VMware Site Recovery Installation and Configuration

VMware Site Recovery
Site Recovery Manager 8.0
vSphere Replication 8.0

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

Contents

About VMware Site Recovery Installation and Configuration

VMware Site Recovery Installation and Configuration provides information about how to install and configure VMware Site Recovery Manager and VMware vSphere Replication on the on-premises site, and how to set up VMware Site Recovery on the recovery site on VMware Cloud on AWS.

This information also provides a general overview of Site Recovery Manager and VMware vSphere Replication.

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

Intended Audience

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

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Overview of VMware Site Recovery

1

VMware Site Recovery 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 on-premises site and a recovery vCenter Server site on VMware Cloud on AWS.

VMware Site Recovery uses the host-based replication feature of VMware vSphere Replication and the orchestration of Site Recovery Manager.

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 is reported but is 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.

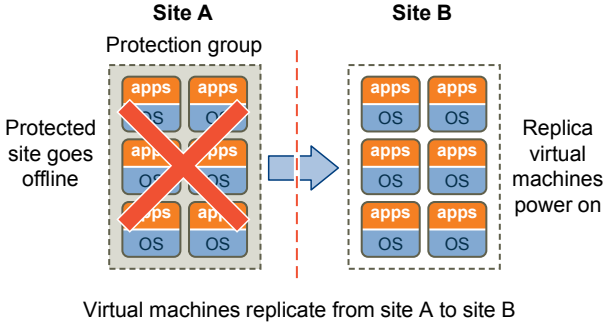
This chapter includes the following topics:

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.
- 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 Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.html.
- Each site must have at least one datacenter.
- You must have 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 Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.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.
- 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 protecting individual virtual machines by using vSphere Replication.

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 Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.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.
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.
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.

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

Component	Heterogeneous or Identical Installations
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 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 Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.html.

This chapter includes the following topics:

VMware Site Recovery 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 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.

VMware Site Recovery License Key

The VMware Site Recovery license key is part of the subscription to the service. When you pair the Site Recovery Manager on-premises instance with the Site Recovery Manager instance on VMware Cloud on AWS, VMware Site Recovery uses the cloud license.

Operational Limits of Site Recovery Manager

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

Protection Maximums for Site Recovery Manager 8.0

Table 2-2. Protection Maximums for Site Recovery Manager 8.0

Item	Maximum
Total number of virtual machines configured for protection using vSphere Replication	2000
Total number of virtual machines per protection group	500
Total number of virtual machines per SDDC on VMware Cloud™ on AWS	500
Total number of vSphere Replication protection groups	250

Table 2-2. Protection Maximums for Site Recovery Manager 8.0 (Continued)

Item	Maximum
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Total number of virtual machines per recovery plan	2000

Bidirectional Protection

If you establish bidirectional protection, in which site B serves as the recovery site for site A and at the same time site A serves as the recovery site for site B, limits apply across both sites, and not per site. In a bidirectional implementation, you can protect a different number of virtual machines on each site, but the total number of protected virtual machines across both sites cannot exceed the limits.

For example, if you protect 1500 virtual machines using vSphere Replication from site A to site B, you can use vSphere Replication to protect a maximum of 500 virtual machines from site B to site A. If you are using vSphere Replication for bidirectional protection, you can protect a maximum of 2000 virtual machines across both sites.

Recovery Maximums for Site Recovery Manager 8.0

Item	Maximum
Total number of concurrently executing recovery plans	10
Total number of virtual machine recoveries that you can start simultaneously across multiple recovery plans	2000

If you protect 5000 virtual machines with Site Recovery Manager, you can recover up to 2000 virtual machines in one recovery plan. After that plan has completed, you can run another recovery plan to recover another 2000 virtual machines. When the second plan has also completed, you can recover the remaining 1000 virtual machines.

If you have 5 recovery plans that each contain 1000 virtual machines, you can start a maximum of two of these plans at the same time. If you have 10 recovery plans that each contains 200 virtual machines, you can start all 10 plans at the same time.

IP Customization Maximums for Site Recovery Manager 8.0

If you implement IP customization for recovered virtual machines, you can configure a maximum of one IP address for each NIC, using DHCP, static IPv4, or static IPv6. For static IPv4 or IPv6 addresses, you provide the following information per NIC:

- 1 IP address
- Subnet information
- 1 gateway server address

- 2 DNS servers (primary and secondary)

You also set 2 WINS addresses for DHCP or IPv4, on Windows virtual machines only.

vSphere Replication System Requirements

3

The environment in which you run the vSphere Replication virtual appliance must meet certain hardware requirements.

vSphere Replication is distributed as a 64-bit virtual appliance packaged in the `.ovf` format. It is configured to use a dual core CPU, a 16 GB and a 2 GB hard disk, and 4 GB of RAM. Additional vSphere Replication servers require 716 MB of RAM.

You must deploy the virtual appliance in a vCenter Server environment by using the OVF deployment wizard on an ESXi host.

vSphere Replication consumes negligible CPU and memory on the source host ESXi and on the guest OS of the replicated virtual machine.

Note vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

- Bandwidth Requirements for vSphere Replication

  Before configuring replications, VMware recommends that determine storage and network bandwidth requirements for vSphere Replication to replicate virtual machines efficiently.

vSphere Replication Network Ports

vSphere Replication uses default network ports for intrasite communication between hosts at a single site and intersite communication between hosts at the protected and recovery sites.

For a list of all the ports that must be open for vSphere Replication, see Chapter 8 Network Ports for VMware Site Recovery.

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

Operational Limits of vSphere Replication

vSphere Replication has certain operational limits.

To ensure successful virtual machine replication, you must verify that your virtual infrastructure respects certain limits before you start the replication.

- You can only deploy one vSphere Replication appliance on a vCenter Server instance. When you deploy another vSphere Replication appliance, during the boot process vSphere Replication detects another appliance already deployed and registered as an extension to vCenter Server. You have to confirm if you want to proceed with the new appliance and recreate all replications or shut it down and reboot the old appliance to restore the original vSphere Replication extension thumbprint in vCenter Server.
- Each newly deployed vSphere Replication appliance can manage a maximum of 2000 replications. See http://kb.vmware.com/kb/2102453 for more information.
- Upgraded vSphere Replication appliances that use the embedded vSphere Replication database require additional configuration to enable the support of a maximum of 2000 replications. See http://kb.vmware.com/kb/2102463. No additional configuration is required for vSphere Replication appliances that are configured to use an external database.

Compatibility of vSphere Replication with Other vSphere Features

vSphere Replication is compatible with certain other vSphere management features.

You can safely use vSphere Replication in combination with certain vSphere features, such as vSphere vMotion. Some other vSphere features, for example vSphere Distributed Power Management, require special configuration for use with vSphere Replication.

Note You cannot upgrade VMware Tools in the vSphere Replication appliance.

Table 3-1. Compatibility of vSphere Replication with Other vSphere Features

vSphere Feature	Compatible with vSphere Replication	Description
vSphere vMotion	Yes	You can migrate replicated virtual machines by using vMotion. Replication continues at the defined recovery point objective (RPO) after the migration is finished.
vSphere Storage vMotion	Yes	You can move the disk files of a replicated virtual machine on the source site using Storage vMotion with no impact on the ongoing replication.
vSphere High Availability	Yes	You can protect a replicated virtual machine by using HA. Replication continues at the defined RPO after HA restarts a virtual machine. vSphere Replication does not perform any special HA handling. **Note** You cannot protect the vSphere Replication appliance itself by using HA.
vSphere Fault Tolerance	No	vSphere Replication cannot replicate virtual machines that have fault tolerance enabled. You cannot protect the vSphere Replication appliance itself with FT.
vSphere DRS	Yes	Replication continues at the defined RPO after resource redistribution is finished.
vSphere Storage DRS	Yes	On the source site, Storage DRS can move the disk files of replicated virtual machines with no impact on the ongoing replication. On the target site, you must register the vSphere Replication appliance with the vCenter Single Sign-On service to enable the communication between Storage DRS and the vSphere Replication Management server. See Register the vSphere Replication Appliance with vCenter Single Sign-On.
VMware Virtual SAN datastore	Yes	You can use VMware Virtual SAN datastores as the source and target datastore when configuring replications. **Note** VMware Virtual SAN is a fully supported feature of vSphere 5.5 Update 1 and later.
vSphere Distributed Power Management	Yes	vSphere Replication coexists with DPM on the source site. vSphere Replication does not perform any special DPM handling on the source site. You can disable DPM on the target site to allow enough hosts as replication targets.
VMware vSphere Flash Read Cache	Yes	You can protect virtual machines that contain disks that use VMware vSphere Flash Read Cache storage. Since the host to which a virtual machine recovers might not be configured for Flash Read Cache, vSphere Replication disables Flash Read Cache on disks when it starts the virtual machines on the recovery site. vSphere Replication sets the reservation to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take note of the virtual machine's cache reservation from the vSphere Web Client. After the recovery, you can migrate the virtual machine to a host with Flash Read Cache storage and restore the original Flash Read Cache setting on the virtual machine manually.
vCloud APIs	Not applicable	No interaction with vSphere Replication.
vCenter Chargeback	Not applicable	No interaction with vSphere Replication
VMware Data Recovery	Not applicable	No interaction with vSphere Replication.

vSphere Replication Compatibility with Other Software

vSphere Replication is compatible with certain versions of ESXi, vCenter Server, Site Recovery Manager, databases, and Web browsers.

vSphere Replication 8.0 is compatible with vCenter Server 6.0 U3, vCenter Server 6.5, and vCenter Server 6.5 U1. vSphere Replication 8.0 requires ESXi 6.0 U3, ESXi 6.5, or ESXi 6.5 U1. See the following documents for more information.

- Compatibility Matrices for vSphere Replication 8.0 at https://www.vmware.com/support/vsphere-replication/doc/vsphere-replication-compat-matrix-8-0.html.
- For vSphere Replication interoperability with backup software when using VSS, see http://kb.vmware.com/kb/2040754.
- VMware Compatibility Guide at http://partnerweb.vmware.com/comp_guide2/search.php
- Browser compatibility at vSphere Client and vSphere Web Client Software Requirements in *vSphere Installation and Setup*.

Bandwidth Requirements for vSphere Replication

Before configuring replications, VMware recommends that determine storage and network bandwidth requirements for vSphere Replication to replicate virtual machines efficiently.

Storage and network bandwidth requirements can increase when using vSphere Replication. The following factors play a role in the amount of network bandwidth vSphere Replication requires for efficient replication.

Network Based Storage

Network bandwidth requirements increase if all storage is network-based because data operations between the host and the storage also use network. When you plan your deployment, be aware of the following levels of traffic:

- Between the host running the replicated virtual machine and the vSphere Replication server.
- Between the vSphere Replication server and a host with access to the replication target datastore.
- Between the host and storage.
- Between storage and the host during redo log snapshots.

Network based storage is a concern when you are replicating virtual machines within a single vCenter Server instance that shares the network for the levels of traffic listed. When you have two sites with a vCenter Server instance on each site, the link speed between the two sites is the most important as it can slow down replication traffic between the two sites.

Dataset Size

vSphere Replication might not replicate every virtual machine nor every VMDK file in the replicated virtual machines. To evaluate the dataset size that vSphere Replication replicates, calculate the percentage of the total storage used for virtual machines, then calculate the number of VMDKs within that subset that you have configured for replication.

For example, you might have 2TB of virtual machines on the datastores and use vSphere Replication to replicate half of these virtual machines. You might only replicate a subset of the VMDKs and assuming all the VMDKs are replicated, the maximum amount of data for replication is 1TB.

Data Change Rate and Recovery Point Objective

The data change rate is affected by the recovery point objective (RPO). To estimate the size of the data transfer for each replication, you must evaluate how many blocks change in a given RPO for a virtual machine. The data change rate within the RPO period provides the total number of blocks that vSphere Replication transfers. This number might vary throughout the day, which alters the traffic that vSphere Replication generates at different times.

vSphere Replication transfers blocks based on the RPO schedule. If you set an RPO of one hour, vSphere Replication transfers any block that has changed in that hour to meet that RPO. vSphere Replication only transfers the block once in its current state at the moment that vSphere Replication creates the bundle of blocks for transfer. vSphere Replication only registers that the block has changed within the RPO period, not how many times it changed. The average daily data change rate provides an estimation of how much data vSphere Replication transfers or how often the transfers occur.

If you use volume shadow copy service (VSS) to quiesce the virtual machine, replication traffic cannot be spread out in small sets of bundles throughout the RPO period. Instead, vSphere Replication transfers all the changed blocks as one set when the virtual machine is idle. Without VSS, vSphere Replication can transfer smaller bundles of changed blocks on an ongoing basis as the blocks change, spreading the traffic throughout the RPO period. The traffic changes if you use VSS and vSphere Replication handles the replication schedule differently, leading to varying traffic patterns.

If you change the RPO, vSphere Replication transfers more or less data per replication to meet the new RPO.

Link Speed

If you have to transfer an average replication bundle of 4GB in a one hour period, you must examine the link speed to determine if the RPO can be met. If you have a 10Mb link, under ideal conditions on a completely dedicated link with little overhead, 4GB takes about an hour to transfer. Meeting the RPO saturates a 10Mb WAN connection. The connection is saturated even under ideal conditions, with no overhead or limiting factors such as retransmits, shared traffic, or excessive bursts of data change rates.

You can assume that only about 70% of a link is available for traffic replication. This means that on a 10Mb link you obtain a link speed of about 3GB per hour. On a 100Mb link you obtain a speed of about 30GB per hour.

To calculate the bandwidth, see Calculate Bandwidth for vSphere Replication.

Calculate Bandwidth for vSphere Replication

To determine the bandwidth that vSphere Replication requires to replicate virtual machines efficiently, you calculate the average data change rate within an RPO period divided by the link speed.

If you have groups of virtual machines that have different RPO periods, you can determine the replication time for each group of virtual machines. For example, you might have four groups with RPO of 15 minutes, one hour, four hours, and 24 hours. Factor in all the different RPOs in the environment, the subset of virtual machines in your environment that is replicated, the change rate of the data within that subset, the amount of data changes within each configured RPO, and the link speeds in your network.

Prerequisites

Examine how data change rate, traffic rates, and the link speed meet the RPO. Then look at the aggregate of each group.

Procedure

1. Identify the average data change rate within the RPO by calculating the average change rate over a longer period then dividing it by the RPO.
2. Calculate how much traffic this data change rate generates in each RPO period.
3. Measure the traffic against your link speed.

For example, a data change rate of 100GB requires approximately 200 hours to replicate on a T1 network, 30 hours to replicate on a 10Mbps network, 3 hours on a 100Mbps network.

Creating the Site Recovery Manager Database

4

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.

Important Site Recovery Manager on AWS uses only the embedded vPostgreSQL database.

You can use an external database for Site Recovery Manager on the protected site. 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 Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.html.

This chapter includes the following topics:

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 `0dbcad32.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 Site Recovery Manager.

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

5

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 Site Recovery Manager 5.x, you used either credential-based authentication or certificate-based authentication to authenticate with vCenter Server. Site Recovery Manager 8.0 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 do not use Enhanced Linked Mode, 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 vCenter Single Sign-On environment with Enhanced Linked Mode, 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 6 Creating SSL/TLS Server Endpoint Certificates for Site Recovery Manager.

Creating SSL/TLS Server Endpoint Certificates for Site Recovery Manager

6

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, there is an option for Site Recovery Manager to generate an SSL/TLS certificate to use as the Site Recovery Manager endpoint certificate. This is the simpler option that requires minimal user action.

You can also provide 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 5.x releases, Site Recovery Manager 8.0 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 5 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 8.0 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 5.x releases of Site Recovery Manager.

- Site Recovery Manager does not accept certificates with MD5 signature algorithms. Use SHA256 or stronger signature algorithms.
- 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. You can use an intermediate CA certificate which is not the root of a trust chain, but that is still 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. The reverse is also true.
- 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 5.x 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 all three servers. 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. For information about certificate requirements for vCenter Server and Platform Services Controller, see *vSphere Security Certificates* in the vSphere 6.5 documentation.
- 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.

Setting Up VMware Site Recovery

7

Before you can use the VMware Site Recovery service, you must install a vSphere Replication appliance and Site Recovery Manager Server instance at the protected on-premises site and activate VMware Site Recovery at the recovery site on VMware Cloud on AWS.

The vSphere Replication appliance contains an embedded vSphere Replication server that manages the replication process. To meet the load balancing needs of your environment, you might need to deploy additional vSphere Replication servers at each site. Additional vSphere Replication servers that you deploy are themselves virtual appliances. You must register any additional vSphere Replication server with the vSphere Replication appliance on the corresponding site.

The vSphere Replication appliance provides a virtual appliance management interface (VAMI). You can use this interface to reconfigure the vSphere Replication database, network settings, public-key certificates, and passwords for the appliances.

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 Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.html.

To activate VMware Site Recovery, you must have an VMware Cloud™ on AWS account and deploy a Software-Defined Data Center (SDDC) on VMware Cloud on AWS. For information about how to create an VMware Cloud™ on AWS account, see Account Creation and Management in *VMware Cloud on AWS Getting Started*. For information on how to deploy SDDC, see Deploying and Managing a Software-Defined Data Center in *VMware Cloud on AWS Getting Started*.

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

Procedure

1 Install vSphere Replication

  The installation procedure of vSphere Replication involves several steps.

2 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.

3 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.

4 Install Site Recovery Manager Server at the Protected Site

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

5 Activate VMware Site Recovery at the Recovery Site

You must activate VMware Site Recovery at the recovery site on VMware Cloud™ on AWS.

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

Before you can use VMware Site Recovery, you must connect the Site Recovery Manager Server and vSphere Replication instances on the protected and the recovery sites. This procedure is known as site pairing.

7 Reconfiguring a Site Pair and Breaking a Site Pair

You can reconfigure or break an existing site pair.

8 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 client connection to the remote Site Recovery Manager Server instance.

9 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.

Install vSphere Replication

The installation procedure of vSphere Replication involves several steps.

Prepare Your Environment to Install vSphere Replication

Before you deploy the vSphere Replication appliance, you must prepare the environment.

Procedure

1 Verify that you have vSphere and vSphere Web Client installations for the protected and recovery sites.

2 In the vSphere Web Client, select the vCenter Server instance on which you are deploying vSphere Replication, click **Configure > Settings > Advanced Settings**, and verify that the `VirtualCenter.FQDN` value is set to a fully-qualified domain name or a literal address.

Note vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

What to do next

You can deploy the vSphere Replication appliance.

Deploy the vSphere Replication Virtual Appliance

vSphere Replication is distributed as an OVF virtual appliance.

You deploy the vSphere Replication appliance by using the standard vSphere OVF deployment wizard.

Note vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

Prerequisites

Download the vSphere Replication ISO image and mount it on a system in your environment.

Procedure

1 Log in to the vSphere Web Client on the protected site.

2 Select **vCenter > Hosts and Clusters**.

3 Right-click a host and select **Deploy OVF template**.

4 Provide the location of the OVF file from which to deploy the vSphere Replication appliance, and click **Next**.

   - Select **URL** and provide the URL to deploy the appliance from an online URL.
   - If you downloaded and mounted the vSphere Replication ISO image on a system in your environment, select **Local file > Browse** and navigate to the `\bin` directory in the ISO image, and select the `vSphere_Replication_OVF10.ovf`, `vSphere_Replication-system.vmdk`, and `vSphere_Replication-support.vmdk` files.

5 Review the virtual appliance details and click **Next**.

6 Accept the end user license agreements (EULA) and click **Next**.

7 Accept the name, select or search for a destination folder or datacenter for the virtual appliance, and click **Next**.

   You can enter a new name for the virtual appliance. The name must be unique within each vCenter Server virtual machine folder.

8 Select the number of vCPUs for the virtual appliance and click **Next**.

   Note Selecting higher number of vCPUs ensures better performance of the vSphere Replication Management Server, but might slow down the replications that run on ESXi host systems that have 4 or less cores per NUMA node. If you are unsure what the hosts in your environment are, select 2 vCPUs.

9 Select a cluster, host, or resource pool where you want to run the deployed template, and click **Next**.

10 Select a destination datastore and disk format for the virtual appliance and click **Next**.

11 Select a network from the list of available networks, set the IP protocol and IP allocation, and click **Next**.

   vSphere Replication supports both DHCP and static IP addresses. You can also change network settings by using the virtual appliance management interface (VAMI) after installation.

12 Set the password for the root account for the customized template, and click **Next**.

   The password must be at least eight characters long.

13 Review the binding to the vCenter Extension vService and click **Next**.

14 Review the settings and click **Finish**.

   The vSphere Replication appliance is deployed.

15 Power on the vSphere Replication appliance. Take a note of the IP address of the appliance and log out of the vSphere Web Client.

What to do next

Register the vSphere Replication appliance with the SSO service.

Register the vSphere Replication Appliance with vCenter Single Sign-On

You must register the vSphere Replication Management Server with vCenter Single Sign-On on the protected on-premises site.

After you deploy the vSphere Replication appliance, you use the Virtual Appliance Management Interface (VAMI) to register the endpoint and the certificate of the vSphere Replication Management Server with the vCenter Lookup Service, and to register the vSphere Replication solution user with the vCenter Single Sign-On administration server.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.
- Verify that the vSphere Replication management server is synchronized with the time of the Single Sign-On server.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
2. Type the root user name and password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication appliance.
3. Click the **Configuration** tab.
4. In the **LookupService Address** text box, enter the IP address or domain name of the server where the lookup service runs.
5. Enter the credentials of a user with administrator privileges to vCenter Single Sign-On.

   Initially, only the user administrator@vsphere.local has these privileges.
6. Click **Save and Restart Service**.

What to do next

Perform optional reconfiguration of the vSphere Replication appliance by using the VAMI. You can install a certificate, change the appliance root password, change the trust policy, or configure vSphere Replication to use an external database.

States of vSphere Replication Displayed in the vSphere Web Client

Before you can start using vSphere Replication, you must register the vSphere Replication appliance with the vCenter Lookup Service and the Single Sign-On administration server in the on-premises environment.

In the vSphere Web Client, on the VMware Site Recovery tab, you can check the list of vCenter Server instances in the Single-Sing On domain, and the status of vSphere Replication on each vCenter Server instance.

The following table lists the vSphere Replication states that you can observe, their meanings, and what you can do to change a state back to normal.

Table 7-1. vSphere Replication States on vCenter Server Instances

Status	Description	Remediation
Not installed	The vSphere Replication extension is not registered in the vCenter Server Extension Manager. The vSphere Replication appliance is either not deployed or the vSphere Replication extension has been deleted from the vCenter Server Extension Manager.	If a vSphere Replication appliance is deployed on this vCenter Server, restart the appliance or the vSphere Replication Management service on the appliance. 1 Use a supported browser to log in to the vSphere Replication VAMI as the root user. The URL for the VAMI is https://*vr-appliance-address*:5480. 2 On the **Configuration** tab, click **Save and Restart Service**.
Enabled (Configuration issue)	A configuration error occurred. The vSphere Replication Management Server is either not registered with the vCenter SSO components, or the configuration is incorrect and must be updated. You cannot manage existing replications, or configure new replications to this server .	Configure the vSphere Replication appliance. 1 Use a supported browser to log in to the vSphere Replication VAMI as the root user. The URL for the VAMI is https://*vr-appliance-address*:5480. 2 On the **Configuration** tab, enter the parameters that were indicated in the error message and click **Save and Restart Service** .
Enabled (Not accessible)	The vSphere Replication Management Server is not accessible. The vSphere Replication extension is registered in the vCenter Server Extension Manager, but the vSphere Replication appliance is missing or powered off, or the vSphere Replication Management service is not running. You cannot manage existing replications, or configure new replications to this server .	■ Verify that the vSphere Replication appliance exists on the vCenter Server. ■ Verify that the vSphere Replication appliance is powered on. ■ Restart the VRM service. a Use a supported browser to log in to the vSphere Replication VAMI as the root user. The URL for the VAMI is https://*vr-appliance-address*:5480. b On the **Configuration** tab, restart the VRM service.
OK	The vSphere Replication appliance is installed, configured, and functioning properly.	Not needed.

Deploying Additional vSphere Replication Servers

Depending on replication traffic, you might need to deploy one or more additional vSphere Replication servers.

Deploy an Additional vSphere Replication Server

The vSphere Replication appliance includes a vSphere Replication server. However, you might need to deploy multiple vSphere Replication servers to meet your load balancing needs.

You can deploy multiple vSphere Replication servers to route traffic from source hosts to target datastores without traveling between different sites managed by the same vCenter Server.

For information about the loads that a vSphere Replication management server and a vSphere Replication server can support, see http://kb.vmware.com/kb/2034768.

Prerequisites

- Deploy vSphere Replication appliances on the source and target sites.
- Deploy vSphere Replication servers on a network that allows them to communicate with the vSphere Replication appliances on the source and target sites.
- Verify that the vSphere Replication servers can communicate with the ESXi Server instances on the source site that hosts the replicated virtual machines.

Procedure

1. Right-click on datacenter, host or cluster, and select **Deploy OVF Template**.
2. Browse for the `vSphere_Replication_AddOn_OVF10.ovf`, `vSphere_Replication-system.vmdk`, and `vSphere_Replication-support.vmdk` files, select them, and click **Next**.
3. Review the virtual appliance details and click **Next**.
4. Follow the prompts to select a destination host, datastore, and disk format for the virtual appliance.
5. Enter a password for the appliance that is at least eight characters long.
6. Set the network properties. Select DHCP or set a static IP address.

   You can change network settings after deployment in the VAMI.
7. Review your settings and click **Finish**.
8. Power on the vSphere Replication appliance.

What to do next

When the OVF file has deployed, register the vSphere Replication server with the vSphere Replication appliance.

Register an Additional vSphere Replication Server

If you deploy additional vSphere Replication servers, you must register these servers with the vSphere Replication appliance to enable them as traffic handlers at the recovery site.

Note You can register additional vSphere Replication servers that run within the same vSphere environment.

Prerequisites

- Verify that the vSphere Replication appliance is deployed and configured.
- Verify that the additional vSphere Replication Server is deployed.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. In the left-hand pane, navigate to **Configure > Replication Servers**, and click **Register**.
4. From the list, select a virtual machine that is a working vSphere Replication server and click **Select**.

The newly registered vSphere Replication server appears in the list of vSphere Replication servers.

Reconfigure vSphere Replication Server Settings

The vSphere Replication appliance contains a vSphere Replication server. If you deploy additional vSphere Replication servers, the server settings are established during deployment. You can modify the settings after you deploy the server.

A vSphere Replication server does not require additional configuration through the virtual appliance management interface (VAMI) after deployment. To increase security, you can change the root password of the vSphere Replication server and install a new certificate. Using a self-signed certificate provides the benefit of public-key based encryption and authentication, although using such a certificate does not provide the level of assurance offered when you use a certificate signed by a certificate authority.

You can also reconfigure the network settings for the vSphere Replication server virtual appliance.

Note vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

Prerequisites

You deployed an optional vSphere Replication server in addition to the vSphere Replication appliance, and the server is powered on.

Procedure

1 Use a supported browser to log in to the VAMI of the additional vSphere Replication Server that you deployed.

The URL for the VAMI is https://*vr-server-address*:5480.

Use the root password that you set when you deployed the vSphere Replication server.

2 Click the **VRS** tab.

3 (Optional) Click **Configuration** to generate or upload a new certificate.

Option	Action
Generate and install a self-signed certificate	Click **Generate and Install**.
Upload an existing SSL certificate	Click **Browse** next to the **Upload PKCS#12 (*.pfx) file** text box to browse for an existing certificate, and click **Upload and Install**.

4 (Optional) Click **Security** to change the Super User password for the vSphere Replication server.

`root` is the Super User.

5 (Optional) Click the **Network** tab to change the network settings.

Option	Action
View current network settings	Click **Status**.
Set static or DHCP IPv4 or IPv6 addresses	■ Click **Address**, and select **DHCP**, **Static**, or **None** for IPv4 addresses. ■ Select **Auto** or **Static** for IPv6 addresses. If you select **Static**, type the default gateway and DNS server addresses to use.
Configure proxy server	Click **Proxy**, select the **Use a proxy server** check box, and type the proxy server address and port number.
Save Settings	If you do not click **Save Settings**, changes are discarded.

Note After the IP address of the vSphere Replication server on the target site changes, you must manually reconfigure replications on the source site to point to the new IP address.

6 (Optional) Select **VRS > Configuration > Restart** to restart the vSphere Replication service.

7 (Optional) Select **System > Reboot** to reboot the vSphere Replication server appliance.

Unregister and Remove a vSphere Replication Server

If you deployed additional vSphere Replication server instances that you no longer require, you must unregister them from the vSphere Replication appliance before you delete them.

Prerequisites

You deployed and registered a vSphere Replication server that you no longer require. Make sure it does not serve any replications, otherwise the operations will fail.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. In the left-hand pane, navigate to **Configure > Replication Servers**.
4. Select a vSphere Replication server from the list, and click **Unregister**.
5. In the Hosts and Clusters view, power off and delete the vSphere Replication server virtual machine.

Disable the Embedded vSphere Replication Server

vSphere Replication includes an embedded vSphere Replication Server by default. If you want to disable the embedded vSphere Replication server, you can do so using ssh.

Prerequisites

Make sure no replications are using the embedded server. Stop the replications or move them to a different server.

Procedure

1. Use ssh into the vSphere Replication appliance and type:

```
# /opt/vmware/hms/bin/hms-configtool -cmd reconfig -property
hms-embedded-hbr=false
```

2. Restart the HMS service.

```
# service hms restart
```

You can now unregister the embedded vSphere Replication server from the vSphere Replication user interface.

What to do next

Rebooting vSphere Replication does not automatically register the embedded server. To restore the default behavior to automatically register the embedded vSphere Replication server, type

```
# /opt/vmware/hms/bin/hms-configtool -cmd reconfig -property
hms-embedded-hbr=true
# service hms restart
```

Isolating the Network Traffic of vSphere Replication

You can isolate the network traffic of vSphere Replication from all other traffic in a data center's network.

Isolating the replication traffic helps you ensure that sensitive information is not routed to the wrong destination, and helps you enhance the network performance in the data center, because the traffic that vSphere Replication generates does not impact other types of traffic. You isolate the network traffic to the vSphere Replication Server by dedicating a VMKernel NIC on each ESXi host on the primary site that sends data to the vSphere Replication Server. See Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host.

If you are using a distributed network switch, you can take advantage of the vSphere Network I/O Control feature to set limits or shares for incoming and outgoing replication traffic on each ESXi host. The feature allows you to manage the network resources that vSphere Replication uses.

By default, the vSphere Replication appliance has one VM network adapter that is used for various traffic types.

- Management traffic between vSphere Replication Management Server and vSphere Replication Server.
- Replication traffic from the source ESXi hosts to the vSphere Replication Server.
- Traffic between vCenter Server and vSphere Replication Management Server.

You can add network adapters to the vSphere Replication appliance and use the VAMI to configure a separate IP address to use for each traffic type.

In the combined vSphere Replication appliance, the IP address that is used for management traffic between the vSphere Replication Management Server and vSphere Replication Server is localhost 127.0.0.1. Therefore, you do not need to add network adapters for this type of traffic.

When the vSphere Replication Management Server and the vSphere Replication Server run on separate appliances, you can specify a non-localhost IP address to be used by the vSphere Replication Management Server.

Note After the IP address of the vSphere Replication server on the target site changes, you must manually reconfigure replications on the source site to point to the new IP address.

In addition you must configure static routes on each ESXi host at the source site with how to communicate with the target site and the reverse. See http://kb.vmware.com/kb/2001426. For replications to flow in the opposite direction, you must configure reverse routes on the target site ESXi hosts.

Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host

You create VMkernel adapters to isolate the outgoing replication traffic on source ESXi hosts.

Note One VMkernel adapter must handle one traffic type.

Perform this procedure for every ESXi host that is used as replication source, and for which you want to isolate the replication traffic.

Prerequisites

- Verify that the vSphere Replication virtual appliance is deployed and registered with the vCenter Server.

- Verify that the ESXi host is version 6.0 or later.
- For distributed network switches, verify that you have a port group that you can dedicate to the new VMkernel adapter.

Procedure

1. In the vSphere Web Client, navigate to the ESXi host.
2. Under **Configure**, select **Networking**, and select **VMkernel adapters**.
3. Click the **Add host networking** icon  .

   The **Add Networking** wizard opens.
4. On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.
5. On the Select target device page, select a port group or a standard switch and click **Next**.
6. On the Port properties page, under VMkernel port settings, configure the IP settings and TCP/IP stack to comply with your environment.

   Note vSphere Replication requires that all components in your environment, such as vCenter Server, ESXi hosts, and the vSphere Replication appliance use the same IP version, IPv4 or IPv6.
7. Under Available services, select **vSphere Replication traffic** and click **Next**.
8. Apply the IP settings, click **Next**, and **Finish** to complete the wizard.

The VMkernel adapter that you created for outgoing vSphere Replication traffic appears in the list of adapters. The outgoing replication data from the ESXi host is sent to the vSphere Replication server through this adapter.

What to do next

You can add a vNIC to the vSphere Replication appliance and use the VAMI to configure an IP address to use for incoming replication data.

Set Up a VMkernel Adapter for vSphere Replication Traffic on a Target Host

You create VMkernel adapters to isolate the incoming replication traffic on target ESXi hosts.

Note One VMkernel adapter must handle one traffic type.

Perform this procedure for every ESXi host that is used as replication target, and for which you want to isolate the replication traffic.

Prerequisites

- Verify that the ESXi host is version 6.0 or later.
- For distributed network switches, verify that you have a port group that you can dedicate to the new VMkernel adapter.

Procedure

1. In the vSphere Web Client, navigate to the ESXi host.
2. Under **Configure**, select **Networking**, and select **VMkernel adapters**.
3. Click the **Add host networking** icon  .

   The **Add Networking** wizard opens.
4. On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.
5. On the Select target device page, select a port group or a standard switch and click **Next**.
6. On the Port properties page, under VMkernel port settings, configure the IP settings and TCP/IP stack to comply with your environment.

   Note vSphere Replication requires that all components in your environment, such as vCenter Server, ESXi hosts, and the vSphere Replication appliance use the same IP version, IPv4 or IPv6.
7. Under Available services, select **vSphere Replication NFC traffic** and click **Next**.
8. Apply the IP settings, click **Next**, and **Finish** to complete the wizard.

The VMkernel adapter that you tagged for NFC traffic appears in the list of adapters. The vSphere Replication Server routes the replication data to the adapter, and the ESXi host saves the data to a datastore.

Create a VM Network Adapter to Use for Incoming Replication Traffic on the Combined vSphere Replication Appliance

By default, the combined vSphere Replication appliance has one VM network adapter that is used by the vSphere Replication server for replication traffic, and by the vCenter Server for virtual machine management.

The IP address that is used for vSphere Replication management traffic is localhost 127.0.0.1. Because the default VM network adapter is used for different types of traffic, you can add a second adapter to the appliance, and configure vSphere Replication to use the second adapter only for incoming replication traffic.

Prerequisites

- Verify that the vSphere Replication virtual appliance is deployed and registered with the vCenter Server.
- Make a note of the IP address of the VM network adapter.

Procedure

1. Power off the vSphere Replication appliance and edit the **VM Hardware** settings to add a new VM NIC.
   a. Right-click the VM and select **Edit Settings**.
   b. From the **New Device** drop-down menu at the bottom of the **Virtual Hardware** tab, select **Network**, and click **Add**.

      The new network adapter appears in the list of devices at the right.
   c. Expand the properties of the new network adapter to verify that **Connect At Power On** is selected.

      You can assign a static MAC address or leave the text box empty to obtain an IP address automatically.
   d. Click **OK** to close the Edit Setting dialog box.
2. Power on the vSphere Replication appliance.
3. From the **Summary** tab of the vSphere Replication appliance, take a note of the IP address of the new network adapter.

   You can click **View all *XX* IP addresses** to check the IP address of the new NIC.
4. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
5. On the **VR** tab, click **Configuration**.
6. In the **IP Address for Incoming Storage Traffic** text box, enter the IP address of the new network adapter that you added.
7. Click **Apply Network Settings**.

The vSphere Replication appliance uses the IP address that you assigned only for incoming replication traffic.

Create VM Network Adapters to Isolate the Network Traffic of a vSphere Replication Server

By default, the vSphere Replication Server appliance has one VM network adapter that is used by the vSphere Replication Server for management and replication traffic.

Because the default VM network adapter is used for different types of traffic, you can add network adapters to the appliance, and configure vSphere Replication to use a separate adapter for each traffic type.

Prerequisites

Verify that you have deployed the vSphere Replication Server appliance in your environment and that it is registered as a vSphere Replication Server in the vSphere Web Client.

Procedure

1. Power off the vSphere Replication appliance and edit the **VM Hardware** settings to add a new VM NIC.
   a. Right-click the VM and select **Edit Settings**.
   b. From the **New Device** drop-down menu at the bottom of the **Virtual Hardware** tab, select **Network**, and click **Add**.

      The new network adapter appears in the list of devices at the right.
   c. Expand the properties of the new network adapter to verify that **Connect At Power On** is selected.

      You can assign a static MAC address or leave the text box empty to obtain an IP address automatically.
   d. Click **OK** to close the Edit Setting dialog box.
2. Repeat Step 1 to add another VM NIC.
3. Power on the vSphere Replication appliance.
4. From the **Summary** tab of the vSphere Replication appliance, take note of the IP address of the new network adapters.

   You can click **View all *XX* IP addresses** to check the IP addresses of the new NICs.
5. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
6. On the **VRS** tab, click **Configuration**.
7. Enter the IP addresses of the new VM NICs that you want to use to isolate the network traffic of vSphere Replication.

Option	Description
IP Address for Incoming Storage Traffic	The IP address to be used by the vSphere Replication Server for incoming replication data.
IP Address for VRMS Management Traffic	The IP address to be used by the vSphere Replication Management Server to manage the vSphere Replication Server.

8. Click **Apply Network Settings**.

The different types of traffic that vSphere Replication generates are handled by separate NICs.

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 configure vCenter Single Sign-On domains in Enhanced Linked Mode, which federates all of the Platform Services Controller instances from each of the linked 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 an Enhanced Linked Mode Environment

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 an Enhanced Linked Mode environment, that list might include vCenter Server instances from other sites. If you 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 vCenter Server instance. In this case, you must uninstall and reinstall Site Recovery Manager to select the correct vCenter Server instance.

- When you install Site Recovery Manager Server on the protected site, make sure that you 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 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.

After you have installed Site Recovery Manager, if vCenter Server migrates to a different Platform Services Controller or if the address of the Platform Services Controller changes, you can reconfigure Site Recovery Manager with the new Platform Services Controller address. For example, you can change from an embedded Platform Services Controller to an external Platform Services Controller. For information about changing Platform Services Controller, see Reconfigure vCenter Server with Embedded Platform Services Controller to vCenter Server with External Platform Services Controller in *vSphere Installation and Setup*.

You change the Platform Services Controller address by running the Site Recovery Manager installer in Modify mode.

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 an Enhanced Linked Mode Environment

In an Enhanced Linked Mode environment, 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 in Enhanced Linked Mode.

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.

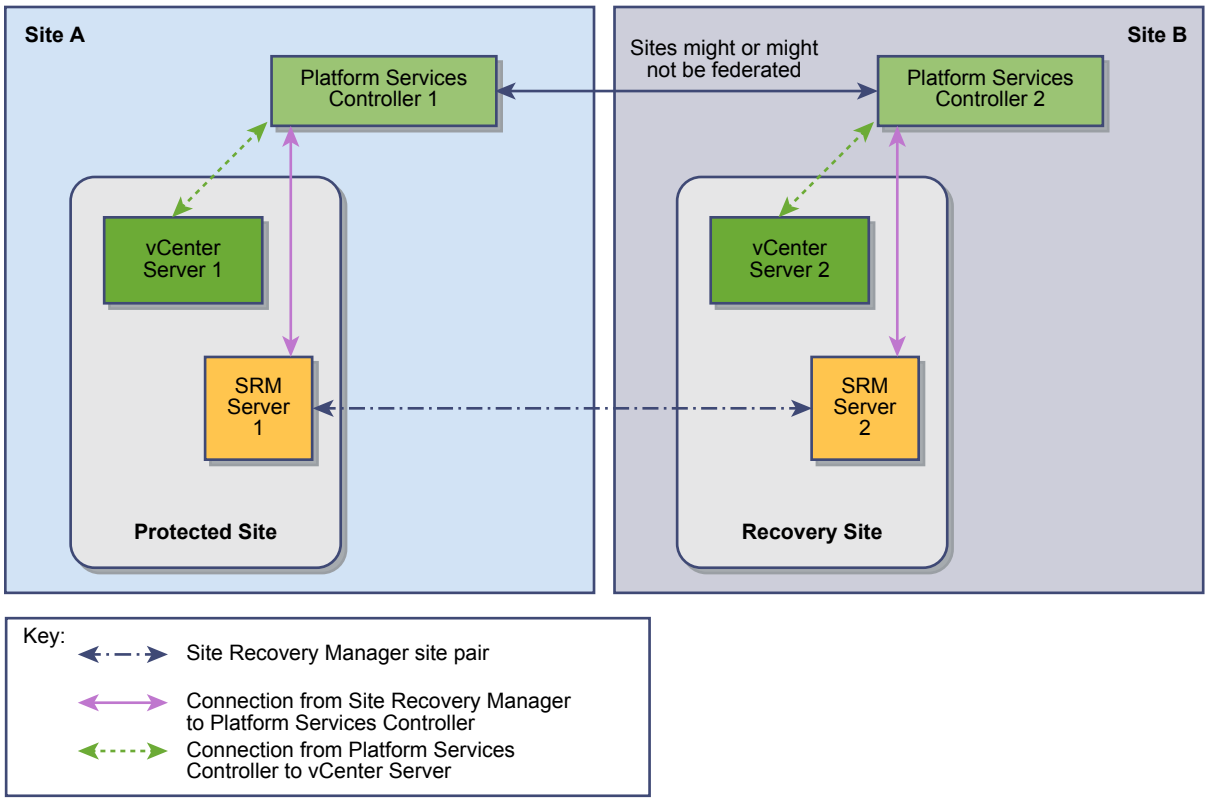
Site Recovery Manager in a Two-Site Topology with One vCenter Server Instance per Platform Services Controller

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 vCenter Single Sign-On domains that are either in Enhanced Linked Mode or are not in Enhanced Linked Mode.

Figure 7-1. Site Recovery Manager in a Two-Site Topology with One vCenter Server Instance per Platform Services Controller



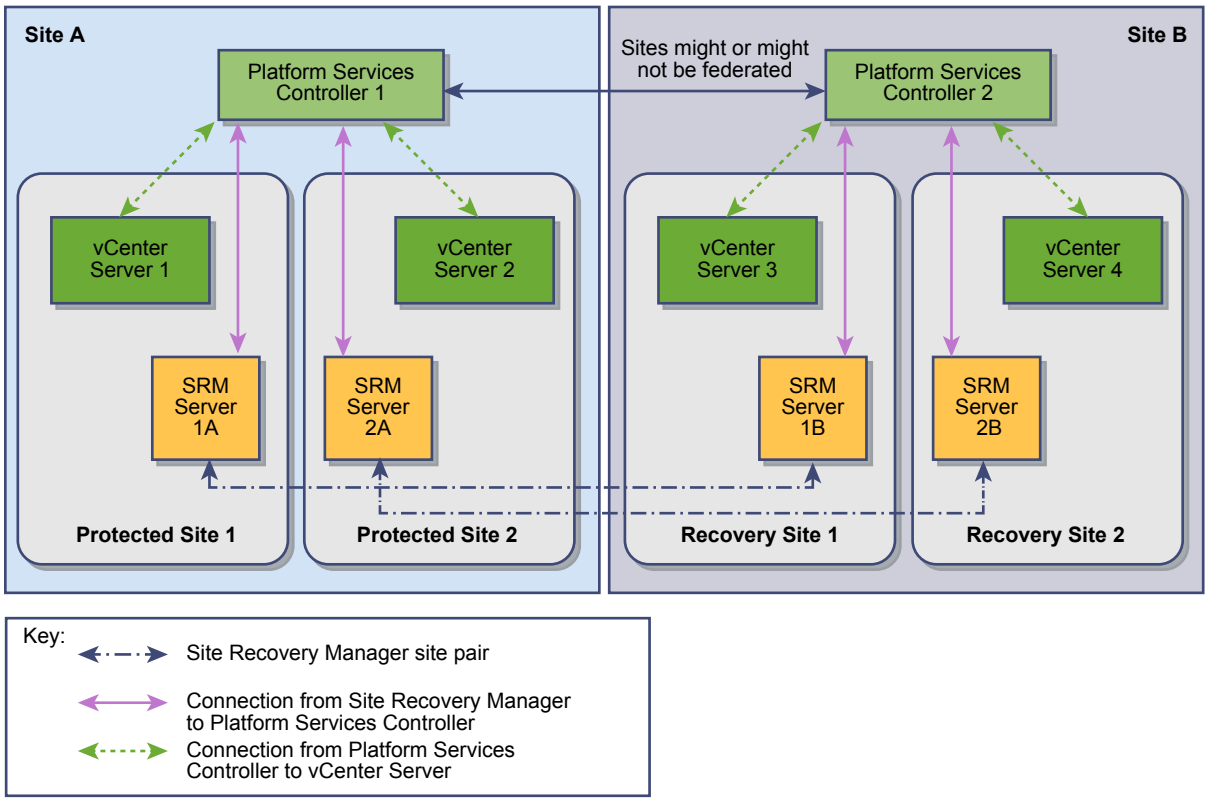
Site Recovery Manager in a Two-Site Topology with Multiple vCenter Server Instances per Platform Services Controller

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 vCenter Single Sign-On domains that are either in Enhanced Linked Mode or are not in Enhanced Linked Mode.

Figure 7-2. Site Recovery Manager in a Two-Site Topology with Two vCenter Server Instances per 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 Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.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 4 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. This verification is not performed if you install vSphere Replication after you install Site Recovery Manager Server, which might lead to incompatible versions. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Web Client to stop working. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrixes for Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.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 at the Protected Site

You must install Site Recovery Manager Server at the protected 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 an environment that uses Enhanced Linked Mode, 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, which 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. 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 and click **Next**.

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 **Use a PKCS#12 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 if the embedded database already exists.

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**.

Activate VMware Site Recovery at the Recovery Site

You must activate VMware Site Recovery at the recovery site on VMware Cloud™ on AWS.

Prerequisites

- Verify that you have deployed a Software-Defined Data Center (SDDC) on VMware Cloud™ on AWS.

Procedure

1 Log in to the VMC Console at https://vmc.vmware.com.

2 Click on your SDDC, and then click **Add-Ons**.

3 Select Site Recovery and click **Activate**.

4 Read the information on the Activate Site Recovery page and click **Activate**.

VMware Site Recovery is activated on your SDDC on VMware Cloud on AWS.

What to do next

Connect the Site Recovery Manager Server instances on the on-premises protected site and the recovery site on VMware Cloud™ on AWS. See Connect the Site Recovery Manager Server Instances on the Protected and Recovery Sites.

VMware Site Recovery Activation Fails

When you attempt to activate the VMware Site Recovery service, the activation fails.

Problem

The activation of the VMware Site Recovery service fails.

Solution

1. Click **Deactivate** and wait for a few minutes.
2. Repeat the activation procedure.

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

Before you can use VMware Site Recovery, you must connect the Site Recovery Manager Server and vSphere Replication instances on the protected and the recovery sites. This procedure is known as site pairing.

Prerequisites

- Verify that you have installed Site Recovery Manager Server instances at the protected and recovery sites

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.
4. Select the vCenter Server and the services you want to pair, and click **Next**.
5. On the Ready to complete page, review the pairing settings, and click **Finish**.

The protected and the recovery sites are connected. The pair appears under **Site Pairs** on the VMware Site Recovery Home tab.

Reconfiguring a Site Pair and Breaking a Site Pair

You can reconfigure or break an existing site pair.

If you have problems with an existing site pair, you can attempt to reconfigure the site pair with the **Reconfigure Site Pair** action. When you provide the required credentials, the reconfiguration operation attempts to repair the existing site pair.

With the **Break Site Pair** action, you can break the pairing between the Site Recovery Manager Server and vSphere Replication instances on the protected and the recovery sites. You can select which pairing to break. For example, you can break the pairing between the two Site Recovery Manager Server instances, the two vSphere Replication appliances, or both.

Note You cannot use the **Reconfigure Site Pair** action to add a missing pairing or a pairing that was manually broken with **Break Site Pair**. If your site pair is missing a pairing, you must use **New Site Pair** to configure it.

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 client connection to the remote Site Recovery Manager Server instance.

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 > Open VMware Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Enter the vCenter Single Sign-On user name and password for the remote site, and click **Login**.

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.

Network Ports for VMware Site Recovery

8

The operation of VMware Site Recovery requires certain ports to be open.

The components that make up the VMware Site Recovery service, namely vCenter Server, vSphere Web Client, Site Recovery Manager Server, the vSphere Replication appliance, and vSphere Replication servers, require different ports to be open. You must ensure that all the required network ports are open for VMware Site Recovery to function correctly.

vCenter Server and ESXi Server network port requirements for Site Recovery Manager 8.0

Site Recovery Manager requires certain ports to be open onvCenter Server, Platform Services Controller, and on ESXi Server.

Default Port	Protocol or Description	Source	Target	Description
443	HTTPS	Site Recovery Manager	vCenter Server	Default SSL Web port.
443	HTTPS	Site Recovery Manager	Platform Services Controller (PSC)	Traffic from Site Recovery Manager Server to local and remote Platform Services Controller.

Default Port	Protocol or Description	Source	Target	Description
443	HTTPS	Site Recovery Manager on the recovery site	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with configured IP customization, or callout commands on recovered virtual machines.
902	TCP and UDP	Site Recovery Manager Server on the recovery site.	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with IP customization, with configured callout commands on recovered virtual machines, or that use raw disk mapping (RDM). All NFC traffic for updating or patching the VMX files of virtual machines that are replicated using vSphere Replication use this port.

Site Recovery Manager Server 8.0 network ports

The Site Recovery Manager Server instances on the protected and recovery sites require certain ports to be open.

Default Port	Protocol or Description	Source	Target	Endpoints or Consumers
443	HTTPS	Site Recovery Manager	vCenter Server	Default SSL Web Port for incoming TCP traffic.
443	HTTPS	Site Recovery Manager	Platform Services Controller	Traffic from Site Recovery Manager Server to local and remote Platform Services Controller.

Default Port	Protocol or Description	Source	Target	Endpoints or Consumers
443	HTTPS	Site Recovery Manager on the recovery site	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with configured IP customization, or callout commands on recovered virtual machines.
902	TCP and UDP	Site Recovery Manager Server on the recovery site.	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with IP customization, with configured callout commands on recovered virtual machines, or that use raw disk mapping (RDM). All NFC traffic for updating or patching the VMX files of virtual machines that are replicated using vSphere Replication use this port.
1433	TCP	Site Recovery Manager	Microsoft SQL Server	Site Recovery Manager connectivity to Microsoft SQL Server (for Site Recovery Manager database)
1521	TCP	Site Recovery Manager	Oracle Database Server	Site Recovery Manager database connectivity to Oracle.

Default Port	Protocol or Description	Source	Target	Endpoints or Consumers
1526	TCP	Site Recovery Manager	Oracle Database Server	Site Recovery Manager database connectivity to Oracle.
9086	HTTPS	vSphere Web Client	Site Recovery Manager	All management traffic to Site Recovery Manager Server goes to this port. This includes traffic by external API clients for task automation and HTTPS interface for downloading the UI plug-in and icons. This port must be accessible from the vCenter Server proxy system. Used by vSphere Web Client to download the Site Recovery Manager client plug-in.

Site Pairing Port Requirements

Port	Source	Target	Description
9086	vCenter Server	Site Recovery Manager Server on target site	From the ESXi host at the protected site to the vSphere Replication appliance at the recovery site.
9086	Site Recovery Manager Server	Site Recovery Manager Server on target site	From the ESXi host at the protected site to the vSphere Replication appliance at the recovery site.
443	Site Recovery Manager	Platform Services Controller and vCenter Server	Site Recovery Manager to vCenter Server communication - local and remote.

Network ports that must be open on Site Recovery Manager and vSphere Replication Protected and Recovery sites

Site Recovery Manager and vSphere Replication require that the protected and recovery sites can communicate.

Port	Protocol or Description	Source	Target	Endpoints or Consumers
31031	Initial replication traffic	ESXi host	vSphere Replication appliance on the recovery site	From the ESXi host at the protected site to the vSphere Replication appliance at the recovery site
8043	HTTPS	Site Recovery Manager	vSphere Replication appliance on the recovery and protected sites	Management traffic between Site Recovery Manager instances and vSphere Replication appliances.

vSphere Replication 8.0 appliance network ports

Table 8-1.

Port	Protocol or Description	Source	Target	Endpoints or Consumers
80	TCP	vSphere Replication appliance	All local and remote PSCs in same vCenter Single Sign-On domain (only if external Platform Services Controller is used)	All management traffic to the vSphere Replication appliance goes to port 80 on the vCenter Server proxy system.
80	TCP	vSphere Replication appliance	Local vCenter Server	All management traffic to the vSphere Replication appliance goes to port 80 on the vCenter Server proxy system.
80	HTTP	vSphere Replication server in the vSphere Replication appliance	ESXi host (intra-site)	Used to establish the connection before initial replication starts.
443	TCP	vSphere Replication appliance	All local and remote Platform Services Controllers in same SSO domain (only if external Platform Services Controller is used)	All management traffic to the vSphere Replication appliance.
443	TCP	vSphere Replication appliance	Local and remote vCenter Server	All management traffic to the vSphere Replication appliance.

Table 8-1. (Continued)

Port	Protocol or Description	Source	Target	Endpoints or Consumers
902	TCP and UDP	vSphere Replication server in the vSphere Replication appliance on secondary site	ESXi host (intra-site) on secondary site	Used by vSphere Replication servers to send replication traffic to the destination ESXi hosts.
5480	HTTPS	Browser	vSphere Replication appliance	vSphere Replication virtual appliance management interface (VAMI) Web UI. Required only for on-premises site, not required for VMware Cloud on AWS site.
7444	TCP	vSphere Replication appliance	vCenter Server (intra-site)	
7444	TCP	vCenter Server	All local and remote PSCs	
8123	SOAP	vSphere Replication appliance	vSphere Replication server	Intra-site management traffic from the vSphere Replication Management server to additional vSphere Replication servers in the environment.
10443	HTTPS	vSphere Web Client on the primary site	vCenter Server Inventory Service on the target site	ThevSphere Replication UI uses the Inventory Service of the remote vCenter Server to list target datastores.
31031	Initial and ongoing replication traffic	ESXi host on source site	vSphere Replication server in the vSphere Replication appliance on the secondary site or an external vSphere Replication server on the secondary site	Initial and outgoing replication traffic from the ESXi host at the source site to the vSphere Replication appliance or vSphere Replication server at the target site.

vSphere Replication server network ports

If you deploy additional vSphere Replication servers, ensure that the subset of the ports that vSphere Replication servers require are open on those servers.

Table 8-2.

Port	Protocol or Description	Source	Target	Endpoints or Consumers
902	TCP and UDP	vSphere Replication server in the vSphere Replication appliance on secondary site	ESXi host (intra-site) on secondary site	Traffic (specifically the NFC service to the destination ESXi servers) between the vSphere Replication server and the ESXihosts on the same site.
5480	VAMI Web UI for additional vSphere Replication servers	Browser	vSphere Replication server	Administrator's web browser. Required only for on-premises site, not required for VMware Cloud on AWS site.
8123	SOAP	vSphere Replication Management server	vSphere Replication server	Intra-site management traffic from the vSphere Replication appliance or vSphere Replication Management server to the vSphere Replication servers.
31031	Initial and ongoing replication traffic	ESXi host on source site	vSphere Replication server	From the ESXi host at the protected site to the vSphere Replication appliance or vSphere Replication server at the recovery site.

Configuring The Customer Experience Improvement Program

9

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

Categories of Information That VMware Receives

This product participates in the VMware Customer Experience Improvement Program (CEIP).

Details regarding the data collected by CEIP and the purposes for which it is used by VMware are available at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

To join or leave the CEIP for this product, see *Join the Customer Experience Improvement Program in the vSphere Web Client* in the *ESXi and vCenter Server* documentation.

Reconfigure the vSphere Replication Appliance

10

If necessary, you can reconfigure the vSphere Replication appliance settings by using the virtual appliance management interface (VAMI).

You provide the settings for the vSphere Replication appliance in the **Deploy OVF** wizard when you deploy the appliance. If you selected automatic configuration of the appliance using an embedded database, you can use the vSphere Replication appliance immediately after deployment. If necessary you can modify the configuration settings of the vSphere Replication appliance after you deploy it.

- Reconfigure General vSphere Replication Settings

  If necessary, you can reconfigure the general settings of the vSphere Replication appliance at the on-premises site after deployment in the virtual appliance management interface (VAMI).

- Change the SSL Certificate of the vSphere Replication Appliance

  vSphere Replication appliance uses certificate-based authentication for all connections that it establishes with vCenter Server and remote site vSphere Replication appliances.

- Change the Password of the vSphere Replication Appliance

  You set the password of the vSphere Replication appliance when you deploy the appliance. You can change the password after installation by using the virtual appliance management interface (VAMI).

- Change Keystore and Truststore Passwords of the vSphere Replication Appliance

  To increase security, you can change the default passwords of the vSphere Replication appliance keystore and truststore. If you copy the keystores from the appliance to another machine, VMware recommends that you change the passwords before the copy operation.

- Configure vSphere Replication Network Settings

  You can review current network settings and change address and proxy settings for the on-premises vSphere Replication. You might make these changes to match network reconfigurations.

- Configure vSphere Replication System Settings

  You can view the vSphere Replication system settings to gather information about the on-premises vSphere Replication appliance. You can also set the system time zone, and reboot or shut down the appliance.

- Update the NTP Server Configuration

  Change the NTP server configuration of your vSphere Replication server if you change the NTP servers that your vSphere Replication server uses.

- Reconfigure vSphere Replication to Use an External Database

  The vSphere Replication appliance contains an embedded vPostgreSQL database that you can use immediately after you deploy the appliance, without any additional database configuration. If necessary, you can reconfigure vSphere Replication to use an external database.

- Use the Embedded vSphere Replication Database

  If you configured vSphere Replication to use an external database, you can reconfigure vSphere Replication to use the embedded database.

Reconfigure General vSphere Replication Settings

If necessary, you can reconfigure the general settings of the vSphere Replication appliance at the on-premises site after deployment in the virtual appliance management interface (VAMI).

The general settings of the vSphere Replication appliance include the name and IP address of the vSphere Replication appliance, the address and port of the vCenter Server instance to which it connects, and an administrator email address. You can change the general settings from the default values in the virtual appliance management interface (VAMI).

For example, you can reconfigure the address of the vSphere Replication appliance if you did not specify a fixed IP address when you deployed the appliance, and DHCP changes the address after deployment. Similarly, you can update the address of the vCenter Server instance if the address changes after deployment.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.

2. Review and confirm the browser security exception, if applicable, to proceed to the login page.
3. Type the root user name and password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication appliance.

4. On the **VR** tab, click **Configuration**.
5. Type the address of the vSphere Replication appliance or click **Browse** to select an IP address from a list.
6. Type the address of the vCenter Server instance to use with this installation.

   You must use the same address format that you used when you installed vCenter Server.

   For example, if you used a fully qualified domain name during installation, you must use that FQDN. If you used an IP address, you must use that IP address.

7 Type an administrator email address.

8 Click **Save and Restart Service** to apply the changes.

You reconfigured the general settings of the vSphere Replication appliance.

Change the SSL Certificate of the vSphere Replication Appliance

vSphere Replication appliance uses certificate-based authentication for all connections that it establishes with vCenter Server and remote site vSphere Replication appliances.

vSphere Replication does not use user name and password based authentication. vSphere Replication generates a standard SSL certificate when the appliance first boots and registers with vCenter Server. The default certificate policy uses trust by thumbprint.

You can change the SSL certificate, for example if your company's security policy requires that you use trust by validity and thumbprint or a certificate signed by a certification authority. You change the certificate by using the virtual appliance management interface (VAMI) of the vSphere Replication appliance. For information about the SSL certificates that vSphere Replication uses, see vSphere Replication Certificate Verification and Requirements When Using a Public Key Certificate with vSphere Replication.

See vSphere Replication Certificate Verification for details of how vSphere Replication handles certificates.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

Procedure

1 Use a supported browser to log in to the vSphere Replication VAMI.

The URL for the VAMI is https://*vr-appliance-address*:5480.

2 Type the root user name and password for the appliance.

You configured the root password during the OVF deployment of the vSphere Replication appliance.

3 (Optional) Click the **VR** tab and click **Security** to review the current SSL certificate.

4 Click **Configuration**.

5 (Optional) To enforce verification of certificate validity, select the **Accept only SSL certificates signed by a trusted Certificate Authority** check box.

6 Generate or install a new SSL certificate.

Option	Action
Generate a self-signed certificate	Click **Generate and Install**. Using a self-signed certificate provides trust by thumbprint only and might not be suitable for environments that require high levels of security. You cannot use a self-signed certificate if you selected **Accept only SSL certificates signed by a trusted Certificate Authority**.
Upload a certificate	Click **Browse** to select a PKCS#12 certificate and click **Upload and Install**. Public key certificates must meet certain requirements. See Requirements When Using a Public Key Certificate with vSphere Replication.

7 Click **Save and Restart Service** to apply the changes.

You changed the SSL certificate and optionally changed the security policy to use trust by validity and certificates signed by a certificate authority.

Note If you change a certificate on one of the source or target sites, the connection status to this site changes to `Connection issue` and you must reconnect the sites.

vSphere Replication Certificate Verification

vSphere Replication verifies the certificates of vCenter Server and remote vSphere Replication servers.

All communication between vCenter Server, the local vSphere Replication appliance, and the remote vSphere Replication appliance goes through a vCenter Server proxy at port 80. All SSL traffic is tunnelled.

vSphere Replication can trust remote server certificates either by verifying the validity of the certificate and its thumbprint or by verifying the thumbprint only. The default is to verify by thumbprint only. You can activate the verification of the certificate validity in the virtual appliance management interface (VAMI) of the vSphere Replication appliance by selecting the option **Accept only SSL certificates signed by a trusted Certificate Authority** when you upload a certificate.

Thumbprint Verification vSphere Replication checks for a thumbprint match. vSphere Replication trusts remote server certificates if it can verify the the thumbprints through secure vSphere platform channels or, in some rare cases, after the user confirms them. vSphere Replication only takes certificate thumbprints into account when verifying the certificates and does not check certificate validity.

Verification of Thumbprint and Certificate Validity vSphere Replication checks the thumbprint and checks that all server certificates are valid. If you select the **Accept only SSL certificates signed by a trusted Certificate Authority** option, vSphere Replication refuses to communicate with a server with an invalid certificate. When verifying certificate validity, vSphere Replication checks expiration dates, subject names and the certificate issuing authorities.

In both modes, vSphere Replication retrieves thumbprints from vCenter Server. vSphere Replication refuses to communicate with a server if the automatically determined thumbprint differs from the actual thumbprint that it detects while communicating with the respective server.

You can mix trust modes between vSphere Replication appliances at different sites. A pair of vSphere Replication appliances can work successfully even if you configure them to use different trust modes.

Requirements When Using a Public Key Certificate with vSphere Replication

If you enforce verification of certificate validity by selecting **Accept only SSL certificates signed by a trusted Certificate Authority** in the virtual appliance management interface (VAMI) of the vSphere Replication appliance, some fields of the certificate request must meet certain requirements.

vSphere Replication can only import and use certificates and private keys from a file in the PKCS#12 format. Sometimes these files have a `.pfx` extension.

- The certificate must be issued for the same server name as the value in the **VRM Host** setting in the VAMI. Setting the certificate subject name accordingly is sufficient, if you put a host name in the **VRM Host** setting. If any of the certificate Subject Alternative Name fields of the certificate matches the **VRM Host** setting, this will work as well.
- vSphere Replication checks the issue and expiration dates of the certificate against the current date, to ensure that the certificate has not expired.
- If you use your own certificate authority, for example one that you create and manage with the OpenSSL tools, you must add the fully qualified domain name or IP address to the OpenSSL configuration file.
  - If the fully qualified domain name of the appliance is `VR1.example.com`, add `subjectAltName = DNS: VR1.example.com` to the OpenSSL configuration file.
  - If you use the IP address of the appliance, add `subjectAltName = IP: vr-appliance-ip-address` to the OpenSSL configuration file.
- vSphere Replication requires a trust chain to a well-known root certificate authority. vSphere Replication trusts all the certificate authorities that the Java Virtual Machine trusts. Also, you can manually import additional trusted CA certificates in `/opt/vmware/hms/security/hms-truststore.jks` on the vSphere Replication appliance.
- vSphere Replication accepts MD5 and SHA1 signatures, but VMware recommends that you use SHA256 signatures.
- vSphere Replication does not accept RSA or DSA certificates with 512-bit keys. vSphere Replication requires at least 1024-bit keys. VMware recommends using 2048-bit public keys. vSphere Replication shows a warning if you use a 1024-bit key.

Change the Password of the vSphere Replication Appliance

You set the password of the vSphere Replication appliance when you deploy the appliance. You can change the password after installation by using the virtual appliance management interface (VAMI).

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
2. Type the root user name and password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication appliance.
3. Click the **VR** tab and click **Security**.
4. Type the current password in the **Current Password** text box.
5. Type the new password in the **New Password** and the **Confirm New Password** text boxes.

   The password must be a minimum of eight characters. vSphere Replication does not support blank passwords.
6. Click **Apply** to change the password.

Change Keystore and Truststore Passwords of the vSphere Replication Appliance

To increase security, you can change the default passwords of the vSphere Replication appliance keystore and truststore. If you copy the keystores from the appliance to another machine, VMware recommends that you change the passwords before the copy operation.

The keystore and truststore passwords might be stored in an access restricted `config` file. vSphere Replication has the following keystores:

- `/opt/vmware/hms/security/hms-keystore.jks`, which contains the vSphere Replication appliance private key and certificate.
- `/opt/vmware/hms/security/hms-truststore.jks`, which contains additional CA certificates besides the ones that Java already trusts.

Procedure

1. To change the `hms-keystore.jks` password, log in as root.

2 Obtain the current hms-keystore password.

```
# /opt/vmware/hms/bin/hms-configtool -cmd list | grep keystore
```

Example of the output `hms-keystore-password = old_password`

3 Change the hms-keystore password.

```
 # /usr/java/default/bin/keytool -storepasswd -storepass old_password -new new_password -
keystore /opt/vmware/hms/security/hms-keystore.jks
```

4 Change the vSphere Replication appliance private key password.

```
# /usr/java/default/bin/keytool -keypasswd -alias jetty -keypass
old_password -new new_password -storepass new_password -keystore
/opt/vmware/hms/security/hms-keystore.jks
```

5 Update the configuration with the new password.

```
/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property
'hms-keystore-password=new_password'
```

6 Update the tomcat `server.xml` file with the new password.

```
sed -i -- 's/old_password/new_password/g' /var/opt/apache-tomcat/conf/server.xml
```

7 Reboot the appliance for the changes to take effect.

```
# reboot
```

8 To change the hms-truststore.jks password, log in as root.

9 Obtain the current hms-truststore password.

```
# /opt/vmware/hms/bin/hms-configtool -cmd list | grep truststore
```

Example of the output: `hms-truststore-password = old_password`

10 Change the hms-truststore password.

```
# /usr/java/default/bin/keytool -storepasswd -storepass
old_password -new new_password -keystore
/opt/vmware/hms/security/hms-truststore.jks
```

11 Update the configuration with the new password.

```
/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property
'hms-truststore-password=new_password'
```

12 Restart the vSphere Replication service.

```
# service hms restart
```

Configure vSphere Replication Network Settings

You can review current network settings and change address and proxy settings for the on-premises vSphere Replication. You might make these changes to match network reconfigurations.

Note vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

Procedure

1 Use a supported browser to log in to the vSphere Replication VAMI.

The URL for the VAMI is https://*vr-appliance-address*:5480.

2 Type the root user name and password for the appliance.

You configured the root password during the OVF deployment of the vSphere Replication appliance.

3 Click the **Network** tab.

4 Click **Status** to review current network settings.

5 Click **Address** to review or modify IPv4 and IPv6 address settings.

IP Address Type	Option	Description
IPv4	DHCP	DHCP is not recommended if the IP address of the appliance might change if it reboots.
IPv4	Static	With a static IPv4 address, you can modify the IP settings, DNS settings, net mask, and host name information.
IPv4	None	Disabling IPv4 addresses forces the use of IPv6 addresses only.
IPv6	Auto	Automatic assignment of IPv6 addresses is not recommended if the IP address of the appliance might change if it reboots.
IPv6	Static	With a static IPv6 address, you can modify the IP address and the address prefix.

6 Click **Save Settings**.

If you do not click **Save Settings**, changes are discarded.

Note After the IP address of the vSphere Replication server on the target site changes, you must manually reconfigure replications on the source site to point to the new IP address.

7 Click **Proxy** to review or modify proxy settings.

a Select **Use a proxy server** to use a proxy server.

b Enter a proxy server name in the **HTTP Proxy Server** text box.

c Enter a proxy port in the **Proxy Port** text box.

d (Optional) Enter a proxy server user name and password.

8 Click **Save Settings**.

If you do not click **Save Settings**, changes are discarded.

What to do next

A network address change might require you to reconnect the source and target sites and might also require a change of certificate if you have activated verification of certificate validity.

Configure vSphere Replication System Settings

You can view the vSphere Replication system settings to gather information about the on-premises vSphere Replication appliance. You can also set the system time zone, and reboot or shut down the appliance.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

Procedure

1 Use a supported browser to log in to the vSphere Replication VAMI.

The URL for the VAMI is https://*vr-appliance-address*:5480.

2 Type the root user name and password for the server.

3 Click the **System** tab.

4 Click **Information**.

You can review information about vSphere Replication, and reboot or shutdown the appliance.

Option	Description
Vendor	Vendor name
Appliance Name	vSphere Replication appliance name

Option	Description
Appliance Version	vSphere Replication version
Hostname	Hostname of the appliance
OS Name	Operating system name and version
Reboot	Reboots the virtual appliance
Shutdown	Shuts down the virtual appliance

Shutting down the vSphere Replication appliance stops configured replications and prevents you from configuring replication of new virtual machines as well as modifying existing replication settings.

5 Click **Time Zone**.

Option	Description
System Time Zone	Time zones are available from the drop-down list
Save Settings	Saves settings
Cancel Changes	Discards changes

Update the NTP Server Configuration

Change the NTP server configuration of your vSphere Replication server if you change the NTP servers that your vSphere Replication server uses.

Prerequisites

- Verify that the remote console of your vSphere Replication virtual machine is open and that you use **`root`** credentials.
- Verify that the status of the NTP service of your vSphere Replication server is *running*.

Procedure

1 Open the `/etc/ntp.conf` file.

2 Update the IP address or name of the NTP server or servers.

3 (Optional) To add an additional NTP server add the following line.

```
server your_NTP_server_IP_address_or_name
```

4 Save the change and close `ntp.conf` file.

5 Run the `service ntp reload` command to reload the NTP configuration.

Your vSphere Replication server is synchronized with the new NTP server.

Reconfigure vSphere Replication to Use an External Database

The vSphere Replication appliance contains an embedded vPostgreSQL database that you can use immediately after you deploy the appliance, without any additional database configuration. If necessary, you can reconfigure vSphere Replication to use an external database.

Each vSphere Replication appliance requires its own database. If the database at either site is corrupted, vSphere Replication does not function. vSphere Replication cannot use the vCenter Server database because it has different database schema requirements. However, if you do not use the embedded vSphere Replication database you can use the vCenter database server to create and support an external vSphere Replication database.

You might need to use an external database to improve performance or load balancing, for easier backup, or to meet your company's database standards.

Note vSphere Replication server inside the vSphere Replication appliance uses its own embedded database and config files. Configuring VRMS to use external database does not provide protection of losing the vSphere Replication appliance or any Additional vSphere Replication Server appliance.

If you reinitialize the database after you deploy vSphere Replication, you must go to the vSphere Replication virtual appliance management interface (VAMI) to reconfigure vSphere Replication to use the new database connection.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.
- You must create and configure the external database before you connect it to vSphere Replication. See Databases that vSphere Replication Supports for the configuration requirements for each supported type of database.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
2. Review and confirm the browser security exception, if applicable, to proceed to the login page.
3. Type the root user name and password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication appliance.
4. On the **VR** tab, click **Configuration**.
5. Select **Manual configuration** to specify a configuration or select **Configure from an existing VRM database** to use a previously established configuration.

6 In the DB text boxes, provide information about the database for vSphere Replication to use.

Option	Setting
DB Type	Select **SQL Server** or **Oracle**.
DB Host	IP address or fully qualified domain name of the host on which the database server is running.
DB Port	Port on which to connect to the database.
DB Username	Username for the vSphere Replication database user account that you create on the database server.
DB Password	Password for the vSphere Replication database user account that you create on the database server.
DB Name	Name of the vSphere Replication database instance.

7 Click **Save and Restart Service** to apply the changes.

You configured vSphere Replication to use an external database instead of the database that is embedded in the vSphere Replication appliance.

Databases that vSphere Replication Supports

The vSphere Replication virtual appliance includes the VMware standard embedded vPostgreSQL database. You can also configure vSphere Replication to use an external database.

Automated migration between the embedded database and any external databases is not supported in any direction. If you must configure an external database, you must manually migrate the data or manually recreate all replications.

You can configure vSphere Replication to use one of the supported external databases.

- Microsoft SQL
- Oracle

External vPostgreSQL databases are not supported. vSphere Replication supports the same database versions as vCenter Server. For supported database versions, see the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

- Configure Microsoft SQL Server for vSphere Replication

  When you create a Microsoft SQL Server database, you must configure it correctly to support vSphere Replication.

- Configure Oracle Server for vSphere Replication

  You must configure an Oracle Server database correctly to support vSphere Replication.

Configure Microsoft SQL Server for vSphere Replication

When you create a Microsoft SQL Server database, you must configure it correctly to support vSphere Replication.

You use SQL Server Management Studio to create and configure an SQL Server database for vSphere Replication.

This information provides the general steps that you must perform to configure an SQL Server database for vSphere Replication. For instructions about how to perform the relevant steps, see the SQL Server documentation.

Prerequisites

Verify that the SQL Server Browser service is running.

Procedure

1. Select **Mixed Mode Authentication** when you create the database instance.

   The vSphere Replication appliance and the database server run on different hosts, so you must use mixed mode authentication and not Windows Authentication.

2. Use either a named instance or the default instance of SQL Server.

   If you intend to use dynamic TCP ports, you must use a named instance of SQL Server.

3. Enable TCP on the database instance.

4. Set a TCP port.

Option	Action
Static TCP port	Set the TCP port to the default of 1433.
Dynamic TCP port	a Use a named instance of SQL Server. You can only use dynamic ports with a named instance of SQL Server. b Select the **Show DB URL** check box in the virtual appliance management interface (VAMI) of the vSphere Replication appliance. c Modify the **DB URL** value. Replace port=*port_number* with instanceName=*instance_name* in the URL. d Use the `PortQuery` command from a remote machine to check that the port on which the SQL Server Browser service runs is not blocked by a firewall. The SQL Server Browser runs on port 1434. Type the `PortQuery` command in a terminal window. `PortQry.exe –n Machine_Name –p UDP –e 1434`

5. Verify that the firewall on the database server permits inbound connections on the TCP port.

6. Create the vSphere Replication security login.

7. Create the vSphere Replication database and set the vSphere Replication security login as the database owner.

8. Keep the dbo user and dbo schema settings.

   Because the vSphere Replication security login is the database owner, it maps to the database user dbo and uses the dbo schema.

Configure Oracle Server for vSphere Replication

You must configure an Oracle Server database correctly to support vSphere Replication.

You create and configure an Oracle Server database for vSphere Replication 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 vSphere Replication. For instructions about how to perform the relevant steps, see the Oracle documentation.

Procedure

1. When creating the database instance, select UTF-8 encoding.
2. Create the vSphere Replication database user account.
3. If they are not selected already, select the **CONNECT** and **RESOURCE** roles.

   These roles provide the privileges that vSphere Replication requires.

Use the Embedded vSphere Replication Database

If you configured vSphere Replication to use an external database, you can reconfigure vSphere Replication to use the embedded database.

The vSphere Replication appliance includes an embedded vPostgreSQL database. The embedded database is preconfigured for use with vSphere Replication and is enabled if you accept the default **Performs initial configuration of the appliance using an embedded database** option when you deploy the vSphere Replication appliance. If you reconfigured vSphere Replication to use an external database after deployment, you can switch to the embedded database. After switching databases, you must manually configure replications again as the replication management data is not migrated to the database. You can use the reset feature in the embedded database to drop replications, site connections and external vSphere Replication registrations.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.
- You must have reconfigured vSphere Replication to use an external database.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
2. Review and confirm the browser security exception, if applicable, to proceed to the login page.
3. Type the root user name and password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication appliance.
4. On the **VR** tab, click **Configuration**.
5. Select **Configure using the embedded database**.
6. (Optional) Click **Reset Embedded Database** to reset the database.

7 Click **Save and Restart Service** to apply the changes.

You configured vSphere Replication to use the embedded vSphere Replication database.

Modifying and Uninstalling Site Recovery Manager

11

You can modify an existing Site Recovery Manager installation to reflect changes in your infrastructure. To uninstall Site Recovery Manager cleanly, you must follow the correct procedure.

- 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.

- Reconfigure the Connection Between Sites

  You must reconfigure the connection between the sites if you made modifications to your Site Recovery Manager installation.

- Break the Site Pairing and Connect to a New Remote Site

  To connect a Site Recovery Manager site to a new remote site, you must remove the existing Site Recovery Manager configurations and break the pairing between the existing sites.

- 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 on the on-premises site.

- Rename a Site Recovery Manager Site

  After you have installed Site Recovery Manager, you can rename a site directly in the VMware Site Recovery interface.

- Uninstall Site Recovery Manager on the on-premises site

  If you no longer require Site Recovery Manager, you must follow the correct procedure to cleanly uninstall Site Recovery Manager.

- 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.

Modify a Site Recovery Manager Server Installation

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

Installing Site Recovery Manager Server binds the installation to a number of values that you supply, including the vCenter Server instance to extend, the Site Recovery Manager database type, DSN and credentials, the 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 Platform Services Controller address, if the vCenter Server instance that Site Recovery Manager extends moves to a different Platform Services Controller
- 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 can change the Platform Services Controller address if vCenter Server migrated to a different Platform Services Controller after the initial installation of Site Recovery Manager. **Important** If you change the Platform Services Controller address, you must reconfigure the connection between the Site Recovery Manager sites after you have updated the installation.
HTTPS Port	Change the Platform Services Controller port if it changed after the initial installation of Site Recovery Manager.
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
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 Verify 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. This only appears if you use the embedded database. You cannot change this value.
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	This only appears if you use the embedded database. You cannot change this value.
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.

What to do next

When the modification operation is finished and the Site Recovery Manager Server restarts, log in to the vSphere Web Client to check the connection between the sites. If the connection is broken, or if you changed the Platform Services Controller address, reconfigure the site pairing. For instructions about how to reconfigure the site pairing, see Reconfigure the Connection Between Sites.

Reconfigure the Connection Between Sites

You must reconfigure the connection between the sites if you made modifications to your Site Recovery Manager installation.

You cannot reconfigure the site pairing to connect Site Recovery Manager to a different vCenter Server instance. You reconfigure an existing pairing to update Site Recovery Manager on both sites if the infrastructure has changed on one or both of the sites.

- You upgraded Site Recovery Manager to a new version.
- You changed the Site Recovery Manager certificate.
- You changed the Platform Services Controller or vCenter Server certificate.
- You changed the Platform Services Controller address.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 Select **Site Pair > Summary**, and click **Reconfigure Site Pair**.

   You can initiate the reconfiguration from either site, even if you only changed the installation on one of the sites.

4 Enter the address of the Platform Services Controller on the remote site, provide the vCenter Single Sign-On username and password, and click **Next**.

5 Select the vCenter Server and the services you want to pair, and click **Next**.

If the Platform Services Controller manages more than one vCenter Server instance, the other vCenter Server instances appear in the list but you cannot select a different instance. You can only select the vCenter Server instance that Site Recovery Manager already extends.

6 On the Ready to complete page, review the pairing settings, and click **Finish**.

Break the Site Pairing and Connect to a New Remote Site

To connect a Site Recovery Manager site to a new remote site, you must remove the existing Site Recovery Manager configurations and break the pairing between the existing sites.

Site pairing makes modifications on both Site Recovery Manager sites. You cannot reconfigure an existing pairing between Site Recovery Manager sites to connect Site Recovery Manager on one site to a new Site Recovery Manager site. You must remove all configuration from both sites in the existing pair, then break the connection between the sites before you can configure a new site pairing. You cannot break the site pairing until you have removed all existing configurations between the sites.

Prerequisites

- You have an existing Site Recovery Manager installation with two connected sites.
- Make a full backup of the Site Recovery Manager database on both sites by using the tools that the database software provides. For instructions about how to back up the embedded database, see Back Up and Restore the Embedded vPostgres Database.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 Select the **Recovery Plans** tab, right-click on a recovery plan and select **Delete**.

You cannot delete recovery plans that a running.

4 Select the **Protection Groups** tab, click on a protection group, and select the **Virtual Machines** tab.

5 Highlight all virtual machines, right-click, and select **Remove Protection**.

Removing protection from a virtual machine deletes the placeholder virtual machine from the recovery site. Repeat this operation for all protection groups.

6 In the **Protection Groups** tab, right-click a protection group and select **Delete** .

You cannot delete a protection group that is included in a recovery plan. You cannot delete vSphere Replication protection groups that contain virtual machines on which protection is still configured.

7 Select **Site Pair > Configure**, and remove all inventory mappings.

a Click each of the **Network Mappings**, **Folder Mappings**, and **Resource Mappings** tabs.

b In each tab, select a site, right-click a mapping, and select **Delete**.

8 For both sites, click **Placeholder Datastores**, right-click the placeholder datastore, and select **Remove**.

9 Select **Site Pair > Summary**, and click **Break Site Pair**.

Breaking the site pairing removes all information related to registering Site Recovery Manager with Site Recovery Manager, vCenter Server and the Platform Services Controller on the remote site.

The connection between the sites is broken. You can reconfigure Site Recovery Manager to connect to a new remote site.

What to do next

- Install a new Site Recovery Manager instance on the new remote site. For instructions about installing Site Recovery Manager, see Install Site Recovery Manager Server at the Protected Site.

  Important The new Site Recovery Manager instance must have the same Site Recovery Manager extension ID as the existing site.

- Optionally uninstall Site Recovery Manager Server from the previous remote site. For instructions about uninstalling Site Recovery Manager Server, see the steps of Uninstall Site Recovery Manager on the on-premises site from the **Break Pairing** step onwards.
- Reconfigure the inventory mappings and placeholder datastore mappings to map objects on the existing site to objects on the new remote site. For instructions about configuring mappings, see *VMware Site Recovery Administration*.
- Reconfigure the replication of virtual machines from the existing site to the new remote site. For information about configuring vSphere Replication, see *Replicating Virtual Machines* in *VMware Site Recovery Administration*.
- Create new protection groups and recovery plans to recover virtual machines to the new remote site. For information about creating protection groups and recovery plans, see *VMware Site Recovery Administration*.

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 on the on-premises site.

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

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.

Rename a Site Recovery Manager Site

After you have installed Site Recovery Manager, you can rename a site directly in the VMware Site Recovery interface.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 Click **Site Pair > Summary**, and in the Site Recovery Manager box click **Rename** next to the name of the site you want to rename.

4 Enter a new name for the site and click **Save**.

Uninstall Site Recovery Manager on the on-premises site

If you no longer require Site Recovery Manager, you must follow the correct procedure to cleanly uninstall Site Recovery Manager.

Installing Site Recovery Manager, creating inventory mappings, protecting virtual machines by creating protection groups, and creating and running recovery plans makes significant changes on both Site Recovery Manager sites. Before you uninstall Site Recovery Manager, you must remove all Site Recovery Manager configurations from both sites in the correct order. If you do not remove all configurations before uninstalling Site Recovery Manager, some Site Recovery Manager components, such as placeholder virtual machines, might remain in your infrastructure.

If you use Site Recovery Manager with vSphere Replication, you can continue to use vSphere Replication after you uninstall Site Recovery Manager.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 Select the **Recovery Plans** tab, right-click on a recovery plan and select **Delete**.

You cannot delete recovery plans that a running.

4 Select the **Protection Groups** tab, click on a protection group, and select the **Virtual Machines** tab.

5 Highlight all virtual machines, right-click, and select **Remove Protection**.

Removing protection from a virtual machine deletes the placeholder virtual machine from the recovery site. Repeat this operation for all protection groups.

6 In the **Protection Groups** tab, right-click a protection group and select **Delete** .

You cannot delete a protection group that is included in a recovery plan. You cannot delete vSphere Replication protection groups that contain virtual machines on which protection is still configured.

7 Select **Site Pair > Configure**, and remove all inventory mappings.

a Click each of the **Network Mappings**, **Folder Mappings**, and **Resource Mappings** tabs.

b In each tab, select a site, right-click a mapping, and select **Delete**.

8 For both sites, click **Placeholder Datastores**, right-click the placeholder datastore, and select **Remove**.

9 Select **Site Pair > Summary**, and click **Break Site Pair**.

10 Log into the Site Recovery Manager Server host for the on-premises site.

11 Use Windows Control Panel to uninstall Site Recovery Manager, selecting the option **Delete Site Recovery Manager Data**.

Do not uninstall the Site Recovery Manager database before you uninstall Site Recovery Manager.

12 (Optional) If you use the embedded database, use Windows Control Panel to uninstall the Site Recovery Manager Embedded Database.

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 from the Site Pair tab **Site Pair > Configure > Advanced Settings** in the VMware Site Recovery plug-in.

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 any advanced settings.