models

  You can use Site Recovery Manager in a shared recovery site configuration in any of the deployment models that vCenter Server supports.

- 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.

Shared Recovery Sites and vCenter Server Deployment Models

You can use Site Recovery Manager in a shared recovery site configuration in any of the deployment models that vCenter Server supports.

For information about how the vCenter Server deployment model affects Site Recovery Manager, see Site Recovery Manager and vCenter Server Deployment Models.

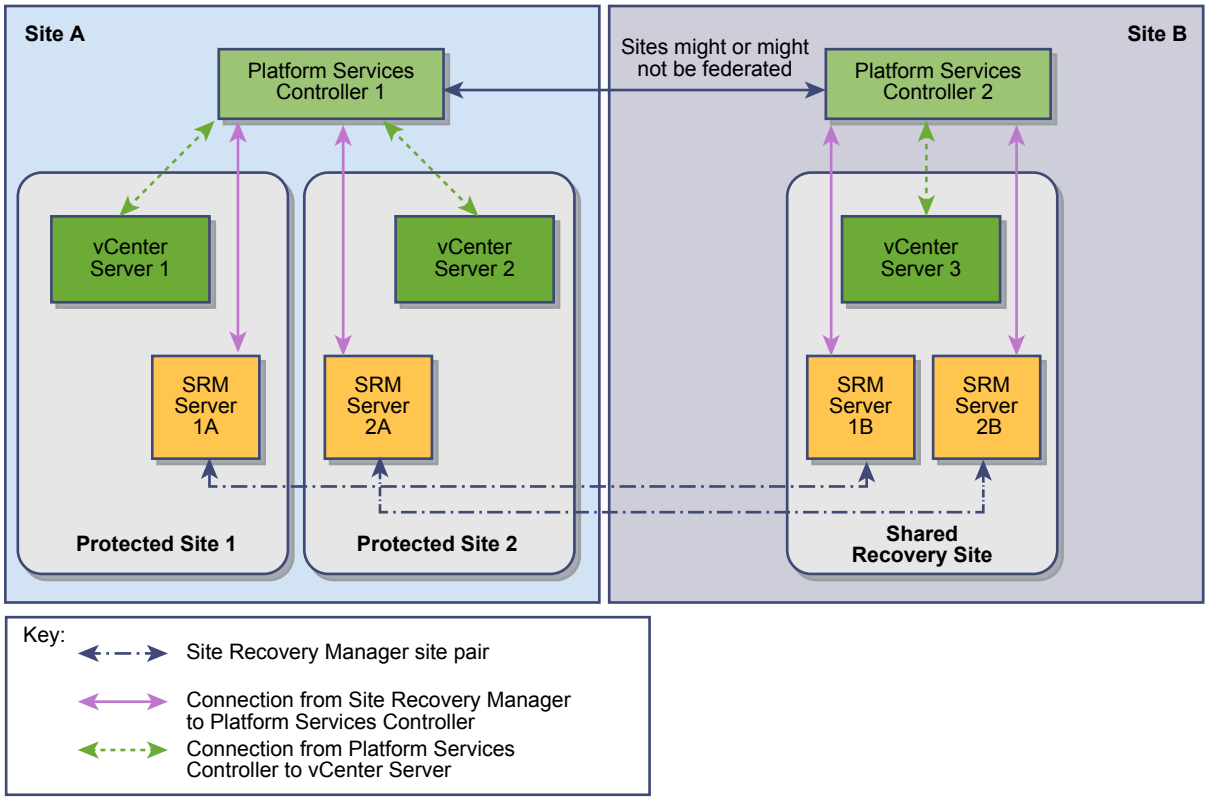
Site Recovery Manager in a Shared Recovery Site Configuration

In a shared recovery site configuration, the Site Recovery Manager Server instances on the recovery site connect to the same vCenter Server and Platform Services Controller instances.

The Site Recovery Manager Server instances on the protected sites can connect to vCenter Server instances that share a Platform Services Controller or that each connect to a different Platform Services Controller.

Figure 9-2 shows one possible shared recovery site configuration. In this example, the Site Recovery Manager Server instances on the protected sites connect to a single Platform Services Controller instance that two vCenter Server instances share.

Figure 9-2. Site Recovery Manager in a Shared Recovery Site Configuration



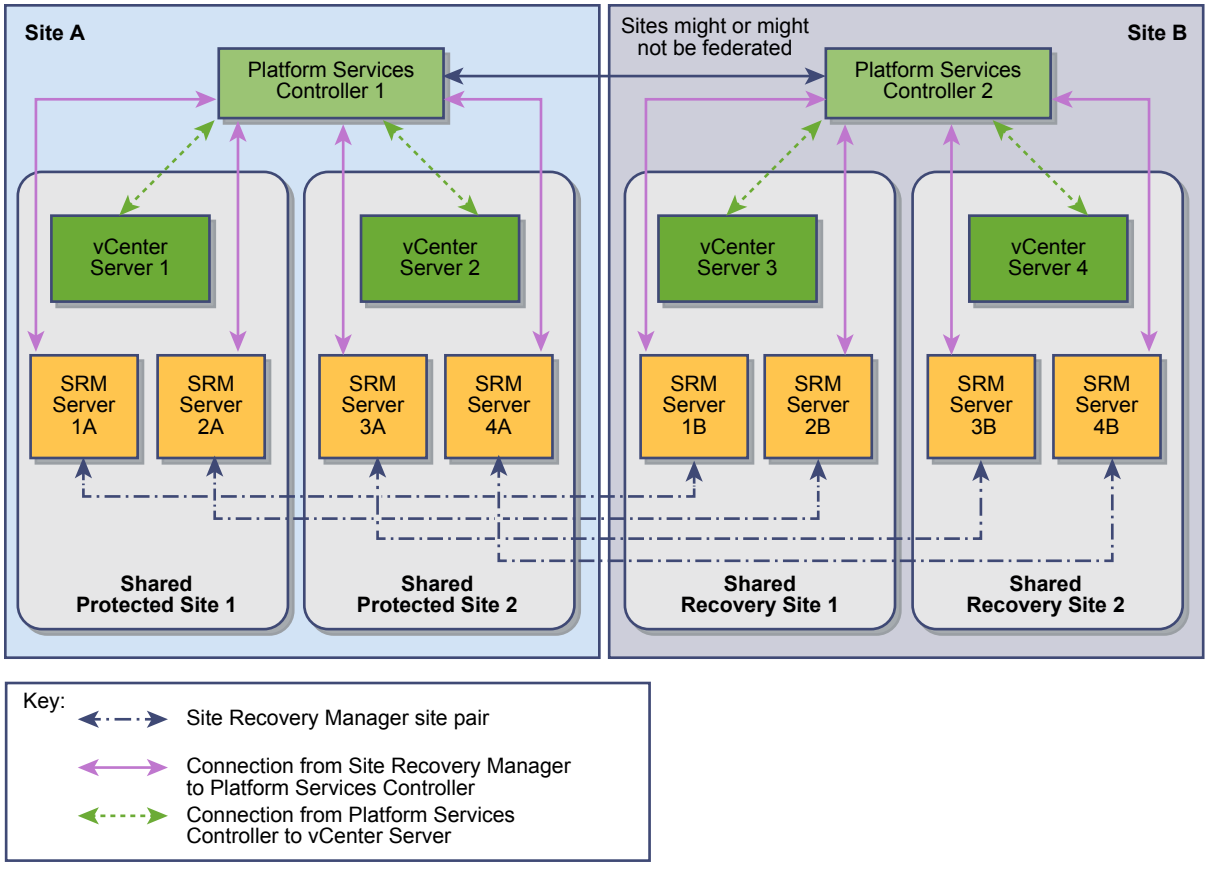
Site Recovery Manager in a Shared Protected Site Configuration

In a shared protected site configuration, the Site Recovery Manager Server instances on the protected site connect to the same vCenter Server and Platform Services Controller instances.

The Site Recovery Manager Server instances on the recovery sites can share vCenter Server and Platform Services Controller instances, or they can connect to a different vCenter Server and Platform Services Controller instances.

Figure 9-3 shows one possible shared protected site configuration. In this example, two Site Recovery Manager Server instances share a vCenter Server instance on each of two shared protected sites. The vCenter Server instances on both of the shared protected sites share a single Platform Services Controller. On the recovery sites, two Site Recovery Manager Server instances share a vCenter Server instance on each shared recovery site. The vCenter Server instances on both of the shared recovery sites share a single Platform Services Controller.

Figure 9-3. Site Recovery Manager in a Shared Protected Site and 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 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.
- 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/2105500 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. Increase the `remoteManager.defaultTimeout` timeout value on the Site Recovery Manager Server on the recovery site.

   For example, increase the timeout from the default of 300 seconds to 1200 seconds. For information about how to increase the `remoteManager.defaultTimeout` setting, see Change Remote Manager Settings in *Site Recovery Manager Administration*.

2. Go to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` on the Site Recovery Manager Server host machine on the recovery site.
3. Open `vmware-dr.xml` in a text editor.
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 http://kb.vmware.com/kb/2105500.

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. 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 6.0* at https://www.vmware.com/support/srm/srm-compat-matrix-6-0.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.

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 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.

4. 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 corresponding 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 Platform Services Controller for the Site Recovery Manager Server on the remote site, and click **Next**.

   The address that you provide for the Platform Services Controller must be an exact match of the of address that you provided when you installed Site Recovery Manager Server on the remote site.

   Important To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
4. Select the vCenter Server instance with which Site Recovery Manager Server is registered on the remote site, provide the vCenter Single Sign-On username and password, and click **Finish**.

   If several Site Recovery Manager Server instances are registered with this vCenter Server instance, Site Recovery Manager connects to the Site Recovery Manager Server instance that has the corresponding Site Recovery Manager ID.
5. Repeat Step 1 to Step 4 to configure the site pairing for all of the sites that use the shared recovery site.
6. (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.
7. (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 http://kb.vmware.com/kb/2105500.

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 8 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 7 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 7 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 perform in-place upgrade of Site Recovery Manager Server, 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 perform in-place upgrade of Site Recovery Manager Server, 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.