

# VMware Site Recovery for VMware Cloud on AWS Evaluation Guide

TECHNICAL WHITE PAPER

## Table of Contents

<b>Introduction</b>	<b>4</b>
<b>Pre-requisites</b>	<b>4</b>
Site Recovery Manager Server .....	4
DNS .....	5
NTP .....	5
<b>Deployment</b>	<b>5</b>
Activating Site Recovery .....	6
Installing Site Recovery Manager .....	7
Installing vSphere Replication.....	16
<b>Firewall configuration</b>	<b>26</b>
Simple Firewall Configuration .....	27
<b>Pairing Sites and Mapping Resources</b>	<b>32</b>
Pair Sites.....	32
Map Resources.....	35
Network Mapping.....	36
Test Networks.....	37
IP Subnet Mapping.....	39
Folder Mapping.....	40
Resource Pool and Storage Policy Mapping.....	42
Placeholder Datastores .....	43
<b>Protect VMs</b>	<b>45</b>
Replication .....	45
Protection Groups .....	48
Recovery Plans.....	49
Monitoring Replications .....	50
Priority Groups and Dependencies.....	50
Shutdown Actions.....	52
Startup Actions .....	52
Post Power On Steps .....	53
<b>Workflows</b>	<b>53</b>
Test.....	53
Cleanup.....	55
Failover .....	55
Reprotect.....	57
<b>Reporting</b>	<b>58</b>





**VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)**

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

## Introduction

The purpose of this guide is to support a self-guided evaluation of the primary features and benefits of using VMware Site Recovery for VMware Cloud on AWS. This guide walks through the different features and offerings in the VMware Site Recovery service and provides guidance how to configure and test them.

The exercises in this guide should be completed in the order prescribed for best results. Some exercises have dependencies on previously completed items.

## Pre-requisites

This guide assumes that you have already completed the steps in the [VMware Cloud on AWS Evaluation Guide](#) related to AWS account linking, network configuration and initial firewall configuration, and therefore have access to a fully functional SDDC. In addition to this there are the following requirements before activating and installing VMware Site Recovery.

### Test Virtual Machines

To test the operation of VMware Site Recovery it is recommended to use a few Windows or Linux based virtual machines with a current version of VMware Tools installed.

### Network connectivity

There are a couple of different topologies for implementing VMware Site Recovery and some network connectivity requirements are unique to each.

#### Customer Site to VMware Cloud on AWS

For VMware Site Recovery connectivity, you must have a network connection from the remote site to the SDDC Management Gateway. This connection can either be a VPN or a private VIF. Instructions for how to set this up are available in the [documentation](#) and the [VMware Cloud on AWS Evaluation Guide](#)

#### VMware Cloud on AWS to VMware Cloud on AWS

VMware Site Recovery also supports protecting virtual machines running in an SDDC in one region to be protected to another SDDC in the same or another region. The same connectivity options are supported for this option as well. There are a few differences as far as deployment and operations with this topology, they will be noted in this guide.

#### Site Recovery Manager Server

When deploying Site Recovery Manager on-premises it must be installed on a Windows server. Before proceeding with this evaluation guide deploy a VM with Windows Server (2016, 2012 64-bit or 2008 R2 64-bit) with a static IP address.



## DNS

DNS forward and reverse lookups need to be configured for the IP addresses that will be used for the on-premises Site Recovery Manager (SRM) server and vSphere Replication appliance. If this is being configured between SDDCs this is not required.

Make sure that the remote site firewall allows for DNS requests from the VMware Cloud on AWS Management Gateway private IP address. Without this, DNS forwarding from VMware Cloud on AWS to the remote site will fail.

## NTP

All parts of VMware Site Recovery are sensitive to time skew. vCenters and PSCs as well as for the Site Recovery Manager server and vSphere Replication appliance. The VMware Cloud on AWS vCenter, SRM server and vSphere Replication appliance all are configured and enabled for NTP. No user configuration is required for NTP for management components within VMware Cloud on AWS.

## Deployment

The steps for deployment of VMware Site Recovery are:

- Activate the Site Recovery Add On
- Install on-premises components (SRM and vSphere Replication)
- Configure VMware Cloud on AWS Firewall
- Pair sites
- Map resources
- Configure placeholder datastores

After these steps are completed VMware Site Recovery is ready to start protecting and recovering VMs.

If deploying VMware Site Recovery between two SDDCs the steps are:

- Activate the Site Recovery Add On in both SDDCs
- Configure VMware Cloud on AWS Firewall
- Pair sites
- Map resources
- Configure placeholder datastores

**Recommendation:** Use default settings for all components - installation paths, TCP port settings, and so on - wherever possible, to minimize complexity in the evaluation environment. Use consistent naming conventions, usernames, and passwords during evaluation environment deployment.

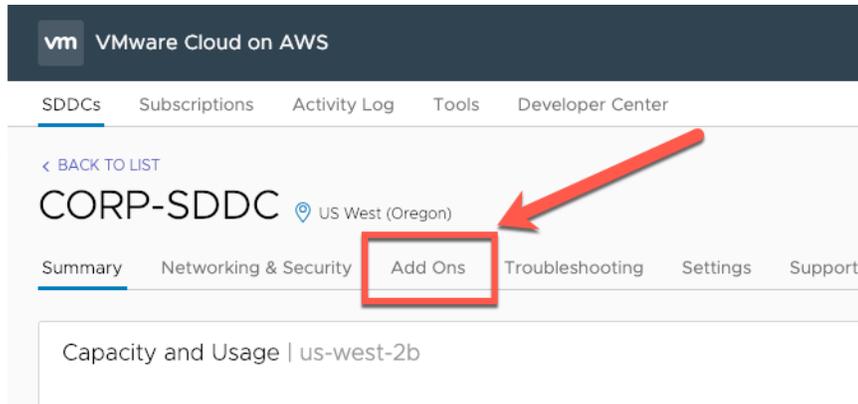
**Recommendation:** Use descriptive names for the components such as servers and port groups in a VMware virtualized environment. These names appear in the user interface and VMware Site Recovery history reports. Descriptive names improve the quality of these reports and ease troubleshooting. Use the same naming convention for items such as network



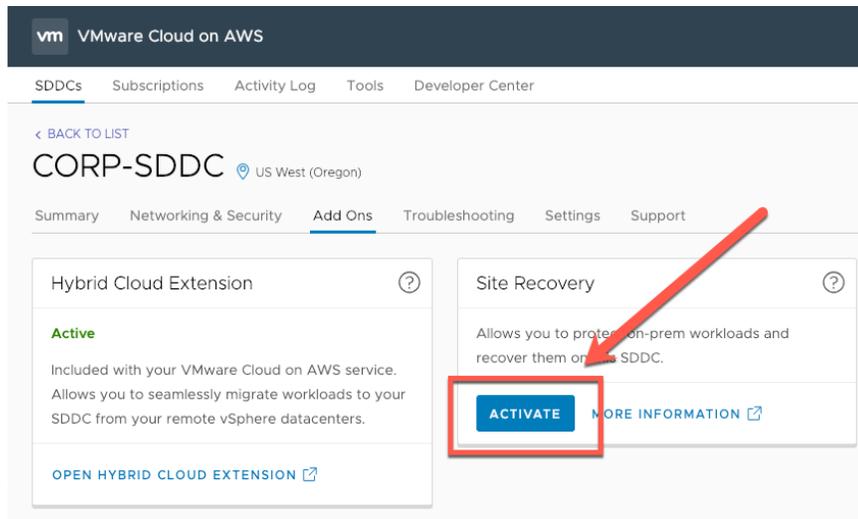
port groups at the protected site and the recovery site, as this will simplify inventory mappings.

**Activating Site Recovery**

Start by selecting “Add Ons” from the SDDC main menu within the VMware Cloud on AWS console.



Click “Activate”



Choose the Default extension ID unless this installation involves more than a single pair of SRM servers. If using the custom extension ID make sure that it exactly matches (case sensitive) the remote site custom extension ID. Click “Activate”



Activate Site Recovery for CORP-SDDC ×

VMware Site Recovery allows you to protect on-premises workloads and recover them on this SDDC.

 After Site Recovery is activated, you need to install on-premises components on the SDDC you wish to protect. Download the components from <http://www.vmware.com/go/download-site-recovery> 

 VMware Site Recovery requires you create several firewall rules after activation. Please see the help topic *What firewall rules do I need for Site Recovery* by pressing the  icon on the card.

Extension ID

Default extension ID (com.vmware.vcDr)

Custom extension ID com.vmware.vcDr- \_\_\_\_\_

[MORE INFORMATION](#) 

CANCEL

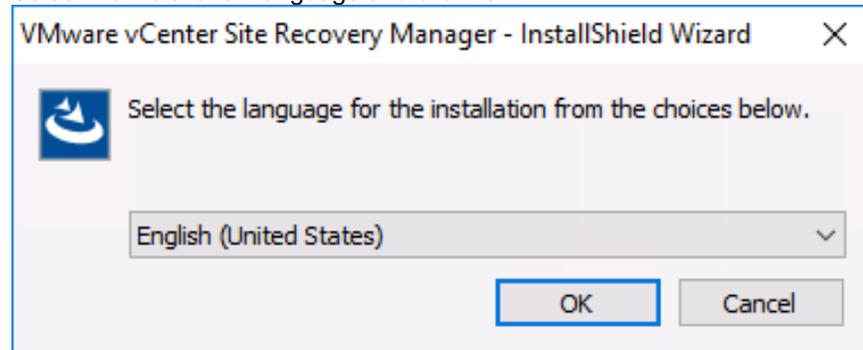
ACTIVATE

No other user action is required for activation. While the VMware Site Recovery add-on is being activated start downloading and installing the on-premises components.

### Installing Site Recovery Manager

Run the SRM installer executable

Select the installation language and click “OK”

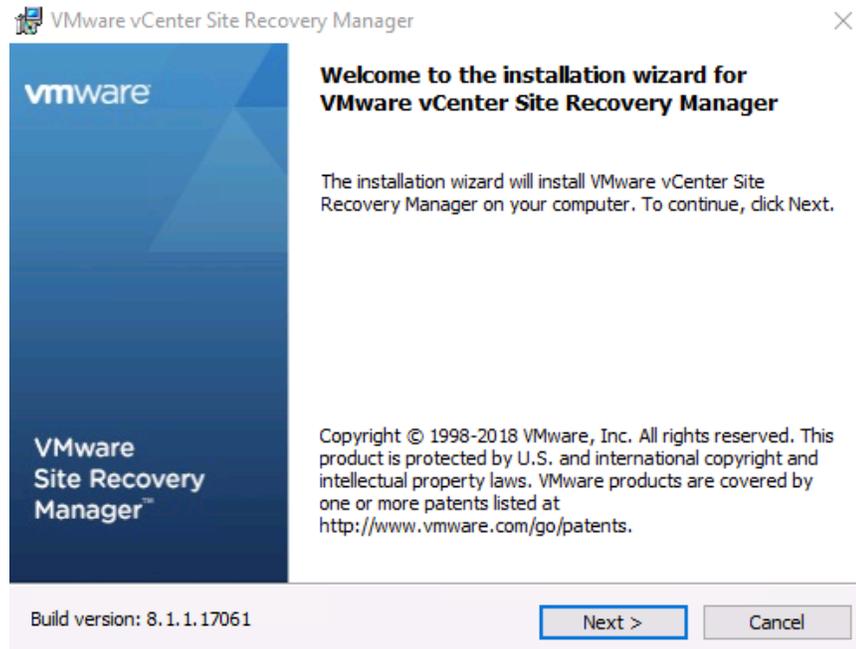


Click “Next”



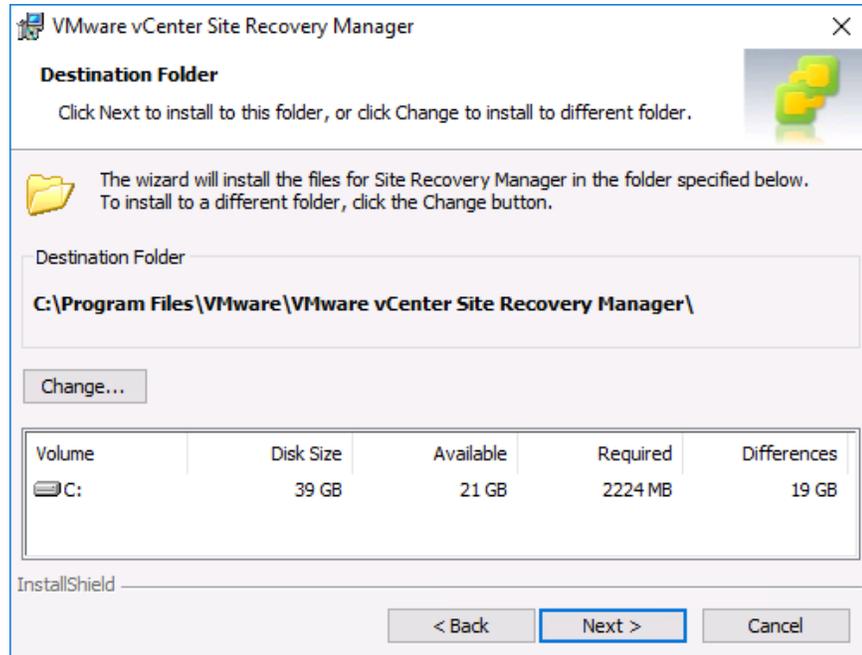
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

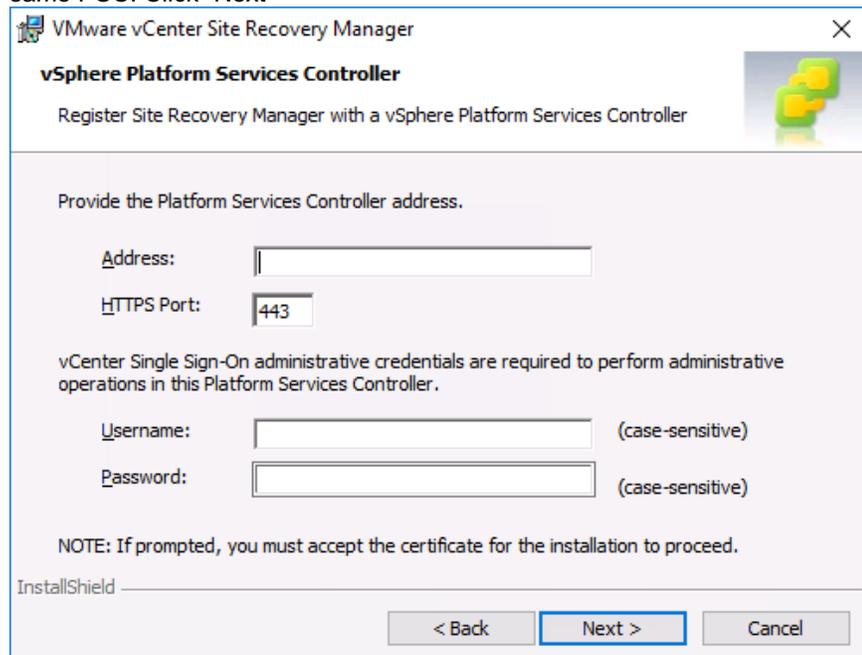


- Click "Next" at the VMware Patents dialog
- Read the License Agreement and select "I agree", click "Next"
- Confirm that the [installation pre-requisites](#) have been completed, click "Next"
- Select the destination folder, click "Next"



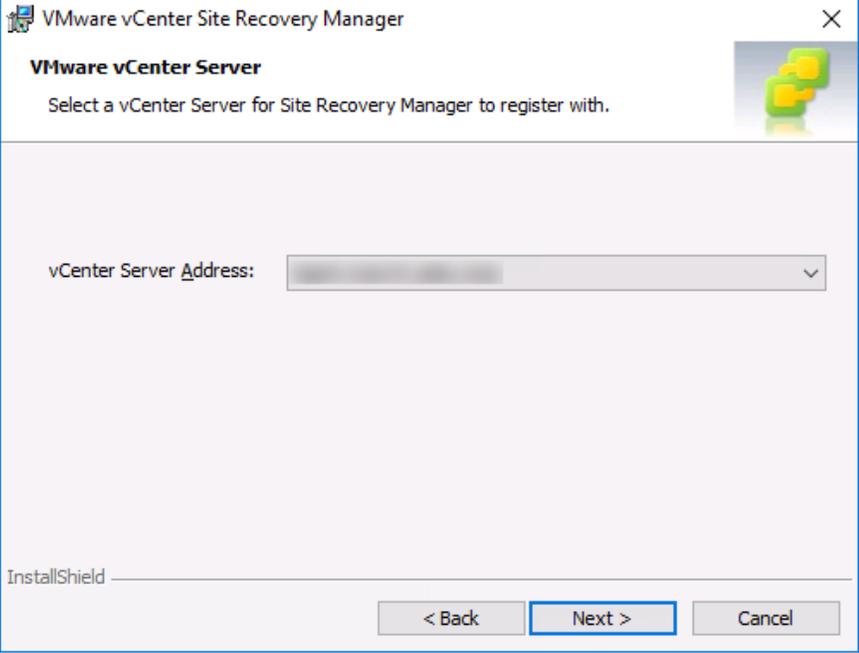


Provide the address (IP address or preferably FQDN) of the on-premises PSC and the SSO credentials to perform administrative operations on the same PSC. Click "Next"



Verify and accept the windows certificate if applicable

Select the appropriate vCenter Server for SRM to register with. Click "Next"



VMware vCenter Site Recovery Manager

**VMware vCenter Server**

Select a vCenter Server for Site Recovery Manager to register with.

vCenter Server Address:

InstallShield

< Back   Next >   Cancel

Enter a name for the Local Site, eg. "San Jose", "Site A", etc. Enter an email address for system notifications and select the address on the local host to be used for SRM (the default is usually good). We do not recommend changing the listener or SRM UI ports for an evaluation. Click "Next"



**VMware vCenter Site Recovery Manager**  
**Site Recovery Manager Extension**  
 Information to register the Site Recovery Manager extension.

Local Site Name:   
 A unique display name for this Site Recovery Manager site

Administrator E-mail:   
 An email address to use for system notifications

Local Host:   
 The address on the local host to be used by Site Recovery Manager

Listener Port:  SRM UI Port:

InstallShield

< Back Next > Cancel

Select the same option and if using the Custom SRM Plug-in Identifier enter the exact same, case sensitive string in the “Plug-in ID” field (type only the text that was entered, not the “com.vmware.vcDr-“ portion.

**VMware vCenter Site Recovery Manager**  
**Site Recovery Manager Plug-in ID**  
 Specify a plug-in ID to identify this instance of Site Recovery Manager.

The default Site Recovery Manager plug-in identifier is recommended for most configurations. For shared recovery site installations, in which multiple sites connect to a shared recovery site, use a unique custom Site Recovery Manager plug-in identifier for each Site Recovery Manager Server pair.

Default Site Recovery Manager Plug-in Identifier  
 Custom Site Recovery Manager Plug-in Identifier

Plug-in ID:   
 Paired Site Recovery Manager sites must have a matching plug-in ID

Organization:   
 Enter the organization, for example, the company name

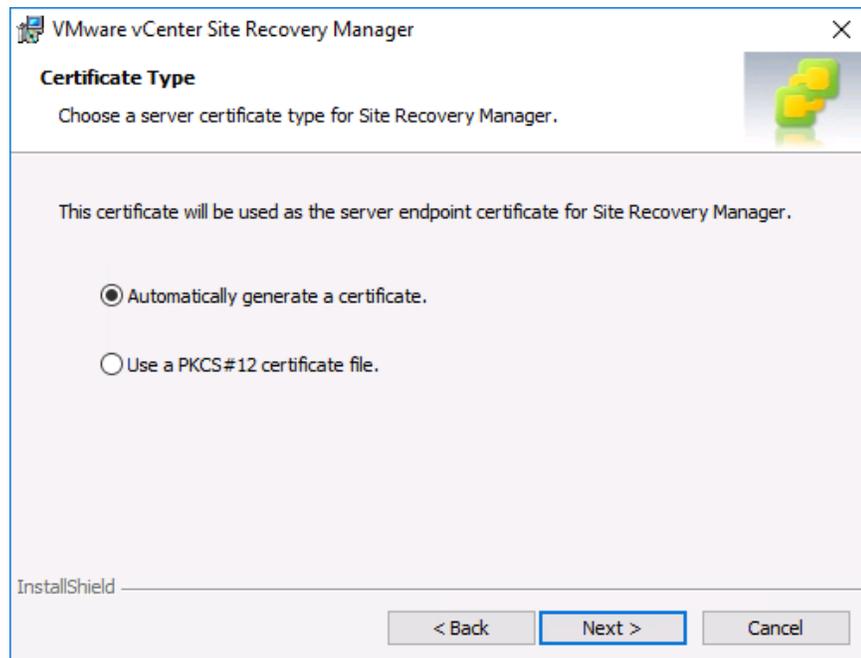
Description:   
 Enter a description to appear in the vSphere plug-ins list

InstallShield

< Back Next > Cancel

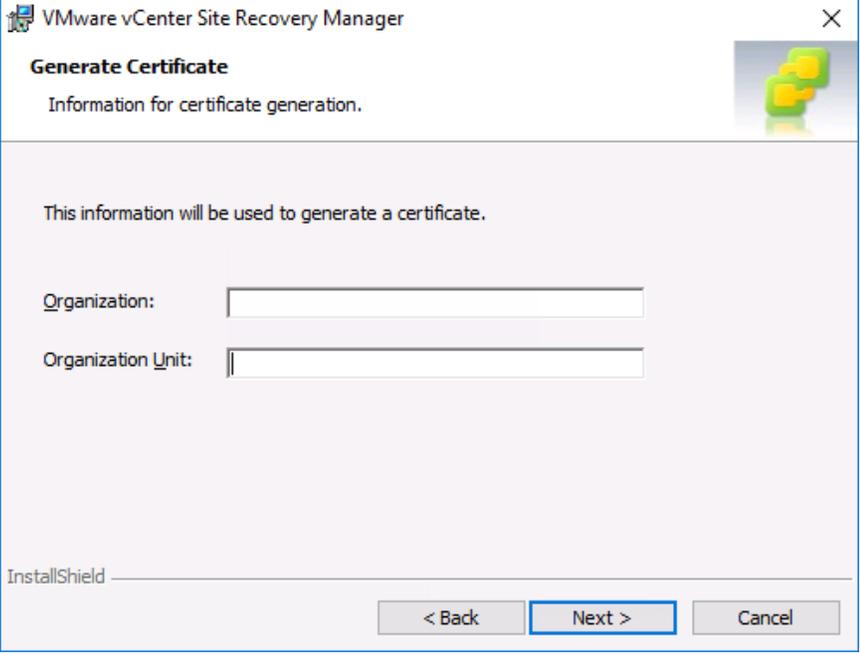


Select the certificate option as appropriate. For the purpose of this evaluation guide we will select "Automatically generate a certificate". If you have the requirement to use a signed certificate follow the installation directions [here](#). Click "Next"



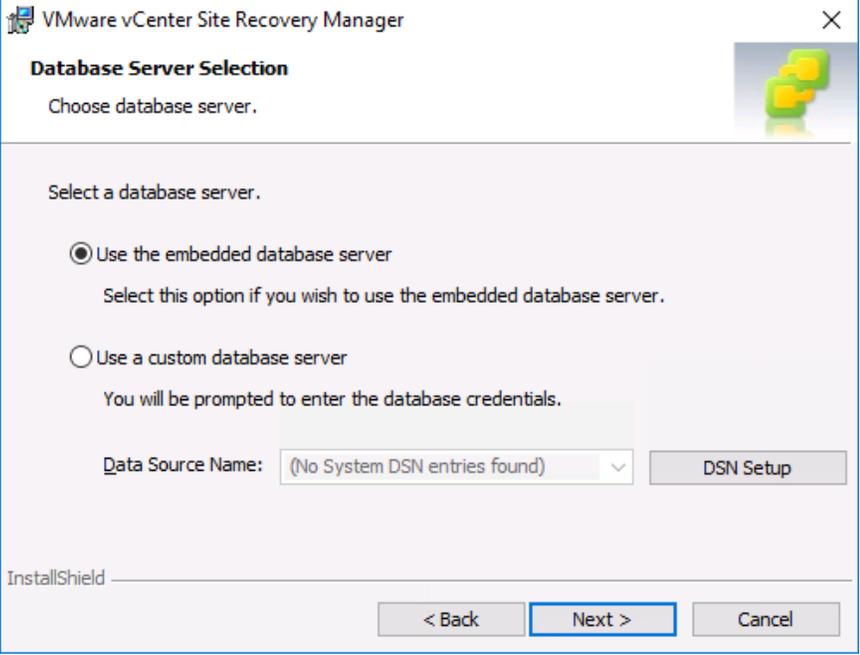
Enter the Organization and Organization Unit for the certificate. Click "Next"





The screenshot shows the 'Generate Certificate' dialog box in VMware vCenter Site Recovery Manager. The title bar reads 'VMware vCenter Site Recovery Manager'. The main heading is 'Generate Certificate' with the subtitle 'Information for certificate generation.' Below this, a message states: 'This information will be used to generate a certificate.' There are two text input fields: 'Organization:' and 'Organization Unit:'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border. The 'InstallShield' logo is visible in the bottom left corner.

Select "Use the embedded database server". The embedded database supports the full scale of VMware Site Recovery. If there is a requirement to use an external database follow the guidance in the [SRM installation guide](#).



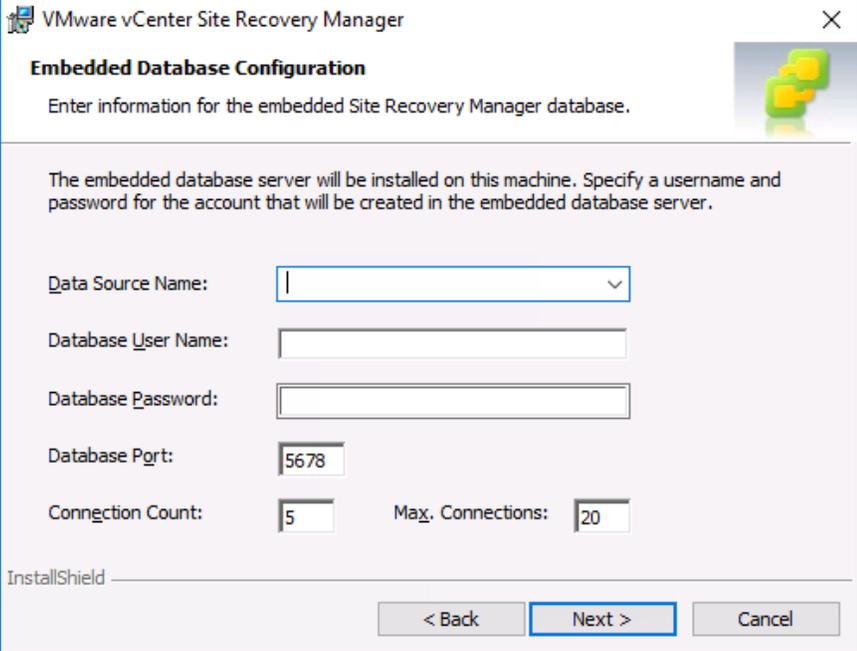
The screenshot shows the 'Database Server Selection' dialog box in VMware vCenter Site Recovery Manager. The title bar reads 'VMware vCenter Site Recovery Manager'. The main heading is 'Database Server Selection' with the subtitle 'Choose database server.' Below this, a message states: 'Select a database server.' There are two radio button options: 'Use the embedded database server' (which is selected) and 'Use a custom database server'. Under the selected option, it says: 'Select this option if you wish to use the embedded database server.' Under the unselected option, it says: 'You will be prompted to enter the database credentials.' There is a 'Data Source Name:' label followed by a dropdown menu showing '(No System DSN entries found)' and a 'DSN Setup' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border. The 'InstallShield' logo is visible in the bottom left corner.



Enter the following:

- Data Source Name (may only contain alphanumeric characters and underscores)
- Database User Name (may only contain lower case alphanumeric characters and underscores. You may not use “postgres”)
- Database Password (may not contain any white spaces, quotation marks, backslashes or extended ASCII characters).
- Do not change the database port, connection count or max connections

Make sure to note down the DSN, DB User Name and DB Password. Click “Next”



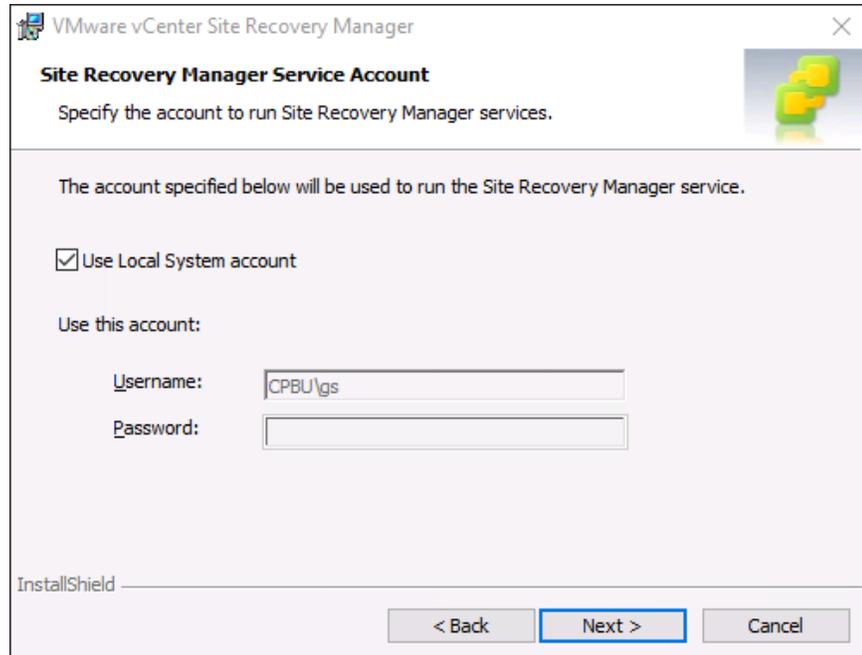
The screenshot shows the 'Embedded Database Configuration' dialog box in VMware vCenter Site Recovery Manager. The dialog has a title bar with the VMware logo and the text 'VMware vCenter Site Recovery Manager'. Below the title bar, the text 'Embedded Database Configuration' is displayed in bold, followed by the instruction 'Enter information for the embedded Site Recovery Manager database.' and a small graphic of three green spheres. The main content area contains the following fields and labels:

- Data Source Name: A dropdown menu with a downward arrow.
- Database User Name: A text input field.
- Database Password: A text input field.
- Database Port: A text input field containing the value '5678'.
- Connection Count: A text input field containing the value '5'.
- Max. Connections: A text input field containing the value '20'.

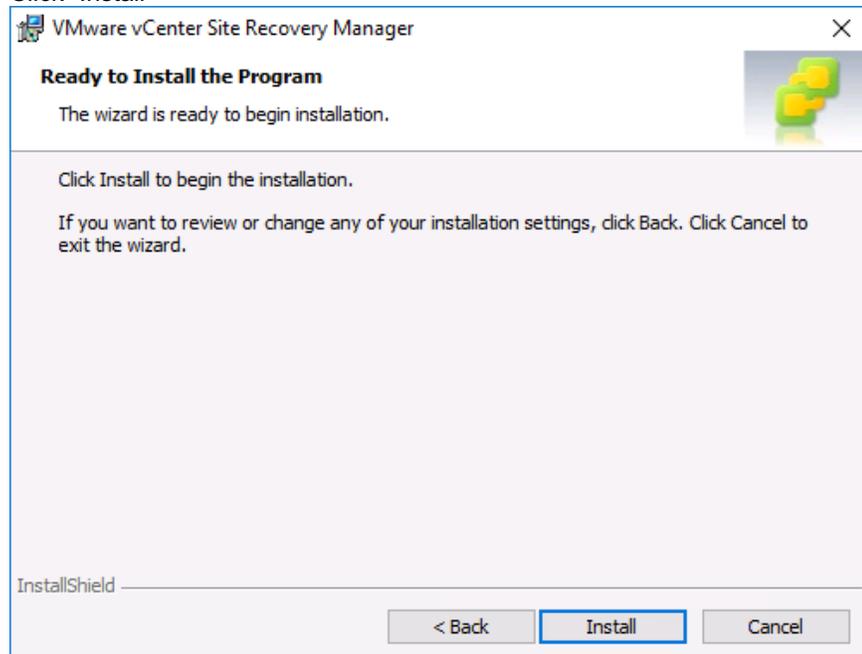
At the bottom of the dialog, the 'InstallShield' logo is visible on the left, and three buttons are on the right: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Select the account used for running the SRM service. Unless otherwise required select the default (Local System Account). Click “Next”



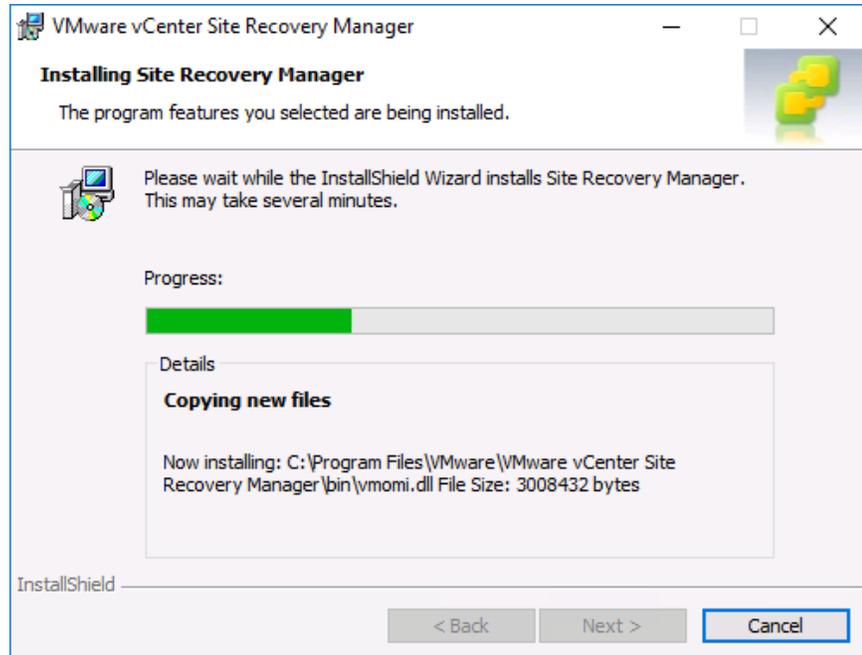


Click "Install"

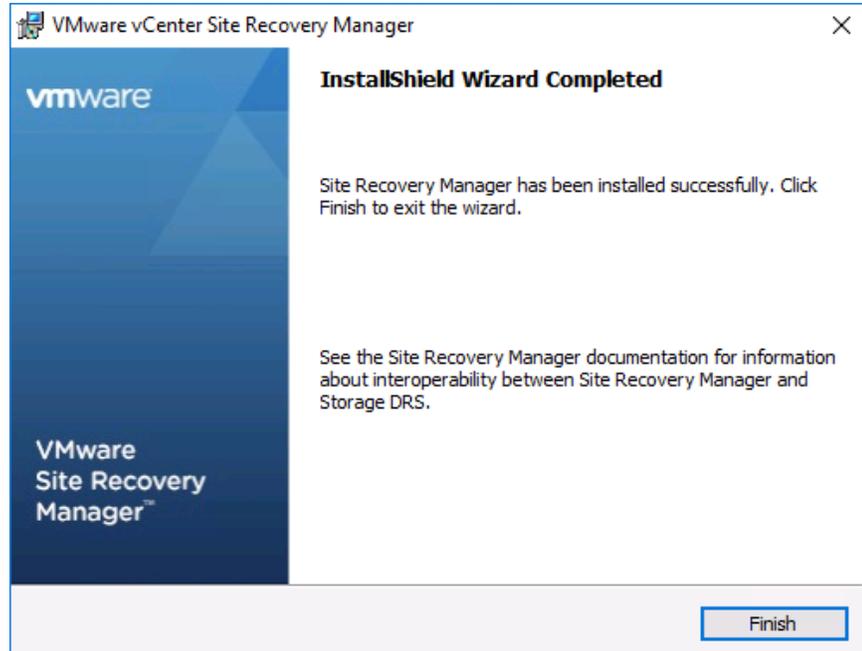


While SRM is installing you can start deploying the vSphere Replication Appliance.





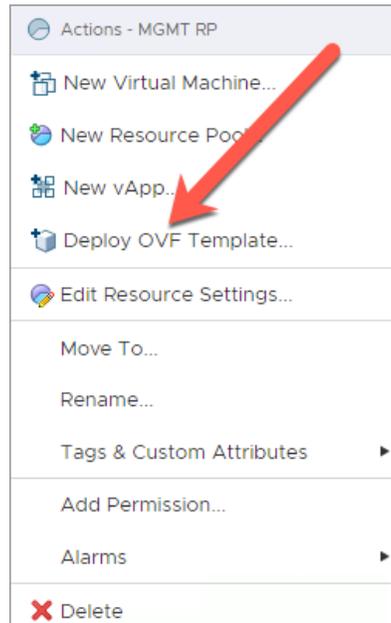
When the installation has finished click "Finish"



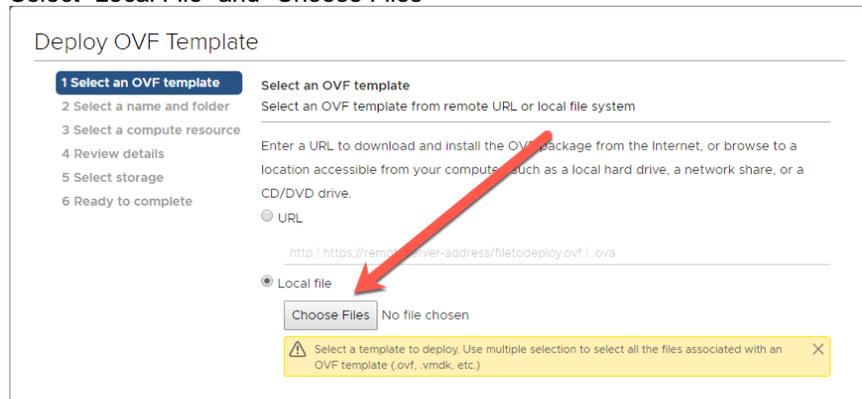
### Installing vSphere Replication



From within the on-premises vCenter, right-click the Cluster or Resource Pool where the appliance will be deployed and select "Deploy OVF Template"



Select "Local File" and "Choose Files"

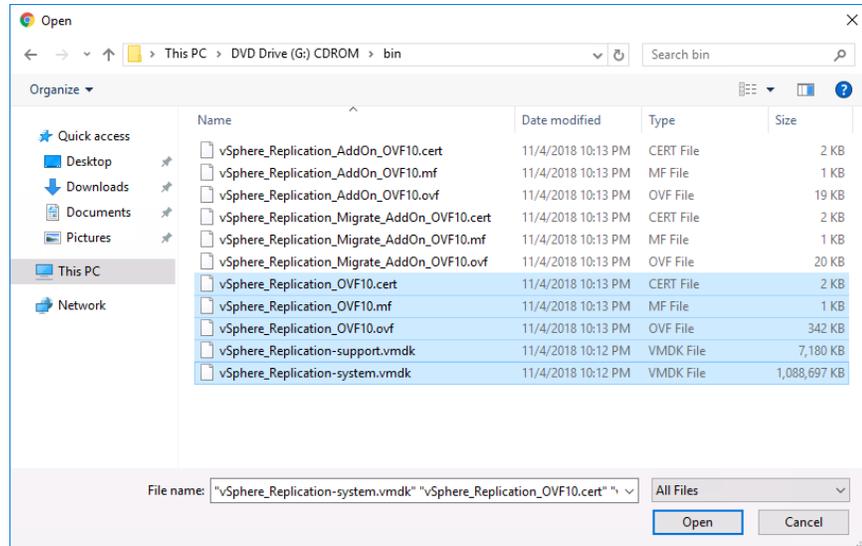


Browse to the CDROM image and the bin folder. Select the following files

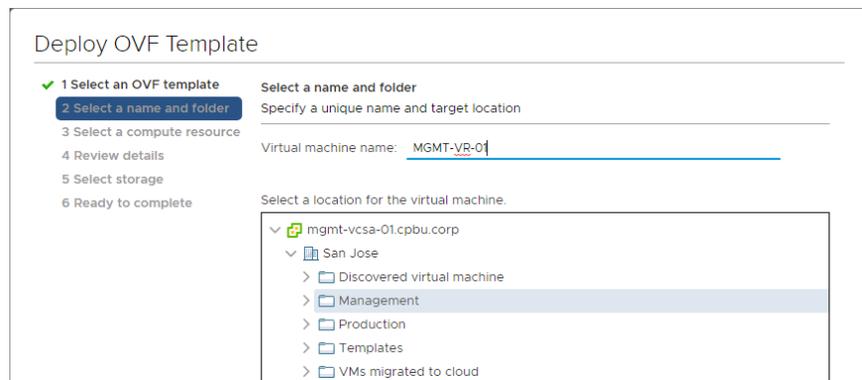
- vSphere\_Replication\_OVF10.cert
- vSphere\_Replication\_OVF10.mf
- vSphere\_Replication\_OVF10.ovf
- vSphere\_Replication-support.vmdk
- vSphere\_Replication-system.vmdk

and click "open" then click "next"



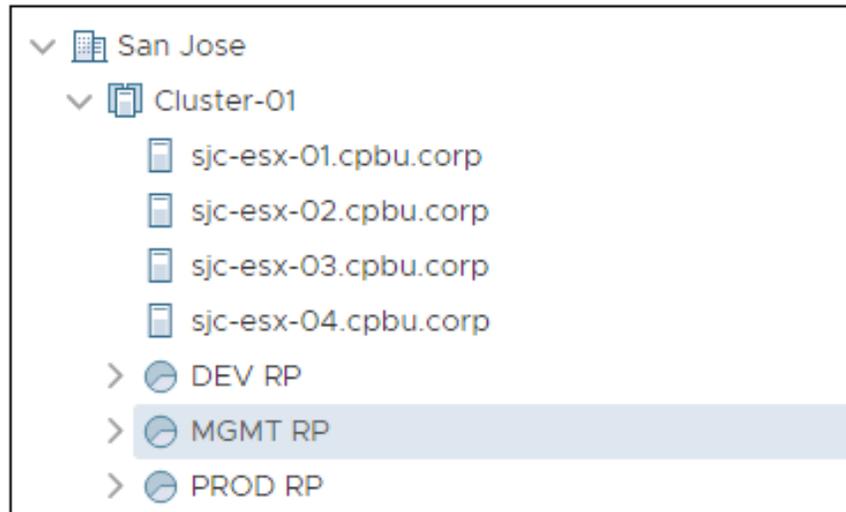


Specify a unique name and target folder for the vSphere Replication Appliance

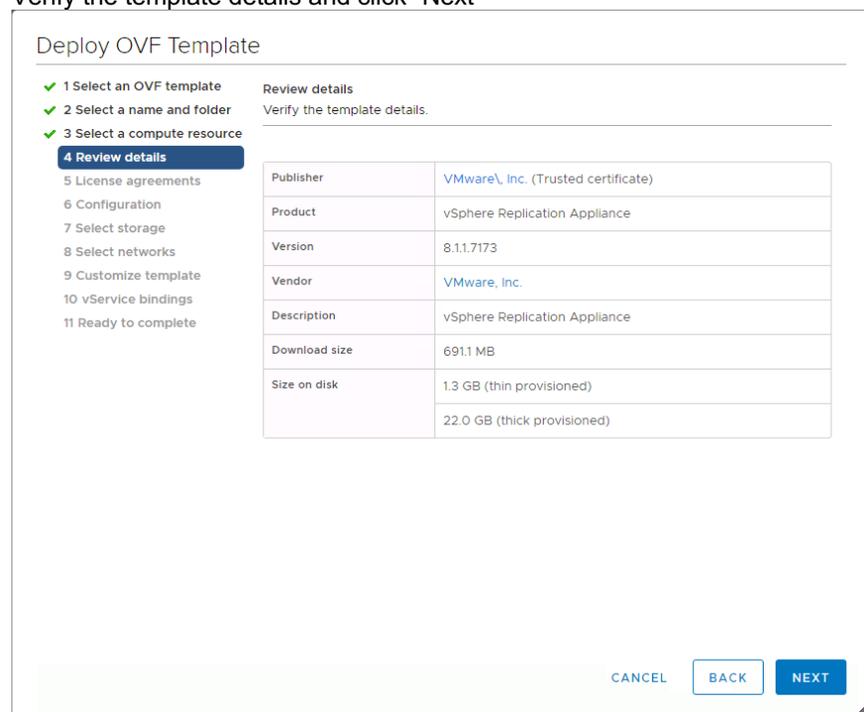


Select a compute resource





Verify the template details and click “Next”



Select the “I accept all license agreements” checkbox. Click “Next”



### Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 vService bindings
- 11 Ready to complete

#### License agreements

The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

vSphere Replication

Copyright (c) 2011, 2012, 2013, 2014, 2015, 2016, 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE

I accept all license agreements.

CANCEL BACK NEXT

Leave the configuration on 4 vCPU. Click “Next”

### Configuration

#### Select a deployment configuration

2 vCPU

4 vCPU

Select a storage location for the vSphere Replication Appliance



Select virtual disk format: As defined in the VM storage policy ▾

VM Storage Policy: Datastore Default ▾

Name	Capacity	Provisioned	Free	Type
 nfs-datastore	57.93 TB	25.24 TB	39.44 TB	NFS
 sjc-esx-01-local	104.25 GB	7.17 GB	97.08 GB	VMFS
 sjc-esx-02-local	104.25 GB	7.17 GB	97.08 GB	VMFS
 sjc-esx-03-local	104.25 GB	7.17 GB	97.08 GB	VMFS
 sjc-esx-04-local	104.25 GB	7.17 GB	97.08 GB	VMFS
 vsanDatastore	10.48 TB	11.67 TB	8.35 TB	Virtual SAN

#### Compatibility

✓ Compatibility checks succeeded.

Select a network for the management interface and an IP allocation. Use a “Static – Manual” configuration for simplicity.

Source Network	Destination Network
Management Network	SJC-CORP-MGMT

1 items

#### IP Allocation Settings

IP allocation: Static - Manual ▾

IP protocol: IPv4 ▾

Enter the password, NTP servers, Hostname and Networking properties for the appliance and click “Next”



**Customize template**

Customize the deployment properties of this software solution.

Application	3 settings
<p>Password</p> <p>The password for the appliance 'root' account.</p> <p>Password <input type="password" value="....."/></p> <p>Confirm <input type="password" value="....."/></p> <p>Password</p>	
<p>NTP Servers</p> <p>A comma-separated list of hostnames or IP addresses of NTP Servers.</p> <p><input type="text" value="....."/></p>	
<p>Hostname</p> <p>The host name for this virtual machine. Provide the FQDN if you use a static IP. Leave blank to reverse look up the IP address if you use DHCP.</p> <p><input type="text" value="....."/></p>	



▼ Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. (from the IP Pool associated with the vSphere network mapped to the 'Management Network' network)  _____
Domain Name	The domain name of this VM. (from the IP Pool associated with the vSphere network mapped to the 'Management Network' network)  _____
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. (from the IP Pool associated with the vSphere network mapped to the 'Management Network' network)  _____
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). (from the IP Pool associated with the vSphere network mapped to the 'Management Network' network)  _____
Management Network IP Address	The IP address for this interface.  _____
Management Network Netmask	The netmask or prefix for this interface.  _____

Click "Next" at the vCenter Extension Installation. Do not change any settings. Click "Finish"



**Ready to complete**

Click Finish to start creation.

Provisioning type	Deploy from template
Name	MGMT-VR-01
Template name	vSphere_Replication_OVF10
Download size	691.1 MB
Size on disk	22.0 GB
Folder	Management
Resource	MGMT RP
Storage mapping	1
All disks	Datastore: vsanDatastore; Format: As defined in the VM storage policy
Network mapping	1
Management Network	SJC-CORP-MGMT
IP allocation settings	
IP protocol	IPV4

After the template has completely deployed and VMware Tools are responding, open a browser to this address: <https://<mgmt IP address or DNS name>:5480>

At the login screen enter the username “root” and the password entered when deploying the OVF



User name:

Password:



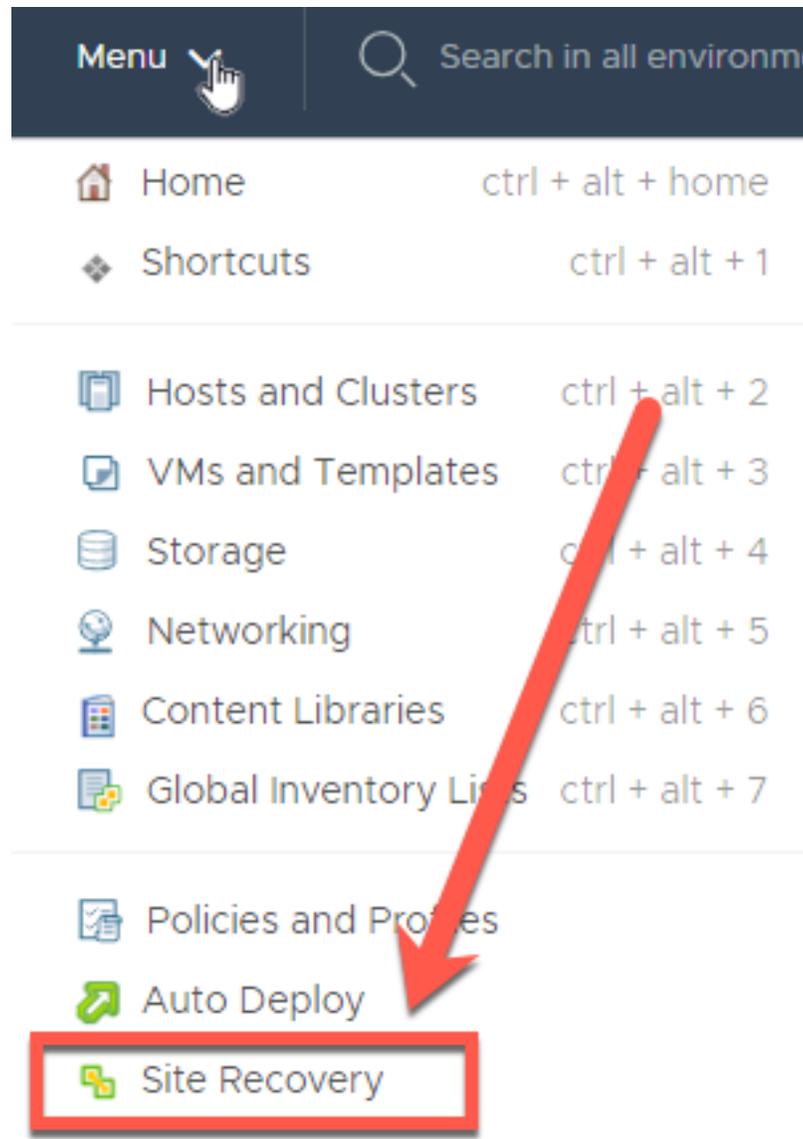
From the Getting Started screen select “Configuration”. Verify that the address of the PSC is entered in the “LookupService Address” field and then type the SSO administrator password. If desired, change the VRM Site Name.

When settings are as desired, click “Save and Restart Service” to complete configuration and start services.



After configuring the vSphere Replication Appliance logout of the vSphere Web Client and then login again.





### Firewall configuration

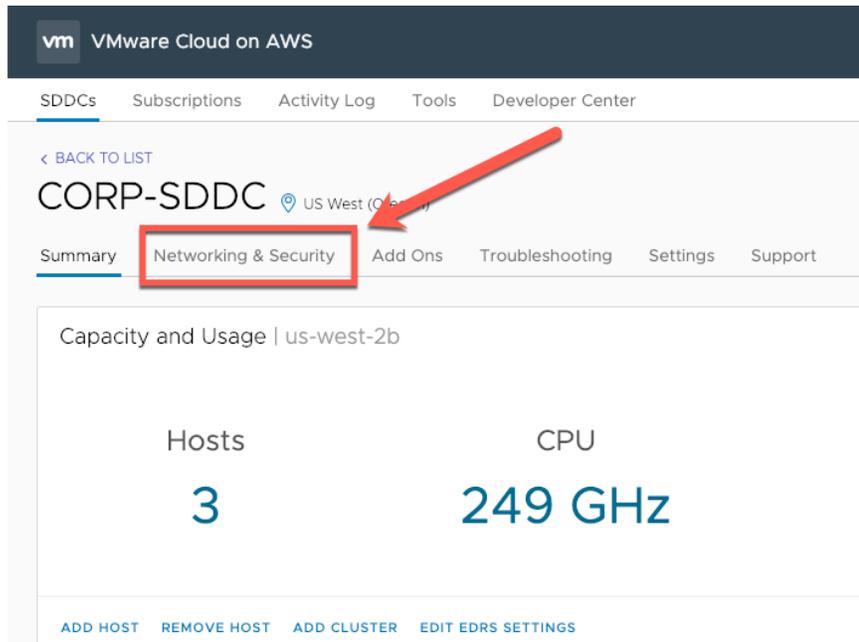
To allow communication and replication traffic between the remote site and the VMware Cloud on AWS SDDC requires the addition of some firewall rules to the management gateway. Rules may also need to be added for the remote site firewall. Those changes are outside of the scope of this guide.

The VMware Cloud on AWS firewall provides flexibility in how strictly is configured. In a basic configuration rules are kept general to allow for a simpler setup and fewer rules. In a highly secure configuration, all aspects of

the rules are explicit which results in a higher level of security and more rules. This evaluation guide will provide details about the simple configurations. For details on the highly secure configuration see the [VMware Site Recovery documentation](#).

### Simple Firewall Configuration

From the SDDC management page select “Networking & Security”



The screenshot shows the VMware Cloud on AWS management console. At the top, there is a navigation bar with the VMware logo and "VMware Cloud on AWS". Below this is a secondary navigation bar with links for "SDDCs", "Subscriptions", "Activity Log", "Tools", and "Developer Center". The main content area displays the details for a SDDC named "CORP-SDDC" located in the "US West (Oregon)" region. A red arrow points to the "Networking & Security" tab, which is highlighted with a red box. Other tabs include "Summary", "Add Ons", "Troubleshooting", "Settings", and "Support". Below the tabs, the "Capacity and Usage | us-west-2b" section shows two metrics: "Hosts" with a value of "3" and "CPU" with a value of "249 GHz". At the bottom of this section, there are links for "ADD HOST", "REMOVE HOST", "ADD CLUSTER", and "EDIT EDRS SETTINGS".

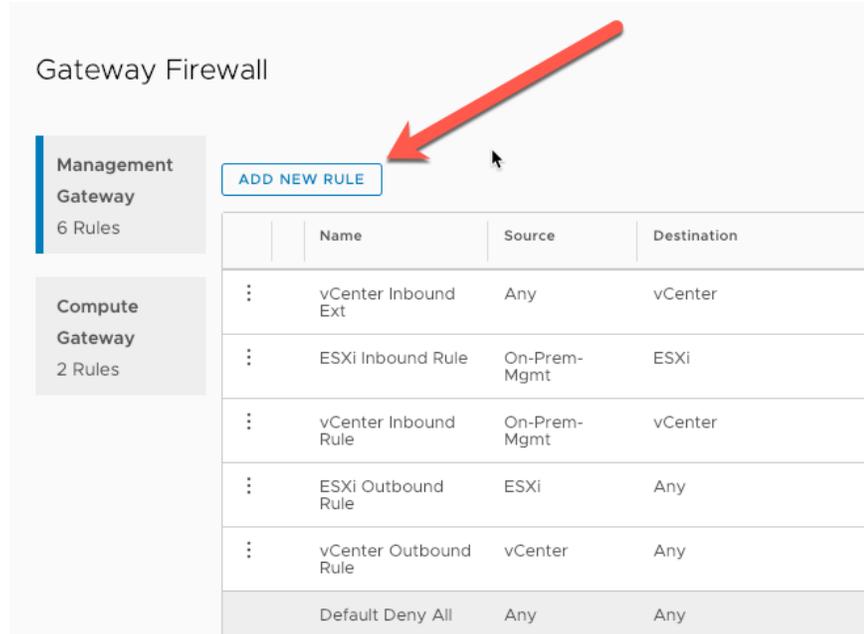
Select the Gateway Firewall



The screenshot displays the VMware Cloud on AWS console interface. At the top, the header shows 'vm VMware Cloud on AWS' and navigation links for 'SDDCs', 'Subscriptions', 'Activity Log', 'Tools', and 'Developer Center'. Below this, the specific SDDC 'CORP-SDDC' is identified, located in 'US West (Oregon)'. A secondary navigation bar includes 'Summary', 'Networking & Security', 'Add Ons', 'Troubleshooting', 'Settings', and 'Support'. On the left, a sidebar menu lists various categories: Overview, Network (Segments, VPN, NAT), Security (Gateway Firewall, Distributed Firewall), Inventory (Groups, Services), Tools (IPFIX, Port Mirroring), and System (DNS, Public IPs, Direct Connect, Connected VPC). The 'Gateway Firewall' option under Security is highlighted with a red box and a red arrow pointing to it. The main content area, titled 'Overview', shows a network diagram. It features a 'Management Gateway' (vCenter NSX) with 'Appliance Subnet' and 'Infrastructure Subnet' details, and a 'Compute Gateway' (Workloads) with '3 Segments, 2 Gateway Firewall Rules & 0 Distributed Firewall Rules, 0 Groups, 0 Public IPs'. The diagram also shows connections to 'Internet', 'On Prem' (with '1 VPN(s) over Internet' and 'No Direct Connect Configured'), and 'Amazon VPC'.

Click "Add New Rule"





Create the following rules (note that for a configuration between SDDCs these would need to be configured at both):

Name	Source	Destination	Services
SRM-VR Inbound to SRM	User defined group that contains remote site SRM, VR and Admin console(s)	VMC on AWS SRM	VMware Site Recovery SRM
SRM-VR Inbound to VR	User defined group that contains remote site SRM, VR, ESXi hosts and Admin console(s)	VMC on AWS VR	VMware Site Recovery vSphere Replication
SRM-VR Inbound to VC	User defined group that contains remote site SRM, VR and Admin console(s)	VMC on AWS vCenter	HTTPS
SRM Outbound	System group – SRM	Remote site group containing VC, PSC, SRM & VR	ANY
VR Outbound	System group – VR	Remote site group containing VC, PSC, SRM & VR	ANY
ESXi Outbound	System group - ESXi	Remote site group containing VR	ANY



Enter the rule "Name"

	Name	Source	Destination	Services
⋮	<input type="text"/>	<a href="#">Set Source</a>	<a href="#">Set Destination</a>	<input type="text"/>

Click "Set Source"

Depending on the rule, select either system defined groups or user defined groups and select the appropriate item from the list.

Select Source(s) - SRM-VR Inbound to SRM ×

Select  Any  System Defined Groups  User Defined Groups

Select System Defined Group(s)

	Name	Member Type	Members
<input type="radio"/>	ESXI	IP Address	10.2.16.0/20, <a href="#">1 more</a>
<input type="radio"/>	HCX	IP Address	10.2.224.25/32
<input type="radio"/>	NSX Manager	IP Address	10.2.192.3/32
<input type="radio"/>	Site Recovery Manager	IP Address	10.2.224.24/32

[REFRESH](#)

1 - 6 of 6 Groups

For User Defined rules if the required group doesn't exist it can be created by clicking on "Create New Group"



Select Source(s) - SRM-VR Inbound to SRM

Select  Any  System Defined Groups  User Defined Groups

Select Group(s)

Name	Member Type	Members
<input type="checkbox"/> On-Prem-Mgmt	IP Address	2 more
<input type="checkbox"/> SRM and VR	IP Address	1 more

REFRESH 1 - 2 of 2 Groups

**CREATE NEW GROUP** CANCEL SAVE

Click on “Set Destination” and select the appropriate destination from the table above.

Select Destination(s) - SRM-VR Inbound to SRM

Select  Any  System Defined Groups  User Defined Groups

*You must select 'System Defined Groups' for destination as source is set to Any/User defined groups for this rule.*

Select System Defined Group(s)

Site Recovery Manager X

Name	Member Type	Members
<input type="radio"/> NSX Manager	IP Address	10.2.192.3/32
<input checked="" type="radio"/> Site Recovery Manager	IP Address	10.2.224.24/32
<input type="radio"/> vCenter	IP Address	10.2.224.4/32
<input type="radio"/> vSphere Replication	IP Address	10.2.224.23/32

Click on the “Services” field. A dropdown will display the supported services. Choose the appropriate service from the table above.

Name	Source	Destination	Services	Action
SRM-VR Ir *	SRM and VR	Site Recovery Manager	<input type="text"/>	Allow
ESXi outbound	ESXi	On-Prem-Mgmt	VM... VMware Site Recovery SRM	Allow

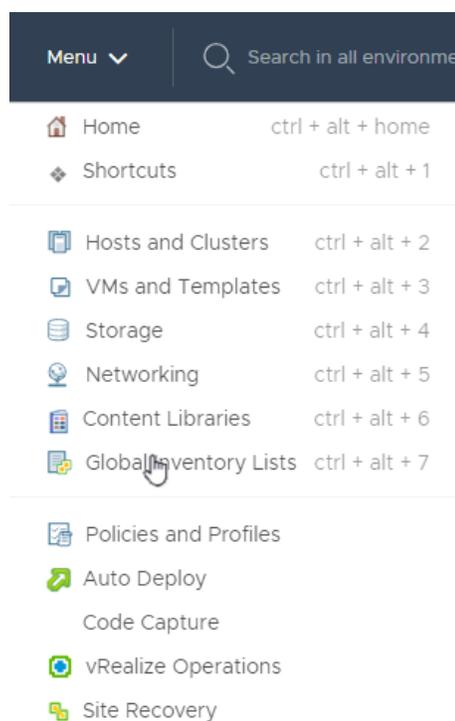


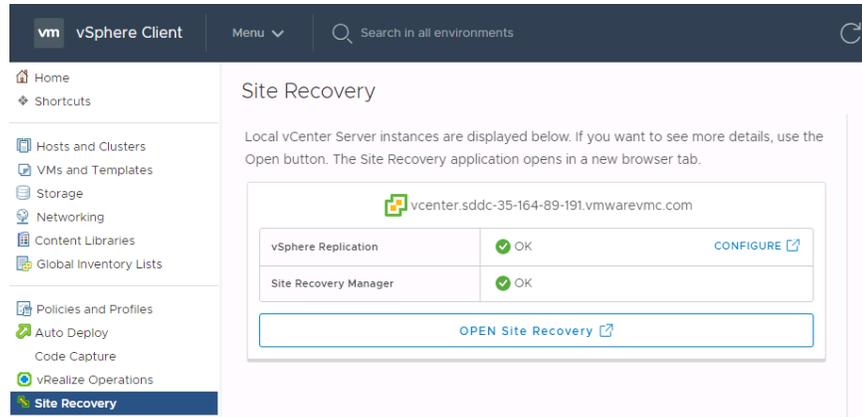
After confirming that the rule has been entered correctly click “Publish” and then enter the next rule. Repeat until all rules have been entered.

## Pairing Sites and Mapping Resources

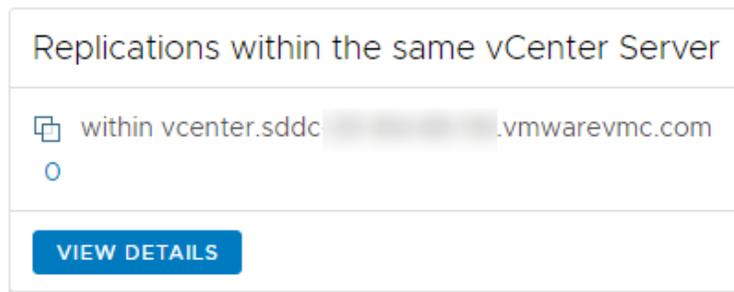
### Pair Sites

To pair VMware Site Recovery open vCenter select Menu > “Site Recovery” and click “Open Site Recovery”. This operation can be run from either the remote site or VMware Cloud on AWS vCenter.





From the Site Recovery screen select “New Site Pair”



Select the vCenter for the first site, the vCenter where this workflow was started and then enter the PSC host name, user name and password for the second site. Click “Next”



**New Site Pair**

- 1 Site details
- 2 vCenter Server and services
- 3 Ready to complete

**Site details**

First site  
Select a local vCenter Servers you want to pair.

vCenter Server  
vcenter.sddc-vmwarevmc.com

Second site  
 Platform Services Controller  
 vCloud Availability (vCloud Director Virtual Datacenter)

Enter the Platform Services Controller details for the vCenter Server

PSC host name: mgmt-vcsa-01.cpbu.corp PSC port: 443  
 User name: administrator@vsphere.local  
 Password: .....

CANCEL NEXT

Select the vCenter you want to pair and then select both the vSphere Replication and Site Recovery Manager services. Click “Next”

**New Site Pair**

- 1 Site details
- 2 vCenter Server and services
- 3 Ready to complete

**vCenter Server and services**

Select the vCenter Server you want to pair.

vCenter Server  
mgmt-vcsa-01.cpbu.corp

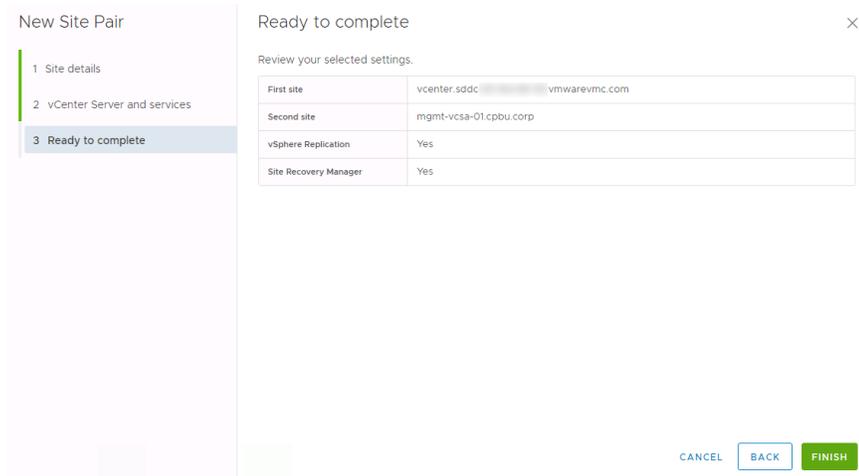
The following services have been identified on the vCenter Servers. Select the ones you want to pair:

Service	vmwarevmc.com	mgmt-vcsa-01.cpbu.corp
<input checked="" type="checkbox"/> vSphere Replication	vmwarevmc.com	San Jose
<input checked="" type="checkbox"/> Site Recovery Manag...	vmwarevmc.com	San Jose

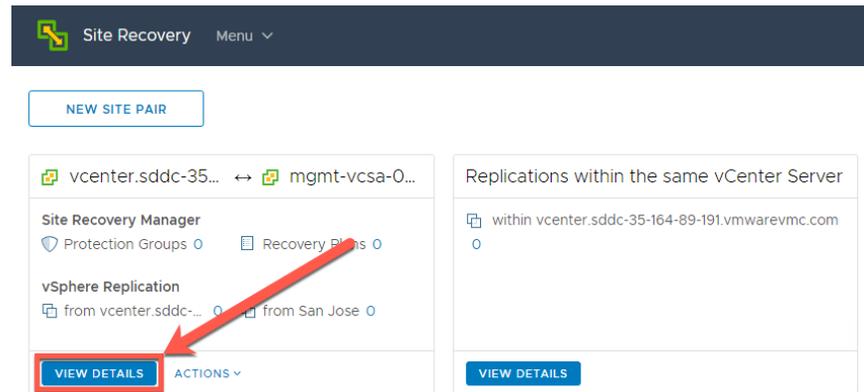
CANCEL BACK NEXT

Confirm the settings and click “Finish”





Once the pairing operation is complete the Site Recovery window now shows the site pair of Site Recovery Manager and vSphere Replication. Click “View Details” to start mapping resources.



### Map Resources

Inventory mappings consist of four types: Resource mappings, folder mappings, storage policy mappings and network mappings. These mappings provide default settings for recovered virtual machines. For example, a mapping can be configured between a network port group named “Production” at the remote site site and a network port group named “Production” at the VMware Cloud on AWS SDDC. As a result of this mapping, virtual machines connected to “Production” at the protected site will, by default, automatically be connected to “Production” at the recovery site.

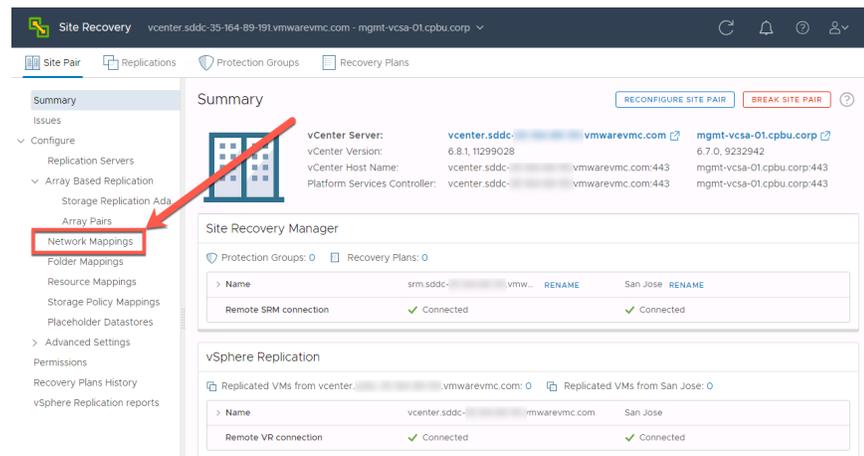


There is no issue with having a port group at each site with the same name since each site is managed by a separate vCenter Server instance. Having port groups at each site with the same name eases VMware Site Recovery configuration. If port groups at the protected and recovery site have different names, the mappings must be created manually.

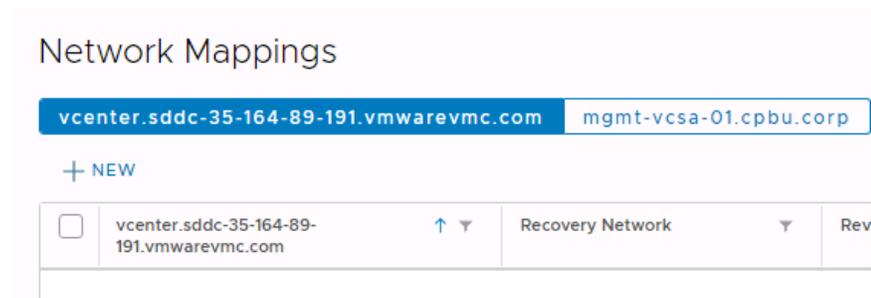
Recommendation: Provide the same name to folders and network port groups with similar functionality at the protected and recovery sites so that mappings can be prepared automatically. Use 1-1 mappings so that reverse mappings can be utilized. These practices will ease inventory-mapping configuration and minimize complexity in the environment.

### Network Mapping

Select “Network Mappings” from the Site Recovery menu

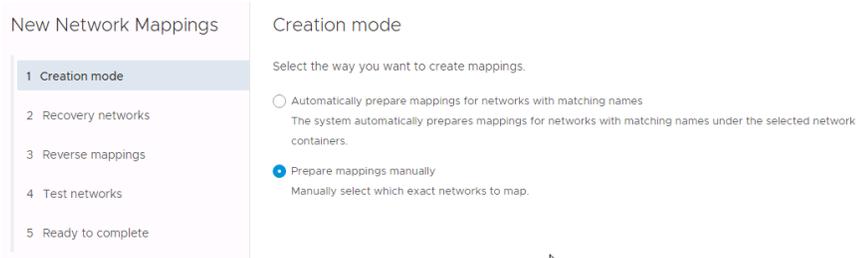


Select “+New”

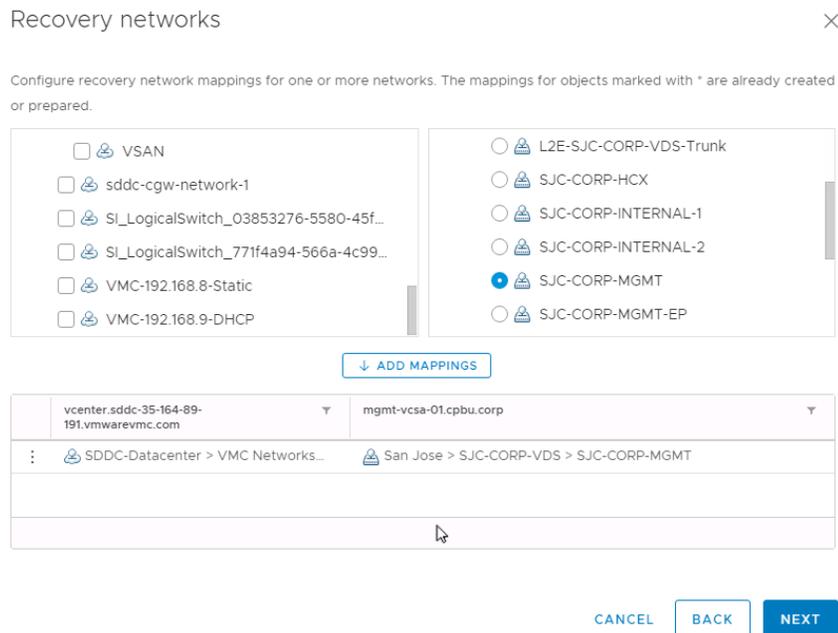


If networks are named the same at the remote site and VMware Cloud on AWS sites choose “Automatically prepare mappings” otherwise choose “Prepare mappings manually”. In this walkthrough the manual option will be selected. Click “Next”

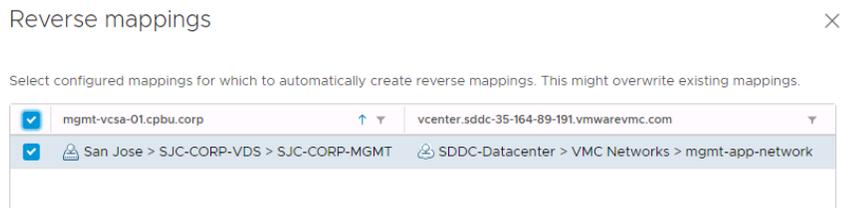




Select networks from each side, one set at a time, that need to be matched. Once they are selected click “Add Mappings” for each then click “Next”



Select the networks that need to have a reverse mapping created. This is usually all networks. Click “Next”



## Test Networks



To support non-disruptive testing of recovery plans VMware Site Recovery supports connecting virtual machines to a test network when a recovery plan test is run. These networks can be one of two type:

- Isolated network (auto created)
- A regular virtual network

### Test networks ✕

Test networks are used instead of the recovery networks while running tests. Isolated networks are automatically created and used during tests for all networks.

i If you want to use different networks for testing, you can do so in the table below. This affects all network mappings that use the same network on the remote site.

Recovery Network	Test Network
San Jose > SJC-CORP-MGMT	Isolated network (auto created)
	Isolated network (auto created)
	L2E-SJC-CORP-VDS-Trunk
	none
	SJC-CORP-HCX
	SJC-CORP-INTERNAL-1

The isolated network is a virtual portgroup that is created on each host at the recovery site with no uplinks. The advantage of this is that no additional network configuration is required. The downside is that virtual machines on different networks and on different hosts won't be able to communicate with each other.

Using a regular virtual network provides the advantage of simulating a production environment including the ability to conduct application testing. The challenge is that it requires work to keep the test traffic isolated. This is a challenge because currently all routed networks in VMware Cloud on AWS are routed to all others. This obviously won't work to keep test traffic isolated from production.

In a VMware Cloud on AWS SDDC the current ways to keep test traffic isolated are:

- Stretched L2 networks to the on-premises site and route those networks at the on-premises site
- Use HCX between the on-premises site and the VMware Cloud on AWS SDDC and route traffic at the on-premises site

In this guide the auto created isolated network will be used. Click "Next"



### Test networks

Test networks are used instead of the recovery networks while running tests. Isolated networks are automatically created and used during tests for all networks.

ⓘ If you want to use different networks for testing, you can do so in the table below. This affects all network mappings that use the same network on the remote site.

Recovery Network	Test Network
San Jose > SJC-CORP-MGMT	Isolated network (auto created)
	Isolated network (auto created)
	L2E-SJC-CORP-VDS-Trunk
	none
	SJC-CORP-HCX
	SJC-CORP-INTERNAL-1

### IP Subnet Mapping

To customize IP addresses as part of failover VMware Site Recovery supports either customizing addresses on an individual virtual machine basis or, by combining network mapping with IP customization. This allows for any virtual machine that is associated with the network mapping to automatically have its IP address changed.

In the IP Customization section click “Add”

Network Mappings Learn more

vcenter.sddc-35-164-89-191.vmwarevmc.com | mgmt-vcasa-01.cpbu.corp

+ NEW | EDIT | DELETE | ...

	Recovery Network	Reverse Mapping	Test Network	IP Customization
<input checked="" type="checkbox"/>	vcenter.sddc-35-164-89-191.vmwarevmc.com			
<input checked="" type="checkbox"/>	VMC-192.168.8-Static	SJC-CORP-WORKLOADS	Yes	Isolated network (auto created)

1 network mapping(s)

IP Customization

There is no IP customization rule attached to this network mapping.

**ADD**

Enter the appropriate information for the source and recovery site and click “Save”



This rule is used for IP customization of the eligible virtual machines.

Specify subnet IP ranges to be mapped on the protected and recovery sites.

	vcenter.sddc-35-164-89-191.vmwarevmc.com	mgmt-vcsa-01.cpbu.corp
Network:	VMC-192.168.8-Static	SJC-CORP-WORKLOADS
Subnet:	192.168.8.0 / 24	172.17.31.0 / 24
Subnet mask:	255.255.255.0	255.255.255.0
Range:	192.168.8.0 - 192.168.8.255	172.17.31.0 - 172.17.31.255

Enter settings for the recovery network.

Gateway:

DNS addresses:

DNS suffixes:

## Network Mappings

[Learn more](#)

	vcenter.sddc-35-164-89-191.vmwarevmc.com	mgmt-vcsa-01.cpbu.corp				
<a href="#">+ NEW</a>   <a href="#">EDIT</a>   <a href="#">DELETE</a>   ...	<input checked="" type="checkbox"/>	vcenter.sddc-35-164-89-191.vmwarevmc.com	Recovery Network	Reverse Mapping	Test Network	IP Customization
<input checked="" type="checkbox"/>	VMC-192.168.8-Static	SJC-CORP-WORKLOADS	Yes	Isolated network (auto created)	Yes	

1 network mapping(s)

## IP Customization

[EDIT](#) [REMOVE](#)

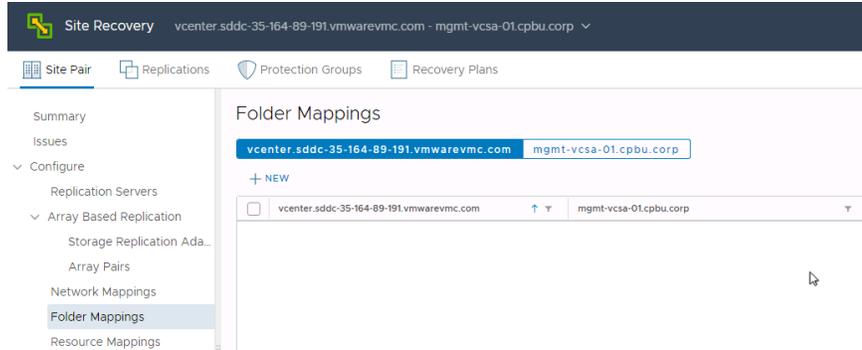
Site	vcenter.sddc-35-164-89-191.vmwarevmc.com	mgmt-vcsa-01.cpbu.corp
Network	VMC-192.168.8-Static	SJC-CORP-WORKLOADS
Subnet	192.168.8.0	172.17.31.0
Subnet mask	255.255.255.0	255.255.255.0
Range start	192.168.8.0	172.17.31.0
Range end	192.168.8.255	172.17.31.255

Next select the other vCenter and create the reverse IP customization rule

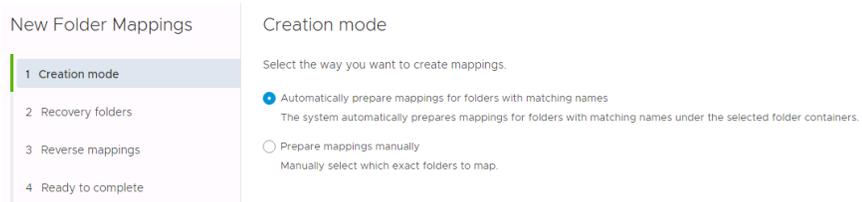
## Folder Mapping

Folder mappings are much the same as network mappings without the added complexity of IP customization and test networks. To create folder mappings, select "Folder Mappings" and click "+New".

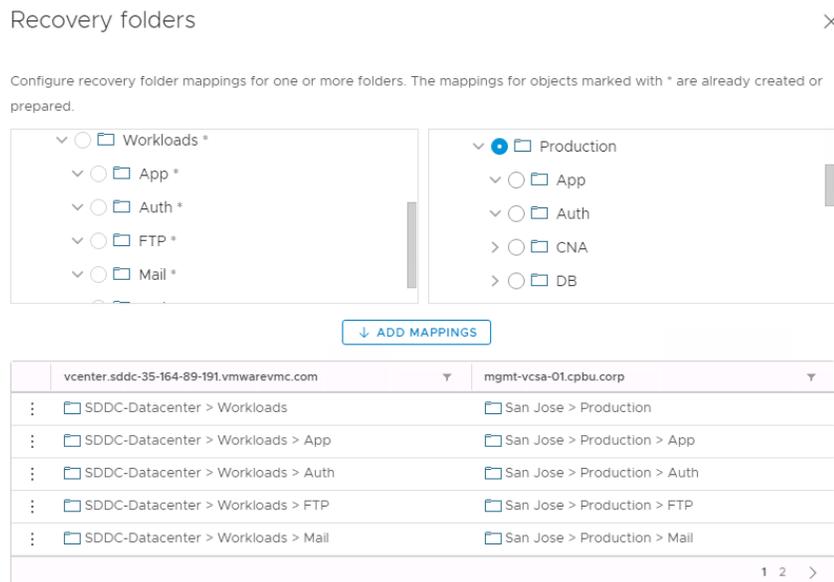




This example will show the “Automatically prepare mappings” option. Select it and click “Next”



Select the level of the hierarchy where the folder names match and click “Add Mappings” and after all mappings have been added “Next”



Select all to create reverse mappings and click “Next”



### Reverse mappings



Select configured mappings for which to automatically create reverse mappings. This might overwrite existing mappings.

<input checked="" type="checkbox"/>	mgmt-vcsa-01.cpbu.corp	↑ ↓	vcenter.sddc-35-164-89-191.vmwarevmc.com	↓
<input checked="" type="checkbox"/>	San Jose > Production		SDDC-Datacenter > Workloads	
<input checked="" type="checkbox"/>	San Jose > Production > App		SDDC-Datacenter > Workloads > App	
<input checked="" type="checkbox"/>	San Jose > Production > Auth		SDDC-Datacenter > Workloads > Auth	
<input checked="" type="checkbox"/>	San Jose > Production > FTP		SDDC-Datacenter > Workloads > FTP	
<input checked="" type="checkbox"/>	San Jose > Production > Mail		SDDC-Datacenter > Workloads > Mail	
<input checked="" type="checkbox"/>	San Jose > Production > Web		SDDC-Datacenter > Workloads > Web	

Review the settings and click “Finish”

vcenter.sddc-35-164-89-191.vmwarevmc.com	mgmt-vcsa-01.cpbu.corp	Reverse Mapping
<input type="checkbox"/> SDDC-Datacenter > Workloads	<input type="checkbox"/> San Jose > Production	Yes
<input type="checkbox"/> SDDC-Datacenter > Workloads > App	<input type="checkbox"/> San Jose > Production > App	Yes
<input type="checkbox"/> SDDC-Datacenter > Workloads > Auth	<input type="checkbox"/> San Jose > Production > Auth	Yes
<input type="checkbox"/> SDDC-Datacenter > Workloads > FTP	<input type="checkbox"/> San Jose > Production > FTP	Yes
<input type="checkbox"/> SDDC-Datacenter > Workloads > Mail	<input type="checkbox"/> San Jose > Production > Mail	Yes
<input type="checkbox"/> SDDC-Datacenter > Workloads > Web	<input type="checkbox"/> San Jose > Production > Web	Yes

### Folder Mappings

[Learn more](#)

vcenter.sddc-35-164-89-191.vmwarevmc.com		mgmt-vcsa-01.cpbu.corp		Reverse Mapping Exists
<input type="checkbox"/>	App	<input type="checkbox"/>	App	Yes
<input type="checkbox"/>	Auth	<input type="checkbox"/>	Auth	Yes
<input type="checkbox"/>	FTP	<input type="checkbox"/>	FTP	Yes
<input type="checkbox"/>	Mail	<input type="checkbox"/>	Mail	Yes
<input type="checkbox"/>	Web	<input type="checkbox"/>	Web	Yes
<input type="checkbox"/>	Workloads	<input type="checkbox"/>	Production	Yes

### Resource Pool and Storage Policy Mapping

Resource Pool and Storage Policy mappings are handled in the same way as Folder mappings. All resources for virtual machines that will be failed over need to be mapped.



### Resource Mappings

vcenter.sddc-35-164-89-191.vmwarevmc.com mgmt-vcsa-01.cpbu.corp

+ NEW

<input type="checkbox"/>	vcenter.sddc-35-164-89-191.vmwarevmc.com	↑ ▾	mgmt-vcsa-01.cpbu.corp	▾	Reverse Mapping
<input type="checkbox"/>	Compute-ResourcePool		Cluster-01		Yes
<input type="checkbox"/>	DEV RP		DEV RP		Yes
<input type="checkbox"/>	PROD RP		PROD RP		Yes

### Storage Policy Mappings

[Learn more](#)

vcenter.sddc-35-164-89-191.vmwarevmc.com mgmt-vcsa-01.cpbu.corp

+ NEW

<input type="checkbox"/>	vcenter.sddc-35-164-89-191.vmwarevmc.com	↑ ▾	mgmt-vcsa-01.cpbu.corp	▾	Reverse Mapping Exists	▾
<input type="checkbox"/>	Datastore Default		Datastore Default		Yes	
<input type="checkbox"/>	Host-local PMem Default Storage Policy		Host-local PMem Default Storage Policy		Yes	
<input type="checkbox"/>	VM Encryption Policy		VM Encryption Policy		Yes	
<input type="checkbox"/>	vSAN Default Storage Policy		vSAN Default Storage Policy		Yes	
<input type="checkbox"/>	VVol No Requirements Policy		VVol No Requirements Policy		Yes	

### Placeholder Datastores

Placeholder datastores are used to store placeholder virtual machines. A placeholder datastore must be defined for each site.

A placeholder virtual machine is a subset of virtual machine files. VMware Site Recovery uses that subset of files to register a virtual machine with vCenter Server on the recovery site.

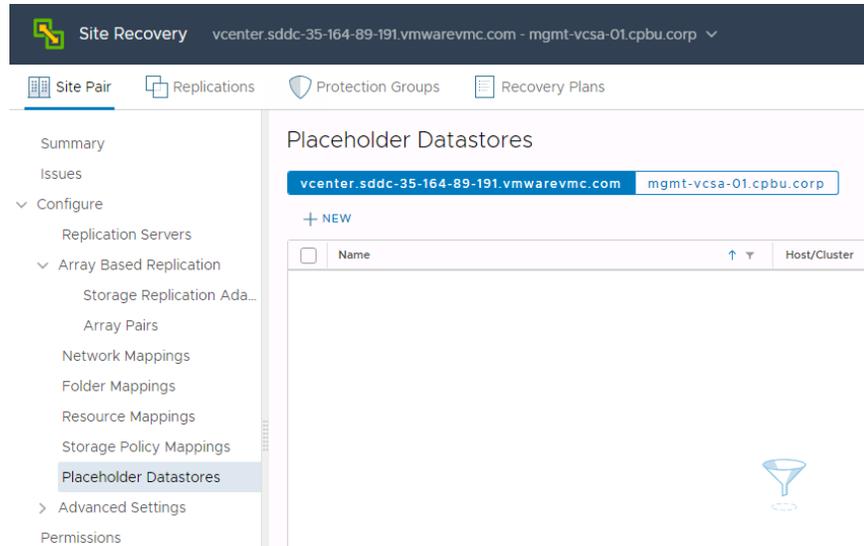
The files of the placeholder virtual machines are very small, and do not represent full copies of the protected virtual machines.

The placeholder virtual machine does not have any disks attached to it.

The placeholder virtual machine reserves compute resources on the recovery site and provides the location in the vCenter Server inventory to which the protected virtual machine recovers when you run recovery.

Select "Placeholder Datastores" from the Site Recovery Menu and click "+New"





For the VMware Cloud on AWS SDDC select the Workload Datastore and click “Add”

### New Placeholder Datastore ✕

Select non-replicated datastores in which SRM creates placeholder virtual machines. To enable planned migration and reprotect, you must select placeholder datastores at both sites.



For the remote site site, choose any datastore that is accessible from all hosts and isn't replicated.



New Placeholder Datastore ×

Select non-replicated datastores in which SRM creates placeholder virtual machines. To enable planned migration and reprotect, you must select placeholder datastores at both sites.

<input type="checkbox"/>	Name	↑ ↓
<input type="checkbox"/>	nfs-datastore	
<input type="checkbox"/>	sjc-esx-01-local	
<input type="checkbox"/>	sjc-esx-02-local	
<input type="checkbox"/>	sjc-esx-03-local	
<input type="checkbox"/>	sjc-esx-04-local	
<input checked="" type="checkbox"/>	vsanDatastore	

## Placeholder Datastores

vcenter.sddc-35-164-89-191.vmwarevmc.com **mgmt-vcsa-01.cpbu.corp**

+ NEW

<input type="checkbox"/>	Name	↑ ↓	Host/Cluster
<input type="checkbox"/>	vsanDatastore		Cluster-01

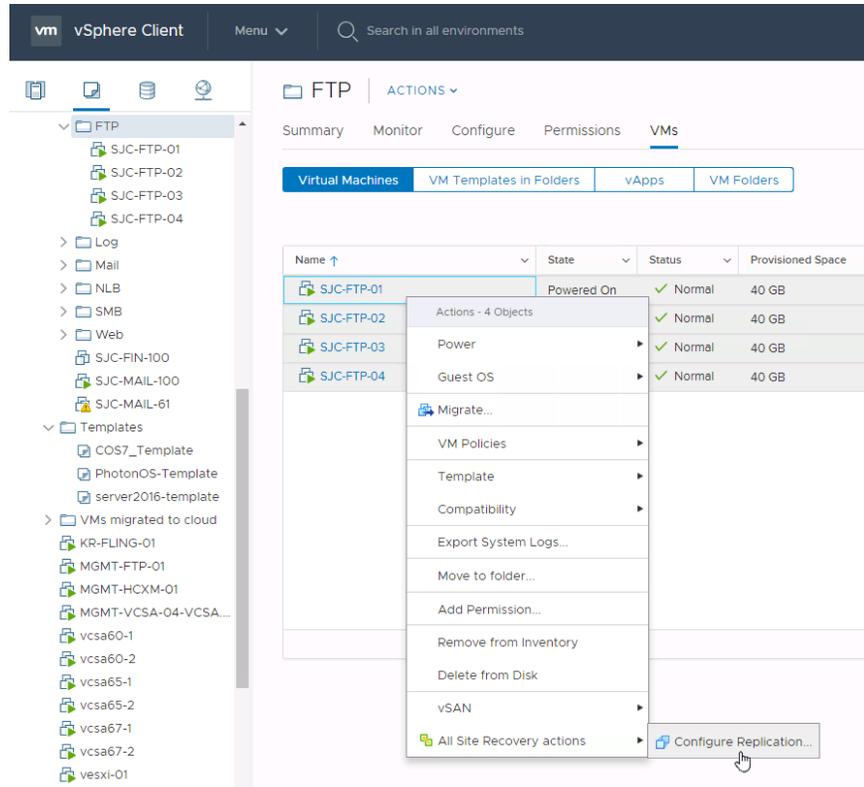
**Protect VMs**

With mapping completed the next step is to start replicating and protecting virtual machines. The process of replicating virtual machines and adding them to protection groups and recovery plans is combined in VMware Site Recovery.

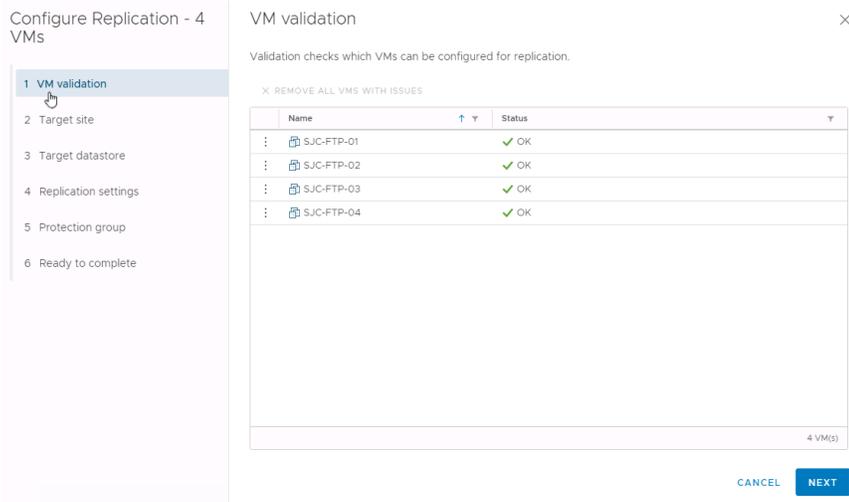
**Replication**

The easiest way to replicate virtual machines is to select them in the vSphere Web Client, right-click them and select "All Site Recovery actions" > "Configure Replication"





Select “Yes” to the “Open Configure replication wizard for the 4 selected virtual machines?” dialog. Confirm the correct virtual machines have been selected and click “Next”



Select the target site for the replicated virtual machines. In this example we are protecting virtual machines that are running remote site so we will select our VMware Cloud on AWS SDDC. Then click “Next”

Target site ✕

ⓘ Select a target site for the replicated virtual machine. ✕

Select the target site where the virtual machines will be replicated.

	Target Site	Status
<input type="radio"/>	mgmt-vcasa-01.cpbu.corp	✓ Logged in
<input checked="" type="radio"/>	vcenter.sddc-35-164-89-191.vmwarevmc.com	✓ Logged in

2 site(s)

Select the vSphere Replication server that will handle the replication.

Auto-assign vSphere Replication Server  
 Manually select vSphere Replication Server

	Name	Replications
<input type="radio"/>	vr (embedded)	0

1 replication server(s)

CANCEL
BACK
NEXT

Next select the target disk format, storage policy and datastore

Target datastore ✕

Select a datastore for the replicated files.

Configure datastore per virtual machine

The selected virtual machines are using 59.36 GB. ⓘ

Disk format: Same as source

VM storage policy: Datastore Default

	Name	Capacity	Free	Type
<input checked="" type="radio"/>	WorkloadDatastore	31.1 TB	25.34 TB	vsan

Now select replication settings. Recovery Point Objective (RPO) can be adjusted per virtual machine from 5 minutes up to 24 hours. vSphere Replication also supports guest OS quiescing for modern Windows virtual machines and some versions of Linux. If bandwidth is a concern some CPU can be traded for some bandwidth by enabling network compression. Note that point in time instances are not currently support for VMware Site Recovery. Select options and click “Next”



### Replication settings ×

Configure the replication settings for the virtual machines.

Recovery point objective (RPO) ⓘ

5 minutes 
|
|
|
 24 hours

1 hour

Enable point in time instances ⓘ

Keep  instances per day for the last  days

If the RPO period is longer than 8 hours, you might want to decrease the RPO value to allow vSphere Replication to create the number of instances that you want to keep.

Enable guest OS quiescing ⓘ

Enable network compression for VR data ⓘ

CANCEL
BACK
NEXT

### Protection Groups

Protection groups are groups of virtual machines that are recovered together. They often are made up of all the virtual machines that make up an application. A virtual machine can only belong to a single protection group however a protection group can belong to one or more recovery plans. Workflows like failover, test and reprotect are run at the recovery plan level so this separation creates flexibility.



### Configure Replication - 4 VMs

- 1 VM validation
- 2 Target site
- 3 Target datastore
- 4 Replication settings
- 5 Protection group
- 6 Recovery plan
- 7 Ready to complete

### Protection group

You can add these virtual machines to a protection group.

Add to existing protection group  
 Add to new protection group  
 Do not add to protection group now

Protection group name:

### Recovery Plans

A recovery plan is like an automated run book. It controls every step of the recovery process, including the order in which VMware Site Recovery powers on and powers off virtual machines, the network addresses that recovered virtual machines use, and so on. Recovery plans are flexible and customizable.

A recovery plan includes one or more protection groups. You can include a protection group in more than one recovery plan. For example, you can create one recovery plan to handle a planned migration of services from the protected site to the recovery site for the whole organization, and another set of plans per individual departments. In this example, having these different recovery plans referencing one protection group allows you to decide how to perform recovery.

### Configure Replication - 4 VMs

- 1 VM validation
- 2 Target site
- 3 Target datastore
- 4 Replication settings
- 5 Protection group
- 6 Recovery plan
- 7 Ready to complete

### Recovery plan

You can optionally add this protection group to a recovery plan.

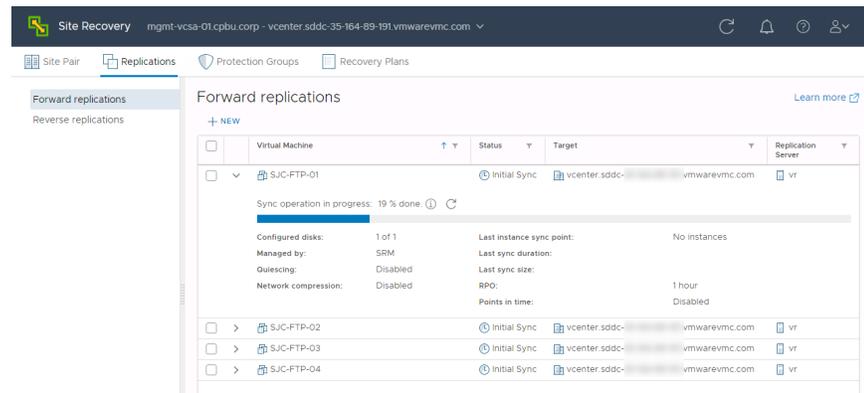
Add to existing recovery plan  
 Add to new recovery plan  
 Do not add to recovery plan now

Recovery plan name:



## Monitoring Replications

Replication status can be monitored in the “Replications” section of the Site Recovery interface

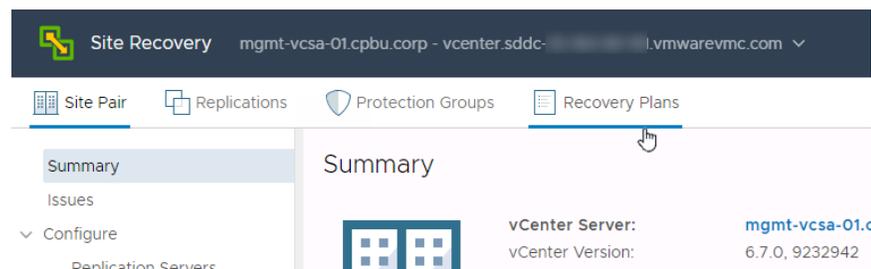


## Priority Groups and Dependencies

VMware Site Recovery starts virtual machines on the recovery site according to the priority that you set. VMware Site Recovery starts priority 1 virtual machines first, then priority 2 virtual machines second, and so on. VMware Site Recovery uses VMware Tools heartbeat to discover when a virtual machine is running on the recovery site. In this way, VMware Site Recovery can ensure that all virtual machines of a given priority are running before it starts the virtual machines of the next priority. For this reason, you must install VMware Tools on protected virtual machines.

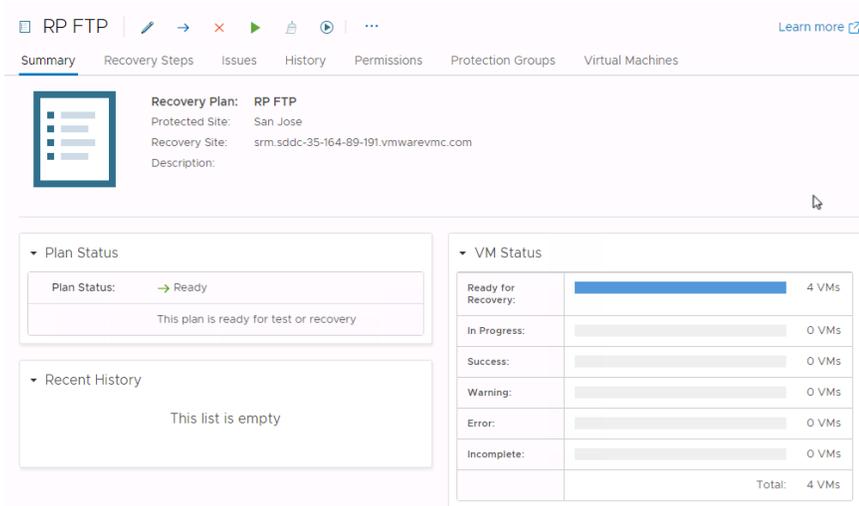
If a virtual machine depends on services that run on another virtual machine in the same protection group, you can configure a dependency between the virtual machines. By configuring a dependency, you can ensure that the virtual machines start on the recovery site in the correct order. Dependencies are only valid if the virtual machines have the same priority.

To select priority groups and create dependencies navigate to the “Recovery Plans” section and click on the recovery plan

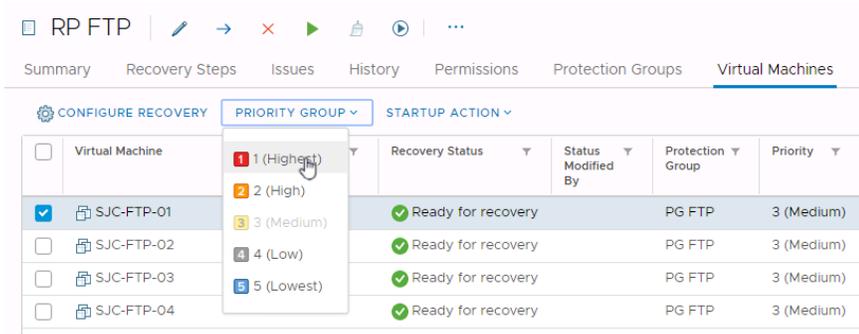


Now select “Virtual Machines”





Select one or more virtual machines and click the “Priority Group” dropdown to adjust the priority group for them



By selecting “Configure Recovery” you will see a number of additional options.



## VM Recovery Properties - SJC-FTP-04

Changes to these properties will apply to this VM in all recovery plans.

Recovery Properties IP Customization

Priority Group 3 (Medium) ⓘ

VM Dependencies

View all

Select the VMs which will be started before this VM:

<input type="checkbox"/>	Virtual Machine	Status	Priority Group	Protection Group
<input type="checkbox"/>	SJC-FTP-01	Higher Priority	1 (Highest)	PG FTP
<input type="checkbox"/>	SJC-FTP-02	Higher Priority	2 (High)	PG FTP
<input checked="" type="checkbox"/>	SJC-FTP-03	OK	3 (Medium)	PG FTP
<input checked="" type="checkbox"/>	1			3 VM(s)

VM dependencies are ignored if the VMs are not in the same priority group. If VM dependencies fail, a warning will be displayed, but the recovery plan will continue.

vMotion Disabled (VM is not in a storage policy protection group)

Shutdown Action Shutdown guest OS before power off (requires VMware Too ⓘ)

### Shutdown Actions

Shutdown actions apply to the protected virtual machines at the protected site during the run of a recovery plan. Shutdown actions are not used during the test of a recovery plan. By default, VMware Site Recovery will issue a guest OS shutdown, which requires VMware Tools and there is a time limit of five minutes. The time limit can be modified. If the guest OS shutdown fails and the time limit is reached, the virtual machine is powered off. Shutting down and powering off the protected virtual machines at the protected site when running a recovery plan is important for a few reasons:

- Quiesces the guest OS and applications before the final storage synchronization occurs
- Avoids the potential conflict of having virtual machines with duplicate network configurations (hostname, IP addresses) on the same network

Optionally, the shutdown action can be changed to simply power off virtual machines. Powering off virtual machines does not shut them down gracefully, but this option can reduce recovery times in situations where the protected site and recovery site maintain network connectivity during the run (not test) of a recovery plan. An example of this is a disaster avoidance scenario.

**Recommendation:** In most cases, minimizing risk and data loss are higher priorities than recovery time. Keep the default Shutdown Action setting of "Shutdown guest OS before power off" to properly quiesce the guest OS and applications, where possible, during a planned migration and disaster recovery.

### Startup Actions

A startup action applies to a virtual machine that is recovered by VMware Site Recovery. Powering on a virtual machine after it is recovered is the default setting and this is typically not changed. In some cases, it might be desirable



to recover a virtual machine, but leave it powered off. Startup actions are applied when a recovery plan is tested or run.

With the default setting of “Power on”, it is possible to configure the amount of time VMware Site Recovery waits for VMware Tools heartbeats before issuing an error message. VMware Tools heartbeats are used to validate a virtual machine started successfully. The default timeout value is five minutes. Changing the timeout value for this setting might be useful for virtual machines that take longer to start up. For example, if a virtual machine takes six minutes to fully boot, an error message would be produced even though the virtual machine is recovered without issue. Changing the timeout value to more than six minutes would eliminate this “false positive” error message.

Another configurable option in this section is the delay before running a post power on step, which will be covered next. A common example of a post power on step is running a script in the guest OS of a virtual machine. A delay might be needed to provide adequate time for a system service to start before running a script.

### **Post Power On Steps**

Running a script inside of a virtual machine is supported as a post power on step.

VMware Site Recovery can also display a visual prompt as a pre or post power on step. This prompt might be used to remind an operator to place a call to an application owner, modify the configuration of a router, or verify the status of a physical machine.

### **Workflows**

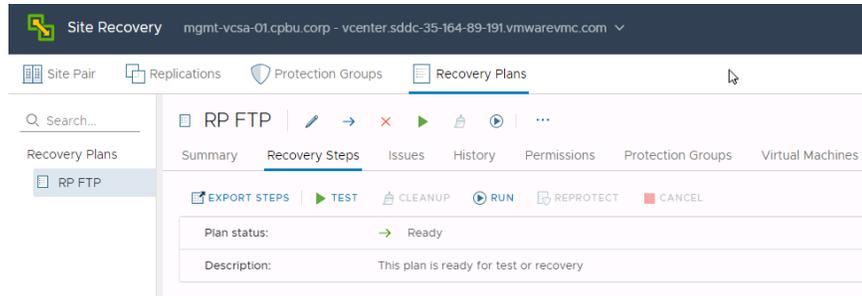
Now that virtual machines are being replicated and assigned to protection groups and recovery plans it is time to see what non-disruptive testing, failover and reprotect look like.

### **Test**

After creating a recovery plan, it is beneficial to test the recovery plan to verify it works as expected. VMware Site Recovery features a non-disruptive testing mechanism to facilitate testing at any time. It is common for an organization to test a recovery plan multiple times after creation to resolve any issues encountered the first time the recovery plan was tested.

Verify the recovery plan is ready for testing or running by checking the “Plan status”. It should show “Ready”. Click the green arrow below “Recovery Plans” or click the “Test” button under the recovery steps option to begin the test process.

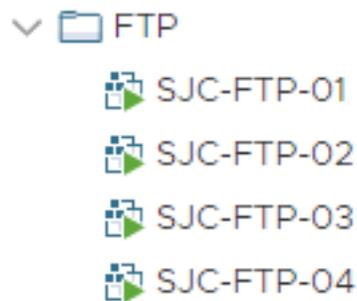




When testing a recovery plan, there is an option to replicate recent changes, which is enabled by default. Replicating recent changes will provide the latest data for the testing process. However, it will also lengthen the amount of time required to recover virtual machines in the recovery plan, as replication has to finish before the virtual machines are recovered.

A question often asked is whether replication continues during the test of a recovery plan. The answer is yes. VMware Site Recovery utilizes virtual machine snapshots with vSphere Replication - as part of the recovery plan test process. This approach allows powering on and modifying virtual machines recovered as part of the test while replication continues to avoid any change to RPO.

Virtual machines that are in a recovery plan that is being tested will display unique icons in the vCenter Server inventory at the recovery site.



At this point, guest operating system administrators and application owners can log into their recovered virtual machines to verify functionality, perform additional testing, and so on. VMware Site Recovery easily supports recovery plan testing periods of varying lengths - from a few minutes to several days. However, longer tests tend to consume more storage capacity at the recovery site. This is due to the nature of snapshot growth as data is written to the snapshot.

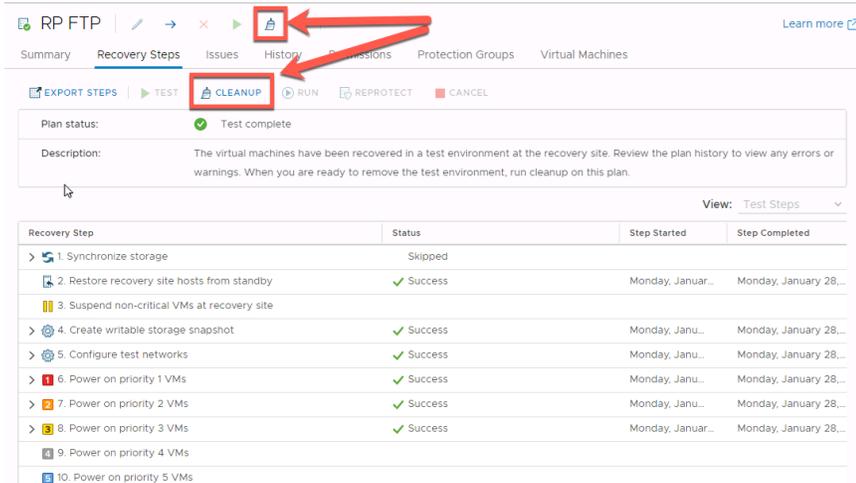
**Recommendation:** Closely monitor storage capacity utilization at the recovery site during recovery plan tests, if capacity is limited. Configure vCenter Server



alarms to alert administrators when free space is getting low on datastores at the recovery site.

## Cleanup

When testing is complete, a recovery plan must be “cleaned up”. This operation powers off virtual machines and removes snapshots associated with the test. Once the cleanup workflow is finished, the recovery plan is ready for testing or running.



The screenshot shows the VMware Site Recovery Manager interface for a recovery plan named 'RP FTP'. The 'Recovery Steps' tab is active, and the 'CLEANUP' button is highlighted with a red box and an arrow. The plan status is 'Test complete'. Below the description, a table lists the recovery steps and their status.

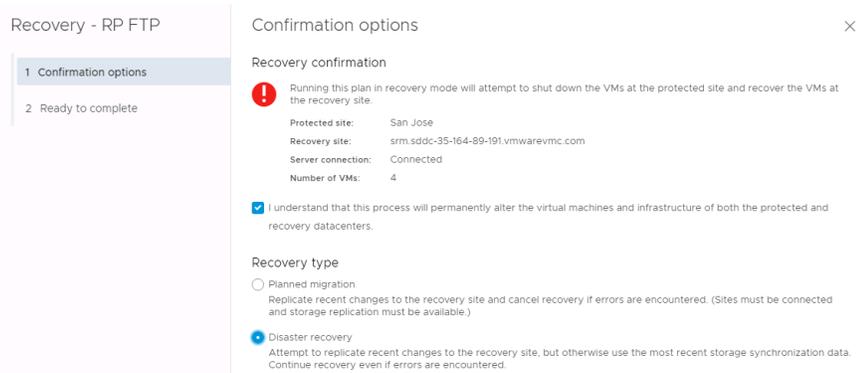
Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	Skipped		
2. Restore recovery site hosts from standby	Success	Monday, Januar...	Monday, January 28...
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	Success	Monday, Janu...	Monday, January 28...
5. Configure test networks	Success	Monday, Janu...	Monday, January 28...
6. Power on priority 1 VMs	Success	Monday, Janu...	Monday, January 28...
7. Power on priority 2 VMs	Success	Monday, Janu...	Monday, January 28...
8. Power on priority 3 VMs	Success	Monday, Januar...	Monday, January 28...
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

## Failover

Running a recovery plan differs from testing a recovery plan. Testing a recovery plan does not disrupt virtual machines at the protected site. When running a recovery plan, VMware Site Recovery will attempt to shut down virtual machines at the protected site before the recovery process begins at the recovery site. Recovery plans are run when a disaster has occurred, and failover is required or when a planned migration is desired.

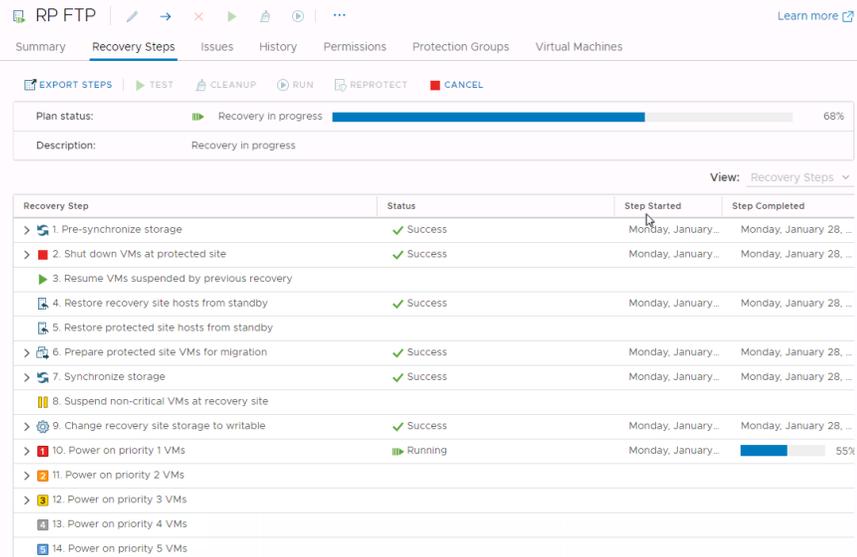
Clicking the Run Recovery Plan button opens a confirmation window requiring the selection of a recovery type - either a planned migration or a disaster recovery. In both cases, VMware Site Recovery will attempt to replicate recent changes from the protected site to the recovery site. It is assumed that for a planned migration, no loss of data is the priority. A planned migration will be cancelled if errors in the workflow are encountered. For disaster recovery, the priority is recovering workloads as quickly as possible after disaster strikes. A disaster recovery workflow will continue even if errors occur.





After a recovery type is selected, the operator must also populate a confirmation checkbox as an additional safety measure. The idea behind this checkbox is to make sure the operator knows that he or she is running (not testing) a recovery plan.

The first step in running a recovery plan is the attempt to synchronize storage. Then, protected virtual machines at the protected site are shut down. This effectively quiesces the virtual machines and commits any final changes to disk as the virtual machines complete the shutdown process. Storage is synchronized again to replicate any changes made during the shutdown of the virtual machines. Replication is performed twice to minimize downtime and data loss. Once these steps have been completed, the recovery process at the recovery site is started.



If the protected site is offline due to a disaster, for example, the disaster recovery type should be selected. VMware Site Recovery will still attempt to



synchronize storage as described in the previous paragraph. Since the protected site is offline, VMware Site Recovery will begin recovering virtual machines at the recovery site using the most recently replicated data.

Since running a recovery plan is a disruptive operation, VMware Site Recovery administrators commonly limit the ability to run recovery plans to just a few people in the organization. This is accomplished through VMware Site Recovery roles and permissions that are added to vCenter Server when VMware Site Recovery is installed. For example, an administrator can assign the “SRM Recovery Test Administrator” role to application owners allowing these individuals to test recovery plans for their applications, but not run recovery plans.

**Recommendation:** Considering the disruptive nature of running (not testing) a recovery plan, limit the permission to run a recovery plan to only a few individuals in the organization similar to the way root or domain administrator permissions are typically limited. All individuals with this permission should be fully trained on the operation of VMware Site Recovery. However, more than one person should have this permission to avoid a single point of failure.

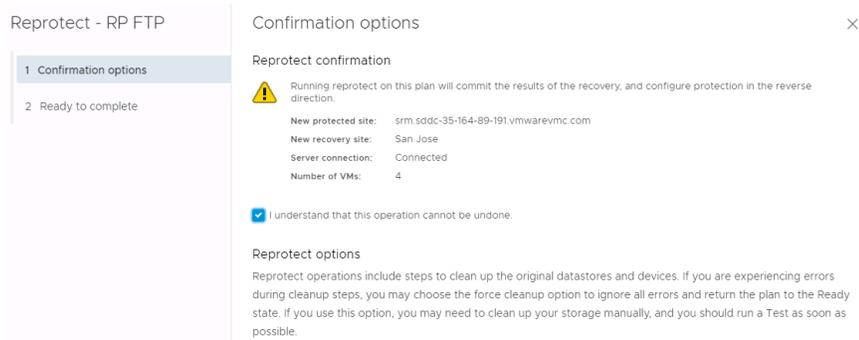
There are several roles and permissions available. For more information on roles and permissions, see [VMware Site Recovery Privileges, Roles, and Permissions](#) in the VMware Site Recovery documentation.

### **Reprotect**

VMware Site Recovery features the ability to not only fail over virtual machine workloads, but also fail them back to their original site. However, this assumes that the original protected site is still intact and operational. An example of this is a disaster avoidance situation: The threat could be rising floodwaters from a major storm and VMware Site Recovery is used to migrate virtual machines from the protected site to the recovery site. Fortunately, the floodwater subsides before any damage was done leaving the protected site unharmed.

A recovery plan cannot be immediately failed back from the recovery site to the original protected site. The recovery plan must first undergo a reprotect workflow. This operation involves reversing replication and setting up the recovery plan to run in the opposite direction.





Reprotecting a recovery plan can take a considerable amount of time depending on the number of protection groups and virtual machines in the recovery plan and the amount of data that must be replicated to resynchronize storage. Upon completion of the reprotect workflow, a history reports will be created, and the recovery plan can be failed back. Essentially, the original recovery site becomes the protected site and the original protected site becomes the recovery site for the virtual machines in the recovery plan. Run the recovery plan to fail back the virtual machines to their original protected site.

**NOTE:** Be sure to reprotect a recovery plan after it has been run (virtual machines have been failed over or failed back). Failure to do this important step will prevent future testing and running of the recovery plan until the reprotect workflow has been run.

**Recommendation:** Test a recovery plan as soon as possible after a reprotect workflow has run to verify the recovery plan will work properly.

## Reporting

### Recovery Plans History

EXPORT ALL

	Plan Name	Operation	Result	Date
<input type="radio"/>	RP FTP	Recovery	✓ Success	Monday, January 28, 2019 3:43:55 AM
<input type="radio"/>	RP FTP	Cleanup	✓ Success	Monday, January 28, 2019 3:40:06 AM
<input type="radio"/>	RP FTP	Test	✓ Success	Monday, January 28, 2019 3:26:38 AM

When workflows such as a recovery plan test and cleanup are performed in VMware Site Recovery, history reports are automatically generated. These reports document items such as the workflow name, execution times, successful operations, failures, and error messages. History reports are useful for a number of reasons including internal auditing, proof of disaster recovery protection for regulatory requirements, and troubleshooting. Reports



can be exported to HTML, XML, CSV, or a Microsoft Excel or Word document.

Recovery Plan History Report  
VMware Site Recovery Manager 8.1.1

Plan Summary	
Name:	RP FTP
Description:	
Protected Site:	San Jose
Recovery Site:	sm.s[redacted] vmwarevmc.com

Run Summary	
Operation:	Recovery
Recovery Type:	Disaster recovery
Started By:	VMC.LOCAL\cloudadmin
Start Time:	2019-01-28 11:43:55 (UTC 0)
End Time:	2019-01-28 11:50:42 (UTC 0)
Elapsed Time:	00:06:48
Result:	Success
Errors:	0
Warnings:	0

Recovery Step	Result	Step Started	Step Completed	Execution Time
1. Pre-synchronize storage	Success	2019-01-28 11:44:02 (UTC 0)	2019-01-28 11:44:02 (UTC 0)	00:00:00
1.1. Protection Group PG FTP	Success	2019-01-28 11:44:02 (UTC 0)	2019-01-28 11:44:02 (UTC 0)	00:00:00
2. Shut down VMs at protected site	Success	2019-01-28 11:44:02 (UTC 0)	2019-01-28 11:45:01 (UTC 0)	00:00:59
2.1. Shut down the priority 5 VMs	Inactive			
2.2. Shut down the priority 4 VMs	Inactive			
2.3. Shut down the priority 3 VMs	Success	2019-01-28 11:44:02 (UTC 0)	2019-01-28 11:44:31 (UTC 0)	00:00:29
2.3.1. SJC-FTP-04	Success	2019-01-28 11:44:02 (UTC 0)	2019-01-28 11:44:14 (UTC 0)	00:00:12
2.3.1.1. Power off	Success	2019-01-28 11:44:02 (UTC 0)	2019-01-28 11:44:14 (UTC 0)	00:00:12
2.3.2. SJC-FTP-03	Success	2019-01-28 11:44:14 (UTC 0)	2019-01-28 11:44:31 (UTC 0)	00:00:17
2.3.2.1. Power off	Success	2019-01-28 11:44:14 (UTC 0)	2019-01-28 11:44:31 (UTC 0)	00:00:17
2.4. Shut down the priority 2 VMs	Success	2019-01-28 11:44:31 (UTC 0)	2019-01-28 11:44:44 (UTC 0)	00:00:13
2.4.1. SJC-FTP-02	Success	2019-01-28 11:44:31 (UTC 0)	2019-01-28 11:44:44 (UTC 0)	00:00:13

