Site Recovery Manager Installation and Configuration

Modified on 16 AUG 2022

Site Recovery Manager 8.5

vmware by Broadcom

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

https://docs.vmware.com/

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

Contents

About VMware Site Recovery Manager Installation and Configuration

Site Recovery Manager Installation and Configuration provides information about how to install, upgrade, and configure VMware 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 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
16 AUG 2022	Added Chapter 14 Migrating Storage Policy Protection Groups to Array-Based Replication Protection Groups.
05 OCT 2021	Initial release.

Overview of VMware Site Recovery Manager

1

VMware 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 protect virtual machines in different ways.

Datastore groups

Protect the virtual machines in datastore groups by using third-party disk replication mechanisms to configure array-based replication. Array-based replication surfaces replicated datastores to recover virtual machine workloads.

Individual virtual machines

Protect the individual virtual machines on a host by using Site Recovery Manager in combination with VMware vSphere Replication.

Storage policies

Protect virtual machines based on their association with specific storage policies. Protecting virtual machines by using storage policies requires array-based replication.

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

Planned migration

The orderly evacuation of virtual machines from the protected site to the recovery site. Planned migration prevents data loss when migrating workloads in an orderly fashion. For planned migration to succeed, both sites must be running and fully functioning.

Disaster recovery

Similar to planned migration except that disaster recovery does not require that both sites be up and running, for example if the protected site goes offline unexpectedly. During a disaster recovery operation, failure of operations on the protected site is reported but is otherwise ignored.

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

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

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

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

- About Protected Sites and Recovery Sites

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

- Bidirectional Protection

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

- Heterogeneous Configurations on the Protected and Recovery Sites

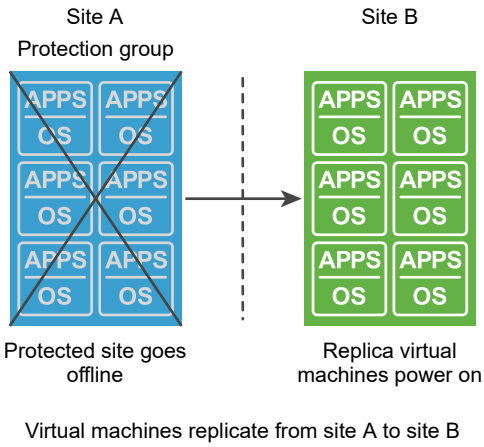
  Some components in the Site Recovery Manager and vCenter Server installations must be identical on each site. Because the protected and recovery sites are often in different physical locations, some components on the protected site can be of a different type to their counterparts on the recovery site.

About Protected Sites and Recovery Sites

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

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

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



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

- The version of vCenter Server must be compatible with the version of Site Recovery Manager. For information about compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.5* at https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.
- Each site must have at least one datacenter.
- If you are using array-based replication, the same replication technology must be available at both sites, and the arrays must be paired.
- If you are using vSphere Replication, you require a vSphere Replication appliance on both sites. The vSphere Replication appliances must be connected to each other.
- The vSphere Replication version must be compatible with the version of Site Recovery Manager. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.5* at https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.
- The recovery site must have hardware, network, and storage resources that can support the same virtual machines and workloads as the protected site. You can oversubscribe the recovery site by running additional virtual machines there that are not protected. In this case, during a recovery you must suspend noncritical virtual machines on the recovery site.
- The sites must be connected by a reliable IP network. If you are using array-based replication, ensure that your network connectivity meets the arrays' network requirements.
- The recovery site should have access to comparable public and private networks as the protected site, although not necessarily the same range of network addresses.

Bidirectional Protection

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

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

Heterogeneous Configurations on the Protected and Recovery Sites

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

Site Recovery Manager is compatible with N-1 version of Site Recovery Manager on the paired site. For example, if the current version of Site Recovery Manager is 8.5, the supported versions for the paired site is 8.4 and later.

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 https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.

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

Component	Heterogeneous or Identical Installations
Site Recovery Manager Server	Must be a compatible version on both sites. Site Recovery Manager is compatible with N-1 version of Site Recovery Manager on the paired site.
vCenter Server and Platform Services Controller	The Site Recovery Manager version must be compatible with the vCenter Server and Platform Services Controller version.
vSphere Replication	Must be a compatible version on both sites. The vSphere Replication version must be compatible with the Site Recovery Manager version and the vCenter Server version.
vCenter Server Appliance or vCenter Server for Windows instance	Can be different on each site. You can run a vCenter Server Appliance on one site and a vCenter Server for Windows instance on the other site.

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

Component	Heterogeneous or Identical Installations
Storage arrays for array-based replication	Can be different versions on each site. You can use different versions of the same type of storage array on each site. The Site Recovery Manager Server instance on each site requires the appropriate storage replication adapter (SRA) for each version of storage array for that site. Check SRA compatibility with all versions of your storage arrays to ensure compatibility.
Site Recovery Manager database	Can be different on each site. You can use different versions of the same type of database on each site.

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 in the Japanese locale
  - Site Recovery Manager extends a vCenter Server Appliance instance
- Site B in the United States:
  - Site Recovery Manager Server runs 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 System Requirements

2

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

Minimum System Requirements for the Site Recovery Manager Virtual Appliance

Site Recovery Manager is distributed as a 64-bit virtual appliance packaged in the `.ovf` format. You must deploy the virtual appliance in a vCenter Server environment by using the OVF deployment wizard on an ESXi host.

Deployment type	Requirement
Light	2 vCPU, 8 GB RAM, one 16 GB hard disk, and one 4 GB hard disk, 1 Gbit network card. You can use the light deployment type for deployments that protect less than 1000 virtual machines. **Note** To increase the number of vCPUs and RAM, edit the settings of the Site Recovery Manager appliance virtual machine.
Standard	4 vCPU, 12 GB RAM, one 16 GB hard disk, and one 4 GB hard disk, 1 Gbit network card. Use the standard deployment type for deployments that protect more than 1000 virtual machines.

- Site Recovery Manager Licensing

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

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

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

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, contact your VMware sales representative.

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

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

Site Recovery Manager License Keys and Shared Platform Services Controller Instances

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

Site Recovery Manager License Keys and Protected and Recovery Sites

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

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

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

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 for each site, that you install on both the protected and the recovery site to allow bidirectional protection between the sites.

You have two sites that contain 25 virtual machines each for Site Recovery Manager to protect.

- For reprotect, you require a license for at least 50 virtual machines for each site, that you install on both the protected and the recovery site to allow bidirectional protection between the sites.

Operational Limits of Site Recovery Manager

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

Protection Maximums for Site Recovery Manager 8.5

Table 2-1. Protection Maximums for Site Recovery Manager 8.5

Item	Maximum
Total number of virtual machines configured for protection (array-based replication, vSphere Replication, Virtual Volumes Replication, and storage policy protection combined)	5000
Total number of virtual machines configured for protection using array-based replication	5000
Total number of virtual machines configured for protection using vSphere Replication	3000
Total number of virtual machines configured for protection using Virtual Volumes Replication	500 **Note** Contact your storage vendor for exact number of supported virtual machines, replicated with Virtual Volumes Replication.
Total number of virtual machines configured for storage policy protection	2000
Total number of virtual machines configured for storage policy protection with stretched storage	1000
Total number of virtual machines configured for protection using array-based replication with stretched storage	1000
Total number of virtual machines per protection group	500

Table 2-1. Protection Maximums for Site Recovery Manager 8.5 (continued)

Item	Maximum
Total number of array-based replication protection groups and vSphere Replication protection groups	500
Total number of storage policy protection groups	32
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Total number of virtual machines per recovery plan	2000
Total number of replicated datastores (using array-based replication)	255
Total number of replicated devices (using array-based replication)	255
Total number of replicated datastores and replicated devices (using array-based replication)	255

You can run array-based protection groups alongside vSphere Replication protection groups and storage policy protection groups in the same Site Recovery Manager server instance. The total number of protection groups cannot exceed 500 for all protection types combined. For example, you cannot create 250 array-based replication protection groups and then create 350 vSphere Replication protection groups, as this creates 600 protection groups in total.

If you have 250 array-based protection groups, you can create additional 250 vSphere Replication protection groups, to make a total of 500 protection groups. Similarly, in a setup that combines an array-based replication and vSphere Replication, you can protect a maximum of 5,000 virtual machines, even if you combine replication types. The protection limit for array-based replication is 5,000 virtual machines. The protection limit for vSphere Replication is 3,000 virtual machines. However, the maximum number of virtual machines that you can protect by using a combination of array-based and vSphere Replication is still 5,000 virtual machines, and not 8,000.

If you protect 3,000 virtual machines with vSphere Replication, you can protect a maximum of another 2,000 virtual machines with array-based replication.

If you protect 1,000 virtual machines with array-based replication, you can protect a maximum of another 3,000 virtual machines with vSphere Replication.

Bidirectional Protection

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

If you protect 3,000 virtual machines using array-based replication from site A to site B, you can use array-based replication to protect a maximum of 2,000 virtual machines from site B to site A. If you are using array-based replication for bidirectional protection, you can protect a total of 5,000 virtual machines across both sites.

If you protect 155 replicated datastores using array-based replication from site A to site B, you can use array-based replication to protect a maximum of 100 replicated datastores from site B to site A. If you are using array-based replication for bidirectional protection, you can protect a total of 255 replicated datastores across both sites.

If you protect 1500 virtual machines using vSphere Replication from site A to site B, you can use vSphere Replication to protect a maximum of 1500 virtual machines from site B to site A. If you are using vSphere Replication for bidirectional protection, you can protect a maximum of 3000 virtual machines across both sites.

If you protect 3,000 virtual machines using array-based replication from site A to site B and 1,000 virtual machines using vSphere Replication from site A to site B, you can protect a maximum of 1,000 virtual machines from site B to site A. If you are using a combination of array-based replication and vSphere Replication for bidirectional protection, you can protect a maximum of 5,000 virtual machines across both sites, of which you can protect a maximum of 3,000 by using vSphere Replication.

Recovery Maximums for Site Recovery Manager 8.5

Item	Maximum
Total number of concurrently running recovery plans.	10
Total number of virtual machine recoveries that you can start simultaneously, for array-based replication, vSphere Replication, and storage policy protection combined, across multiple recovery plans.	2000

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

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

IP Customization Maximums for Site Recovery Manager 8.5

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

- 1 IP address

- Subnet information
- 1 gateway server address
- 2 DNS servers (primary and secondary)

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

Deployment Maximums for Site Recovery Manager 8.5 in a Shared Recovery Site Configuration

In a shared recovery site configuration, you can deploy a maximum of 10 Site Recovery Manager server instances for each vCenter Server instance. The limits apply to each Site Recovery Manager pair in a shared recovery site configuration.

Network Ports for Site Recovery Manager

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

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

vCenter Server and ESXi Server network port requirements for Site Recovery Manager 8.5

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

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

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

Site Recovery Manager Server 8.5 network ports

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

Default Port	Protocol or Description	Source	Target	Endpoints or Consumers
443	HTTPS	Site Recovery Manager HTML 5 user interface	Site Recovery Manager	Default port for the Site Recovery Manager HTML 5 user interface.
443	HTTPS	Site Recovery Manager HTML 5 user interface	Local and remote vCenter Server or all vCenter Server instances in Enhanced Linked Mode on which there is a registered Site Recovery Manager. For more information about Enhanced Linked Mode, see *vCenter Enhanced Linked Mode for vCenter Server Appliance* in the *vCenter Server Installation and Setup* documentation.	Default port for the Site Recovery Manager HTML 5 user interface. when you open it from the Site Recovery Manager appliance.
443	HTTPS	Site Recovery Manager HTML 5 user interface	Local and remote Platform Services Controller (PSC) or all Platform Services Controller instances in Enhanced Linked Mode on which there is a registered Site Recovery Manager.	Default port for the Site Recovery Manager HTML 5 user interface. when you open it from the Site Recovery Manager appliance.
443	HTTPS	Site Recovery Manager	vCenter Server	Default SSL Web Port for incoming TCP traffic.
443	HTTPS	Site Recovery Manager	Platform Services Controller	Traffic from Site Recovery Manager Server to local and remote Platform Services Controller.

Default Port	Protocol or Description	Source	Target	Endpoints or Consumers
443	HTTPS	Site Recovery Manager on the recovery site	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with configured IP customization, or callout commands on recovered virtual machines.
443	HTTPS	vSphere Web Client	Site Recovery Manager Appliance	All management traffic to Site Recovery Manager Server goes to this port. This includes traffic by external API clients for task automation and HTTPS interface for downloading the UI plug-in and icons. This port must be accessible from the vCenter Server proxy system. Used by vSphere Web Client to download the Site Recovery Manager client plug-in.
443	TCP	Site Recovery Manager Appliance	https://vcsa.vmware.com	Customer Experience Improvement Program (CEIP) for Site Recovery Manager

Default Port	Protocol or Description	Source	Target	Endpoints or Consumers
902	TCP and UDP	Site Recovery Manager Server on the recovery site.	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with IP customization, with configured callout commands on recovered virtual machines, or that use raw disk mapping (RDM). All NFC traffic for updating or patching the VMX files of virtual machines that are replicated using vSphere Replication use this port.
5480	HTTPS	Web Browser	Site Recovery Manager Appliance	Site Recovery Manager Appliance Management Interface

Site Pairing Port Requirements

Port	Protocol	Source	Target	Description
443	HTTPS	vCenter Server	Site Recovery Manager Server	vCenter Server and target Site Recovery Manager Appliance communication.
443	HTTPS	Site Recovery Manager Server	Site Recovery Manager Server on target site	Bi-directional communication between Site Recovery Manager servers.
443	HTTPS	Site Recovery Manager	Platform Services Controller and vCenter Server	Site Recovery Manager to vCenter Server communication - local and remote.

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

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

Port	Protocol or Description	Source	Target	Endpoints or Consumers
31031	Initial replication traffic	ESXi host	vSphere Replication appliance on the recovery site	From the ESXi host at the protected site to the vSphere Replication appliance at the recovery site
32032	TCP	ESXi host on the source site	vSphere Replication server at the target site	Initial and outgoing replication traffic from the ESXi host at the source site to the vSphere Replication appliance or vSphere Replication server at the target site for replication traffic with network encryption.
8043	HTTPS	Site Recovery Manager	vSphere Replication appliance on the recovery and protected sites	Management traffic between Site Recovery Manager instances and vSphere Replication appliances.

Creating the Site Recovery Manager Database

3

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

Site Recovery Manager provides an embedded vPostgreSQL database that requires fewer steps to configure than an external database. The embedded vPostgreSQL database supports a full-scale Site Recovery Manager environment.

Each Site Recovery Manager site requires its own instance of the Site Recovery Manager database.

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

For the list of database software that Site Recovery Manager supports, see the *Compatibility Matrices for Site Recovery Manager 8.5* at https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.

Back Up and Restore the Embedded vPostgres Database

When you deploy the Site Recovery Manager appliance, Site Recovery Manager creates a vPostgres database during the installation process. You can back up and restore the embedded vPostgres database by using PostgreSQL commands.

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

Prerequisites

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

Procedure

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. In the Site Recovery Manager Appliance Management Interface, click **Services**, and stop the Site Recovery Manager service.
3. Log into the Site Recovery Manager host machine.
4. Create a backup of the embedded vPostgres database by using the `pg_dump` command.

   ```
   /opt/vmware/vpostgres/current/bin/pg_dump -Fc --username=db_username srmdb > srm_backup_name
   ```

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

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

   ```
   /opt/vmware/vpostgres/current/bin/pg_restore -Fc --username=db_username --dbname=srmdb srm_backup_name
   ```
7. (Optional) To restore the database on the same system from which you created the backup, you must use the `--clean` option with the `pg_restore` command.

   ```
   /opt/vmware/vpostgres/current/bin/pg_restore --clean -Fc --username=db_username --dbname=srmdb srm_backup_name
   ```
8. Start the Site Recovery Manager service.

Site Recovery Manager Authentication

4

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

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

Solution User Authentication

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

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

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

Solution Users and Site Recovery Manager Site Pairing

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

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

If you change the solution user or renew the solution user certificate at the remote site, you must reconfigure the Site Recovery Manager site pairing.

Site Recovery Manager SSL/TLS Server Endpoint Certificates

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

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

Creating SSL/TLS Server Endpoint Certificates for Site Recovery Manager

5

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

The Site Recovery Manager 8.5 appliance generates a self-signed SSL certificate when the appliance first boots. The Site Recovery Manager 8.5 self-signed certificate expires after five years from the first boot of the appliance.

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

Note For information about how Site Recovery Manager authenticates with vCenter Server, see Chapter 4 Site Recovery Manager Authentication.

Read the following topics next:

- Requirements When Using Custom SSL/TLS Certificates With Site Recovery Manager
- Enable the SHA-1 Hashing Function

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

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

Site Recovery Manager 8.x uses standard PKCS#12 certificates. Site Recovery Manager places some requirements on the contents of those certificates.

- Site Recovery Manager does not accept certificates with MD5 signature algorithms. Use SHA256 or stronger signature algorithms.
- By default, Site Recovery Manager does not accept certificates with SHA-1 signature algorithms. Use SHA256 or stronger signature algorithms.
- The Site Recovery Manager certificate is not the root of a trust chain. You can use an intermediate CA certificate which is not the root of a trust chain, but that is still a CA certificate.

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

Enable the SHA-1 Hashing Function

You can install certificates, signed with the SHA-1 hashing function in the Site Recovery Manager Appliance in case your environment requires it.

By default, the Site Recovery Manager server rejects installation of new certificates, which are signed with the SHA-1 hashing function. To install a certificate, signed with the SHA-1 hashing function, you must enable it in the Site Recovery Manager Appliance.

Procedure

1 Establish an SSH connection to the Site Recovery Manager Appliance.

2 Navigate to the `/opt/vmware/srm/conf/` folder and open the `vmware-dr.xml` and the `drconfig.xml` files in a text editor.

3 Find the `<connections>` section and add a `<allowSha1>` section.

```
<connections>
   <allowSha1>true</allowSha1>
</connections>
```

4 Save the files and restart the Site Recovery Manager Server service.

5 Use the following command to restart the *dr-configurator* service.

```
sudo systemctl restart dr-configurator
```

Deploying the Site Recovery Manager Appliance

6

The Site Recovery Manager Virtual Appliance is a preconfigured virtual machine that is optimized for running Site Recovery Manager and its associated services. You deploy the appliance on an ESXi host in your vSphere environment.

You can use the Site Recovery Manager Appliance Management Interface to configure the Site Recovery Manager Appliance and edit the appliance settings.

After you deploy and configure Site Recovery Manager instances on both sites, the Site Recovery Manager plug-in appears in the vSphere Web Client or the vSphere Client.

The Site Recovery Manager Appliance supports only the vPostgress embedded database.

For information about the compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.5* at https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.

Read the following topics next:

- Site Recovery Manager and vCenter Server Deployment Models
- Prerequisites and Best Practices for Site Recovery Manager Server Deployment
- Deploy the Site Recovery Manager Virtual Appliance
- Log In to the VMware Site Recovery Manager Appliance Management Interface
- Configure the Site Recovery Manager Appliance to Connect to a vCenter Server
- Connect to the Site Recovery Manager Appliance Embedded vPostgres Database
- How to Set Up a Trusted Environment for the Site Recovery Manager Virtual Appliance
- Use the VMware OVF Tool to Deploy the Site Recovery Manager Virtual Appliance Virtual Machine from a Client OVF Template
- Connect the Site Recovery Manager Server Instances on the Protected and Recovery Sites
- Reconnect a Site Pair and Breaking a Site Pair
- Establish a Client Connection to the Remote Site Recovery Manager Server Instance
- Install the Site Recovery Manager License Key
- Unregister an Incompatible Version of vSphere Replication

Site Recovery Manager and vCenter Server Deployment Models

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

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

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

- Each Platform Services Controller can have its own vCenter Single Sign-On domain.
- Several Platform Services Controller instances can join the same vCenter Single Sign-On domain.
- You can configure vCenter Single Sign-On domains in Enhanced Linked Mode, which federates all of the Platform Services Controller instances from each of the linked domains.

For information about the deployment models that vCenter Server supports, see Deploying the vCenter Server Appliance in *vCenter Server Installation and Setup*.

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

Configuring the Platform Services Controller and Selecting the Correct vCenter Server Instance in an Enhanced Linked Mode Environment

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

- When you install Site Recovery Manager Server on the protected site, make sure that you select the vCenter Server instance that manages the virtual machines to protect.
- When you install Site Recovery Manager Server on the recovery site, make sure that you select the vCenter Server instance to which to recover virtual machines.

- Ensure that the Platform Services Controller, vCenter Server, and Site Recovery Manager Server are all located on the protected site, or all on the recovery site.

After you have installed Site Recovery Manager, if vCenter Server migrates to a different Platform Services Controller or if the address of the Platform Services Controller changes, you can reconfigure Site Recovery Manager with the new Platform Services Controller address. For example, you can change from an embedded Platform Services Controller to an external Platform Services Controller. For information about changing Platform Services Controller, see Converging vCenter Server with an External Platform Services Controller to a vCenter Server with an Embedded Platform Services Controller in *vCenter Server Installation and Setup*. If you plan on converging an external Platform Services Controller to an embedded Platform Services Controller, you must perform the steps in the correct order to ensure the proper operation of Site Recovery Manager.

1. Converge the external Platform Services Controller on the protected site to an embedded Platform Services Controller.
2. Reconfigure Site Recovery Manager and vSphere Replication at the protected site to use the new embedded Platform Services Controller. Verify through the Site Recovery user interface that Site Recovery Manager and vSphere Replication are connected to the new Platform Services Controller.
3. Converge the external Platform Services Controller on the recovery site to an embedded Platform Services Controller.
4. Reconfigure Site Recovery Manager and vSphere Replication at the recovery site to use the new embedded Platform Services Controller. Verify through the Site Recovery user interface that Site Recovery Manager and vSphere Replication are connected to the new Platform Services Controller.
5. If necessary, reconnect the protected and the recovery sites.

Note If you are in an Enhanced Linked Mode environment, you must first converge the Platform Services Controller of all federated partners before reconfiguring Site Recovery Manager and vSphere Replication.

You change the Platform Services Controller address by reconfiguring the Site Recovery Manager appliance. If you are unable to connect Site Recovery Manager or vSphere Replication to the new Platform Services Controller, see KB 85970.

Sharing Platform Services Controller Instances Across Site Recovery Manager Sites

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

Concurrent Installations of Site Recovery Manager in an Enhanced Linked Mode Environment

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

- If the installation of one Site Recovery Manager Server instance overlaps with the installation of another Site Recovery Manager Server instance under two different Platform Services Controller instances.
- Those Platform Services Controller instances are in Enhanced Linked Mode.

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

Site Recovery Manager and External Platform Services Controller Instances

Site Recovery Manager supports Platform Services Controller HA, a load-balanced pair of Platform Services Controller instances which uses a third-party load balancer. For more information about supported load balancers, see *vCenter HA Deployment Options* in the *vSphere Availability* documentation.

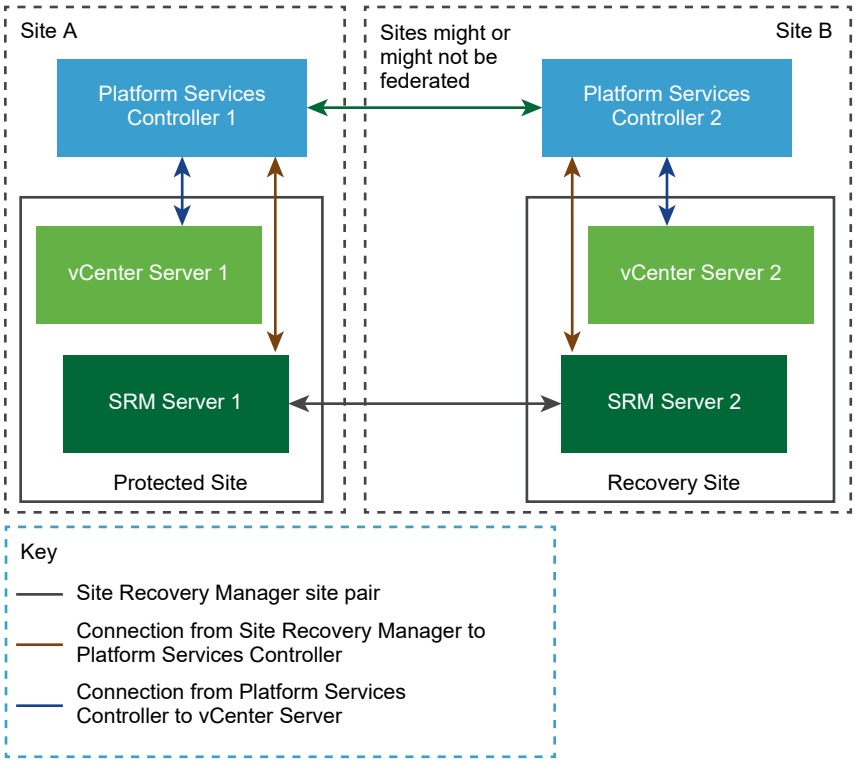
Site Recovery Manager in a Two-Site Topology with One vCenter Server Instance per Platform Services Controller

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

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

The Platform Services Controller instances can belong to vCenter Single Sign-On domains that are either in Enhanced Linked Mode or are not in Enhanced Linked Mode.

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



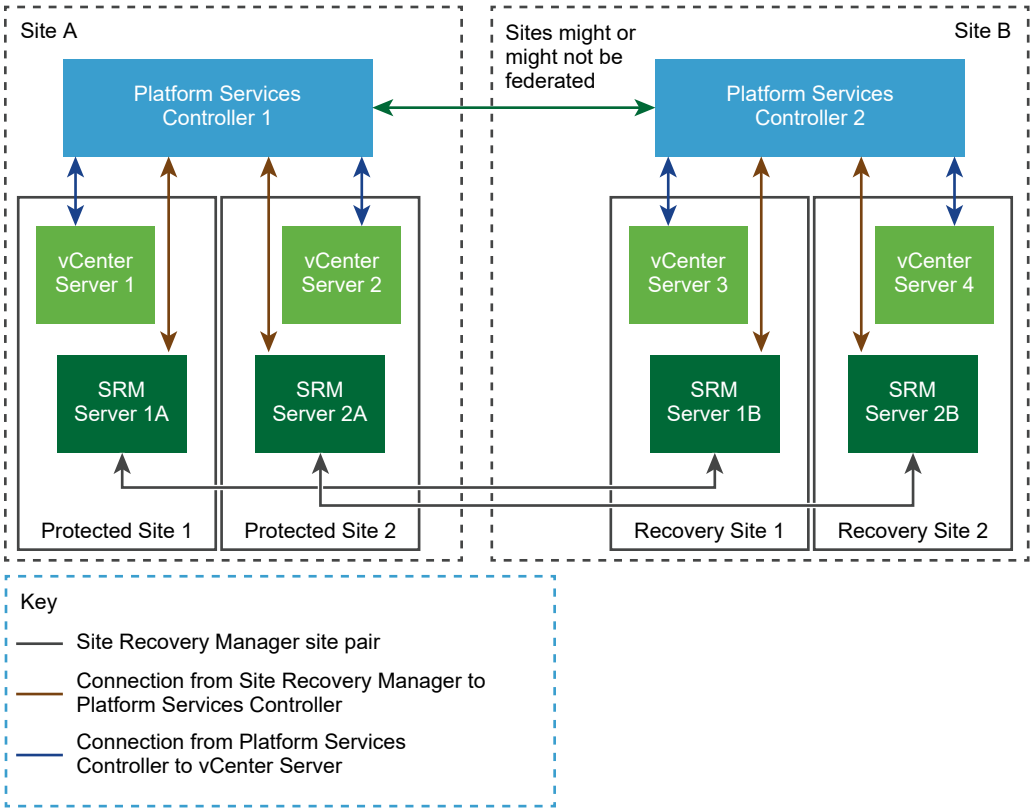
Site Recovery Manager in a Two-Site Topology with Multiple vCenter Server Instances per Platform Services Controller

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

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

The Platform Services Controller instances can belong to vCenter Single Sign-On domains that are either in Enhanced Linked Mode or are not in Enhanced Linked Mode.

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



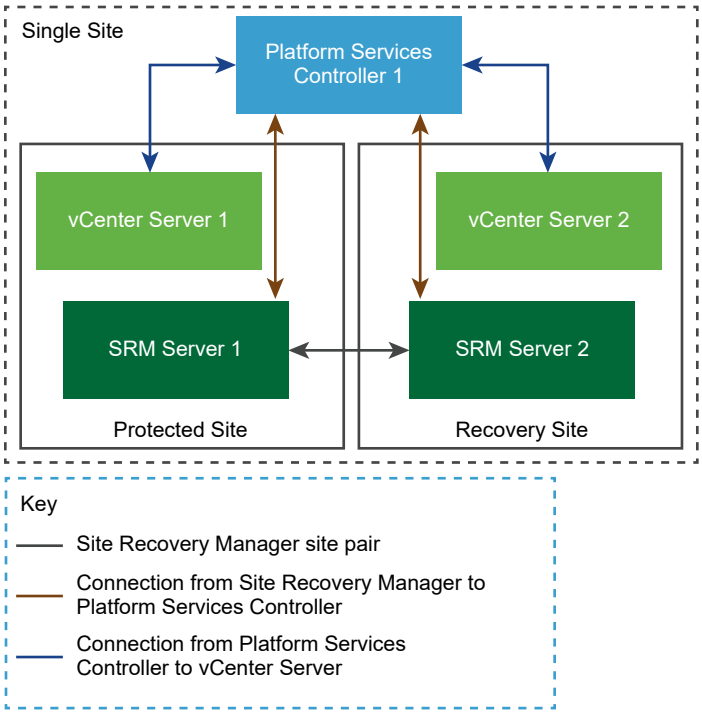
Site Recovery Manager in a Single Site Topology with a Shared Platform Services Controller

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

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

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

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



Prerequisites and Best Practices for Site Recovery Manager Server Deployment

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

- Install the appropriate version of Platform Services Controller and vCenter Server on both sites. For information about compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.5* at https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.
- When you install and configure Platform Services Controller, vCenter Server, and vSphere Replication, use fully qualified domain names (FQDN) whenever possible rather than IP addresses. Using FQDN rather than IP addresses allows you to change the vSphere infrastructure, for example by using DHCP, without having to redeploy or reconfigure Site Recovery Manager. You must also use FQDN if you use custom certificates, because most certificate authorities do not accept certificates that use IP addresses for the SAN or CN value.
- The way in which you deploy Platform Services Controller, vCenter Server, and vCenter Single Sign-On on a site affects how you deploy Site Recovery Manager. For information about how the vCenter Server deployment model affects Site Recovery Manager, see Site Recovery Manager and vCenter Server Deployment Models.

- Obtain the address of the Platform Services Controller instance for both sites. The Platform Services Controller must be running and accessible during Site Recovery Manager installation.
- Synchronize the clock settings of the systems on which Platform Services Controller, vCenter Server, and Site Recovery Manager Server run. To avoid conflicts in the time management across these systems, use a persistent synchronization agent such as network time protocol daemon (NTPD), W32Time, or VMware Tools time synchronization. If you run Platform Services Controller, vCenter Server, and Site Recovery Manager Server in virtual machines, set up NTP time synchronization on the ESXi host on which the virtual machines run. For information about timekeeping best practices, see http://kb.vmware.com/kb/1318.
- Obtain the vCenter Single Sign-On administrator user name and password for both of the local and remote sites.
- If you use custom certificates, obtain an appropriate certificate file. See Requirements When Using Custom SSL/TLS Certificates With Site Recovery Manager.
- If you configure Site Recovery Manager in an IPv6 network, verify that the IPv6 address of the Site Recovery Manager Server, vCenter Server, the ESXi hosts, and the external database, if used, are mapped to fully qualified domain names on the DNS server. Deploy the Site Recovery Manager Server using FQDN and use only FQDNs, not static IPv6 addresses, for all connections.
- To use Site Recovery Manager with vSphere Replication, deploy the appropriate version of vSphere Replication on both of the protected and recovery sites before you deploy Site Recovery Manager Server. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Client to stop working. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.5* at https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.
- If you cannot upgrade an existing incompatible version of vSphere Replication, you must unregister vSphere Replication from both vCenter Server instances before you deploy Site Recovery Manager. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Client to stop working. See Unregister an Incompatible Version of vSphere Replication.

Deploy the Site Recovery Manager Virtual Appliance

To run Site Recovery Manager and its associated services on the preconfigured Site Recovery Manager Appliance, you deploy the appliance both at the protected and at the recovery site.

Prerequisites

If you are not deploying the appliance from an online URL, download the Site Recovery Manager ISO image and mount it on a system in your environment.

Procedure

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

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

3 Provide the location of the OVF file from which to deploy the Site Recovery Manager Appliance, and click **Next**.

Option	Description
Online URL	Select **URL** and provide the URL to deploy the appliance from an online URL.
Downloadable ISO file	a Select **Local file > Browse**, and navigate to the `\bin` directory in the ISO image. b Select the `srm-va_OVF10.ovf`, `srm-va-system.vmdk`, `srm-va-support.vmdk`, `srm-va_OVF10.cert`, and `srm-va_OVF10.mf` files.

4 Enter the name for the virtual appliance or accept the default, select, or search for a destination folder or data center for the appliance, and click **Next**.

The name must be unique within each vCenter Server virtual machine folder.

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

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

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

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

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

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

Site Recovery Manager supports both DHCP and static IP addresses. You can also change the network settings by using the appliance management interface after installation.

11 On the **Customize template** page, select an option for the Site Recovery Manager Appliance hostname.

Option	Description
Leave the text box blank	The DNS server on your network performs reverse lookup of the host name, or the Site Recovery Manager Appliance is registered with its IP address as its host name.
Enter a host name	Depending on your network settings, select one of the following options: ■ If you have assigned a static IP address to the appliance, enter an FQDN for that IP. ■ If you do not use a DNS server, enter a host name that you have already mapped to an IP address in your network.

12 (Optional) To enable the SSHD service of the appliance, select the **Enable SSHD** check box.

13 Set the admin, database, and root user passwords, and click **Next**.

Setting	Action
Initial admin user password	Set the password for the **admin** user account, which you use for access to the Site Recovery Manager Appliance Management Interface and for an SSH access to the appliance OS.
Initial database password	Set the password for the **srmdb** database account, which you use to connect to the embedded vPostgres database.
Initial root password	Set the password for the **root** account, which you use to log in to the OS of the virtual appliance.
NTP Servers	Enter one or more NTP server host names or IP addresses.

Note The admin, database, and root user passwords must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.

14 (Optional) To check the integrity of the Site Recovery Manager Appliance binary files, select the **File Integrity Flag** check box.

If the Site Recovery Manager Appliance detects changes to the binary files, it sends log traces to the syslog.

15 (Optional) To enable VMware HCX support, select the **HCX Flag** check box.

If you integrate Site Recovery Manager with HCX, you cannot use vSphere Replication in the same Site Recovery Manager instance.

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

The Site Recovery Manager Appliance is deployed.

17 Power on the Site Recovery Manager Appliance.

18 Take a note of the IP address of the appliance and log out of the vSphere Web Client or the vSphere Client.

19 To deploy Site Recovery Manager on the recovery site, repeat the procedure.

What to do next

Configure the Site Recovery Manager Appliance instances to connect to vCenter Server at both the protected and the recovery site.

Log In to the VMware Site Recovery Manager Appliance Management Interface

To access the Site Recovery Manager Appliance configuration settings, you must log in to the Site Recovery Manager Appliance Management Interface using the admin account.

Prerequisites

Deploy the Site Recovery Manager Virtual Appliance and power it on.

Procedure

1. In a web browser, go to the Site Recovery Manager Appliance Management Interface at https://*appliance-IP-address-or-FQDN*.
2. Click **Launch SRM Appliance Management**.
3. Log in as admin.

   The default password is the admin user account password that you set during the deployment of the Site Recovery Manager Appliance.

Configure the Site Recovery Manager Appliance to Connect to a vCenter Server

To start protecting virtual machines, you must configure the Site Recovery Manager Appliance to connect to a vCenter Server instance on both the protected and the recovery sites.

Prerequisites

Deploy the Site Recovery Manager Virtual Appliance and power it on.

Procedure

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click the **Summary** tab, and click **Configure appliance**.
3. On the **Platform Services Controller** page, enter the information about the site where you deployed the Site Recovery Manager Appliance.

Menu Item	Description
PSC host name	Enter the host name (in lowercase letters) or IP address of the Platform Services Controller for the vCenter Server with which to register Site Recovery Manager.
PSC port	Accept the default value of `443`, or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS.
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the Platform Services Controller instance.
Password	The password for the specified vCenter Single Sign-On user name.

4 If prompted, click **Connect** to verify the Platform Services Controller certificate.

5 On the **vCenter Server** page, select the vCenter Server instance with which to register the Site Recovery Manager Appliance, and click **Next**.

Caution The drop-down menu includes all the vCenter Server instances that are registered with the Platform Services Controller. In an environment that uses Enhanced Linked Mode, it might also include vCenter Server instances from other Platform Services Controller instances. Make sure that you select the correct vCenter Server instance. After you configure the Site Recovery Manager Appliance, you cannot select a different vCenter Server instance.

6 On the **Name and Extension** page, enter the necessary information to register the Site Recovery Manager with vCenter Server, and select the default Site Recovery Manager extension identifier, or create a custom extension identifier.

a Enter the site name, administrator email address, and local host IP address or name.

Menu Item	Description
Site name	A name for this Site Recovery Manager site, which appears in the Site Recovery Manager interface. The vCenter Server address is used by default. Use a different name for each Site Recovery Manager instance in the pair.
Administrator email	The email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.
Local host	The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the Site Recovery Manager Appliance detects is not the interface that you want to use. **Note** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

b Select the default Site Recovery Manager extension identifier, or create a custom extension ID for this Site Recovery Manager pair, and click **Next**.

Both Site Recovery Manager instances in a site pair must use the same extension ID.

Menu Item	Description
Default extension ID	Use this option when you deploy Site Recovery Manager in a standard configuration with one protected site and one recovery site.
Custom extension ID	Use this option when you deploy Site Recovery Manager in a shared recovery site configuration, with multiple protected sites and one recovery site. Enter the details for the custom extension ID. ■ Extension ID. A unique identifier. Assign the same identifier to the Site Recovery Manager instances on the protected site and the shared recovery site. ■ Organization. The name of the organization to which this Site Recovery Manager sites

Menu Item	Description
	pair belongs. This name helps to identify Site Recovery Manager pairs in a shared recovery site configuration, especially when multiple organizations use the shared recovery site. ■ Description. An optional description of the Site Recovery Manager pair.

7 On the **Ready to Complete** page, review your settings and click **Finish**.

8 To configure the Site Recovery Manager Appliance on the other site, repeat the procedure.

Connect to the Site Recovery Manager Appliance Embedded vPostgres Database

If you need to access the content in the Site Recovery Manager Appliance embedded vPostgres database, you must connect to the database through the appliance OS.

Procedure

1 Log in to the OS of the Site Recovery Manager Appliance as admin.

You set the password for the **admin** user account during the deployment of the appliance.

2 Run `/opt/vmware/vpostgres/current/bin/psql –U user –d dbname`. Enter a user name, the database name, and when prompted the respective password which you set during the deployment of the Site Recovery Manager Appliance.

User	Description
admin	The embedded vPostgres database super user account. **Note** The **admin** account uses the same password to access both the appliance OS and the embedded database.
srmdb	The embedded vPostgres database user account. Site Recovery Manager Server uses this account to access the embedded vPostgres database.

How to Set Up a Trusted Environment for the Site Recovery Manager Virtual Appliance

To set up a trusted environment with your custom root CA certificates, you must manually import the certificates into the Site Recovery Manager Virtual Appliance .

The certificates must be in a `.pem` format.

Procedure

1 Log in to the Site Recovery Manager Virtual Appliance host machine as admin.

2 Run the following command.

```
su
```

3 Enter the root password.

4 Copy the certificates to `/etc/ssl/certs`.

5 To modify the certificates' permissions, run the following command.

```
chmod a+r <new-root-ca>.pem
```

6 Run `c_rehash`.

7 To import the Site Recovery Manager Server certificates, use the Site Recovery Manager Appliance Management Interface.

a Log in to the Site Recovery Manager Appliance Management Interface as admin.

b Click the **Access** tab, and then, in the **Certificate** pane, click **Change**.

c Select a certificate type.

Menu item	Description
Generate a self-signed certificate.	Use an automatically generated certificate. 1 Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company. 2 Accept the default FQDN and IP values. **Note** Using a self-signed certificate is not recommended for production environments.
Use a PKCS #12 certificate file.	Use a custom certificate. 1 Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. 2 (Optional) Enter the optional private key encryption password.
Use a CA-signed certificate generated from CSR.	Use a CA-signed certificate generated from a CSR. 1 In the **Certificate file** row, click **Browse**, navigate to the certificate file, and click **Open**. 2 (Optional) In the **CA chain** row, click **Browse**, navigate to the CA chain, and click **Open**.

d Click **Change**.

8 To import the Site Recovery HTML 5 client trust certificate in the JRE keystore, run the following command.

```
keytool -importcert -v -noprompt -file root.pem -alias root-ca -keystore /usr/java/jre-vmware/lib/security/cacerts -storepass changeit
```

Use the VMware OVF Tool to Deploy the Site Recovery Manager Virtual Appliance Virtual Machine from a Client OVF Template

You can use the VMware OVF Tool to deploy the Site Recovery Manager Virtual Appliance virtual machine from a client OVF template.

VMware OVF Tool (`ovftool`) is a flexible command-line utility that you can use to import and export OVF packages to and from a wide variety of VMware products. For more information about the `ovftool`, see the VMware OVF Tool documentation.

Prerequisites

Verify that you have downloaded and installed VMware OVF Tool 4.2 or later.

Procedure

- To deploy the Site Recovery Manager Virtual Appliance with the VMware OVF Tool, use one the following command lines.

  a If you want to obtain network settings through DHCP:

```
ovftool
  --acceptAllEulas
  --ipAllocationPolicy=dhcpPolicy
  --ipProtocol=IPv4
  --deploymentOption=light | standard
  --name=SRM-VA-NAME
  --datastore=DATASTORE-NAME
  --network=NETWORK-NAME
  --net:"Network 1"=NETWORK-NAME
  --prop:varoot-password=ROOT-PASSWORD
  --prop:vaadmin-password=ADMIN-PASSWORD
  --prop:dbpassword=DB-PASSWORD
  --prop:ntpserver=NTP-SERVER
  --prop:network.netmode.VMware_Site_Recovery_Manager_Appliance='dhcp'
  --prop:network.addrfamily.VMware_Site_Recovery_Manager_Appliance='ipv4'
  http://HOST/PATH/srm-va_OVF10.ovf
  vi://VC_USERNAME:VC_PASSWORD@VC_ADDRESS/DATACENTER-NAME/host/CLUSTER-NAME/Resources/
RESOURCE-POOL-NAME
```

  b If you want to obtain network settings through a static IP address:

```
ovftool
  --acceptAllEulas
  --ipAllocationPolicy=dhcpPolicy
  --ipProtocol=IPv4
  --deploymentOption=light | standard
  --name=SRM-VA-NAME
  --datastore=DATASTORE-NAME
  --network=NETWORK-NAME
  --net:"Network 1"=NETWORK-NAME
  --prop:varoot-password=ROOT-PASSWORD
  --prop:vaadmin-password=ADMIN-PASSWORD
  --prop:dbpassword=DB-PASSWORD
  --prop:ntpserver=NTP-SERVER
  --prop:"network.ip0.VMware_Site_Recovery_Manager_Appliance"="VA IP"
  --prop:"network.netprefix0.VMware_Site_Recovery_Manager_Appliance"="NETWORK PREFIX"
  --prop:"network.gateway.VMware_Site_Recovery_Manager_Appliance"="GATEWAY IP"
  --prop:"network.DNS.VMware_Site_Recovery_Manager_Appliance"="DNS SERVER 1, DNS
SERVER 2"
  --prop:"network.searchpath.VMware_Site_Recovery_Manager_Appliance"="DNS SEARCH PATH
- DOMAIN"
  --prop:"network.netmode.VMware_Site_Recovery_Manager_Appliance"='static'
  --ipAllocationPolicy="fixedPolicy"
  --prop:network.addrfamily.VMware_Site_Recovery_Manager_Appliance='ipv4'
  http://HOST/PATH/srm-va_OVF10.ovf
  vi://VC_USERNAME:VC_PASSWORD@VC_ADDRESS/DATACENTER-NAME/host/CLUSTER-NAME/Resources/
RESOURCE-POOL-NAME
```

You must replace the variables in the example with values from your environment.

Variable	Description
light | *standard*	The deployment type for the Site Recovery Manager Appliance virtual machine. Use the light deployment type for deployments that protect less than 1000 virtual machines. Use the standard deployment type for deployments that protect more than 1000 virtual machines.
SRM-VA-NAME	The name of the Site Recovery Manager Appliance virtual machine.
DATASTORE-NAME	The target datastore name.
NETWORK-NAME	The name of the target network.
ROOT-PASSWORD	The password for the **`root`** account, which you use to log in to the OS of the virtual appliance. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
ADMIN-PASSWORD	The password for the **`admin`** user account, which you use for access to the Site Recovery Manager Appliance Management Interface and for SSH access to the appliance OS. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
DB-PASSWORD	The password for the **`srmdb`** database account, which you use to connect to the embedded vPostgres database. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
NTP-SERVER	The NTP server host name.
HOST	The host address of the source virtual machine.
PATH	The path to the OVF package.
NETWORK PREFIX	The network prefix of the Site Recovery Manager Appliance.
DNS SEARCH PATH - DOMAIN	The domain search path for this virtual machine (use a comma or a space to separate the different names).
GATEWAY IP ADDRESS	The Gateway address of the Site Recovery Manager Appliance.
VA IP	The IP address of the Site Recovery Manager Appliance virtual machine.
DNS IP ADDRESS	The DNS address of the Site Recovery Manager Appliance .
VC_USERNAME	The user name for the target vCenter Server.

Variable	Description
VC_PASSWORD	The password for the target vCenter Server.
VC_ADDRESS	The address of the target vCenter Server.
DATACENTER-NAME	The name of the target data center.
CLUSTER-NAME	The name of the target cluster.
RESOURCE-POOL-NAME	The name of the target resource pool.

What to do next

Configure the Site Recovery Manager Appliance to Connect to a vCenter Server at both the protected and the recovery site.

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

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

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.

Prerequisites

- Verify that you installed Site Recovery Manager Server instances at the protected and recovery sites.
- If you did not select the default plug-in ID when you installed Site Recovery Manager Server, you must have assigned the same custom plug-in ID to the Site Recovery Manager Server instances on each of the sites.

Procedure

1. In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select a local vCenter Server from the list, select a pair type, and click **Next**.
   - Pair with a peer vCenter Server located in a different Single Sign-On domain
   - Pair with a peer vCenter Server located in the same Single Sign-On domain

4 Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Find vCenter Server Instances**.

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

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

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

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

Results

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

Reconnect a Site Pair and Breaking a Site Pair

You can reconfigure or break an existing site pair.

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

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

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

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

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

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

Prerequisites

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

Procedure

1. Connect to the vSphere Client or the vSphere Web Client on one of the sites, and select **Site Recovery > Open Site Recovery**.
2. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
3. Enter the vCenter Single Sign-On user name and password for the remote site, and click **Log in**.

Install the Site Recovery Manager License Key

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

Prerequisites

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

Procedure

1. Log in to the vSphere Client.
2. Click **Menu > Administration**.
3. Expand **Licensing** and click **Licenses**.
4. On the **Assests** tab, click the **Solutions** tab.
5. Select the vCenter Server instance on which Site Recovery Manager is installed.
6. Click **Assign License**.
7. In the **Assign License** dialog box, click **New License** tab.
8. In the **Assign License** dialog box, type or copy and paste a license key and click **OK**.
9. Enter a name for the new license and click **OK**.

   Details about the product, product features, capacity, and expiration period appear on the page.
10. Click **OK**.
11. In the **Assign License** dialog box, select the newly created license, and click **OK**.
12. Repeat the steps to assign Site Recovery Manager license keys to all appropriate vCenter Server instances.

Unregister an Incompatible Version of vSphere Replication

Site Recovery Manager requires the corresponding version of vSphere Replication. The Site Recovery Manager installer verifies the version of vSphere Replication and stops if it detects an incompatible version.

Problem

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

Cause

vSphere Web Client stops working, if you install an incompatible version of vSphere Replication after you have installed Site Recovery Manager.

Solution

If you installed an incompatible version of vSphere Replication after you deployed this version of Site Recovery Manager, you must upgrade vSphere Replication to the correct version.

For information about the compatible versions of vSphere Replication, see https://interopmatrix.vmware.com/#/Interoperability.

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

Reconfiguring the Site Recovery Manager Virtual Appliance

7

If necessary, you can reconfigure the Site Recovery Manager Virtual Appliance settings by using the Site Recovery Manager Appliance Management Interface.

- Reconfigure the Site Recovery Manager Appliance

  You reconfigure the Site Recovery Manager virtual appliance settings by using the Site Recovery Manager Virtual Appliance Management Interface.

- Change the Site Recovery Manager Appliance Hostname

  To change the Site Recovery Manager appliance hostname, you use the Site Recovery Manager Appliance Management Interface .

- Configure the Time Zone and Time Synchronization Settings for the Site Recovery Manager Appliance

  When you deploy the Site Recovery Manager Appliance, you either use the time settings of the ESXi host on which the appliance is running, or you configure time synchronization with an NTP server. If the time settings in your network change, you can edit the time zone and time synchronization settings of the appliance.

- Start, Stop, and Restart Site Recovery Manager Appliance Services

  If changes in your environment require the restart of certain services, you can use the Site Recovery Manager Appliance Management Interface to view the state of the services and to start, stop, and restart them.

- Configure the Site Recovery Manager Appliance Network Settings

  You can use the Site Recovery Manager Appliance Management Interface to customize the network settings of the appliance for privacy, speed, or security reasons.

- Change the Site Recovery Manager Appliance Certificate

  You can use the Site Recovery Manager Appliance Management Interface to change the appliance certificate for security reasons or if your certificate is expiring.

- Add or Delete Additional Certificates

  You use the Site Recovery Manager Appliance Management Interface to add or delete additional intermediate and root certificates.

- Change the Site Recovery Manager Appliance Password

  You use the Site Recovery Manager Appliance Management Interface to change the appliance password and the database password.

- Activate or Deactivate SSH Access to the Site Recovery Manager Appliance

  You can use the Site Recovery Manager Appliance Management Interface to edit the appliance SSH access settings.

- Forward Site Recovery Manager Appliance Log Files to Remote Syslog Server

  You can forward the Site Recovery Manager Appliance log files to a remote syslog server to conduct an analysis of your logs.

- Reconfigure the Connection Between Sites

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

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

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

- Rename a Site Recovery Manager Site

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

- Unregister the Site Recovery Manager Appliance

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

- Clean up the vCenter Lookup Service

  Use the Managed Object Browser (MOB) to clean up the old Site Recovery Manager registration in Lookup Service after deleting the Site Recovery Manager Appliance.

Reconfigure the Site Recovery Manager Appliance

You reconfigure the Site Recovery Manager virtual appliance settings by using the Site Recovery Manager Virtual Appliance Management Interface.

Deploying the Site Recovery Manager Server binds the instance to a number of values that you supply, including the vCenter Server instance to extend, DSN and credentials, the certificate, and so on. You can change some of the values from the Site Recovery Manager Virtual Appliance Management Interface.

Procedure

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click **Summary**, and click **Reconfigure**.

3 On the **Platform Services Controller** page, enter the information about the site where you deployed the Site Recovery Manager Appliance.

Menu Item	Description
PSC host name	Enter the host name (in lowercase letters) or IP address of the Platform Services Controller for the vCenter Server with which to register Site Recovery Manager.
PSC port	Accept the default value of `443`, or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS.
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the Platform Services Controller instance.
Password	The password for the specified vCenter Single Sign-On user name.

4 If prompted, click **Connect** to verify the Platform Services Controller certificate.

5 On the **vCenter Server** page, click **Next**.

After the initial configuration of the Site Recovery Manager Appliance, you cannot select a different vCenter Server instance.

6 On the **Name and Extension** page, enter the site name, administrator email address, and local host IP address or name, to register the Site Recovery Manager with vCenter Server.

Menu Item	Description
Site name	A name for this Site Recovery Manager site, which appears in the Site Recovery Manager interface. The vCenter Server address is used by default. Use a different name for each Site Recovery Manager instance in the pair.
Administrator email	The email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.
Local host	The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the Site Recovery Manager Appliance detects is not the interface that you want to use. **Note** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

7 On the **Ready to Complete** page, review your settings and click **Finish**.

8 To configure the Site Recovery Manager Appliance on the other site, repeat the procedure.

What to do next

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

Change the Site Recovery Manager Appliance Hostname

To change the Site Recovery Manager appliance hostname, you use the Site Recovery Manager Appliance Management Interface .

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click **Networking** and then click **Edit**.

3 Change the hostname and if necessary the IP address of the Site Recovery Manager virtual appliance.

4 Close the browser and open it again to clear the old session.

5 Log in to the Site Recovery Manager Appliance Management Interface with the new hostname as admin.

6 To change the certificate with the new hostname information, click **Certificate** and then click **Change**.

7 Close the browser and open it again to clear the old session.

8 Log in to the Site Recovery Manager Appliance Management Interface with the new hostname as admin.

9 To reconfigure the Site Recovery Manager Appliance with the new hostname, click **Summary**, then click **Reconfigure**, and complete the wizard.

10 Close the Site Recovery Manager Appliance Management Interface and open the Site Recovery User Interface.

11 On the **Site Recovery** home tab, select the site pair, click **View Details**, and verify the connection status.

12 (Optional) If the sites are not connected, click **Reconnect** and provide the required credentials.

What to do next

Verify the status of all protections groups and recovery plans.

Configure the Time Zone and Time Synchronization Settings for the Site Recovery Manager Appliance

When you deploy the Site Recovery Manager Appliance, you either use the time settings of the ESXi host on which the appliance is running, or you configure time synchronization with an NTP server. If the time settings in your network change, you can edit the time zone and time synchronization settings of the appliance.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click the **Time** tab.

3 Configure Site Recovery Manager Appliance time zone settings.

   a On the **Time zone** pane, click **Edit**.

   b From the **Time zone** drop-down menu, select a location or a time zone and click **Save**.

4 On the **Time synchronization** pane, click **Edit**.

5 Configure the time synchronization settings and click **Save**.

Mode	Description
Disabled	No time synchronization. Uses the system time zone settings.
Host	Uses VMware Tools to synchronize the time of the appliance with the time of the ESXi host.
NTP	Enables NTP synchronization. You must enter the IP address or FQDN of one or more NTP servers.

Start, Stop, and Restart Site Recovery Manager Appliance Services

If changes in your environment require the restart of certain services, you can use the Site Recovery Manager Appliance Management Interface to view the state of the services and to start, stop, and restart them.

You can start, stop, and restart the Site Recovery Manager Server service, the embedded database service, and the `dr-client` service.

Procedure

1 Log in to the Site Recovery Manager Appliance Management as admin.

2 In the Site Recovery Manager Appliance Management Interface, click **Services**.

The Services page displays a table of the installed services that can be sorted by name, startup type, and state.

3 Select a service and click **Start**, **Stop**, or **Restart**, then click **OK**.

Restarting some services might lead to functionality becoming temporarily unavailable.

4 Restart the appliance for the changes to take effect.

Configure the Site Recovery Manager Appliance Network Settings

You can use the Site Recovery Manager Appliance Management Interface to customize the network settings of the appliance for privacy, speed, or security reasons.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click **Networking**.

3 To configure your network settings, click **Edit**.

4 Configure the DNS settings in the **Hostname and DNS** pane.

Menu Item	Description
Obtain DNS settings automatically	Obtains the DNS settings automatically from the network.
Enter DNS settings manually	Uses the DNS address settings that you set manually. If you select this option, you must provide the IP addresses for a primary and a secondary DNS server.

5 In the **eth0** pane, select the IPv4 or theIPv6 protocol type and configure the IP address settings.

- Configure the IPv4 address settings.

Option	Description
Obtain IPv4 settings automatically	Obtains the IP address for the appliance from the network.
Enter IPv4 settings manually	Uses an IPv4 address that you set manually. 1 Enter the IPv4 address 2 Enter subnet prefix length. 3 Enter the default IPv4 gateway.

- Configure the IPv6 address settings.

Option	Description
Obtain IPv6 settings automatically using DHCP	Assigns IPv6 addresses to the appliance from the network by using DHCP. **Note** To apply this setting, you must restart the Site Recovery Manager Appliance.
Obtain IPv6 settings automatically using router advertisement	Assigns IPv6 addresses to the appliance from the network by using router advertisement.
Use static IPv6 addresses	Uses static IPv6 addresses that you set up manually. 1 Enter the IPv6 address and the subnet prefix length in the address box. 2 To enter additional IPv6 addresses, click **Add**. 3 Enter the default IPv6 gateway.

6 Click **Save**.

7 (Optional) If you change the IP address of the Site Recovery Manager Appliance, you must first reconfigure the Site Recovery Manager Appliance, then change the certificate, and then reconfigure the Site Recovery Manager Appliance again to register the new certificate into the vCenter Server Platform Services Controller.

a Log in to the Site Recovery Manager Appliance Management Interface as admin.

b Click the **Summary** tab, click **Configure appliance**, and complete the wizard.

c Click the **Access** tab, and then, in the **Certificate** pane, click **Change**.

d Select a certificate type, and click **Change**.

e Click the **Summary** tab, click **Configure appliance**, and complete the wizard.

Change the Site Recovery Manager Appliance Certificate

You can use the Site Recovery Manager Appliance Management Interface to change the appliance certificate for security reasons or if your certificate is expiring.

The certificate must be in a `.pem` format.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click **Certificates** and then click **Change**.

3 Select a certificate type.

Menu item	Description
Generate a self-signed certificate	Use an automatically generated certificate. a Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company. b Accept the default FQDN and IP values. **Note** Using a self-signed certificate is only recommended for non-production environments.
Use a PKCS #12 certificate file	Use a custom certificate. a Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. b (Optional) Enter the optional private key encryption password.
Use a CA-signed certificate generated from CSR	Use a CA-signed certificate generated from a CSR. a In the **Certificate file** row, click **Browse**, navigate to the certificate file, and click **Open**. b (Optional) In the **CA chain** row, click **Browse**, navigate to the CA chain, and click **Open**.

4 Click **Change**.

Generate and Download a Certificate Signing Request for the Site Recovery Manager Appliance

A certificate signing request (CSR) is an encrypted text file that contains specific information, such as organization name, common name, locality, and country. You send the CSR file to a certificate authority (CA) to apply for a digital identity certificate.

You generate a CSR and a matching private key. The private key remains on the Site Recovery Manager Appliance.

Attention Generating a new private key invalidates any existing CSR configuration.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click the **Access** tab.

3 In the **Certificate** pane, click **Generate CSR**.

4 Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company.

5 Accept the default FQDN and IP values and click **Generate and download**.

What to do next

To submit a certificate request to the CA in accordance with the CA enrollment process, use the contents of the CSR file.

The CA creates a server certificate based on the information in the CSR file, signs it with its private key, and sends you the certificate, which you can then import to the Site Recovery Manager Appliance.

Add or Delete Additional Certificates

You use the Site Recovery Manager Appliance Management Interface to add or delete additional intermediate and root certificates.

The certificate must be in a `.pem` format.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click **Certificates**, and then click the **Intermediate** or the **Root** tab.

3 Click **Add**, insert the certificate, and then click **Add**.

4 (Optional) To delete a certificate, select the certificate, and click **Delete**.

Change the Site Recovery Manager Appliance Password

You use the Site Recovery Manager Appliance Management Interface to change the appliance password and the database password.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click **Access**, and change the password from the **Password** pane.

Option	Description
SRM appliance password	Use this option to change the password for the **admin** account.
Embedded database password	Use this option to change the password for the embedded database.

3 Click **Change**, provide the necessary information, and click **Change** again.

Activate or Deactivate SSH Access to the Site Recovery Manager Appliance

You can use the Site Recovery Manager Appliance Management Interface to edit the appliance SSH access settings.

You can activate or deactivate an SSH access to the appliance only for the **admin** account.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click **Access**.

3 In the **SSH** pane, click **Enable** or **Disable**.

Forward Site Recovery Manager Appliance Log Files to Remote Syslog Server

You can forward the Site Recovery Manager Appliance log files to a remote syslog server to conduct an analysis of your logs.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 In the Site Recovery Manager Appliance Management Interface, select **Syslog Forwarding**.

3 Click **New**, and enter the server address of the destination host in the **New Syslog Forwarding** pane.

4 From the **Protocol** drop-down menu, select the protocol to use.

5 In the **Port** text box, enter the port number to use with the destination host.

The default port number is **514**.

6 Click **OK**.

7 Verify that the remote syslog server is receiving messages.

8 In the **Syslog Forwarding** section, click **Send Test Message**.

9 Verify that the test message is received on the remote syslog server.

Reconfigure the Connection Between Sites

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

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

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

Procedure

1. In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
3. Select **Site Pair > Summary**, and click **Reconnect**.

   You can initiate the reconnect from either site, even if you only changed the installation on one of the sites.
4. Select the services you want to pair. Enter the address of the Platform Services Controller on the remote site, provide the vCenter Single Sign-On username and password, and click **Reconnect**.

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

Break the Site Pairing and Connect to a New Remote Site

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

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

Prerequisites

- You have an existing Site Recovery Manager installation with two connected sites.

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

Procedure

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

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

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

   You cannot delete recovery plans that are running.

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

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

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

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

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

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

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

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

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

9 (Optional) If you use array-based replication, select **Configure > Array Based Replication > Array Pairs**, and remove all array pairs.

   a Select an array pair, click **Array Pair**, and click **Disable**.

   b Click **Array Manager Pair** and click **Remove**.

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

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

Results

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

What to do next

- Install a new Site Recovery Manager instance on the new remote site. For instructions about installing Site Recovery Manager, see Deploy the Site Recovery Manager Virtual Appliance.

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

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

Rename a Site Recovery Manager Site

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

Procedure

1. In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
3. Click **Site Pair > Summary**, and in the Site Recovery Manager box click **Rename** next to the name of the site you want to rename.
4. Enter a new name for the site and click **Save**.

Unregister the Site Recovery Manager Appliance

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

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

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

Procedure

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

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

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

   You cannot delete recovery plans that are running.

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

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

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

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

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

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

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

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

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

9 (Optional) If you use array-based replication, select **Configure > Array Based Replication > Array Pairs**, and remove all array pairs.

   a Select an array pair, click **Array Pair**, and click **Disable**.

   b Click **Array Manager Pair** and click **Remove**.

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

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

11 Log in to the Site Recovery Manager Appliance Management Interface as admin.

12 Click **Summary**, and click **Unregister**.

13 Provide the required credentials, review the information, and click **Unregister**.

Important Unregistering the Site Recovery Manager Appliance deletes the embedded database. This process cannot be reversed.

14 Repeat the procedure on the other site.

Clean up the vCenter Lookup Service

Use the Managed Object Browser (MOB) to clean up the old Site Recovery Manager registration in Lookup Service after deleting the Site Recovery Manager Appliance.

If you delete the Site Recovery Manager Appliance before you unregister it from the environment, you cannot use the Site Recovery Manager virtual appliance management interface (VAMI) to unregister Site Recovery Manager from vCenter Server.

Prerequisites

Verify that you have the credentials of a vSphere administrator.

Procedure

1 Log in with vCenter Server credentials to `https://<vCenter_Server_address>/lookupservice/mob/?moid=ServiceRegistration&method=List&vmodl=1`.

Note If you have an external Platform Services Controller (PSC), use the PSC address instead of the vCenter Server address.

2 To search for the Site Recovery Manager registrations, replace the value in the **Value** field with the following text and click **Invoke Method**.

```
<filterCriteria>
   <serviceType>
      <product>com.vmware.dr</product>
      <type>vcDr</type>
   </serviceType>
</filterCriteria>
```

3 Look for the old Site Recovery Manager registration and copy its **serviceId** value.

4 Navigate to `https://<vCenter_Server_address>/lookupservice/mob/?moid=ServiceRegistration&method=Delete`.

5 To delete the service registration, enter the **serviceId** value and click **Invoke Method**.

Deploying Site Recovery Manager on Azure VMware Solution

8

You can use Site Recovery Manager 8.5.x and vSphere Replication 8.5.x with Azure VMware Solution.

Azure VMware Solution is an infrastructure-as-a-service private cloud offering built on VMware Cloud Foundation stack. It is a service sold and supported by Microsoft, verified by VMware, that runs on Azure infrastructure.

You can use Site Recovery Manager 8.5.x and vSphere Replication 8.5.x to plan, test, and run the recovery of virtual machines between a protected vCenter Server on-premises site and a recovery vCenter Server site on Azure VMware Solution and the reverse, or between two Azure VMware Solution cloud sites.

Procedure

1 Operational Limits of Site Recovery Manager on Azure VMware Solution

Each Site Recovery Manager instance on Azure VMware Solution can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries.

2 Deploy Site Recovery Manager on Azure VMware Solution

This topic explains how to deploy Site Recovery Manager and vSphere Replication on Azure VMware Solution.

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

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

4 How do I connect a Site Recovery Manager instance on an Azure VMware Solution SDDC to a VMware Site Recovery instance in a VMware Cloud on AWS SDDC

This use case provides instructions for connecting a Site Recovery Manager instance on an Azure VMware Solution SDDC site to a VMware Site Recovery instance on a VMware Cloud on AWS SDDC. You must use a VPN connection to access VMware Site Recovery on VMware Cloud on AWS and the Site Recovery Manager instance on Azure VMware Solution.

Operational Limits of Site Recovery Manager on Azure VMware Solution

Each Site Recovery Manager instance on Azure VMware Solution can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries.

Protection and Recovery Maximums for Site Recovery Manager

Table 8-1. Protection and Recovery Maximums for Site Recovery Manager

Item	Maximum
Total number of protected virtual machines per SDDC on Azure VMware Solution	3000 **Note** To achieve the 3000 virtual machines scale, you must manually balance the replications between the different vSphere Replication nodes. Contact Microsoft for the scale up/down of vSphere Replication appliances within Azure VMware Solution. You must manually add additional vSphere Replication servers to your on-premises environment, see Deploying Additional vSphere Replication Servers in the *vSphere Replication Administration* guide.
Maximum number of protected virtual machines per vSphere Replication appliance (through embedded vSphere Replication server).	300
Maximum number of protected virtual machines per vSphere Replication server.	300
Total number of virtual machines per protection group	500
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Total number of virtual machines per recovery plan	2000
Total number of virtual machine recoveries that you can start simultaneously across multiple recovery plans	2000

Bidirectional Protection

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

For example, if you protect 1600 virtual machines using vSphere Replication from site A to site B, you can use vSphere Replication to protect a maximum of 1400 virtual machines from site B to site A. If you are using vSphere Replication for a bidirectional protection, you can protect a maximum of 3000 virtual machines across both sites.

IP Customization Maximums for VMware Site Recovery

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

- 1 IP address
- Subnet information
- 1 gateway server address
- 2 DNS servers (primary and secondary)

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

Recovery Point Objective lower than 15 minutes

For information about Recovery Point Objective (RPO) lower than 15 minutes, see Recovery Point Objective in the *vSphere Replication Administration* guide.

Custom Command Recovery Steps

You cannot run commands on Site Recovery Manager Server on Azure VMware Solution. See Types of Custom Recovery Steps.

Deploy Site Recovery Manager on Azure VMware Solution

This topic explains how to deploy Site Recovery Manager and vSphere Replication on Azure VMware Solution.

Prerequisites

For a cloud to cloud recovery, make sure that the following ports are open: 80, 443, 902, 1433, 1521, 1526, 5480, 8123, 9086, 31031, 32032, 8043, 10000-10010.

Procedure

1. Log in to the Azure portal.
2. Navigate to your subscription **avs-2.*xxx*** and search for **Azure VMware Solution**.
3. Click a private cloud, go to **Manage** and click **Add-ons**.
4. On the right-side pane, click **Start** under **Disaster Recovery**.
5. From the drop-down menu, select **VMware Site Recovery Manager (SRM) - vSphere replication** as a disaster recovery solution.
6. Provide a license key or select to use an evaluation version.
7. Accept the terms and conditions and click **Install**.
8. Once the Site Recovery Manager installation completes, go back to **Manage** and click **Add-ons**.

9 On the right-side pane, click **Start** under **Disaster Recovery**.

10 Go to **Setup replication**. From the drop-down menu, select **vSphere Replication** and click **Install**.

What to do next

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

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

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

Procedure

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

2 Click the **New Site Pair** button.

3 Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.

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

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

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

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

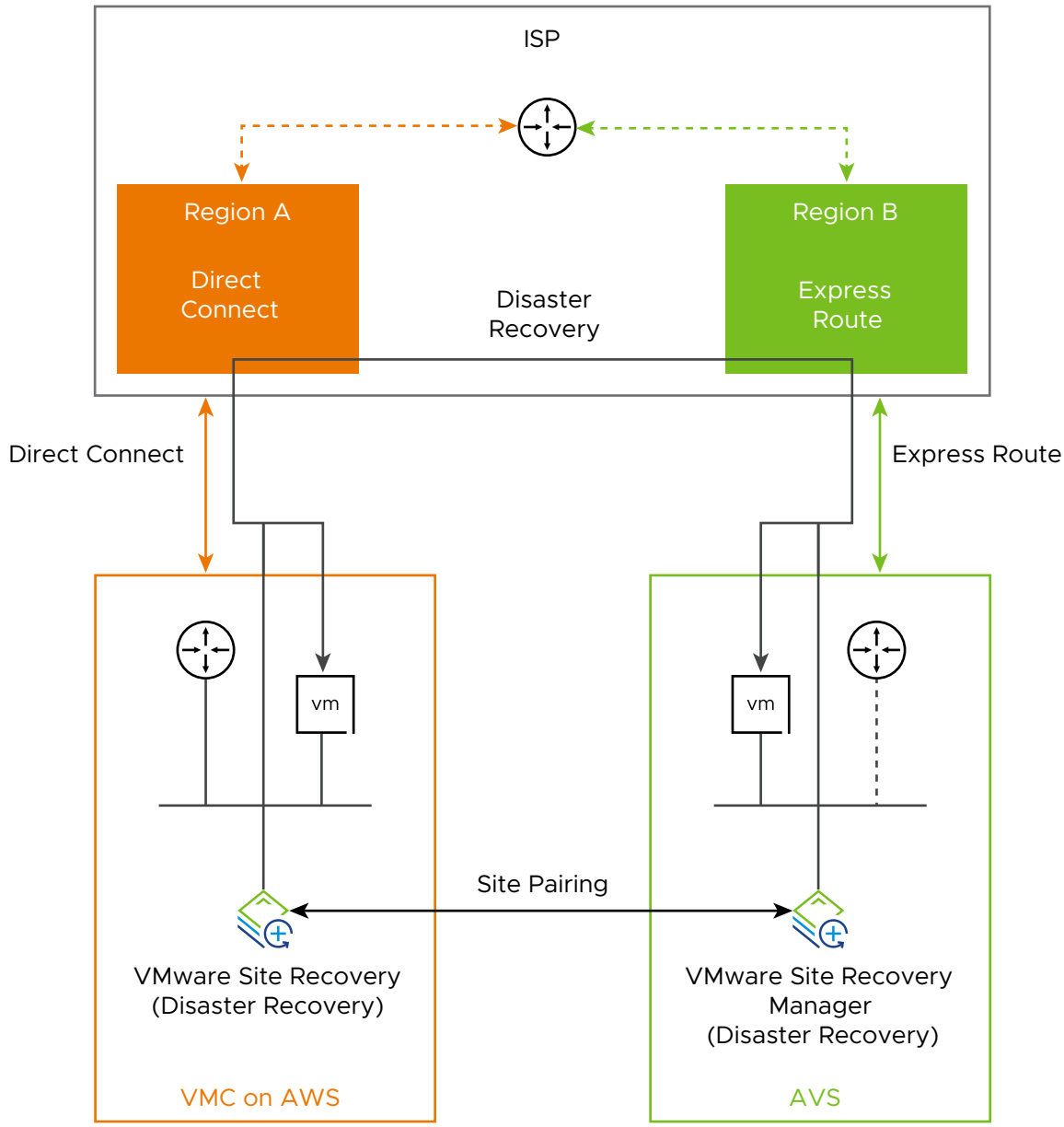
Results

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

How do I connect a Site Recovery Manager instance on an Azure VMware Solution SDDC to a VMware Site Recovery instance in a VMware Cloud on AWS SDDC

This use case provides instructions for connecting a Site Recovery Manager instance on an Azure VMware Solution SDDC site to a VMware Site Recovery instance on a VMware Cloud on AWS SDDC. You must use a VPN connection to access VMware Site Recovery on VMware Cloud on AWS and the Site Recovery Manager instance on Azure VMware Solution.

Figure 8-1. Network connectivity between VMware Site Recovery on VMware Cloud on AWS and VMware Site Recovery Manager on Azure VMware Solution



Prerequisites

Verify that you have deployed Site Recovery Manager and vSphere Replication on Azure VMware Solution. See Deploy Site Recovery Manager on Azure VMware Solution.

Procedure

1 Activate VMware Site Recovery

To use your Site Recovery Manager instance on an Azure VMware Solution SDDC with a VMware Site Recovery service, you must activate the VMware Site Recovery service on a VMware Cloud™ on AWS SDDC.

2 Set the NSX-T Edge Management Gateway Firewall Rules for VMware Site Recovery

   To enable VMware Site Recovery on your SDDC environment that uses VMware NSX-T®, you must create firewall rules between your VMware Cloud on AWS SDDC and the Management Gateway. After the initial firewall rules configuration, you can add, edit or delete any rules as needed.

3 Connect the Site Recovery Manager Server Instances on the Azure VMware Solution SDDC and the VMware Cloud on AWS SDDC

   Before you can protect your virtual machines between an Azure VMware Solution SDDC and a VMware Cloud on AWS SDDC and the reverse, you must connect the Site Recovery Manager Server and vSphere Replication instances on the protected and the recovery sites. This procedure is known as site pairing.

Activate VMware Site Recovery

To use your Site Recovery Manager instance on an Azure VMware Solution SDDC with a VMware Site Recovery service, you must activate the VMware Site Recovery service on a VMware Cloud™ on AWS SDDC.

Prerequisites

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

Procedure

1 Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.

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

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

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

Set the NSX-T Edge Management Gateway Firewall Rules for VMware Site Recovery

To enable VMware Site Recovery on your SDDC environment that uses VMware NSX-T®, you must create firewall rules between your VMware Cloud on AWS SDDC and the Management Gateway. After the initial firewall rules configuration, you can add, edit or delete any rules as needed.

Procedure

1 Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.

2 Select **Networking & Security > Gateway Firewall > Management Gateway**.

3 Click **Add New Rule**.

4 Enter the management gateway rule parameters.

Management gateway controls management traffic that flows in and out of the SDDC.

Option	Description
Name	Enter a descriptive name for the rule.
Source	Click **Set Source** and enter or select one of the following options: ■ Select **Any** to allow traffic from any source address or address range. **Important** Although you can select **Any** as the source address in a firewall rule, using **Any** as the source address in this firewall rule can enable attacks on your SDDC and might lead to compromise of your SDDC. As a best practice, configure this firewall rule to allow access only from trusted source addresses. See VMware Knowledge Base article 84154. ■ Select **System Defined Groups** and select one of the following source options. ■ **vCenter** to allow traffic from your SDDC's vCenter Server ■ **Site Recovery Manager** to allow traffic from your SDDC's Site Recovery Manager. ■ **vSphere Replication** to allow traffic from your SDDC's vSphere Replication. ■ Select **User Defined Groups** to enter the name and CIDR IP range of a remote network.
Destination	Click **Set Destination** and enter or select one of the following options: ■ Select **Any** to allow traffic to any destination address or address range. ■ Select **System Defined Groups** and select one of the following destination options. ■ **vCenter** to allow traffic to your SDDC's vCenter Server. ■ **Site Recovery Manager** to allow traffic to your SDDC's Site Recovery Manager. ■ **vSphere Replication** to allow traffic to your SDDC's vSphere Replication. ■ Select **User Defined Groups** to enter the name and CIDR IP range of a remote network.
Service	Select one of the services to apply the rule to. ■ HTTPS (TCP 443) applies to vCenter Server and vSphere Replication as destinations. ■ VMware Site Recovery SRM applies only to Site Recovery Manager as a destination. ■ VMware Site Recovery vSphere Replication applies only to vSphere Replication as a destination.
Action	The only action available for management gateway firewall rules is **Allow**.

5 Repeat the previous step to apply the following firewall rules for VMware Site Recovery.

Name	Source	Destination	Service	Action
Remote SRM to vCenter Server	User-Defined Group that includes the remote Site Recovery Manager IP address.	vCenter	**HTTPS (TCP 443)**	Allow
Remote VR to vCenter Server	User-Defined Group that includes the remote vSphere Replication IP address.	vCenter	**HTTPS (TCP 443)**	Allow
Remote network to SRM (SRM Server Management)	User-Defined Group that includes the remote Site Recovery Manager and vSphere Replication IP addresses.	Site Recovery Manager	**VMware Site Recovery SRM**	Allow
Remote network to VR (VM Replication)	User-Defined Group that includes the remote ESXi hosts IP addresses.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
Remote network to VR (VR Server Management)	or User-Defined Group that includes the remote Site Recovery Manager and vSphere Replication IP addresses.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
Remote network to VR (UI and API)	User-Defined Group that includes the remote browser IP address.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
SRM (HTTPS) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote Platform Services Controller and vCenter Server IP addresses.	**Any**	Allow
VR (HTTPS) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote Platform Services Controller and vCenter Server IP addresses.	**Any**	Allow

Name	Source	Destination	Service	Action
SRM (SRM Server Management) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote Site Recovery Manager IP address.	**Any**	Allow
VR (SRM Server Management) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote Site Recovery Manager IP address.	**Any**	Allow
ESXi (VM Replication) to remote network	ESXi	Any or User-Defined Group that includes the remote vSphere Replication IP addresses (combined vSphere Replication appliance and any add-on vSphere Replication appliances).	**Any**	Allow
SRM (VR Server Management) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote vSphere Replication IP address.	**Any**	Allow
VR (VR Server Management) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote vSphere Replication IP address.	**Any**	Allow

6 Click **Publish**.

Results

After the firewall rules are created, they are shown in the Management Gateway Edge Firewall list.

Connect the Site Recovery Manager Server Instances on the Azure VMware Solution SDDC and the VMware Cloud on AWS SDDC

Before you can protect your virtual machines between an Azure VMware Solution SDDC and a VMware Cloud on AWS SDDC and the reverse, you must connect the Site Recovery Manager Server and vSphere Replication instances on the protected and the recovery sites. This procedure is known as site pairing.

Procedure

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

Results

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

Deploying Site Recovery Manager on Google Cloud VMware Engine

9

You can use Site Recovery Manager 8.5.x and vSphere Replication 8.5.x with Google Cloud VMware Engine.

Google Cloud VMware Engine is an infrastructure-as-a-service offering built on Google Cloud's highly performant scalable infrastructure and VMware Cloud Foundation stack. It enables a fast path to the cloud, seamlessly migrating or extending existing VMware workloads from on-premises environments to Google Cloud Platform.

You can use Site Recovery Manager 8.5.x and vSphere Replication 8.5.x to plan, test, and run the recovery of virtual machines between a protected vCenter Server on-premises site and a recovery vCenter Server site on Google Cloud VMware Engine and the reverse, or between two Google Cloud VMware Engine cloud sites.

Procedure

1 Operational Limits of Site Recovery Manager on Google Cloud VMware Engine

Each Site Recovery Manager instance on Google Cloud VMware Engine can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries.

2 Setting Up Site Recovery Manager on Google Cloud VMware Engine

To ensure a successful vSphere Replication and Site Recovery Manager deployments, follow the sequence of tasks required.

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

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

Operational Limits of Site Recovery Manager on Google Cloud VMware Engine

Each Site Recovery Manager instance on Google Cloud VMware Engine can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries.

Protection and Recovery Maximums for Site Recovery Manager

Table 9-1. Protection and Recovery Maximums for Site Recovery Manager

Item	Maximum
Total number of protected virtual machines per SDDC on Google Cloud VMware Engine	3000 **Note** To achieve the 3000 virtual machines scale, you must manually balance the replications between the different vSphere Replication nodes. You must manually add additional vSphere Replication servers to your environments, see Deploying Additional vSphere Replication Servers in the *vSphere Replication Administration* guide.
Maximum number of protected virtual machines per vSphere Replication appliance (through embedded vSphere Replication server).	300
Maximum number of protected virtual machines per vSphere Replication server.	300
Total number of virtual machines per protection group	500
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Total number of virtual machines per recovery plan	2000
Total number of virtual machine recoveries that you can start simultaneously across multiple recovery plans	2000

Bidirectional Protection

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

For example, if you protect 1600 virtual machines using vSphere Replication from site A to site B, you can use vSphere Replication to protect a maximum of 1400 virtual machines from site B to site A. If you are using vSphere Replication for a bidirectional protection, you can protect a maximum of 3000 virtual machines across both sites.

IP Customization Maximums for VMware Site Recovery

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

- 1 IP address

- Subnet information
- 1 gateway server address
- 2 DNS servers (primary and secondary)

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

Recovery Point Objective lower than 15 minutes

For information about Recovery Point Objective (RPO) lower than 15 minutes, see Recovery Point Objective in the *vSphere Replication Administration* guide.

Setting Up Site Recovery Manager on Google Cloud VMware Engine

To ensure a successful vSphere Replication and Site Recovery Manager deployments, follow the sequence of tasks required.

Setting up your private cloud environment

You can use your Google Cloud VMware Engine private cloud as a disaster recovery site for your on-premises site.

1. Create a private cloud in the VMware Engine portal. See Creating a private cloud in the *Google Cloud VMware Engine documentation*.
2. Set up private cloud networking for Site Recovery Manager. See Creating a subnet in the *Google Cloud VMware Engine documentation*.
3. Set up the on-premises to cloud connectivity. You must use a site-to-site VPN or Cloud Interconnect. For more information, see the Google Cloud Cloud VPN documentation and the Google Cloud Cloud Interconnect documentation.
4. Set up the infracstructure services in your private cloud. For more information, see Configuring disaster recovery using SRM in the *Google Cloud VMware Egine documentation*.

Setting up vSphere Replication and Site Recovery Manager on your Google Cloud VMware Engine private cloud

1. Prepare a solution user account for installation. See Using solution user accounts in the *Google Cloud VMware Egine documentation*.
2. Deploy the vSphere Replication appliance on your private cloud. The procedure is the same as installing vSphere Replication on your on-premises site. See Installing and Setting Up vSphere Replication in the *vSphere Replication Administration* guide.
3. Configure firewall rules for the vSphere Replication appliance. See Firewall tables in the *Google Cloud VMware Egine documentation*.

4 Install Site Recovery Manager on your private cloud. The procedure is the same as the procedure for the on-premises installation. See Deploy the Site Recovery Manager Appliance.

5 Configure firewall rules for the Site Recovery Manager appliance. See Firewall tables in the *Google Cloud VMware Egine documentation*.

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

7 Install the Site Recovery Manager License Key. See Install the Site Recovery Manager License Key.

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

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

Procedure

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

2 Click the **New Site Pair** button.

3 Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.

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

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

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

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

Results

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

Deploying Site Recovery Manager on Oracle Cloud VMware Solution

10

You can use Site Recovery Manager 8.5.x and vSphere Replication 8.5.x with Oracle Cloud VMware Solution.

Oracle Cloud VMware Solution integrates VMware on-premises tools, skillsets, and processes with public Oracle Cloud services. The solution is a fully customer-managed, customer-operated native VMware cloud environment based on VMware Validated Solutions for use with the public Oracle Cloud Infrastructure.

You can use Site Recovery Manager 8.5.x and vSphere Replication 8.5.x to plan, test, and run the recovery of virtual machines between a protected vCenter Server on-premises site and a recovery vCenter Server site on Oracle Cloud VMware Solution and the reverse, or between two Oracle Cloud VMware Solution cloud sites.

Procedure

1 Operational Limits of Site Recovery Manager on Oracle Cloud VMware Solution

   Each Site Recovery Manager instance on Oracle Cloud VMware Solution can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries.

2 Setting Up Site Recovery Manager on Oracle Cloud VMware Solution

   To ensure a successful vSphere Replication and Site Recovery Manager deployments, follow the sequence of required tasks.

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

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

Operational Limits of Site Recovery Manager on Oracle Cloud VMware Solution

Each Site Recovery Manager instance on Oracle Cloud VMware Solution can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries.

Protection and Recovery Maximums for Site Recovery Manager

Table 10-1. Protection and Recovery Maximums for Site Recovery Manager

Item	Maximum
Total number of protected virtual machines per SDDC on Oracle Cloud VMware Solution	3000 **Note** To achieve the 3000 virtual machines scale, you must manually balance the replications between the different vSphere Replication nodes. You must manually add additional vSphere Replication servers to your environments, see Deploying Additional vSphere Replication Servers in the *vSphere Replication Administration* guide.
Maximum number of protected virtual machines per vSphere Replication appliance (through embedded vSphere Replication server).	300
Maximum number of protected virtual machines per vSphere Replication server.	300
Total number of virtual machines per protection group	500
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Total number of virtual machines per recovery plan	2000
Total number of virtual machine recoveries that you can start simultaneously across multiple recovery plans	2000

Bidirectional Protection

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

For example, if you protect 1600 virtual machines using vSphere Replication from site A to site B, you can use vSphere Replication to protect a maximum of 1400 virtual machines from site B to site A. If you are using vSphere Replication for a bidirectional protection, you can protect a maximum of 3000 virtual machines across both sites.

IP Customization Maximums for VMware Site Recovery

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

- 1 IP address

- Subnet information
- 1 gateway server address
- 2 DNS servers (primary and secondary)

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

Recovery Point Objective lower than 15 minutes

For information about Recovery Point Objective (RPO) lower than 15 minutes, see Recovery Point Objective in the *vSphere Replication Administration* guide.

Setting Up Site Recovery Manager on Oracle Cloud VMware Solution

To ensure a successful vSphere Replication and Site Recovery Manager deployments, follow the sequence of required tasks.

Setting up your private cloud environment

You can use your Oracle Cloud VMware Solution private cloud as a disaster recovery site for your on-premises site.

1. Deploy an Oracle Cloud VMware Solution SDDC on Oracle Cloud Infrastructure. See the Deploy a highly available VMware-based SDDC to the cloud Playbook in the *Oracle Help Center*.
2. Configure the DNS settings for your SDDC. See Configure DNS for an Oracle Cloud VMware Solution SDDC in the *Protect your VMware SDDC in the cloud against disasters* Playbook.
3. Configure the network and connectivity of your primary on-premiese site. See Configure the Primary Site in the *Protect your VMware SDDC in the cloud against disasters* Playbook.
4. Configure the Oracle Cloud VMware Solution site. For more information, see Configure the Recovery Site in the *Protect your VMware SDDC in the cloud against disasters* Playbook.
5. Pair the sites over FastConnect or IPSec VPN. For more information about FastConnect, see FastConnect in the *Oracle Cloud Infrastructure Documentation*. For more information about IPSec VPN, see Site-to-Site VPN in the *Oracle Cloud Infrastructure Documentation*.

Setting up vSphere Replication and Site Recovery Manager on your Oracle Cloud VMware Solution private cloud

1. Deploy the vSphere Replication appliance on your private cloud. The procedure is the same as installing vSphere Replication on your on-premises site. See Installing and Setting Up vSphere Replication in the *vSphere Replication Administration* guide.
2. Install Site Recovery Manager on your private cloud. The procedure is the same as the procedure for the on-premises installation. See Deploy the Site Recovery Manager Appliance.

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

4 Install the Site Recovery Manager License Key.

For more information about the architecture and the different use cases, see Learn About Protecting your VMware SDDC in the Cloud Against Disasters in the *Protect your VMware SDDC in the cloud against disasters* Playbook.

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

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

Procedure

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

2 Click the **New Site Pair** button.

3 Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.

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

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

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

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

Results

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

Configuring the Customer Experience Improvement Program 11

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

To join or leave the CEIP for this product, see *Join or Leave Customer Experience Improvement Program in vSphere Client* in the *VMware vSphere Product Documentation*.

Read the following topics next:

- Categories of Information that VMware Receives
- Join or Leave Customer Experience Improvement Program

Categories of Information that VMware Receives

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

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

Join or Leave Customer Experience Improvement Program

You can activate or deactivate data collection at any time.

Prerequisites

- CEIP participation requires connection from the Site Recovery Manager virtual appliance to **`https://vcsa.vmware.com:443`**.
- If the system uses a firewall or a proxy to connect to the Internet, you must specify a firewall or a proxy rule allowing outbound traffic through for **`https://vcsa.vmware.com:443/ph/api/*`**.
- Verify that you are a member of the Administrators@vsphere.local group.

Procedure

1. Log in to the vCenter Server instance as a member of Administrators@vsphere.local by using the vSphere Client.

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

3 Under Deployment, click **Customer Experience Improvement Program**.

4 To join the CEIP, click **Join Program**. To leave the Program, click **Leave Program**.

Provide Feedback with the Site Recovery User Interface

12

You can use the feedback tool in the Site Recovery User Interface to provide timely feedback to our developers.

Procedure

1. In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. From the Site Recovery home screen, click the feedback icon in the top right-corner.
3. Select the type of feedback you want to give and enter your feedback in the **Description** window.
4. (Optional) Provide an email address and screenshots or other images.
5. Click **Send**.

Exporting and Importing Site Recovery Manager Configuration Data

13

You can use the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool to export and import configuration data.

If you plan to migrate Site Recovery Manager to a different host, you can use the tool to export inventory mappings, recovery plans, protection groups, and the related objects into an XML file. You can then import the configuration data from the previously exported file.

The VMware Site Recovery Manager 8.5 Configuration Import/Export Tool is available through the Site Recovery User Interface and as a standalone `.jar` file. When you deploy the Site Recovery Manager appliance, the tool is also deployed with the appliance. The tool is located in the `/opt/vmware/impex` directory.

Requirements for Using the Standalone Configuration Tool

- You must have Java 1.8.x or later installed on the Site Recovery Manager host machine.
- The `JAVA_HOME` environment variable must be properly configured. For example, `JAVA_HOME=/usr/java/jre1.8.0_152`.

Requirements for Exporting and Importing Site Recovery Manager Configuration Data

- Before you can export a configuration, you must have a site pair with Site Recovery Manager 8.5.x up and running on both the protected and the recovery site.
- Import is supported in a clean Site Recovery Manager 8.5.x installation, registered to the same vCenter Server instance or to a vCenter Server instance which contains the same inventory.

Input Parameters Required for Import with the Standalone Configuration Tool

- Lookup Service host name. The host name of the Platform Services Controller or the vCenter Server host name, if you are using vCenter Server with an Embedded Platform Services Controller.

- vCenter Single Sign-On administrator user name and password for both sites or solution user certificates in a Java Keystore (JKS).

Exported Information

The VMware Site Recovery Manager 8.5 Configuration Import/Export Tool exports the Site Recovery Manager version, build number, local and remote site names, inventory mappings, and placeholder datastores. Other exported information includes advanced settings, array managers with SRA information, protection groups, recovery plans, and so on. The information is stored in an XML file. You can validate the XML file by using the following XSD schema.

Read the following topics next:

- Export Site Recovery Manager Configuration Data Through the User Interface
- Export Site Recovery Manager Configuration Data by Using a Script Without Credentials
- Modify the Export Script of the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool
- Schedule an Export of Site Recovery Manager Configuration Data by Using a Cron Job
- Export Site Recovery Manager Appliance Configuration Data by Using a Callout
- Export Site Recovery Manager Configuration Data with the Standalone Import/Export Tool
- Use a Properties File to Export Site Recovery Manager Configuration Data
- Import the Site Recovery Manager Configuration Data through the User Interface
- Import Site Recovery Manager Configuration Data with the Standalone Import/Export Tool
- Use a Properties File to Import Site Recovery Manager Configuration Data
- Syntax of the Import/Export Tool
- Properties for Automated Export and Import of Site Recovery Manager Configuration Data
- Troubleshooting the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool

Export Site Recovery Manager Configuration Data Through the User Interface

You use the Site Recovery User Interface to export Site Recovery Manager configuration data in an XML file.

Prerequisites

Verify that you have a site pair with Site Recovery Manager running on both the protected and the recovery sites.

Procedure

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

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

3 On the **Summary** pane, click **Export/Import SRM Configuration > Export**, and click **Download**.

Export Site Recovery Manager Configuration Data by Using a Script Without Credentials

The Site Recovery Manager virtual appliance is bundled with a script generated during pairing that you can use to export Site Recovery Manager configuration data.

When you use the script to export Site Recovery Manager configuration data, you are not required to enter any credentials.

Prerequisites

Ensure that you have a working Site Recovery Manager pair.

Procedure

1 Log in to the Site Recovery Manager virtual appliance host machine as root by using `su`.

2 To export the configuration data, run `sh /opt/vmware/impex/bin/export.sh`.

The VMware Site Recovery Manager 8.5 Configuration Import/Export Tool exports the configuration data to `/opt/vmware/impex/exports/`.

Modify the Export Script of the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool

The Site Recovery Manager virtual appliance is bundled with a script that you can use to export Site Recovery Manager configuration data. You can modify the script to change the default export location, the number of exports, and so on.

Procedure

1 Log in to the Site Recovery Manager virtual appliance host machine.

2 Log in as root by using `su`.

3 SSH to the following location `/opt/vmware/impex/bin/`.

4 Use a text editor to open the `export.sh` file and add the following text to the last line of the script.

Option	Description
To change the location of the export files.	Add "`-e|--exportPath` *`/path/to/export`*". The default location is `/opt/vmware/impex/exports/`.
To change the maximum number of export files.	Add "`-m|--maxExports` *`NumberOfMaxExports`*". The default number of export files is 24.

5 Save the changes and close the editor.

Schedule an Export of Site Recovery Manager Configuration Data by Using a Cron Job

The Site Recovery Manager virtual appliance is bundled with a script that you can use to schedule a cron job for the export of Site Recovery Manager configuration data.

Prerequisites

Ensure that you have a working Site Recovery Manager pair.

Procedure

1 Log in to the Site Recovery Manager virtual appliance host virtual machine.

2 Run `su`.

3 Run the following command `crontab -e`.

4 Enter the configuration data.

For example, to export the configuration data at every hour enter the following information.`0 * * * * /usr/bin/sudo /bin/bash /opt/vmware/impex/bin/export.sh`

Export Site Recovery Manager Appliance Configuration Data by Using a Callout

You can use a top-level recovery step in the recovery plan to export configuration data from the Site Recovery Manager appliance.

Prerequisites

- Verify that you are using the Site Recovery Manager virtual appliance.
- Ensure that you have a working Site Recovery Manager pair.

Procedure

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

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

3 On the **Recovery Plans** tab, select a recovery plan, and click **Recovery Steps**.

4 Use the **View** drop-down menu and select **Recovery Steps**.

5 Select where to add the step.

- To add a step before a step, right-click the step, and select **Add Step Before**.
- To add a step after the last step, right-click the last step, and select **Add Step After**.

6 Select **Command on SRM Server**.

7 In the **Name** text box, enter a name for the step.

The step name appears in the list of steps in the **Recovery Steps** view.

8 Enter the following command in the **Content** text box. `/usr/bin/sudo /bin/bash /opt/vmware/impex/bin/export.sh`

9 (Optional) Modify the **Timeout** setting for the command to run on Site Recovery Manager Server.

10 Click **Add** to add the step to the recovery plan.

Results

When you run the recovery plan, the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool exports the configuration data on the recovery site. The default location for the exported configuration data is `/opt/vmware/impex/exports`. You can change the location by modifying the export script, see Modify the Export Script of the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool.

Export Site Recovery Manager Configuration Data with the Standalone Import/Export Tool

You can use the standalone VMware Site Recovery Manager 8.5 Configuration Import/Export Tool to export Site Recovery Manager configuration data in an XML file.

Prerequisites

- Verify that you have Java 1.8.x or later installed and environment variables configured on the Site Recovery Manager host virtual machine.
- Verify that you have a site pair with Site Recovery Manager running on both the protected and the recovery sites.

Procedure

1 Log in to the Site Recovery Manager virtual appliance host virtual machine.

2 Navigate to `/opt/vmware/impex`, and run the following command.

```
java -jar import-export.jar --exportInteractive
```

To make the XML file more human-readable, add the `format` option. Adding the `format` option significantly increases the XML file size.

```
java -jar import-export.jar --exportInteractive --format
```

3 Enter the host name or the IP address of the Lookup Service.

4 Enter the port number or press Enter, if you use the default port.

5 Accept the SHA-1 Thumbprint.

6 (Optional) Select whether to use Java keystore instead of the local vCenter Server credentials.

Note The Java keystore must hold certificate and key for a **solution** user with read permissions for the local vCenter Server and Site Recovery Manager.

a If you select yes, follow the prompts and provide the necessary information.

Option	Description
Keystore type	Press Enter to use the default keystore type JCEKS, or provide a keystore type.
Keystore path	Path to the Java keystore. For example, *path:/opt/vmware/impex/ks/ks.keystore*.
Keystore password	The password for the Java keystore.
Keystore certificate	The certificate alias for the solution user for the local vCenter Server.
Keystore key	The key alias for the solution user for the local vCenter Server.
Keystore key password	The key password for the solution user for the local vCenter Server.

7 If you selected no, enter the user name and password for the local vCenter Server instance.

8 Select a local Site Recovery Manager instance.

9 (Optional) Select whether to use Java keystore instead of the remote vCenter Server credentials.

Note The Java keystore must hold certificate and key for a **solution** user with read permissions for the remote vCenter Server and Site Recovery Manager.

a If you select yes, follow the prompts and provide the necessary information.

Option	Description
Keystore type	Press Enter to use the default keystore type JCEKS, or provide a keystore type.
Keystore path	Path to the Java keystore. For example, *path:/opt/vmware/impex/ks/ks.keystore*.
Keystore password	The password for the Java keystore.
Keystore certificate	The certificate alias for the solution user for the remote vCenter Server.
Keystore key	The key alias for the solution user for the remote vCenter Server.
Keystore key password	The key password for the solution user for the remote vCenter Server.

10 If you selected no, enter user name and password for the remote vCenter Server instance.

Use a Properties File to Export Site Recovery Manager Configuration Data

You can use a properties file to simplify or automate the export of Site Recovery Manager configuration data in an XML file.

If you are using the Site Recovery Manager appliance, you can Schedule an Export of Site Recovery Manager Configuration Data by Using a Cron Job.

Prerequisites

- Verify that you have Java 1.8.x or later installed on the Site Recovery Manager host virtual machine.
- Verify that you have a site pair with Site Recovery Manager running on both the protected and the recovery site.
- Verify that you have Properties for Automated Export and Import of Site Recovery Manager Configuration Data.

Procedure

1. Log in to the Site Recovery Manager virtual appliance host virtual machine.
2. Navigate to `/opt/vmware/impex`, and run the following command.

   ```
   java -jar import-export.jar --exportProperties=Path_to_properties_file
   ```

   To make the XML file more readable, add the `format` option.

   ```
   java -jar import-export.jar --exportProperties=Path_to_properties_file --format
   ```

Import the Site Recovery Manager Configuration Data through the User Interface

You can use the Site Recovery User Interface to import Site Recovery Manager configuration data from a previously exported XML file.

Prerequisites

Provide a clean Site Recovery Manager installation, registered with the same vCenter Server instance or with a vCenter Server instance with the same inventory as the exported.

Procedure

1. In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
3. On the **Summary** tab, click **Export/Import SRM Configuration > Import**.
4. On the **Confirmation** page, select the check boxes, and click **Next**.
5. Click **Browse**, navigate to the previously exported XML file, and click **Import**.

6 If the selected export file contains array managers, select which array manager pairs to import and provide credentials, and click **Import**.

   If there are problems with an import stage, you can download a CSV report file.

7 When the import is complete, click **Close**.

Import Site Recovery Manager Configuration Data with the Standalone Import/Export Tool

You can use the standalone VMware Site Recovery Manager 8.5 Configuration Import/Export Tool to import Site Recovery Manager configuration data from a previously exported XML file.

Prerequisites

- Provide a clean Site Recovery Manager installation, registered with the same vCenter Server instance or with a vCenter Server instance with the same inventory as the exported.
- Verify that you have Java 1.8.x or later installed and environment variables configured on the Site Recovery Manager host virtual machine.

Procedure

1 Log in to the Site Recovery Manager virtual appliance host virtual machine.

2 Navigate to `/opt/vmware/impex`, and run the following command.

   ```
   java -jar import-export.jar --importInteractive --path Path_to_exported_XML_file
   ```

   By default the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool is set to retry the import of virtual machines recovery settings after a delay of 10 000 milliseconds up to five times. You can manually change the default values for retry counts and delay between retries by adding the `retries` and `delay` options to the import command. For example, to make 10 retries with a 20 seconds delay, run the following command.

   ```
   java -jar import-export.jar --importInteractive --path Path_to_exported_XML_file --delay 20000 --retries 10
   ```

3 Enter the host name or the IP address of the Platform Services Controller.

4 Enter the port number or press Enter to use the default.

5 Accept the SHA-1 Thumbprint.

6 (Optional) Select whether to use Java keystore instead of the local vCenter Server credentials or not.

a If you select yes, follow the prompts and provide the necessary information.

Option	Description
Keystore type	Press Enter to use the default keystore type JCEKS, or provide a keystore type.
Keystore path	Path to the Java keystore. For example, *path:/opt/vmware/impex/ks/ks.keystore*.
Keystore password	The password for the Java keystore.
Keystore certificate	The certificate alias for the solution user for the local vCenter Server.
Keystore key	The key alias for the solution user for the local vCenter Server.
Keystore key password	The key password for the solution user for the local vCenter Server.

7 If you selected no, enter user name and password for the local vCenter Server instance.

8 Select a local Site Recovery Manager.

9 (Optional) Select whether to use Java keystore instead of the remote vCenter Server credentials or not.

a If you select yes, follow the prompts and provide the necessary information.

Option	Description
Keystore type	Press Enter to use the default keystore type JCEKS, or provide a keystore type.
Keystore path	Path to the Java keystore. For example, *path:/opt/vmware/impex/ks/ks.keystore*.
Keystore password	The password for the Java keystore.
Keystore certificate	The certificate alias for the solution user for the remote vCenter Server.
Keystore key	The key alias for the solution user for the remote vCenter Server.
Keystore key password	The key password for the solution user for the remote vCenter Server.

10 If you selected no, enter user name and password for the remote vCenter Server instance.

11 Provide credentials for the array managers.

Results

The VMware Site Recovery Manager 8.5 Configuration Import/Export Tool imports the Site Recovery Manager configuration data to the new Site Recovery Manager instance.

Use a Properties File to Import Site Recovery Manager Configuration Data

You can use a properties file to simplify or automate the import of Site Recovery Manager configuration data from an XML file.

Prerequisites

- Provide a clean Site Recovery Manager installation, registered with the same vCenter Server instance or with a vCenter Server instance with the same inventory as the exported.
- Verify that you have Java 1.8.x or later installed and environment variables configured on the Site Recovery Manager host virtual machine.
- Verify that you have Properties for Automated Export and Import of Site Recovery Manager Configuration Data.

Procedure

1. Log in to the Site Recovery Manager virtual appliance host virtual machine.
2. Navigate to `/opt/vmware/impex`, and run the following command.

   ```
   java -jar import-export.jar --importProperties=Path_to_properties_file --path
   Path_to_exported_XML_file
   ```

Syntax of the Import/Export Tool

The VMware Site Recovery Manager 8.5 Configuration Import/Export Tool includes options that you can use to import or export configuration data. You can also use the options to change the delay between retries when importing virtual machine recovery settings, to customize the number of retries, to override the network mappings with the mappings from the XML file, and so on.

Table 13-1. VMware Site Recovery Manager 8.5 Configuration Import/Export Tool Options

Option	Description
`--export`	Required when doing an export. Cannot be used together with `--import`.
`--exportProperties`	Used for exporting data by using a properties file.
`--exportInteractive`	Used to start an interactive export with prompts for the required information.
`--importProperties`	Required when importing configuration data with a properties file. Cannot be used together with `--export`.
`--importInteractive`	Used to start an interactive import with prompts for the required information.
`--lspp`	The Platform Services Controller address. It can be an IP address or FQDN.

Table 13-1. VMware Site Recovery Manager 8.5 Configuration Import/Export Tool Options (continued)

Option	Description
`--port <[1, 2147483647]>`	The port number for the Lookup Service. The default value is 443.
`--localSrmName`	The name of the local Site Recovery Manager Server. Required unless you use `--localSrmGuid`.
`--localSrmGuid`	The guid of the local Site Recovery Manager Server. Required unless you use `--localSrmName`.
`--localAuthUseKeystore`	Used to specify whether to use a Java Keystore (JKS) file to log in to the local site.
`--localAuthCredsUsername`	Required when not using JKS. The user name for the local vCenter Server.
`--localAuthCredsPass`	Required when not using JKS. The password for the local vCenter Server.
`--localAuthKsType`	Used to specify the type of the JKS. The default type is JCEKS.
`--localAuthKsPath`	Used to specify the path to the local JKS.
`--localAuthKsPass`	Used to specify the JKS password.
`--localAuthKsCertAlias`	Used to specify the local solution user certificate alias.
`--localAuthKsKeyAlias`	Used to specify the local solution user key alias.
`--localAuthKsKeyPass`	Used to specify the local solution user key password.
`--remoteAuthUseKeystore`	Use to specify whether to use a Java Keystore file to log in to the remote site.
`--remoteAuthCredsUsername`	Required when not using JKS. The password for the remote vCenter Server.
`--remoteAuthCredsPass`	Required when not using JKS. The password for the remote vCenter Server.
`--remoteAuthKsType`	Used to specify the type of the JKS. The default type is JCEKS.
`--remoteAuthKsPath`	Used to specify the path to the remote JKS.
`--remoteAuthKsPass`	Used to specify the remote JKS password.
`--remoteAuthKsCertAlias`	Used to specify the remote solution user certificate alias.
`--remoteAuthKsKeyAlias`	Used to specify the remote solution user key alias.
`--remoteAuthKsKeyPass`	Used to specify the remote solution user key password.
`--path`	Used for importing data. Path to the previously exported file.

Table 13-1. VMware Site Recovery Manager 8.5 Configuration Import/Export Tool Options (continued)

Option	Description
`--delay <[1, 2147483647]>`	An integer value for the desired delay between retries in milliseconds when importing recovery settings. The default value is 10000.
`--retries <[1, 2147483647]>`	An integer value for the count of the retries when importing recovery settings. The default value is 5.
`--overrideProtectionSettings`	Used to override the network mappings. ■ If there is a protection group, the tool attempts to update the network mappings for each protected virtual machine (override the site-level mappings) with the mappings from the XML file. ■ If there is a recovery plan, the tool attempts to update the test network mappings for the recovery plan with the mappings from the XML file.
`--format`	Used to make the exported XML file better formatted and human-readable. The `--format` option significantly increases the file size.
`--exportPath`	Path to a directory in which to create the exported file.

Properties for Automated Export and Import of Site Recovery Manager Configuration Data

You can use the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool properties file to automate the export and import of configuration data.

The use of *`srm_configuration`*`.properties` file with the standalone VMware Site Recovery Manager 8.5 Configuration Import/Export Tool is optional.

Table 13-2. Required Parameters for the Properties File

Parameter	Description
`lookup.service.address`	The Platform Services Controller address. Can be an IP address or FQDN.
`local.srm.name`	The name of the local Site Recovery Manager Server.
`local.auth.use.keystore`	Set this parameter to true to use Java Keystore to log in to the local site. The default value is **`false`**.
`local.auth.credentials.vc.username`	The user name for the local vCenter Server. Required when `local.auth.use.keystore` is set to **`false`**.
`local.auth.credentials.vc.password`	The password for the local vCenter Server. Required when `local.auth.use.keystore` is set to **`false`**.
`local.auth.keystore.type`	The type of Java Keystore. Required when `local.auth.use.keystore` is set to **`true`**. The default type is JCEKS.

Table 13-2. Required Parameters for the Properties File (continued)

Parameter	Description
`local.auth.keystore.path`	Path to the Java Keystore. Required when `local.auth.use.keystore` is set to **`true`**.
`local.auth.keystore.pass`	Password for the Java Keystore. Required when `local.auth.use.keystore` is set to **`true`**.
`local.auth.keystore.certAlias`	Certificate alias for the local solution user in the Java Keystore. Required when `local.auth.use.keystore` is set to **`true`**.
`local.auth.keystore.keyAlias`	Key alias for the local solution user in the Java Keystore. Required when `local.auth.use.keystore` is set to **`true`**.
`local.auth.keystore.keyPass`	The key password for the local solution user in the Java Keystore. Required when `local.auth.use.keystore` is set to **`true`**.
`remote.auth.use.keystore`	Set this parameter to true to use Java Keystore to log in to the remote site. The default value is **`false`**.
`remote.auth.credentials.vc.username`	The user name for the remote vCenter Server. Required when `remote.auth.use.keystore` is set to **`false`**. Required if your environment is not federated.
`remote.auth.credentials.vc.password`	The password of the user for the remote vCenter Server. Required when `remote.auth.use.keystore` is set to **`false`**. Required if your environment is not federated.
`remote.auth.keystore.type`	The type of Java Keystore. Required when `remote.auth.use.keystore` is set to **`true`**. The default type is JCEKS.
`remote.auth.keystore.path`	Path to the Java Keystore. Required when `remote.auth.use.keystore` is set to **`true`**.
`remote.auth.keystore.pass`	Password for the Java Keystore. Required when `remote.auth.use.keystore` is set to **`true`**.
`remote.auth.keystore.certAlias`	Certificate alias for the remote solution user in the Java Keystore. Required when `remote.auth.use.keystore` is set to **`true`**.
`remote.auth.keystore.keyAlias`	Key alias for the remote solution user in the Java Keystore. Required when `remote.auth.use.keystore` is set to **`true`**.
`remote.auth.keystore.keyPass`	The key password for the remote solution user in the Java Keystore. Required when `remote.auth.use.keystore` is set to **`true`**.
`array.manager.n.name`	The name of the array manager, where `n` is a number. All array managers must be defined at least by a name and a skip flag. Required field for import, if your environment contains any array managers.

Table 13-2. Required Parameters for the Properties File (continued)

Parameter	Description
`array.manager.n.skip`	Sets whether the array manager must be imported or skipped. The default value is **`false`**. Required if `array.manager.n.name` is present.
`array.manager.n.username`	The user name for the array manager. Required if `array.manager.n.name` is present and `array.manager.n.skip` value is set to **`false`**.
`array.manager.n.password`	The password for the array manager. Required if `array.manager.n.name` is present and `array.manager.n.skip` value is set to **`false`**.

Table 13-3. Optional Parameters for the Properties File

Parameter	Description
`port`	The port number for the Lookup Service. The default value is 443.
`continue.after.array.manager.errors`	If you set the value to **`true`**, the tool does not fail when an array manager is missing or there is an array-based error. The default value is **`false`**.

Example: Sample Properties File

```
lookup.service.address=my.psc.address.com
port=443
local.srm.name=My local SRM
local.auth.credentials.vc.username=localAdmin
local.auth.credentials.vc.password=localAdminSecretPass
remote.auth.credentials.vc.username=remoteAdmin
remote.auth.credentials.vc.password=remoteAdminSecretPass
continue.after.array.manager.errors=false
array.manager.1.name=am_1
array.manager.1.skip=false
array.manager.1.username=am1AdminUserName
array.manager.1.password=am1AdminSecretPass
array.manager.2.name=am_2
array.manager.2.skip=true
array.manager.3.name=am_3
array.manager.3.skip=true
array.manager.4.name=am_4
array.manager.4.skip=true
```

Troubleshooting the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool

If you encounter problems with exporting or importing Site Recovery Manager configuration data, you can troubleshoot the problem.

When searching for the cause of a problem, also check the VMware knowledge base at http://kb.vmware.com/.

- Export Fails with an Error About a Duplicate Key

  When you try to export Site Recovery Manager configuration data, the export fails with an error about duplicate INSTANCE_UUID values.

Export Fails with an Error About a Duplicate Key

When you try to export Site Recovery Manager configuration data, the export fails with an error about duplicate INSTANCE_UUID values.

Problem

When you try to export Site Recovery Manager configuration data, the export fails due to the following error `"Export ended with errors, check log for more information. Error: Duplicate key l_vm_vm-123456"`.

Cause

The problem can occur when a virtual machine and a virtual machine template in one of the vCenter Server inventories have the same INSTANCE_UUIDs. The virtual machine and the virtual machine template must have different INSTANCE_UUID values.

The `l_` prefix in the error message means that the objects with the same INSTANCE_UUIDs are in the inventory of the local site. An `r_` prefix in the error message means that the objects with the same INSTANCE_UUIDs are in the inventory of the remote site. The local site is the site from which the export operation is initiated, the remote site is the other site in the Site Recovery Manager pair. The end part of the error message `vm-123456` represents the ManagedObjectReference value of one of the vCenter Server objects.

Solution

Delete the virtual machine or the virtual machine template from the vCenter Server inventory. Deleting one of the objects removes the duplicate key.

Migrating Storage Policy Protection Groups to Array-Based Replication Protection Groups

14

Site Recovery Manager 8.5.x is the last general version that supports storage policy protection groups (SPPG).

Site Recovery Manager version 8.5.0.5 and later has a dedicated Storage Policy Protection Group migration tool that you can use to migrate your SPPGs to regular array-based replication protection groups.

Prerequisites

Verify that you have upgraded your environment to Site Recovery Manager 8.5.0.5 or later.

Procedure

1. Check Your Environment for Storage Policy Protection Groups

   Before migrating the storage policy protection groups (SPPG) to regular array-based replication protection groups, you must check the protection groups for errors.

2. Migrate your Storage Policy Protection Groups to Array-Based Replication Protection Groups

   You use the Storage Policy Protection Group (SPPG) migration tool to migrate storage policy protection groups to regular array-based replication protection groups.

3. Syntax of the Storage Policy Protection Groups Migration Tool

   The Storage Policy Protection Groups Migration Tool includes options that you can use to specify the migration of storage policy protection groups. You can change the port number, specify a user, deactivate certificate validation checks, and so on.

Check Your Environment for Storage Policy Protection Groups

Before migrating the storage policy protection groups (SPPG) to regular array-based replication protection groups, you must check the protection groups for errors.

Procedure

1. Log in to the Site Recovery Manager appliance host virtual machine as **root**.

2 Navigate to `/opt/vmware/srm/bin`, and run the following command.

   a (Optional) For a vCenter Server instance with an internal Platform Services Controller, run the following command `./migrate-sppg -cmd check -vc FQDN_of_the_vCenter_Server -srm FQDN_of_Site_Recovery_Manger`.

   b (Optional) For a vCenter Server instance with an internal Platform Services Controller and a specified user, run the following command `./migrate-sppg -cmd check -vc FQDN_of_the_vCenter_Server -srm FQDN_of_Site_Recovery_Manger -u user_name@vsphere.local`.

   c (Optional) For a vCenter Server instance with an external Platform Services Controller, run the following command `./migrate-sppg -cmd check -vc FQDN_of_the_vCenter_Server -psc FQDN_of_Platform_Services_Controller -srm FQDN_of_Site_Recovery_Manger`.

3 Accept the SHA2 thumbprints of the certificates and provide the required credentials.

Results

The Storage Policy Protection Group migration tool checks the protection groups for errors. You must fix any errors and warnings before proceeding with the migration.

What to do next

Migrate the Storage Policy Protection Groups to regular array-based replication protection groups.

Migrate your Storage Policy Protection Groups to Array-Based Replication Protection Groups

You use the Storage Policy Protection Group (SPPG) migration tool to migrate storage policy protection groups to regular array-based replication protection groups.

The Storage Policy Protection Group migration tool preserves the information for the current migration tasks and if there is an unexpected failure, you can rerun the migrate command and resume the failed task. An example of an unexpected error might include network or electricity glitches.

Note If there is an SPPG with errors and there are other SPPGs with no errors, the tool attempts to migrate the groups and recovery plans that have no errors.

Prerequisites

Verify that you have checked your storage policy protection groups for errors. You must fix all errors for the migration of an SPPG to complete successfully.

Procedure

1 Log in to the Site Recovery Manager appliance host virtual machine as **root**.

2 Navigate to `/opt/vmware/srm/bin`, and run the following command.

   a (Optional) For a vCenter Server instance with an internal Platform Services Controller, run the following command `./migrate-sppg -cmd migrate -vc FQDN_of_the_vCenter_Server -srm FQDN_of_Site_Recovery_Manger`.

   b (Optional) For a vCenter Server instance with an internal Platform Services Controller and a specified user, run the following command `./migrate-sppg -cmd migrate -vc FQDN_of_the_vCenter_Server -srm FQDN_of_Site_Recovery_Manger -u user_name@vsphere.local`.

   c (Optional) For a vCenter Server instance with an external Platform Services Controller, run the following command `./migrate-sppg -cmd migrate -vc FQDN_of_the_vCenter_Server -psc FQDN_of_Platform_Services_Controller -srm FQDN_of_Site_Recovery_Manger`.

3 Accept the SHA2 thumbprints of the certificates and provide the required credentials.

4 Confirm that you want to proceed with the migration of protection groups without errors.

5 Confirm that you want to reconfigure the related recovery plans.

Syntax of the Storage Policy Protection Groups Migration Tool

The Storage Policy Protection Groups Migration Tool includes options that you can use to specify the migration of storage policy protection groups. You can change the port number, specify a user, deactivate certificate validation checks, and so on.

Storage Policy Protection Groups Migration Tool Options

Table 14-1. Common Options

Option	Description
`--version`	Shows version of the Storage Policy Protection Groups Migration Tool.
`--help arg`	Shows help for the Storage Policy Protection Groups Migration Tool. Optionally, you can specify a command.
`--cfg arg`	Optional. Configuration file. If not specified, the program will try to load a configuration file with the executable name and .XML extension in the current working directory. If such file is not available, the program will use default configuration values.
`--cmd arg`	Required. Command to execute. Supported commands are `check` and `migrate`.
`--check`	Checks the status of all storage policy protection groups.
`--migrate`	Migrate all storage policy protection groups that are ready for migration.

Table 14-2. Specific Options for the Check and Migrate Commands

Option	Description
`--psc arg`	Optional. FQDN of the Platform Services Controller node. If not specified, the vCenter Server node is also considered as PSC node.
`--psc_port arg`	Optional. Port of the Platform Services Controller node. The default value is 443.
`--vc arg`	Required. FQDN of the vCenter Server node where Site Recovery Manager is registered.
`--vc_port arg`	Optional. Port of the vCenter Server node. The default value is 443. It is taken into account only if the `psc` argument is set and is different then the `vc` argument. If that is not the case, the tool uses the `psc_port`.
`--srm arg`	Required. FQDN of the Site Recovery Manager node.
`--srm_port arg`	Optional. Port of the Site Recovery Manager node. The default value is 443.
`--u arg`	Optional. Name of the Site Recovery Manager administrative account registered with the specified vCenter Server node. The default user is `administrator@vsphere.local`.
`--ru arg`	Optional. Name of the Site Recovery Manager administrative account registered with the remote vCenter Server. The specified Site Recovery Manager server is expected to be paired with a Site Recovery Manager server that is registered with the remote vCenter Server where this account can login. The default user is administrator@vsphere.local
`--y`	Optional. Flag to specify yes answer to all questions. The default behavior is to ask for confirmation.
`--no_ssl`	Optional. Flag to deactivate certificate validation checks. The default behavior is to verify SSL certificates.

Upgrading Site Recovery Manager 15

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

For information about supported upgrade paths, see **Upgrade Path > VMware Site Recovery Manager** in the VMware Product Interoperability Matrixes at https://interopmatrix.vmware.com/Upgrade before you upgrade.

- Information That Site Recovery Manager Upgrade Preserves

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

- Prerequisites and Best Practices for Site Recovery Manager Upgrade

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

- Order of Upgrading vSphere and Site Recovery Manager Components

  There are alternative strategies for the upgrade of Site Recovery Manager sites. You can upgrade all components of one of your sites before upgrading all the components on the other site or you can upgrade the Site Recovery Manager components on both sites.

- Update the Site Recovery Manager Virtual Appliance

  You use the Site Recovery Manager Appliance Management Interface to apply patches and updates to the virtual appliance.

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 preserves only protection groups and recovery plans that are in a valid state.

Site Recovery Manager License

Site Recovery Manager preserves the license only during an upgrade within the same version, for example, from version 8.3.0.x to version 8.3.1, or from version 8.4.0.1 to version 8.4.0.2. During an upgrade to a different version, for example, from 8.4 to 8.5 or later, Site Recovery Manager reverts to an evaluation license. After the upgrade, you must reinstall your Site Recovery Manager license key.

Prerequisites and Best Practices for Site Recovery Manager Upgrade

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

- Make a full backup of the Site Recovery Manager database by using the tools that the database software provides. For information about how to back up the embedded database, see Back Up and Restore the Embedded vPostgres Database. Migration of data from an external database to the embedded database is not supported. Failure to back up the database results in the loss of all Site Recovery Manager data if the upgrade fails.
- Perform a configuration export by using the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool. See, Chapter 13 Exporting and Importing Site Recovery Manager Configuration Data.
- If you configured advanced settings in the existing installation, take a note of the settings that you configured in **Site Pair > Configure > Advanced Settings** in the Site Recovery user interface.
- Before you upgrade, check the supported upgrade paths.

  For information about supported upgrade paths, see **Upgrade Path > VMware Site Recovery Manager** in the VMware Product Interoperability Matrixes at https://interopmatrix.vmware.com/Upgrade before you upgrade.
- The local and remote Platform Services Controller and vCenter Server instances must be running when you upgrade Site Recovery Manager.

- Upgrade Platform Services Controller and vCenter Server on the site on which you are upgrading Site Recovery Manager to a supported version.
  - When you upgrade or migrate a vCenter Server deployment using an external Platform Services Controller, you must first converge the external Platform Services Controller to an embedded Platform Services Controller and then perform the upgrade or migration. For more information, see Upgrade or Migration for vCenter Server Instances with an External Platform Services Controller.
  - For information about how to upgrade vCenter Server and its components, see *vCenter Server Upgrade* in the *ESXi and vCenter Server Documentation*.
  - For information about compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.5* at https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.
  - For information about the order in which to upgrade the components on each site, see Order of Upgrading vSphere and Site Recovery Manager Components.
- Obtain the address of the Platform Services Controller instance for both sites.
- Obtain the vCenter Single Sign-On administrator user name and password for both of the local and remote sites.
- To use Site Recovery Manager with vSphere Replication, upgrade vSphere Replication before you upgrade Site Recovery Manager Server. After upgrading vSphere Replication, you must restart the Site Recovery Manager Server. See Order of Upgrading vSphere and Site Recovery Manager Components.
  - For information about how to upgrade vSphere Replication, see Upgrading vSphere Replication in *vSphere Replication Administration*.
  - For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.5* at https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.
- If you cannot upgrade an existing incompatible version of vSphere Replication, you must unregister vSphere Replication from both vCenter Server instances before you upgrade Site Recovery Manager. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Web Client to stop working. See Unregister an Incompatible Version of vSphere Replication.
- If you use custom certificates, obtain an appropriate certificate file. Custom certificates must use at least the SHA1, or preferably SHA256, thumbprint algorithm. This release of Site Recovery Manager does not support certificates that use the MD5 thumbprint algorithm. See Requirements When Using Custom SSL/TLS Certificates With Site Recovery Manager.

- **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 the protection groups is OK.
  - The protection status of all the individual virtual machines in the protection groups is OK.
  - The recovery status of all the protection groups is Ready.

Order of Upgrading vSphere and Site Recovery Manager Components

There are alternative strategies for the upgrade of Site Recovery Manager sites. You can upgrade all components of one of your sites before upgrading all the components on the other site or you can upgrade the Site Recovery Manager components on both sites.

When you upgrade all components of one of your sites, it is a best practice to upgrade the Site Recovery Manager components before the Platform Services Controller and the vCenter Server components.

An alternative strategy is to upgrade the Site Recovery Manager components on both sites before upgrading the Platform Services Controller and vCenter Server components.

You can upgrade the ESXi hosts at any time.

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.

Upgrading Site Recovery Manager by Sites

Upgrade the protected site first, so you can perform a disaster recovery on the recovery site if you encounter problems during the upgrade that render the protected site unusable.

1. If you use vSphere Replication, upgrade any additional vSphere Replication servers on the protected site.
2. Upgrade the vSphere Replication appliance on the protected site.
3. Upgrade Site Recovery Manager Server on the protected site.
4. If you use array-based replication, upgrade the storage replication adapters (SRA) on the protected site.
5. (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the protected site.
6. (Optional) Upgrade the ESXi host on the protected site.

7 If you use vSphere Replication, upgrade any additional vSphere Replication servers on the recovery site.

8 Upgrade the vSphere Replication appliance on the recovery site.

9 Upgrade Site Recovery Manager Server on the recovery site.

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

11 (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the recovery site.

12 (Optional) Upgrade the ESXi hosts on the recovery site.

13 Verify the connection between the Site Recovery Manager sites.

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

15 (Optional) Upgrade the virtual hardware and VMware Tools on the virtual machines on the ESXi hosts.

Upgrading Site Recovery Manager by Components

With this strategy, you can decide when to upgrade certain components. For example, you can delay the upgrade of the Platform Services Controller appliances and vCenter Server components or the ESXi hosts. Verify which new functionalities are available with earlier versions of vCenter Server.

1 If you use vSphere Replication, upgrade any additional vSphere Replication servers on the protected site.

2 Upgrade the vSphere Replication appliance on the protected site.

3 Upgrade Site Recovery Manager Server on the protected site.

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

5 If you use vSphere Replication, upgrade any additional vSphere Replication servers on the recovery site.

6 Upgrade the vSphere Replication appliance on the recovery site.

7 Upgrade Site Recovery Manager Server on the recovery site.

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

9 (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the protected site.

10 (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the recovery site.

11 Verify the connection between the Site Recovery Manager sites.

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

13 (Optional) Upgrade the ESXi host on the recovery site.

14 (Optional) Upgrade the ESXi host on the protected site.

15 (Optional) Upgrade the virtual hardware and VMware Tools on the virtual machines on the ESXi hosts.

Update the Site Recovery Manager Virtual Appliance

You use the Site Recovery Manager Appliance Management Interface to apply patches and updates to the virtual appliance.

Prerequisites

- If you are not updating the appliance from an online URL, download the Site Recovery Manager ISO image and mount it on a system in your environment.
- Perform a configuration export by using the VMware Site Recovery Manager 8.5 Configuration Import/Export Tool. See, Chapter 13 Exporting and Importing Site Recovery Manager Configuration Data.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click **Update**.

3 To configure your update settings, click **Edit**.

Option	Description
Online repository	To use the repository, you must copy the `update` folder from the ISO image to a web server and provide the URL of that folder. a Select **Use repository**. b Enter the repository URL, user name (optional), and password (optional).
Downloadable ISO file	Select **Use CD-ROM**.

4 Click **OK**.

5 In the **Available updates** pane, click **Install**.

6 Accept the end-user license agreement, and click **Install**.

After the update is complete, the appliance restarts.

7 Refresh the browser window to reload the Site Recovery Manager Appliance Management Interface.

8 Log in to the Site Recovery Manager Appliance Management Interface as admin.

9 Click **Reconfigure**.

10 Follow the prompts, provide the required information, and click **Finish**.

Migrating from Site Recovery Manager for Windows to the Site Recovery Manager Virtual Appliance

16

To upgrade your Site Recovery Manager 8.3.x for Windows instance to Site Recovery Manager 8.5, you must first migrate your Site Recovery Manager 8.3.x instance from Windows to the Site Recovery Manager 8.3.x Virtual Appliance.

- Migrate from Site Recovery Manager for Windows to Site Recovery Manager Virtual Appliance

  To migrate from Site Recovery Manager 8.3.x for Windows to the Site Recovery Manager 8.3.x Virtual Appliance, you must perform certain operations.

Migrate from Site Recovery Manager for Windows to Site Recovery Manager Virtual Appliance

To migrate from Site Recovery Manager 8.3.x for Windows to the Site Recovery Manager 8.3.x Virtual Appliance, you must perform certain operations.

Note If you are using a federated IPv6 environment and migrate to the Site Recovery Manager Virtual Appliance, you must use the Site Recovery Manager Appliance Management Interface to reconfigure the appliance.

Prerequisites

- Verify that you have upgraded your Site Recovery Manager for Windows instance to version 8.3.x.
- Stop the Site Recovery Manager Server on the Windows host machine.
- Deploy the Site Recovery Manager 8.3.x Virtual Appliance. The appliance can use the same or a different IP address and hostname.

Procedure

1. Log in to the Site Recovery Manager for Windows host machine.
2. Open a command prompt, and navigate to the `bin` folder in the Site Recovery Manager installation directory `%SRM_INSTALL_DIR%\bin`.

3 Run the following script.

```
export-srm-data.bat <export_dir>
```

Note You must have write access to the <export_dir>.

4 When prompted, enter a password.

5 Log in to the Site Recovery Manager Virtual Appliance Management Interface as admin and enable SSH so that you can copy the migration files and connect to the appliance to complete the migration.

6 Transfer the exported directory to the Site Recovery Manager Virtual Appliance host machine.

7 Shut down the Windows host machine.

8 Log in to the Site Recovery Manager Virtual Appliance host machine as root.

9 (Optional) If in a trusted environment, import the user-specific root CA certificates and the Site Recovery Manager Server certificates by using the Site Recovery Manager Appliance Management Interface.

Note The certificates must be in the `.pem` format.

10 Run the following script.

```
/opt/vmware/srm/bin/import-srm-data.sh <export_dir>
```

a (Optional) If in a trusted environment, enter the OS admin password.

b (Optional) If prompted, enter the Platform Services Controller and the vCenter Server thumbprints.

c Enter the vCenter Single Sign-On administrator user name.

d Enter the vCenter Single Sign-On administrator password.

e Enter the root password.

f Enter the password set during the export of the data for the credentials file.

11 (Optional) Configure the DNS settings of the Site Recovery Manager Appliance.

a Log in to the Site Recovery Manager Appliance Management Interface as admin.

b Click **Networking**.

c To configure your network settings, click **Edit**.

d Configure the DNS settings in the **Hostname and DNS** pane.

Menu Item	Description
Obtain DNS settings automatically	Obtains the DNS settings automatically from the network
Enter DNS settings manually	Uses the DNS address settings that you set manually. If you select this option, you must provide the IP addresses for a primary and a secondary DNS server.

e In the **eth0** pane, select the IPv4 or the IPv6 protocol type and configure the IP address settings.

- Configure the IPv4 address settings.

Option	Description
Obtain IPv4 settings automatically	Obtains the IP address for the appliance from the network
Enter IPv4 settings manually	Uses an IPv4 address that you set manually. 1 Enter the IPv4 address. 2 Enter the subnet prefix length. 3 Enter the default IPv4 gateway.

- Configure the IPv6 address settings.

Option	Description
Obtain IPv6 settings automatically using DHCP	Assigns IPv6 addresses to the appliance from the network by using DHCP. **Note** To apply this setting, you must restart the Site Recovery Manager Appliance.
Obtain IPv6 settings automatically using router advertisement	Assigns IPv6 addresses to the appliance from the network by using router advertisement
Use static IPv6 addresses	Uses static IPv6 addresses that you set up manually. 1 Enter the IPv6 address and the subnet prefix length in the address box. 2 To enter additional IPv6 addresses, click **Add**. 3 Enter the default IPv6 gateway.

f Click **Save**.

12 (Optional) Import the Storage Replication Adapters (SRAs) through the Site Recovery Manager Appliance Management Interface.

a Log in to the Site Recovery Manager Appliance Management Interface as admin.

b Click **Storage Replication Adapters**, and click **New Adapter**.

c Click **Upload**, navigate to the directory where you saved the SRA file, and select it.

d When the process finishes, click **Close**.

13 On the **Site Recovery** home tab, select the site pair, and click **Actions > Reconnect**.

   a Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.

   b Select the vCenter Server and the services you want to reconfigure, and click **Next**.

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

Installing Site Recovery Manager to Use with a Shared Recovery Site

17

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, fan-in, or an N:1 configuration.

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 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 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.

Site Recovery Manager also supports shared protected site (one-to-many, fan-out, or 1:N) and many-to-many (N:N) configurations.

Converting One-to-One Site Recovery Manager Configuration 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.

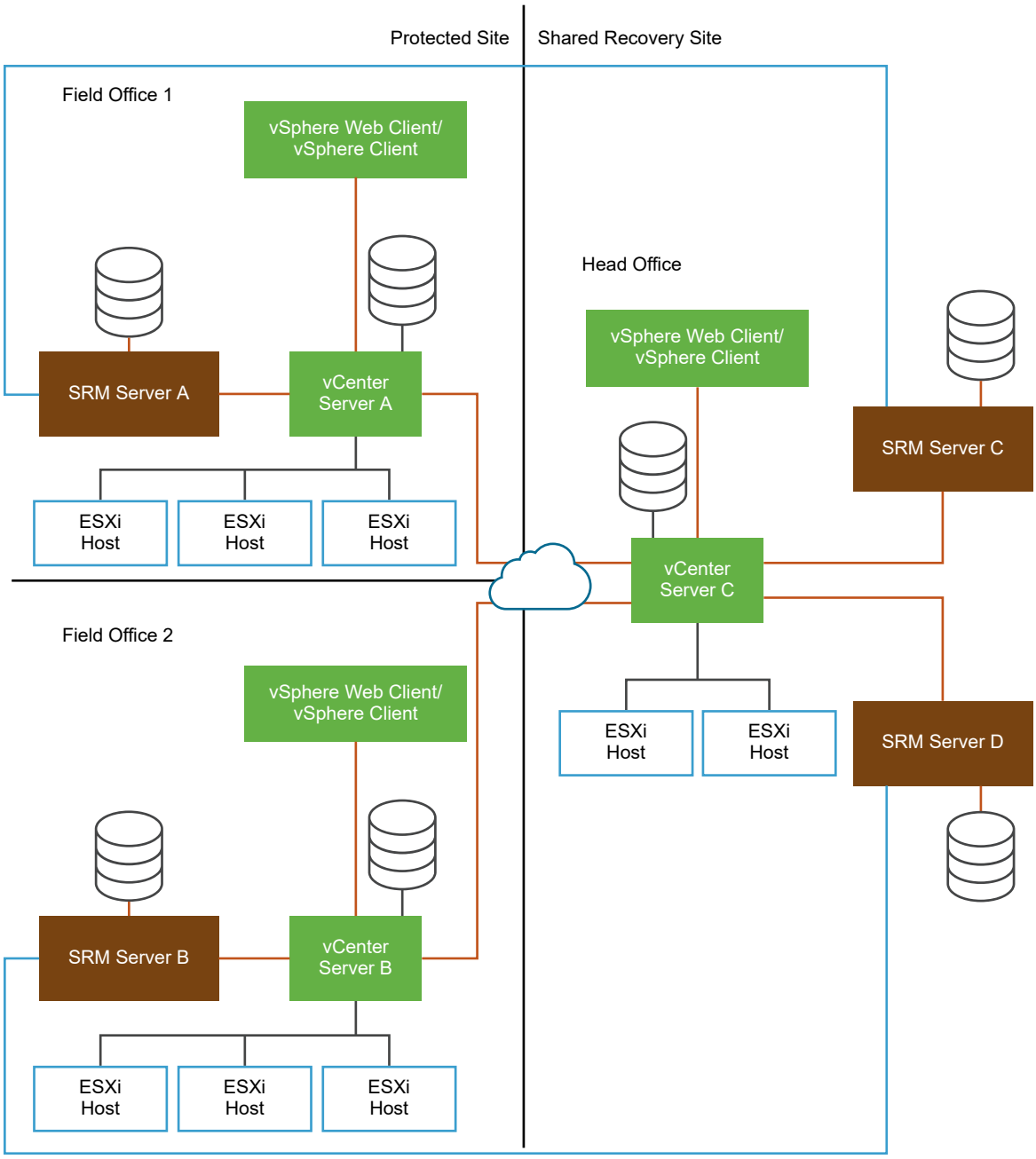
For example, if you installed a one-to-one configuration that uses the default Site Recovery Manager extension ID, you must deploy all subsequent Site Recovery Manager Server pairs with different custom extension IDs.

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 17-1. Using Site Recovery Manager in a Shared Recovery Site Configuration



Read the following topics next:

- Shared Recovery Sites and vCenter Server Deployment Models
- Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration
- Models for Assigning Site Recovery Manager Licenses in a Shared Recovery Site Configuration
- Install Site Recovery Manager In a Shared Recovery Site Configuration
- Upgrade Site Recovery Manager in a Shared Recovery Site Configuration

Shared Recovery Sites and vCenter Server Deployment Models

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

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

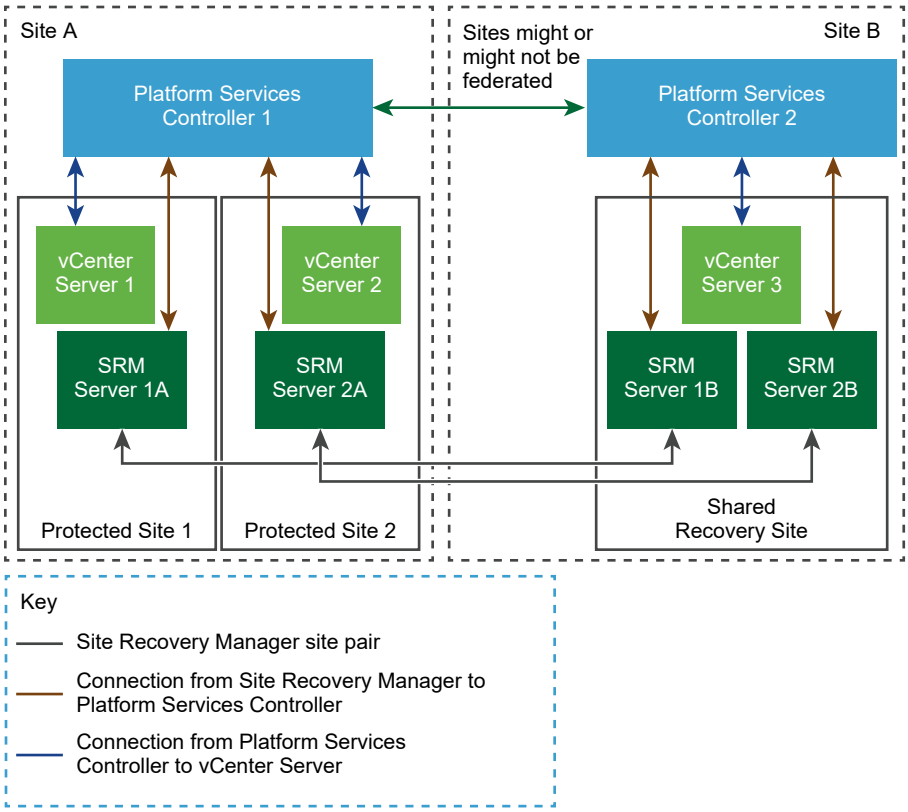
Site Recovery Manager in a Shared Recovery Site Configuration

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

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

In this example, the Site Recovery Manager Server instances on the protected sites connect to a single Platform Services Controller instance that two vCenter Server instances share.

Figure 17-2. Site Recovery Manager in a Shared Recovery Site Configuration



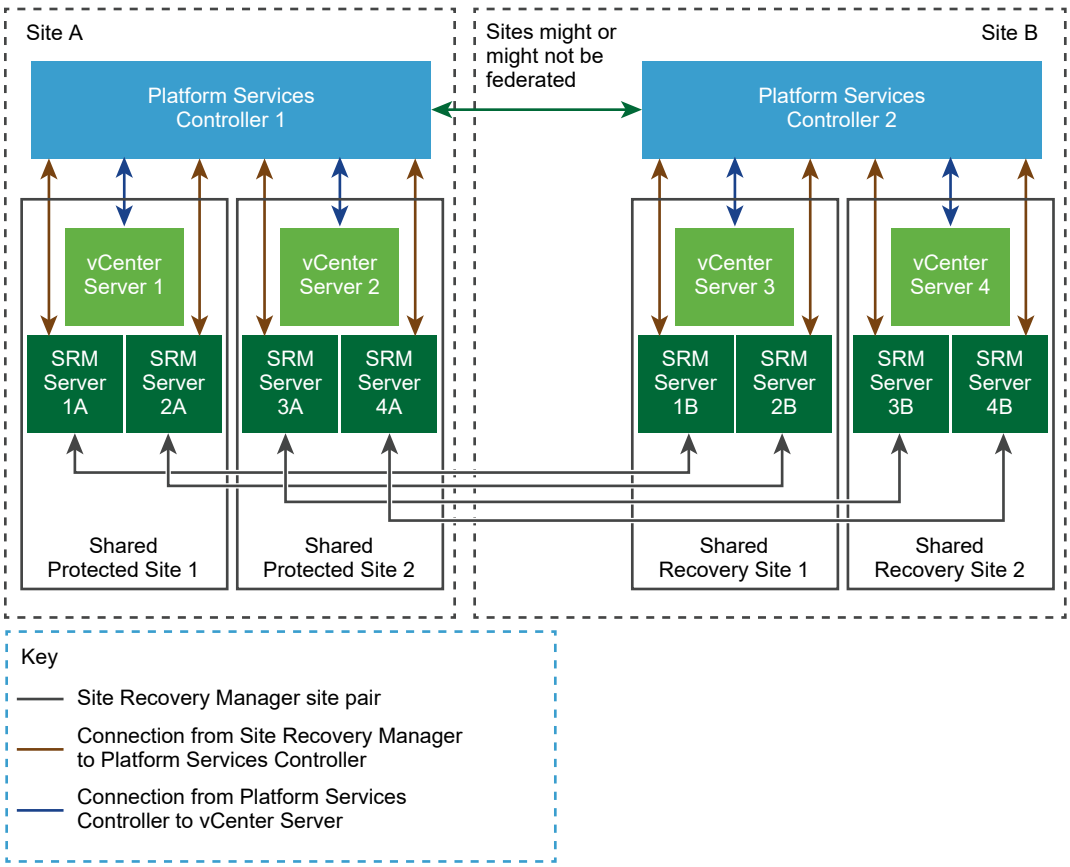
Site Recovery Manager in a Shared Protected Site Configuration

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

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

In this example, two Site Recovery Manager Server instances share a vCenter Server instance on each of two shared protected sites. The vCenter Server instances on both of the shared protected sites share a single Platform Services Controller. On the recovery sites, two Site Recovery Manager Server instances share a vCenter Server instance on each shared recovery site. The vCenter Server instances on both of the shared recovery sites share a single Platform Services Controller.

Figure 17-3. Site Recovery Manager in a Shared Protected Site and Shared Recovery Site Configuration



Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration

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

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

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

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

Problem

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

Cause

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

Solution

1. Increase the `remoteManager.defaultTimeout` timeout value on the Site Recovery Manager Server on the recovery site.

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

   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.

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

   The `vmware-dr.xml` file is located in the `/opt/vmware/srm/conf/` directory.

3. Set the timeout for reading from the vSphere Web Client or the vSphere Client.

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

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

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.

Models for Assigning Site Recovery Manager Licenses in a Shared Recovery Site Configuration

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

In a shared recovery site configuration, you install Site Recovery Manager license keys on each of the protected sites to enable recovery.

- You can install the same license key on the shared recovery site and assign it to the partner Site Recovery Manager Server instance to enable bidirectional operation, including reprotect.
- You can use the same license key for both Site Recovery Manager Server instances in the Site Recovery Manager pair, in the same way as for a one-to-one configuration.
- Alternatively, you can install one Site Recovery Manager license key on the shared recovery site. All Site Recovery Manager Server instances on the shared recovery site share this license. In this configuration, you must ensure that you have sufficient licenses for the total number of virtual machines that you protect on the shared recovery site, for all protected sites.

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

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

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

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

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

Install Site Recovery Manager In a Shared Recovery Site Configuration

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

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

Procedure

1. Use vSphere Replication in a Shared Recovery Site Configuration

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

2. Configure the Site Recovery Manager Appliance on Multiple Protected Sites to Use with a Shared Recovery Site

   You must deploy and configure a Site Recovery Manager Appliance on each protected site to use with a shared recovery site.

3. Configure Multiple Site Recovery Manager Server Instances on a Shared Recovery Site

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

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

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

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

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

6. Configure Placeholders and Mappings in a Shared Recovery Site Configuration

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

Use vSphere Replication in a Shared Recovery Site Configuration

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

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

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

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

Prerequisites

- To use Site Recovery Manager with vSphere Replication, deploy the appropriate version of vSphere Replication on both of the protected and recovery sites before you install Site Recovery Manager Server. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.5* at https://docs.vmware.com/en/Site-Recovery-Manager/8.5/rn/srm-compat-matrix-8-5.html.
- If you have existing vSphere Replication appliances on the sites, you must either upgrade them to the correct version or unregister them from both vCenter Server instances before you install Site Recovery Manager.

Procedure

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

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

Configure the Site Recovery Manager Appliance on Multiple Protected Sites to Use with a Shared Recovery Site

You must deploy and configure a Site Recovery Manager Appliance on each protected site to use with a shared recovery site.

Prerequisites

Deploy the Site Recovery Manager Virtual Appliance and power it on. See *Deploy the Site Recovery Manager Virtual Appliance*.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click the **Summary** tab, and click **Configure appliance**.

3 On the **Platform Services Controller** page, enter the information about the site where you deployed the Site Recovery Manager Appliance.

Menu Item	Description
Address	Enter the host name (in lowercase letters) or IP address of the Platform Services Controller for the vCenter Server with which to register Site Recovery Manager.
PSC port	Accept the default value of `443`, or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS.
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the Platform Services Controller instance.
Password	The password for the specified vCenter Single Sign-On user name.

4 If prompted, click **Connect** to verify the Platform Services Controller certificate.

5 On the **vCenter Server** page, select the vCenter Server instance with which to register the Site Recovery Manager Appliance, and click **Next**.

Caution The drop-down menu includes all the vCenter Server instances that are registered with the Platform Services Controller. In an environment that uses Enhanced Linked Mode, it might also include vCenter Server instances from other Platform Services Controller instances. Make sure that you select the correct vCenter Server instance. After you configure the Site Recovery Manager Appliance, you cannot select a different vCenter Server instance.

6 On the **Name and Extension** page, enter the necessary information to register the Site Recovery Manager with vCenter Server, and select the default Site Recovery Manager extension identifier, or create a custom extension identifier.

a Enter the site name, administrator email address, and local host IP address or name.

Menu Item	Description
Local site name	A name for this Site Recovery Manager site, which appears in the Site Recovery Manager interface. The vCenter Server address is used by default. Use a different name for each Site Recovery Manager instance in the pair.
Administrator email	The email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.
Local host	The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the Site Recovery Manager Appliance detects is not the interface that you want to use. **Note** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

b Select the default Site Recovery Manager extension identifier, or create a custom extension ID for this Site Recovery Manager pair, and click **Next**.

Both Site Recovery Manager instances in a site pair must use the same extension ID.

Menu Item	Description
Default extension ID	Use this option when you deploy Site Recovery Manager in a standard configuration with one protected site and one recovery site.
Custom extension ID	Use this option when you deploy Site Recovery Manager in a shared recovery site configuration, with multiple protected sites and one recovery site. Enter the details for the custom extension ID. ■ Extension ID. A unique identifier. Assign the same identifier to the Site Recovery Manager instances on the protected site and the shared recovery site. ■ Organization. The name of the organization to which this Site Recovery Manager sites

Menu Item	Description
	pair belongs. This name helps to identify Site Recovery Manager pairs in a shared recovery site configuration, especially when multiple organizations use the shared recovery site. ■ Description. An optional description of the Site Recovery Manager pair.

7 On the **Ready to Complete** page, review your settings and click **Finish**.

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

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

The Site Recovery Manager Server instances that you deploy 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 Extension ID.
- This information presumes knowledge of the standard procedure for deploying Site Recovery Manager. See Deploy the Site Recovery Manager Virtual Appliance for information about a standard Site Recovery Manager deployment.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click the **Summary** tab, and click **Configure appliance**.

3 On the **Platform Services Controller** page, enter the information about the site where you deployed the Site Recovery Manager Appliance.

Menu Item	Description
Address	Enter the host name (in lowercase letters) or IP address of the Platform Services Controller for the vCenter Server with which to register Site Recovery Manager.
PSC port	Accept the default value of `443`, or enter a new value if Platform Services Controller uses a different port. Platform Services Controller only supports connections over HTTPS.

Menu Item	Description
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the Platform Services Controller instance.
Password	The password for the specified vCenter Single Sign-On user name.

4 If prompted, click **Connect** to verify the Platform Services Controller certificate.

5 On the **vCenter Server** page, select the vCenter Server instance with which to register the Site Recovery Manager Appliance, and click **Next**.

Caution The drop-down menu includes all the vCenter Server instances that are registered with the Platform Services Controller. In an environment that uses Enhanced Linked Mode, it might also include vCenter Server instances from other Platform Services Controller instances. Make sure that you select the correct vCenter Server instance. After you configure the Site Recovery Manager Appliance, you cannot select a different vCenter Server instance.

6 On the **Name and Extension** page, enter the necessary information to register the Site Recovery Manager with vCenter Server, and select the default Site Recovery Manager extension identifier, or create a custom extension identifier.

a Enter the site name, administrator email address, and local host IP address or name.

Menu Item	Description
Local site name	A name for this Site Recovery Manager site, which appears in the Site Recovery Manager interface. The vCenter Server address is used by default. Use a different name for each Site Recovery Manager instance in the pair.
Administrator email	The email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.
Local host	The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the Site Recovery Manager Appliance detects is not the interface that you want to use. **Note** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

b Create a custom extension ID for this Site Recovery Manager pair as the partner of a Site Recovery Manager Server instance on a protected site, and click **Next**.

Both Site Recovery Manager instances in a site pair must use the same extension ID.

Menu Item	Description
Default extension ID	Use this option when you deploy Site Recovery Manager in a standard configuration with one protected site and one recovery site.
Custom extension ID	Enter the same Site Recovery Manager ID as you provided for the corresponding Site Recovery Manager Server instance on the protected site. Enter the details for the custom extension ID. ■ Extension ID. A unique identifier. Assign the same identifier to the Site Recovery Manager instances on the protected site and the shared recovery site. ■ Organization. The name of the organization to which this Site Recovery Manager sites

Menu Item	Description
	pair belongs. This name helps to identify Site Recovery Manager pairs in a shared recovery site configuration, especially when multiple organizations use the shared recovery site. ■ Description. An optional description of the Site Recovery Manager pair.

7 On the **Ready to Complete** page, review your settings and click **Finish**.

What to do next

Repeat the procedure to configure further Site Recovery Manager Server instances on the shared recovery site, each with a Site Recovery Manager Extension ID that matches a Site Recovery Manager Server instance on another protected site. Each additional Site Recovery Manager Server instance that you deploy and configure on the recovery site connects to the vCenter Server instance. You can connect a maximum of 10 Site Recovery Manager Server instances to a single vCenter Server instance.

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

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

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

Prerequisites

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

Procedure

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

2 Click the **New Site Pair** button.

3 Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.

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

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

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

   If several Site Recovery Manager Server instances are registered with this vCenter Server instance, Site Recovery Manager connects to the Site Recovery Manager Server instance that has the corresponding Site Recovery Manager ID.

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

6 Repeat Step 1 to Step 4 to configure the site pairing for all of the sites that use 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. You can use storage from multiple vendors on the shared recovery site, as long as they correspond to storage that you use on the respective protected sites. You must install the appropriate SRA for each type of storage that you use on the shared recovery site.

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

Prerequisites

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

Procedure

1 Set up storage arrays on the protected sites following the instructions that your storage array provides.

2 Install the appropriate SRAs on Site Recovery Manager Server systems on the protected sites.

3 Install the appropriate SRAs on Site Recovery Manager Server systems on the shared recovery site.

4 Configure the array managers on the protected sites and on the shared recovery sites.

5 Configure the mappings from the resources on the protected sites to resources on the shared recovery site and configure the placeholder datastores.

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 Managing Permissions in a Shared Recovery Site Configuration in *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 *Site Recovery Manager Administration*.

Procedure

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

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

3 On the **Site Pair** tab expand **Configure**, and select the type of resource to configure, **Network Mappings**, **Folder Mappings**, **Resource Mappings**, **Storage Policy Mappings**, and **Placeholder Datastores**.

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.

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

Avoid using the same datastore as the target for vSphere Replication as you use as the placeholder datastore for Site Recovery Manager.

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

Upgrade Site Recovery Manager in a Shared Recovery Site Configuration

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

When you upgrade a Site Recovery Manager installation that uses a shared recovery site, apply the same recommendations for upgrading a standard one-to-one installation of Site Recovery Manager. See Chapter 15 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 must complete all the upgrades to perform recovery.

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 15 Upgrading Site Recovery Manager.
- Evaluate the importance of each protected site, and prioritize the upgrade of the sites accordingly.

Procedure

1. (Optional) Upgrade vCenter Server on the most critical of the protected sites.
2. (Optional) If you use vSphere Replication, upgrade the vSphere Replication appliance that connects to the vCenter Server instance that you upgraded in Step 1.
3. Upgrade the Site Recovery Manager Server instance that connects to the vCenter Server instance that you upgraded in Step 1.
4. (Optional) If you use array-based replication, upgrade the storage replication adapters (SRA) on the Site Recovery Manager Server host machine that you upgraded in Step 3.
5. Repeat Step 1 to Step 4 for each of the protected sites that connect to the shared recovery site.
6. (Optional) Upgrade vCenter Server on the shared recovery site.
7. (Optional) If you use vSphere Replication, upgrade the vSphere Replication appliance on the shared recovery site.
8. Upgrade the Site Recovery Manager Server instance on the shared recovery site that is paired with the first protected site that you upgraded.
9. (Optional) If you use array-based replication, upgrade the SRAs for this Site Recovery Manager Server instance on the shared recovery site.
10. Repeat Step 8 and Step 9 for each of the remaining Site Recovery Manager Server instances on the shared recovery site.
11. (Optional) 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.