



VMware Site Recovery Technical Overview

VMware DRaaS

Table of contents

VMware Site Recovery Technical Overview	4
Introduction	5
Features and Benefits of VMware Site Recovery	6
Overview	7
Use Cases	8
Overview	8
Disaster Recovery	8
Disaster Avoidance	8
Upgrade and Patch Testing	8
Topologies	9
Overview	9
Active-Passive	9
Active-Active	9
Bi-Directional	9
Deployment and Configuration	10
Overview	10
Enable add-on	10
Install on-premises components	10
Create Firewall Rules and Pair sites	11
Inventory Mappings	11
Placeholder Virtual Machines and Datastores	12
Replication	13
Protection Groups	14
Overview	14
Recovery Plans	15
Overview	15
Priority Groups	15
Dependencies	16
Shutdown and Startup Actions	16
Pre and Post Power On Steps	17
IP customization	17
Workflows	19

Testing and Cleanup 19

Planned Migration and Disaster Recovery 20

Re-Protect and Failback 22

History Reports 22

..... 22

..... 22

Next Steps 23

Terminology 23

Sample Workflow Report 24

VMware Site Recovery Technical Overview

Technical overview of the features and capabilities of VMware Site Recovery for VMware Cloud on AWS

Introduction

VMware Site Recovery™ brings VMware enterprise-class Software-Defined Data Center (SDDC) Disaster Recovery as a Service to the AWS Cloud. It enables customers to protect and recover applications without the requirement for a dedicated secondary site. It is delivered, sold, supported, maintained, and managed by VMware as an on-demand service. IT teams manage their cloud-based resources with familiar VMware tools—without the difficulties of learning new abilities or utilizing new tools.

VMware Site Recovery is an add-on feature to VMware Cloud on AWS, powered by VMware Cloud Foundation™. VMware Cloud on AWS integrates VMware's flagship compute, storage, and network virtualization products—VMware vSphere, VMware vSAN™, and VMware NSX®—along with VMware vCenter Server® management. It optimizes them to run on elastic, bare-metal AWS infrastructure. With the same architecture and operational experience on-premises and in the cloud, IT teams can now get instant business value via the AWS and VMware hybrid cloud experience.

The VMware Cloud on AWS solution enables customers to have the flexibility to treat their private cloud and public cloud as equal partners and to easily transfer workloads between them—for example, to move applications from DevTest to production or burst capacity. Users can leverage the global AWS footprint while getting the benefits of elastically scalable SDDC clusters, a single bill from VMware for its tightly integrated software plus AWS infrastructure, and on-demand or subscription services like VMware Site Recovery Service.

VMware Site Recovery extends VMware Cloud on AWS to provide managed disaster recovery, disaster avoidance, and non-disruptive testing capabilities to VMware customers without the need for a secondary site, or complex configuration.

VMware Site Recovery works in conjunction with VMware Site Recovery Manager™ and VMware vSphere Replication™ to automate the process of recovering, testing, re-protecting, and failing-back virtual machine workloads.

VMware Site Recovery utilizes VMware Site Recovery Manager servers to coordinate the operations of the VMware SDDC. This is so that as virtual machines at the protected site are shut down, copies of these virtual machines at the recovery site startup. By using the data replicated from the protected site these virtual machines assume responsibility for providing the same services.

VMware Site Recovery can be used between a customer's datacenter and an SDDC deployed on VMware Cloud on AWS or it can be used between two SDDCs deployed to different AWS availability zones or regions. The second option allows VMware Site Recovery to provide a fully VMware-managed and maintained Disaster Recovery solution.

Migration of protected inventory and services from one site to the other is controlled by a recovery plan that specifies the order in which virtual machines are shut down and started up, the resource pools to which they are allocated, and the networks they can access. VMware Site Recovery enables the testing of recovery plans, using a temporary copy of the replicated data, and isolated networks in a way that does not disrupt ongoing operations at either site. Multiple recovery plans can be configured to migrate individual applications or entire sites providing finer control over what virtual machines are failed over and failed back. This also enables flexible testing schedules.

VMware Site Recovery extends the feature set of the virtual infrastructure platform to provide for rapid business continuity through partial or complete site failures.

The screenshot displays the VMware Site Recovery Manager (SRM) console. The top navigation bar includes 'Site Recovery', 'Replications', 'Protection Groups', and 'Recovery Plans'. The left sidebar shows a tree view with 'Summary' selected, followed by 'Issues', 'Configure' (with sub-items: Replication Servers, Network Mappings, Folder Mappings, Resource Mappings, Placeholder Datastores), 'Advanced Settings', 'Permissions', and 'Recovery Plans History'.

The main content area is titled 'Summary' and features a 'RECONFIGURE SITE PAIR' button and a 'BREAK SITE PAIR' button. Below this is a 'vCenter Server' section with a table comparing two vCenters:

vCenter Server:	vcenter.sddc-52-27-147-146.vmc.vmware.com	vccentersitea.vsanpe.vmware.com
vCenter Version:	6.6.2, 6814799	6.5.0, 5973321
vCenter Host Name:	vcenter.sddc-52-27-147-146.vmc.vmware.com:443	vccentersitea.vsanpe.vmware.com:443
Platform Service Controller:	vcenter.sddc-52-27-147-146.vmc.vmware.com:443	psscsitea.vsanpe.vmware.com:443

Below the vCenter section is the 'Site Recovery Manager' section, which shows 'Protection Groups: 0' and 'Recovery Plans: 0'. It contains a table for 'Remote SRM connection' with two entries, both showing a 'Connected' status with a green checkmark.

The 'vSphere Replication' section follows, showing 'Replicated VMs from vcenter.sddc-52-27-147-146.vmc.vmware.com: 0' and 'Replicated VMs from vccentersitea.vsanpe.vmware.com: 0'. It contains a table for 'Remote VR connection' with two entries, both showing a 'Connected' status with a green checkmark.

Features and Benefits of VMware Site Recovery

- Provides familiar features and functionality with enhanced workflows to reduce time to protection and risk
- An easy-to-use disaster recovery/secondary site that is supported and maintained by VMware. This lowers capital costs and makes it easier to protect more virtual machines faster.
- Application-agnostic protection eliminates the need for app-specific point solutions
- Automated orchestration of site failover and failback with a single click reduces recovery times
- Frequent, non-disruptive testing of recovery plans ensures highly predictable recovery objectives
- Enhanced, easy to use, consolidated protection workflow simplifies replicating and protecting virtual machines
- Centralized management of recovery plans from the vSphere Web Client replaces manual runbooks
- vSphere Replication integration delivers VM-centric, replication that eliminates dependence on a particular type of storage
- Flexible versioning allows for easier upgrades and ongoing management

Overview

VMware Site Recovery is deployed in a paired configuration, for example, protected/customer site and recovery/VMware Cloud on AWS site. This document will use the two terms interchangeably because either the customer site or VMware Cloud on AWS site can be either the protected or recovery sites.

VMware Site Recovery utilizes VMware Site Recovery Manager and vSphere Replication. For the VMware Cloud on AWS instance, VMware automatically installs and configures this software when the add-on is enabled. For the customer site, VMware Site Recovery Manager and vSphere Replication are both deployed as an appliance by the customer. VMware Site Recovery requires a VMware vCenter Server at the customer site as well. The customer site vCenter can be running VMware vCenter Server version 7.0 or higher. One or more vSphere hosts must run version 7.0 or higher at the customer site. VMware Site Recovery utilizes vSphere Replication for transferring data between sites.

VMware Site Recovery and VMware vCenter Server and the workloads they protect require infrastructure services like DNS, DHCP, and Active Directory. These must be in place at both the protected and recovery sites.

The screenshot shows the vSphere Client interface. The top navigation bar includes the VMware logo, 'vSphere Client', a menu, a search bar, a 'Getting Started' button, a refresh icon, a help icon, and a user profile 'cloudadmin@vmc.local'. The left-hand navigation pane lists various sections: Home, Shortcuts, Hosts and Clusters, VMs and Templates, Storage, Networking, Content Libraries, Global Inventory Lists, Policies and Profiles, Auto Deploy, Site Recovery (highlighted with a red arrow), Administration, Tasks, Events, Tags & Custom Attributes, and New Search. The main content area displays the 'Home' dashboard for 'VCENTER.SDDC-52-27-147-146.VMC.VMWARE.COM'. It features three summary cards: CPU (317.54 GHz free, 13.55 GHz used, 331.09 GHz total), Memory (1.79 TB free, 218.87 GB used, 2 TB total), and Storage (80.33 TB free, 2.61 TB used, 82.95 TB total). Below these are two summary cards: 'VMs' (134 total, 101 Powered On, 33 Powered Off, 0 Suspended) and 'Hosts' (4 total, 4 Connected, 0 Disconnected, 0 Maintenance). At the bottom, there is a card for 'Objects with most alerts' (0 items) and a card for 'Installed Plugins' (4 items, including VMware Site Recovery, SDDC NSX Manager, VMware Update Manager, and vShield Manager).

VMware Site Recovery supports protection for up to 1500 virtual machines, and 250 recovery plans and can simultaneously run up to 10 recovery plans. Up to 250 virtual machines can be included in a single protection group, and VMware Site Recovery supports up to 250 protection groups.

Use Cases

Overview

Though the most obvious use case for VMware Site Recovery is disaster recovery from one site to another, it can handle a number of different use cases and provide significant capability and flexibility to customers. For all use cases and situations, VMware Site Recovery supports non-disruptive testing of recovery plans in network and storage isolated environments. This provides for the ability to test disaster recovery, disaster avoidance, or planned migrations as frequently as desired to ensure confidence in the configuration and operation of recovery plans.

Disaster Recovery

Disaster recovery or an unplanned failover is what VMware Site Recovery was specifically designed to accomplish. This is the most critical but least frequently used use case for VMware Site Recovery. Unexpected site failures don't happen often but when they do a fast recovery is critical to business. VMware Site Recovery can help in this situation by automating and orchestrating the recovery of critical business systems for partial or full site failures ensuring the fastest RTO.

Disaster Avoidance

Preventive failover is another common use case for VMware Site Recovery. This can be anything from an oncoming storm to the threat of power issues.

VMware Site Recovery allows for the graceful shutdown of virtual machines at the protected site, full replication of data, and ordered startup of virtual machines and applications at the recovery site ensuring app-consistency and zero data loss.

Upgrade and Patch Testing

The VMware Site Recovery test environment provides a perfect location for conducting operating system and application upgrade and patch testing. Test environments are complete copies of production environments configured in an isolated network segment which ensures that testing is as realistic as possible while at the same time not impacting production workloads or replication.

Topologies

Overview

VMware Site Recovery can be used in a number of different failover scenarios depending on customer requirements, constraints, and objectives. All of these arrangements are supported and easily configured.

Active-Passive

In the traditional active-passive scenario there is a production site running applications and services and a secondary or recovery site that is idle until needed for recovery. This topology is common and though it provides dedicated recovery resources it means paying for a site, servers, and storage that aren't utilized much of the time.

Active-Active

VMware Site Recovery can be used where low-priority workloads such as test and development run at the recovery site and are powered off as part of the recovery plan. This allows for the utilization of recovery site resources as well as sufficient capacity for critical systems in case of a disaster.

Bi-Directional

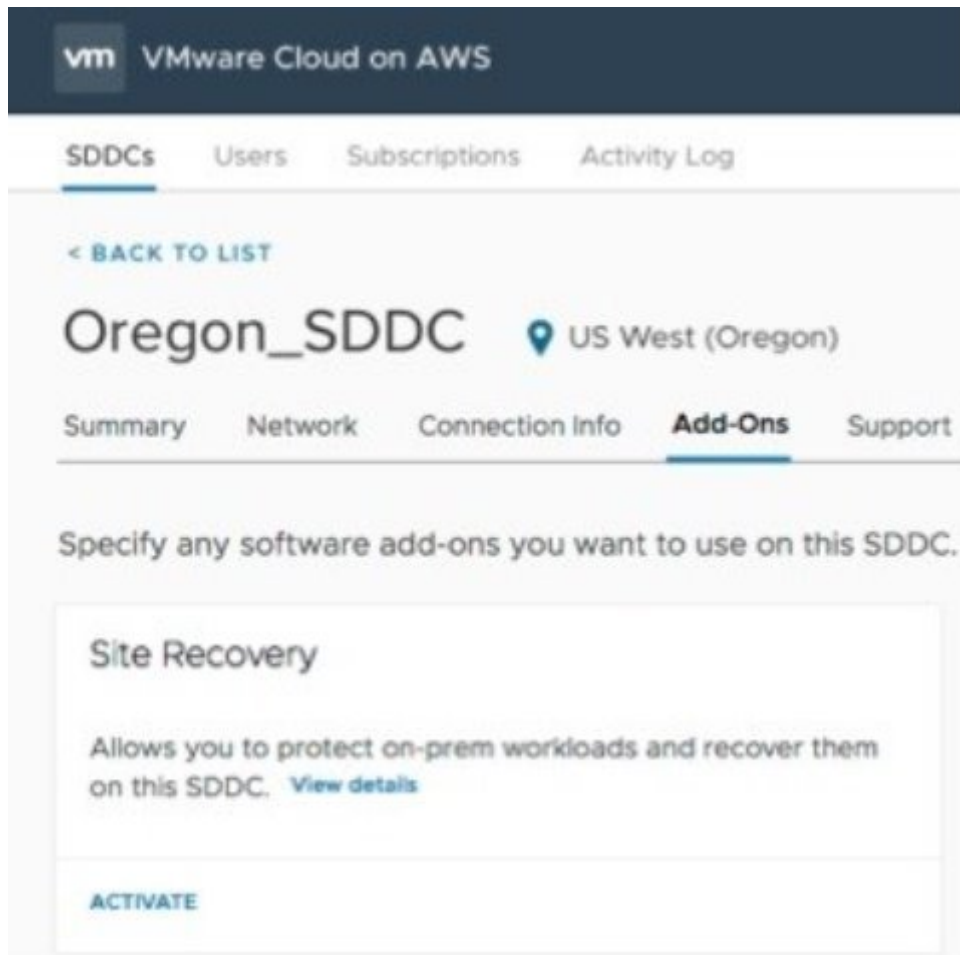
In situations where production applications are operating at both sites, VMware Site Recovery supports protecting virtual machines in both directions (eg. virtual machines at Site A protected at site B and virtual machines at site B protected at site A).

Deployment and Configuration

Overview

The process of deploying and configuring VMware Site Recovery is simple and logical. This document will cover these steps at a high level. For detailed installation and configuration instructions please see the VMware Site Recovery Installation and Administration Guides.

Enable add-on



Enabling the VMware Site Recovery add-on is a single click operation that takes 10-15 minutes to complete. It involves VMware automatically deploying and configuring VMware Site Recovery Manager and vSphere Replication for the customers VMware Cloud on AWS SDDC. If the customer is configuring disaster recovery between two VMware Cloud on AWS SDDCs the entire deployment process is automated for both.

Install on-premises components

If using an on-premises environment, while VMware Site Recovery components are being deployed to the VMware Cloud on AWS SDDC the on-premises components can be downloaded and installed. This entails deploying the vSphere Replication appliance from an OVF and installing VMware Site Recovery Manager on a Windows server.

Deploy OVF Template

- 1 Select template
- 2 Select name and location
- 3 Select a resource
- 4 Review details
- 5 Accept license agreements
- 6 Select configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 vService bindings**
- 11 Ready to complete

vService bindings
Select the vServices to which the deployed OVF template should bind

vCenter Extension Installation

This appliance requires a binding to the vCenter Extension vService, which allows it to register as a vCenter Extension at runtime.

Provider: vCenter Extension vService

Binding status: ✓

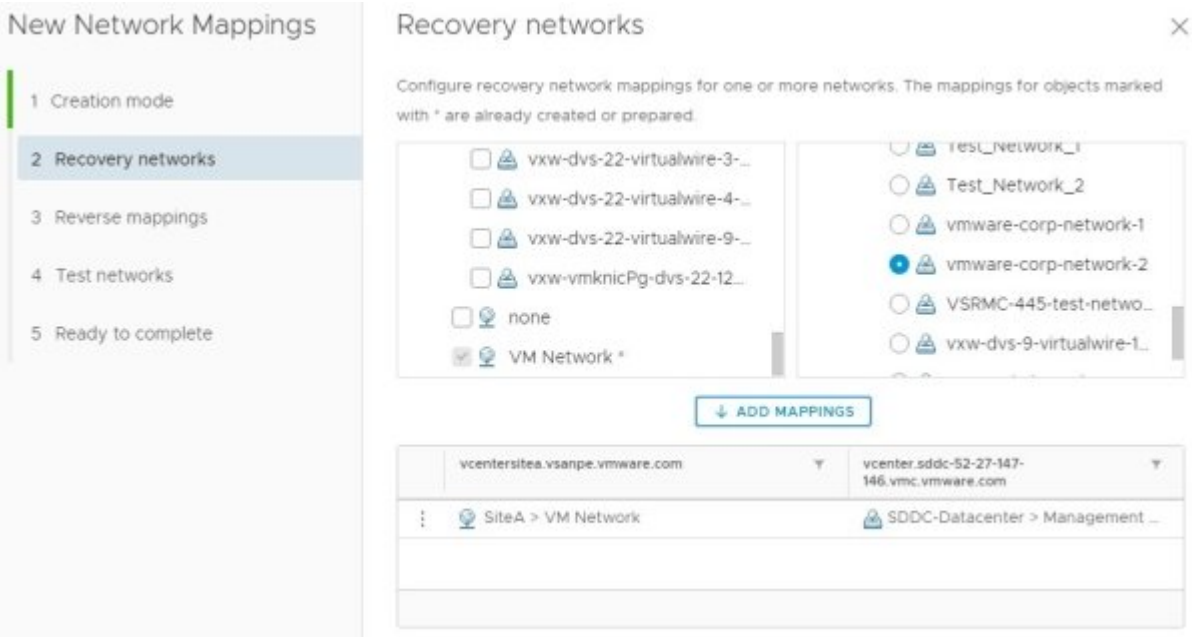
Validation Message: Success

Create Firewall Rules and Pair sites

Creating firewall rules in VMware Cloud on AWS involves creating four rules to allow the customers on-premises components to communicate with the VMware Cloud on AWS components. Site pairing connects VMware Site Recovery and vSphere Replication at the two sites together. This enables the two sites to operate with each other.

Rule Name	Action	Source	Destination
VSR - SRM Ma...	Allow	10.0.0.0/8	Site Recovery Manager
Service		Ports	
SRM Server Management (TCP 9086)		9086	
Rule Name	Action	Source	Destination
VSR - VM Repli...	Allow	10.0.0.0/8	vSphere Replication
Service		Ports	
Any (All Traffic)		31031, 44046	
Rule Name	Action	Source	Destination
VSR - VR Mana...	Allow	10.0.0.0/8	vSphere Replication
Service		Ports	
VR Server Management (TCP 8043)		8043	
Rule Name	Action	Source	Destination
VSR - UI/API	Allow	10.0.0.0/8	vSphere Replication
Service		Ports	
HTTPS (TCP 443)		443	

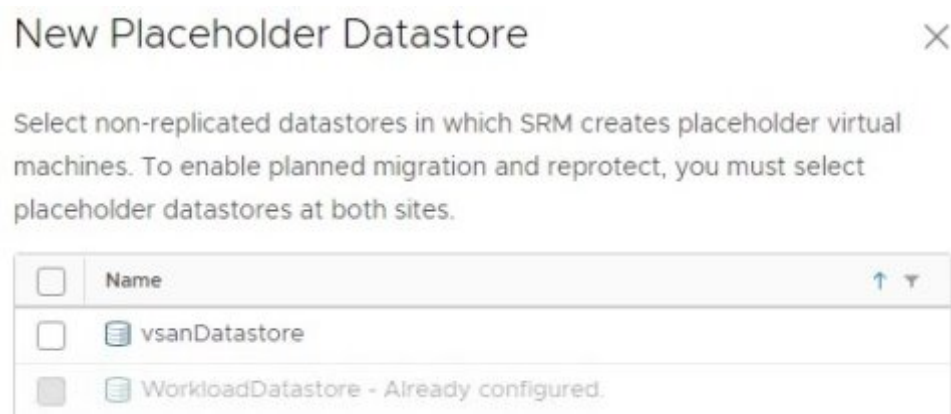
Inventory Mappings



There are multiple types of inventory mappings in VMware Site Recovery: Resource mappings, folder 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 “VM Network” at the protected site and a network port group named “vmware-corp-network-2” at the recovery site. As a result of this mapping, virtual machines connected to “VM Network” at the protected site will, by default, automatically be connected to “vmware-corp-network-2” at the recovery site. Networks to be used during testing can also be configured in the same area.

Placeholder Virtual Machines and Datastores

For each protected virtual machine VMware Site Recovery creates a placeholder virtual machine at the recovery site. Placeholder virtual machines are contained in a datastore, and registered with the VMware vCenter Server at the site. This datastore is called the “placeholder datastore”. Since placeholder virtual machines do not have virtual disks they consume a minimal amount of storage.



The protected and recovery sites will each require that a datastore that is accessible by all hosts at that site be created or allocated for use as the placeholder datastore. For VMware Site Recovery the vSAN Workload Datastore would be used. Each site requires at least one placeholder datastore to allow for failover as well as fallback.

Replication

VMware Site Recovery utilizes vSphere Replication to move virtual machine data between sites. vSphere Replication is able to utilize any storage supported by vSphere so there is no requirement for storage arrays, similar or otherwise, at either site.

vSphere Replication supports RPOs from 5 mins to 24 hours and also supports network compression, traffic encryption, multiple point-in-time recovery, and file-system quiescing for both Windows and Linux.

Configure Replication - 20 VMs

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

Replication settings [X]

Configure the replication settings for the virtual machines.

Recovery Point Objective (RPO) ⓘ

5 minutes [Slider] 24 hours

5 minutes

☐ Enable guest OS quiescing ⓘ

☒ Enable network compression for VR data ⓘ

For more details about vSphere Replication see the [vSphere Replication Technical Overview](#)

Protection Groups

Overview

Protection groups are a way of grouping virtual machines that will be recovered together. In many cases, a protection group will consist of the virtual machines that support a service or application such as email or an accounting system. For example, an application might consist of a two-server database cluster, three application servers, and four web servers. In most cases, it would not be beneficial to fail over part of this application, only two or three of the virtual machines in the example, so all nine virtual machines would be included in a single protection group.

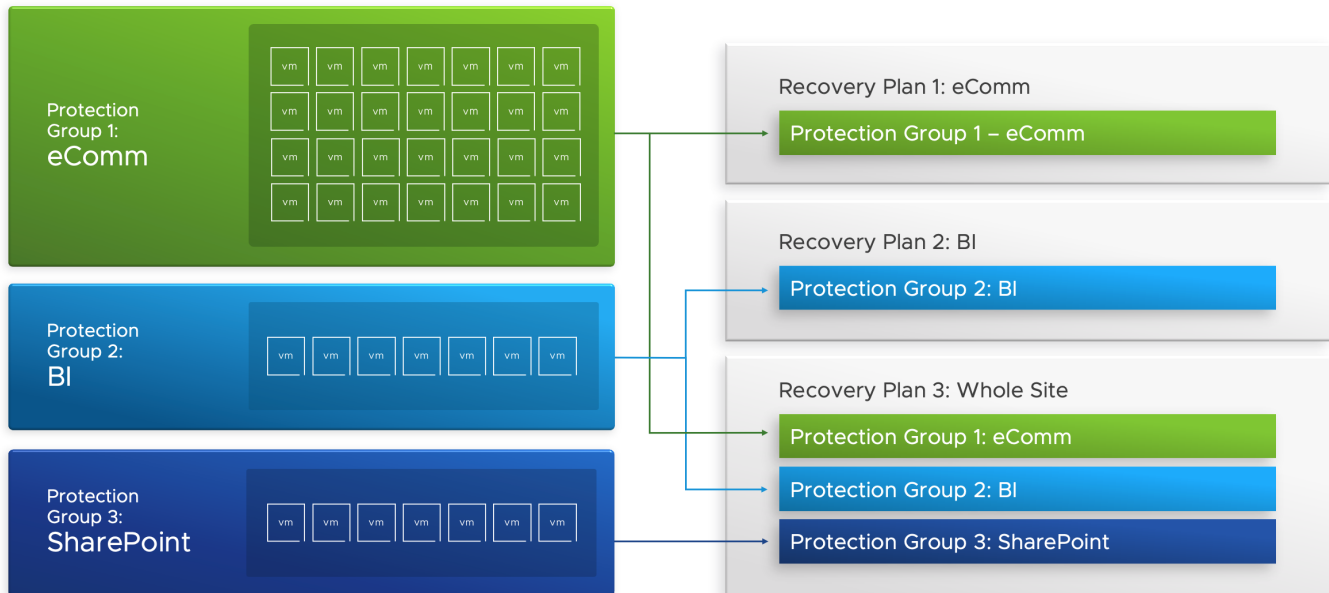
Creating a protection group for each application or service has the benefit of selective testing. Having a protection group for each application enables non-disruptive, low-risk testing of individual applications allowing application owners to non-disruptively test disaster recovery plans as needed. Note that a virtual machine can only belong to a single protection group. However, a protection group can belong to one or more recovery plans.

For virtual machines protected by VMware Site Recovery, deciding what virtual machines are going to belong to what protection group is simple. Since virtual machines are replicated on an individual basis, whatever makes sense from a recovery standpoint. vSphere replication protection groups are not tied to storage type or configuration.

Recovery Plans

Overview

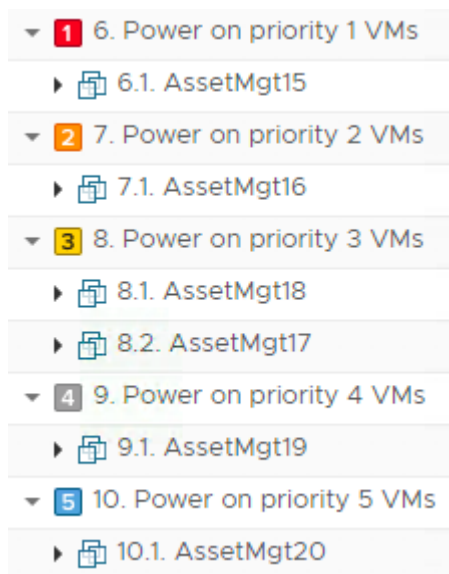
Recovery Plans in VMware Site Recovery are like an automated runbook, controlling all the steps in the recovery process. The recovery plan is the level at which actions like failover, planned migration, testing, and re-protect are conducted. A recovery plan contains one or more protection groups and a protection group can be included in more than one recovery plan. This provides for the flexibility to test or recover an application by itself and also test or recover a group of applications or the entire site.



In the example above there are two protection groups: Accounting and Email. And there are three recovery plans: The Accounting recovery plan containing the Accounting protection group, the Email recovery plan containing the Email protection group, and the Entire Site recovery plan containing both protection groups.

Priority Groups

There are five priority groups in VMware Site Recovery. The virtual machines in priority group one are recovered first, then the virtual machines in priority group two are recovered, and so on. All virtual machines in a priority group are started at the same time and the next priority group is started only after all virtual machines are booted up and responding.



This provides administrators with one option for prioritizing the recovery of virtual machines. For example, the most important virtual machines with the lowest RTO are typically placed in the first priority group and less important virtual machines in

subsequent priority groups. Another example is by application tier - database servers could be placed in priority group two; application and middleware servers in priority group 3; client and web servers in priority group four.

Dependencies

When more granularity is needed for startup order dependencies can be used. A dependency requires that before a virtual machine can start, another specified virtual machine must already be running. For example, a virtual machine named “acct02” can be configured to have a dependency on a virtual machine named “acct01” - VMware Site Recovery will wait until “acct01” starts before powering on “acct02”. VMware Tools heartbeats are used to validate when a virtual machine has started successfully.

VM Recovery Properties - AssetMgt18



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

Recovery Properties IP Customization

Priority Group
3 (Medium)

VM Dependencies

View VM dependencies

The following VMs will be started before this VM:

Virtual Machine	Status	Priority Group	Protection Group
AssetMgt17	OK	3 (Medium)	PG_Asset_Mgmt

1 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.

Shutdown and Startup 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. First, shutting it down quiesces the guest OS and applications before the final storage synchronization occurs. And second, it avoids the potential conflict of having virtual machines with duplicate network configurations 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.

Shutdown Action

Shutdown guest OS before power off (requires VMware Tools)

Timeout

5 minutes 0 seconds

In Disaster Recovery mode, the VM will be powered off if Shutdown guest OS fails.

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. 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.

Startup Action

Power on

VMware Tools

☒ Wait for VMware tools

5

minutes

0

seconds

Additional Delay

☐ Additional delay before running Post Power On steps and starting dependent VMs.

0

minutes

0

seconds

Pre and Post Power On Steps

As part of a recovery plan, VMware Site Recovery can run a command on a recovered virtual machine after powering it on. A common use case is calling a script to perform actions such as making changes to DNS and modifying application settings on a physical server. VMware Site Recovery can also display a visual prompt before or after any step in the recovery plan. 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.

Plan status:

Waiting for user input

68%

Description:

The test has paused at a user prompt. Dismiss the prompt to resume the test.

Prompts:

Verify Database Servers Are Ready

DISMISS

Connect into each of the priority one database servers and run the transaction test to verify they are ready for the application servers to be turned on.

IP customization

The most commonly modified virtual machine recovery property is IP customization. The majority of organizations have different IP address ranges at the protected and recovery sites. When a virtual machine is failed over, VMware Site Recovery can automatically change the network configuration (IP address, default gateway, etc.) of the virtual network interface card(s) in the virtual machine. This functionality is available in both failover and failback operations.

There are multiple IP customization modes in VMware Site Recovery. For example, it is possible to create an IP customization rule that maps one range of IP addresses to another. In the figure below, an administrator has mapped 10.10.10.0/24 to 192.168.100.0/24.

	vcentersitea.vsanpe.vmware.com	vcenter.sddc-52-27-147-146.vmc.vmware.com
Network:	DPG_VM_Network_1284	sddc-cgw-network-1
Subnet:	10.10.10.0 / 24	192.168.100.0 / 24
Subnet mask:	255.255.255.0	255.255.255.0
Range:	10.10.10.0 - 10.10.10.255	192.168.100.0 - 192.168.100.255

Enter settings for the recovery network.

Gateway:

192.168.100.254

DNS addresses:

192.168.100.10

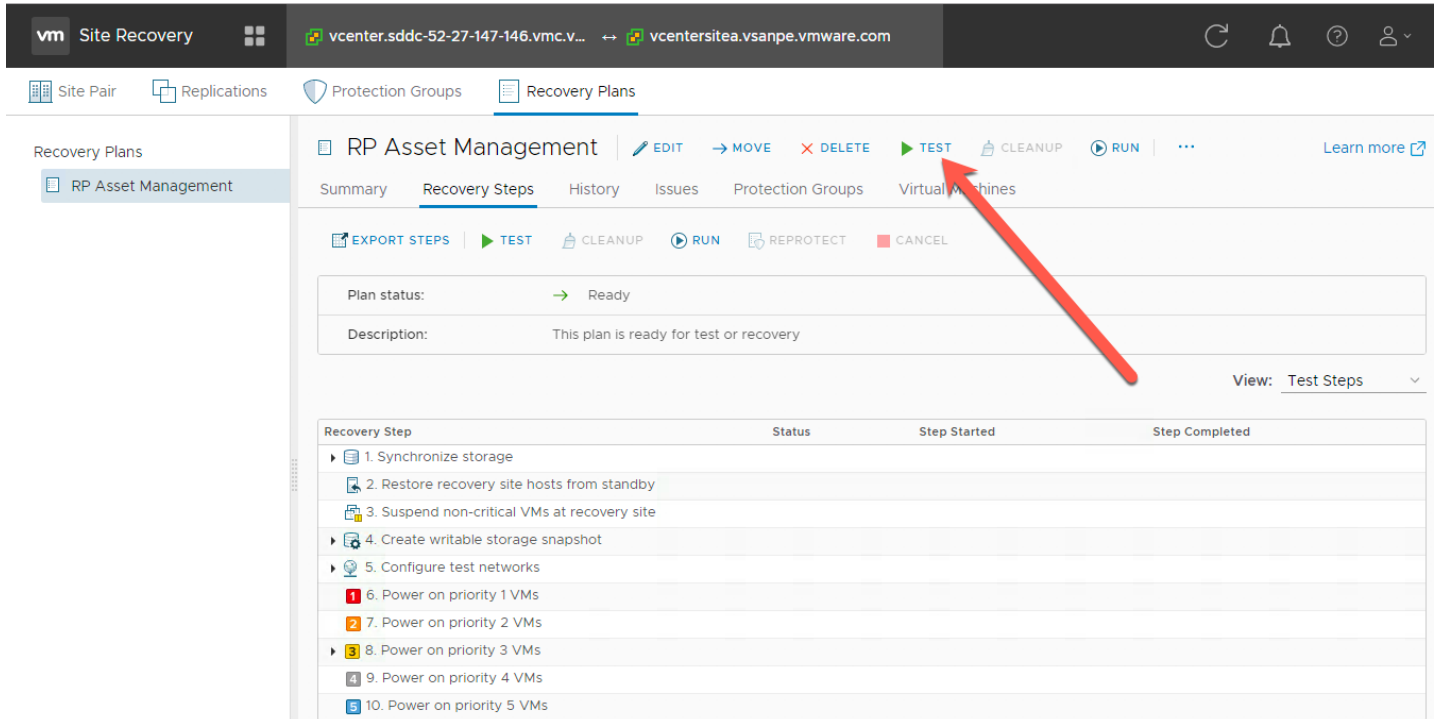
DNS suffixes:

rainpole.com

Workflows

Testing and Cleanup

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.



The screenshot shows the VMware Site Recovery console interface. The top navigation bar includes 'Site Pair', 'Replications', 'Protection Groups', and 'Recovery Plans'. The 'Recovery Plans' section is active, showing 'RP Asset Management'. A red arrow points to the 'TEST' button in the top navigation bar. Below the navigation bar, the 'RP Asset Management' page is displayed, showing a 'Summary' tab and a 'Recovery Steps' tab. The 'Recovery Steps' tab is selected, showing a list of steps: 1. Synchronize storage, 2. Restore recovery site hosts from standby, 3. Suspend non-critical VMs at recovery site, 4. Create writable storage snapshot, 5. Configure test networks, 6. Power on priority 1 VMs, 7. Power on priority 2 VMs, 8. Power on priority 3 VMs, 9. Power on priority 4 VMs, and 10. Power on priority 5 VMs. The 'TEST' button is highlighted in the top navigation bar.

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. This is useful for testing a disaster avoidance scenario. Unchecking the option to replicate recent changes provides a more realistic disaster recovery test.

A question often asked is whether replication continues during the test of a recovery plan. The answer is yes. vSphere Replication utilizes virtual machine snapshots at the recovery site 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 RPO violations.

To keep test networks isolated VMware Site Recovery supports two different options. One, automatically created networks on each host. This has the advantage of not requiring any additional networking configuration. However, because this option limits VM connectivity it is best used for testing the function of the recovery plan, not for testing application functionality.

The second network testing option is manually created test network(s) that are configured to duplicate production networks at the recovery site without a connection to the production portion of the network. This is easily possible at the VMware Cloud on AWS site through the tight integration with VMware NSX. See the administration and configuration guide for details about configuring this. This option requires additional configuration upfront and provides the ability to fully test the functionality of both the recovery plan and the application.

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.

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.

vm Site Recovery

vcentersitea.vsan... ↔ vcenter.sddc-52-2...

Site Pair

Replications

Protection Groups

Recovery Plans

Recovery Plans

RP Asset Management

RP_ERP

RP_Payroll

RP_ERP

EDIT MOVE DELETE TEST CLEANUP RUN

Summary Recovery Steps History Issues Protection Groups Virtual Machines

EXPORT STEPS TEST CLEANUP RUN REPROTECT CANCEL

Plan status: Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.

View: Test Steps

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	Skipped		
2. Restore recovery site hosts from stand...	Success	Tuesday, November 28, ...	Tuesday, November 28, ...
3. Suspend non-critical VMs at recovery s...			
4. Create writable storage snapshot	Success	Tuesday, November 28, ...	Tuesday, November 28, ...
5. Configure test networks	Success	Tuesday, November 28, ...	Tuesday, November 28, ...
6. Power on priority 1 VMs	Success	Tuesday, November 28, ...	Tuesday, November 28, ...
7. Prompt: Verify Database Servers Are R...	Success	Tuesday, November 28, ...	Tuesday, November 28, ...
8. Power on priority 2 VMs	Success	Tuesday, November 28, ...	Tuesday, November 28, ...
9. Power on priority 3 VMs	Success	Tuesday, November 28, ...	Tuesday, November 28, ...
10. Power on priority 4 VMs	Success	Tuesday, November 28, ...	Tuesday, November 28, ...
11. Power on priority 5 VMs	Success	Tuesday, November 28, ...	Tuesday, November 28, ...

Planned Migration and Disaster Recovery

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.

Recovery - RP Asset Management

1 Confirmation options

2 Ready to complete

Confirmation options

Recovery confirmation



Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site: vcentersitea.vsanpe.vmware.com
Recovery site: vcenter.sddc-52-27-147-146.vmc.vmware.com
Server connection: Connected
Number of VMs: 6

☐ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

☒ Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

☐ Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

A planned migration will be canceled 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. The default selection is a planned migration.

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 the virtual machine 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.

RP Asset Management

[EDIT](#)
[MOVE](#)
[DELETE](#)
[TEST](#)
[CLEANUP](#)
[RUN](#)

Learn more

[Summary](#)
[Recovery Steps](#)
[History](#)
[Issues](#)
[Protection Groups](#)
[Virtual Machines](#)

[EXPORT STEPS](#)
[TEST](#)
[CLEANUP](#)
[RUN](#)
[REPROTECT](#)
[CANCEL](#)

Plan status: → Ready

Description: This plan is ready for test or recovery

View: Recovery Steps

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize storage			
2. Shut down VMs at protected site			
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby			
5. Restore protected site hosts from standby			
6. Prepare protected site VMs for migration			
7. Synchronize storage			
8. Suspend non-critical VMs at recovery site			
9. Change recovery site storage to writable			
10. Power on priority 1 VMs			
11. Power on priority 2 VMs			
12. Power on priority 3 VMs			
13. Power on priority 4 VMs			
14. Power on priority 5 VMs			

If the protected/customer 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.

Re-Protect and Failback

VMware Site Recovery features the ability to not only failover 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.

RP Asset Management | [EDIT](#) | [MOVE](#) | [DELETE](#) | [TEST](#) | [CLEANUP](#) | [RUN](#) | [Learn more](#)

Summary | **Recovery Steps** | History | Issues | Protection Groups | Virtual Machines

[EXPORT STEPS](#) | [TEST](#) | [CLEANUP](#) | [RUN](#) | [REPROTECT](#) | [CANCEL](#)

Plan status: ✔ Recovery complete

Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

View: Recovery Steps ▾

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize storage	✔ Success	Wednesday, November 22, 2017 8:...	Wednesday, November 22, 2017 8:...
2. Shut down VMs at protected site	✔ Success	Wednesday, November 22, 2017 8:...	Wednesday, November 22, 2017 8:...
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby	✔ Success	Wednesday, November 22, 2017 8:...	Wednesday, November 22, 2017 8:...
5. Restore protected site hosts from standby			
6. Prepare protected site VMs for migration	✔ Success	Wednesday, November 22, 2017 8:...	Wednesday, November 22, 2017 8:...
7. Synchronize storage	✔ Success	Wednesday, November 22, 2017 8:...	Wednesday, November 22, 2017 8:...
8. Suspend non-critical VMs at recovery site			
9. Change recovery site storage to writable	✔ Success	Wednesday, November 22, 2017 8:...	Wednesday, November 22, 2017 8:...
10. Power on priority 1 VMs			
11. Power on priority 2 VMs			

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

History Reports

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. Click [here](#) for a sample history report.

Next Steps

Additional Resources

For more information about vSphere Site Recovery for VMware Cloud on AWS, please visit the [product pages](#). Below are links to documentation and other resources:

[Product Documentation](#) (includes Install Guide, Administration Guide, and more)

Terminology

Recovery time objective (RTO): The targeted amount of time a business process should be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity.

Recovery point objective (RPO): The maximum age of files recovered from backup storage for normal operations to resume if a system goes offline as a result of a hardware, program, or communications failure.

Protected site: Site that contains protected virtual machines. This can be either the customer's datacenter or VMware Cloud on AWS.

Recovery site: Site where protected virtual machines are recovered in the event of a failover. This can be either the customer's datacenter or VMware Cloud on AWS.

Note: It is possible for the same site to serve as a protected site and recovery site when replication is occurring in both directions and VMware Site Recovery is protecting virtual machines at both sites.

Providing Feedback

VMware appreciates your feedback on the material included in this guide and in particular, would be grateful for any guidance on the following topics:

How useful was the information in this guide? What other specific topics would you like to see covered?

Please send your feedback to docfeedback@vmware.com, with "VMware Site Recovery Technical Overview" in the subject line. Thank you for your help in making this guide a valuable resource.

About the Author

Cato Grace is a Senior Technical Marketing Architect at VMware. He works on business continuity and disaster recovery solutions in the Storage and Availability Business Unit. Cato started as a VMware customer in 2005 and has also worked as a VMware partner. He has worked in Technical Marketing at VMware since 2013.

Cato regularly blogs [here](#)

[Follow Cato on Twitter](#)

Sample Workflow Report

Recovery Plan History Report

VMware Site Recovery Manager 8.0

Plan Summary	
Name:	RP Asset Management
Description:	
Protected Site:	vcenter.sddc-52-27-147-146.vmc.vmware.com
Recovery Site:	vcentersitea.vsanpe.vmware.com

Run Summary	
Operation:	Recovery
Recovery Type:	Planned migration
Started By:	VSPHERE.LOCAL\\Administrator
Start Time:	2017-11-27 22:49:03 (UTC 0)
End Time:	2017-11-27 22:51:43 (UTC 0)
Elapsed Time:	00:02:40
Result:	Success
Errors:	0
Warnings:	0

Recovery Step	Result	Step Started	Step Completed	Execution Time
1. Pre-synchronize storage	Success	2017-11-27 22:49:22 (UTC 0)	2017-11-27 22:49:22 (UTC 0)	00:00:00
1.1. Protection Group PG Asset Management	Success	2017-11-27 22:49:22 (UTC 0)	2017-11-27 22:49:22 (UTC 0)	00:00:00
2. Shut down VMs at protected site	Success	2017-11-27 22:49:22 (UTC 0)	2017-11-27 22:49:37 (UTC 0)	00:00:15
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	2017-11-27 22:49:22 (UTC 0)	2017-11-27 22:49:37 (UTC 0)	00:00:15
2.3.1. AssetMgt20	Success	2017-11-27 22:49:22 (UTC 0)	2017-11-27 22:49:26 (UTC 0)	00:00:04
2.3.1.1. Power off	Success	2017-11-27 22:49:22 (UTC 0)	2017-11-27 22:49:26 (UTC 0)	00:00:04

