Site Recovery Manager Installation and Configuration

Site Recovery Manager 5.5

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 Site Recovery Manager Installation and Configuration

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

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

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

Intended Audience

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

Updated Information

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

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

Revision	Description
EN-001111-10	Updated Requirements When Using Trusted SSL Certificates with Site Recovery Manager with new requirements for public authority certificates with internal server names.
EN-001111-09	■ Added recommendation to select different datastores as the replication target and for placeholders in Configure a Placeholder Datastore. ■ Added that you cannot map individual hosts from clusters to other objects in Select Inventory Mappings.
EN-001111-08	■ Added that advanced settings are not retained during upgrade in Information That Site Recovery Manager Upgrade Preserves. ■ Expanded the upgrade prerequisites in Prepare for Site Recovery Manager Upgrade. ■ Added that only in-place upgrade is possible to upgrade to an update or patch release in In-Place Upgrade of Site Recovery Manager Server and Upgrade the Site Recovery Manager Server with Migration. ■ Corrected the path to SRA downloads on myvmware.com and clarified that you can download certified SRAs from third party sites in Configure the Upgraded Site Recovery Manager Installation and Install Storage Replication Adapters.
EN-001111-07	■ Corrected Compatibility of vSphere Replication with Other vSphere Features to state that using vSphere Replication with Virtual SAN storage is supported on both the source and target sites. ■ Expanded Chapter 11 Installing Site Recovery Manager to Use with a Shared Recovery Site to state that converting a one-to-one configuration into a shared recovery site configuration is possible. Removed the statement from Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration that stated that such a conversion is not possible. ■ Added that shared protected site and multiple-to-multiple site configurations are supported in Chapter 11 Installing Site Recovery Manager to Use with a Shared Recovery Site. Removed the recommendation against implementing shared protected site configurations from Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration. ■ Added that Site Recovery Manager does not support replication to multiple targets in Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration. ■ Added topic Upgrade Site Recovery Manager in a Shared Recovery Site Configuration.
EN-001111-06	Corrected note about installations with custom permissions requiring upgrade with migration in In-Place Upgrade of Site Recovery Manager Server.
EN-001111-05	Further clarification of Subject Name requirements in Requirements When Using Trusted SSL Certificates with Site Recovery Manager.

Revision	Description
EN-001111-04	Corrected information about Subject Name in Requirements When Using Trusted SSL Certificates with Site Recovery Manager.
EN-001111-03	Clarified supported upgrade paths in Chapter 6 Upgrading Site Recovery Manager.
EN-001111-02	■ Added statement of full support for VMware Virtual SAN in vSphere 5.5u1 and vSphere Replication 5.5.1. ■ Added Bandwidth Requirements for vSphere Replication. ■ Clarified how Site Recovery Manager interacts with vSphere Flash Read Cache in Using Array-Based Replication with Site Recovery Manager and Compatibility of vSphere Replication with Other vSphere Features. ■ Expanded the information about the use of SQL authentication and Windows authentication in Requirements when Using Microsoft SQL Server with Site Recovery Manager and Create an ODBC System DSN for Site Recovery Manager. ■ Clarified that the Site Recovery Manager administrator email address is not used by Site Recovery Manager Server in Install the Site Recovery Manager Server and Modify the Installation of Site Recovery Manager Server. ■ Clarified that you upgrade vSphere Replication to 5.5 by using the downloadable ISO image and you install 5.5.x update releases by using the VAMI or vSphere Update Manager in Chapter 9 Upgrading vSphere Replication. ■ Added Update vCenter Server IP Address in vSphere Replication Management Server.
EN-001111-01	Clarified that upgrade to vSphere Replication 5.5 is only available via the downloadable ISO image in Chapter 9 Upgrading vSphere Replication.
EN-001111-00	Initial release.

Overview of VMware vCenter Site Recovery Manager

1

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

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

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

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

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

- At the protected site, Site Recovery Manager shuts down virtual machines cleanly, 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.

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

About Protected Sites and Recovery Sites

In a typical Site Recovery Manager installation, the protected site provides business-critical datacenter services. The recovery site is an alternative facility 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.

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

- Each site must have at least one datacenter.
- If you are using array-based replication, identical replication technologies must be available at both sites and the sites must be paired.
- 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 non-critical virtual machines on the recovery site.
- The sites must be connected by a reliable IP network. If you are using array-based replication, ensure that your network connectivity meets the arrays' network requirements.

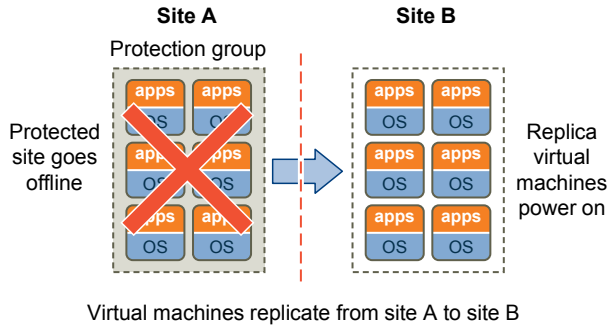
- The recovery site should have access to comparable public and private networks as the protected site, although not necessarily the same range of network addresses.

Pairing the Protected and Recovery Sites

You must pair the protected and recovery sites before you can use Site Recovery Manager.

Site Recovery Manager includes a wizard that guides you through the site-pairing process. You must establish a connection between the sites and you must provide authentication information for the two sites so that they can exchange information. Site pairing requires vSphere administrative privileges at both sites. To begin the site-pairing process, you must know the user name and password of a vSphere administrator at each site. If you are using vSphere Replication, you must pair the vSphere Replication appliances.

Figure 1-1. Site Recovery Manager Site Pairing and Recovery Process



Bidirectional Protection

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

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

For information about the numbers of virtual machines for which you can establish bidirectional protection between two sites, see http://kb.vmware.com/kb/2034768.

Heterogeneous Configurations on the Protected and Recovery Sites

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

Example: Heterogenous Configurations on the Protected and Recovery Sites

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

- Site A in Japan:
  - Site Recovery Manager Server runs on Windows Server 2008 in the Japanese locale
  - Site Recovery Manager extends a vCenter Server Appliance instance
  - Site Recovery Manager Server uses an SQL Server 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

Using Array-Based Replication with Site Recovery Manager

When you use array-based replication, one or more storage arrays at the protected site replicate data to peer arrays at the recovery site. With storage replication adapters (SRAs), you can integrate Site Recovery Manager with a wide variety of arrays.

To use array-based replication with Site Recovery Manager, you must configure replication first before you can configure Site Recovery Manager to use it.

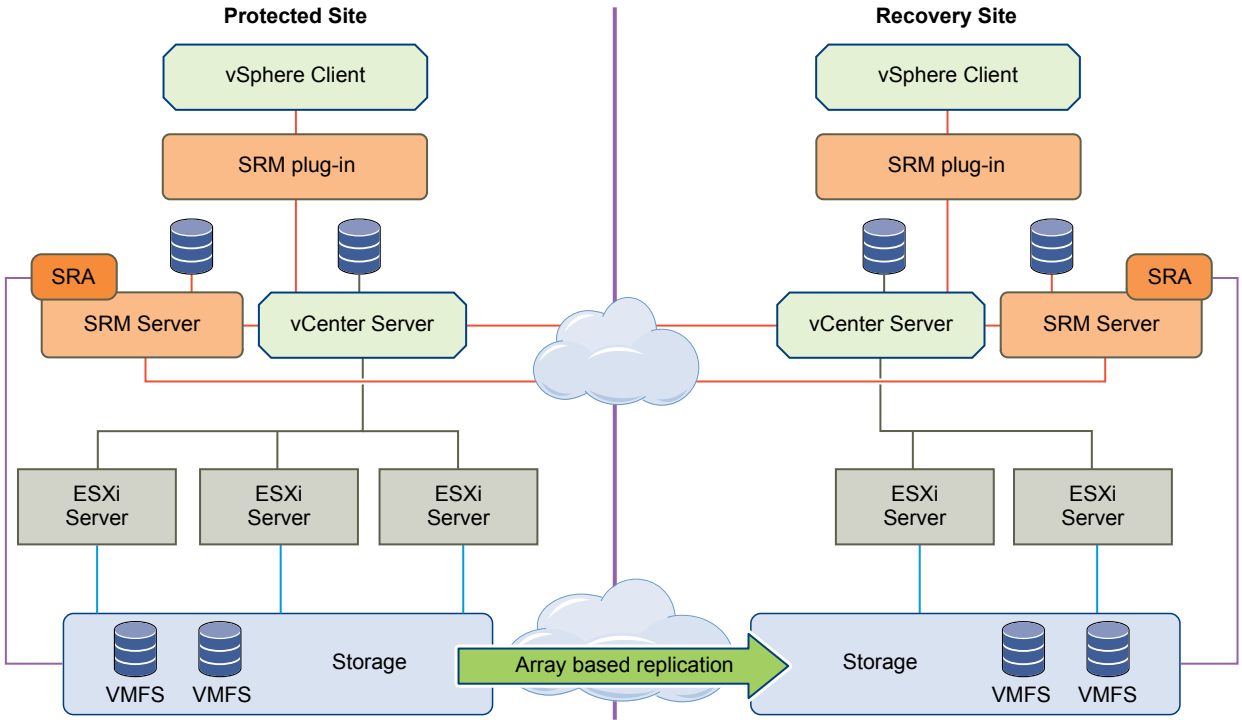
If your storage array supports consistency groups, Site Recovery Manager is compatible with vSphere Storage DRS and vSphere Storage vMotion. You can use Storage DRS and Storage vMotion to move virtual machine files within a consistency group that Site Recovery Manager protects. If your storage array does not support consistency groups, you cannot use Storage DRS and Storage vMotion in combination with Site Recovery Manager.

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, Site Recovery Manager disables Flash Read Cache on disks when it starts the virtual machines on the recovery site. Site Recovery Manager sets the reservation to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take a note of 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 manually restore the original Flash Read Cache setting on the virtual machine.

Storage Replication Adapters

Storage replication adapters are not part of a Site Recovery Manager release. Your array vendor develops and supports them. You must install an SRA specific to each array that you use with Site Recovery Manager on the Site Recovery Manager Server host. Site Recovery Manager supports the use of multiple SRAs.

Figure 1-2. Site Recovery Manager Architecture with Array-Based Replication



Using vSphere Replication with Site Recovery Manager

Site Recovery Manager can use vSphere Replication to replicate data to servers at the recovery site.

You deploy vSphere Replication as a virtual appliance. The vSphere Replication appliance contains two components.

- A vSphere Replication management server:
  - Configures the vSphere Replication server on the recovery site.
  - Enables replication from the protected site.
  - Authenticates users and checks their permissions to perform vSphere Replication operations.
  - Manages and monitors the replication infrastructure.
- A vSphere Replication server:
  - Listens for virtual machine updates from the vSphere Replication host agent on the protected site.
  - Applies the updates to the virtual disks on the recovery site.

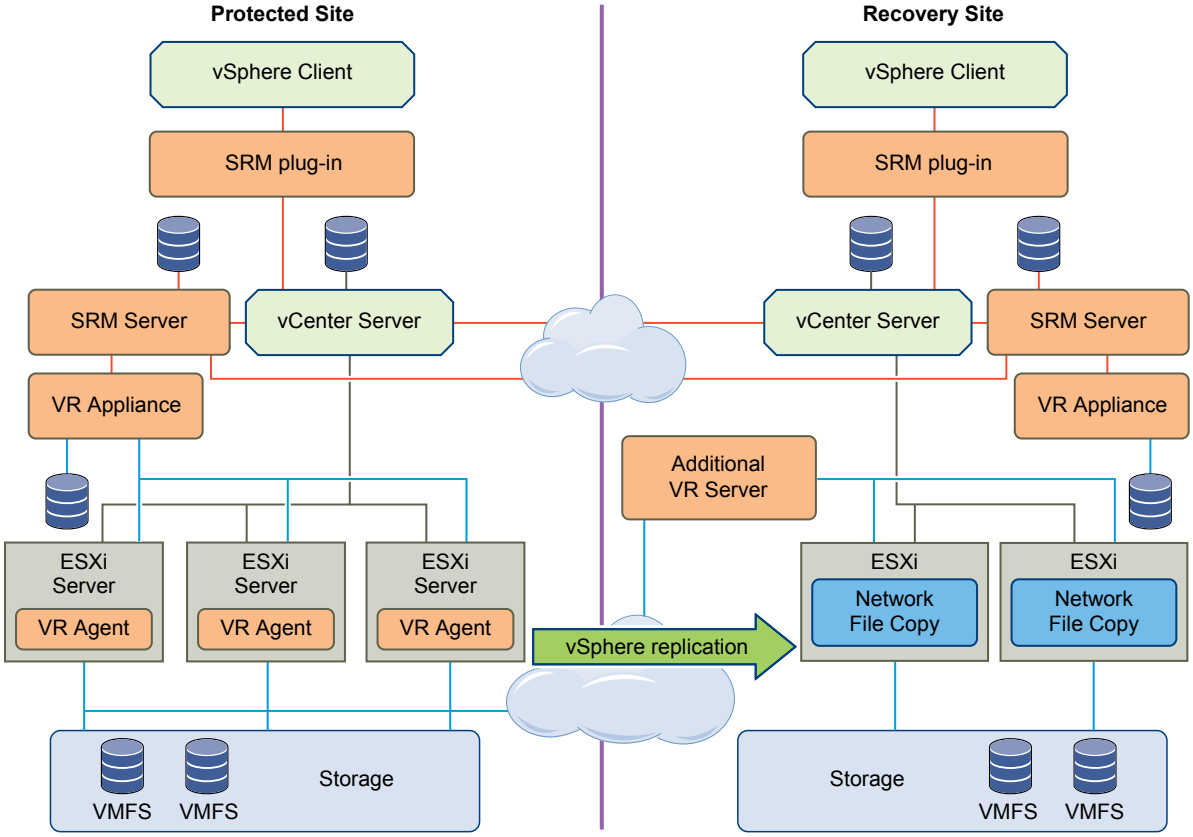
If necessary, you can deploy multiple vSphere Replication servers on a site to balance the replication load across your virtual infrastructure.

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.

vSphere Replication does not require storage arrays. The vSphere Replication storage replication source and target can be any storage device, including, but not limited to, storage arrays.

You can configure vSphere Replication to regularly create and retain snapshots of protected virtual machines on the recovery site. Taking multiple point-in-time (PIT) snapshots of virtual machines allows you to retain more than one replica of a virtual machine on the recovery site. Each snapshot reflects the state of the virtual machine at a certain point in time. You can select which snapshot to recover when you use vSphere Replication to perform a recovery.

Figure 1-3. Site Recovery Manager Architecture with vSphere Replication



Using vSphere Replication and Site Recovery Manager with vSphere Storage vMotion and vSphere Storage DRS

vSphere Replication is compatible with vSphere Storage vMotion and vSphere Storage DRS on the protected site. You can use Storage vMotion and Storage DRS to move the disk files of a virtual machine that vSphere Replication protects, with no impact on replication.

Using vSphere Replication and VMware Virtual SAN Storage with Site Recovery Manager

You can use VMware Virtual SAN storage with vSphere Replication and Site Recovery Manager.

Note VMware Virtual SAN is a fully supported feature of vSphere 5.5u1.

- You can use Virtual SAN in production environments with vSphere Replication 5.5.1 and vSphere 5.5u1.
- Virtual SAN is an experimental feature in vSphere 5.5. You can perform testing with Virtual SAN with vSphere Replication 5.5.0 and vSphere 5.5, but it is not supported for use in production environments. See the release notes for the vSphere Replication 5.5.0 release for information about how to enable Virtual SAN in vSphere 5.5.

How vSphere Replication Works

With vSphere Replication, you can configure replication of a virtual machine from a source site to a target site, monitor and manage the status of the replication, and recover the virtual machine at the target site.

When you configure a virtual machine for replication, the vSphere Replication agent sends changed blocks in the virtual machine disks from the source site to the target site, where they are applied to the copy of the virtual machine. This process occurs independently of the storage layer. vSphere Replication performs an initial full synchronization of the source virtual machine and its replica copy. You can use replication seeds to reduce the amount of time and bandwidth required for the initial replication.

During replication configuration, you can set a recovery point objective (RPO) and enable retention of instances from multiple points in time (MPIT).

As administrator, you can monitor and manage the status of the replication. You can view information for incoming and outgoing replications, source and target site status, replication issues, and for warnings and errors.

vSphere Replication stores replication configuration data in its embedded database. You can also configure vSphere Replication to use an external database.

Contents of the vSphere Replication Appliance

The vSphere Replication appliance provides all the components that vSphere Replication requires.

- An embedded database that stores replication configuration and management information.
- A vSphere Replication management server:
  - Configures the vSphere Replication server.
  - Enables, manages, and monitors replications.
  - Authenticates users and checks their permissions to perform vSphere Replication operations.
- A vSphere Replication server that provides the core of the vSphere Replication infrastructure.

You can use vSphere Replication immediately after you deploy the appliance. The vSphere Replication appliance provides a virtual appliance management interface (VAMI) that you can use to reconfigure the appliance after deployment, if necessary. For example, you can use the VAMI to change the appliance security settings, change the network settings, or configure an external database. You can deploy additional vSphere Replication Servers using a separate .ovf package.

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.

Table 1-2. 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. You can 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	You can move the disk files of a replicated virtual machine on the source site using Storage DRS with no impact on the ongoing replication.
VMware Virtual SAN datastore	Fully supported in vSphere Replication 5.5.1. Experimental support in vSphere Replication 5.5.	You can use VMware Virtual SAN datastores as the source and target datastores when configuring replications. **Note** VMware Virtual SAN is a fully supported feature of vSphere 5.5u1. ■ You can use Virtual SAN in production environments with vSphere Replication 5.5.1 and vSphere 5.5u1. ■ Virtual SAN is an experimental feature in vSphere 5.5. You can perform testing with Virtual SAN with vSphere Replication 5.5.0 and vSphere 5.5, but it is not supported for use in production environments. See the release notes for the vSphere Replication 5.5.0 release for information about how to enable Virtual SAN in vSphere 5.5.
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. Disable DPM on the target site to allow enough hosts as replication targets.

Table 1-2. Compatibility of vSphere Replication with Other vSphere Features (Continued)

vSphere Feature	Compatible with vSphere Replication	Description
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, Site Recovery Manager disables Flash Read Cache on disks when it starts the virtual machines on the recovery site. Site Recovery Manager sets the reservation to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take a note of 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 manually restore the original Flash Read Cache setting on the virtual machine.
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.

Using Array-Based Replication and vSphere Replication with Site Recovery Manager

You can use a combination of array-based replication and vSphere Replication in your Site Recovery Manager deployment.

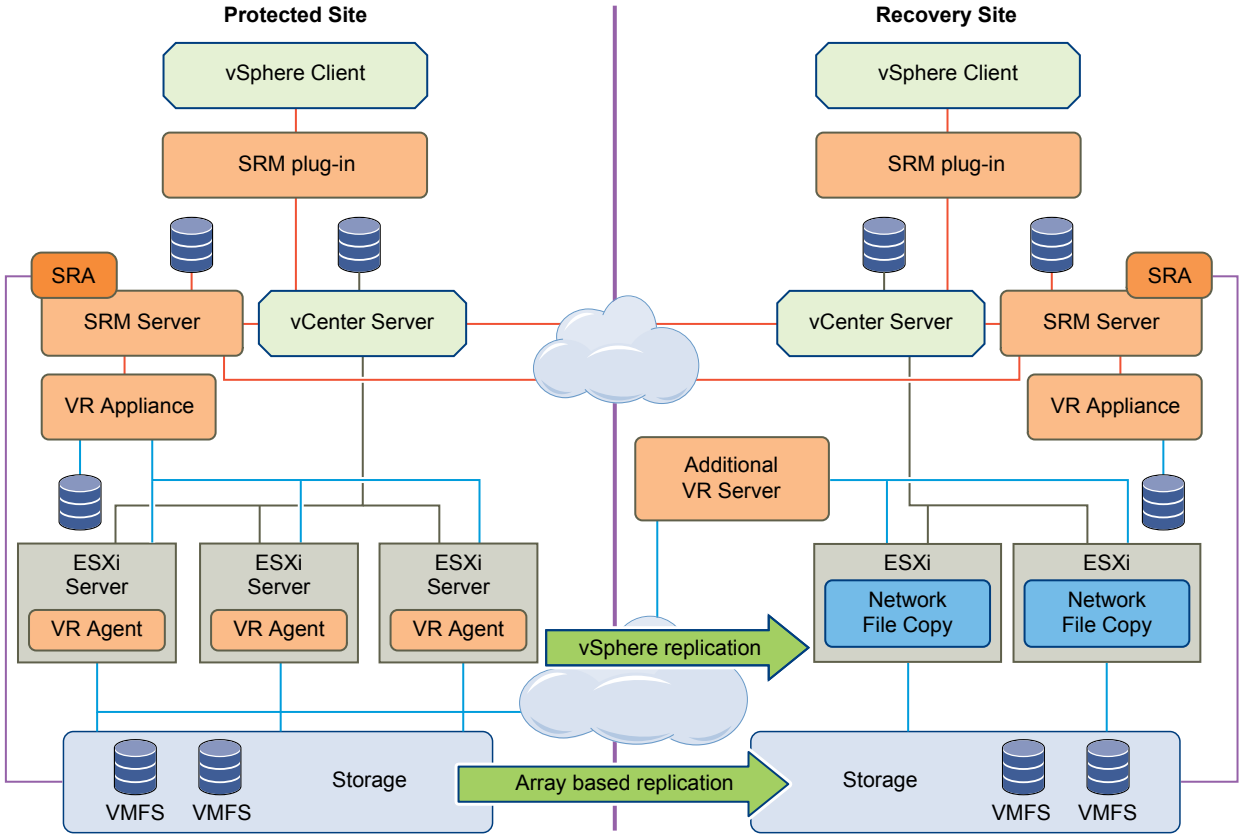
To create a mixed Site Recovery Manager deployment that uses array-based replication and vSphere Replication, you must configure the protected and recovery sites for both types of replication.

- Set up and connect the storage arrays and install the appropriate storage replication adapters (SRA) on both sites.
- Deploy vSphere Replication appliances on both sites and configure the connection between the appliances.
- Configure virtual machines for replication using either array-based replication or vSphere Replication, as appropriate.

  Note Do not attempt to configure vSphere Replication on a virtual machine that resides on a datastore that you replicate by using array-based replication.

You create array-based protection groups for virtual machines that you configure with array-based replication, and vSphere Replication protection groups for virtual machines that you configure with vSphere Replication. You cannot mix replication types in a protection group. You can mix array-based protection groups and vSphere Replication protection groups in the same recovery plan.

Figure 1-4. Site Recovery Manager Architecture with Array-Based Replication and vSphere Replication



Site Recovery Manager and vCenter Server

Site Recovery Manager Server operates as an extension to the vCenter Server at a site. Because the Site Recovery Manager Server depends on vCenter Server for some services, you must install and configure vCenter Server at a site before you install Site Recovery Manager.

Site Recovery Manager takes advantage of vCenter Server services, such as storage management, authentication, authorization, and guest customization. Site Recovery Manager also uses the standard set of vSphere administrative tools to manage these services.

You can use Site Recovery Manager and vSphere Replication with the vCenter Server Appliance or with a standard vCenter Server installation. You can have vCenter Server Appliance on one site and a standard vCenter Server installation on the other.

How Changes to vCenter Server Inventory Affect Site Recovery Manager

Because Site Recovery Manager protection groups apply to a subset of the vCenter Server inventory, changes to the protected inventory made by vCenter Server administrators and users can affect the integrity of Site Recovery Manager protection and recovery. Site Recovery Manager depends on the availability of certain objects, such as virtual machines, folders, resource pools, and networks, in the

vCenter Server inventory at the protected and recovery sites. Deletion of resources such as folders or networks that are referenced by recovery plans can invalidate the plan. Renaming or relocating objects in the vCenter Server inventory does not affect Site Recovery Manager, unless it causes resources to become inaccessible during test or recovery.

Site Recovery Manager can tolerate certain changes at the protected site without disruption.

- Deleting protected virtual machines.
- Deleting an object for which an inventory mapping exists.

Site Recovery Manager can tolerate certain changes at the recovery site without disruption.

- Moving placeholder virtual machines to a different folder or resource pool.
- Deleting an object for which an inventory map exists.

Site Recovery Manager and the vCenter Server Database

If you update the vCenter Server installation that Site Recovery Manager extends, do not reinitialize the vCenter Server database during the update. Site Recovery Manager stores identification information about all vCenter Server objects in the Site Recovery Manager database. If you reinitialize the vCenter Server database, the identification data that Site Recovery Manager has stored no longer matches identification information in the new vCenter Server instance and objects are not found.

Site Recovery Manager and Other vCenter Server Solutions

You can run other VMware solutions such as vCenter Update Manager, vCenter Server Heartbeat, VMware Fault Tolerance, vSphere Storage vMotion, vSphere Storage DRS, and vCenter CapacityIQ in deployments that you protect using Site Recovery Manager. However, use caution before connecting other VMware solutions to the vCenter Server instance to which the Site Recovery Manager Server is connected. Connecting other VMware solutions to the same vCenter Server instance as Site Recovery Manager might cause problems when you upgrade Site Recovery Manager or vSphere. Check the compatibility and interoperability of these solutions with Site Recovery Manager before by consulting the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

Site Recovery Manager System Requirements

2

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

Table 2-1. Site Recovery Manager System Requirements

Component	Requirement
Processor	2.0GHz or higher Intel or AMD x86 processor
Memory	2GB minimum
Disk Storage	5GB minimum
Networking	1 Gigabit recommended for communication between Site Recovery Manager sites. Use a trusted network for the management of ESXi hosts.

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

- Site Recovery Manager Licensing

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

- Site Recovery Manager Network Ports

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

- Operational Limits of Site Recovery Manager

  Each Site Recovery Manager server can support a certain number of virtual machines, protection groups, datastore groups, vSphere Replication management server instances per host, and vSphere Replication servers per vSphere Replication appliance.

- 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.

Site Recovery Manager Licensing

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

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

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

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

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

Site Recovery Manager License Keys and Protected and Recovery Sites

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

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

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

Example: Site Recovery Manager Licenses Required for Recovery and Reprotect

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

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

Site Recovery Manager Network Ports

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

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

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

For a list of all the ports that must be open for Site Recovery Manager and vSphere Replication, see http://kb.vmware.com/kb/1009562.

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

Operational Limits of Site Recovery Manager

Each Site Recovery Manager server can support a certain number of virtual machines, protection groups, datastore groups, vSphere Replication management server instances per host, and vSphere Replication servers per vSphere Replication appliance.

For details about the operational limits of Site Recovery Manager and vSphere Replication, see http://kb.vmware.com/kb/2034768.

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 usevSphere 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

3

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

The Site Recovery Manager database is a critical part of a Site Recovery Manager installation. You must create the Site Recovery Manager 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 an SQL Server database on the other.

If you are updating Site Recovery Manager to a new version, you can use the existing database. Before you attempt a Site Recovery Manager environment 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 *Site Recovery Manager Compatibility Matrixes*.

- Requirements when Using Microsoft SQL Server with Site Recovery Manager

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

- Requirements for Using Oracle Server with Site Recovery Manager

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

- Create an ODBC System DSN for Site Recovery Manager

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

Requirements when Using Microsoft SQL Server with Site Recovery Manager

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

You use SQL Server Management Studio to create and configure an SQL Server database and to create the database user account for Site Recovery Manager to use.

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 Windows authentication to connect to SQL Server, and SQL Server runs on a different machine from Site Recovery Manager Server, use a domain account that also has administrative privileges on the Site Recovery Manager Server machine. Instead of using a local administrator account, use the same domain account to install Site Recovery Manager Server. You must use this domain account so that the Site Recovery Manager installer can perform database operations during installation. After installing Site Recovery Manager Server, ensure that the Site Recovery Manager service is running under the domain account, rather than under the local system account.
  - If SQL Server is running on the same machine as Site Recovery Manager Server and you use Windows authentication, the same requirements apply as for a remote SQL Server, but you can use a local administrator account instead of a domain user account.
  - 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.
  - Grant the Site Recovery Manager database user account the **bulk insert**, **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.

General:: Default database	Type the database name.
Server Roles	Select the **Public** and **Admin** roles.
User Mapping	Select the check box to map the login to the database.

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

Requirements for Using Oracle Server with Site Recovery Manager

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

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

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

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

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

Create an ODBC System DSN for Site Recovery Manager

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

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

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

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** or **SQL Server Native Client 11.0**.
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	Type a name for this data source, for example **SRM**.
Description	Type a description of the data source, for example **SRM**.
Server	Select the running database instance to which to connect or type 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**.

c 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	Type a name for this data source, for example **SRM**.
Description	Type a description of the data source, for example **SRM**.
TNS Service Name	Type the address of the database server in the format ***database_server_address*:1521/*database_name***.
User ID	Type the database user name.

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

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

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

The ODBC driver for your database is ready to use.

Site Recovery Manager Authentication

4

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

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

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

Credential-Based Authentication

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

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

Custom Certificate-Based Authentication

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

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

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

Certificate Warnings

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

Requirements When Using Trusted SSL Certificates with Site Recovery Manager

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

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

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

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

- The certificates must have a Subject Name value that must be the same for both members of the Site Recovery Manager pair. The Subject Name value can be constructed from the following components.
  - A Common Name (CN) attribute. A string such as **SRM** is appropriate here. The CN attribute is obligatory.

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

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

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

  ```
  extendedKeyUsage = serverAuth, clientAuth
  ```

- The Site Recovery Manager certificate password must not exceed 31 characters.
- The Site Recovery Manager certificate key length must be a minimum of 2048-bits.
- Site Recovery Manager accepts certificates with MD5RSA and SHA1RSA signature algorithms, but these are not recommended. Use SHA256RSA or stronger signature algorithms.

Installing Site Recovery Manager

5

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

Site Recovery Manager requires a vCenter Server instance of the equivelent version at each site before you install Site Recovery Manager Server. The Site Recovery Manager installer must be able to connect with this vCenter Server instance during installation.

After you install the Site Recovery Manager Server instances, you can download the Site Recovery Manager client plug-in from the Site Recovery Manager Server instance by using the **Manage Plug-ins** menu from your vSphere Client. You use the Site Recovery Manager client plug-in to configure and manage Site Recovery Manager at each site.

Procedure

1 Install the Site Recovery Manager Server

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

2 Install the Site Recovery Manager Client Plug-In

   To install the Site Recovery Manager client plug-in, you use a vSphere Client to connect to the vCenter Server at the protected or recovery site. You download the plug-in from the Site Recovery Manager Server and enable it in the vSphere Client.

3 Connect to Site Recovery Manager

   You use the vSphere Client to connect to Site Recovery Manager.

4 Connect the Protected and Recovery Sites

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

5 Install the Site Recovery Manager License Key

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

6 Modify the Installation of Site Recovery Manager Server

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

7 Repair the Installation of Site Recovery Manager Server

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

Install the Site Recovery Manager Server

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

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

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

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

Prerequisites

- Install the same version of vCenter Server as the version of Site Recovery Manager to install.
- Configure and start the Site Recovery Manager database service before you install the Site Recovery Manager Server. See Chapter 3 Creating the Site Recovery Manager Database.
- Download the Site Recovery Manager installation file to a folder on the machine on which to install Site Recovery Manager.
- 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.
- Verify that you have the following information:
  - A user account with sufficient privileges to install Site Recovery Manager. This account is often an Active Directory domain administrator, but can also be a local administrator.
  - The fully qualified domain name (FQDN) or IP address of the site's vCenter Server instance. The server must be running and accessible during Site Recovery Manager installation. You must use the address format that you use to connect Site Recovery Manager to vCenter Server when you later pair the Site Recovery Manager sites. Using FQDNs is preferred, but if that is not universally possible, use IP addresses for all cases.
  - The user name and password of the vCenter Server administrator account.
  - A user name and password for the Site Recovery Manager database.

- If you are using certificate-based authentication, the pathname to an appropriate certificate file. See Chapter 4 Site Recovery Manager Authentication and Requirements When Using Trusted SSL Certificates with Site Recovery Manager.

Procedure

1. Double-click the Site Recovery Manager installer icon, select an installation language, and click **OK**.
2. Follow the prompts and accept the license agreement.
3. Click **Change** to change the folder in which to install Site Recovery Manager, select a target volume, and click **Next**.

   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 170 characters including the end slash, and cannot include non-ASCII characters.
4. Select whether to install vSphere Replication and click **Next**.

   If you connect Site Recovery Manager to a vCenter Server instance that is already running vSphere Replication as a registered extension, you must still select the **Install vSphere Replication** option. Selecting this option installs components that Site Recovery Manager requires to work with vSphere Replication. You can also install vSphere Replication after you install Site Recovery Manager by running the installer again in Repair mode.
5. Type information about the vCenter Server instance at the site where you are installing Site Recovery Manager and click **Next**.

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

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

If you are using certificate-based authentication, there is no prompt to accept the certificate.

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

Option	Description
Use credential-based authentication	a Select **Automatically generate certificate** and click **Next**. b Type text values for your organization and organization unit, typically your company name and the name of your group in the company.
Use certificate-based authentication	a Select **Use a PKCS #12 certificate file** and click **Next**. b Type the path to the certificate file. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. c Type the certificate password. d The local host value must be the same as the Subject Alternative Name (SAN) value of the Site Recovery Manager Server certificate. This is usually the fully qualified domain name of the Site Recovery Manager Server host.

8 Type the administrator and host configuration information and click **Next**.

Option	Description
Local Site Name	A name for this installation of Site Recovery Manager. A suggested name is generated, but you can type any name. It cannot be the same name that you use for another Site Recovery Manager installation with which this one will be paired.
Administrator E-mail	Email address of the Site Recovery Manager administrator, for potential use by vCenter Server. This field is required even though email notifications are not implemented in this version.
Additional E-mail	An optional email address of another Site Recovery Manager administrator, for potential use by vCenter Server.
Local Host	Name or IP address of the local host. This value is obtained by the Site Recovery Manager installer and needs to be changed only if it is incorrect. For example, the local host might have more than one network interface and the one detected by the Site Recovery Manager installer is not the interface you want to use. If you use certificate-based authentication, the **Local Host** value must be the same as the SAN value of the supplied certificate. This is usually the fully qualified domain name of the Site Recovery Manager Server host.
Listener Ports	SOAP and HTTP port numbers to use.
API Listener Port	SOAP port number for API clients to use.

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

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

Option	Action
Database Client	Select a database client type from the drop-down menu.
Data Source Name	Select an existing 64-bit DSN from the drop-down menu. You can also click **ODBC 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.

Option	Action
Username	Type a user ID valid for the specified database.
Password	Type the password for the specified user ID.
Connection Count	Type the initial connection pool size. If all connections are in use and a new one is needed, a connection is created as long as it does not exceed the maximum number of connections allowed. It is faster for Site Recovery Manager to use a connection from the pool than to create one. In most cases, it is not necessary to change this setting. Before changing this setting, consult with your database administrator.
Max Connections	Type the maximum number of database connections that can be open simultaneously. If the database administrator has 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 changing this setting, consult with your database administrator.

10 Click **Install**.

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

What to do next

Repeat the installation process on the recovery site.

Install the Site Recovery Manager Client Plug-In

To install the Site Recovery Manager client plug-in, you use a vSphere Client to connect to the vCenter Server at the protected or recovery site. You download the plug-in from the Site Recovery Manager Server and enable it in the vSphere Client.

When you install the Site Recovery Manager Server, the Site Recovery Manager client plug-in becomes available as a download from the vCenter Server instance that the Site Recovery Manager Server installation extends. You can download, install, and enable the Site Recovery Manager client plug-in on any host where a vSphere Client is installed.

Prerequisites

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

Procedure

1 Start the vSphere Client and connect to vCenter Server at either the protected or recovery site.

2 Select **Plugins > Manage Plug-ins**.

3 Under **Available Plug-ins**, locate **VMware vCenter Site Recovery Manager Extension** and click **Download and Install**.

4 Review and accept the certificate.

This step only occurs if you use certificate-based authentication.

5 After the download finishes, click **Run** to start the installation wizard, select the installation language, and click **OK**.

6 Click **Next** to start the installation, then click **Next** again at the VMware Patents page.

7 Select **I accept the terms in the license agreement**, and click **Next**.

8 Click **Install**.

9 When the installation finishes, click **Finish**.

   If the installation replaced any open files, you are prompted to shut down and restart Windows.

Connect to Site Recovery Manager

You use the vSphere Client to connect to Site Recovery Manager.

Site Recovery Manager does not require that you connect to a specific Site Recovery Manager site in a Site Recovery Manager deployment. You can change the protected and recovery sites by connecting to vCenter Server at either site.

Prerequisites

- Verify that you installed Site Recovery Manager Server instances at the protected and recovery sites.
- Verify that you installed the Site Recovery Manager client plug-in in the vSphere Client.
- Verify that you have a user account that is paired with a role that has the necessary permissions to connect to Site Recovery Manager.

Procedure

1 Open a vSphere Client and connect to vCenter Server on either the protected site or the recovery site.

2 On the vSphere Client Home page, click the **Site Recovery** icon.

Connect the Protected and Recovery Sites

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

When you enter the address of the vCenter Server instance on the recovery site, take a note of the address format that you use. You must use the same address format that you use to connect the Site Recovery Manager sites for later configuration operations. You must enter exactly the same vCenter Server address format here that you entered when installing the Site Recovery Manager Server at the recovery site. If you used an IP address when installing the Site Recovery Manager Server at the recovery site, use an IP address to pair the Site Recovery Manager sites. If you entered a hostname when installing the Site Recovery Manager Server, use the same hostname to pair the Site Recovery Manager sites.

Important Site Recovery Manager does not support network address translation (NAT). If the network that you use to connect the Site Recovery Manager sites uses NAT, attempting to connect the sites results in an error. Use credential-based authentication and network routing without NAT when connecting the sites.

If you are using an untrusted certificate, several of the steps in this procedure produce certificate warnings. You can ignore the warnings.

Prerequisites

- Verify that you installed Site Recovery Manager Server instances at the protected and recovery sites.
- Verify that you installed the Site Recovery Manager client plug-in in the vSphere Client.

Procedure

1. In the vSphere Client, connect to the Site Recovery Manager Server on the protected site.
2. Click **Sites** in the left pane and click **Configure Connection** on either the **Summary** tab or the **Getting Started** tab.
3. On the **Remote Site Information** page, type the IP address or hostname of the vCenter Server instance at the recovery site and the port to which to connect and click **Next**.

   Port 80 is used for the initial connection to the remote site. After the initial HTTP connection is made, the two sites establish an SSL connection for subsequent connections.
4. On the **vCenter Server Authentication** page, provide the vCenter administrator user name and password for the recovery site and click **Next**.

   You must enter exactly the same information here that you entered when installing the Site Recovery Manager Server at the recovery site.
5. On the Complete Connections page, click **Finish** after all of the site paring steps have completed successfully.
6. In the **Remote vCenter Server** window, enter credentials for the vCenter Server instance at the recovery site.
7. Connect another vSphere Client instance to the vCenter Server instance on the recovery site and go to the Site Recovery Manager interface.
8. In the **Remote vCenter Server** window, enter credentials for the vCenter Server instance at the protected site.

Install the Site Recovery Manager License Key

The 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.

Site Recovery Manager uses the vSphere licensing infrastructure for license management. Additionally, vSphere itself needs to be licensed sufficiently for Site Recovery Manager to protect and recover virtual machines.

Procedure

1. Open a vSphere Client and connect to a vCenter Server instance on which Site Recovery Manager is installed.

2 On the vSphere Client Home page, click **Licensing**.

3 For the **View by** mode, select **Product**.

4 Click **Manage vSphere Licenses**.

5 On the Add License Keys page, enter the Site Recovery Manager license key in the **vSphere license keys** text box, type an optional label for the key, and click **Add License Keys**.

6 Review the details of the Site Recovery Manager license and click **Next**.

7 Click the **Solutions** tab in the Assign Licenses page.

8 Select **VMware vCenter Site Recovery Manager** in the **Asset** panel.

9 Select the Site Recovery Manager license key from the list of available licenses, and click **Next**.

10 Click **Next** to skip the Remove License Keys page.

11 Click **Finish** to confirm the license changes.

What to do next

Repeat the process to assign Site Recovery Manager license keys to all appropriate vCenter Server instances.

Modify the Installation of Site Recovery Manager Server

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

Installing the 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 DSN and credentials, the type of authentication, and so on. The Site Recovery Manager installer supports a modify mode that allows you to change certain values that you configured when you installed Site Recovery Manager Server.

- The user name and password of the vCenter Server administrator
- The type of authentication (certificate-based or credential-based), the authentication details, or both
- The user name, password, and connection numbers for the Site Recovery Manager database

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

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

Prerequisites

Verify that you have administrator privileges on the Site Recovery Manager Server or that you are a member of the Administrators group. If you are a member of the Administrators group but you are not an administrator, disable Windows User Account Control (UAC) before you attempt the change operation.

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. Type the username and password for the vCenter Server instance.

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

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

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

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

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

9 Select **Use existing database** or **Recreate the database** and click **Next**.

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

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

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

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

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

Repair the Installation of Site Recovery Manager Server

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

Running the installer in repair mode fixes missing or corrupted files, shortcuts, and registry entries in the Site Recovery Manager Server installation. Running the installer in repair mode also allows you to install vSphere Replication if you did not do so when you installed Site Recovery Manager.

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

Prerequisites

Verify that you have administrator privileges on the Site Recovery Manager Server or that you are a member of the Administrators group. If you are a member of the Administrators group but you are not an administrator, disable Windows User Account Control (UAC) before you attempt the change operation.

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 (Optional) If you did not install vSphere Replication when you installed Site Recovery Manager, select whether to install it now.

   If you already installed vSphere Replication, this option does not appear.

7 Click **Install** to repair the installation and optionally install vSphere Replication.

   The installer makes the requested repairs, optionally installs vSphere Replication, and restarts the Site Recovery Manager Server.

Upgrading Site Recovery Manager

6

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

Due to update release schedules, upgrading to certain 5.5.x releases is not supported for all 5.0.x and 5.1.x releases. Check **Solution Upgrade Path > VMware vCenter Site Recovery Manager** in the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php? before you upgrade, to ensure that your upgrade path is supported.

Important Upgrade versions of Site Recovery Manager earlier than 5.0 to a Site Recovery Manager 5.0.x release before you upgrade to Site Recovery Manager 5.5.x. Upgrading vCenter Server directly from 4.1.x to 5.5 is a supported upgrade path. However, upgrading Site Recovery Manager directly from 4.1.x to 5.5.x is not a supported upgrade path. When upgrading a vCenter Server 4.1.x instance that includes a Site Recovery Manager installation, you must upgrade vCenter Server to version 5.0.x before you upgrade Site Recovery Manager to 5.0.x. If you upgrade vCenter Server from 4.1.x to 5.5 directly, when you attempt to upgrade Site Recovery Manager from 4.1.x to 5.0.x, the Site Recovery Manager upgrade fails. Site Recovery Manager 5.0.x cannot connect to a vCenter Server 5.5 instance.

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

To revert to Site Recovery Manager 5.0.x or 5.1.x after upgrading to Site Recovery Manager 5.5, see Revert to a Previous Release of Site Recovery Manager.

- Information That Site Recovery Manager Upgrade Preserves

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

- Types of Upgrade that Site Recovery Manager Supports

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

- Order of Upgrading vSphere and Site Recovery Manager Components

  You must upgrade the components in your vSphere and Site Recovery Manager environment in the correct order.

- Upgrade Site Recovery Manager

  You perform several tasks to upgrade Site Recovery Manager.

- Revert to a Previous Release of Site Recovery Manager

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

Information That Site Recovery Manager Upgrade Preserves

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

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

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

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

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

Types of Upgrade that Site Recovery Manager Supports

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

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

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

Order of Upgrading vSphere and Site Recovery Manager Components

You must upgrade the components in your vSphere and Site Recovery Manager environment in the correct order.

You must upgrade certain components of your vSphere environment before you upgrade Site Recovery Manager. You must upgrade Site Recovery Manager Server before you upgrade other Site Recovery Manager components and vSphere Replication.

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

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

1. Upgrade vCenter Server on the protected site.
2. Upgrade Site Recovery Manager Server on the protected site.
3. Upgrade the storage replication adapters (SRA) on the protected site.
4. Upgrade the vSphere Replication appliance on the protected site.
5. Upgrade any additional vSphere Replication server instances on the protected site.
6. Upgrade vCenter Server on the recovery site.
7. Upgrade Site Recovery Manager Server on the recovery site.
8. Upgrade the storage replication adapters (SRA) on the recovery site.
9. Upgrade the vSphere Replication appliance on the recovery site.
10. Upgrade any additional vSphere Replication server instances on the recovery site.
11. Configure the connection between the Site Recovery Manager sites and vSphere Replication appliances.
12. Verify that your protection groups and recovery plans are still valid.
13. Upgrade ESXi Server on the recovery site.
14. Upgrade ESXi Server on the protected site.
15. Upgrade the virtual hardware and VMware Tools on the virtual machines on the ESXi hosts.

Upgrade Site Recovery Manager

You perform several tasks to upgrade Site Recovery Manager.

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

Prerequisites

Due to update release schedules, upgrading to certain 5.5.x releases is not supported for all 5.0.x and 5.1.x releases. Check **Solution Upgrade Path > VMware vCenter Site Recovery Manager** in the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php? before you upgrade, to ensure that your upgrade path is supported.

Important Upgrade versions of Site Recovery Manager earlier than 5.0 to a Site Recovery Manager 5.0.x release before you upgrade to Site Recovery Manager 5.5.x. Upgrading vCenter Server directly from 4.1.x to 5.5 is a supported upgrade path. However, upgrading Site Recovery Manager directly from 4.1.x to 5.5.x is not a supported upgrade path. When upgrading a vCenter Server 4.1.x instance that includes a Site Recovery Manager installation, you must upgrade vCenter Server to version 5.0.x before you upgrade Site Recovery Manager to 5.0.x. If you upgrade vCenter Server from 4.1.x to 5.5 directly, when you attempt to upgrade Site Recovery Manager from 4.1.x to 5.0.x, the Site Recovery Manager upgrade fails. Site Recovery Manager 5.0.x cannot connect to a vCenter Server 5.5 instance.

Procedure

1. Prepare for Site Recovery Manager Upgrade

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

2. In-Place Upgrade of Site Recovery Manager Server

   You can upgrade the Site Recovery Manager Server on the same host as an existing Site Recovery Manager Server installation.

3. Upgrade the Site Recovery Manager Server with Migration

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

4. Upgrade the Site Recovery Manager Client Plug-In

   You must upgrade the Site Recovery Manager client plug-in for all vSphere Client instances that you use to manage Site Recovery Manager.

5. Configure the Upgraded Site Recovery Manager Installation

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

Prepare for Site Recovery Manager Upgrade

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

Site Recovery Manager 5.0.x uses a 32-bit open database connectivity (ODBC) database source name (DSN), but Site Recovery Manager 5.5 requires a 64-bit DSN to connect to the Site Recovery Manager database. If you are upgrading from Site Recovery Manager 5.0.x, you must create a 64-bit DSN. See Create an ODBC System DSN for Site Recovery Manager.

Prerequisites

- Due to update release schedules, upgrading to certain 5.5.x releases is not supported for all 5.0.x and 5.1.x releases. Check **Solution Upgrade Path > VMware vCenter Site Recovery Manager** in the VMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php? before you upgrade, to ensure that your upgrade path is supported.

  Important Upgrade versions of Site Recovery Manager earlier than 5.0 to a Site Recovery Manager 5.0.x release before you upgrade to Site Recovery Manager 5.5.x. Upgrading vCenter Server directly from 4.1.x to 5.5 is a supported upgrade path. However, upgrading Site Recovery Manager directly from 4.1.x to 5.5.x is not a supported upgrade path. When upgrading a vCenter Server 4.1.x instance that includes a Site Recovery Manager installation, you must upgrade vCenter Server to version 5.0.x before you upgrade Site Recovery Manager to 5.0.x. If you upgrade vCenter Server from 4.1.x to 5.5 directly, when you attempt to upgrade Site Recovery Manager from 4.1.x to 5.0.x, the Site Recovery Manager upgrade fails. Site Recovery Manager 5.0.x cannot connect to a vCenter Server 5.5 instance.

- **Important** Verify that there are no pending cleanup operations on recovery plans and that there are no configuration issues for the virtual machines that Site Recovery Manager protects.
  - All recovery plans are in the Ready state.
  - The protection status of all of the protection groups is OK.
  - The protection status of all of the individual virtual machines in the protection groups is OK.
  - The recovery status of all of the protection groups is Ready.
- If you configured advanced settings in the existing installation, take a note of the settings that you configured before upgrading.
- The local and remote vCenter Server instances must be running when you upgrade Site Recovery Manager.
- Upgrade all of the vCenter Server components and Site Recovery Manager on one site before you upgrade vCenter Server and Site Recovery Manager on the other site.
- Download the Site Recovery Manager installation file to a folder on the machines on which to upgrade Site Recovery Manager.

- Verify that no reboot is pending on the Windows machine on which to install Site Recovery Manager Server. Verify that no other installation is running, including the silent installation of Windows updates. Pending reboots or running installations can cause the installation of Site Recovery Manager Server to fail.

Procedure

1. Log in to the machine on the protected site on which you have installed Site Recovery Manager.
2. Back up the Site Recovery Manager database by using the tools that the database software provides.
3. (Optional) If you are upgrading from Site Recovery Manager 5.0.x, create a 64-bit DSN.
4. Upgrade the vCenter Server instance to which Site Recovery Manager connects to vCenter Server 5.5.

   If you are upgrading from vCenter Server and Site Recovery Manager 4.1.x, you must upgrade the vCenter Server and Site Recovery Manager Server instances in the correct sequence before you can upgrade to Site Recovery Manager 5.5.

   a. Upgrade vCenter Server from 4.1.x to 5.0.x.

   b. Upgrade Site Recovery Manager from 4.1.x to 5.0.x.

   c. Upgrade vCenter Server from 5.0.x to 5.5.

In-Place Upgrade of Site Recovery Manager Server

You can upgrade the Site Recovery Manager Server on the same host as an existing Site Recovery Manager Server installation.

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

Note If you are updating Site Recovery Manager 5.5 to a 5.5.x update release or to a 5.5.x.x patch release, you must perform in-place upgrade. You cannot perform upgrade with migration if you are updating Site Recovery Manager 5.5 to a 5.5.x update release or to a 5.5.x.x patch release.

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

An in-place upgrade provides a quick way to upgrade the Site Recovery Manager Server to a new release without changing any of the information that you provided for the current installation. To change any installation information, for example, database connections, the authentication method, certificate location, or administrator credentials, you must run the installer in modify mode after you upgrade an existing Site Recovery Manager Server.

If you connect Site Recovery Manager to a vCenter Server instance that is already running vSphere Replication as a registered extension, you must still select the **Install vSphere Replication** option. Selecting this option installs components that Site Recovery Manager requires to work with vSphere Replication. You can also install vSphere Replication after you install Site Recovery Manager by running the installer again in Repair mode.

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

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

Prerequisites

- You completed the tasks in Prepare for Site Recovery Manager Upgrade.
- Log into the Site Recovery Manager host to upgrade. Log in using an account with sufficient privileges. This is often an Active Directory domain administrator, but can also be a local administrator.
- Download the Site Recovery Manager installation file to a folder on the Site Recovery Manager Server host.

Procedure

1. Double-click the Site Recovery Manager installer icon, select an installation language, and click **OK**.
2. If you are upgrading from Site Recovery Manager 5.0.x, click **OK** to confirm that you created a 64-bit ODBC DSN to connect Site Recovery Manager to the existing database.

   This prompt does not appear when you upgrade from Site Recovery Manager 5.1.
3. Follow the prompts and accept the license agreement.
4. Click **Change** to change the folder in which to install Site Recovery Manager, select a target volume, and click **Next**.

   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 170 characters including the end slash, and cannot include non-ASCII characters.
5. Select whether to install vSphere Replication and click **Next**.
6. Provide the username and password for vCenter Server and click **Next**.

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

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

   If you are using certificate-based authentication, there is no prompt to accept the certificate.

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

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

Option	Description
Use credential-based authentication	a Select **Automatically generate certificate** and click **Next**. b Type text values for your organization and organization unit, typically your company name and the name of your group in the company.
Use certificate-based authentication	a Select **Use a PKCS #12 certificate file** and click **Next**. b Type the path to the certificate file. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. c Type the certificate password. d The local host value must be the same as the Subject Alternative Name (SAN) value of the Site Recovery Manager Server certificate. This is usually the fully qualified domain name of the Site Recovery Manager Server host.

10 Verify the Administrator E-mail and Local Host values and click **Next**.

11 Select the 64-bit ODBC DSN from the **Data Source Name** drop-down menu, provide the username and password for the database, and click **Next**.

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

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

13 Click **Install**.

Upgrade the Site Recovery Manager Server with Migration

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

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

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

If you connect Site Recovery Manager to a vCenter Server instance that is already running vSphere Replication as a registered extension, you must still select the **Install vSphere Replication** option. Selecting this option installs components that Site Recovery Manager requires to work with vSphere Replication. You can also install vSphere Replication after you install Site Recovery Manager by running the installer again in Repair mode.

Note You cannot perform upgrade with migration if you are updating Site Recovery Manager 5.5 to a 5.5.x update release or to a 5.5.x.x patch release. To upgrade Site Recovery Manager 5.5 to a 5.5.x update release or to a 5.5.x.x patch release, see In-Place Upgrade of Site Recovery Manager Server.

Prerequisites

- You completed the tasks in Prepare for Site Recovery Manager Upgrade.
- Log into the Site Recovery Manager host to upgrade. Log in using an account with sufficient privileges. This is often an Active Directory domain administrator, but can also be a local administrator.
- Log in to the host on which to install the new version of Site Recovery Manager Server.
- Download the Site Recovery Manager installation file to a folder on the new Site Recovery Manager Server host.

Procedure

1. Stop the Site Recovery Manager Server service on the old Site Recovery Manager Server host.

   Important Do not uninstall the previousSite Recovery Manager Server installation.

2. On the host on which to install the new version of Site Recovery Manager Server, double-click the Site Recovery Manager installer icon, select an installation language, and click **OK**.
3. Follow the prompts and accept the license agreement.
4. Click **Change** to change the folder in which to install Site Recovery Manager, select a target volume, and click **Next**.

   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 170 characters including the end slash, and cannot include non-ASCII characters.
5. Select whether to install vSphere Replication and click **Next**.

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

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

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

If you are using certificate-based authentication, there is no prompt to accept the certificate.

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

Option	Description
Use credential-based authentication	a Select **Automatically generate certificate** and click **Next**. b Type text values for your organization and organization unit, typically your company name and the name of your group in the company.
Use certificate-based authentication	a Select **Use a PKCS #12 certificate file** and click **Next**. b Type the path to the certificate file. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. c Type the certificate password. d The local host value must be the same as the Subject Alternative Name (SAN) value of the Site Recovery Manager Server certificate. This is usually the fully qualified domain name of the Site Recovery Manager Server host.

9 Type the administrator and host configuration information and click **Next**.

Option	Description
Local Site Name	A name for this installation of Site Recovery Manager. A suggested name is generated, but you can type any name. It cannot be the same name that you use for another Site Recovery Manager installation with which this one will be paired.
Administrator E-mail	Email address of the Site Recovery Manager administrator, for potential use by vCenter Server. This field is required even though email notifications are not implemented in this version.
Additional E-mail	An optional email address of another Site Recovery Manager administrator, for potential use by vCenter Server.
Local Host	Name or IP address of the local host. This value is obtained by the Site Recovery Manager installer and needs to be changed only if it is incorrect. For example, the local host might have more than one network interface and the one detected by the Site Recovery Manager installer is not the interface you want to use. If you use certificate-based authentication, the **Local Host** value must be the same as the SAN value of the supplied certificate. This is usually the fully qualified domain name of the Site Recovery Manager Server host.
Listener Ports	SOAP and HTTP port numbers to use.
API Listener Port	SOAP port number for API clients to use.

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

10 Provide the connection information for the Site Recovery Manager database that you used with the previous installation, and click **Next**.

Option	Action
Database Client	Select a database client type from the drop-down menu.
Data Source Name	Select an existing 64-bit DSN that connects to the Site Recovery Manager database that you used with the previous installation.
Username	Type a valid user ID for the specified database.
Password	Type the password for the specified user ID.
Connection Count	Type the initial connection pool size. In most cases, it is not necessary to change this setting. Before changing this setting, consult with your database administrator.
Max Connections	Type the maximum number of database connections that can be open simultaneously. In most cases, it is not necessary to change this setting. Before changing this setting consult with your database administrator.

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

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

12 Click **Install**.

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

Upgrade the Site Recovery Manager Client Plug-In

You must upgrade the Site Recovery Manager client plug-in for all vSphere Client instances that you use to manage Site Recovery Manager.

Prerequisites

- Verify that you upgraded vCenter Server, the Site Recovery Manager Server, and the vSphere Client.
- Log in to the machine on which the vSphere Client is installed.
- Uninstall the old Site Recovery Manager client plug-in, if it is installed.

Procedure

1. Start the vSphere Client and connect to vCenter Server at either the protected or recovery site.
2. Select **Plugins > Manage Plug-ins**.
3. Under **Available Plug-ins**, locate **VMware vCenter Site Recovery Manager Extension** and click **Download and Install**.
4. Review and accept the certificate.

   This step only occurs if you use certificate-based authentication.
5. After the download finishes, click **Run** to start the installation wizard, select the installation language, and click **OK**.

   If you did not uninstall the previous version of the Site Recovery Manager client plug-in, the installer prompts you to do so and stops the installation.
6. Click **Next** to start the installation, then click **Next** again at the VMware Patents page.
7. Select **I accept the terms in the license agreement**, and click **Next**.
8. Click **Install**.
9. When the installation finishes, click **Finish**.

   If the installation replaced any open files, you are prompted to shut down and restart Windows.

What to do next

Repeat this process for other vSphere Client instances that you use to connect to this Site Recovery Manager site.

Configure the Upgraded Site Recovery Manager Installation

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

Site Recovery Manager 5.5 is a 64-bit application. If you are upgrading from Site Recovery Manager 5.0.x and you use array-based replication, even if you performed an in-place upgrade of Site Recovery Manager, you must install 64-bit storage array adapters (SRA) that are compatible with Site Recovery Manager 5.5.

Prerequisites

- You upgraded vCenter Server and Site Recovery Manager.
- If you use array-based replication, check the availability of an SRA for your type of storage by consulting the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.
- Download the SRA by going to https://my.vmware.com/web/vmware/downloads, selecting **VMware vCenter Site Recovery Manager > Download Product**, then selecting **Drivers & Tools > Storage Replication Adapters > Go to Downloads**.
- If you obtain an SRA from a different vendor site, verify that it has been certified for the Site Recovery Manager release you are using by checking the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.

Procedure

1. In the Site Recovery Manager client, select **Sites > Summary** and click **Configure Connection** to pair the Site Recovery Manager Server instances.
2. (Optional) If you use array-based replication, reinstall and reconfigure the SRA on the Site Recovery Manager Server hosts that you upgraded.

   You must perform these tasks on both sites.

   a. Reinstall all SRAs.

   b. Click **Rescan SRAs** in the **Array Managers > SRAs** tab.

   c. Reconfigure all array managers with the correct credentials.

Revert to a Previous Release of Site Recovery Manager

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

Prerequisites

- Verify that your installation of vCenter Server supports the Site Recovery Manager release that you are reverting to. For information about the vCenter Server releases that support different versions of Site Recovery Manager, see the *Site Recovery Manager Compatibility Matrixes*, at http://www.vmware.com/support/pubs/srm_pubs.html. For information about reverting a vCenter Server installation, see the vSphere documentation.
- Verify that you made a backup of the Site Recovery Manager database before you upgraded Site Recovery Manager from a previous release to this release.

Procedure

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

   If you connected the Site Recovery Manager Server instances at the protected and recovery sites, you must uninstall Site Recovery Manager at both sites. If you uninstall Site Recovery Manager from one side of a site pairing but not the other, the database on the remaining site becomes inconsistent.
2. Use the Windows Control Panel options to uninstall the Site Recovery Manager plug-in from any vSphere Client instances on which you installed it.
3. Restore the Site Recovery Manager database from the backup that you made when you upgraded Site Recovery Manager from the previous release.

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

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

Configuring Array-Based Protection

7

After you pair the protected and recovery sites, you must configure protection for virtual machines. If you are using array-based replication, you must configure storage replication adapters (SRAs) at each site.

If you are using only vSphere Replication, you do not require an SRA. See Chapter 8 Installing vSphere Replication.

Procedure

1 Install Storage Replication Adapters

   If you are using array-based replication, you must install a Storage Replication Adapter (SRA) specific to each storage array that you use with Site Recovery Manager. An SRA is a program that an array vendor provides that enables Site Recovery Manager to work with a specific kind of array.

2 Configure Array Managers

   After you pair the protected site and recovery site, configure their respective array managers so that Site Recovery Manager can discover replicated devices, compute datastore groups, and initiate storage operations.

3 Rescan Arrays to Detect Configuration Changes

   Site Recovery Manager checks arrays for changes to device configurations every 24 hours. However, you can force an array rescan at any time.

4 Edit Array Managers

   Use the Edit Array Manager wizard to modify an array manager's name or other settings, such as the IP address or user name and password.

Install Storage Replication Adapters

If you are using array-based replication, you must install a Storage Replication Adapter (SRA) specific to each storage array that you use with Site Recovery Manager. An SRA is a program that an array vendor provides that enables Site Recovery Manager to work with a specific kind of array.

You must install an appropriate SRA on the Site Recovery Manager Server hosts at the protected and recovery sites. If you use more than one type of storage array, you must install the SRA for each type of array on both of the Site Recovery Manager Server hosts.

Note You can configure Site Recovery Manager to use more than one type of storage array, but you cannot store the virtual machine disks for a single virtual machine on multiple arrays from different vendors. You must store all of the disks for a virtual machine on the same array.

Storage replication adapters come with their own installation instructions. You must install the version of an SRA that corresponds to a specific Site Recovery Manager version. Install the same version of the SRA at both sites. Do not mix SRA versions.

If you are using vSphere Replication, you do not require an SRA.

Prerequisites

- Check the availability of an SRA for your type of storage by consulting the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.
- Download the SRA by going to https://my.vmware.com/web/vmware/downloads, selecting **VMware vCenter Site Recovery Manager > Download Product**, then selecting **Drivers & Tools > Storage Replication Adapters > Go to Downloads**.
- Read the documentation provided with your SRA. SRAs do not support all features that storage arrays support. The documentation that your SRA provides details what the SRA supports and requires. For example, HP and EMC have detailed physical requirements which must be met for the SRA to perform as expected.
- Install Site Recovery Manager Server before you install the SRAs.
- Your SRA might require the installation of other vendor-provided components. You might need to install some of these components on the Site Recovery Manager Server host. Other components might require only network access by the Site Recovery Manager Server. For the latest information on such requirements, review the release notes and readme files for the SRAs you are installing.
- Enable the storage array's capability to create snapshot copies of the replicated devices. See your SRA documentation.

Procedure

1 Install the SRA on each Site Recovery Manager Server host.

The installer installs the SRA in `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra`.

2 Using the vSphere Client, connect to Site Recovery Manager, select **Array Managers** in the left pane, click the **SRAs** tab, and click **Rescan SRAs**.

This action refreshes SRA information, allowing Site Recovery Manager to discover the SRA.

Configure Array Managers

After you pair the protected site and recovery site, configure their respective array managers so that Site Recovery Manager can discover replicated devices, compute datastore groups, and initiate storage operations.

You typically configure array managers only once, after you connect the sites. You do not need to reconfigure them unless array manager connection information or credentials change, or you want to use a different set of arrays.

Prerequisites

- Connect the sites as described in Connect the Protected and Recovery Sites.
- Install SRAs at both sites as described in Install Storage Replication Adapters.

Procedure

1 Select **Array Managers** in the Site Recovery Manager interface, and select the site on which you want to configure array managers.

2 Click the **Summary** tab and click **Add Array Manager**.

3 Type a name for the array in the **Display Name** text box.

Use a descriptive name that makes it easy for you to identify the storage associated with this array manager.

4 Select the array manager type that you want Site Recovery Manager to use from the **SRA Type** drop-down menu.

If no manager type appears, rescan for SRAs or check that you have installed an SRA on the Site Recovery Manager Server host.

5 Provide the required information for the type of SRA you selected.

The SRA creates these text boxes. For more information about how to fill in these text boxes, see the documentation that your SRA vendor provides. Text boxes vary between SRAs, but common text boxes include IP address, protocol information, mapping between array names and IP addresses, and user name and password.

6 Click **Finish**.

7 Repeat steps Step 1 through Step 6 to configure an array manager for the recovery site.

8 Select an array in the **Array Managers** panel and click the **Array Pairs** tab.

9 (Optional) Click **Refresh** to scan for new array pairs.

10 Select an array pair in the Discovered Array Pairs panel, and click **Enable**.

If you have added array managers, but no array pairs are visible, click **Refresh** to collect the latest information about array pairs.

Rescan Arrays to Detect Configuration Changes

Site Recovery Manager checks arrays for changes to device configurations every 24 hours. However, you can force an array rescan at any time.

You can reconfgure the frequency with which Site Recovery Manager preforms regular array scans by changing the `storage.minDsGroupComputationInterval` option in Advanced Settings. See Change Storage Settings in *Site Recovery Manager Administration*.

Configuring array managers causes Site Recovery Manager to compute datastore groups based on the set of replicated storage devices that it discovers. If you change the configuration of the array at either site to add or remove devices, Site Recovery Manager must rescan the arrays and recompute the datastore groups.

Procedure

1 Click **Array Managers** and select an array.

2 Click the **Devices** tab.

The **Devices** tab provides information about all the storage devices in the array, including the local device name, the device it is paired with, the direction of replication, the protection group to which the device belongs, whether the datastore is local or remote, and the consistency group ID for each SRA device.

3 Click **Refresh** to rescan the arrays and recompute the datastore groups.

Edit Array Managers

Use the Edit Array Manager wizard to modify an array manager's name or other settings, such as the IP address or user name and password.

For more information about how to fill in the adapter fields, see the documentation that your SRA vendor provides. While fields vary among SRAs, common fields include IP address, protocol information, mapping between array names and IP addresses, and user names and passwords.

Procedure

1 Click **Array Managers** in the left pane, and select an array manager.

2 Right-click an array and select **Edit Array Manager**.

3 Modify the name for the array in the **Display Name** field.

   Use a descriptive name that makes it easy for you to identify the storage associated with this array manager. You cannot modify the array manager type.

4 Modify the adapter information.

   These fields are created by the SRA.

5 Click **Finish** to complete the modification of the array manager.

Installing vSphere Replication

8

vSphere Replication uses the replication technologies included in ESXi with the assistance of virtual appliances to replicate virtual machines between source and target sites.

The vSphere Replication appliance registers with the corresponding vCenter Server instance. For example, on the source site, the vSphere Replication appliance registers with the vCenter Server instance on the source site.

The vSphere Replication appliance contains a 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 servers 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.

Before you can use vSphere Replication with Site Recovery Manager, you must configure the Site Recovery Manager infrastructure.

- When installing Site Recovery Manager, make sure that you select the vSphere Replication option. If you did not select the vSphere Replication option when you installed Site Recovery Manager, you can add that option by running the installer again in repair mode.
- Pair the Site Recovery Manager Server instances as described in Connect the Protected and Recovery Sites.

The **Getting Started page** in the vSphere Replication view of the Site Recovery Manager interface provides guidance to ensure that you complete the installation and configuration process correctly.

Procedure

1 Deploy the vSphere Replication Virtual Appliance

vSphere Replication is distributed as an OVF virtual appliance. You must deploy the appliance at both of the primary and secondary sites.

2 Configure vSphere Replication Connections

To use vSphere Replication between two sites managed by different vCenter Server instances, you need to configure a connection between the two vSphere Replication appliances.

3 Reconfigure the vSphere Replication Appliance

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

4 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.

5 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.

6 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.

7 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.

8 Uninstall vSphere Replication

You uninstall vSphere Replication by unregistering the appliance from vCenter Server and removing it from your environment.

9 Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted

If the vSphere Replication appliance virtual machine does not exist because it was deleted, you cannot use the virtual appliance management interface (VAMI) to unregister vSphere Replication from vCenter Server. Instead, you can use the Managed Object Browser (MOB) to delete the vSphere Replication extension.

Deploy the vSphere Replication Virtual Appliance

vSphere Replication is distributed as an OVF virtual appliance. You must deploy the appliance at both of the primary and secondary sites.

Site Recovery Manager deploys the OVF file from the vCenter Server instance that Site Recovery Manager extends. The vSphere Replication OVF file is also available at `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\www\vSphere_Replication_SRM_OVF10.ovf` on the Site Recovery Manager Server machine. If deploying the vSphere Replication OVF from the default location fails or is slow, you can also deploy it from Site Recovery Manager Server.

Prerequisites

- You opted to install vSphere Replication when you installed Site Recovery Manager.

- In the vSphere Client, go to **Administration > vCenter Server Settings > Advanced Settings** on the vCenter Server instance on which you are deploying vSphere Replication. Verify that the `VirtualCenter.FQDN` value is set to a fully-qualified domain name or a literal address.

Procedure

1. Select **vSphere Replication** in the Site Recovery Manager interface.
2. Click **Deploy VR Appliance** in the **Summary** tab.
3. Click **OK** to start the **Deploy OVF Template** wizard.
4. Click **Next** to deploy the OVF file from the default location.
5. Review the virtual appliance details and click **Next**.
6. Accept the default name and destination folder or provide a new name and folder for the virtual appliance, and click **Next**.
7. Follow the prompts to select a destination host, datastore, and disk format for the virtual appliance.
8. Set the appliance properties, and click **Next**.

Option	Description
Password	Type and confirm a root password for the appliance.
Initial Configuration	Use the embedded vSphere Replication database. If you use the embedded database, you can use vSphere Replication immediately after deployment. Deselect the checkbox to use vSphere Replication with an external database. If you use an external database, you must set up the database before you can use vSphere Replication.
Networking Properties	If you do not set network settings, the appliance uses DHCP. Set a static IP address for the appliance. You can also reconfigure network settings after deployment by using the virtual appliance management interface (VAMI).

9. Review the binding to the vCenter Extension vService and click **Next**.
10. (Optional) Select the **Power on virtual machine** check box and click **Finish**.

    If you deploy the vSphere Replication OVF file from the default location, the check box is selected automatically.
11. Repeat the procedure to install vSphere Replication on the secondary site.

When the OVF deployment finishes and the appliance has booted, vSphere Replication registers as an extension with vCenter Server. The vSphere Replication appliance appears under the site name in the vSphere Replication tab of the Site Recovery Manager interface. vSphere Replication is ready for use immediately after you deploy the appliance. No manual configuration or registration is required.

What to do next

Connect the vSphere Replication sites. You can also perform optional reconfiguration of the vSphere Replication appliance.

Configure vSphere Replication Connections

To use vSphere Replication between two sites managed by different vCenter Server instances, you need to configure a connection between the two vSphere Replication appliances.

You can complete this process on either site on which you have installed a vSphere Replication appliance. If you are using an untrusted certificate, certificate warnings might appear during the process.

Prerequisites

Verify that you have deployed Site Recovery Manager at two sites and configured the connection between the Site Recovery Manager sites. Verifiy that you have deployed the vSphere Replication appliances at the two sites.

Procedure

1. Click **vSphere Replication** in the left pane of the Site Recovery Manager interface, and select a site.

   A site is indicated by a folder icon.
2. Click the **Summary** tab.
3. Click **Configure VR Connection**.
4. Click **Yes** to confirm that you want to connect the sites.
5. Click **OK**.

Reconfigure the vSphere Replication Appliance

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

  You can use vSphere Replication immediately after you deploy the vSphere Replication appliance. If necessary, you can reconfigure the general settings 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 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 vSphere Replication appliance. You can also set the system time zone, and reboot or shut down the appliance.

- 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

You can use vSphere Replication immediately after you deploy the vSphere Replication appliance. If necessary, you can reconfigure the general settings 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.
- You must have administrator privileges to configure the vSphere Replication appliance.
- You updated vCenter Server, the vSphere Client, Site Recovery Manager, and the Site Recovery Manager client to the corresponding 5.5.x update release.

Procedure

1. Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

   You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.
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. Select the **VR** tab and 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 username 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.

Prerequisites

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

- You updated vCenter Server, the vSphere Client, Site Recovery Manager, and the Site Recovery Manager client to the corresponding 5.5.x update release.

Procedure

1. Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

   You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.
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.

   See vSphere Replication Certificate Verification for details of how vSphere Replication handles certificates.
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 the SSL certificate, the vSphere Replication status changes to disconnected. Validate the certificate to reconnect the source and target sites before replicating a virtual machine.

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.
- You must have administrator privileges to configure the vSphere Replication appliance.
- You updated vCenter Server, the vSphere Client, Site Recovery Manager, and the Site Recovery Manager client to the corresponding 5.5.x update release.

Procedure

1. Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

   You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.
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/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/hms-configtool -cmd reconfig -property
'hms-keystore-password=new_password'
```

6 Reboot the appliance for the changes to take effect.

```
# reboot
```

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

8 Obtain the current hms-truststore password.

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

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

9 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
```

10 Update the configuration with the new password.

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

11 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 vSphere Replication. You might make these changes to match network reconfigurations.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- You must have administrator privileges to configure the vSphere Replication appliance.
- You updated vCenter Server, the vSphere Client, Site Recovery Manager, and the Site Recovery Manager client to the corresponding 5.5.x update release.

Procedure

1 Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.

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, netmask, and host name information.
IPv4	None	Deactivates IPv4 addresses.
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.

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

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

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

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

d (Optional) Type 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 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.
- You must have administrator privileges to configure the vSphere Replication appliance.
- You updated vCenter Server, the vSphere Client, Site Recovery Manager, and the Site Recovery Manager client to the corresponding 5.5.x update release.

Procedure

1 Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.

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
Appliance Version	vSphere Replication version
Hostname	Hostname of the appliance
OS Name	Operating system name and version
OVF Environment: View	Displays information about the OVF environment
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

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.
- You must 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. Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

   You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.
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. Select the **VR** tab and click **Configuration**.
4. Select **Manual configuration** to specify a configuration or select **Configure from an existing VRM database** to use a previously established configuration.
5. 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.
DB URL	Auto-generated and hidden by default. Advanced users can fine-tune other database properties by modifying the URL, for example if you use a named instance of SQL Server.

6 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.

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, specify 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.
- You must have administrator privileges to configure the vSphere Replication appliance.
- You must have reconfigured vSphere Replication to use an external database.

Procedure

1. Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

   You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.
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. Select the **VR** tab and click **Configuration**.
4. Select **Configure using the embedded database**.
5. (Optional) Click **Reset Embedded Database** to reset the database.
6. Click **Save and Restart Service** to apply the changes.

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

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.

vSphere Replication server is distributed as an OVF virtual appliance. Site Recovery Manager deploys the OVF file from the vCenter Server instance that Site Recovery Manager extends. The vSphere Replication server OVF file is also available at `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\www\vSphere_Replication_Server_SRM_OVF10.ovf` on the Site Recovery Manager Server machine. If deploying the vSphere Replication server OVF from the default location fails or is slow, you can also deploy it from Site Recovery Manager Server.

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 protected and recovery sites.
- Connect the vSphere Replication appliances.
- Deploy vSphere Replication servers on a network that allows them to communicate with the vSphere Replication appliances on the protected and recovery sites.
- Verify that the vSphere Replication servers can communicate with the ESXi Server instances on the primary site that hosts the replicated virtual machines.
- Connect to Site Recovery Manager as described in Connect to Site Recovery Manager.

Procedure

1. Click **vSphere Replication** in the Site Recovery Manager interface, and click the **Summary** tab.
2. Click **Deploy VR Server**.
3. Click **OK** to start the **Deploy OVF Template** wizard.
4. Click **Next** to deploy the OVF file from the default location.
5. Review the virtual appliance details and click **Next**.
6. Accept the default name and destination folder or provide a new name and folder for the virtual appliance, and click **Next**.
7. Follow the prompts to select a destination host, datastore, and disk format for the virtual appliance.

8 Set the appliance properties, and click **Next**.

Option	Description
Password	Type and confirm a root password for the appliance.
Networking Properties	If you do not set network settings, the appliance uses DHCP. Set a static IP address for the appliance. You can also reconfigure network settings after deployment by using the virtual appliance management interface (VAMI).

9 Review your settings and select **Power on after deployment** to start the appliance immediately after deployment completes.

If you deploy the vSphere Replication server OVF file from the default location, the **Power on after deployment** check box is selected automatically.

10 Click **Finish**.

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.

Prerequisites

Verify that the vSphere Replication appliance is deployed and configured.

Verify that the additional vSphere Replication server is deployed.

Procedure

1 Click **vSphere Replication** in the left pane, select a site, and click **Register VR Server** in the **Summary** tab.

2 Select a virtual machine in the inventory that is a working vSphere Replication server, and click **OK**.

The newly registered vSphere Replication server appears in the list.

3 Click **Yes** to confirm registration of the vSphere Replication server.

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.

Prerequisites

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

Procedure

1. In the Site Recovery Manager interface, select **vSphere Replication**.
2. Select a vSphere Replication server and click the **Configure VR Server** link.

   Alternatively, you can connect to the Web interface of the vSphere Replication server by entering the server's IP address and port 5480 in a browser. A sample address might be https://192.168.1.2:5480.
3. Log in to the vSphere Replication server configuration interface as **`root`**.

   Use the root password you set when you deployed the vSphere Replication server.
4. Click the **VRS** tab.
5. (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**.

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

   `root` is the Super User.

7 (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.

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

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

What to do next

If you change the SSL certificate of the vSphere Replication server and the server is already registered, the vSphere Replication status is disconnected. Click **Register VR Server** in the vSphere Replication view of the Site Recovery Manager interface to validate the certificate and reconnect the vSphere Replication appliance with the additional server.

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 Select the vSphere Replication view in the Site Recovery Manager interface.

2 Select the vSphere Replication server to remove and click the **Virtual Machines** tab.

3 Select the virtual machines that the vSphere Replication server manages.

- Click **Remove Replication** to stop replication of a virtual machine.
- Click **Configure Replication** to use a different virtual vSphere Replication server to handle the replication of a virtual machine.

4 Right-click the vSphere Replication server to remove and select **Remove VR Server**.

Removing the vSphere Replication server unregisters it from the vSphere Replication management server in the vSphere Replication appliance.

5 In the Hosts and Clusters view, power off and delete the vSphere Replication server virtual machine.

Uninstall vSphere Replication

You uninstall vSphere Replication by unregistering the appliance from vCenter Server and removing it from your environment.

Prerequisites

- Verify that the vSphere Replication virtual appliance is powered on.
- Stop all existing outgoing or incoming replications to the site.
- Disconnect any connections to other vSphere Replication sites.

Procedure

1. Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

   You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.
2. Select the **Configuration** tab.
3. Click **Unregister from vCenter Server**.
4. In the vSphere Client, power off and delete the vSphere Replication appliance.

You removed vSphere Replication from your environment.

Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted

If the vSphere Replication appliance virtual machine does not exist because it was deleted, you cannot use the virtual appliance management interface (VAMI) to unregister vSphere Replication from vCenter Server. Instead, you can use the Managed Object Browser (MOB) to delete the vSphere Replication extension.

Prerequisites

Log in to https://<*vCenter_Server_address*>/mob/?moid=ExtensionManager with vCenter Server credentials.

Procedure

1. In the extensionList property, click the corresponding link for the com.vmware.vcHms extension key to check the key details.
2. Verify that the displayed data is for a vSphere Replication appliance that is already lost.
3. In ExtensionManager, click **unregisterExtension**.
4. Type **`com.vmware.vcHms`** for the extension key value, and click **Invoke Method**.

5 Verify that the result displays `void` and not an error message.

   An error message might appear if the specified extension is not registered, or if an unexpected runtime error occurs.

6 Close the window.

7 Refresh the ExtensionManager page and verify that the extensionList entry does not include com.vmware.vcHms.

What to do next

Deploy a new vSphere Replication appliance and perform any optional configuration.

Upgrading vSphere Replication

9

If you installed vSphere Replication as part of a previous Site Recovery Manager installation, you must upgrade vSphere Replication after you upgrade Site Recovery Manager.

If you upgrade Site Recovery Manager, vSphere Replication is not upgraded automatically. You must upgrade vSphere Replication as a separate process from upgrading Site Recovery Manager.

You might have installed an earlier version of vSphere Replication as part of an earlier Site Recovery Manager installation, or you might have installed the standalone version of vSphere Replication.

- vSphere Replication 1.0.x was delivered with Site Recovery Manager 5.0.x.
- vSphere Replication 5.1.x was delivered with Site Recovery Manager 5.1.x and is also available as a standalone product, independently of Site Recovery Manager.

The upgrade preserves the configuration from the previous installation, including the database configuration, certificates, vSphere Replication site pairings, registered vSphere Replication servers, and configured replications.

You upgrade vSphere Replication 1.0.x and 5.1.x to vSphere Replication 5.5.x by using a downloadable ISO image. The downloadable ISO image is the only means of upgrading from vSphere Replication 1.0.x or 5.1.x to vSphere Replication 5.5.x. You cannot upgrade vSphere Replication from version 1.0.x or 5.1.x to to version 5.5.x by using vSphere Update Manager or the virtual appliance management interface (VAMI) of the vSphere Replication appliance. After you have upgraded vSphere Replication to version 5.5.x by using the ISO image, you can use the VAMI or Update Manager to install later 5.5.x update releases.

In Site Recovery Manager 5.0 the vSphere Replication management server and the vSphere Replication server are separate appliances. In Site Recovery Manager 5.1 and later and vSphere Replication 5.1 and later, vSphere Replication is a single appliance named the vSphere Replication appliance, that contains both the vSphere Replication management server and a vSphere Replication server.

When upgrading vSphere Replication 1.0.x to vSphere Replication 5.5, the upgrade process upgrades the vSphere Replication management server to the combined vSphere Replication 5.5 appliance. As a consequence, an upgraded installation of vSphere Replication uses the vSphere Replication server that is embedded in the combined appliance. If your infrastructure uses more than one vSphere Replication server, you must upgrade them to vSphere Replication 5.5 and reregister them with the vSphere Replication appliance.

Note After you upgrade vSphere Replication 1.0.x, the port on which the vSphere Replication appliance publishes the VAMI changes from 8080 to 5480.

Using Standalone vSphere Replication with Site Recovery Manager

vSphere Replication 5.1 and later is available as a standalone extension of vCenter Server, that is independent of Site Recovery Manager. If you installed a standalone version of vSphere Replication and then install Site Recovery Manager, all existing pairings and replications are immediately accessible through the Site Recovery Manager user interface, except for pairings and replications in a single vCenter Server. Pairings and replications in a single vCenter Server are visible only in the vSphere Replication user interface in the vSphere Web Client.

Migration of the vSphere Replication database is not supported. If you upgrade vSphere Replication 5.1 to Site Recovery Manager 5.5, vSphere Replication uses the embedded database. The standalone version of vSphere Replication and Site Recovery Manager can coexist and work together in the same infrastructure. For example, you can replicate 100 virtual machines with vSphere Replication but choose to protect only 50 of them by using Site Recovery Manager. You can manage all of the replications by using either the vSphere Replication interface in the vSphere Web Client or by using the Site Recovery Manager interface. Some limitations apply to the management of the replications, depending on which interface you use.

- You cannot manage replications in a single vCenter Server instance in the Site Recovery Manager interface.
- You cannot use the vSphere Replication interface in the vSphere Web Client to manually recover virtual machines that Site Recovery Manager protects.
- You must use the vSphere Web Client to configure vSphere Replication to retain point-in-time snapshots of virtual machines.

Example: vSphere Replication Upgrade Scenarios

These examples of upgrade and update scenarios are not exhaustive. For the full list of supported upgrade paths, see the *Compatibility Matrixes for vSphere Replication 5.5* at https://www.vmware.com/support/vsphere5/doc/vsphere-replication-compat-matrix-5-5.html.

- You can upgrade from vSphere Replication 1.0.3 to vSphere Replication 5.5.1 by using the ISO file for vSphere Replication 5.5.1.

- You can upgrade from vSphere Replication 5.1.2 to vSphere Replication 5.5.1 by using the ISO file for vSphere Replication 5.5.1.
- You can update vSphere Replication 5.5.0 to 5.5.1 by using the ISO file for vSphere Replication 5.5.1.
- You cannot upgrade from vSphere Replication 1.0.3 to 5.5.1 by using Update Manager or the VAMI.
- You cannot upgrade from vSphere Replication 5.1.2 to 5.5.1 by using Update Manager or the VAMI.
- You can update vSphere Replication 5.5.0 to 5.5.1 by using Update Manager or the VAMI.

This section includes the following topics:

Upgrade vSphere Replication by Using the Downloadable ISO Image

You upgrade the vSphere Replication appliance and the vSphere Replication server by using a downloadable ISO image.

Prerequisites

- Upgrade the vCenter Server instance that vSphere Replication extends.
- Upgrade Site Recovery Manager by running the new version of the Site Recovery Manager installer.
- Download the `VMware-vSphere_Replication-5.5.x.x-build_number.iso` ISO image from the vSphere downloads page. Copy the ISO image file to a datastore that is accessible from the vCenter Server instance that you use with vSphere Replication.
- Power off the vSphere Replication virtual machine.

Procedure

1. Right-click the vSphere Replication virtual machine and select **Edit Settings**.
2. In **Virtual Hardware**, select **CD/DVD Drive > Datastore ISO File**.
3. Navigate to the ISO image in the datastore.
4. For **File Type**, select **ISO Image** and click **OK**.
5. For **New device**, select **CD/DVD Drive** and click **Add**.
6. Check the box to connect at power on and follow the prompts to add the CD/DVD Drive to the vSphere Replication virtual machine.
7. Restart the vSphere Replication virtual machine.

8 In a Web browser, log in to the virtual appliance managment interface (VAMI).

   If you are updating vSphere Replication 5.1, go to https://*vr_appliance_address*:5480.

   If you are upgrading vSphere Replication 1.0.x, go to https://*vr_appliance_address*:8080.

9 Click the **Update** tab.

10 Click **Settings** and select **Use CDROM Updates**, then click **Save**.

11 Click **Status** and click **Check Updates**.

   The appliance version appears in the list of available updates.

12 Click **Install Updates** and click **OK**.

13 After the updates install, click the **System** tab and click **Reboot** to complete the upgrade.

What to do next

If your infrastructure uses more than one vSphere Replication server, you must upgrade all of the vSphere Replication servers to 5.5. Repeat these steps to upgrade each vSphere Replication server.

Update vCenter Server IP Address in vSphere Replication Management Server

After you upgrade vCenter Server and the vSphere Replication appliance, if the vCenter Server certificate or the IP address changed during the upgrade, you must perform additional steps.

To update the vCenter Server certificate, see vSphere Replication is Inaccessible After Changing vCenter Server Certificate.

If vCenter Server uses a static IP address, it preserves the IP address by default after upgrade. If the vCenter Server uses a DHCP address that changed during the upgrade, and the vSphere Replication management server is configured to use the vCenter Server IP address and not FQDN, update the IP address in the vSphere Replication management server.

Procedure

1 Upgrade vCenter Server to the new appliance.

2 Upgrade vSphere Replication.

3 Power off the vSphere Replication appliance and power it on to retrieve the OVF environment.

4 On the vSphere Replication VAMI **Configuration** tab, type the new IP address of the vCenter Server.

5 Click **Save and Restart**.

Update vSphere Replication By Using vSphere Update Manager

You can update vSphere Replication from version 5.5.x to a later 5.5.x update release by using vSphere Update Manager.

Update Manager 5.5.x contains the update information for vSphere Replication 5.5.x update releases. Using Update Manager is the easiest way to update vSphere Replication, especially for large environments that contain multiple vSphere Replication servers. You can update multiple vSphere Replication servers at the same time.

Prerequisites

- You installed vSphere Replication 5.5.x or upgraded vSphere Replication to version 5.5.x by using the downloadable ISO file. If you are running an older version of vSphere Replication, you must upgrade to version 5.5.x before you can use Update Manager to install a later 5.5.x update release.
- You updated vCenter Server, the vSphere Client, Site Recovery Manager, and the Site Recovery Manager client to the corresponding 5.5.x update release.
- Verify that you installed Update Manager 5.5.x and installed the Update Manager client plug-in on the vCenter Server instance that you use with vSphere Replication.

Procedure

1. In the Update Manager interface, click the **Configuration** tab, click **Download Settings**, and select the **VMware VAs** download source.

   You can deselect all other download sources.
2. Click **Apply** and click **Download Now** to download the latest updates.
3. Click the **Baselines and Groups** tab, select **VMs/VAs**, and click **Create** to create an update baseline for virtual appliances.
4. Type a name and a description for this update baseline, and select **VA Upgrade** as the baseline type.
5. Click **Add Multiple Rules** and set the update rules to create the update baseline.

Option	Description
Vendor	Select **VMware Inc.**
Appliances	Select **vSphere Replication Appliance** and **vSphere Replication Server**
Upgrade To	Select **Latest**

6. Click **OK**, click **Next**, and click **Finish**.

   The update baseline is created.
7. In the VMs and Templates view, select the vSphere Replication appliance and click the **Update Manager** tab.

8 Click **Attach**, select the baseline that you created, and click **Attach** to attach the baseline to the vSphere Replication appliance.

9 Click **Scan** to discover the update version available.

10 Click **Remediate** and follow the prompts to start the update of the vSphere Replication appliance.

You can monitor the progress of the update in the Recent Tasks panel and verify that the appliance is updated after the task finishes.

11 Select a vSphere Replication server in the Inventory and click the **Update Manager** tab.

12 Click **Attach**, select the baseline that you created, and click **Attach** to attach the baseline to the vSphere Replication server.

13 Click **Remediate** and follow the prompts to start the update of the vSphere Replication server.

14 Repeat Step 11 to Step 13 for all vSphere Replication servers.

What to do next

If you configured vSphere Replication to accept only certificates that are signed by a trusted certificate authority, after an update you must reconnect the vSphere Replication appliances.

Update vSphere Replication by Using the VAMI

You can update vSphere Replication from version 5.5.x to a later 5.5.x update release by using the virtual appliance management interface (VAMI) of the vSphere Replication management server.

Important Do not select the option in **Update > Settings** in the VAMI to automatically update vSphere Replication. If you select automatic updates, the VAMI updates vSphere Replication to the latest version, which might be incompatible with vCenter Server 5.5.x. Leave the update setting set to **No automatic updates**.

Prerequisites

- You installed vSphere Replication 5.5.x or upgraded vSphere Replication to version 5.5.x by using the downloadable ISO file. If you are running an older version of vSphere Replication, you must upgrade to version 5.5.x before you can update to a 5.5.x update release.
- You updated vCenter Server, the vSphere Client, Site Recovery Manager, and the Site Recovery Manager client to the corresponding 5.5.x update release.

Procedure

1 Connect to the VAMI of the vSphere Replication appliance in a Web browser.

The URL for the VAMI of the vSphere Replication appliance is https://*vrms-address*:5480.

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

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

3 Click the **Update** tab.

4 Click **Check Updates**.

By default, the VAMI shows the most recently available version. If you want to update to an older update release when the next update release is already available, you must manually change the update URL:

a Click **Settings**.

b Select **Use Specified Repository** and paste the update URL into the **Repository URL** text box.

See the release notes of the update release for the exact URL.

c Click **Save Settings**.

d Click **Status**.

e Click **Check Updates**.

The update checker shows that a new version is available.

5 Click **Install Updates** and click **OK**.

6 When the update finishes, select the **System** tab, and click **Reboot**.

7 Repeat the process on the target site.

What to do next

If you configured vSphere Replication to accept only certificates that are signed by a trusted certificate authority, after an update you must reconnect the vSphere Replication appliances.

If your infrastructure uses more than one vSphere Replication server, update the vSphere Replication server appliances.

Update vSphere Replication Servers by Using the VAMI

If your infrastructure uses more than one vSphere Replication server, you must update all of the vSphere Replication servers to the same update release version as the vSphere Replication appliance.

Prerequisites

- You installed vSphere Replication 5.5.x or upgraded vSphere Replication and the additional vSphere Replication servers to version 5.5.x by using the downloadable ISO file. If you are running an older version of vSphere Replication, you must upgrade the vSphere Replication appliance and the additional vSphere Replication servers to version 5.5.x before you can update to a later 5.5.x update release.
- You updated vCenter Server, the vSphere Client, Site Recovery Manager, and the Site Recovery Manager client to the corresponding 5.5.x update release.

Procedure

1. In a Web browser, connect to the VAMI of the vSphere Replication server to update.

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

2. Type the root user name and password for the vSphere Replication server appliance.
3. Click the **Update** tab.
4. Click **Check Updates**.

   By default, the VAMI shows the most recently available version. If you want to update to an older update release when the next update release is already available, you must manually change the update URL:

   a. Click **Settings**.

   b. Select **Use Specified Repository** and paste the update URL into the **Repository URL** text box.

      See the release notes of the update release for the exact URL.

   c. Click **Save Settings**.

   d. Click **Status**.

   e. Click **Check Updates**.

      The update checker shows that a new version is available.

5. Click **Install Updates** and click **OK**.
6. When the update finishes, select the **System** tab, and click **Reboot**.
7. Repeat the procedure to update any other vSphere Replication server instances.

Creating Site Recovery Manager Placeholders and Mappings

10

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

- About Placeholder Virtual Machines

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

- About Inventory Mappings

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

- About Placeholder Datastores

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

- Configure Datastore Mappings for vSphere Replication

  You configure datastore mappings to determine which datastores vSphere Replication uses to store replicated virtual machine disks and configuration files at the recovery site.

About Placeholder Virtual Machines

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

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

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

About Placeholder Virtual Machine Templates

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

About Inventory Mappings

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

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

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

- Networks
- Folders
- Compute resources
- Placeholder datastores

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

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

Configuring Inventory Mappings for Individual Virtual Machines

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

Changing Inventory Mappings

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

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

How Site Recovery Manager Applies Mappings During Reprotect

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

Select Inventory Mappings

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

Unless you intend to configure mappings individually for each member of a protection group, you should configure inventory mappings for a site before you create protection groups.

Procedure

1. Click **Sites** in the left pane of the Site Recovery Manager interface and select the site for which to configure inventory mappings.
2. Select a tab for a type of inventory object to configure.
3. Select an inventory object and click **Configure Mapping**.

4 Expand the inventory items and navigate to the resources on the recovery site to which to map the protected site resource.

Option	Action
Resource Mappings	Select a resource pool, a host, or a cluster on the recovery site. You can also click **New Resource Pool** to create a resource pool on the host on the recovery site in which to place the recovered virtual machines. You cannot create a new resource pool on a cluster. You can map any type of resource on one site to any type of resource on the other site. **Note** You cannot map individual hosts that are part of clusters to other resource objects.
Folder Mappings	Select a datacenter or virtual machine folder on the recovery site. You can also click **New Folder** to create a virtual machine folder on the host on the recovery site in which to place the recovered virtual machines. You cannot create a new folder on a cluster.
Network Mappings	Select a network on the recovery site to use to connect the recovered virtual machines.

The selected resource appears in the Recovery Site Resource column. The path to the resource relative to the root of the vCenter Server on the recovery site appears in the Recovery Site Path column.

5 Repeat Step 2 through Step 4 for all resource types for which to establish mappings.

About Placeholder Datastores

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

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

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

Placeholder datastores must meet certain criteria.

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

Configure a Placeholder Datastore

You can specify a placeholder datastore for Site Recovery Manager to use for the storage of placeholder virtual machines.

Prerequisites

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

Procedure

1. Select **Sites** in the left pane of the Site Recovery Manager interface, and select a site.
2. Click the **Placeholder Datastores** tab.
3. Click **Configure Placeholder Datastore**.
4. Expand the folders to find a datastore to designate as the location for placeholder virtual machines, click the datastore, and click **OK**.

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

   Important If you use vSphere Replication, do not select a placeholder datastore that you already use as the target datastore for replications. Selecting the same datastore for placeholder virtual machines as you use to contain the replica virtual machines that vSphere Replication creates can cause problems.

   The selected placeholder datastore appears in the Datastore column. If the datastore is on a standalone host, the host name appears. If the datastore is on a host that is in a cluster, the cluster name appears.

Configure Datastore Mappings for vSphere Replication

You configure datastore mappings to determine which datastores vSphere Replication uses to store replicated virtual machine disks and configuration files at the recovery site.

You can use datastore mappings when you configure vSphere Replication for virtual machines as a way to select the default destination datastores.

You configure datastore mappings from the source datastores of the virtual machines being configured for replication to destination datastores for the replicated files. A source datastore can be a single datastore that contains a single virtual machine, or it can be many datastores with many virtual machines with files spread across the datastores.

When you configure replication for a single virtual machine, you can override the datastore mappings for a site, but when you configure replication for multiple virtual machines, you can use only the site-wide datastore mappings, and you cannot override them.

Procedure

1. Click **vSphere Replication** in the left pane, and select a site.
2. Click the **Datastore Mappings** tab, and select a source datastore.
3. Click **Configure Mapping**.
4. Browse through the hierarchy of datastores at the recovery site and select a datastore to which to map.

Installing Site Recovery Manager to Use with a Shared Recovery Site

11

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

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

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

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

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

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

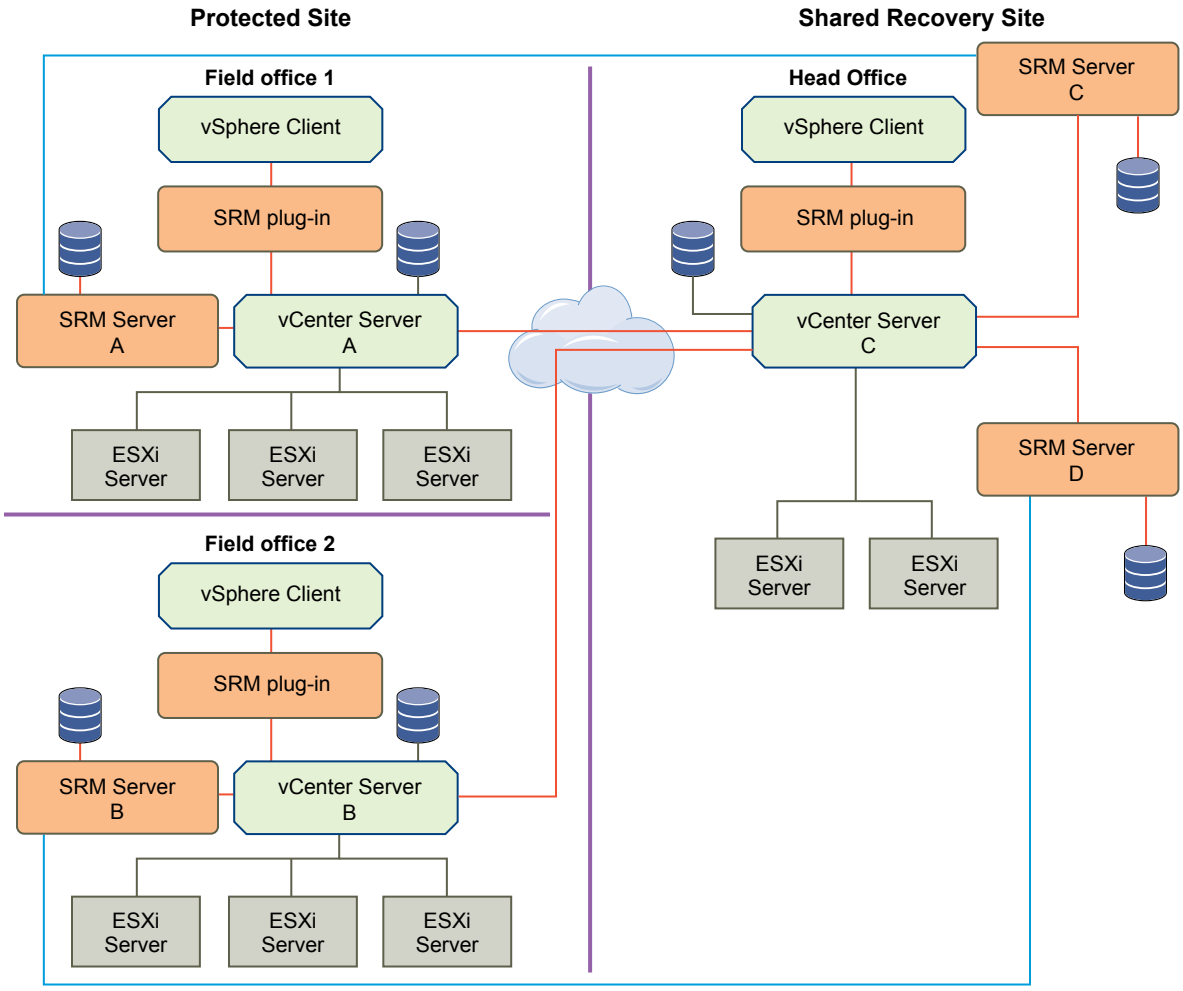
In addition to the shared recovery site configuration, Site Recovery Manager also allows and supports shared protected site (1:N) and many-to-many (N:N) configurations.

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

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

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

Figure 11-1. Example of Using Site Recovery Manager in a Shared Recovery Site Configuration



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

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

- Site Recovery Manager Licenses in a Shared Recovery Site Configuration

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

- Install Site Recovery Manager In a Shared Recovery Site Configuration

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

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

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

- Use vSphere Replication in a Shared Recovery Site Configuration

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

- Upgrade Site Recovery Manager in a Shared Recovery Site Configuration

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

Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration

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

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

- When connecting to Site Recovery Manager on the shared recovery site, every customer can see all of the Site Recovery Manager extensions that are registered with the shared recovery site, including company names and descriptions. All customers of a shared recovery site can have access to other customers' folders and potentially to other information at the shared recovery site.

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

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

Problem

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

Cause

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

Solution

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

   The default timeout value is 900 seconds (15 minutes). Increase the timeout to, for example, 1200 seconds (20 minutes).

   ```
   <RemoteManager>
     <DefaultTimeout>1200</DefaultTimeout>
   </RemoteManager>
   ```

4. Restart the Site Recovery Manager Server service.

What to do next

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

Site Recovery Manager Licenses in a Shared Recovery Site Configuration

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

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

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

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

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

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

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

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

Install Site Recovery Manager In a Shared Recovery Site Configuration

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

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

Procedure

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

   You install Site Recovery Manager Server to use with a shared recovery site by running the Site Recovery Manager installer from the command line with a custom setup option.

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

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

3 Install the Site Recovery Manager Client Plug-In In a Shared Recovery Site Configuration

   After you install Site Recovery Manager Server instances on the shared recovery site, you must install the Site Recovery Manager client plug-in.

4 Connect to Site Recovery Manager in a Shared Recovery Site Configuration

   When you log in to Site Recovery Manager on a site on which more than one Site Recovery Manager Server is running, Site Recovery Manager prompts you to select one of the Site Recovery Manager Server instances to which to connect.

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

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

6 Configure Placeholders and Mappings in a Shared Recovery Site Configuration

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

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

You install Site Recovery Manager Server to use with a shared recovery site by running the Site Recovery Manager installer from the command line with a custom setup option.

When you run the installer from the command line with the custom setup option, the Site Recovery Manager installer presents additional screens on which you specify a unique Site Recovery Manager extension ID.

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

Prerequisites

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

Procedure

1. Start the Site Recovery Manager installer by typing the custom setup command in a command line terminal.

   `VMware-srm-`*`version-build_number`*`.exe /v"CUSTOM_SETUP=1"`

2. Follow the prompts to begin the Site Recovery Manager installation.
3. At the **VMware vCenter Site Recovery Manager Plugin Identifier** page of the installer, select **Custom SRM Plugin Identifier** and click **Next**.
4. Provide information to identify this custom Site Recovery Manager extension and click **Next**.

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

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

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

What to do next

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

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

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

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

Prerequisites

- You created one or more protected sites, each with a Site Recovery Manager Server instance for which you configured a unique Site Recovery Manager ID.
- Download the Site Recovery Manager installation file to a folder on the Site Recovery Manager Server host.
- This information presumes knowledge of the standard procedure for installing Site Recovery Manager. See Install the Site Recovery Manager Server for information about a standard Site Recovery Manager installation.

Procedure

1. Start the Site Recovery Manager installer by typing the custom setup command in a command line terminal.

   `VMware-srm-version-build_number.exe /v"CUSTOM_SETUP=1"`

2. At the **VMware vCenter Site Recovery Manager Plugin Identifier** page of the installer, select **Custom SRM Plugin Identifier** and click **Next**.
3. Provide information to identify this Site Recovery Manager extension as the partner of a Site Recovery Manager Server server on a protected site, and click **Next**.

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

4. Follow the prompts to complete the remainder of the installation.
5. Repeat Step 1 to Step 4 to install a Site Recovery Manager Server with a Site Recovery Manager ID that matches a Site Recovery Manager Server on another protected site.

   Each additional Site Recovery Manager Server instance that you install connects to the vCenter Server instance on the shared recovery site.

What to do next

Install the Site Recovery Manager client plug-in.

Install the Site Recovery Manager Client Plug-In In a Shared Recovery Site Configuration

After you install Site Recovery Manager Server instances on the shared recovery site, you must install the Site Recovery Manager client plug-in.

After you install the Site Recovery Manager client plug-in, client plug-ins from other Site Recovery Manager Server instances running on the same shared site show as Available in the Manage Plug-ins interface. Install the client plug-in only once. Subsequent installations overwrite each other.

Prerequisites

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

Procedure

1. Connect the vSphere Client to vCenter Server on the shared recovery site.
2. Select **Plugins > Manage Plug-ins**.
3. Under **Available Plug-ins**, locate **VMware vCenter Site Recovery Manager Extension** and click **Download and Install**.

   A client plug-in is available from each of the Site Recovery Manager Server instances that are running on the shared recovery site. You can install the Site Recovery Manager client plug-in from any Site Recovery Manager Server instance. Install the client plug-in only once. Subsequent installations overwrite each other.
4. Follow the prompts of the installer to complete the installation of the Site Recovery Manager client plug-in.
5. Repeat Step 1 through Step 4 to install the Site Recovery Manager client plug-in on all instances of the vSphere Client that you use to connect to Site Recovery Manager on the protected and recovery sites.

What to do next

Connect the protected sites to the shared recovery site.

Connect to Site Recovery Manager in a Shared Recovery Site Configuration

When you log in to Site Recovery Manager on a site on which more than one Site Recovery Manager Server is running, Site Recovery Manager prompts you to select one of the Site Recovery Manager Server instances to which to connect.

For each Site Recovery Manager Server instance that is running at the shared recovery site, the prompt lists the Site Recovery Manager ID, organization, and description that you supplied when you installed Site Recovery Manager Server.

Prerequisites

- You installed one or more Site Recovery Manager Server instances on a shared recovery site.
- You assigned the same Site Recovery Manager extension ID to a Site Recovery Manager Server instance on a protected site and to a Site Recovery Manager Server instance on the shared recovery site.
- You connected the vSphere Client to vCenter Server on the shared recovery site.
- You installed the Site Recovery Manager client plug-in.

Procedure

1. Click **Home** in the vSphere Client.
2. Click **Site Recovery** under Solutions and Applications.
3. Select the Site Recovery Manager ID of the Site Recovery Manager Server instance to connect to and click **Open**.

What to do next

Configure the connections between the protected sites and the shared recovery site.

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

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

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

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

Prerequisites

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

Procedure

1. Log in to Site Recovery Manager on a protected site or log in to one of the Site Recovery Manager instances on the shared recovery site.
2. Select **Sites**, click the **Summary** tab, and click **Configure Connection**.
3. Type the address of the vCenter Server on the remote site and click **Next**.
   - If you logged in to Site Recovery Manager on a protected site, type the address of vCenter Server on the shared recovery site.
   - If you logged in to Site Recovery Manager on the shared recovery site, type the address of vCenter Server on the corresponding protected site. The Site Recovery Manager extension of this vCenter Server instance must have a Site Recovery Manager ID that matches theSite Recovery Manager ID of the Site Recovery Manager instance from which you are connecting.
4. Follow the prompts to accept certificates and provide the login credentials for vCenter Server on the remote site and click **Finish**.

Configure Placeholders and Mappings in a Shared Recovery Site Configuration

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

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

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

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

Prerequisites

- You installed Site Recovery Manager in a shared recovery site configuration.
- You connected the protected sites with the shared recovery site.
- Familiarize yourself with the procedure for configuring placeholders and mappings. For information about configuring placeholders and mappings in a standard configuration, see Chapter 10 Creating Site Recovery Manager Placeholders and Mappings.

Procedure

1 Click **Sites** in the Site Recovery Manager interface on the protected sites and use the **Resource Mappings**, **Folder Mappings**, **Network Mappings**, and **Placeholder Datastores** tabs to configure the mappings.

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

2 (Optional) If you use vSphere Replication, select **vSphere Replication > Datastore Mappings** on the protected sites to map the datastores to a datastore or datastores on the shared recovery site.

The datastore mappings determine in which datastores on the recovery site vSphere Replication places replicated virtual machines.

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

Use Array-Based Replication in a Shared Recovery Site Configuration

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

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

Each protected site can either share the same storage on the shared recovery site, or you can allocate storage individually for each protected site. The type of storage that you use on the shared recovery site can be different than the storage that you use on the protected sites. You can use storage from multiple vendors on the shared recovery site. You must install the appropriate SRA for each type of storage that you use on the shared recovery site.

For information about protection and recovery limits when you use array-based replication with Site Recovery Manager in a shared recovery site configuration, see KB 2008061.

Prerequisites

- You installed Site Recovery Manager in a shared recovery site configuration.
- You connected the protected sites with the shared recovery site.
- Familiarize yourself with the procedure for configuring array-based replication. For information about how to configure array-based replication in a standard configuration, see Chapter 7 Configuring Array-Based Protection.

Procedure

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

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

Use vSphere Replication in a Shared Recovery Site Configuration

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

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

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

You can deploy the vSphere Replication appliance on the shared recovery site from any of the Site Recovery Manager instances on the shared recovery site. After deployment, the vSphere Replication appliance registers with vCenter Server on the shared recovery site and is available to all of the Site Recovery Manager instances on the shared recovery site.

You can deploy multiple additional vSphere Replication servers on the shared recovery site to distribute the replication load. For example, you can deploy on the shared recovery site a vSphere Replication server for each of the protected sites that connects to the shared recovery site. For information about protection and recovery limits when using vSphere Replication with Site Recovery Manager in a shared recovery site configuration, see KB 2008061.

Prerequisites

- You installed Site Recovery Manager in a shared recovery site configuration.
- You connected the protected sites with the shared recovery site.
- Familiarize yourself with the procedure for deploying vSphere Replication. For information about a standard vSphere Replication installation, see Chapter 8 Installing vSphere Replication.

Procedure

1. Deploy a vSphere Replication appliance on each of the protected sites.
2. Deploy one vSphere Replication appliance on the shared recovery site.
3. Log in to Site Recovery Manager on each of the protected sites and configure the vSphere Replication connection to the recovery site.

   All of the vSphere Replication appliances on the protected sites connect to the same vSphere Replication appliance on the recovery site.
4. (Optional) Deploy additional vSphere Replication servers on the shared recovery site.
5. (Optional) Register the additional vSphere Replication servers with the vSphere Replication appliance on the shared recovery site.

   The vSphere Replication servers become available to all Site Recovery Manager instances on the shared recovery site.
6. Configure the mappings from the resources on the protected sites to resources on the shared recovery site and configure the placeholder datastores.
7. Configure the vSphere Replication datastore mappings from the protected sites to datastores on the shared recovery site.

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

Upgrade Site Recovery Manager in a Shared Recovery Site Configuration

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

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

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

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

Prerequisites

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

Procedure

1. Upgrade vCenter Server on the most critical of the protected sites.
2. Upgrade the Site Recovery Manager Server instance that connects to the vCenter Server instance that you upgraded in Step 1.
   - If you upgrade Site Recovery Manager Server without migration, run the Site Recovery Manager installer as for a one-to-one upgrade or installation. The installer obtains from the registry the Site Recovery Manager extension ID that you set during the previous installation. There is no option to modify the Site Recovery Manager extension ID during upgrade.
   - If you upgrade Site Recovery Manager Server with migration, you must run the installer from the command line with the custom setup option. Specify the same Site Recovery Manager extension ID as you used for the previous installation.
3. (Optional) If you use vSphere Replication, upgrade the vSphere Replication appliance that connects to the vCenter Server instance that you upgraded in Step 1.
4. (Optional) If you use array-based replication, upgrade the storage replication adapters (SRA) on the Site Recovery Manager Server host machine that you upgraded in Step 2.
5. Repeat Step 1 to Step 4 for each of the protected sites that connect to the shared recovery site.
6. Upgrade vCenter Server on the shared recovery site.

7 Upgrade the Site Recovery Manager Server instance on the shared recovery site that is paired with the first protected site that you upgraded.

   - If you upgrade Site Recovery Manager Server without migration, the installer obtains from the registry the Site Recovery Manager extension ID that you set during the previous installation. There is no option to modify the Site Recovery Manager extension ID during upgrade.
   - If you upgrade Site Recovery Manager Server with migration, you must specify the same Site Recovery Manager extension ID as you used for the previous installation.

8 (Optional) If you use vSphere Replication, upgrade the vSphere Replication appliance on the shared recovery site.

9 (Optional) If you use array-based replication, upgrade the SRAs for this Site Recovery Manager Server instance on the shared recovery site.

10 Repeat Step 7 and Step 9 for each of the remaining Site Recovery Manager Server instances on the shared recovery site.

11 Upgrade the ESXi Server instances on the shared recovery sites and each of the protected sites.

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

Troubleshooting Site Recovery Manager Installation and Configuration

12

Known troubleshooting information can help you diagnose and correct problems during the installation and configuration of Site Recovery Manager.

Solution

- Cannot Restore SQL Database to a 32-Bit Target Virtual Machine During Site Recovery Manager Upgrade

  You might encounter problems restoring a SQL database on a 32-bit target virtual machine when you upgrade or migrate Site Recovery Manager.

- Site Recovery Manager Server Does Not Start

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

- vSphere Client Cannot Connect to Site Recovery Manager

  Connecting to the Site Recovery Manager interface in the vSphere Client fails.

- Site Pairing Fails Because of Different Certificate Trust Methods

  If you use custom certificates that a certificate authority signs, connecting the Site Recovery Manager sites fails if the root certificate from the certificate authority is not present on Site Recovery Manager Server.

- Error at vService Bindings When Deploying the vSphere Replication Appliance

  When you deploy the vSphere Replication appliance, you get an error at vService bindings in the Deploy OVF Template wizard.

- OVF Package is Invalid and Cannot be Deployed

  When you attempt to deploy OVF for the vSphere Replication appliance, an OVF package error might occur.

- vSphere Replication Appliance or vSphere Replication Server Does Not Deploy from the Site Recovery Manager Interface

  If problems occur when you use the Site Recovery Manager interface to deploy a vSphere Replication appliance or a vSphere Replication server, you can deploy the OVF manually.

- vSphere Replication Cannot Establish a Connection to the Hosts

  Replications fail because vSphere Replication cannot connect to the hosts.

- Connection Errors Between vSphere Replication and SQL Server Cannot be Resolved

  You cannot resolve a connection error between the vSphere Replication appliance and SQL Server.
- 404 Error Message when Attempting to Pair vSphere Replication Appliances

  Pairing vSphere Replication appliances might result in a 404 error message.
- vSphere Replication Service Fails with Unresolved Host Error

  If the address of vCenter Server is not set to a fully qualified domain name (FQDN) or to a literal address, the vSphere Replication service can stop unexpectedly or fail to start after a reboot.
- Increase the Memory of the vSphere Replication Server for Large Deployments

  If you deploy an additional vSphere Replication server, you might need to increase the memory of the vSphere Replication server if that server manages large numbers of virtual machines.
- vSphere Replication Appliance Extension Cannot Be Deleted

  If you delete the vSphere Replication appliance virtual machine, the virtual appliance management interface (VAMI) is not available to delete the appliance extension that still exists in vCenter Server.
- Uploading a Valid Certificate to vSphere Replication Results in a Warning

  When you upload a custom certificate to the vSphere Replication appliance, you see a warning even if the certificate is valid.
- vSphere Replication Status Shows as Disconnected

  The status of the vSphere Replication appliance shows as Disconnected if you are running the Site Recovery Manager client plug-in on Windows XP SP2 x64.
- vSphere Replication Server Registration Takes Several Minutes

  vSphere Replication server registration might take a long time depending on the number of hosts in the vCenter Server inventory.
- vSphere Replication is Inaccessible After Changing vCenter Server Certificate

  If you change the SSL certificate of vCenter Server, you cannot access vSphere Replication.

Cannot Restore SQL Database to a 32-Bit Target Virtual Machine During Site Recovery Manager Upgrade

You might encounter problems restoring a SQL database on a 32-bit target virtual machine when you upgrade or migrate Site Recovery Manager.

Problem

If you use an SQL Express database and upgrade or migrate Site Recovery Manager to a new database server, restoring the database on a 32-bit operating system might fail.

Use Attach rather than Restore when you migrate the SQL Express database on the 64-bit target virtual machine rather than on a 32-bit target virtual machine.

If you use SQL Express bundled with vCenter Server, note the following conditions:

- If you uninstall vCenter Server, SQL Express is also removed and you lose all your Site Recovery Manager data.
- Create and manage a separate database instance in the SQL Express server. Site Recovery Manager does not install on a database, that is pointed to by a DSN that contains vCenter Server data, regardless of database vendor, version, or edition.

Solution

1. To install SQL Express and migrate the database during Site Recovery Manager upgrade, stop the Site Recovery Manager service and back up your database.
2. Install SQL Express on the new host or virtual machine.
3. Copy the backup file to the new host or virtual machine and restore the database from it.
4. Create a system DSN that points to the restored database.
5. Install Site Recovery Manager and select **Use existing database** for both migration and upgrade.

Site Recovery Manager Server Does Not Start

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

Problem

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

Cause

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

Solution

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

   If the vCenter Server service is running on a different host to the Site Recovery Manager Server and the vCenter Server service stops, the Site Recovery Manager Server will start succesfully and then stop after a short period.
2. Verify that the Site Recovery Manager database service is running.
3. Log in to the machine on which you installed the Site Recovery Manager Server.
4. Verify that Site Recovery Manager can connect to vCenter Server.
   a. Open **Programs and Features** from the Windows Control Panel.
   b. Select the entry for **VMware vCenter Site Recovery Manager** and click **Change**.

c Click **Next**.

d Select **Modify**.

e Check that the address for vCenter Server is correct.

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

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

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

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

h Type the credentials for the Site Recovery Manager database and click **Next**.

If the connection to the database fails, close the Site Recovery Manager installer and go to Step 5.

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

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

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

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

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

c Check that Site Recovery Manager is attempting to connect to the correct database server and click **Next**.

d Enter the login credentials for the Site Recovery Manager database and click **Next**.

e Review the database settings on the next pages, and click **Finish**.

f Click **Test Data Source**.

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

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

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

If the Site Recovery Manager logs contain the message `GetConnection: Still waiting for available connections`, increase the maximum number of database connections.

Note Consult with your database administrator before changing these settings.

a Open the `vmware-dr.xml` file in a text editor.

You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder on the Site Recovery Manager Server host.

b Change the `<connectionCount>` value to increase the size of the pool of database connections from the default of 5.

```
<connectionCount>10</connectionCount>
```

c Change the `<maxConnections>` value to increase the maximum number of database connections from the default of 20.

```
<maxConnections>30</maxConnections>
```

d Restart the Site Recovery Manager service.

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

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

- Windows Server
- Windows Workstation
- Protected Storage

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

vSphere Client Cannot Connect to Site Recovery Manager

Connecting to the Site Recovery Manager interface in the vSphere Client fails.

Problem

When you click the **Site Recovery** icon in the Home page of the vSphere Client, the connection to Site Recovery Manager fails with the message:

```
Connection to local Site Recovery Manager https:SRM_address:8095/dr failed
```

The Site Recovery Manager logs show a certificate error.

```
Failed to establish connection to VMware vCenter.
: std::exception 'class Vmacore::Ssl::SSLVerifyException'
"SSL Exception:
The remote host certificate has these problems:
* The host name used for the connection does not match the subject name on the host certificate
* The host certificate chain is not complete.
```

Cause

This problem can occur if the certificate for vCenter Server does not match the certificate that Site Recovery Manager requires, for example if the certificate for vCenter Server changed since you installed Site Recovery Manager.

Solution

Restore the vCenter Server certificate to the certificate that you used when you installed Site Recovery Manager or install a new vCenter Server certificate.

Site Pairing Fails Because of Different Certificate Trust Methods

If you use custom certificates that a certificate authority signs, connecting the Site Recovery Manager sites fails if the root certificate from the certificate authority is not present on Site Recovery Manager Server.

Problem

When you try to connect Site Recovery Manager sites, the connection fails with the error `Local and Remote servers are using different certificate trust methods`.

Cause

You did not install the root certificate for the certificate authority that signs the Site Recovery Manager certificate on Site Recovery Manager Server.

Solution

1. Use the Windows Certificate Manager utility to install the root certificate for the certificate authority that you use to sign the Site Recovery Manager certificate.

   The Certificate Manager utility is at `C:\Windows\System32\certmgr.msc` on the Site Recovery Manager Server host.
2. From the Windows Control Panel, run the Site Recovery Manager installer in Modify mode.
3. At the Certificate Type Selection page of the installer, select **Use a PKCS#12 certificate file** and browse to the custom Site Recovery Manager certificate.
4. Follow the prompts and click **Finish** to run the Site Recovery Manager installer in Modify mode.

Error at vService Bindings When Deploying the vSphere Replication Appliance

When you deploy the vSphere Replication appliance, you get an error at vService bindings in the Deploy OVF Template wizard.

Problem

When you deploy the vSphere Replication, an error appears at vService bindings in the Deploy OVF Template wizard.

```
Unsupported section '{http://www.vmware.com/schema/ovf}vServiceDependencySection'(A vService
dependency)
```

Cause

This error is typically the result of the vCenter Management Web service being paused or stopped.

Solution

Attempt to start the vCenter Management Web service. If vCenter Server is running as a Linux virtual appliance, reboot the appliance.

OVF Package is Invalid and Cannot be Deployed

When you attempt to deploy OVF for the vSphere Replication appliance, an OVF package error might occur.

Problem

The error `OVF package is invalid and cannot be deployed` might appear while you attempt to deploy the vSphere Replication appliance.

Cause

This problem is due to the vCenter Server port being changed from the default of 80.

Solution

If possible, change the vCenter Server port back to 80.

vSphere Replication Appliance or vSphere Replication Server Does Not Deploy from the Site Recovery Manager Interface

If problems occur when you use the Site Recovery Manager interface to deploy a vSphere Replication appliance or a vSphere Replication server, you can deploy the OVF manually.

Problem

Deployment of the vSphere Replication appliance or vSphere Replication server from the Site Recovery Manager interface fails.

Solution

1. Select **File > Deploy OVF Template** in the vSphere Client.
2. Navigate to the vSphere Replication appliance or vSphere Replication server OVF file in the www directory in the Site Recovery Manager installation.

Option	OVF File
vSphere Replication appliance	`C:\Program Files\VMware\VMware vCenter Site Recovery Manager\www\vSphere_Replication_SRM_OVF10.ovf`
vSphere Replication server	`C:\Program Files\VMware\VMware vCenter Site Recovery Manager\www\vSphere_Replication_Server_SRM_OVF10.ovf`

3. Follow the prompts to deploy the vSphere Replication appliance or the vSphere Replication server.

vSphere Replication Cannot Establish a Connection to the Hosts

Replications fail because vSphere Replication cannot connect to the hosts.

Problem

vSphere Replication needs access to port 80. You might see forbidden HTTP connections in the vSphere Replication logs.

Solution

Make sure the vSphere Replication appliance has access to port 80 on the storage hosts.

For a list of ports that must be open for vSphere Replication, see Site Recovery Manager Network Ports.

Connection Errors Between vSphere Replication and SQL Server Cannot be Resolved

You cannot resolve a connection error between the vSphere Replication appliance and SQL Server.

Problem

vSphere Replication might not be able to connect to SQL Server, and you have insufficient information to solve this problem.

Cause

Several issues can cause this problem, and initially available information about the problem is insufficient to affect a resolution.

Solution

1. Use a file management tool to connect to the vSphere Replication appliance.

   For example, you might use SCP or WinSCP. Connect using the root account, which is the same account used to connect to the VAMI.
2. Delete any files you find in `/opt/vmware/hms/logs`.
3. Connect to the VAMI and attempt to save the vSphere Replication configuration.

   This action recreates the SQL error.
4. Connect to the vSphere Replication appliance again and find the `hms-configtool.log` file which is in `/opt/vmware/hms/logs`.

   This log file contains information about the error that just occurred. Use this information to troubleshoot the connection issue, or provide the information to VMware for further assistance. See Reconfigure vSphere Replication to Use an External Database.

404 Error Message when Attempting to Pair vSphere Replication Appliances

Pairing vSphere Replication appliances might result in a 404 error message.

Problem

vSphere Replication might fail with a 404 error when you are pairing vSphere Replication appliances.

This problem happens if you paired the Site Recovery Manager Server instances by using a vCenter Server address that differs from the address in the **vCenter Server Address** entry in the vSphere Replication virtual appliance management interface (VAMI).

Cause

By default, vSphere Replication uses the IP address of the vCenter Server instance to connect to vCenter Server.

If you paired the Site Recovery Manager sites using host names, the vSphere Replication pairing fails with an error.

```
Unexpected status code: 404
```

The vCenter Server address value in the VAMI must match the address that you provide when you connect the sites.

- If you used an IP address to pair the Site Recovery Manager sites, you must use the same IP address to connect vSphere Replication to vCenter Server.
- If you used a host name to pair the Site Recovery Manager sites, you must use the same host name to connect vSphere Replication to vCenter Server.

Solution

1. Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

   You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.
2. Type the same IP address or host name for vCenter Server as you used when you configured the pairing of the Site Recovery Manager sites.
3. Click **Save and Restart Service** to apply the changes.

vSphere Replication Service Fails with Unresolved Host Error

If the address of vCenter Server is not set to a fully qualified domain name (FQDN) or to a literal address, the vSphere Replication service can stop unexpectedly or fail to start after a reboot.

Problem

The vSphere Replication service stops running or does not start after a reboot. The error `unable to resolve host: non-fully-qualified-name` appears in the vSphere Replication logs.

Solution

1. In the vSphere Client, select **Administration > vCenter Server Settings > Advanced Settings** and check that the `VirtualCenter.FQDN` key is set to either a fully qualified domain name or to a literal address.
2. Connect to the VAMI of the vSphere Replication appliance in a Web browser.

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

   You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.
3. Enter the same FQDN or literal address for vCenter Server as you set for the `VirtualCenter.FQDN` key.

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

Increase the Memory of the vSphere Replication Server for Large Deployments

If you deploy an additional vSphere Replication server, you might need to increase the memory of the vSphere Replication server if that server manages large numbers of virtual machines.

Problem

vSphere Replication supports a maximum of 100 virtual machines per vSphere Replication server. Replication of more than 100 virtual machines on a single vSphere Replication server can cause memory swapping on the vSphere Replication server, which affects performance.

Solution

For deployments that exceed 100 virtual machines per vSphere Replication server, increase the RAM of the vSphere Replication server virtual machine from the default of 512MB to 1GB.

Alternatively, deploy additional vSphere Replication servers and balance the replication load accordingly.

vSphere Replication Appliance Extension Cannot Be Deleted

If you delete the vSphere Replication appliance virtual machine, the virtual appliance management interface (VAMI) is not available to delete the appliance extension that still exists in vCenter Server.

Problem

Deleting the vSphere Replication appliance does not remove the vSphere Replication extension from vCenter Server.

Solution

1 Use the Managed Object Browser (MOB) to delete the vSphere Replication extension manually.

2 Redeploy the appliance and reconfigure the replications.

See Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted

Uploading a Valid Certificate to vSphere Replication Results in a Warning

When you upload a custom certificate to the vSphere Replication appliance, you see a warning even if the certificate is valid.

Problem

When you use the virtual appliance management interface (VAMI) in Internet Explorer to upload certificates to the vSphere Replication appliance, you see a certificate error:

```
The certificate installed with warnings. Remote VRM systems with the 'Accept only SSL certificate
signed by a
trusted CA' option enabled may be unable to connect to this site for the following reason: The
certificate was not issued
for use with the given hostname: vr_appliance_hostname.
```

Solution

Ignore this error, or connect to the VAMI by using a supported browser other than Internet Explorer.

vSphere Replication Status Shows as Disconnected

The status of the vSphere Replication appliance shows as Disconnected if you are running the Site Recovery Manager client plug-in on Windows XP SP2 x64.

Problem

The status of the vSphere Replication appliance shows as Disconnected in the Summary tab for a vSphere Replication site. Attempting to reconfigure the connection results in the error `Lost connection to local VRMS server at server_address:8043. (The client could not send a complete request to the server 'server_address'. (The underlying connection was closed: An unexpected error occurred on a send.))`.

Cause

This problem occurs because the Site Recovery Manager client plug-in and vSphere Client cannot negotiate cryptography when the Site Recovery Manager client plug-in runs on older versions of Windows. If you run the desktop version of vSphere Client and Site Recovery Manager client plug-in on Windows XP SP2 x64, you might encounter incompatibilities between server and client cryptography support. Site Recovery Manager does not support older Windows XP x64 service packs.

Windows XP SP3 x86 is not affected by this issue. Site Recovery Manager does not support older Windows XP x86 service packs.

Solution

Download and install the Microsoft Hotfix from Microsoft KB 948963 http://support.microsoft.com/kb/948963. This hotfix is not applied in any regular Windows updates so you must manually download and apply the fix.

vSphere Replication Server Registration Takes Several Minutes

vSphere Replication server registration might take a long time depending on the number of hosts in the vCenter Server inventory.

Problem

If the vCenter Server inventory contains a few hundred or more hosts, the Register VR Server task takes more than a few minutes to complete.

Cause

vSphere Replication updates each host's SSL thumbprint registry. The vCenter Server Events pane displays `Host is configured for vSphere Replication` for each host as the vSphere Replication server registration task progresses.

Solution

1. Wait for the registration task to complete.

   After it finishes, you can use vSphere Replication for incoming replication traffic.

2. Alternatively, edit `/opt/vmware/hms/conf/hms-configuration.xml` and change `hms-config-host-at-hbr-threadpool-size` parameter to a higher value to enable parallel processing of more hosts at a time and restart the vSphere Replication management server `/etc/init.d/hms restart`

vSphere Replication is Inaccessible After Changing vCenter Server Certificate

If you change the SSL certificate of vCenter Server, you cannot access vSphere Replication.

Problem

vSphere Replication uses certificate-based authentication to connect to vCenter Server. If you change the vCenter Server certificate, vSphere Replication is inaccessible.

Cause

The vSphere Replication database contains the old vCenter Server certificate.

Solution

1. Power off and power on the vSphere Replication appliance.

   vSphere Replication obtains the new certificate from vCenter Server when it powers on.

2 (Optional) If you configured vSphere Replication to use an external database, log into the virtual appliance management interface (VAMI) of the vSphere Replication appliance and click **Configuration > Save and Restart Service**.

   Do not change any configuration information before clicking **Save and Restart Service**.

   vSphere Replication restarts with the new vCenter Server certificate.