VMware Site Recovery Installation and Configuration

Modified on 05 JUL 2024

VMware Site Recovery
Site Recovery Manager 9.0.1
vSphere Replication 9.0.1
Site Recovery Manager 8.8
vSphere Replication 8.8

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 Installation and Configuration

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

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

How does VMware Site Recovery protect virtual machines

1

You can use VMware Site Recovery to implement different types of recovery.

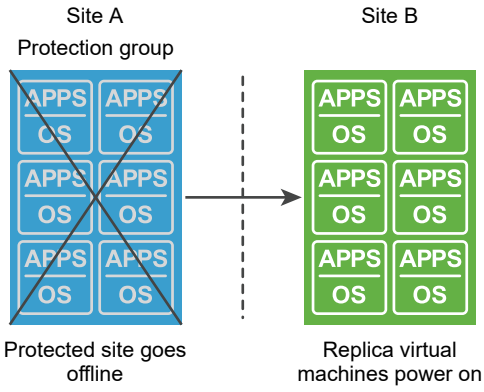
What are protected and recovery sites

In a typical Site Recovery Manager environment, 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.

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.



Virtual machines replicate from site A to site B

Planned migration

You can use VMware Site Recovery for orderly evacuation of virtual machines from a protected site to a 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

Disaster recovery is 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.

In case of site disaster, Site Recovery Manager orchestrates both the recovery process and the replication mechanisms to minimize data loss and system downtime.

- 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.

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.

Read the following topics next:

- Operational Limits of VMware Site Recovery
- Compatibility and Heterogeneous Configurations across the Paired Sites
- Network Ports for VMware Site Recovery

Operational Limits of VMware Site Recovery

Each VMware Site Recovery instance can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries. You must use a VPN connection to access the VMware Site Recovery HTML 5 client.

Protection and Recovery Maximums for VMware Site Recovery

Table 1-1. Protection and Recovery Maximums for VMware Site Recovery

Item	Maximum
Total number of protected virtual machines per NSX-T based SDDC on VMware Cloud™ on AWS	4000 **Note** During the initial activation of VMware Site Recovery, the service is deployed with one vSphere Replication appliance. When you reach 400 incoming replications for the VMware Cloud™ on AWS SDDC, a second vSphere Replication appliance is provisioned automatically. A third vSphere Replication appliance is provisioned when you reach 800 incoming replications, a fourth appliance is provisioned when you reach 1200 incoming replications, a fifth appliance is provisioned when you reach over 1600 replications, and so on. To achieve the 4000 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 on-premises environment, see Chapter 10 Deploying Additional vSphere Replication Servers. To achieve the 4000 virtual machines scale, you must have vSphere 8.0, vSphere Replication 8.6 and later, and VMware Cloud on AWS SDDC version 1.20 and later. vSphere Replication 8.4 and later uses only embedded database and requires additional configuration to enable the support of a maximum of 4000 replications. See https://kb.vmware.com/s/article/2102463.
Maximum number of protected virtual machines per vSphere Replication appliance (through embedded vSphere Replication server).	400
Maximum number of protected virtual machines per vSphere Replication server.	400
Total number of virtual machines per protection group	1500
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Maximum number of protected disks per virtual machine on ESXi 8.0 or earlier version.	64

Table 1-1. Protection and Recovery Maximums for VMware Site Recovery (continued)

Item	Maximum
Maximum number of protected disks per virtual machine on ESXi 8.0 Update 1 or later version.	256
Maximum number of protected disks per host.	8192

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 2600 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 4000 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.

Protection and Recovery Maximums for VMware Site Recovery with enhanced replication

Important Enhanced replication capability is supported only where the target of replication is a site on a VMware Cloud on AWS SDDC version 1.22 with Site Recovery Manager 8.7 or later and vSphere Replication 8.7 or later. Enhanced replication capability requires vCenter Server 8.0u2, and ESXi host 8.0u2 on the target site when the target is an on-premises SDDC..

Table 1-2. Protection and Recovery Maximums for VMware Site Recovery with enhanced replication

Item	Maximum
Total number of protected virtual machines per NSX-T based SDDC on VMware Cloud™ on AWS	4000 **Note** VMware Site Recovery with enhanced replication capability including 1 minute RPO, auto-scaling, and load balancing, scales to a limit of 4000 protected VMs by provisioning additional ESXi hosts to accommodate the workload requirements. Enhanced replication distributes the replications on all hosts available in the target cluster. Re-balancing of the workload occurs automatically every 30 minutes. The number of replicated VMs per host on the target site depends on, but is not limited to the virtual machines disks size, number of disks, change rate, and RPO.
Total number of protected virtual machines per NSX-T based SDDC on VMware Cloud™ on AWS with vSphere Replication 9.0.1 and later	5000 **Note** VMware Site Recovery with enhanced replication capability including 1 minute RPO, auto-scaling, and load balancing, scales to a limit of 5000 protected VMs by provisioning additional ESXi hosts to accommodate the workload requirements. Enhanced replication distributes the replications on all hosts available in the target cluster. Re-balancing of the workload occurs automatically every 30 minutes. The number of replicated VMs per host on the target site depends on, but is not limited to the virtual machines disks size, number of disks, change rate, and RPO.
Total number of virtual machines per protection group	1500
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Maximum number of protected disks per virtual machine on ESXi 8.0 or earlier version.	64
Maximum number of protected disks per virtual machine on ESXi 8.0 Update 1 or later version.	256
Maximum number of protected disks per host.	8192
RPO	1 min, 5 min, 30 min, 60 min, 90 min, 120 min

Protection and Recovery Maximums for VMware Site Recovery on VMware Cloud™ on AWS Outposts

With VMware Site Recovery on VMware Cloud™ on AWS Outposts you can plan, test, and run the recovery of virtual machines between a protected vCenter Server on-premises site and a recovery vCenter Server site on VMware Cloud on AWS Outposts and the reverse, between a protected vCenter Server site on VMware Cloud on AWS Outpost SDDC and a recovery vCenter Server site on VMware Cloud on AWS SDDC and the reverse, and between vCenter Server sites on two VMware Cloud on AWS Outposts SDDCs.

Table 1-3. Protection and Recovery Maximums for VMware Site Recovery on VMware Cloud™ on AWS Outposts

Item	Maximum
Total number of protected virtual machines per SDDC on VMware Cloud™ on AWS Outposts	4000
Maximum number of protected virtual machines per vSphere Replication appliance (through embedded vSphere Replication server).	400
Maximum number of protected virtual machines per vSphere Replication server.	400
Total number of virtual machines per protection group	1000
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Maximum number of protected disks per virtual machine on ESXi 8.0 or earlier version.	64
Maximum number of protected disks per virtual machine on ESXi 8.0 Update 1 or later version.	256
Maximum number of protected disks per host.	8192
RPO	5 min, 30 min, 60 min, 90 min, 120 min

Compatibility and Heterogeneous Configurations across the Paired Sites

Because the protected and recovery sites are often in different locations, some components on the protected site can be of a different type to their counterparts on the recovery site.

VMware Site Recovery is compatible with N-1 version of Site Recovery Manager and vSphere Replication on the paired on-premises site. For example, if the current version of Site Recovery Manager and vSphere Replication on VMware Site Recovery is 8.6, the supported versions for the paired on-premises site is 8.5 and later.

VMware Site Recovery is compatible with N-2 version of VMware vSphere and ESXi on the paired on-premises site. For example, if the current version of VMware vSphere on VMware Site Recovery is 8.0, the supported versions for the paired on-premises site go back to VMware vSphere 6.7 and ESXi 6.7.

Although components can be different on each site, you must use the types and versions of these components that Site Recovery Manager supports.

For more information about compatibility, see VMware Product Interoperability Matrices.

Table 1-4. Heterogeneity of Site Recovery Manager Components Between Sites

Component	Heterogeneous or Identical Installations
Site Recovery Manager Server	Must be a supported version on both sites.
vSphere Replication	Must be a supported 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.
Site Recovery Manager database	Can be different on each site. You can use different versions of the same type of database on each site.
Host operating system of the Site Recovery Manager Server installation	Can be different on each site. You can run different versions of the host operating system and the host operating system can run in different locales on each site.
Host operating system of the vCenter Server installation	Can be different on each site. You can run different versions of the host operating system and the host operating system can run in different locales on each site.

Network Ports for VMware Site Recovery

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

The components that make up the VMware Site Recovery service, namely vCenter Server, vSphere Web Client, Site Recovery Manager Server, the vSphere Replication appliance, and vSphere Replication servers, require different ports to be open. You must ensure that all the required network ports are open for VMware Site Recovery to function correctly. Site Recovery Manager and vSphere Replication do not have public IP addresses. You must use a VPN or Direct Connect to access the HTML 5 user interface. It is recommended to use the private IP address as a Resolution Address for vCenter Server FQDN when using a VPN.

When creating Management Gateway Firewall rules for Inbound access to vCenter Server in a VMware Cloud on AWS SDDC, do not use **Any** as source for the traffic. VMware Cloud might automatically deactivate access to such SDDC for security reasons. Create a User Defined Group with members of some subset of IP addresses used in your on-premises SDDC instead.

Figure 1-1. Site Recovery Manager for Windows at the on-premises SDDC

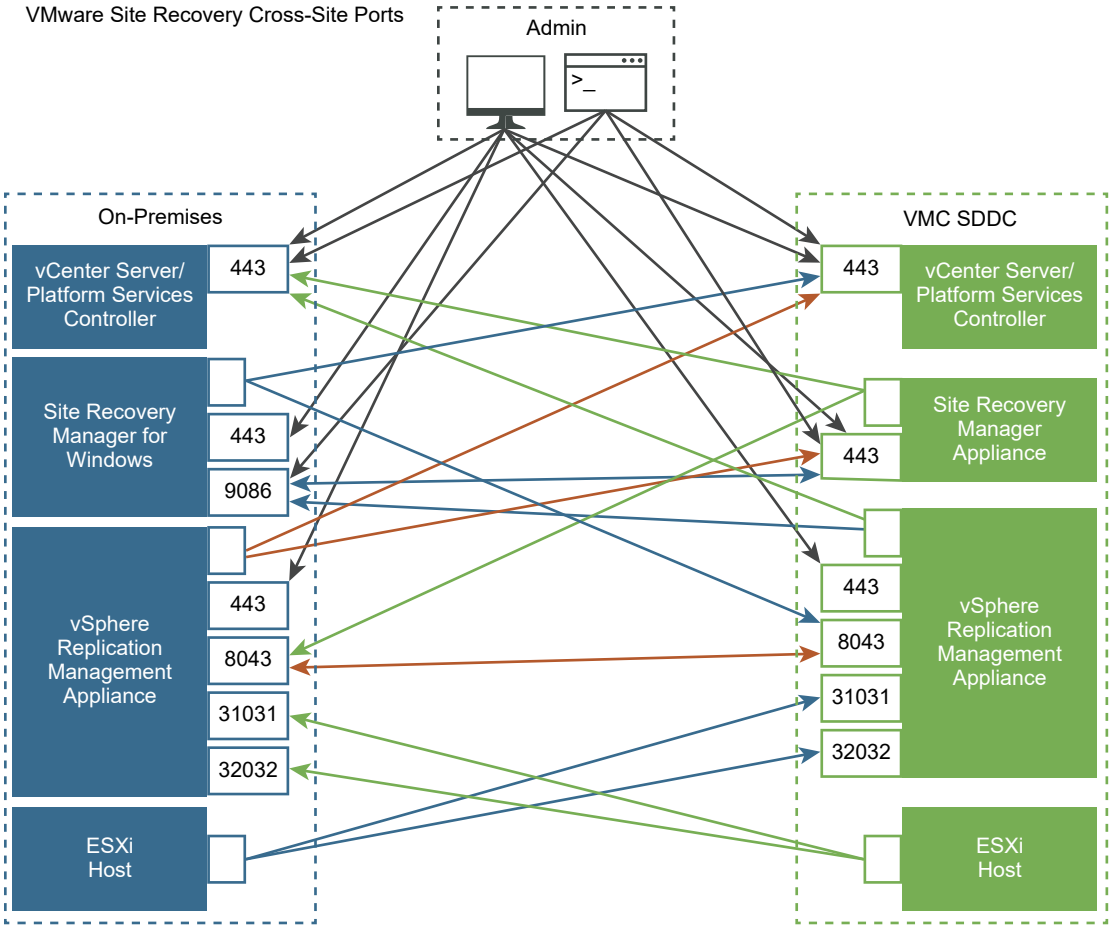
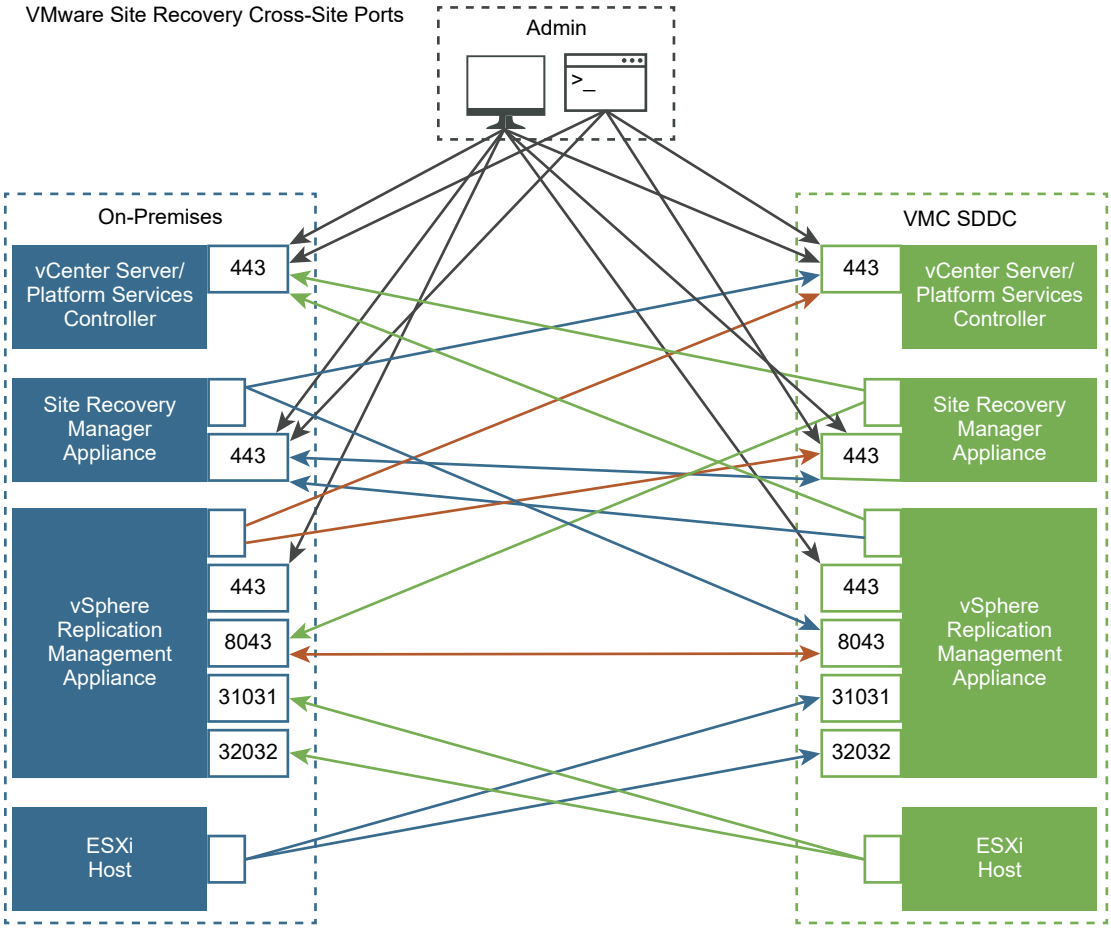


Figure 1-2. Site Recovery Manager Virtual Appliance at the on-premises SDDC



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

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

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

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 network ports

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

Default Port	Protocol or Description	Source	Target	Endpoints or Consumers
443	HTTPS	Site Recovery Manager	vCenter Server	Default SSL Web Port for incoming TCP traffic.
443	HTTPS	Site Recovery Manager HTML 5 user interface	Site Recovery Manager	Default port for the Site Recovery Manager HTML 5 user interface.

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

Site Pairing Port Requirements

Port	Protocol	Source	Target	Description
9086	HTTPS	vCenter Server	Site Recovery Manager Server for Windows	vCenter Server and target Site Recovery Manager for Windows communication.
9086	HTTPS	Site Recovery Manager Server for Windows	Site Recovery Manager Server for Windows on target site	Bi-directional communication between Site Recovery Manager for Windows servers.
443	HTTPS	vCenter Server	Site Recovery Manager Server Appliance	vCenter Server and target Site Recovery Manager Appliance communication.
443	HTTPS	Site Recovery Manager Server Appliance	Site Recovery Manager Server Appliance on target site	Bi-directional communication between Site Recovery Manager Appliance 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	The ESXi host of the replicated VM on the source site	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	The ESXi host of the replicated VM 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.
31031	Unencrypted replication traffic	The ESXi host of the replicated VM on the source site	All ESXi hosts in the cluster of the target datastore.	Required for replications in Scale-out mode.
32032	TCP	The ESXi host of the replicated VM on the source site	All ESXi hosts in the cluster of the target datastore.	Required for replications in Scale-out mode.
8043	HTTPS	vSphere Replication appliance on either site	vSphere Replication appliance on either site	Management traffic between vSphere Replication appliances.
8043	HTTPS	Site Recovery Manager	vSphere Replication appliance on the recovery and protected sites	Management traffic between Site Recovery Manager instances and vSphere Replication appliances.

vSphere Replication appliance network ports

Port	Protocol or Description	Source	Target	Endpoints or Consumers
443	TCP	vSphere Replication appliance	Remote Lookup Service	All calls to the remote Lookup Service.
443	HTTPS	Site Recovery HTML 5 user interface	vSphere Replication appliance	Default port for the Site Recovery HTML 5 user interface when you open it from the vSphere Replication appliance.

Port	Protocol or Description	Source	Target	Endpoints or Consumers
443	HTTPS	Site Recovery HTML 5 user interface	Local and remote vCenter Server or all vCenter Server instances in Enhanced Linked Mode with a registered vSphere Replication.	Default port for the Site Recovery HTML 5 user interface when you open it from the vSphere Replication appliance.
443	HTTPS	Site Recovery HTML 5 user interface	Local and remote Platform Services Controllerinstances or all Platform Services Controller instances in Enhanced Linked Mode with a registered vSphere Replication.	Default port for the Site Recovery HTML 5 user interface when you open it from the vSphere Replication appliance.
443	TCP	Site Recovery HTML 5 user interface	Remote Site Recovery Manager appliance	TCP port 443 must be open when you access the Site Recovery HTML 5 user interface from the vSphere Replication appliance.
443	HTTP	vSphere Replication server in the vSphere Replication appliance	ESXi host (intra-site)	Traffic between the vSphere Replication server and the ESXi hosts on the same site.
443	HTTP	ESXi host (intra-site)	vSphere Replication server in the vSphere Replication appliance	Traffic between the ESXi host and the vSphere Replication server on the same site.
443	TCP	vSphere Replication appliance	Local and remote vCenter Server	All management traffic to the vCenter Server.
443	TCP	vSphere Replication appliance	https://vcsa.vmware.com	Customer Experience Improvement Program (CEIP) for vSphere Replication.
9084	HTTP	vSphere Replication appliance	Local vCenter Server	Used for uploading the hbr agent VIB to vCenter Server during the installation of the VIB file to the source ESXi hosts.

Port	Protocol or Description	Source	Target	Endpoints or Consumers
902	TCP and UDP	vSphere Replication server in the vSphere Replication appliance on secondary site	ESXi host (intra-site) on secondary site	Used by vSphere Replication servers to send replication traffic to the destination ESXi hosts.
5480	HTTPS	Browser	vSphere Replication appliance	vSphere Replication virtual appliance management interface (VAMI) Web UI. Required only for on-premises site, not required for VMware Cloud on AWS site.
8043	SOAP	vSphere Replication appliance	vSphere Replication appliance	Inter-site communication from the vSphere Replication Management servers of the primary and the secondary site.
8043	SOAP	vCenter Server	vSphere Replication appliance	Intra-site communication used for SDRS.
8123	SOAP	vSphere Replication appliance	vSphere Replication server	Intra-site management traffic from the vSphere Replication Management server to additional vSphere Replication servers in the environment.

Port	Protocol or Description	Source	Target	Endpoints or Consumers
31031	Initial and ongoing replication traffic	ESXi host on source site	vSphere Replication server in the vSphere Replication appliance on the secondary site or an external vSphere Replication server on the secondary site	Initial and outgoing replication traffic from the ESXi host at the source site to the vSphere Replication appliance or vSphere Replication server at the target site.
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.

vSphere Replication server network ports

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

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

Port	Protocol or Description	Source	Target	Endpoints or Consumers
31031	Initial and ongoing replication traffic	ESXi host on source site	vSphere Replication server	From the ESXi host at the protected site to the vSphere Replication appliance or vSphere Replication server at the recovery site.
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.

Site Recovery Manager Authentication

2

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

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

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

Solution Users and Site Recovery Manager Site Pairing

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

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

Site Recovery Manager SSL/TLS Server Endpoint Certificates

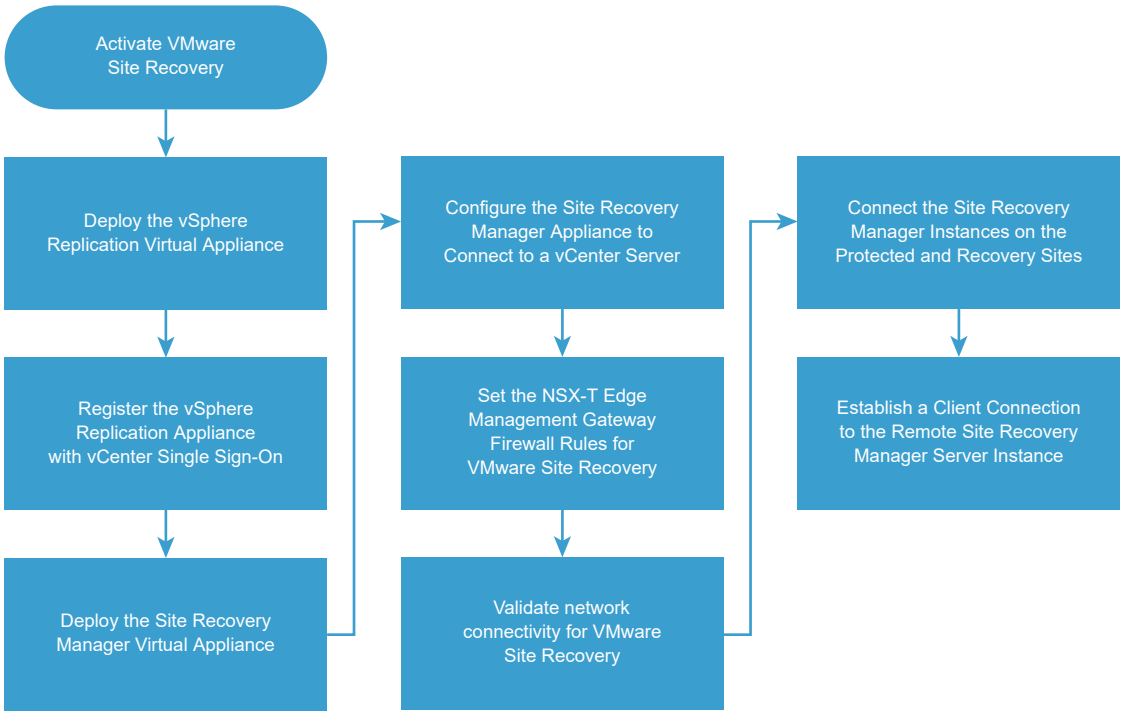
Site Recovery Manager requires an SSL/TLS certificate for use as the endpoint certificate for all TLS connections established to Site Recovery Manager. The Site Recovery Manager server endpoint certificate is separate and distinct from the certificate that is generated during the creation and registration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

For information about the Site Recovery Manager SSL/TLS endpoint certificate, see Creating SSL/TLS Server Endpoint Certificates for Site Recovery Manager in the *Site Recovery Manager Installation and Configuration* guide.

How do I set up VMware Site Recovery in an on-premises to VMware Cloud on AWS environment

3

This use case provides instructions on the most popular scenario for setting up VMware Site Recovery in your environment - with an on-premises protected site and a VMware Cloud on AWS SDDC recovery site.



Prerequisites

Prepare your environment and sign up for cloud services. See Before you begin with VMware Site Recovery.

Procedure

1 Activate VMware Site Recovery at the Recovery Site

To use the VMware Site Recovery service, you must activate VMware Site Recovery at the recovery site on VMware Cloud™ on AWS.

2 Deploy the vSphere Replication Virtual Appliance

vSphere Replication is distributed as an OVF virtual appliance.

3 Register the vSphere Replication Appliance with vCenter Single Sign-On

You must configure the vSphere Replication Appliance to connect to a vCenter Server on the on-premises site.

4 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 at the on-premises site.

5 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.

6 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 on-premises data center and the Management Gateway. After the initial firewall rules configuration, you can add, edit or delete any rules as needed.

7 Validate Network Connectivity for VMware Site Recovery

Use the VMware Cloud on AWS console **Troubleshooting** tab tests to check that all required network connectivity from your VMware Cloud on AWS SDDC to the remote site is in place.

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

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

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

After you connect the Site Recovery Manager Server instances, you must establish a client connection to the remote Site Recovery Manager Server instance.

Activate VMware Site Recovery at the Recovery Site

To use the VMware Site Recovery service, you must activate VMware Site Recovery at the recovery site on VMware Cloud™ on AWS.

Prerequisites

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

Procedure

1. Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.
2. Click your SDDC, and then click **Integrated Services**.
3. Select Site Recovery and click **Activate**.
4. Read the information on the Activate Site Recovery page and click **Activate**.
5. After the service activates, click **Download on-premises components**.

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

Results

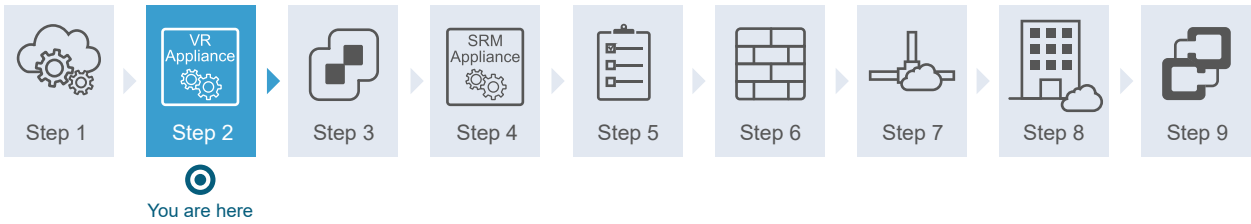
VMware Site Recovery is activated on your SDDC on VMware Cloud on AWS.

What to do next

Deploy the vSphere Replication virtual appliance at the on-premises site.

Deploy the vSphere Replication Virtual Appliance

vSphere Replication is distributed as an OVF virtual appliance.



You deploy the vSphere Replication appliance by using the standard vSphere OVF deployment wizard. Only one vSphere Replication appliance is deployed on each vCenter Server. You can deploy additional vSphere Replication Servers.

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

Prerequisites

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

Procedure

1. Log in to the vSphere Client on the protected site.
2. On the home page, select **Hosts and Clusters**.
3. Right-click a host and select **Deploy OVF template**.
4. Provide the location of the OVF file from which to deploy the vSphere Replication appliance, and click **Next**.
   - Select **URL** and provide the URL to deploy the appliance from an online URL.
   - If you downloaded and mounted the vSphere Replication ISO image on a system in your environment, select **Local file > Browse** and navigate to the `\bin` directory in the ISO image, and select the `vSphere_Replication_OVF10.ovf`, `vSphere_Replication-system.vmdk`, and `vSphere_Replication-support.vmdk` files.
5. Accept the name, select or search for a destination folder or data center for the virtual appliance, and click **Next**.

   You can enter a new name for the virtual appliance. The name must be unique within each vCenter Server virtual machine folder.
6. Select a cluster, host, or resource pool where you want to run the deployed template, and click **Next**.
7. Review the virtual appliance details and click **Next**.
8. Accept the end-user license agreements (EULA) and click **Next**.

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

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

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

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

vSphere Replication supports both DHCP and static IP addresses. You can also change network settings by using the VRMS Appliance Management Interface after installation.

12 On the **Customize template** page, enter one or more NTP server host names or IP addresses.

13 Set the password for the root account and enter the hostname or IP address of at least one NTP server.

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.

14 Click **Next**.

15 To check the integrity of the vSphere Replication appliance binary files, select the **File Integrity Flag** check box.

If the vSphere Replication appliance detects changes to the binary files, it sends log traces to the syslog.

16 (Optional) You can modify the default Network Properties.

Setting	Action
Host Network IP Address Family	Select the Network IP address family. The options are IPv4 or IPv6.
Host Network Mode	Select the host network mode. The options are static, DHCP, or autoconf. Autoconf is avalable only for IPv6.
Default Gateway	Enter the default gateway address for this VM.
Domain Name	Enter the domain name of this VM.
Domain Search Path	Enter the domain search path for this VM. Use comma or space separated domain names.
Domain Name Servers	The domain name server IP Addresses for this VM. Use commas to separate the IP addresses.
Network 1 IP Address	The IP address for the default Ethernet adapter.
Network 1 Netprefix	The prefix for the default Ethernet adapter.

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

The vSphere Replication appliance is deployed.

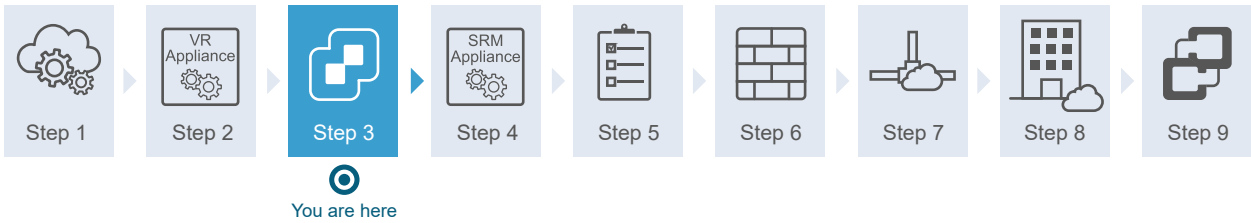
18 Power on the vSphere Replication appliance. Take a note of the IP address of the appliance and log out of the vSphere Client.

What to do next

Register the vSphere Replication appliance with the vCenter Single Sign-On service.

Register the vSphere Replication Appliance with vCenter Single Sign-On

You must configure the vSphere Replication Appliance to connect to a vCenter Server on the on-premises site.



After you deploy the vSphere Replication appliance, you use the virtual appliance management interface (VRMS Appliance Management Interface) to connect the vSphere Replication Management Server with the vCenter Server on the on-premises site.

If you do not connect vSphere Replication with the vCenter Server on the target site, vSphere Replication cannot operate as expected. In addition, storage DRS does not detect the replicated data that vSphere Replication stores on the target site and might destroy it.

Prerequisites

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

Procedure

1 Log in to the VRMS Appliance Management Interface as admin.

The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.

2 Click on **Summary**, then click **Configure Appliance**.

3 On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication 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 vSphere Replication.
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 vSphere Replication 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 vSphere Replication Appliance, you cannot select a different vCenter Server instance.

6 On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.

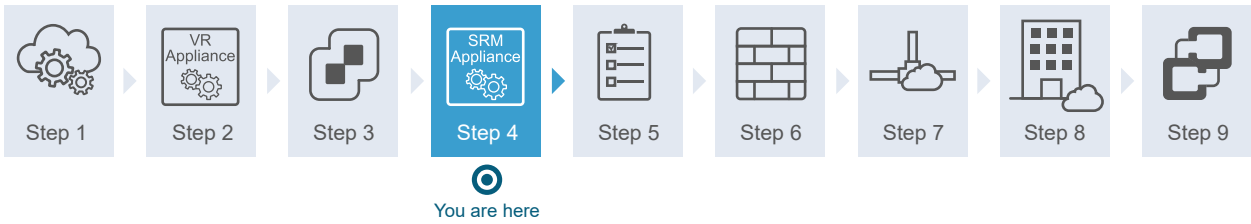
Menu Item	Description
Site name	A name for this vSphere Replication site, which appears in the vSphere Replication interface. The vCenter Server address is used by default. Use a different name for each vSphere Replication instance in the pair.
Administrator email	The email address of the vSphere Replication administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for vSphere Replication events.

Menu Item	Description
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 vSphere Replication 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.
Extension ID	The unique identifier of the vSphere Replication Appliance. The Extension ID is not customizable.
Storage Traffic IP	The IP address of a VM NIC to be used by the vSphere Replication Server for incoming replication data.

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

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 at the on-premises 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 Web Client or the vSphere 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 a 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 host name.

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, choose one of the following options: ■ If you have assigned a static IP address to the appliance, enter an FQDN for that IP. ■ If you don't 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 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) You can modify the default Network Properties.

Setting	Action
Host Network IP Address Family	Select the Network IP address family. The options are IPv4 or IPv6.
Host Network Mode	Select the host network mode. The options are static, DHCP, or autoconf. Autoconf is avalable only for IPv6.
Default Gateway	Enter the default gateway address for this VM.
Domain Name	Enter the domain name of this VM.
Domain Search Path	Enter the domain search path for this VM. Use comma or space separated domain names.
Domain Name Servers	The domain name server IP Addresses for this VM. Use commas to separate the IP addresses.
Network 1 IP Address	The IP address for the default Ethernet adapter.
Network 1 Netprefix	The prefix for the default Ethernet adapter.

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

The Site Recovery Manager Appliance is deployed.

17 Power on the Site Recovery Manager Appliance.

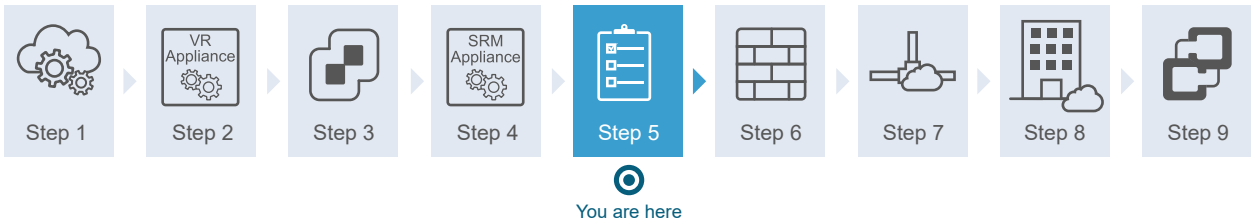
18 Take a note of the IP address of the appliance and log out of the vSphere Web Client or the vSphere Client.

What to do next

Configure the Site Recovery Manager Appliance instance to connect to vCenter Server at the on-premises site.

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
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**.

What to do next

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

Creating Private DNS Entries for VMware Site Recovery Endpoints on VMware Cloud on AWS US GovCloud SDDC

To ensure a proper network communication between your on-premises SDDC and the VMware Cloud on AWS US GovCloud SDDC, you must add DNS entries to your local DNS server.

If you have an existing on-premises SDDC and you want to use VMware Cloud on AWS US GovCloud SDDC as a recovery site, you must establish a private, secure connection between the two sites. You can secure the connection by using a VPN. To ensure that there is a network communication between the on-premises components and the VMware Site Recovery components on the VMware Cloud on AWS US GovCloud SDDC, you must configure your DNS servers with FQDNs and the IP addresses of the components running on the VMware Cloud on AWS US GovCloud SDDC. This topic provides information on how to capture the required information in a VMware Cloud on AWS US GovCloud SDDC.

Prerequisites

Verify that you have activated VMware Site Recovery on your VMware Cloud on AWS US GovCloud SDDC.

Procedure

1 Log in to https://www.vmc-us-gov.vmware.com/.

2 Click your SDDC and the click **Settings**.

3 Click **Open vCenter**, enter your credentials, and click **Site Recovery**.

4 Record the FQDN of the Site Recovery Manager appliance and the vSphere Replication appliance.

5 Click **VMs and Templates** and expand **Management VMs**.

6 Locate the Site Recovery Manager virtual machine and the vSphere Replication virtual machine.

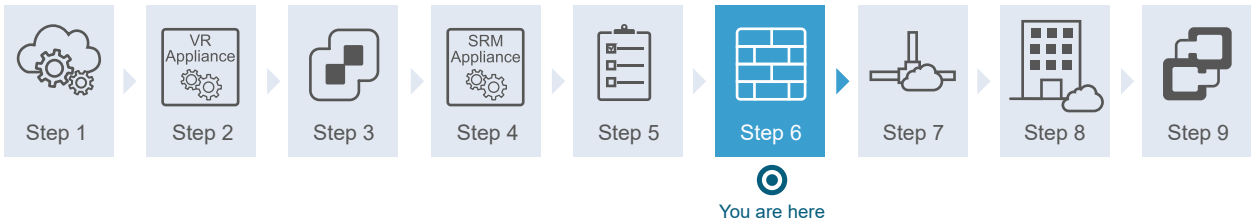
   a Click the Site Recovery Manager virtual machine and record the private IP address.

   b Click the vSphere Replication virtual machine and record the private IP address.

7 Create DNS entries for these components on your local DNS server.

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 on-premises data center and the Management Gateway. After the initial firewall rules configuration, you can add, edit or delete any rules as needed.



Prerequisites

- Verify that you have activated VMware Site Recovery on the SDDC.

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 may 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. ■ **ESXi** to allow traffic from your SDDC's ESXi. ■ 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. ■ **ESXi** to allow traffic to your SDDC's ESXi hosts. ■ 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. ■ VMware Site Recovery ESXi LWD applies only to ESXi 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
Remote network to ESXi (VM Replication scale-out)	User-Defined Group that includes the remote ESXi IP addresses / infrastructure subnet.	ESXi	**VMware Site Recovery ESXi LWD**	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

Name	Source	Destination	Service	Action
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
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
ESXi (VM Replication scale-out) to remote network	ESXi	Any or User-Defined Group that includes the remote ESXi IP addresses / infrastructure subnet.	**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

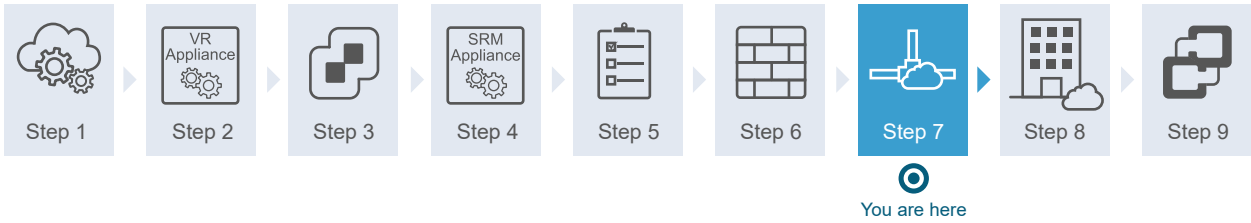
6 Click **Publish**.

Results

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

Validate Network Connectivity for VMware Site Recovery

Use the VMware Cloud on AWS console **Troubleshooting** tab tests to check that all required network connectivity from your VMware Cloud on AWS SDDC to the remote site is in place.



You can use the tests both during the initial setup of VMware Site Recovery, and to troubleshoot connectivity issues during a day-to-day management. In addition to network connectivity, the DNS must also be operating properly. Use fully qualified domain names (FQDN) to test the DNS as well.

Prerequisites

Verify that VMware Site Recovery is activated.

Procedure

1. Log in to the VMware Cloud on AWS console at https://vmc.vmware.com/.
2. Click **View Details** for your SDDC.
3. Click the **Troubleshooting** tab.
4. From the Use Case drop down menu, select **Site Recovery**.

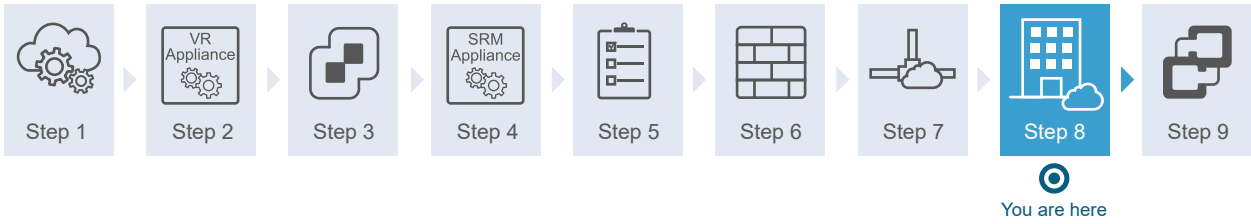
   The VMware Site Recovery tests are shown. Tests are organized in groups according to the input needed for each group.
5. In the **Input** column, enter the required input for each test you want to run.
6. Run one or more tests.
   - To run all tests, click **Run All**.
   - To run a particular test group, click **Run Group** to the right of the group listing.
   - To run an individual test, expand the test group and click **Run** next to the individual test.

Results

The status of each test is displayed as it runs. When a test has finished, you can expand the test to see details of the test results.

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

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



Prerequisites

- Verify that you have activated VMware Site Recovery at the VMware Cloud on AWS SDDC.
- Verify that you have installed Site Recovery Manager Server and vSphere Replication instances at the on-premises 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**.
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 VMware Site Recovery **Home** tab.

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

After you connect the Site Recovery Manager Server instances, you must establish a client connection to the remote Site Recovery Manager Server instance.

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

Prerequisites

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

Procedure

1. Connect to vSphere Web Client on one of the sites, and select **Site Recovery > Open VMware Site Recovery**.
2. On the 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 **Login**.

How do I set up VMware Site Recovery in a VMware Cloud on AWS to VMware Cloud on AWS environment

4

This use case provides instructions for setting up VMware Site Recovery with a VMware Cloud on AWS SDDC protected site and a VMware Cloud on AWS SDDC recovery site.

Prerequisites

Prepare your environment and sign up for cloud services. See Before you begin with VMware Site Recovery.

Procedure

1 Activate VMware Site Recovery

To use the VMware Site Recovery service, you must activate VMware Site Recovery at the protected and the recovery sites on VMware Cloud™ on AWS.

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 data center and the Management Gateway. After the initial firewall rules configuration, you can add, edit or delete any rules as needed.

3 Validate Network Connectivity for VMware Site Recovery

Use the VMware Cloud on AWS console **Troubleshooting** tab tests to check that all required network connectivity from your VMware Cloud on AWS SDDC to the remote site is in place.

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

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

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

After you connect the Site Recovery Manager Server instances, you must establish a client connection to the remote Site Recovery Manager Server instance.

Activate VMware Site Recovery

To use the VMware Site Recovery service, you must activate VMware Site Recovery at the protected and the recovery sites on VMware Cloud™ on AWS.

Prerequisites

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

Procedure

1. Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.
2. Click your SDDC, and then click **Integrated Services**.
3. Select Site Recovery and click **Activate**.
4. Read the information on the Activate Site Recovery page and click **Activate**.
5. Repeat the procedure at the second VMware Cloud on AWS SDDC.

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 data center and the Management Gateway. After the initial firewall rules configuration, you can add, edit or delete any rules as needed.

Prerequisites

- Verify that you have activated VMware Site Recovery on the SDDC.

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 the 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 may 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. ■ **ESXi** to allow traffic from your SDDC's ESXi. ■ 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. ■ **ESXi** to allow traffic to your SDDC's ESXi. ■ 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. ■ VMware Site Recovery ESXi LWD applies only to ESXi 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)	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
Remote network to ESXi (VM Replication scale-out)	User-Defined Group that includes the remote ESXi IP addresses / infrastructure subnet.	ESXi	**VMware Site Recovery ESXi LWD**	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

Name	Source	Destination	Service	Action
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
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
ESXi (VM Replication scale-out) to remote network	ESXi	Any or User-Defined Group that includes the remote ESXi IP addresses / infrastructure subnet.	**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**.

7 Repeat the procedure at the second VMware Cloud on AWS SDDC.

Results

The firewall rules are shown in the Management Gateway Edge Firewall list.

When Direct Connect Private Virtual Interface Is Attached to a VMware Cloud on AWS Environment, You Cannot Use VPN Connectivity for Replication Traffic

When Direct Connect private virtual interface is attached to a VMware Cloud on AWS environment, you cannot use VPN connectivity for replication traffic communication from this environment.

Problem

When you have Direct Connect private virtual interface attached to a VMware Cloud on AWS environment, you cannot use VPN connectivity for replication traffic communication from this environment.

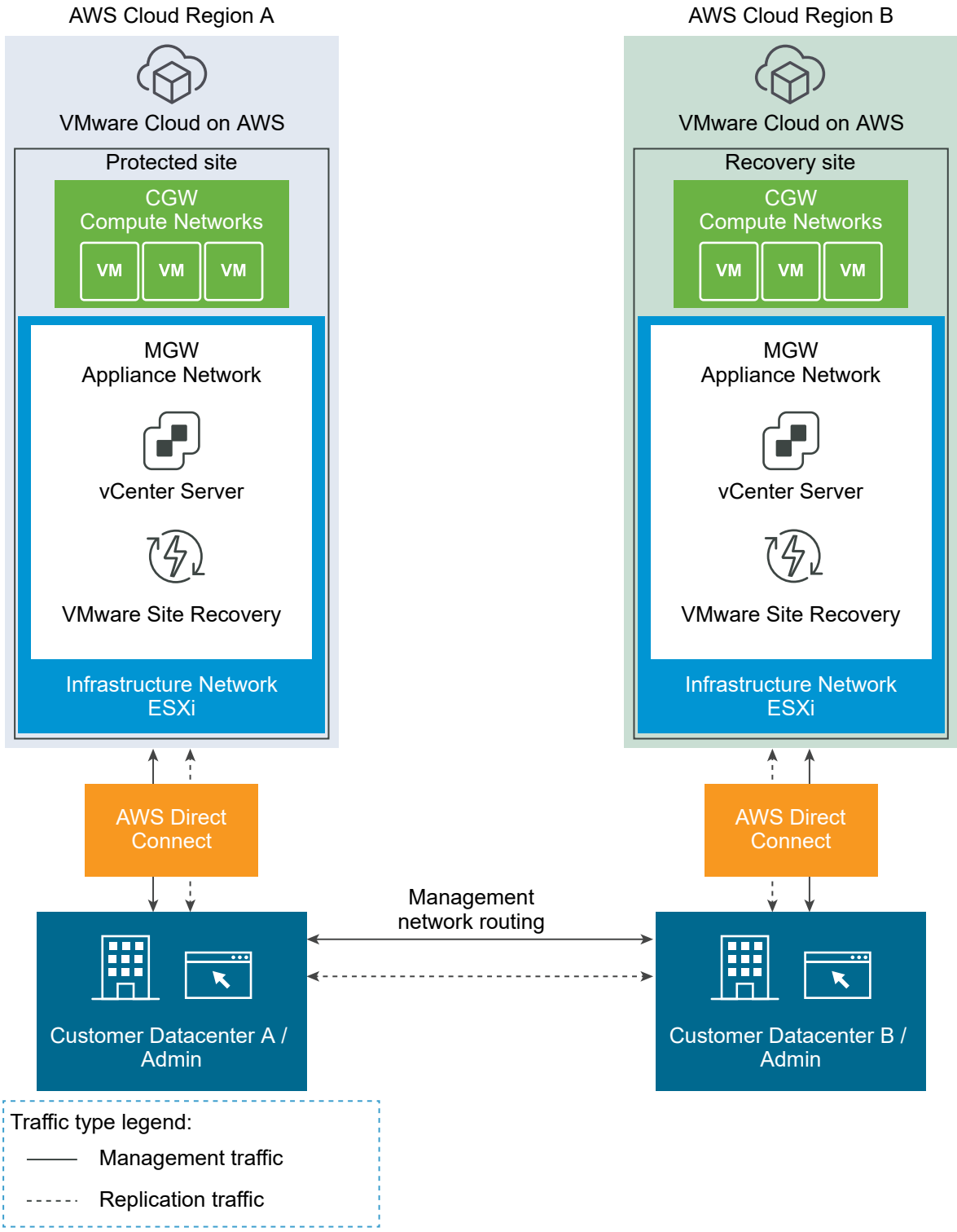
Cause

With private virtual interface, the only possible external connectivity option for ESXi traffic is Direct Connect. If there is a VPN between the source and the target sites, the ESXi to vSphere Replication appliance traffic uses Direct Connect path, while the return traffic uses VPN path resulting in an asymmetric routing. The firewall in the VMware Cloud on AWS environment drops such traffic.

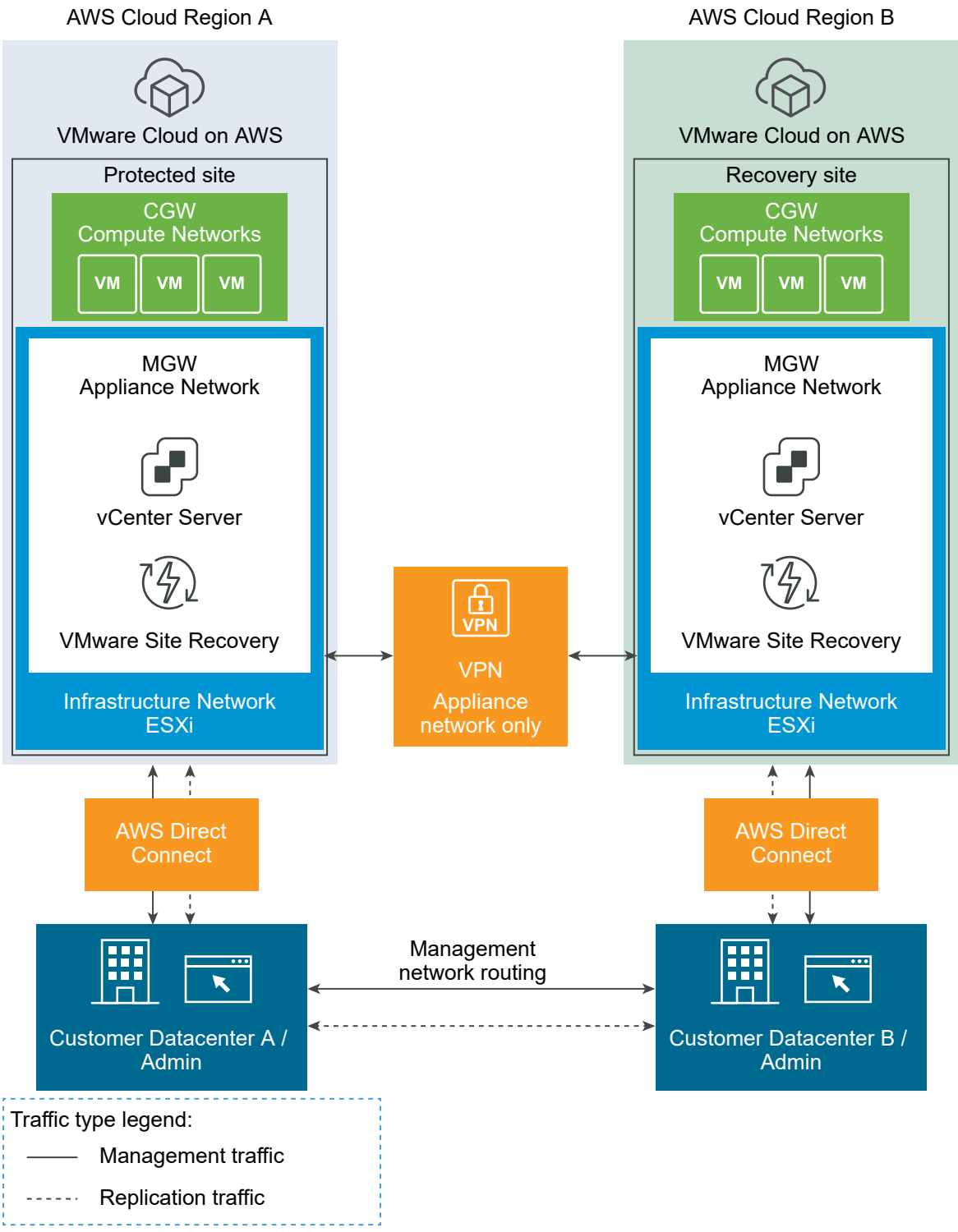
Solution

When you use Direct Connect private virtual interface, route the replication traffic between the source and the target SDDCs through on-premises.

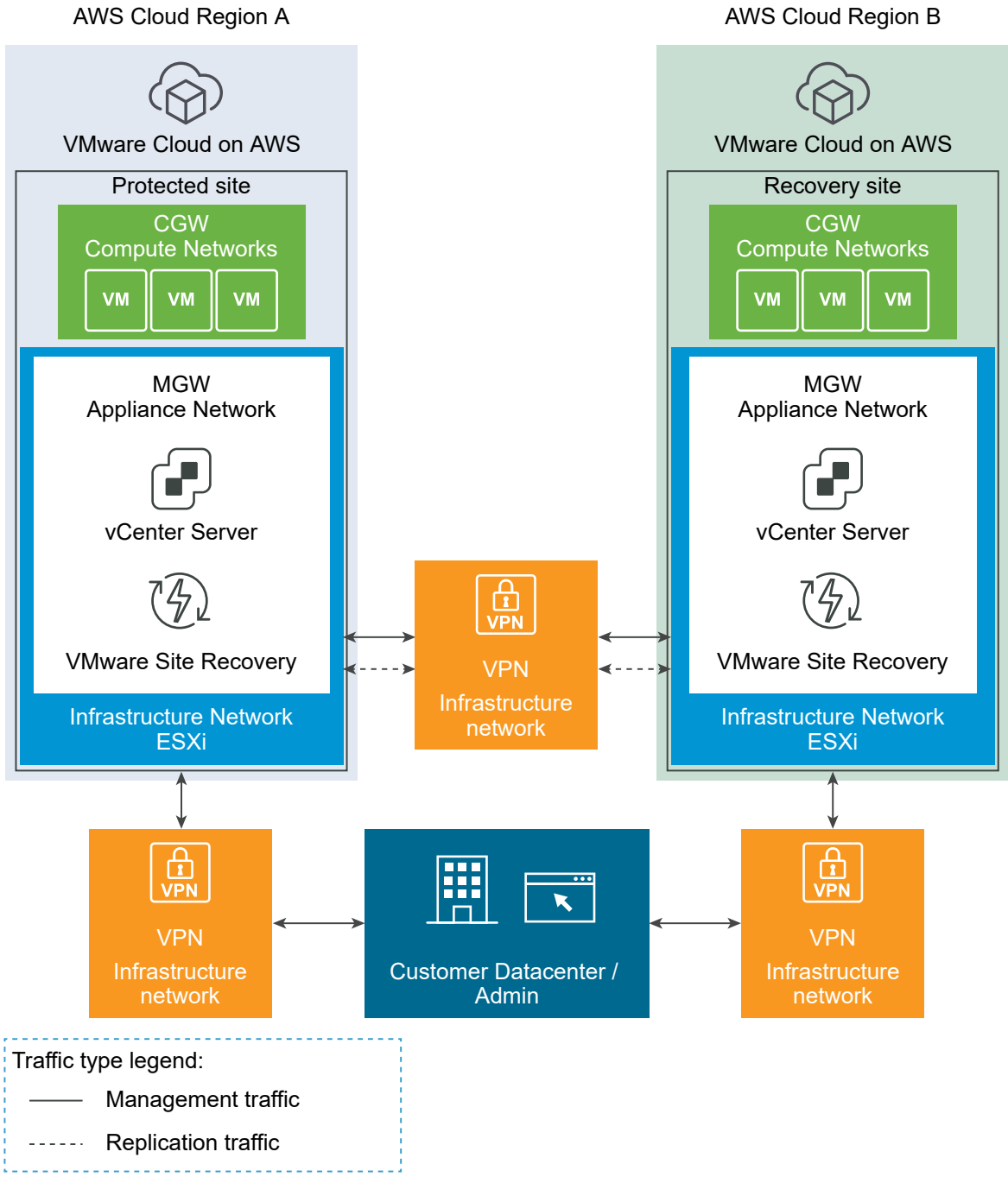
- VMware Cloud on AWS to VMware Cloud on AWS with Direct Connect.



- VMware Cloud on AWS to VMware Cloud on AWS with VPN for the appliance network and Direct Connect for the infrastructure network.



- VMware Cloud on AWS to VMware Cloud on AWS with VPN only.



Problems When Using a VMware Cloud on AWS Environment with an NFS-Mounted Storage provided by a Managed Service Provider over Direct Connect

If you are using a VMware Cloud on AWS environment with an NFS-mounted storage provided by a Managed Service Provider over Direct Connect, VPN connectivity for replication traffic communication does not work by default.

Problem

When you have an NFS-mounted storage in a VMware Cloud on AWS environment and the storage is provided by the Managed Service Provider (MSP), the connectivity between the SDDC and the storage array is over a Direct Connect private virtual interface. Using VPN connectivity for replication traffic communication from such an environment does not work by default. You must have a Direct Connect between the on-premises datacenter and VMware Cloud on AWS or work with your MSP to set up a direct connectivity between the MSP co-location facility and your on-premises datacenter.

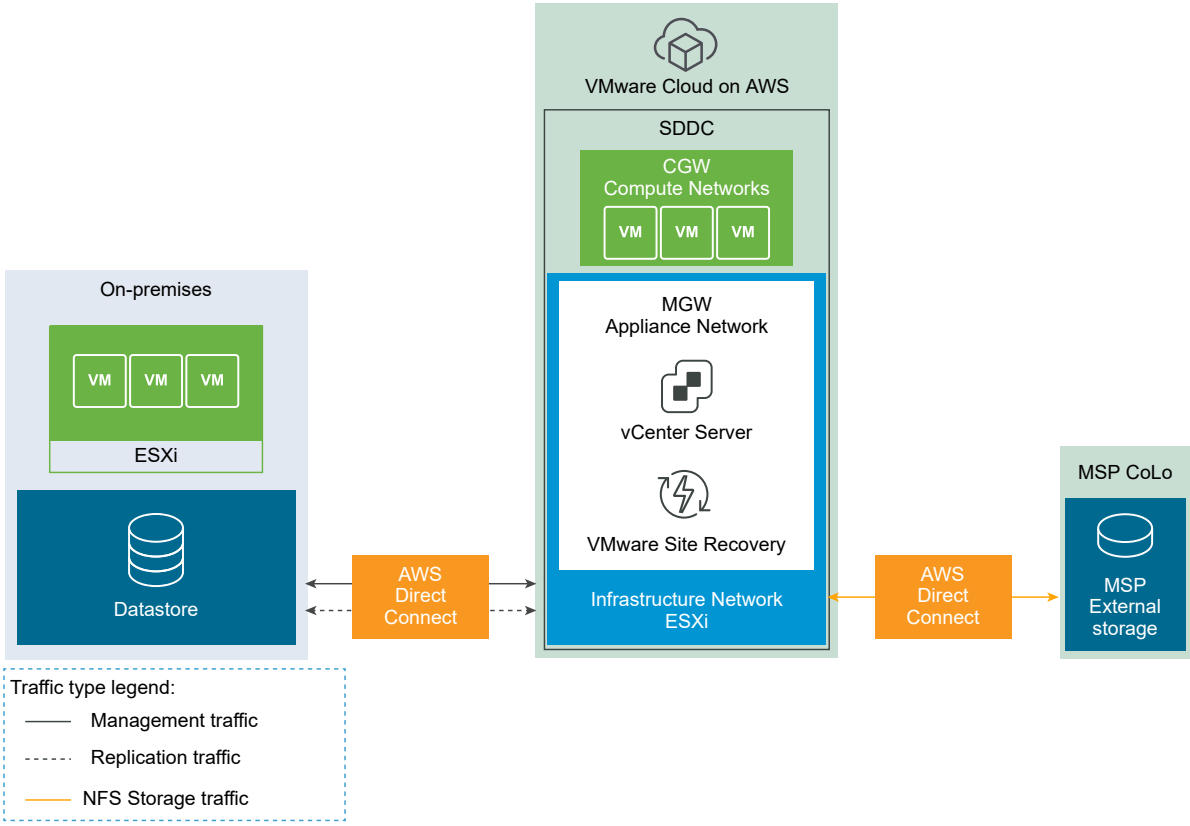
Cause

With a Direct Connect private virtual interface, the only possible external connectivity option for the ESXi traffic is Direct Connect. If there is a VPN between on-premises and the VMware Cloud on AWS SDDC, the ESXi to VMware vSphere Replication appliance traffic uses the Direct Connect path.

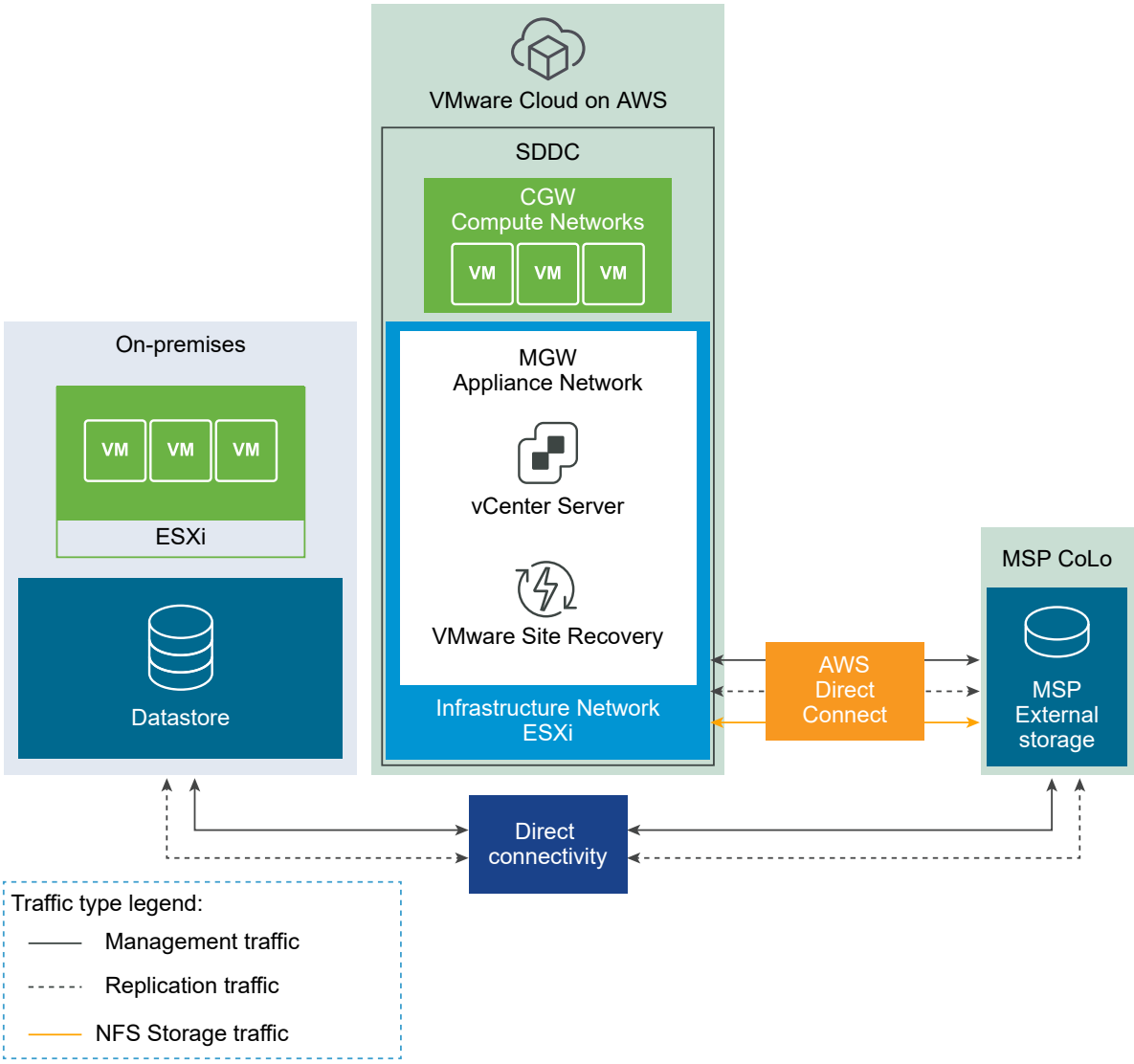
Solution

When you use NFS-mounted storage in a VMware Cloud on AWS SDDC and use VMware Site Recovery in the same SDDC, avoid VPN for the replication traffic. Route the traffic through Direct Connect between on-premises and the VMware Cloud on AWS SDDC - directly or transitively through Direct Connect between the VMware Cloud on AWS and the MSP co-location and then between the MSP co-location and on-premises.

- VMware Cloud on AWS with NFS mounted storage provided by a Managed Service Provider over Direct Connect at co-location, Direct Connect from on-premises to VMware Cloud on AWS.



- VMware Cloud on AWS with NFS mounted storage provided by a Managed Service Provider over Direct Connect at co-location, connectivity from co-location to on-premises.



Validate Network Connectivity for VMware Site Recovery

Use the VMware Cloud on AWS console **Troubleshooting** tab tests to check that all required network connectivity from your VMware Cloud on AWS SDDC to the remote site is in place.

You can use the tests both during the initial setup of VMware Site Recovery, and to troubleshoot connectivity issues during a day-to-day management. In addition to network connectivity, the DNS must also be operating properly. Use fully qualified domain names (FQDN) to test the DNS as well.

Prerequisites

Verify that VMware Site Recovery is activated.

Procedure

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

2 Click **View Details** for your SDDC.

3 Click the **Troubleshooting** tab.

4 From the Use Case drop down menu, select **Site Recovery**.

The VMware Site Recovery tests are shown. Tests are organized in groups according to the input needed for each group.

5 In the **Input** column, enter the required input for each test you want to run.

6 Run one or more tests.

- To run all tests, click **Run All**.
- To run a particular test group, click **Run Group** to the right of the group listing.
- To run an individual test, expand the test group and click **Run** next to the individual test.

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

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

Prerequisites

- Verify that you have activated VMware Site Recovery at both the protected and the recovery VMware Cloud on AWS SDDC.

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**.

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 VMware Site Recovery **Home** tab.

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

After you connect the Site Recovery Manager Server instances, you must establish a client connection to the remote Site Recovery Manager Server instance.

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

Prerequisites

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

Procedure

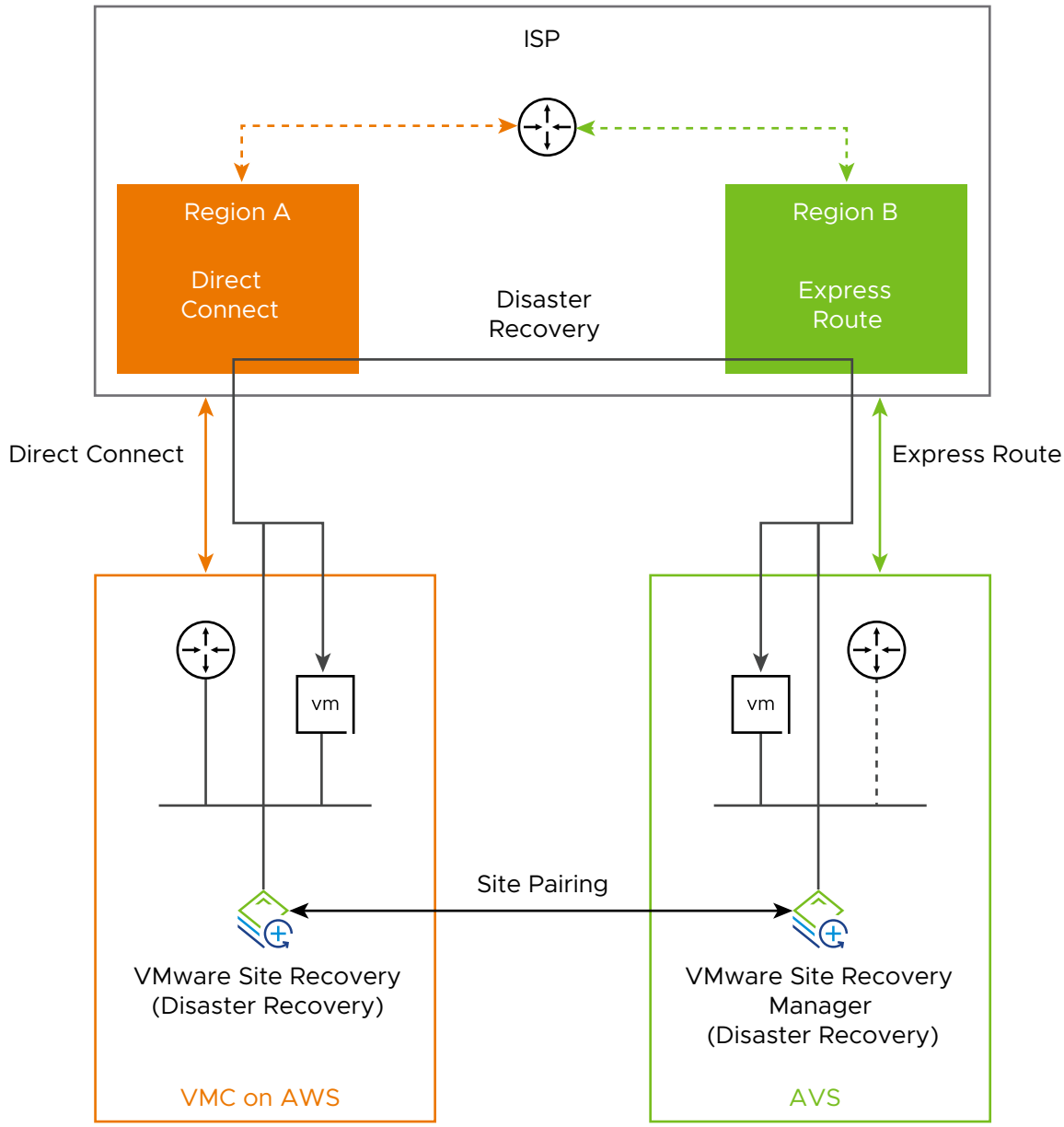
1. Connect to vSphere Web Client on one of the sites, and select **Site Recovery > Open VMware Site Recovery**.
2. On the Site Recovery home tab, select a site pair and click **View Details**.
3. Enter the vCenter Single Sign-On user name and password for the remote site, and click **Login**.

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

5

This use case provides instructions for connecting your VMware Site Recovery instance on a VMware Cloud on AWS SDDC to a Site Recovery Manager instance on an Azure VMware Solution 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 5-1. 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 activated VMware Cloud on AWS on your VMware Cloud on AWS SDDC. See Activate VMware Site Recovery.

- Verify that you have created the firewall rules between your VMware Cloud on AWS SDDC and the Management Gateway. See Set the NSX-T Edge Management Gateway Firewall Rules for VMware Site Recovery.

Procedure

1 Deploy Site Recovery Manager on Azure VMware Solution

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

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

Before you can protect your virtual machines between a VMware Cloud on AWS SDDC and an Azure VMware Solution 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.

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.*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**.

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

Before you can protect your virtual machines between a VMware Cloud on AWS SDDC and an Azure VMware Solution 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 Azure VMware Solution 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 VMware Site Recovery **Home** tab.

How do I setup VMware Site Recovery in a VMware Cloud on AWS Outposts to VMware Cloud on AWS environment

6

This use case provides instructions for setting up VMware Site Recovery with a VMware Cloud on AWS Outposts SDDC protected site and a VMware Cloud on AWS SDDC recovery site.

Prerequisites

- Verify that the two sites are in the same organisation.
- Verify that the LGW route table is 0.0.0.0/0 or a subset that does not overlap with the SDDC's management CIDR.
- Make sure that the VMware Cloud on AWS Outposts SDDC and the VMware Cloud on AWS SDDC are added to the same SDDC group. For detailed information on how to create an SDDC group, see Create or Modify an SDDC Group in the *VMware Cloud on AWS Networking and Security*.

Procedure

1 Connect the Site Recovery Manager Server Instances on VMware Cloud on AWS Outposts SDDC and the VMware Cloud on AWS SDDC

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

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**.

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 VMware Site Recovery **Home** tab.

How do I setup VMware Site Recovery in a VMware Cloud on AWS Outposts to VMware Cloud on AWS Outposts environment

7

This use case provides instructions for setting up VMware Site Recovery with a VMware Cloud on AWS Outposts SDDC protected site and a VMware Cloud on AWS Outposts SDDC recovery site.

Prerequisites

- Verify that the two sites are in the same organisation.
- Verify that the LGW route table is 0.0.0.0/0 or a subset that does not overlap with the SDDC's management CIDR.
- Make sure that the both VMware Cloud on AWS Outposts SDDCs are added to the same SDDC group. For detailed information on how to create an SDDC group, see Create or Modify an SDDC Group in the *VMware Cloud on AWS Networking and Security*.

Procedure

1 Connect the Site Recovery Manager Server Instances on the two VMware Cloud on AWS Outposts SDDCs

Connect the Site Recovery Manager Server Instances on the two VMware Cloud on AWS Outposts SDDCs

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**.

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 VMware Site Recovery **Home** tab.

Learn more about firewall rules and network connectivity

8

Firewall rules control the types of network traffic that can be sent and received through a network gateway. You must set up your firewall rules to enable VMware Site Recovery.

- Troubleshooting VMware Site Recovery Network Connectivity Problems

  If you encounter problems with the network connectivity of VMware Site Recovery, troubleshooting information can help you identify and correct these problems.

Troubleshooting VMware Site Recovery Network Connectivity Problems

If you encounter problems with the network connectivity of VMware Site Recovery, troubleshooting information can help you identify and correct these problems.

Site Recovery Connectivity Use Case Is Not Visible

Site Recovery does not appear in the use case drop-down menu in the **Troubleshooting** tab.

Problem

The Site Recovery entry is missing from the use case drop-down menu in the **Troubleshooting** tab.

Cause

The Site Recovery connectivity use case appears in the drop-down menu only when the service is activated successfully.

Solution

- Ensure that Site Recovery is activated successfully.

What to do next

For more information about the activation of VMware Site Recovery, see Activate VMware Site Recovery at the Recovery Site.

DNS Lookup Failure for a Given FQDN

The DNS lookup test for an on-premises vCenter Server, Platform Services Controller, Site Recovery Manager, or vSphere Replication fails.

Problem

One or more DNS lookup tests fails. The **Resolved Address** text box in the test results shows no result.

Cause

If the DNS lookup for a given FQDN fails, the cause might be one of the following:

- The on-premises DNS server does not have an entry for the given FQDN.
- You entered an incorrect FQDN for the test.

Solution

1. Ensure that you entered the correct FQDN.
2. Check that the on-premises DNS server has an entry for the FQDN.

Port Reachability Failure for a Given FQDN

A test for connectivity to reach a specific port at a given FQDN from a cloud appliance like vCenter Server, Site Recovery Manager, or vSphere Replication fails.

Problem

A test for connectivity to a particular port at a given FQDN fails with the message `Port port-number Connection timed out`.

Cause

The potential causes of this failure include:

- A firewall rule in the current VMware Cloud on AWS SDDC or the remote site is blocking access to the port.
- The remote system with the given FQDN is powered-off.
- The remote site with the given FQDN is not working correctly.

Solution

1. Check the firewall rules set in the VMware Cloud on AWS console to ensure that they are not blocking access to the specified port.
2. Check the remote site firewall rules to ensure that they are not blocking access to the specific port.
3. Check that the remote system with the given FQDN is powered-on and functioning correctly, and power on or restart it if necessary.

Test Failure Due to Internal Error

A test fails due to an internal error.

Problem

Any of the **Troubleshooting** tab tests might fail with an error message beginning with `Internal Error:`.

Cause

This error most commonly occurs when the Connectivity Checker experiences an internal connectivity problem.

Solution

Most of these failures are intermittent and resolve without you needing to do anything. However, if the error persists, contact the VMware customer support.

Learn more about VMware Site Recovery in a multi-site topology

9

With VMware Site Recovery, you can recover virtual machines from multiple protected sites to the same VMware Cloud on AWS SDDC, or recover different sets of virtual machines from a single VMware Cloud on AWS SDDC to multiple recovery sites.

Using VMware Site Recovery with multiple protected sites and a shared recovery site is also known as many-to-one, fan-in, or an N:1 configuration.

Using VMware Site Recovery with a shared protected site and multiple recovery sites is also known as one-to-many, fan-out, or an 1:N configuration.

VMware Site Recovery also supports many-to-many or N:N configurations, and other complex multi-site topologies such as a single site A being protected to a recovery site B, while also serving as a recovery site for a third site C.

You can use VMware Site Recovery in a shared recovery site configuration in any of the deployment models that vCenter Server supports. For information on the relation between Site Recovery Manager and vCenter Server Deployment Models, see the *Site Recovery Manager Installation and Configuration* guide.

How does multi-site topology work

In a multi-site topology, you have multiple remote sites that you configure to recover to or to protect a single, shared VMware Cloud on AWS SDDC.

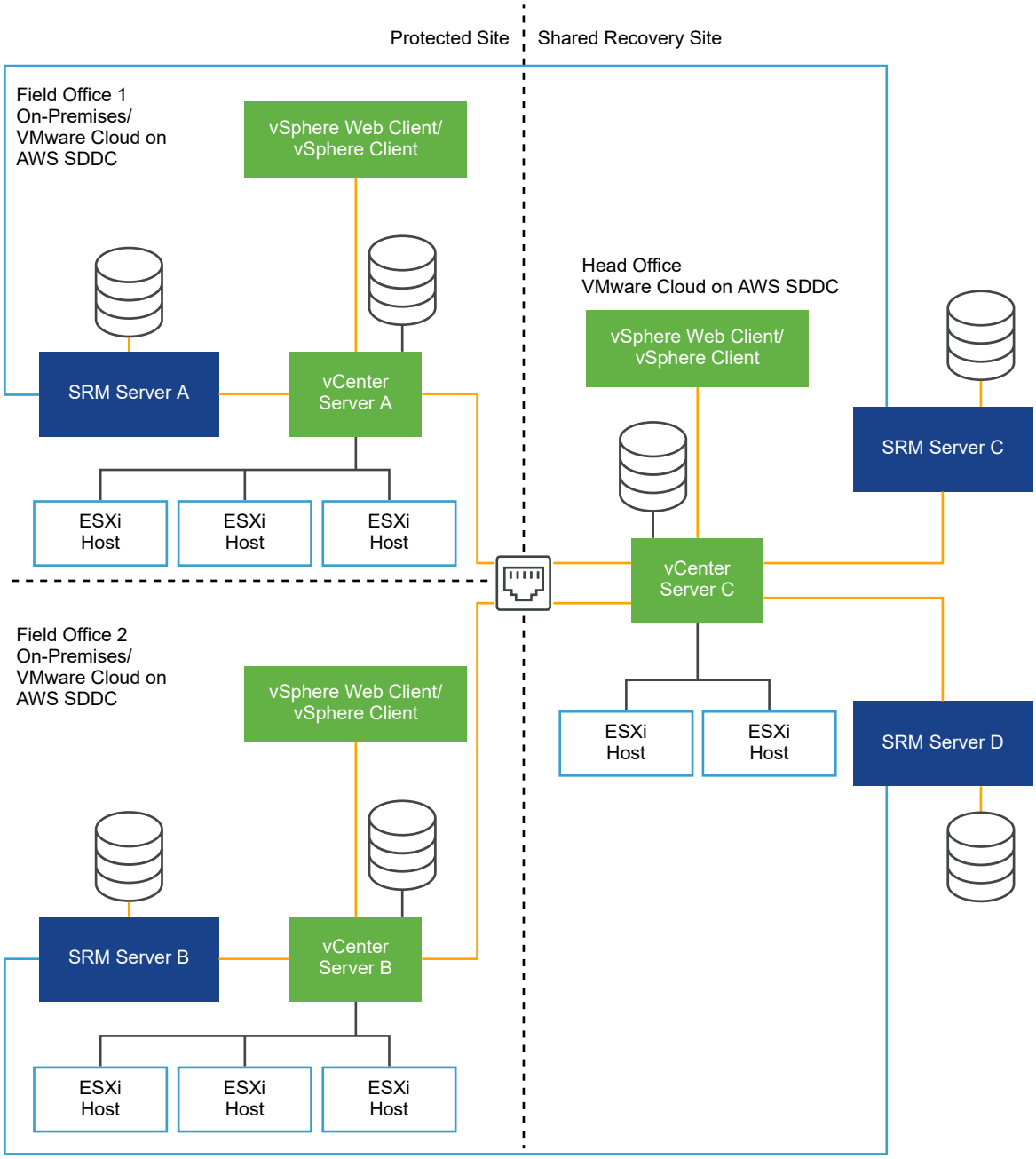
You deploy one Site Recovery Manager Server or VMware Site Recovery instance on each remote site, each of which connects to a different vCenter Server instance. Each Site Recovery Manager Server instance at the remote site must be of the same version number. For example if you deployed Site Recovery Manager Server 8.1.x, each subsequent Site Recovery Manager Server must also be 8.1.x.

On the shared VMware Cloud on AWS SDDC, you set up multiple VMware Site Recovery instances to pair with each of the Site Recovery Manager Server instances on the remote sites. All the Site Recovery Manager Server instances in the shared VMware Cloud on AWS SDDC connect to a single vCenter Server instance. Each Site Recovery Manager Server or Site Recovery Manager Server instance in a pair must have the same plug-in identifier or extension ID, which you can set when you install Site Recovery Manager Server or activate VMware Site Recovery.

The Site Recovery Manager plug-in identifier or custom extension ID specified on the remote site must match the custom extension ID of the paired VMware Site Recovery instance on the shared VMware Cloud on AWS SDDC. For example, you can set up the first pair of sites with the default Site Recovery Manager extension ID, then deploy subsequent pairs of sites with custom extension IDs.

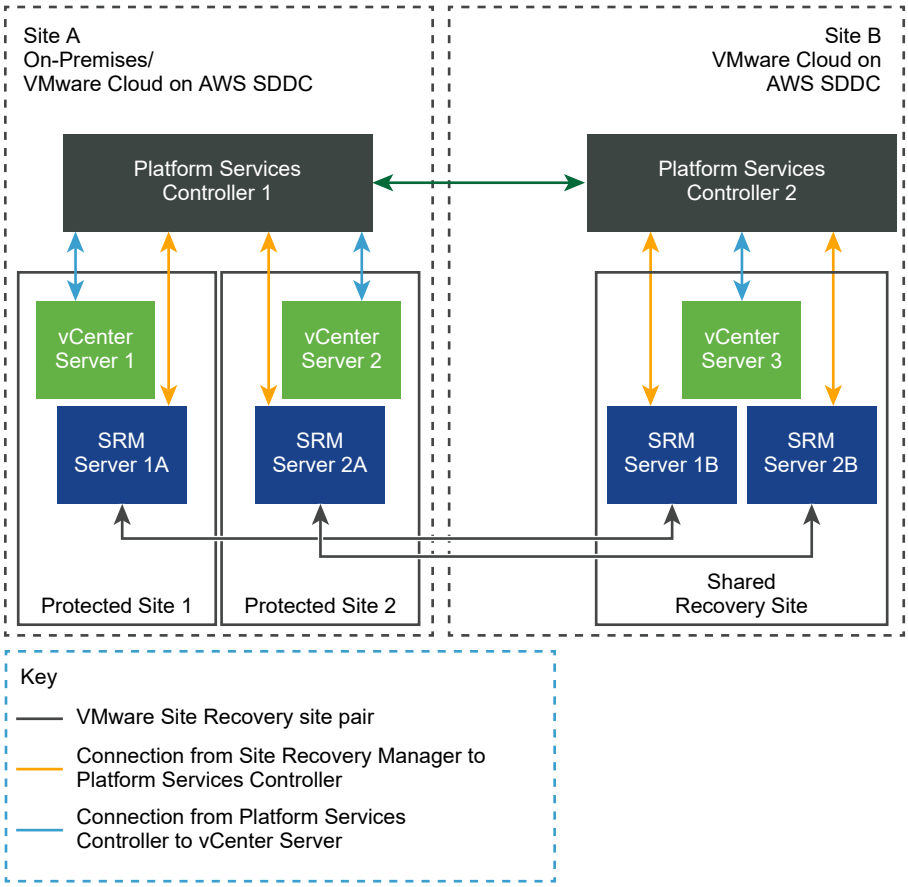
Note Site Recovery Manager supports a point-to-point replication. Site Recovery Manager does not support replication to multiple targets, even in a multi-site configuration.

Example: Example of Using VMware Site Recovery in a Shared Recovery Site Configuration



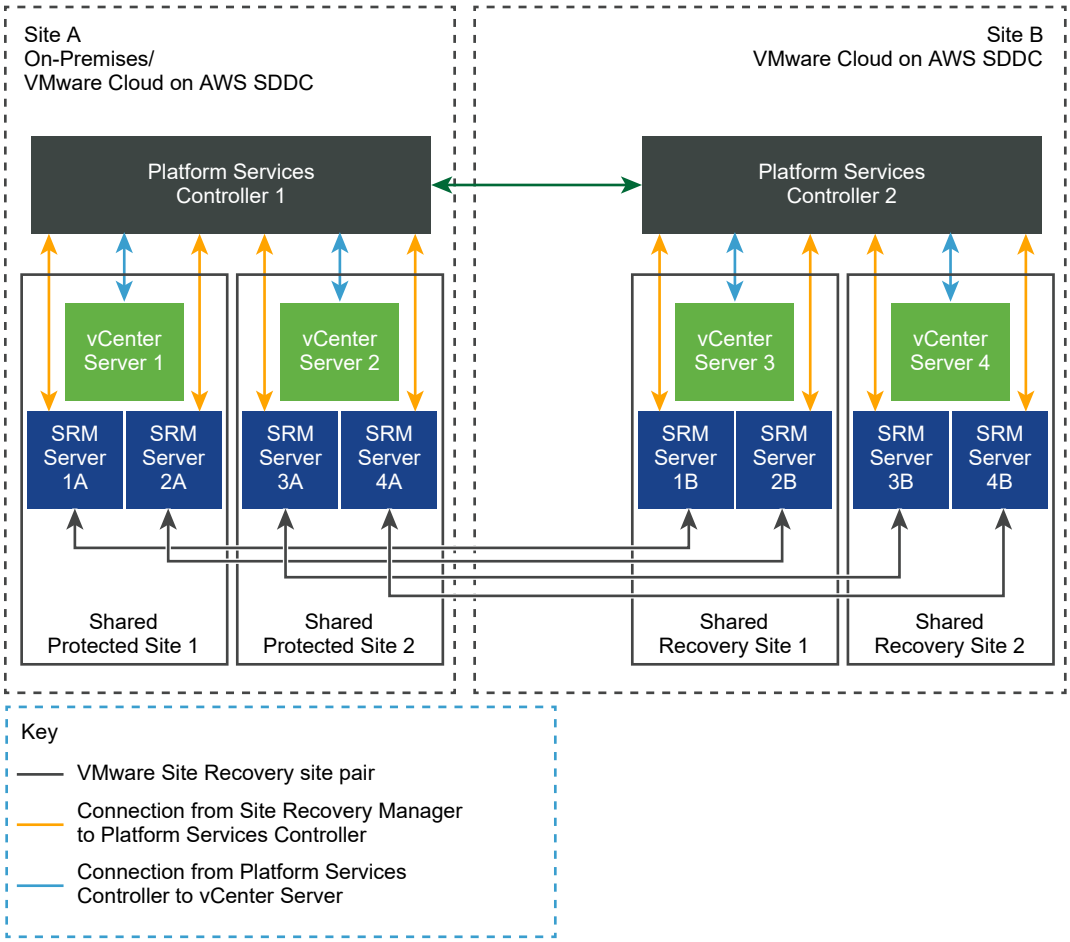
Example: VMware Site Recovery in a Shared Recovery Site Configuration

In the following 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.



Example: VMware Site Recovery in a Shared Protected Site and Shared Recovery Site Configuration

In the following 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 in VMware Cloud on AWS, two VMware Site Recovery 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.



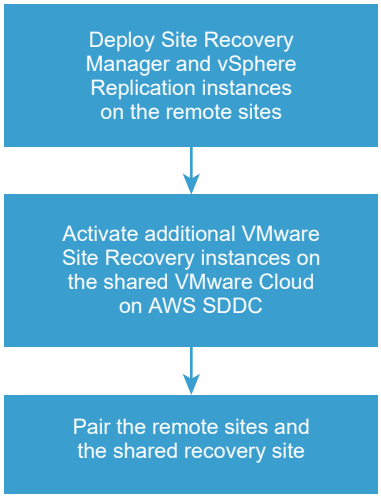
Read the following topics next:

- How do I set up VMware Site Recovery in a multi-site topology

How do I set up VMware Site Recovery in a multi-site topology

To deploy VMware Site Recovery in a multi-site topology, you deploy Site Recovery Manager Server instances on one or more remote sites, and deploy a corresponding number of VMware Site Recovery instances on the shared VMware Cloud on AWS SDDC.

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



Procedure

1 Configure Site Recovery Manager Appliances on multiple remote sites to use with Shared VMware Cloud on AWS SDDC

   You must deploy and configure a Site Recovery Manager Appliance on each remote site to use with a shared VMware Cloud on AWS SDDC.

2 Activate additional VMware Site Recovery instances on the shared VMware Cloud on AWS SDDC

   To use VMware Site Recovery in a multi-site topology that involves pairing a single VMware Cloud on AWS SDDC to multiple protected and recovery sites, you must activate additional VMware Site Recovery instances on that VMware Cloud on AWS SDDC.

3 Connect the Site Recovery Manager sites in a shared recovery site configuration

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

Configure Site Recovery Manager Appliances on multiple remote sites to use with Shared VMware Cloud on AWS SDDC

You must deploy and configure a Site Recovery Manager Appliance on each remote site to use with a shared VMware Cloud on AWS SDDC.

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**.

Activate additional VMware Site Recovery instances on the shared VMware Cloud on AWS SDDC

To use VMware Site Recovery in a multi-site topology that involves pairing a single VMware Cloud on AWS SDDC to multiple protected and recovery sites, you must activate additional VMware Site Recovery instances on that VMware Cloud on AWS SDDC.

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 **New Instance**.

4 Either select the default Site Recovery extension ID, or create a custom extension ID for this Site Recovery pair.

Option	Description
Default extension ID	Use this option for VMware Site Recovery in a standard configuration with one protected site and one recovery site.
Custom extension ID	Use this option for VMware Site Recovery: ■ In a shared recovery site configuration, with multiple protected sites and one recovery site. ■ In a single protected site configuration, with multiple recovery sites and a single protected site. ■ In a configuration where the same site is used as a protected site for recovery site A, and a recovery site for a different protected site B. ■ Any combination of the preceding scenarios. **Note** The custom extension ID must match the plug-in identifier of the paired on-premises site or the custom extension ID of the paired VMware Cloud on AWS SDDC. The custom extension ID is case-sensitive. The `com.vmware.vcDr-` prefix is automatically included.

5 Read the information on the **Activate Site Recovery** page and click **Add Instance**.

Results

An additional VMware Site Recovery instance is activated at your SDDC on VMware Cloud on AWS.

What to do next

Set the firewall rules for each new instance. See Set the NSX-T Edge Management Gateway Firewall Rules for VMware Site Recovery.

Connect the Site Recovery Manager sites in a shared recovery site configuration

In a multi-site topology, 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 remote sites, Site Recovery Manager uses the Site Recovery Manager ID that you set during the installation to connect to the corresponding Site Recovery Manager Server instance on the shared site.

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

Prerequisites

- You deployed Site Recovery Manager Server on one or more protected sites.
- You deployed one or more Site Recovery Manager Server instances on a shared site.
- You assigned the same Site Recovery Manager extension ID to a Site Recovery Manager Server instance on a remote site and to a Site Recovery Manager Server instance on the shared 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 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 To configure the site pairing for all the sites that use the shared site, repeat the procedure.

Deploying Additional vSphere Replication Servers

10

Depending on replication traffic, you might need to deploy one or more additional vSphere Replication servers in your on-premises data center.

Read the following topics next:

- Deploy an Additional vSphere Replication Server
- Register an Additional vSphere Replication Server
- Reconfigure vSphere Replication Server Settings
- Unregister and Remove a vSphere Replication Server
- Deactivate the Embedded vSphere Replication Server

Deploy an Additional vSphere Replication Server

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

You can deploy multiple vSphere Replication servers to route traffic from source hosts to target datastores without traveling between different sites managed by the same vCenter Server. You cannot deploy a second management server on the same vCenter Server.

For information about the loads that a vSphere Replication management server and a vSphere Replication server can support, see https://kb.vmware.com/s/article/2102453.

Prerequisites

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

Procedure

1. Log in to the vSphere Client on the site where you want to deploy the additional vSphere Replication server.
2. On the home page, select **Hosts and Clusters**.

3 Right-click on a data center, host or cluster, and select **Deploy OVF Template**.

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

   - Select **URL** and provide the URL to deploy the appliance from an online URL.
   - If you downloaded and mounted the vSphere Replication ISO image on a system in your environment, select **Local file > Browse** and navigate to the `\bin` directory in the ISO image, and select the `vSphere_Replication_AddOn_OVF10.ovf`, `vSphere_Replication_AddOn_OVF10.cert`, `vSphere_Replication_AddOn_OVF10.mf`, `vSphere_Replication-system.vmdk`, and `vSphere_Replication-support.vmdk` files. Make sure that you do not select the `vSphere_Replication_OVF10.ovf` file.

5 Accept the name, select or search for a destination folder or data center for the virtual appliance, and click **Next**.

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

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

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

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

   Encrypting the additional vSphere Replication server VM is not necessary to replicate encrypted VMs with vSphere Replication.

9 Set the network properties. Select DHCP or set a static IP address.

   You can change network settings after deployment in the VRMS Appliance Management Interface.

10 Enter a password for the 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.

11 Review your settings and click **Finish**.

12 Power on the vSphere Replication appliance.

What to do next

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

Register an Additional vSphere Replication Server

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

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

Prerequisites

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

Procedure

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. On the **Site Pair** tab, select **Configure > Replication Servers**.
5. Click the **Register** icon.
6. From the list, select a virtual machine that is a working vSphere Replication server and click **Select**.

Results

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

Reconfigure vSphere Replication Server Settings

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

A vSphere Replication server does not require additional configuration through the VRMS Appliance Management Interface after deployment. To increase security, you can change the root password of the vSphere Replication server and install a new certificate. You can use a self-signed certificate, which provides public-key based encryption and authentication, however it does not provide the level of assurance offered when you use a certificate signed by a certificate authority.

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

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

Prerequisites

Verify that the additional vSphere Replication server is powered on.

Procedure

1 Use a supported browser to log in to the VRMS Appliance Management Interface of the additional vSphere Replication Server that you deployed.

The URL for the VRMS Appliance Management Interface is https://*vr-server-address*:5480.

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

2 (Optional) Click **Certificates**, then click **Change**.

3 (Optional) 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 self-signed certificate is not recommended for 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 (Optional) Click **Change**.

5 (Optional) To change the password for the vSphere Replication server, click **Access** and then **VRMS appliance password > Change**.

6 (Optional) To change the network settings, click **Networking**, and then **Edit**.

7 (Optional) 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.

8 (Optional) 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 vSphere Replication 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.

9 (Optional) Click **Save**.

10 (Optional) To restart the vSphere Replication service, click **Services > hms > Restart**.

11 (Optional) To reboot the vSphere Replication server appliance, click **Summary** and click **Restart**.

Unregister and Remove a vSphere Replication Server

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

Prerequisites

Verify that the vSphere Replication server that you want to unregister does not serve any replications, otherwise the operations fails.

Procedure

1. On the Site Recovery home page, select a site pair and click **View Details**.
2. On the **Site Pair** tab, select **Replication Servers** and find the vSphere Replication server in the list.

   If you have both vSphere Replication and Site Recovery Manager installed, you can find **Replication Servers** on the **Site Pair** tab, under **Configure**.
3. Select the server and click the **Unregister** icon.
4. In the **Hosts and Clusters** view of the vSphere Client, power off and delete the vSphere Replication server virtual machine.

Deactivate the Embedded vSphere Replication Server

The vSphere Replication appliance includes an embedded vSphere Replication Server by default. If you want to deactivate the embedded vSphere Replication server, you can do so using SSH.

Prerequisites

Verify that no replications are using the embedded server. Stop the replications or move them to a different server.

Procedure

1. Use SSH into the vSphere Replication appliance and enter:

   ```
   # /opt/vmware/hms/bin/hms-configtool -cmd reconfig -property hms-embedded-hbr=false
   ```
2. Restart the HMS service.

   ```
   # service hms restart
   ```

3 Unregister the embedded vSphere Replication server from the **Replication Servers** view.

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

   b On the **Site Pair** tab, select **Replication Servers** and find the vSphere Replication server in the list.

      If you have both vSphere Replication and Site Recovery Manager installed, you can find **Replication Servers** on the **Site Pair** tab, under **Configure**.

   c Select the server and click the **Unregister** icon.

What to do next

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

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

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.

Categories of Information that VMware Receives

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.

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

Exporting and Importing Replication Configuration Data

12

You can use the vSphere Replication 8.5 Configuration Import/Export Tool to export and import configuration data about the replications created in vSphere Replication.

If you plan to migrate vSphere Replication to a different host, you can use the tool to export replication settings and the related objects into an XML file. You can then import the configuration data from the previously exported file. The vSphere Replication 8.5 Configuration Import/Export Tool supports import and export from an on-premises SDDC to a VMware Cloud on AWS, and from a VMware Cloud on AWS SDDC to another VMware Cloud on AWS SDDC.

When you deploy the vSphere Replication appliance, the tool is also deployed with the appliance. The tool is located in the `/opt/vmware/vr-impex-tool` directory. The tool is also available as a standalone `.jar` file

Requirements for Using the vSphere Replication 8.5 Configuration Import/Export Tooll

- You must have Java 1.8.x installed.
- The `JAVA_HOME` environment variable must be properly configured. For example, `JAVA_HOME=C:\Program Files\Java\jre1.8.0_152` for Windows, or `JAVA_HOME=/usr/java/jre1.8.0_152` for Linux.

Requirements for Exporting and Importing Replication Groups Configuration Data

- Before you can export a configuration, you must have a site pair with vSphere Replication 8.5.x up and running on both the protected and the recovery site.
- Import is supported in a clean vSphere Replication 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

- 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.

Exported Information

The vSphere Replication 8.5 Configuration Import/Export Tool exports the host folder information, compute resources, network and datastore information, datastore paths, RPO settings, multiple points in time (MPIT), quiescing, network compression, and so on.

Network Requirements

The vSphere Replication 8.5 Configuration Import/Export Tool must have access to both the on-premises and VMware Cloud on AWS vCenter Server, lookup service, and vSphere Replication servers to complete the vSphere Replication replication groups export and import. You must verify that the following network ports are open.

Default Port	Target	Description
443	On-premises vCenter Server	vCenter Server HTTPS port
443	On-premises Platform Services Controller / Lookup service	Platform Services Controller HTTPS port
8043	On-premises vSphere Replication	vSphere Replication port
443	VMware Cloud on AWS vCenter Server	vCenter Server HTTPS port
8043	VMware Cloud on AWS vSphere Replication	vSphere Replication port

Read the following topics next:

- Export Replication Configuration Data
- Use a Properties File to Export vSphere Replication Configuration Data
- Import Replication Configuration Data
- Properties for Automated Export and Import of vSphere Replication Configuration Data
- Syntax of the Import/Export Tool

Export Replication Configuration Data

You use the vSphere Replication 8.5 Configuration Import/Export Tool to export replication configuration data in an XML file.

Prerequisites

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

Procedure

1. Download the vSphere Replication 8.5 Configuration Import/Export Tool `.zip`.
2. Extract the tool from the archive.
3. Open a command shell, navigate to the folder where you extracted the tool, and run the following command.

   ```
   java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.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 /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
   --format
   ```

4. Enter the host name or the IP address of the Lookup Service.
5. Enter the port number or press Enter, if you use the default port.
6. Accept the SHA-1 Thumbprint.
7. Enter user name and password for the local vCenter Server instance.
8. Select a paired vSphere Replication instance.
9. Enter user name and password for the remote vCenter Server instance.

Example

Example for Export of Outgoing Replications

```
 java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
--format --exportProperties=/opt/vmware/vr-impex-tool/sample.properties --exportPath=/opt/
vmware/vr-impex-tool/
 ***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating CMD interaction.
Enter host name or IP address of a Lookup Service:
10.92.228.236
Enter port (or press Enter in case you use the default - 443):

Host 10.92.228.236 has untrusted certificate with SHA-1 Thumbprint:
63:50:89:60:76:5C:78:C9:B0:1A:A6:B6:D0:08:D7:8E:31:46:BF:A7 .
Accept thumbprint? (y/n):
y
Enter username for wdc-rdops-vm09-dhcp-228-236.eng.vmware.com:
localAdmin
Enter password for wdc-rdops-vm09-dhcp-228-236.eng.vmware.com:
Establishing connection...
Available HMS servers:
[0] wdc-rdops-vm08-dhcp-221-15.eng.vmware.com
[1] wdc-rdops-vm09-dhcp-228-236.eng.vmware.com

0
One HMS server found: wdc-rdops-vm09-dhcp-228-236.eng.vmware.com
Enter username for pair site 'wdc-rdops-vm08-dhcp-221-15.eng.vmware.com':
```

```
remoteAdmin
Enter password for pair site 'wdc-rdops-vm08-dhcp-221-15.eng.vmware.com':
Collecting data...
Starting export...
2019-09-03 16:28:14,771 DEBUG - Hms inventory export started.
2019-09-03 16:28:14,993 DEBUG - Replication groups export started.
2019-09-03 16:28:15,627 DEBUG - Hms inventory export ended.
2019-09-03 16:28:23,680 DEBUG - Replication groups export ended.
Writing to file started.
Writing to file finished.
Export ended successfully.
```

Use a Properties File to Export vSphere Replication Configuration Data

You can use a properties file to simplify or automate the export of vSphere Replication configuration data.

Prerequisites

- Verify that you have Java 1.8.x installed on the vSphere Replication host machine.
- Verify that you have a site pair with vSphere Replication running on both the protected and the recovery site.
- Prepare an *export_vr_configuration*.properties file. See Properties for Automated Export and Import of vSphere Replication Configuration Data.

Procedure

1. Download the vSphere Replication 8.5 Configuration Import/Export Tool in a folder on the vSphere Replication host virtual machine.
2. Open a command shell, navigate to the folder where you extracted the tool, and run the following command.

   ```
   java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --
   exportPropererties=Path_to_properties_file
   ```

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

   ```
   java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --
   exportProperties=Path_to_properties_file --format
   ```

Example

Example of Export with Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --
exportProperties=/opt/vmware/vr-impex-tool/sample.properties --exportPath=/opt/vmware/vr-
impex-tool/
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
```

```
Initiating using properties file.

Establishing connection...

Collecting data...

Starting export...

2019-10-28 07:56:52,529 DEBUG - VR inventory export started.

2019-10-28 07:56:52,632 DEBUG - Replication groups export started.

2019-10-28 07:56:52,668 DEBUG - VR inventory export ended.

2019-10-28 07:56:53,329 DEBUG - Replication groups export ended.

Writing to file started.

Writing to file finished.

Export ended successfully.
```

Import Replication Configuration Data

You can use the vSphere Replication 8.5 Configuration Import/Export Tool to import replication configuration data from a previously exported XML file.

Prerequisites

- Provide a clean vSphere Replication installation, registered with the same vCenter Server instance or with a vCenter Server instance with the same inventory as the exported.

Procedure

1. Open a command shell, navigate to the folder of the vSphere Replication 8.5 Configuration Import/Export Tool, and run the following command.

   ```
   -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --importInteractive
   ```

2. (Optional) To automate the import process by using a *sample.properties* file, run the following command instead.

   ```
   -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --
   importProperties=sample.properties --path=Path_toexported_XML_file
   ```

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. Enter user name and password for the local vCenter Server instance.

7 Select a paired vSphere Replication instance.

8 Enter user name and password for the remote vCenter Server instance.

Results

The vSphere Replication 8.5 Configuration Import/Export Tool creates new replications using the exported XML file.

Example

Example of Importing the Configuration by Using a Propeties File

```
-jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --importProperties=/opt/
vmware/vr-impex-tool/sample.properties --path=/opt/vmware/vr-impex-tool/
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating using properties file.
Establishing connection...
Collecting data...
2019-08-23 02:13:10,246 INFO - Importing hms data.
Reading file...
Reading file done.
2019-08-23 02:13:10,636 INFO - Import hms configurables started.
2019-08-23 02:13:11,478 DEBUG - Getting profiles for server with guid 'd83b4ce0-4530-4a45-
b493-5f137598d3f2'.
2019-08-23 02:13:11,510 DEBUG - Getting profiles for server with guid '1c0f9490-3ac3-4546-
af4a-10ab4ee634c7'.
2019-08-23 02:13:11,525 DEBUG - Starting import of replications.
2019-08-23 02:13:11,619 DEBUG - Importing Replication Group for server with guid
'd83b4ce0-4530-4a45-b493-5f137598d3f2' is complete.
2019-08-23 02:13:13,834 DEBUG - Importing Replication Group for server with guid
'1c0f9490-3ac3-4546-af4a-10ab4ee634c7' is complete.
2019-08-23 02:13:13,834 INFO - Import VR configurables ended. Imported : 2 .
Import ended successfully.
```

Properties for Automated Export and Import of vSphere Replication Configuration Data

You use the vSphere Replication 8.5 Configuration Import/Export Tool properties file to automate the export and import of replication configuration data.

The vSphere Replication 8.5 Configuration Import/Export Tool properties file must follow a specific structure.

Table 12-1. Parameters for the Properties File

Parameter	Description
`lookup.service.address`	The local Lookup Service address. For a cloud to cloud pairing, use the internal vCenter Server IP address.
`port`	The port number for the Lookup Service. The default value is `443`. This parameter is optional.

Table 12-1. Parameters for the Properties File (continued)

Parameter	Description
`local.vc.address`	The local vCenter Server name.
`local.auth.credentials.vc.username`	The user name of the local vCenter Server.
`local.auth.credentials.vc.password`	The password for the local vCenter Server.
`local.vr.name`	The name of the local vSphere Replication Management server. **Note** The name of the vSphere Replication management server is customizable and can be different from the host name of the FQDN. Retrieve the name from the Site Recovery UI.
`remote.vc.address`	The remotevCenter Server name.
`remote.auth.credentials.vc.username`	The user name for the remote vCenter Server. Required if your environment is not federated.
`remote.auth.credentials.vc.password`	The password for the remote vCenter Server. Required if your environment is not federated.
`remote.vr.name`	The name of the remote vSphere Replication Management server. **Note** The name of the vSphere Replication management server is customizable and can be different from the host name of the FQDN. Retrieve the name from the Site Recovery UI.

Example: Sample Properties File

```
lookup.service.address=my.psc.address.com
local.auth.credentials.vc.username=localAdmin
local.auth.credentials.vc.password=localAdminSecretPass
remote.auth.credentials.vc.username=remoteAdmin
remote.auth.credentials.vc.password=remoteAdminSecretPass
local.vr.name=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
local.srm.name=sc-rdops-vm12-dhcp-104-58.eng.vmware.com
remote.vr.name=sc-rdops-vm12-dhcp-109-104.eng.vmware.com
format=true
```

Syntax of the Import/Export Tool

The vSphere Replication 8.5 Configuration Import/Export Tool includes different options that you can use to import or export configuration data.

Table 12-2. vSphere Replication 8.5 Configuration Import/Export Tool Options

Option	Description
`--export`	Required when doing an export. Cannot be used together with `--import`.
`--properties`	Path to the properties file to load when automating the use of the tool.
`--exportProperties`	Used to start an export by using a properties file.
`--exportInteractive`	Used to start an export interactively with prompts for the required information.
`--exportPath`	Used to specify the directory in which to create the exported file. When the directory is not specified, the file is exported in the location of the import/export tool.
`--import`	Required when importing configuration data. Cannot be used together with `--export`.
`--importInteractive`	Used to start an import interactively with prompts for the required information.
`--importProperties`	Used to start an import by using a properties file.
`--path`	Used for importing data. Path to the previously exported file.
`--lspp`	The Platform Services Controller address. Can be an IP address or FQDN. For vSphere Replication, it must match the `lookup.service.address` property.
`--port <[1, 2147483647]>`	The port number for the Lookup Service. The default value is *443*.
`--localVrName`	The name of the local vSphere Replication Management server. It must match the `local.vr.name` property.
`--remoteVrName`	The name of the remote vSphere Replication Management server. It must match the `remote.vr.name` property.
`--localAuthCredsUsername`	The user name for the local vCenter Server.
`--localAuthCredsPass`	The password for the local vCenter Server.
`--remoteAuthCredsUsername`	The user name for the remote vCenter Server.
`--remoteAuthCredsPass`	The password for the remote vCenter Server.
`--format`	Used to make the exported XML file better formatted and human-readable. The `--format` option significantly increases the file size.

Sample Commands with Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --
exportProperties=/opt/vmware/vr-impex-tool/sample.properties --exportPath=/opt/vmware/vr-
impex-tool/
```

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --
importProperties=/opt/vmware/vr-impex-tool/sample.properties --importPath=/opt/vmware/vr-
impex-tool/sample.xml
```

Sample Properties File

```
lookup.service.address=my.psc.address.com
local.auth.credentials.vc.username=localAdmin
local.auth.credentials.vc.password=localAdminSecretPass
remote.auth.credentials.vc.username=remoteAdmin
remote.auth.credentials.vc.password=remoteAdminSecretPass
local.vr.name=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
#local.srm.name=sc-rdops-vm12-dhcp-104-58.eng.vmware.com
remote.vr.name=sc-rdops-vm12-dhcp-109-104.eng.vmware.com
format=true
```

Sample Commands in Interactive Mode

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
```

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --importInteractive
```

Sample of Using Interactive Mode

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating CMD interaction.
Enter host name or IP address of a Lookup Service:10.193.15.152
Enter port (or press Enter in case you use the default - 443):
Host sc2-rdops-vm08-dhcp-15-152.eng.vmware.com has untrusted certificate with SHA-1
Thumbprint: 82:CF:58:F2:E7:C6:A1:4C:
89:FC:7B:05:31:DD:13:00:28:21:DA:F3 .
Accept thumbprint? (y/n):y
Enter username for sc2-rdops-vm08-dhcp-15-152.eng.vmware.com:administrator@vsphere.local
Enter password for sc2-rdops-vm08-dhcp-15-152.eng.vmware.com:
Establishing connection...
Available VR servers:
[0] sc-rdops-vm12-dhcp-109-104.eng.vmware.com
[1] sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
0
One VR server found: sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
Enter username for pair site 'sc-rdops-vm12-
dhcp-109-104.eng.vmware.com':administrator@vsphere.local
Enter password for pair site 'sc-rdops-vm12-dhcp-109-104.eng.vmware.com':
Collecting data...
Starting export...
2019-10-30 04:21:18,464 DEBUG - VR inventory export started.
```

```
2019-10-30 04:21:18,548 DEBUG - Replication groups export started.
2019-10-30 04:21:18,585 DEBUG - VR inventory export ended.
2019-10-30 04:21:19,228 DEBUG - Replication groups export ended.
Writing to file started.
Writing to file finished.
Export ended successfully.
```

Sample of Using Commands without Properties File

```
java -jar C:\Users\Administrator\Downloads\impex\vr-import-export-tool-8.3.0.jar
--export --localVrName=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com --remoteVrName=sc-
rdops-vm12-dhcp-109-104.eng.vmware.com --lspp=10.193.15.152 --format --
exportPath=/opt/vmware/vr-impex-tool/ --localAuthCredsUsername=administrator@vsphere.local
--remoteAuthCredsUsername=administrator@vsphere.local --localAuthCredsPass=***** --
remoteAuthCredsPass=*****
```

Sample of Using Commands without Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --export
--localVrName=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com --remoteVrName=sc-rdops-vm12-
dhcp-109-104.eng.vmware.com --lspp=10.193.15.152 --format --exportPath=/opt/
vmware/vr-impex-tool/ --localAuthCredsUsername=administrator@vsphere.local --
remoteAuthCredsUsername=administrator@vsphere.local --localAuthCredsPass=***** --
remoteAuthCredsPass=*****
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating CMD interaction.
Establishing connection...
Collecting data...
Starting export...
2019-10-30 04:28:54,426 DEBUG - VR inventory export started.
2019-10-30 04:28:54,508 DEBUG - Replication groups export started.
2019-10-30 04:28:54,543 DEBUG - VR inventory export ended.
2019-10-30 04:28:55,230 DEBUG - Replication groups export ended.
Writing to file started.
Writing to file finished.
Export ended successfully.
```

VMware Site Recovery Upgrades and Maintenance

13

VMware Site Recovery is a managed Disaster Recovery service by VMware. VMware manages the upgrades of VMware Site Recovery on VMware Cloud on AWS.

Overview of VMware Site Recovery Upgrades

To address any security vulnerabilities and known issues, and to bring new features which enhance the service, VMware ensures the upgrade of your VMware Site Recovery deployments on your VMware Cloud on AWS SDDCs to the latest version. A VMware Site Recovery deployment consists of a Site Recovery Manager appliance and a vSphere Replication appliance. For a detailed list of the features of VMware Site Recovery, see the VMware Site Recovery Release Notes.

Prerequisites for Upgrade

To make sure that VMware can upgrade the VMware Site Recovery instances on your VMware Cloud on AWS SDDC to the latest version, you must ensure the following:

- vSphere, the ESXi hosts, Site Recovery Manager, and vSphere Replication on your on-premises site must be upgraded to the compatible versions with the version of VMware Site Recovery we target to upgrade. Use the VMware Product Interoperability Matrix to look up the versions that must be on your on-premises site.
- The version of the VMware Cloud on AWS SDDC must be compatible with the VMware Site Recovery version. Use the VMware Product Interoperability Matrix to check for compatibility by selecting VMware Cloud on AWS and VMware Site Recovery Manager under **Select VMware Products**.
- Ensure that your Recovery Plans are in the following states: Ready, No Protection Groups, Test Complete, Recovery Complete. For more information on how to clean up a recovery plan, see Clean Up After Testing A Recovery Plan.

Scheduling and Upgrading

When a new major version of Site Recovery Manager and vSphere Replication becomes available for VMware Cloud on AWS SDDCs, VMware will send notifications to the customers which have the VMware Site Recovery add-on activated, that they can expect VMware Site Recovery upgrade in the next 2 months. VMware upgrades the VMware Site Recovery add-ons of the VMware Cloud on AWS SDDCs in waves to minimize the risks. When the timeslot for the VMware Site Recovery upgrade of a given SDDC is defined, the information is communicated through additional notification to the owner of the SDDC, at least 7 days before the corresponding timeslot. Additional notifications are sent, when the maintenance starts and completes. The notification for start can be expected at the beginning of the timeslot, while the completion notification can arrive sooner that the end of the timeslot. VMware reserves some buffer time to remediate potential issues, if such occur. The upgrade maintenance is considered completed only when you receive the completion notification.

VMware might have to cancel a scheduled VMware Site Recovery upgrade for various reasons. For example, VMware runs checks to ensure that the SDDC is in a good state for VMware Site Recovery upgrade. If the checks fail at the start of the maintenance, the upgrade is canceled and VMware looks for another opportunity to schedule and perform the upgrade. If a scheduled upgrade is canceled, you receive a corresponding notification. VMware will do their best to work with you, and to assist with meeting the pre-requisites, and schedule and perform the upgrades. VMware aims to complete the upgrades within 6 months of the release of new versions of Site Recovery Manager and vSphere Replication in VMware Cloud on AWS. After that period any older versions of the Site Recovery Manager and vSphere Replication appliances on individual SDDCs are considered not supported and cannot be upgraded. You can deactivate the VMware Site Recovery add-on, and then activate it again to get the current Site Recovery Manager and vSphere Replication versions and go back to a supported state. However, you will have to perform all the Site Recovery Manager and vSphere Replication configurations again, including site pairings, configuring replications, recovery plans, and so on.

Downtime and Customer Impact

During the VMware Site Recovery upgrade maintenance, the Site Recovery Manager and vSphere Replication services in your VMware Cloud on AWS SDDC are restarted. The impact is as follows:

- You cannot open the Site Recovery User Interface for the SDDC under maintenance. From the remote SDDC Site Recovery UI, this site will appear as disconnected.
- Recovery plan failover operations towards the SDDC under maintenance cannot be initiated. Failover operations in progress might fail when maintenance starts.

- Incoming replications are interrupted. Depending on RPO settings and the maintenance duration, RPO violations notification for these replications might appear in the remote Site Recovery UI. RPO violations should disappear automatically sometime after the maintenance is completed, depending on when vSphere Replication manages to sync the accumulated delta. Replications outgoing from the SDDC under maintenance are not affected.

VMware Site Recovery maintenance does not affect the rest of the SDDC services. You can continue to use the SDDC during VMware Site Recovery maintenance.

How do I modify and uninstall Site Recovery Manager

14

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

- 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.

- 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 on the on-premises site

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

- Deactivate VMware Site Recovery

  If you no longer require VMware Site Recovery, you must follow the correct procedure to cleanly deactivate the service.

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 Client to check the connection between the sites. If the connection is broken, or if you changed the Platform Services Controller address, reconfigure the site pairing. For instructions about how to reconfigure the site pairing, see Reconfigure the Connection Between Sites.

Reconfigure the Connection Between Sites

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

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

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

- You changed the Platform Services Controller address.

Procedure

1. In the vSphere 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 reconfiguration 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* in the *Site Recovery Manager Documentation*.

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 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 uninstall Site Recovery Manager Server from the previous remote site. For instructions about uninstalling Site Recovery Manager Server, see the steps of #unique_62 from the **Break Pairing** step onwards.
- Reconfigure the inventory mappings and placeholder datastore mappings to map objects on the existing site to objects on the new remote site. For instructions about configuring mappings, see *VMware Site Recovery Administration*.
- Reconfigure the replication of virtual machines from the existing site to the new remote site. For information about configuring vSphere Replication, see *Replicating Virtual Machines* in *VMware Site Recovery Administration*.

- Create new protection groups and recovery plans to recover virtual machines to the new remote site. For information about creating protection groups and recovery plans, see *VMware Site Recovery Administration*.

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, 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 on the on-premises site

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 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.

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

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

12 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.

13 Repeat the procedure on the other site.

Deactivate VMware Site Recovery

If you no longer require VMware Site Recovery, you must follow the correct procedure to cleanly deactivate the service.

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

Deactivating VMware Site Recovery removes both Site Recovery Manager and vSphere Replication.

Procedure

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

2 Select your SDDC, and then click **Open vCenter**.

3 Log in to the vSphere Client.

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

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

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

You cannot delete recovery plans that are running.

7 Click the **Protection Groups** tab, click a protection group, and select the **Virtual Machines** tab.

8 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.

9 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.

10 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**.

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

12 Click the **Replications** tab, and select all replications from **Outgoing replications** and **Incoming replications**.

13 Click the **Remove** icon.

VMware Site Recovery asks you if you want to stop permanently the replication for the selected virtual machine.

Note The connection between the VMware Site Recovery sites must be working to stop a replication on both sites. Alternatively, you can force stop the replication on the local site by selecting **Force stop replication**. If the remote site is available, you must also use the Site Recovery user interface to force stop the corresponding replication on the remote site. If you force stop a forward replication, you can still recover the replication by using the Site Recovery user interface on the remote site.

14 Click **Remove** to confirm that you want to stop replicating the virtual machines.

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

16 Deactivate VMware Site Recovery.

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

b Click your SDDC, and then click **View Details**.

c Select **Site Recovery** and click **Deactivate**.

What to do next

Inspect the target datastore for any leftover replica disks and files, and delete them.