VMware Site Recovery for VMware Cloud on AWS Evaluation Guide

TECHNICAL WHITE PAPER

Table of Contents

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

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.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

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

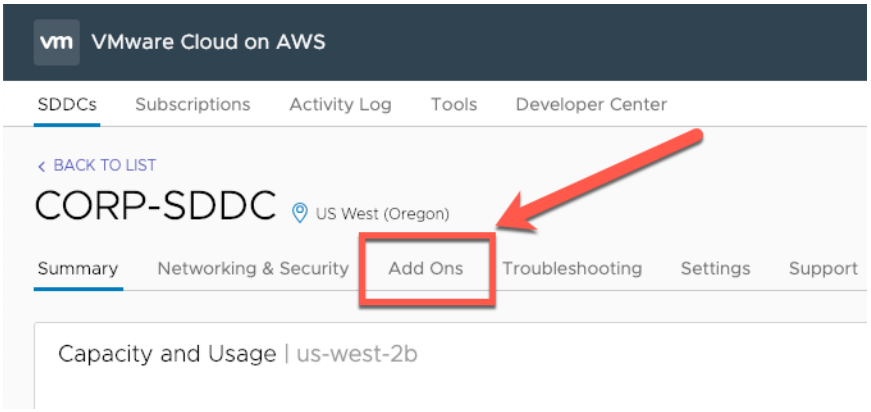
Recommendation: Use default settings for all components - installation paths, TCP port settings, and so on - wherever possible, to minimize complexity in the evaluation environment. Use consistent naming conventions, usernames, and passwords during evaluation environment deployment.

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

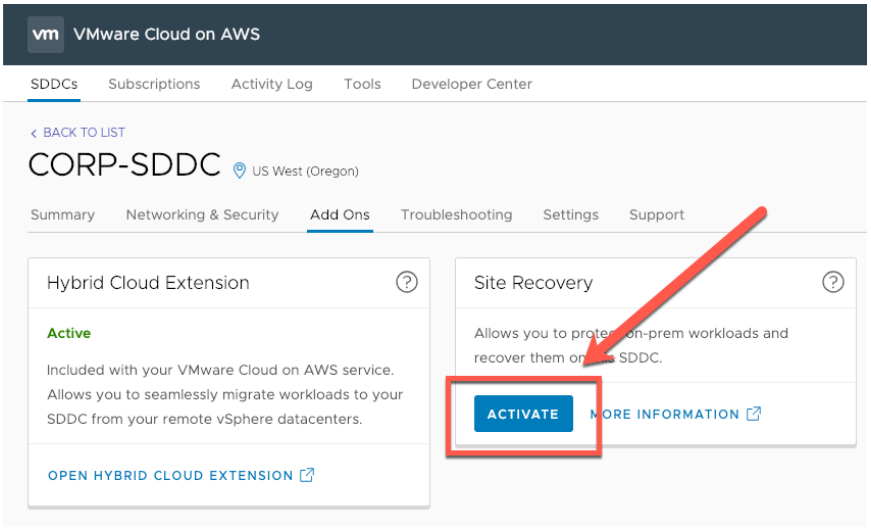
port groups at the protected site and the recovery site, as this will simplify inventory mappings.

Activating Site Recovery

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

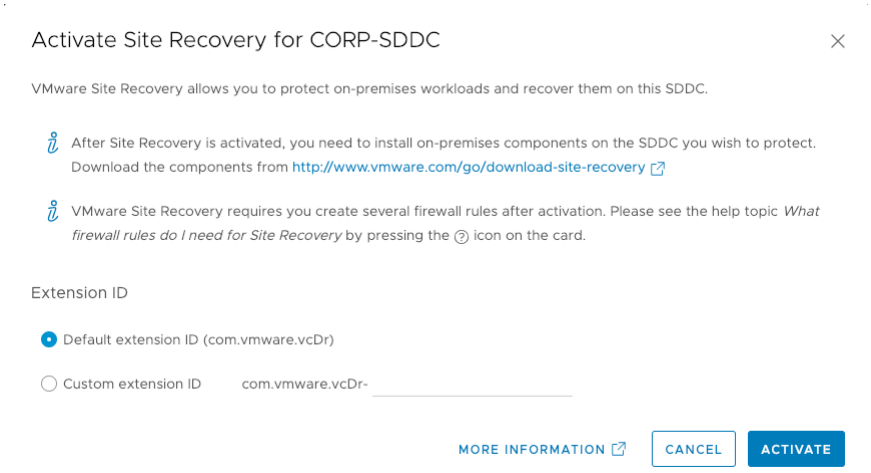


Click “Activate”



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”

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

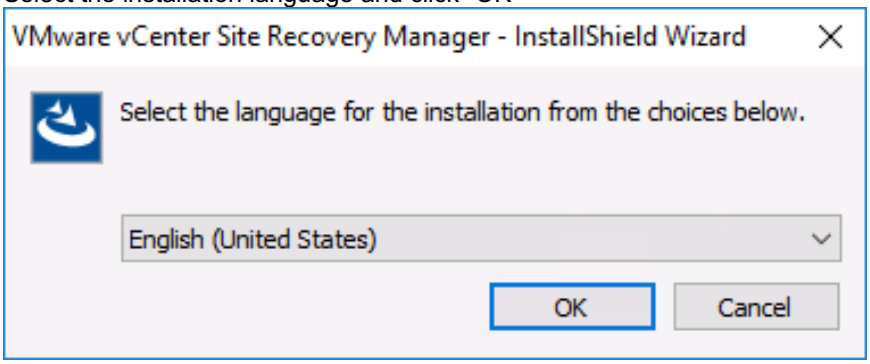


No other user action is required for activation. While the VMware Site Recovery add-on is being activated start downloading and installing the on-premises components.

Installing Site Recovery Manager

Run the SRM installer executable

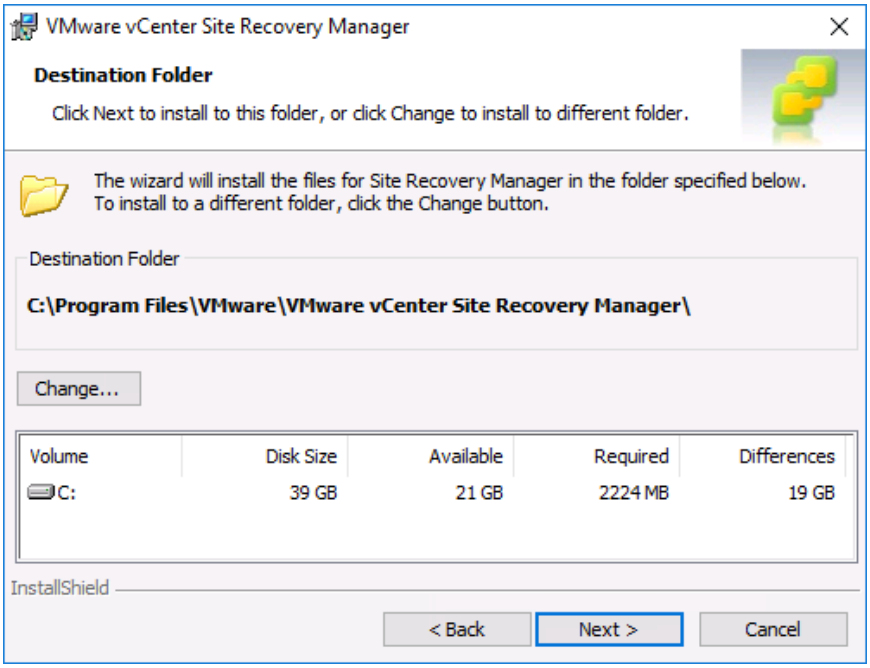
Select the installation language and click “OK”



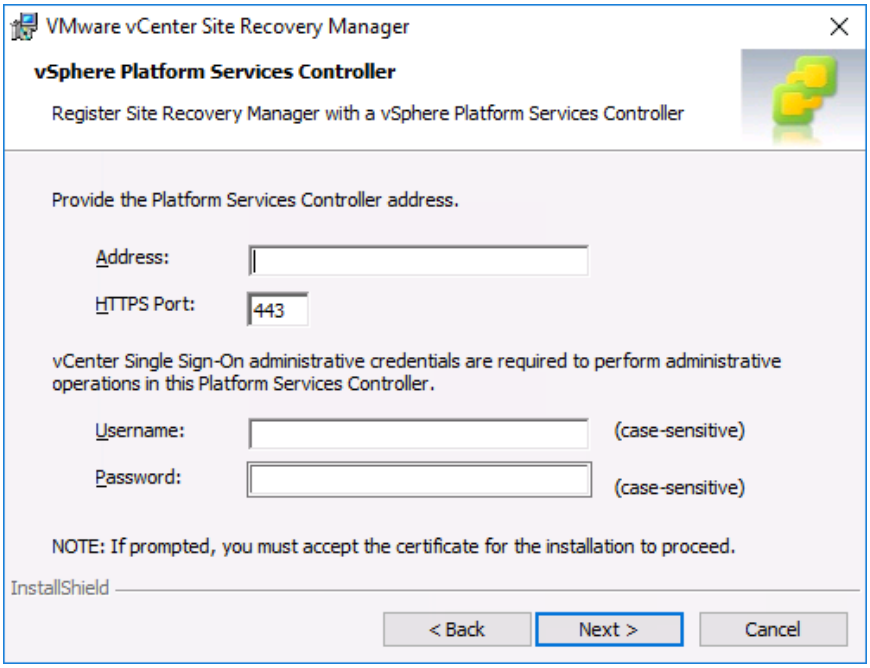
Click “Next”

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”



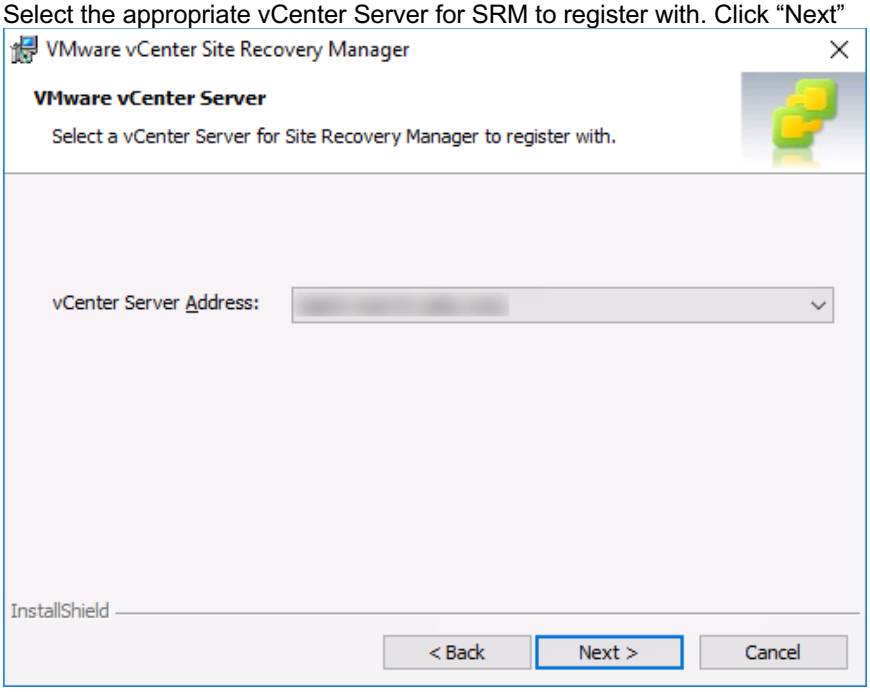
Provide the address (IP address or preferably FQDN) of the on-premises PSC and the SSO credentials to perform administrative operations on the same PSC. Click “Next”



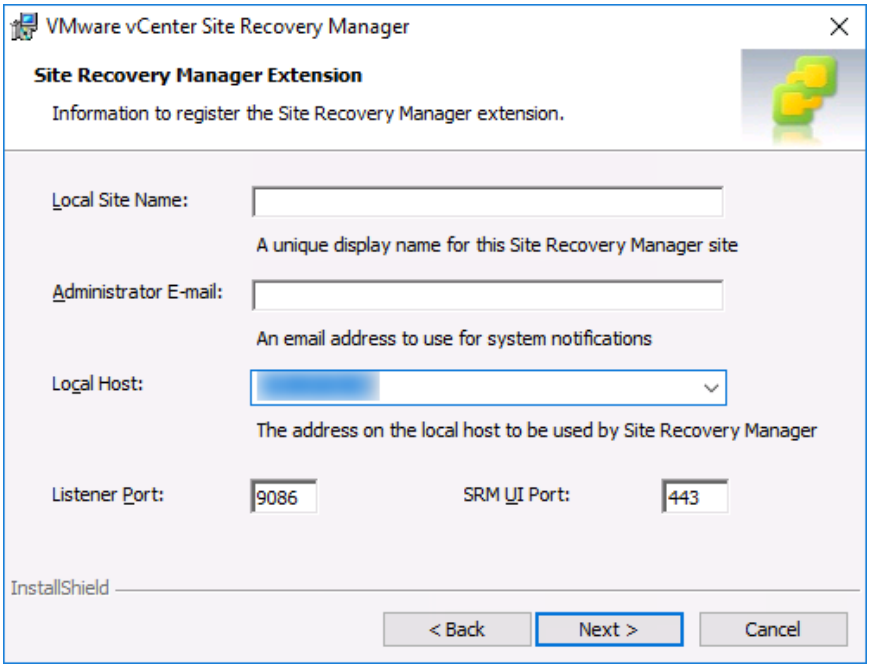
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Verify and accept the windows certificate if applicable

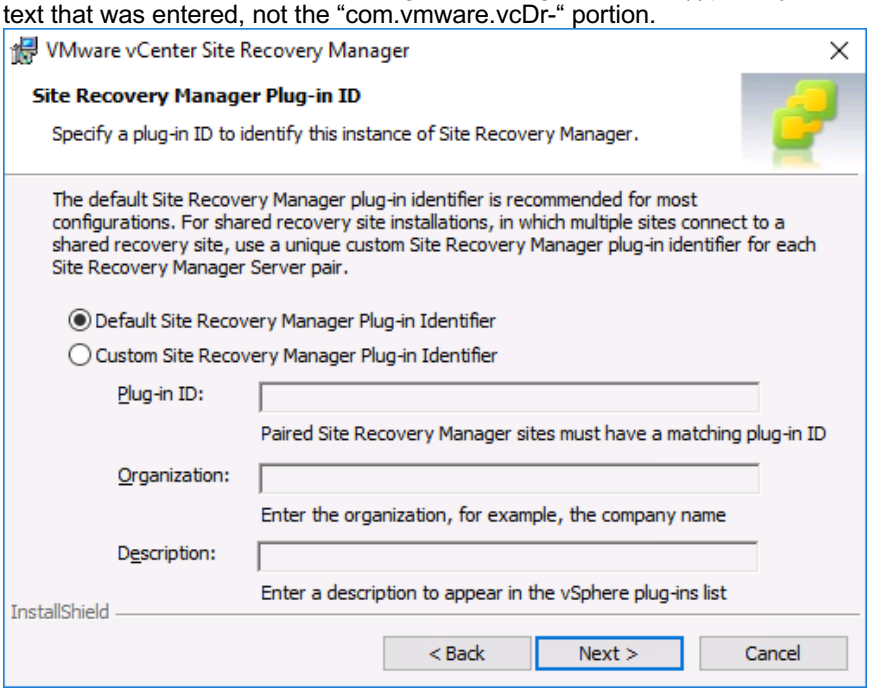
Select the appropriate vCenter Server for SRM to register with. Click “Next”



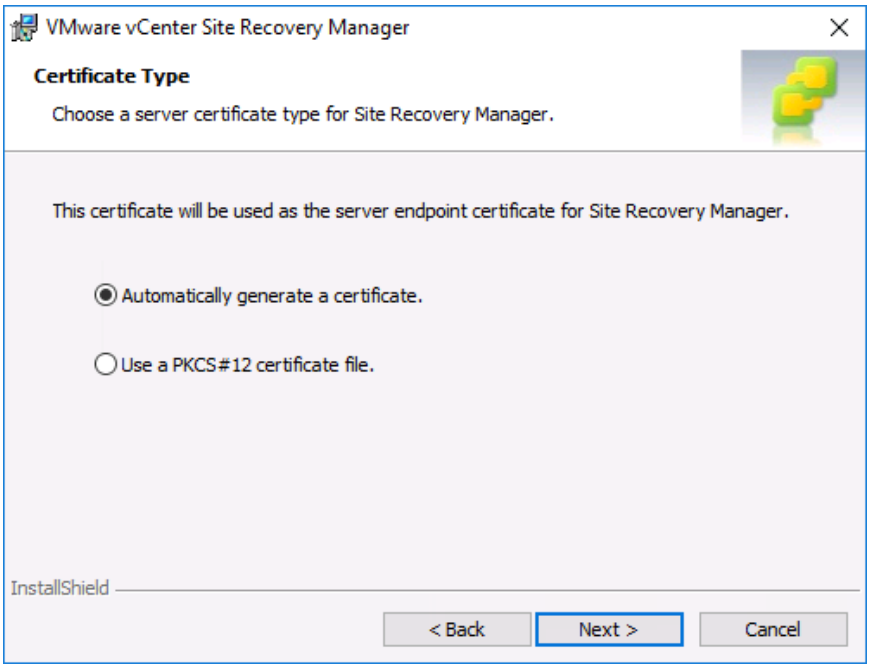
Enter a name for the Local Site, eg. “San Jose”, “Site A”, etc. Enter an email address for system notifications and select the address on the local host to be used for SRM (the default is usually good). We do not recommend changing the listener or SRM UI ports for an evaluation. Click “Next”



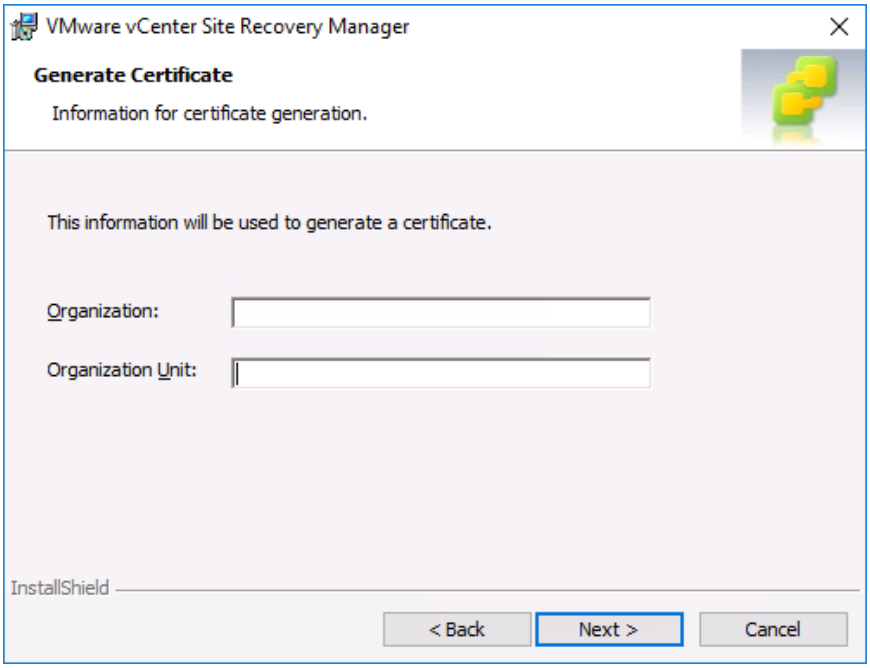
Select the same option and if using the Custom SRM Plug-in Identifier enter the exact same, case sensitive string in the “Plug-in ID” field (type only the text that was entered, not the “com.vmware.vcDr-“ portion.



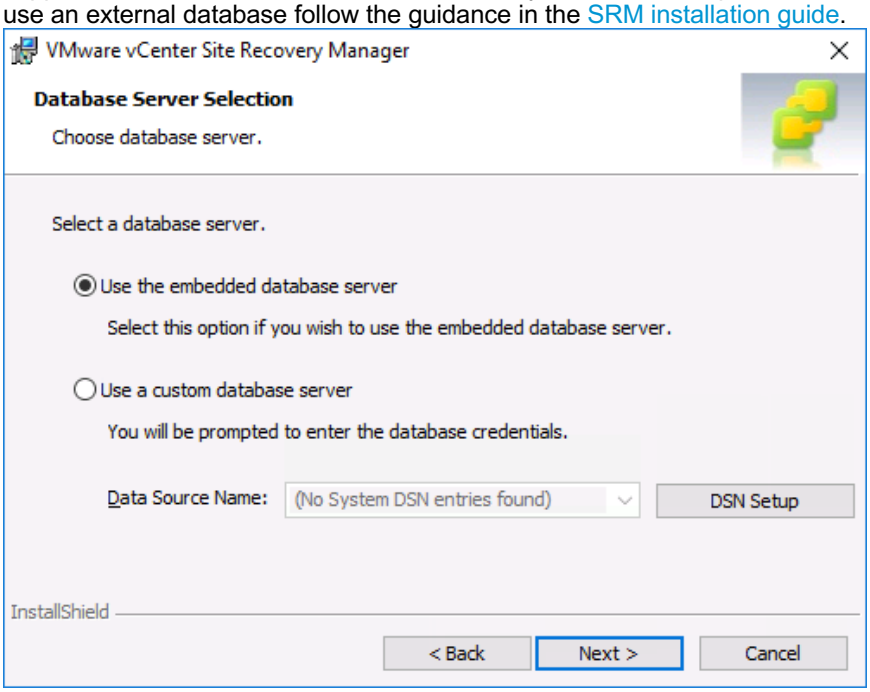
Select the certificate option as appropriate. For the purpose of this evaluation guide we will select “Automatically generate a certificate”. If you have the requirement to use a signed certificate follow the installation directions here. Click “Next”



Enter the Organization and Organization Unit for the certificate. Click “Next”



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.

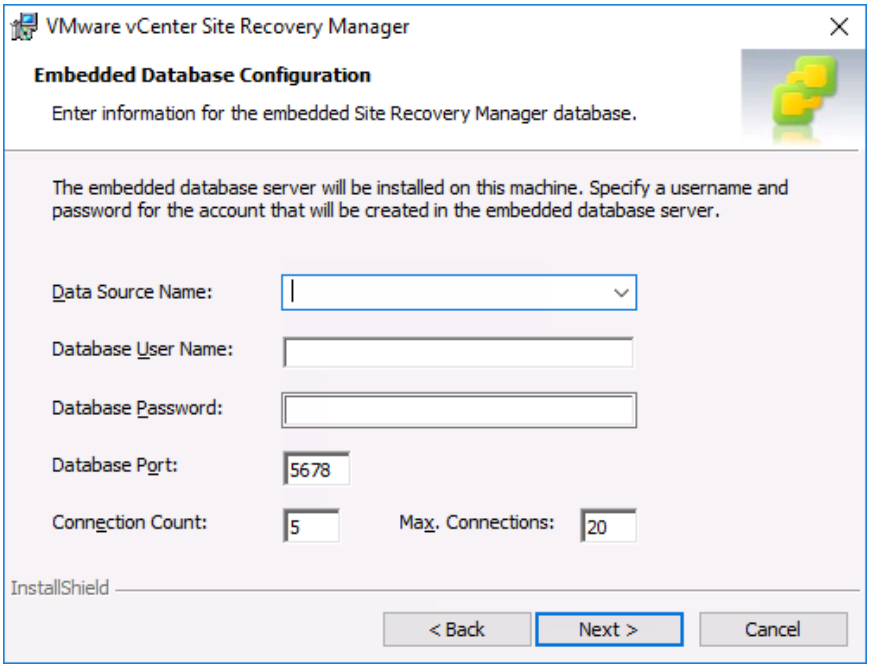


VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

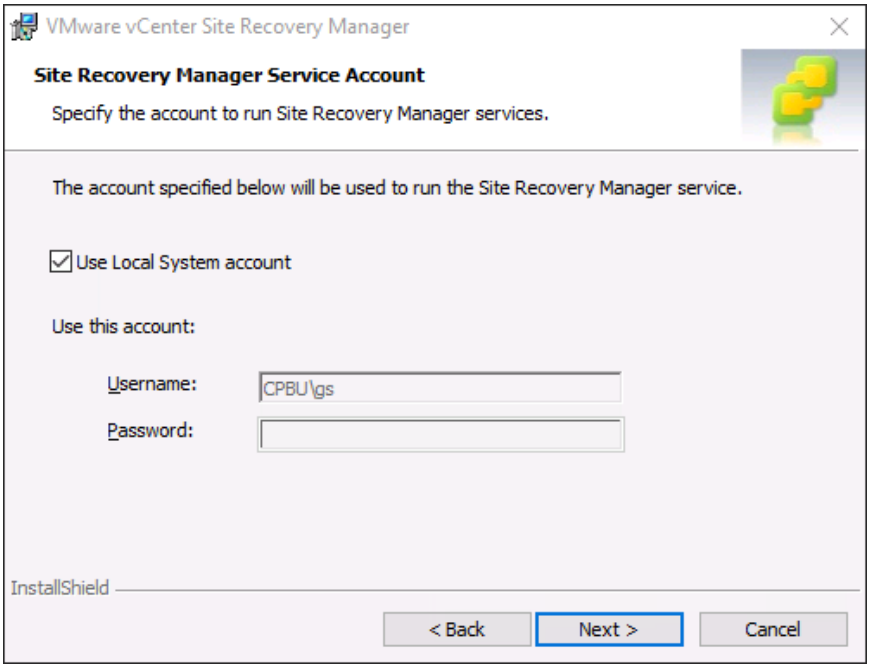
Enter the following:

- 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 “postres”)
- 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

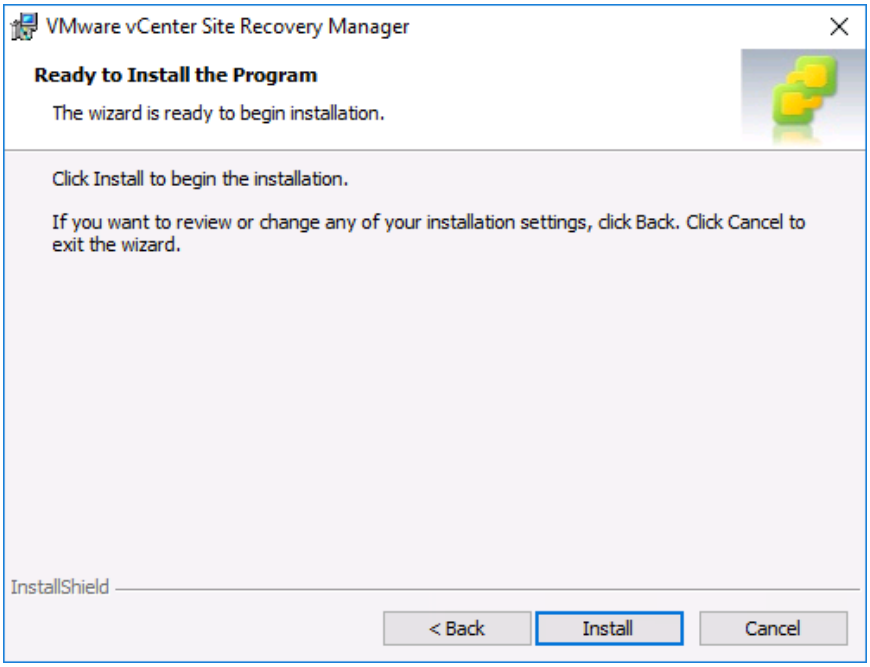
Make sure to note down the DSN, DB User Name and DB Password. Click “Next”



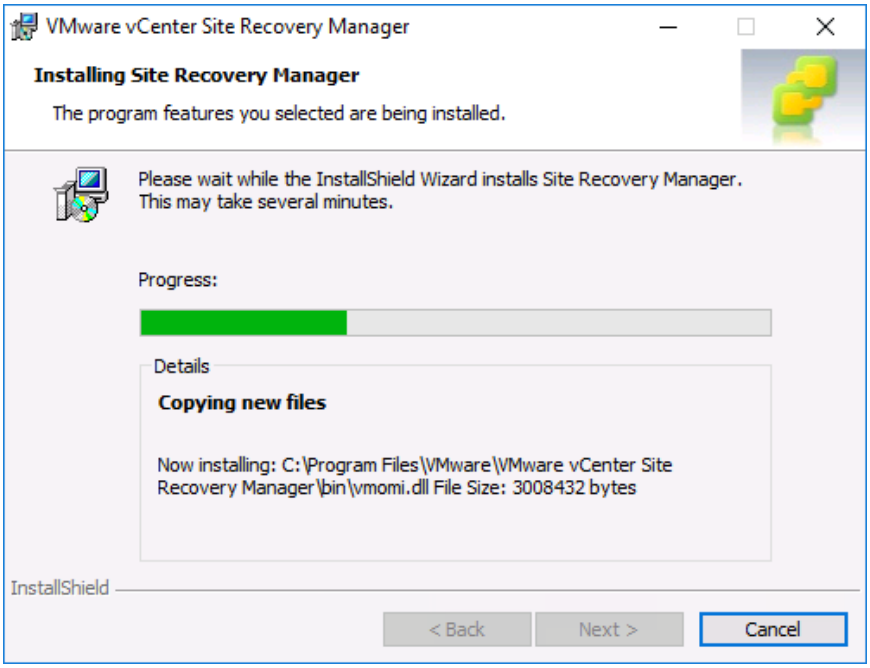
Select the account used for running the SRM service. Unless otherwise required select the default (Local System Account). Click “Next”



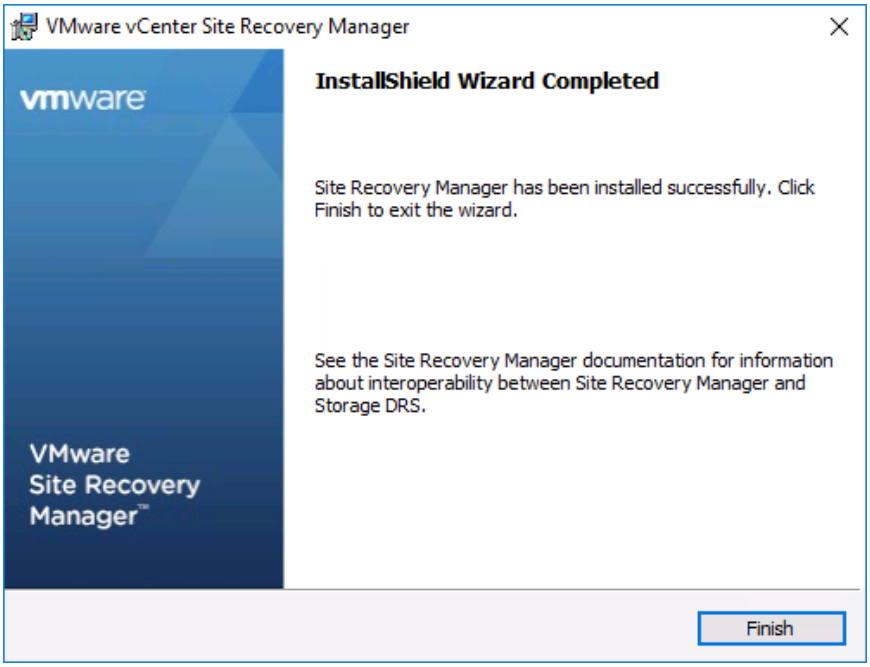
Click “Install”



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



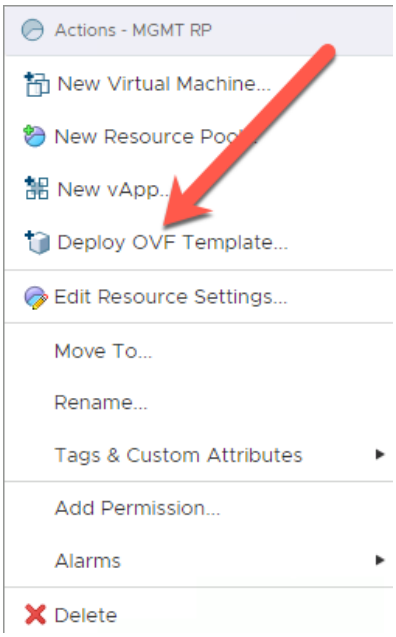
When the installation has finished click “Finish”



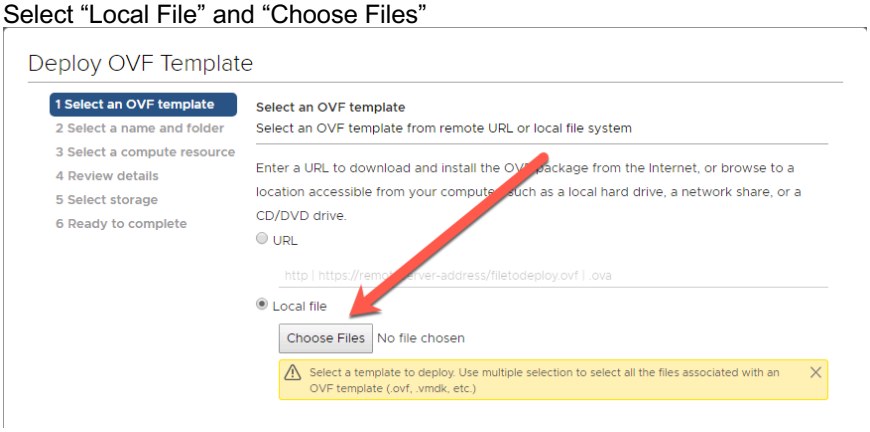
Installing vSphere Replication

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

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



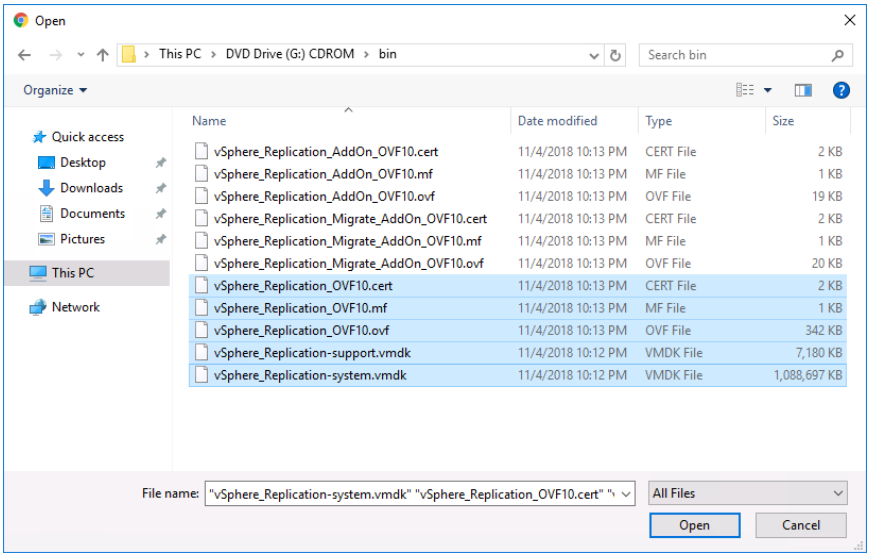
Select “Local File” and “Choose Files”



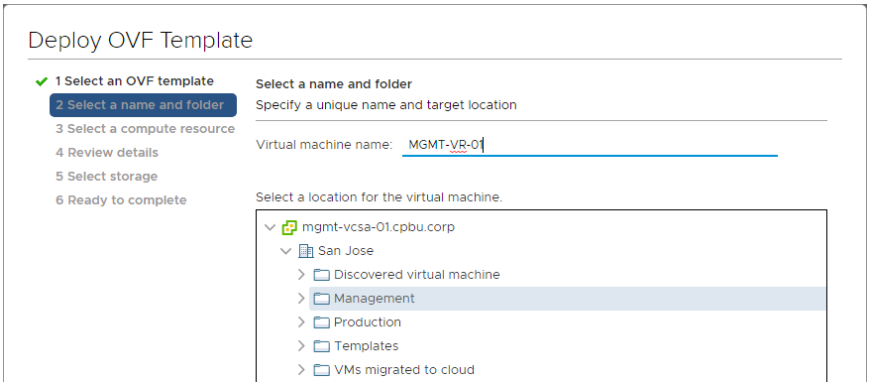
Browse to the CDROM image and the bin folder. Select the following files

- 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”

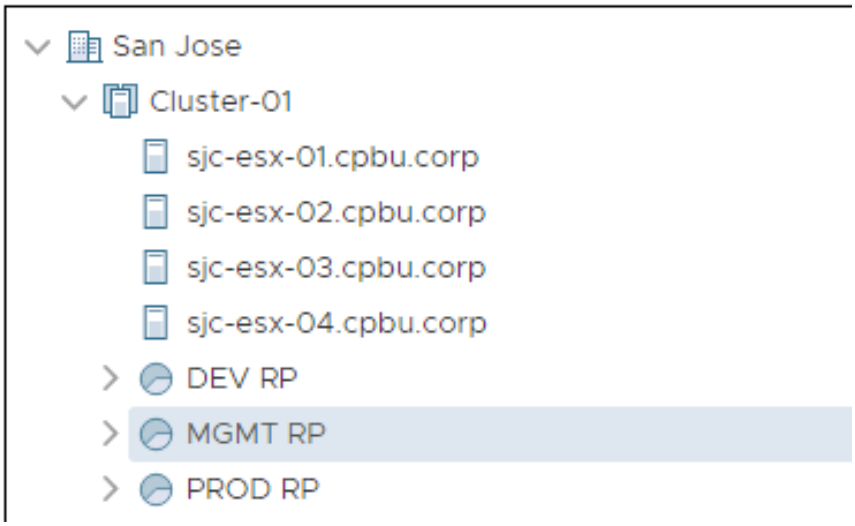


Specify a unique name and target folder for the vSphere Replication Appliance

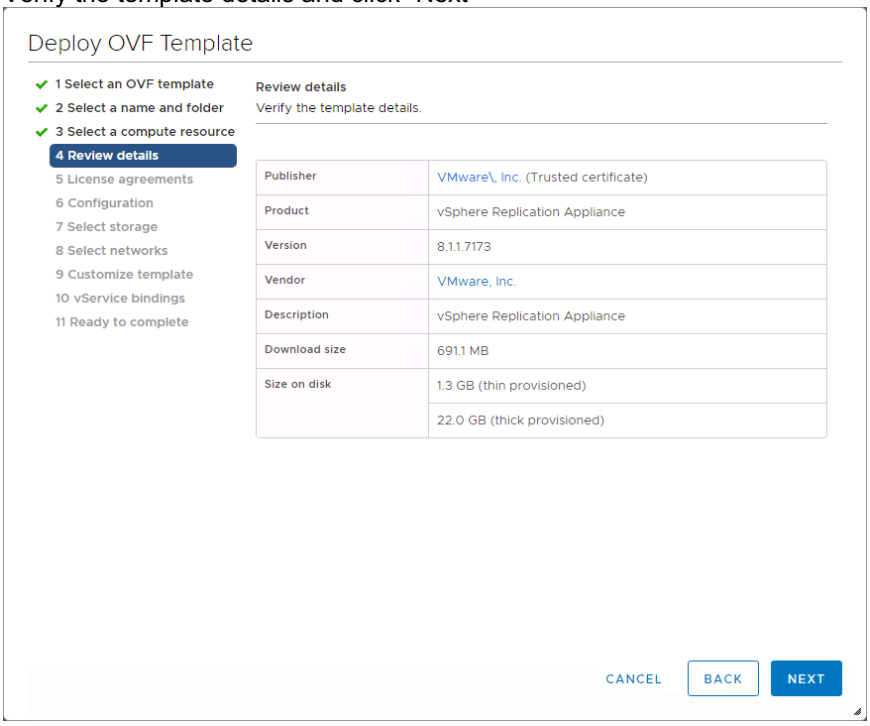


Select a compute resource

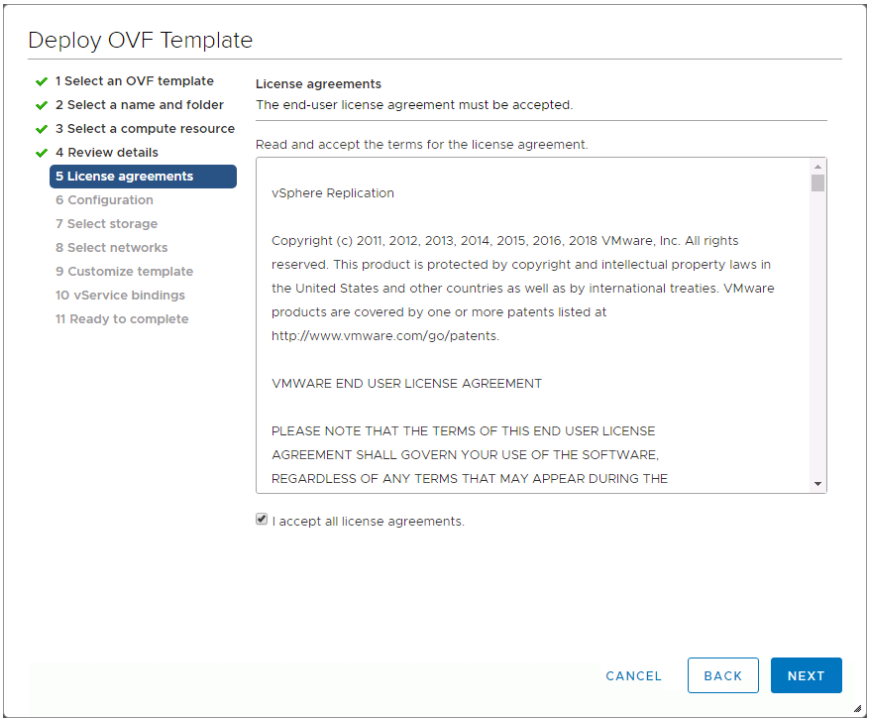
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com



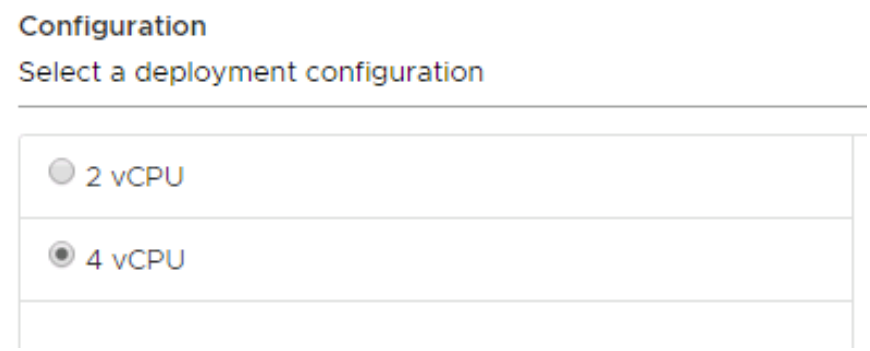
Verify the template details and click “Next”



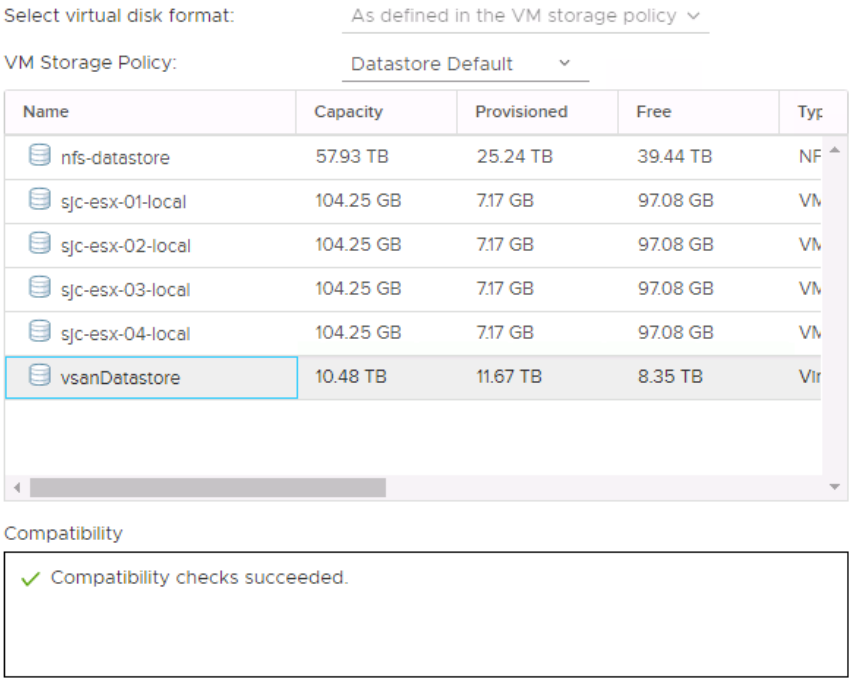
Select the “I accept all license agreements” checkbox. Click “Next”



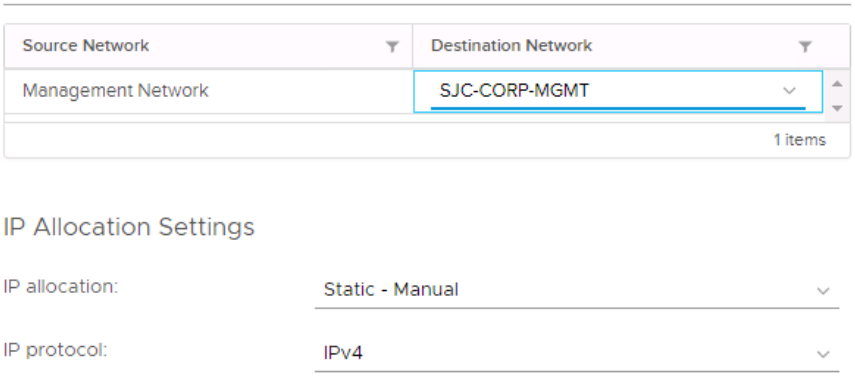
Leave the configuration on 4 vCPU. Click “Next”



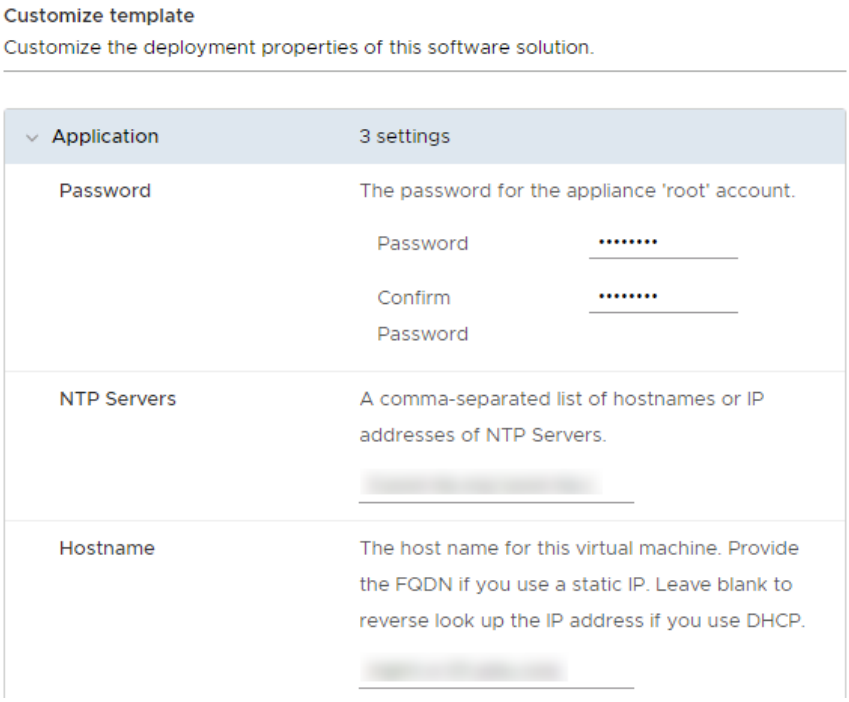
Select a storage location for the vSphere Replication Appliance

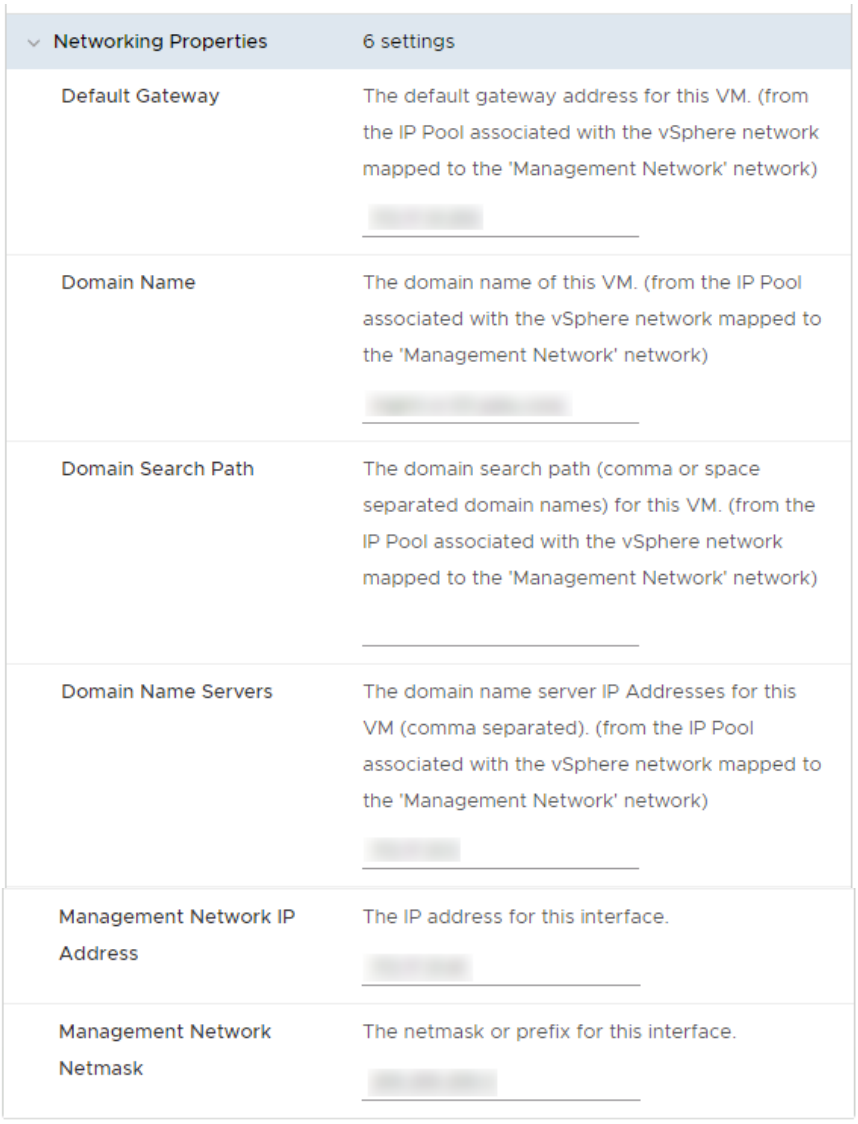


Select a network for the management interface and an IP allocation. Use a "Static – Manual" configuration for simplicity.



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





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”

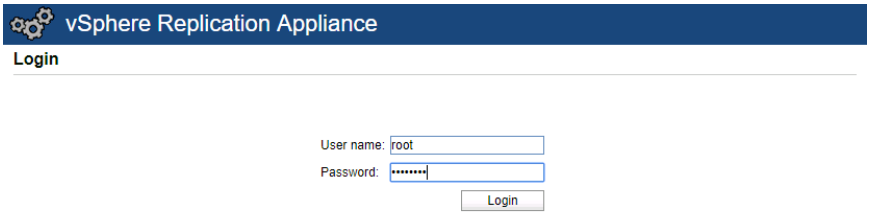
Ready to complete

Click Finish to start creation.

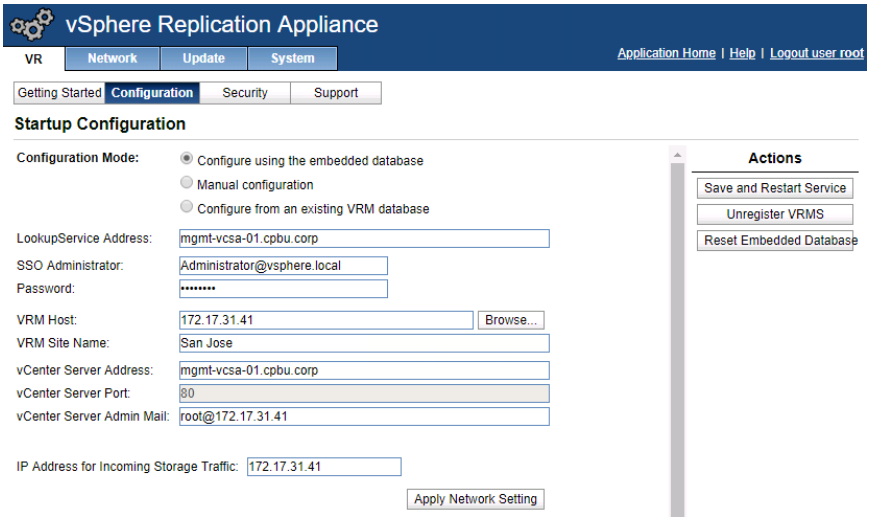
Provisioning type	Deploy from template
Name	MGMT-VR-01
Template name	vSphere_Replication_OVF10
Download size	691.1 MB
Size on disk	22.0 GB
Folder	Management
Resource	MGMT RP
Storage mapping	1
All disks	Datastore: vsanDatastore; Format: As defined in the VM storage policy
Network mapping	1
Management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

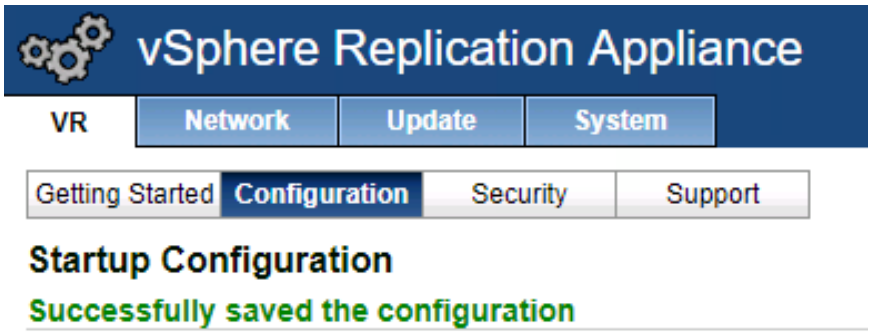
At the login screen enter the username “root” and the password entered when deploying the OVF



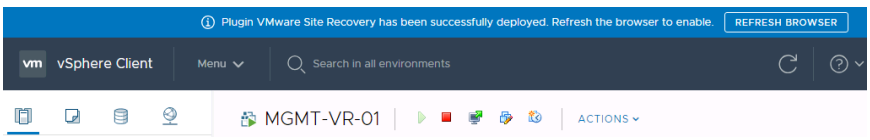
From the Getting Started screen select “Configuration”. Verify that the address of the PSC is entered in the “LookupService Address” field and then type the SSO administrator password. If desired, change the VRM Site Name.

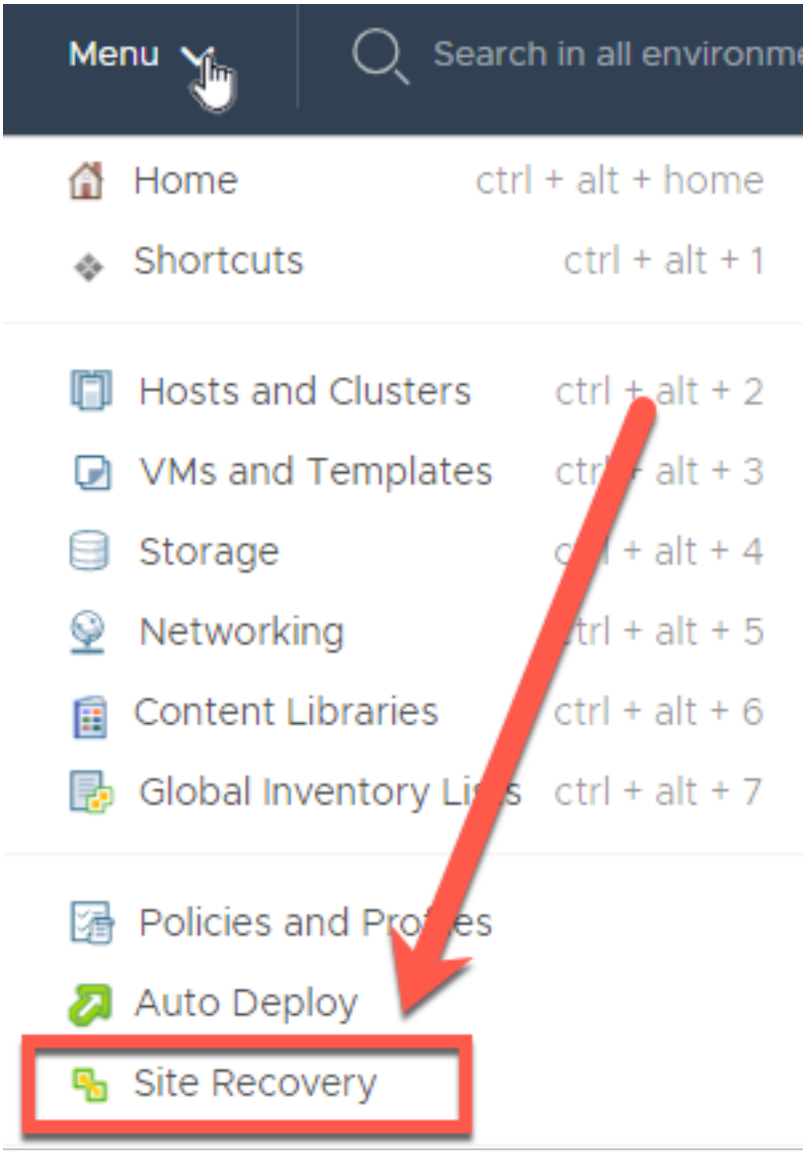


When settings are as desired, click “Save and Restart Service” to complete configuration and start services.



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





Firewall configuration

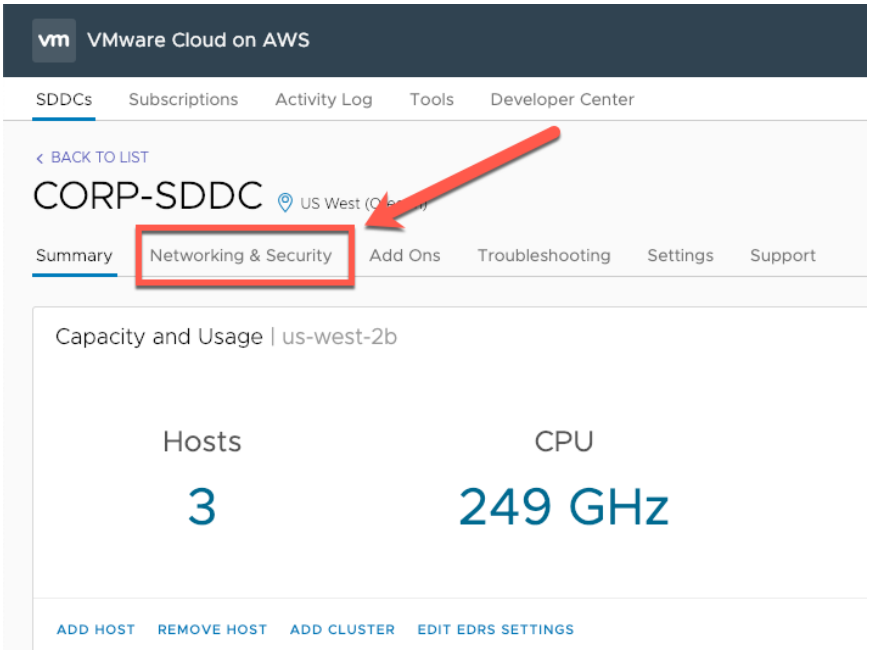
To allow communication and replication traffic between the remote site site and the VMware Cloud on AWS SDDC requires the addition of some firewall rules to the management gateway. Rules may also need to be added for the remote site firewall. Those changes are outside of the scope of this guide.

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.

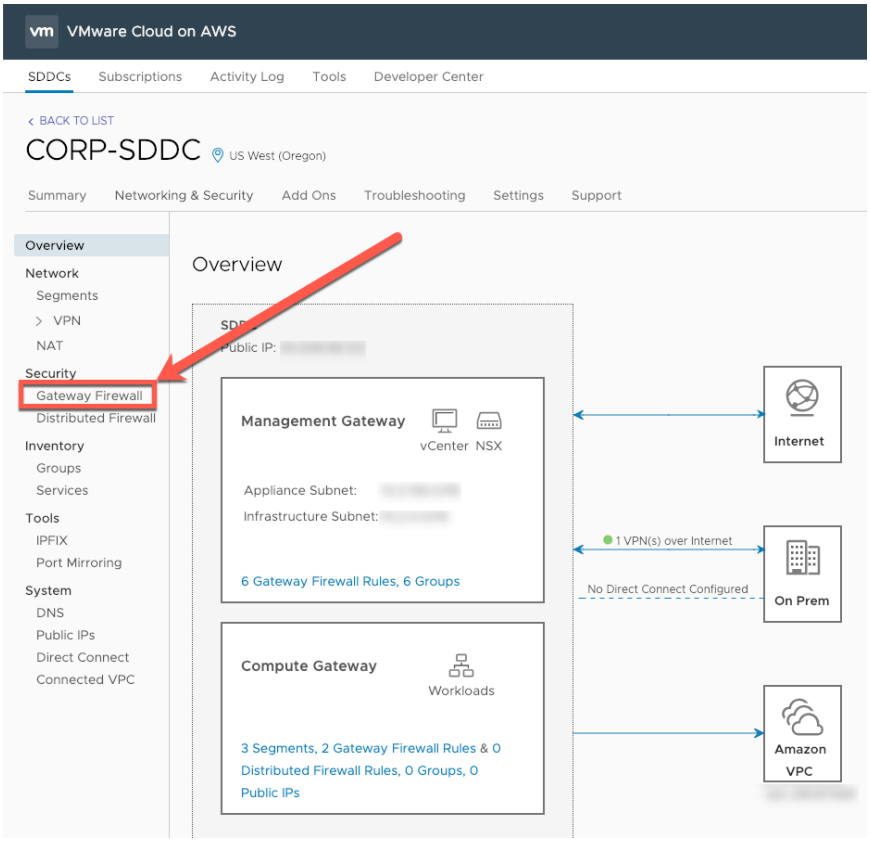
Simple Firewall Configuration

From the SDDC management page select “Networking & Security”

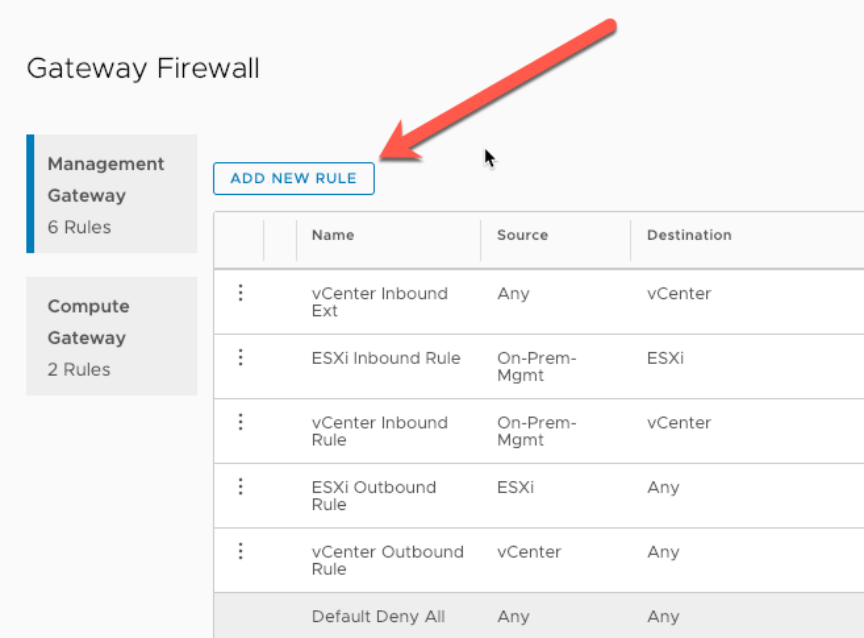


Select the Gateway Firewall

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com



Click “Add New Rule”

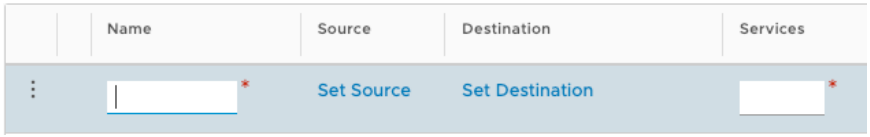


Create the following rules (note that for a configuration between SDDCs these would need to be configured at both):

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

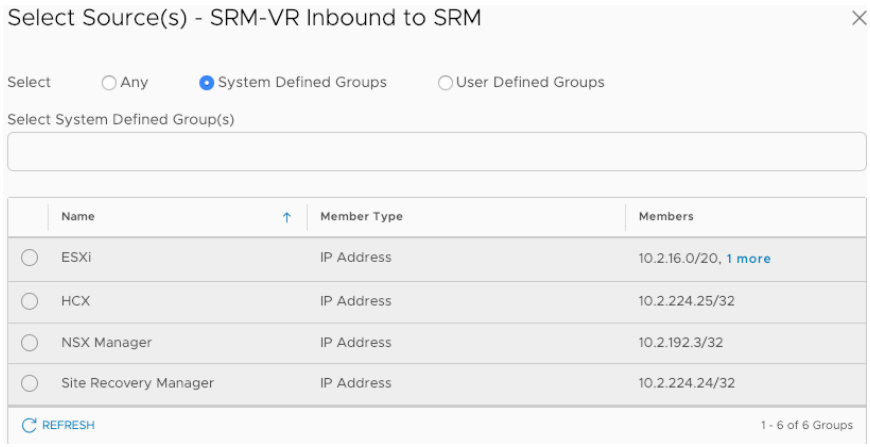
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Enter the rule “Name”

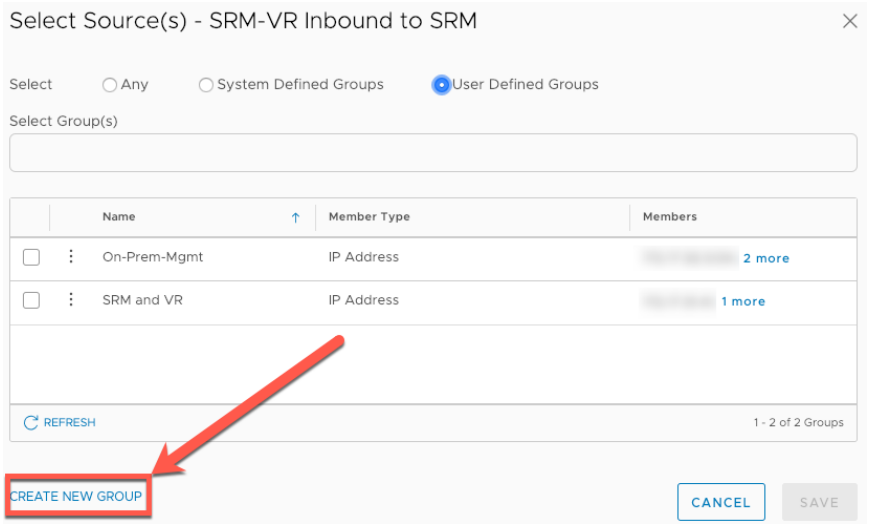


Click “Set Source”

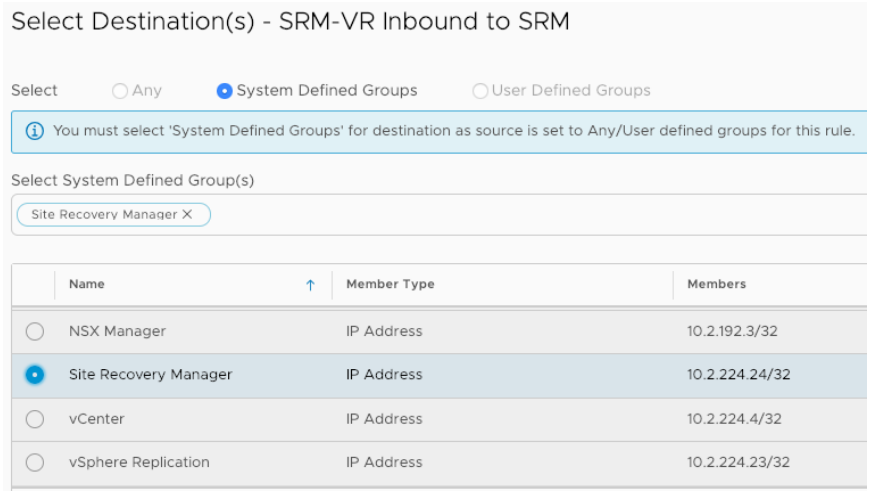
Depending on the rule, select either system defined groups or user defined groups and select the appropriate item from the list.



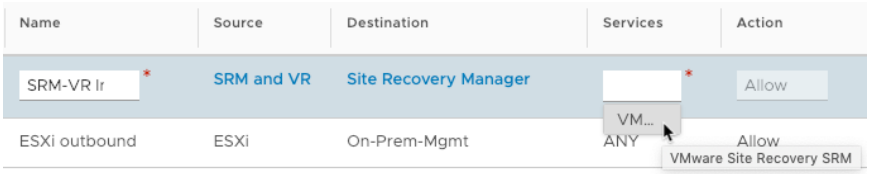
For User Defined rules if the required group doesn’t exist it can be created by clicking on “Create New Group”



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



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

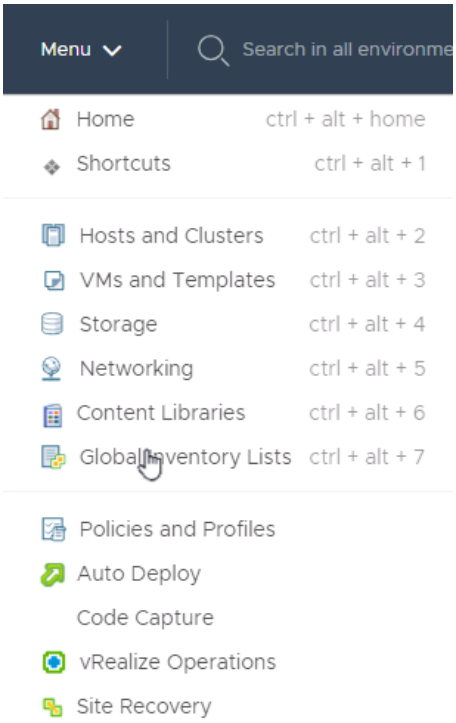


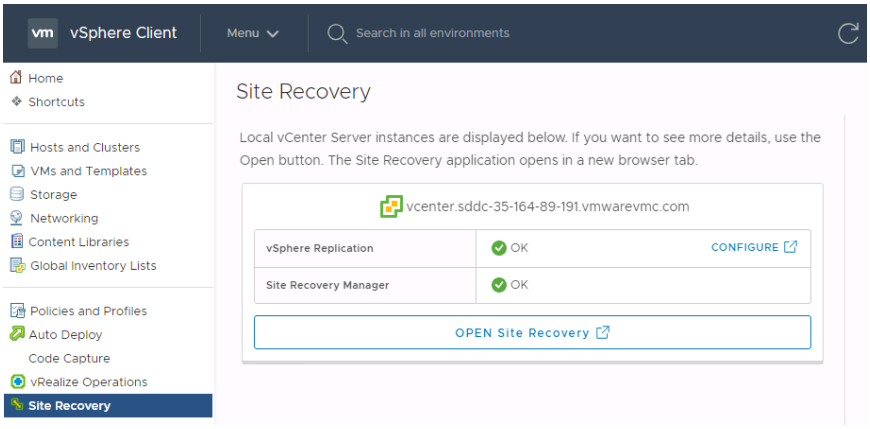
After confirming that the rule has been entered correctly click “Publish” and then enter the next rule. Repeat until all rules have been entered.

Pairing Sites and Mapping Resources

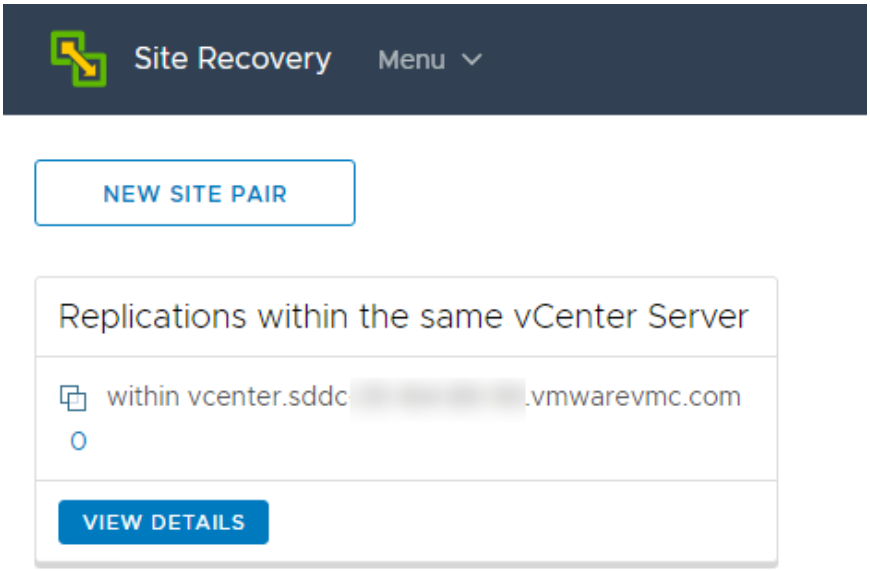
Pair Sites

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.

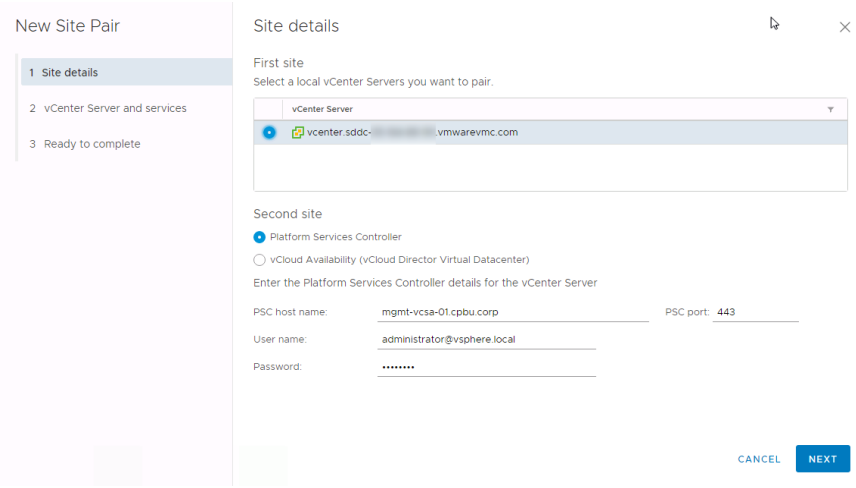




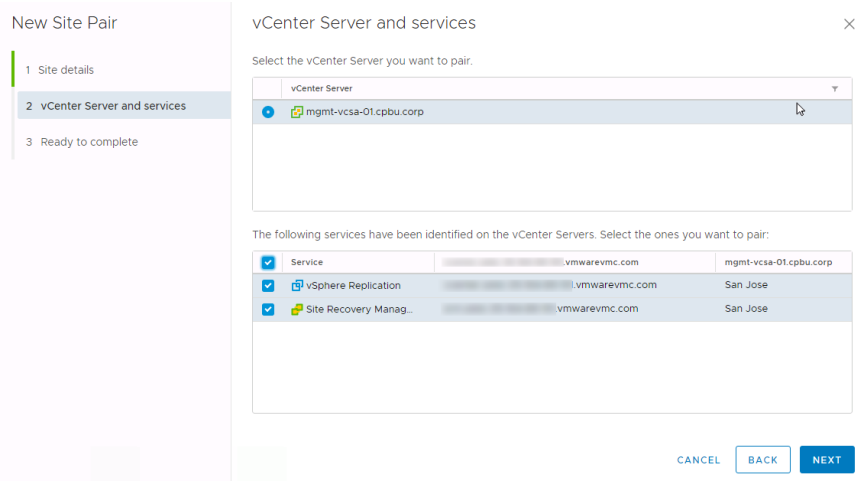
From the Site Recovery screen select “New Site Pair”



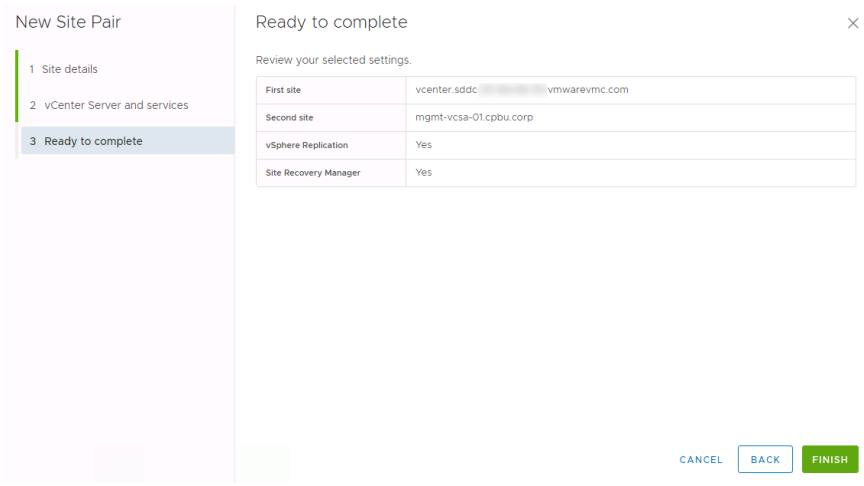
Select the vCenter for the first site, the vCenter where this workflow was started and then enter the PSC host name, user name and password for the second site. Click “Next”



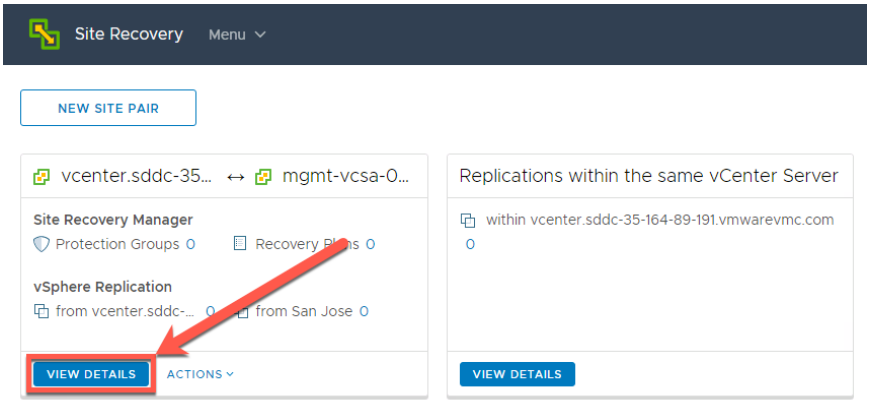
Select the vCenter you want to pair and then select both the vSphere Replication and Site Recovery Manager services. Click “Next”



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

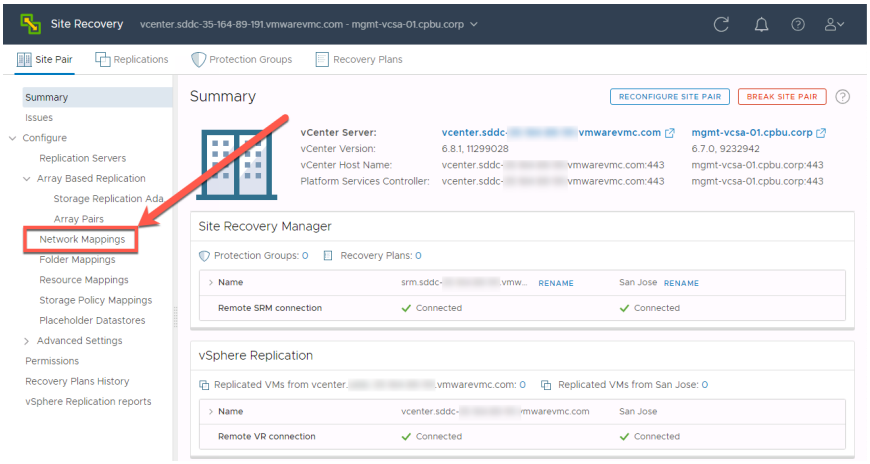
Inventory mappings consist of four types: Resource mappings, folder mappings, storage policy mappings and network mappings. These mappings provide default settings for recovered virtual machines. For example, a mapping can be configured between a network port group named “Production” at the remote site 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.

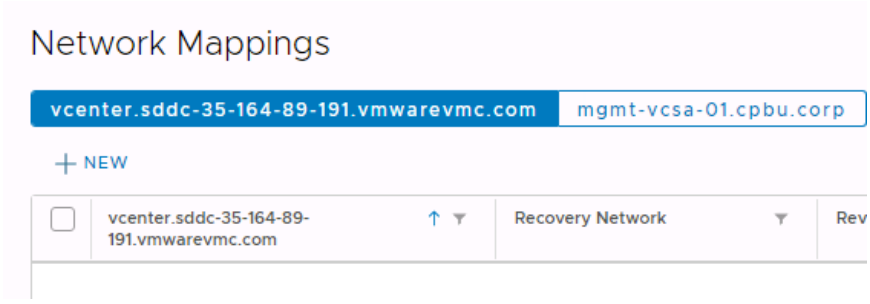
Recommendation: Provide the same name to folders and network port groups with similar functionality at the protected and recovery sites so that mappings can be prepared automatically. Use 1-1 mappings so that reverse mappings can be utilized. These practices will ease inventory-mapping configuration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

Network Mapping

Select “Network Mappings” from the Site Recovery menu

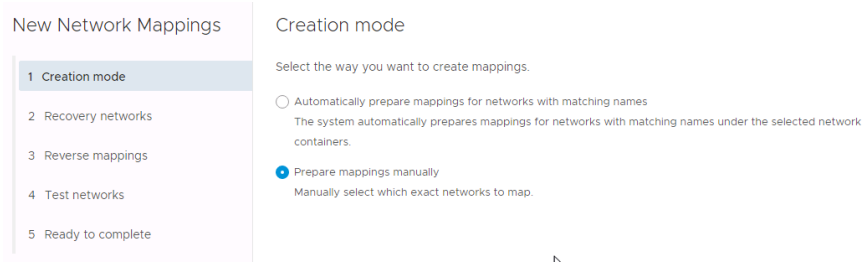


Select “+New”

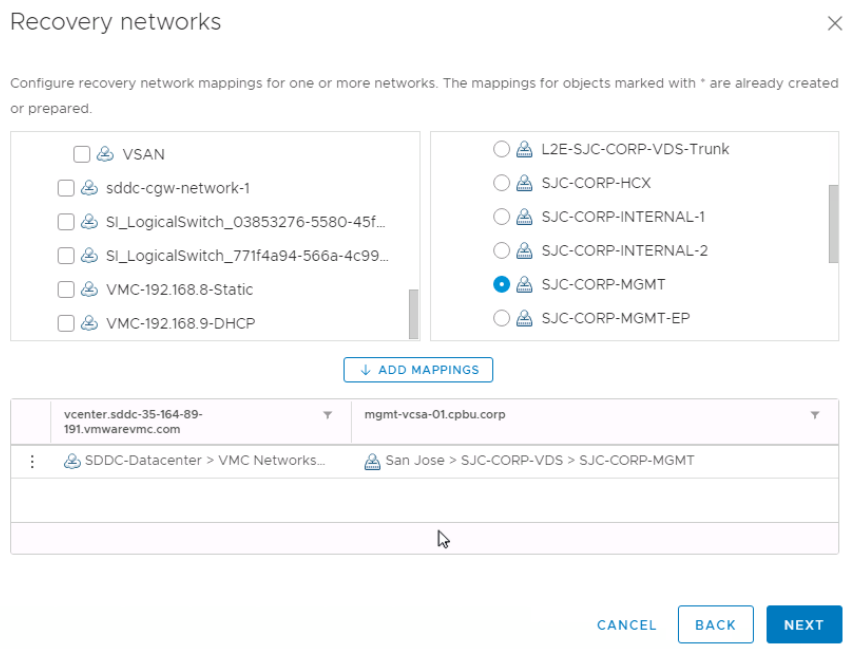


If networks are named the same at the remote site and VMware Cloud on AWS sites choose “Automatically prepare mappings” otherwise choose “Prepare mappings manually”. In this walkthrough the manual option will be selected. Click “Next”

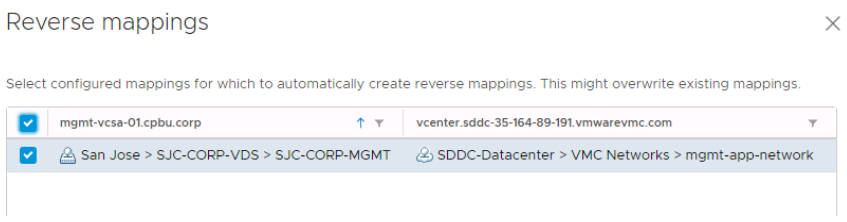
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com



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”

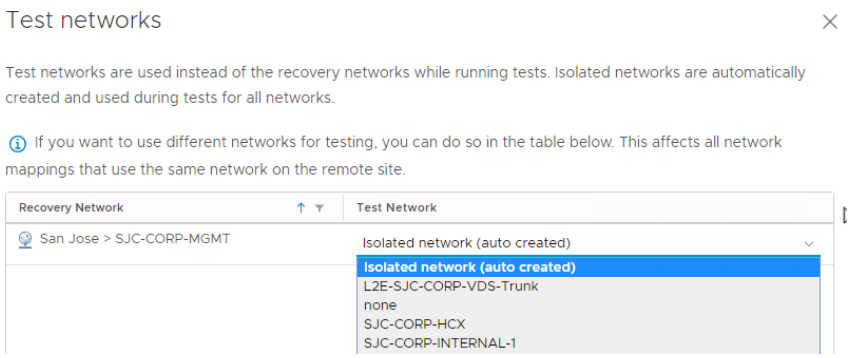


Test Networks

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

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



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.

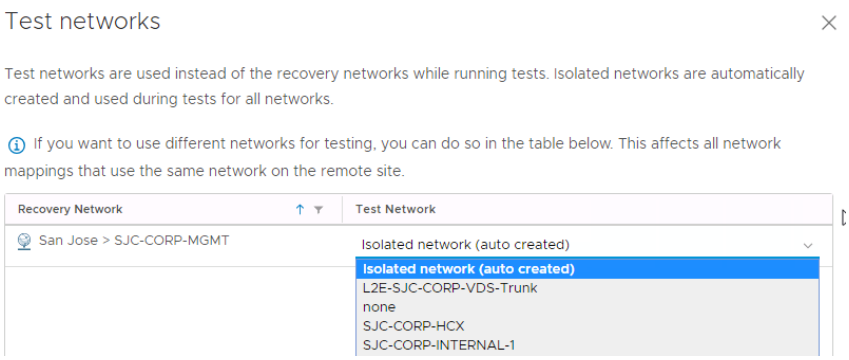
Using a regular virtual network provides the advantage of simulating a production environment including the ability to conduct application testing. The challenge is that it requires work to keep the test traffic isolated. This is a challenge because currently all routed networks in VMware Cloud on AWS 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"

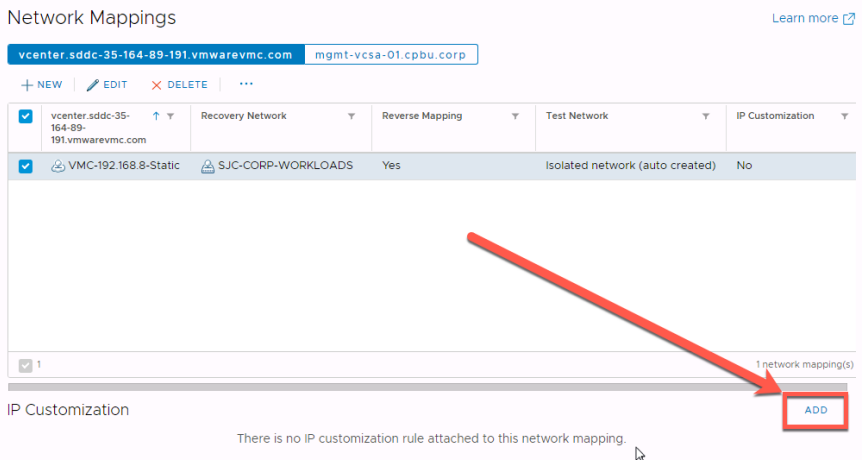
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com



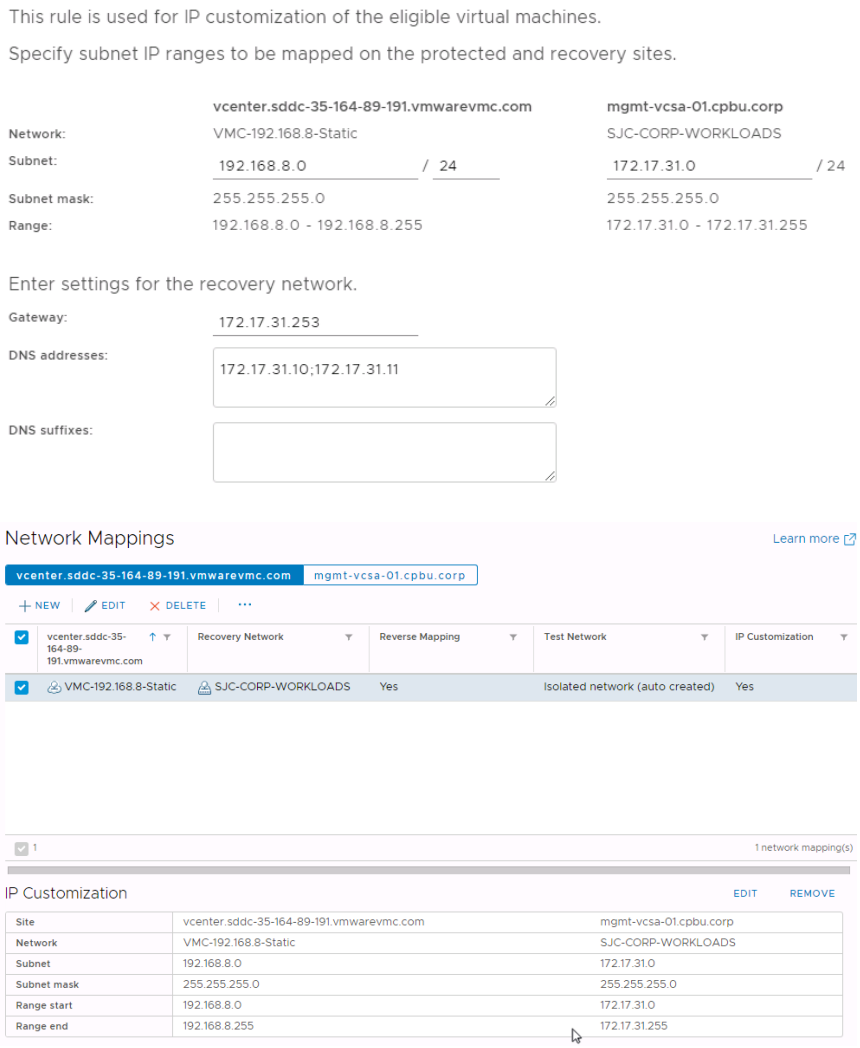
IP Subnet Mapping

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”



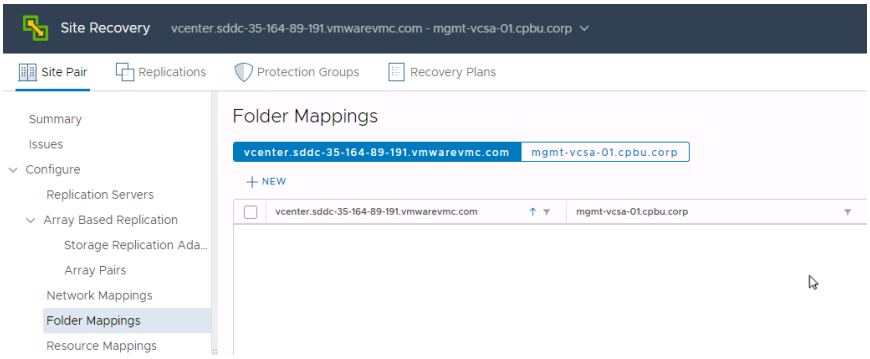
Enter the appropriate information for the source and recovery site and click “Save”



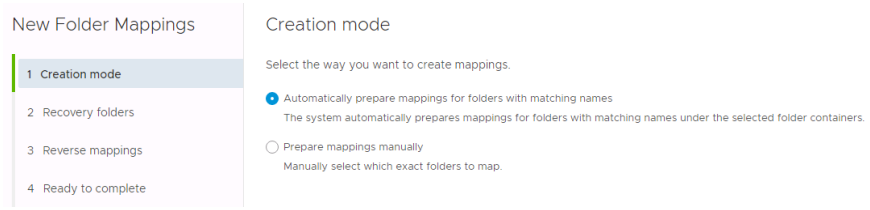
Next select the other vCenter and create the reverse IP customization rule

Folder Mapping

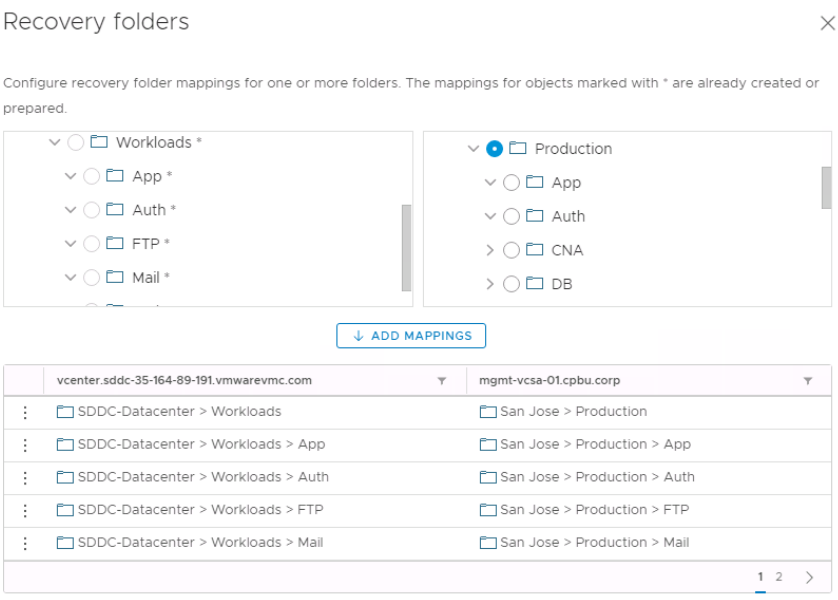
Folder mappings are much the same as network mappings without the added complexity of IP customization and test networks. To create folder mappings, select “Folder Mappings” and click “+New”.



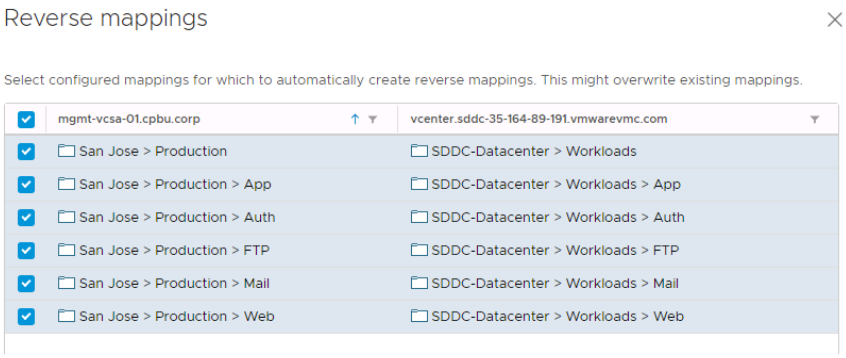
This example will show the “Automatically prepare mappings” option. Select it and click “Next”



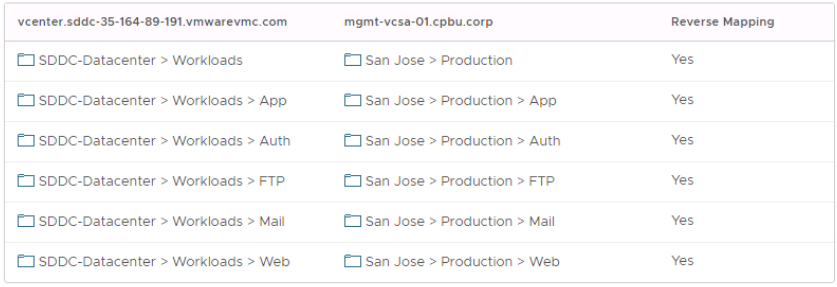
Select the level of the hierarchy where the folder names match and click “Add Mappings” and after all mappings have been added “Next”

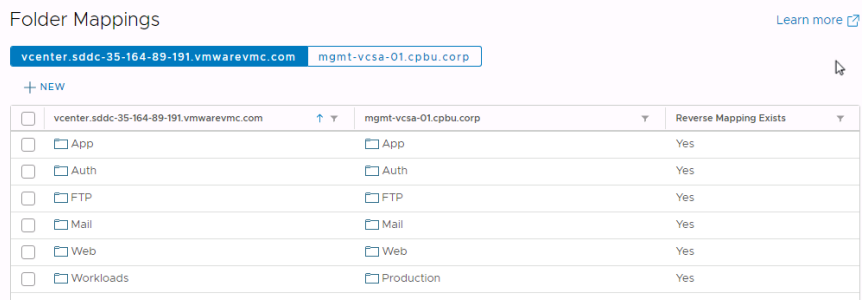


Select all to create reverse mappings and click “Next”



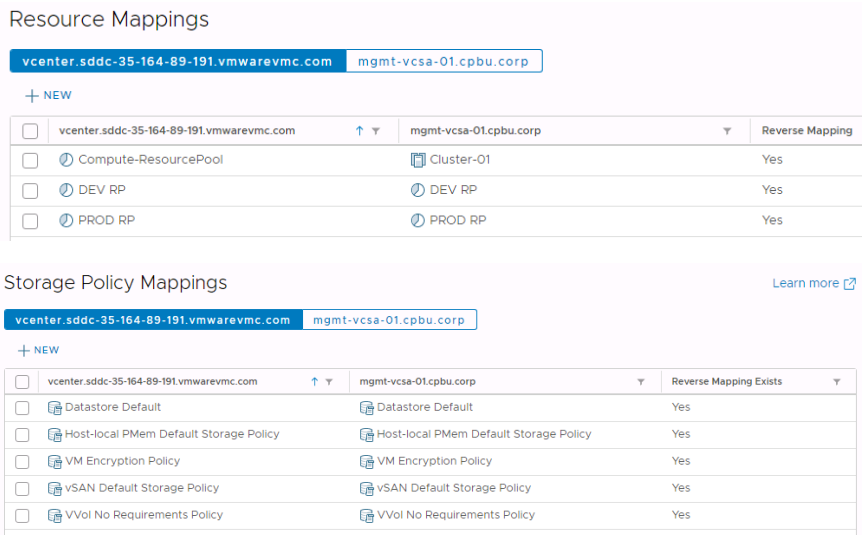
Review the settings and click “Finish”





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.

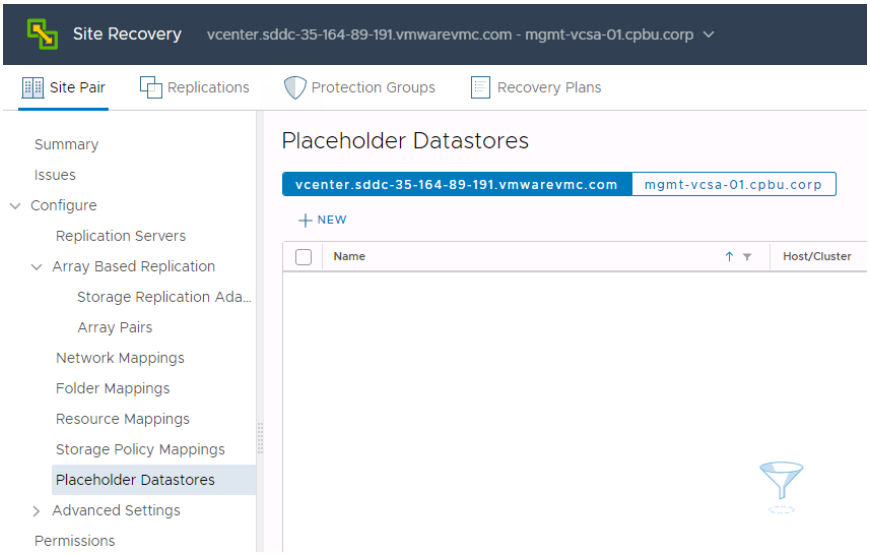


Placeholder Datastores

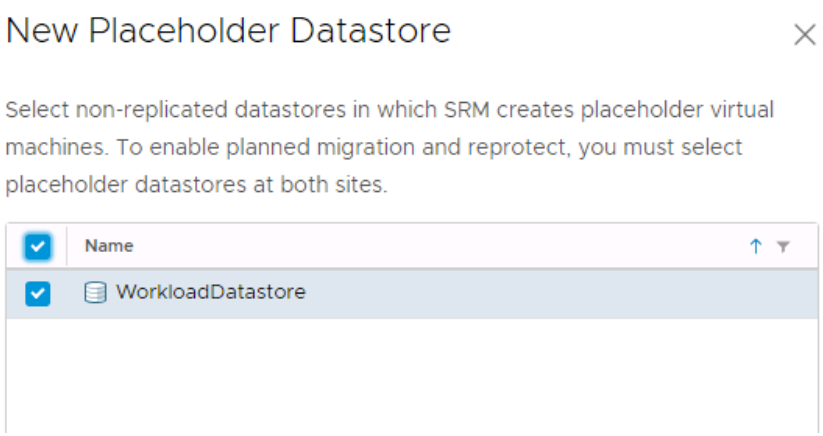
Placeholder datastores are used to store placeholder virtual machines. A placeholder datastore must be defined for each site.
A placeholder virtual machine is a subset of virtual machine files. VMware Site Recovery uses that subset of files to register a virtual machine with vCenter Server on the recovery 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”

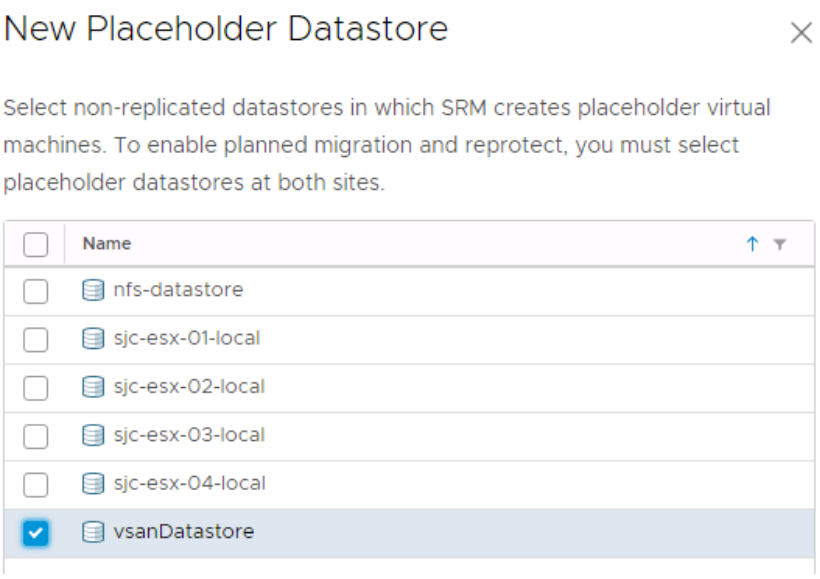


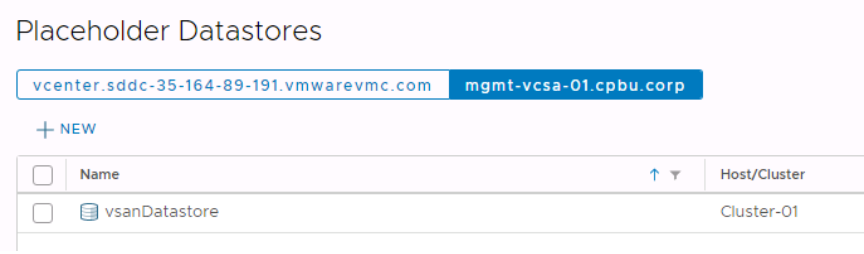
For the VMware Cloud on AWS SDDC select the Workload Datastore and click “Add”



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

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com



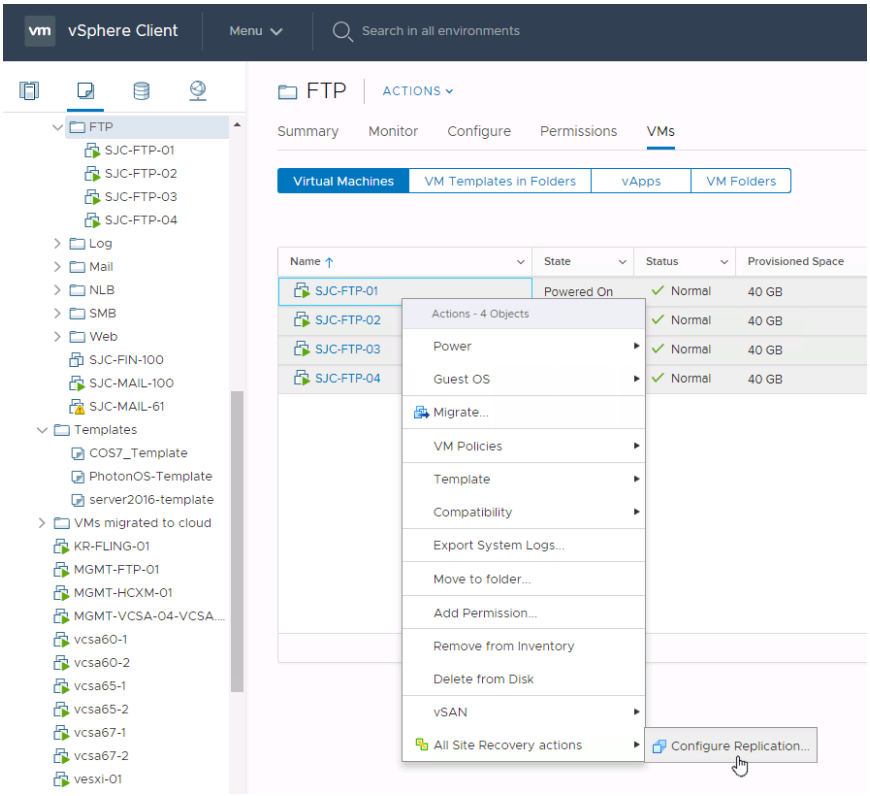


Protect VMs

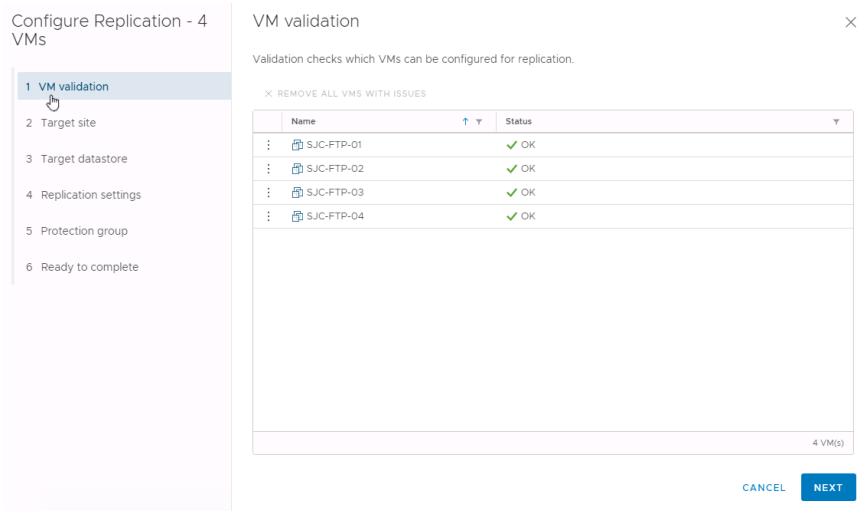
With mapping completed the next step is to start replicating and protecting virtual machines. The process of replicating virtual machines and adding them to protection groups and recovery plans is combined in VMware Site Recovery.

Replication

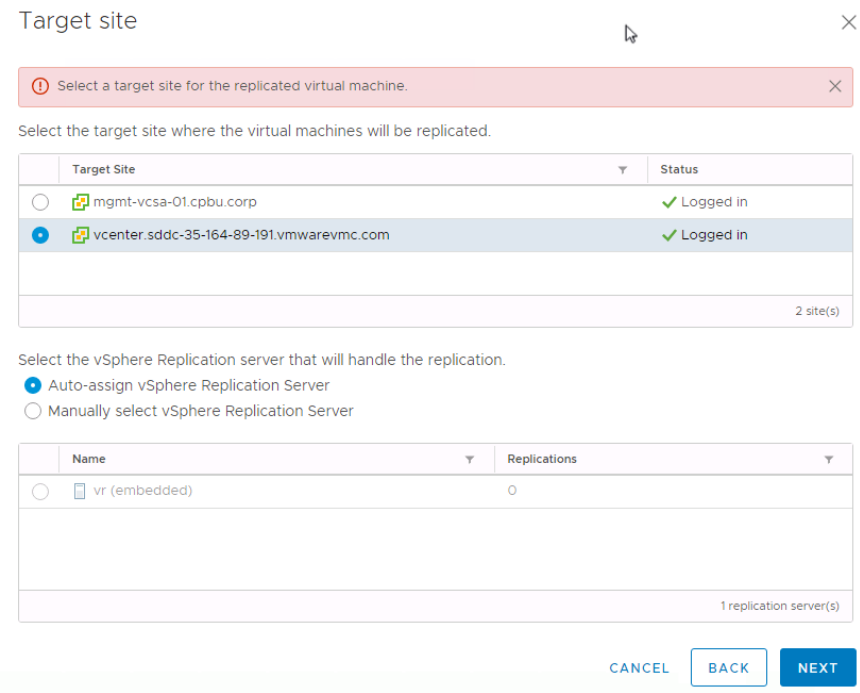
The easiest way to replicate virtual machines is to select them in the vSphere Web Client, right-click them and select “All Site Recovery actions” > “Configure Replication”



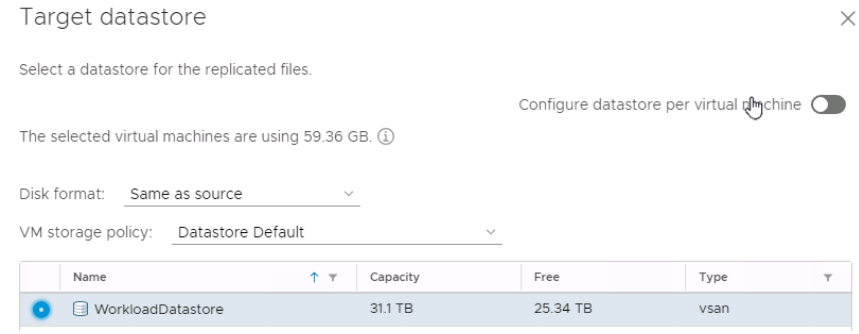
Select “Yes” to the “Open Configure replication wizard for the 4 selected virtual machines?” dialog. Confirm the correct virtual machines have been selected and click “Next”



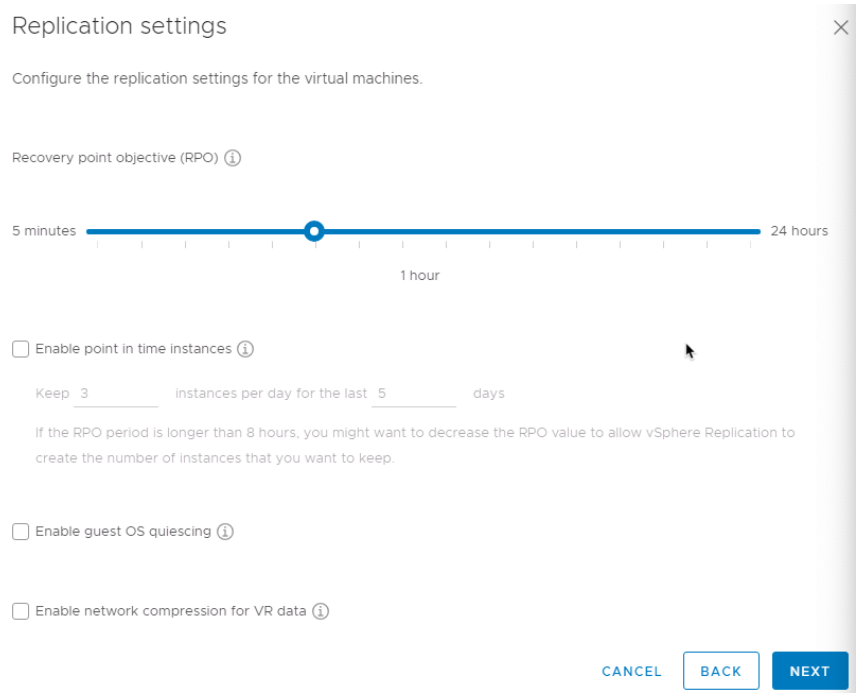
Select the target site for the replicated virtual machines. In this example we are protecting virtual machines that are running remote site so we will select our VMware Cloud on AWS SDDC. Then click “Next”



Next select the target disk format, storage policy and datastore



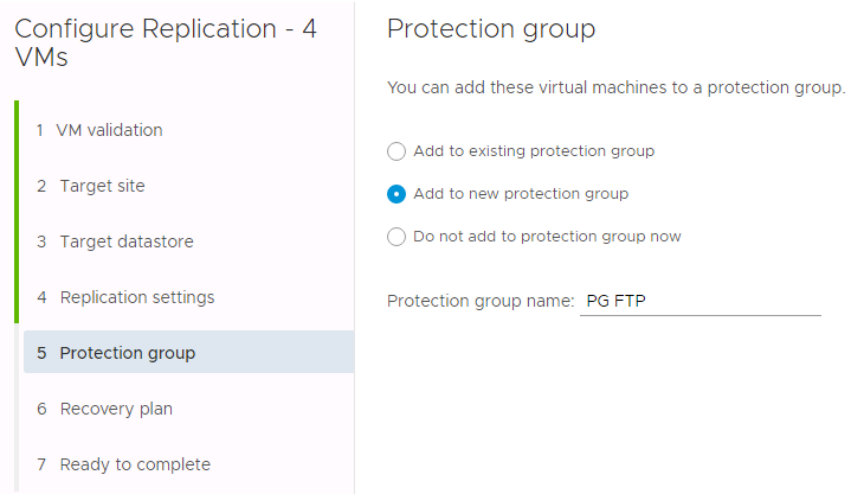
Now select replication settings. Recovery Point Objective (RPO) can be adjusted per virtual machine from 5 minutes up to 24 hours. vSphere Replication also supports guest OS quiescing for modern Windows virtual machines and some versions of Linux. If bandwidth is a concern some CPU can be traded for 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”



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.

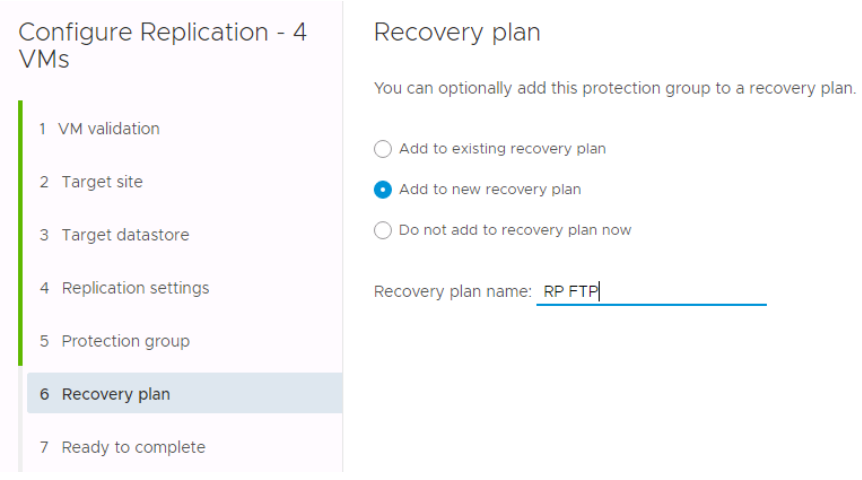
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com



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.

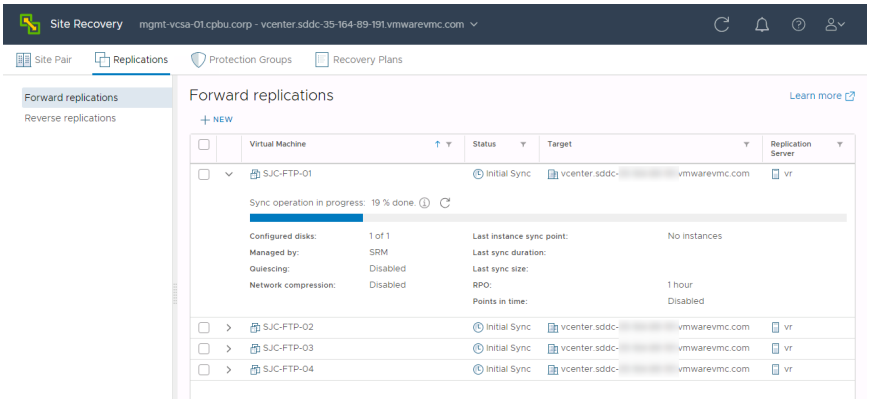
A recovery plan includes one or more protection groups. You can include a protection group in more than one recovery plan. For example, you can create one recovery plan to handle a planned migration of services from the protected site to the recovery site for the whole organization, and another set of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



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Monitoring Replications

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

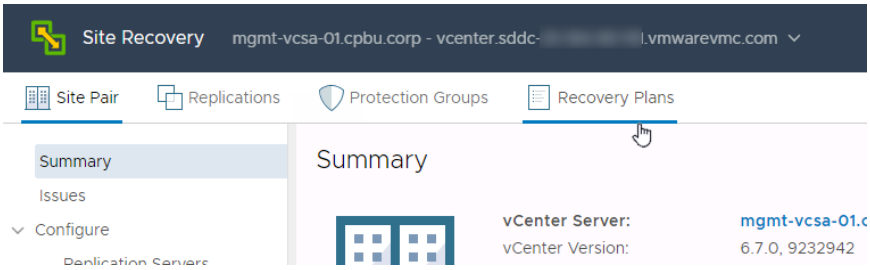


Priority Groups and Dependencies

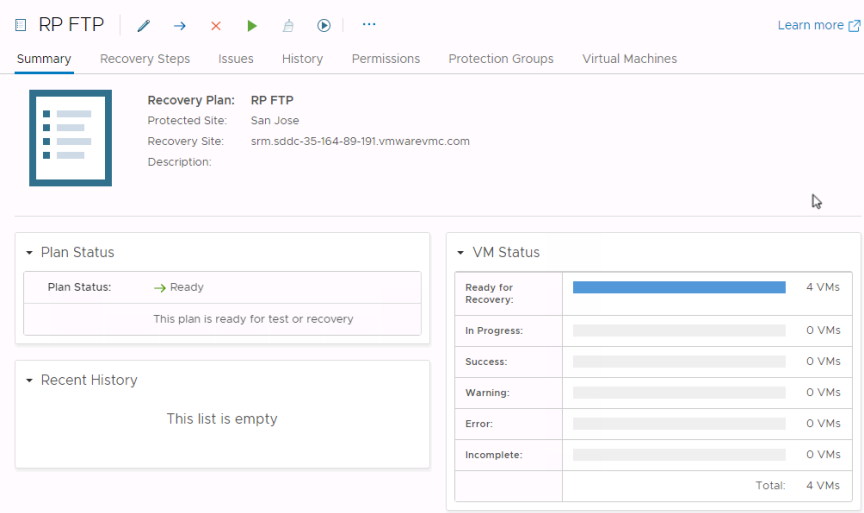
VMware Site Recovery starts virtual machines on the recovery site according to the priority that you set. VMware Site Recovery starts priority 1 virtual machines first, then priority 2 virtual machines second, and so on. VMware Site Recovery uses VMware Tools heartbeat to discover when a virtual machine 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.

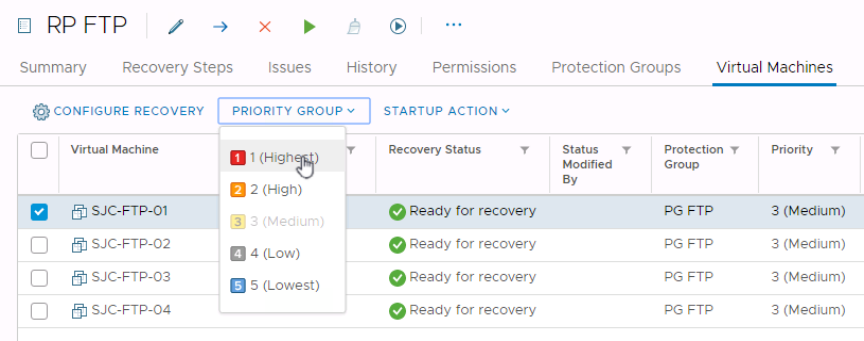
To select priority groups and create dependencies navigate to the “Recovery Plans” section and click on the recovery plan



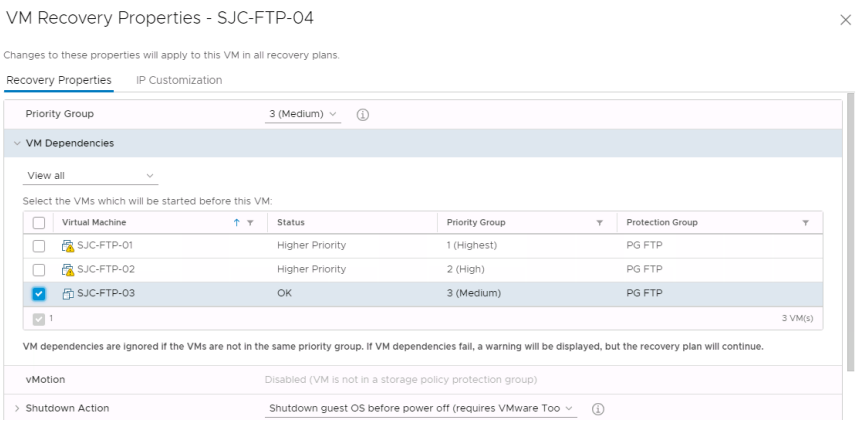
Now select “Virtual Machines”



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.



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

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

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

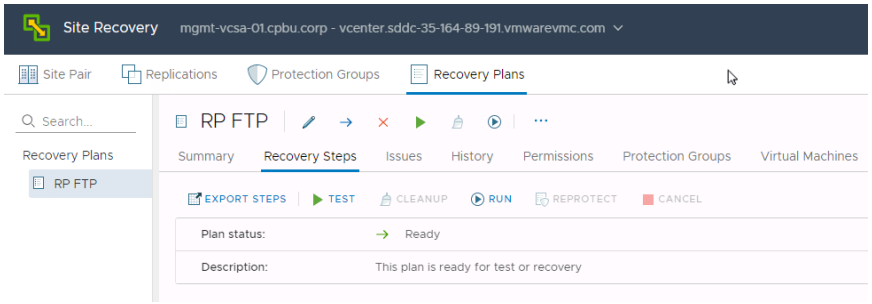
Now that virtual machines are being replicated and assigned to protection groups and recovery plans it is time to see what non-disruptive testing, failover and reprotect look like.

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.

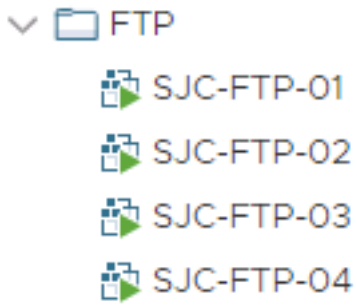
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com



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.



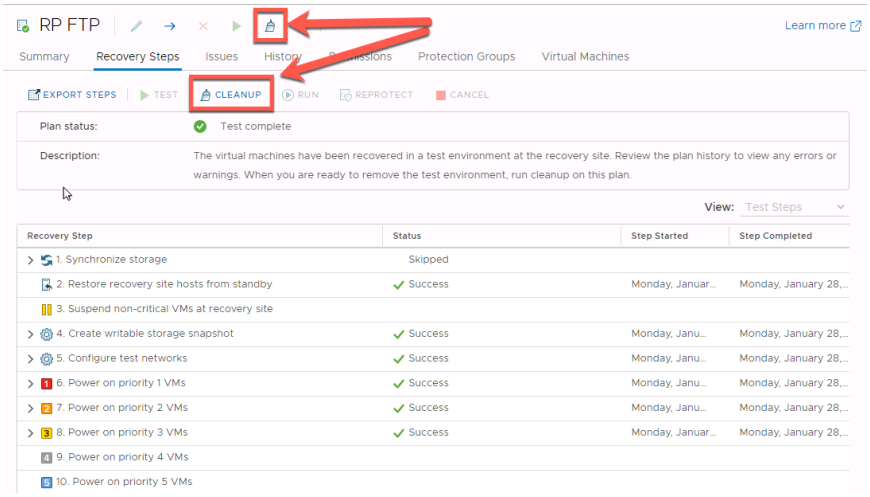
At this point, guest operating system administrators and application owners can log into their recovered virtual machines to verify functionality, perform additional testing, and so on. VMware Site Recovery easily supports recovery plan testing periods of varying lengths - from a few minutes to several 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.

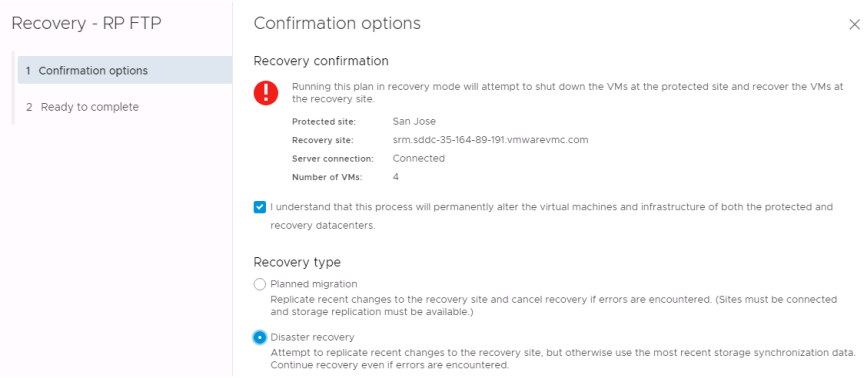


Failover

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.

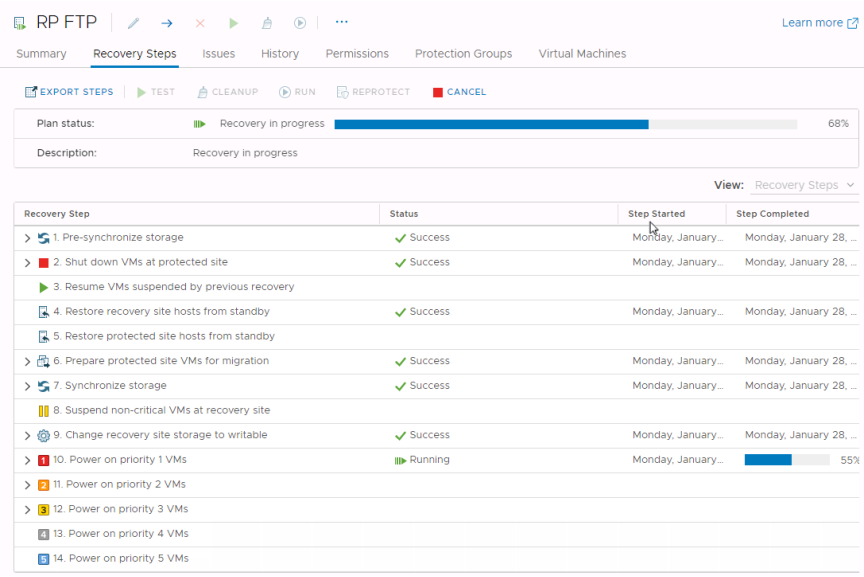
Clicking the Run Recovery Plan button opens a confirmation window requiring the selection of a recovery type - either a planned migration or a disaster recovery. In both cases, VMware Site Recovery will attempt to replicate recent changes from the protected site to the recovery site. It is assumed that 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.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com



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.

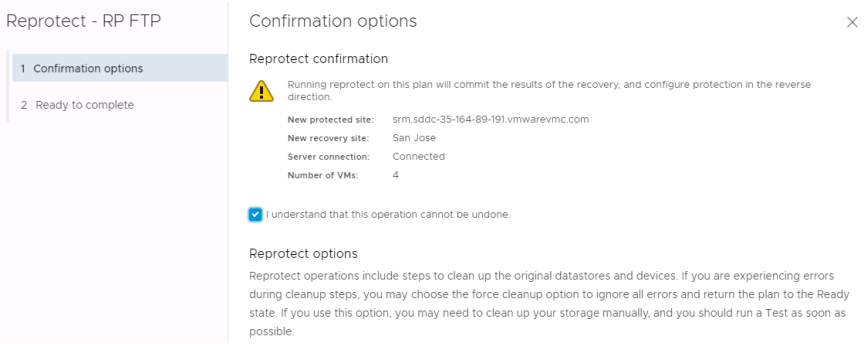
There are several roles and permissions available. For more information on roles and permissions, see VMware Site Recovery Privileges, Roles, and Permissions in the VMware Site Recovery documentation.

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.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

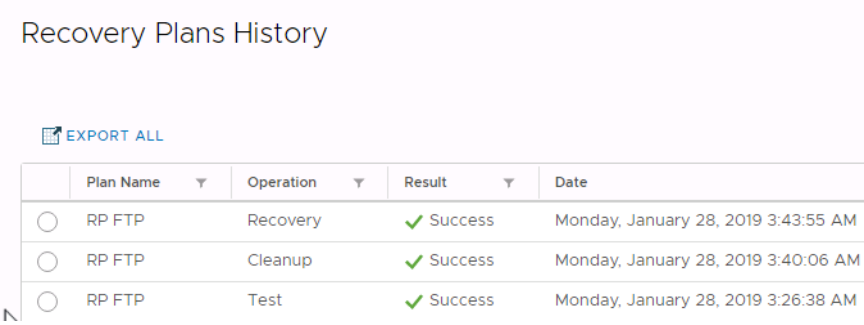


Reprotecting a recovery plan can take a considerable amount of time depending on the number of protection groups and virtual machines in the recovery plan and the amount of data that must be replicated to resynchronize storage. Upon completion of the reprotect workflow, a history reports will be created, 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.

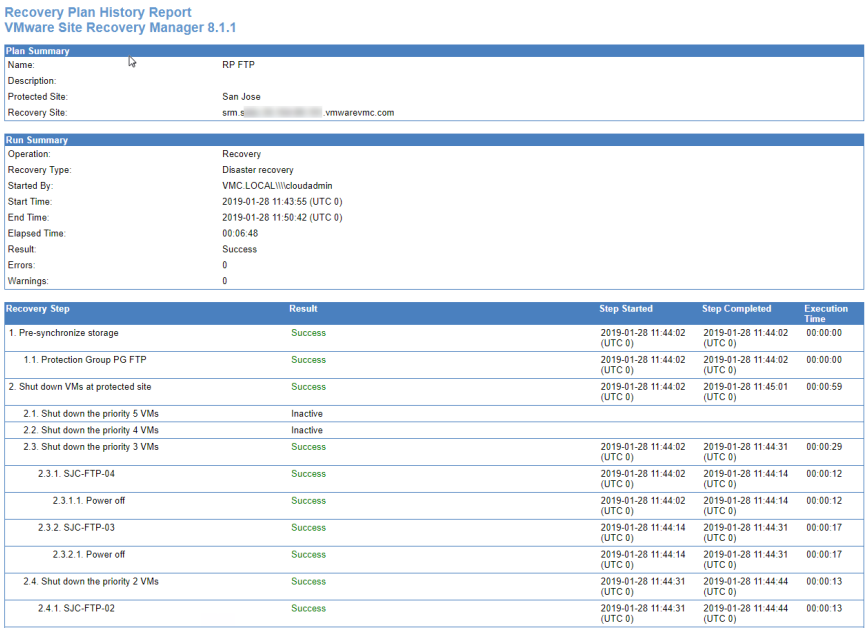
Recommendation: Test a recovery plan as soon as possible after a reprotect workflow has run to verify the recovery plan will work properly.

Reporting



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:	srm.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

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com