Site Recovery Manager Technical Overview

VMware BC/DR

© VMware LLC.

Table of contents

© VMware LLC.

Site Recovery Manager Technical Overview

Introduction

VMware Site Recovery Manager™ 8.4 is an extension to VMware vCenter™ that provides disaster recovery, site migration, and non-disruptive testing capabilities to VMware customers.

Overview

VMware Site Recovery Manager™ 8.4 is an extension to VMware vCenter™ that provides disaster recovery, site migration, and non-disruptive testing capabilities to VMware customers. It is fully integrated with VMware vCenter Server and utilizes an HTML5 based "Clarity" UI.

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

Site Recovery Manager servers coordinate the operations of the VMware vCenter Server™ at two sites. 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.

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. Site Recovery Manager 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 and entire sites providing finer control over what virtual machines are failed over and failed back. This also enables flexible testing schedules.

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

Features and Benefits of Site Recovery Manager

- 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
- Centralized management of recovery plans from the HTML5 UI replaces manual runbooks
- Planned migration workflow enables disaster avoidance and data center mobility
- VMware vSAN™ integration reduces the DR footprint through hyper-converged, software-defined storage
- Supports multiple versions of vCenter enabling flexible pairing and upgrading
- vSphere Replication integration delivers VM-centric, replication that eliminates dependence on storage
- Support for array-based replication including support for Virtual Volumes (vVols) offers choice and options for synchronous replication with zero data loss
- Self-service, policy-based provisioning via Storage Policy Based Protection Groups, VMware vRealize™ Orchestrator, and VMware vRealize Automation automates protection

Terminology

Recovery time objective (RTO): 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): 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.

Consistency group: One or more LUNs or volumes that are replicated at the same time. When recovering items in a consistency group, all items are restored to the same point in time.

Protected site: Site that contains protected virtual machines.

Recovery site: Site where protected virtual machines are recovered in the event of a failover.

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 Site Recovery Manager is protecting virtual machines at both sites.

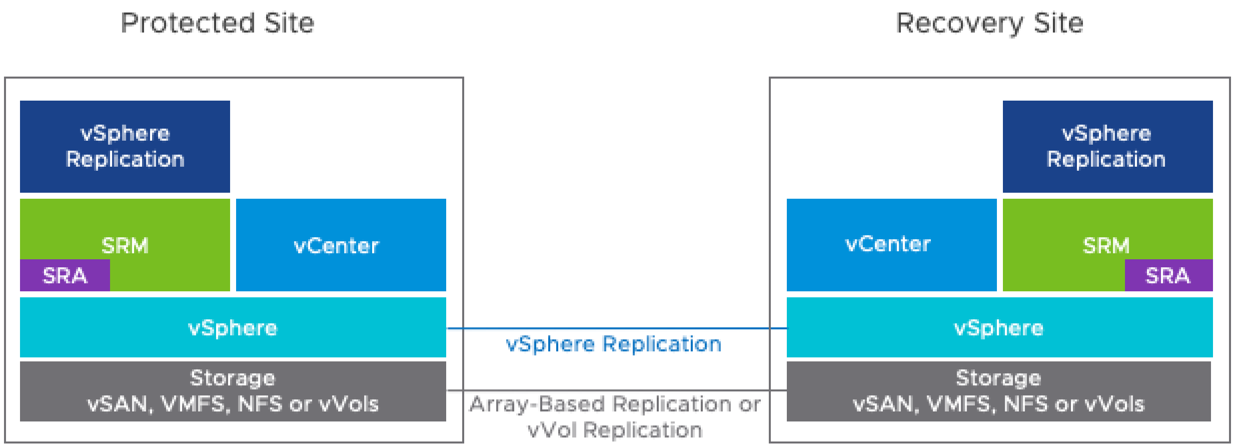
Datastore group: One or more datastores that are treated as a unit in Site Recovery Manager. A common example is a consistency group in an array replication solution.

Architectural Overview

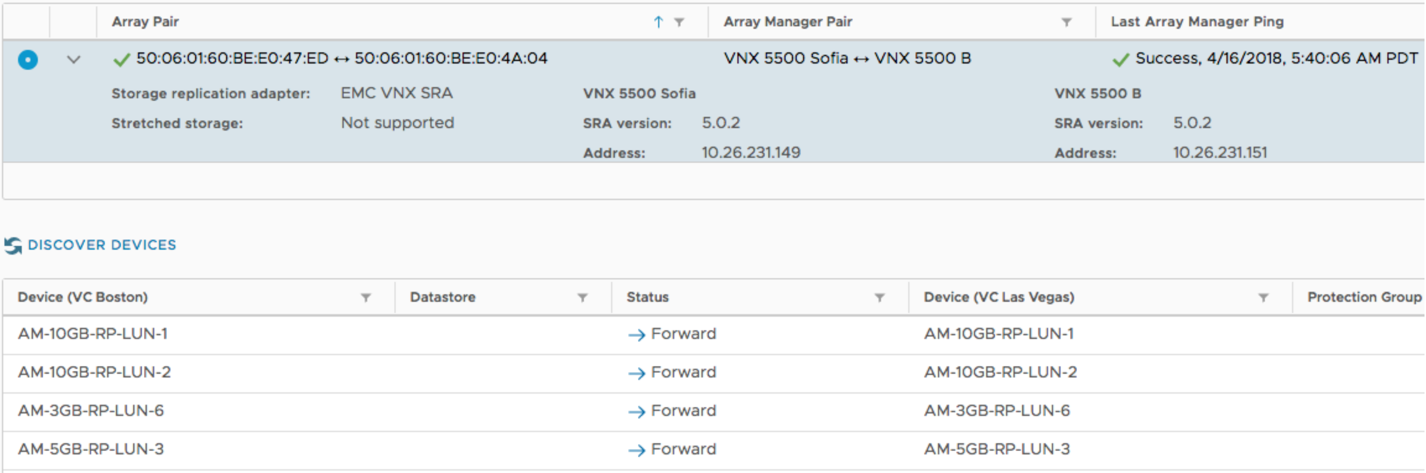
Site Recovery Manager 8.4 is deployed in a paired configuration, for example, protected site and recovery site.

Overview

Site Recovery Manager 8.4 is deployed in a paired configuration, for example, a protected site and a recovery site. The Site Recovery Manager 8.4 software is deployed as an appliance at both sites. It supports multiple versions of vCenter at either site. There must be one or more vSphere hosts running version 6.5 or higher at each site. See the Compatibility Matrixes for Site Recovery Manager 8.4 for specific details



Site Recovery Manager utilizes either vSphere Replication, array-based replication, Virtual Volume (vVols) replication, or stretched storage for transferring data between sites. Array-based replication and stretched storage must be licensed and configured and the appropriate storage replication adaptor must be installed on the Site Recovery Manager server at each site. Virtual Volume (vVols) replication must be licensed and configured as well, however, there is no requirement for a storage replication adaptor when using Virtual Volumes (vVols).



Array Pair	Array Manager Pair	Last Array Manager Ping
✓ 50:06:01:60:BE:E0:47:ED ↔ 50:06:01:60:BE:E0:4A:04	VNX 5500 Sofia ↔ VNX 5500 B	✓ Success, 4/16/2018, 5:40:06 AM PDT

Storage replication adapter: EMC VNX SRA
Stretched storage: Not supported

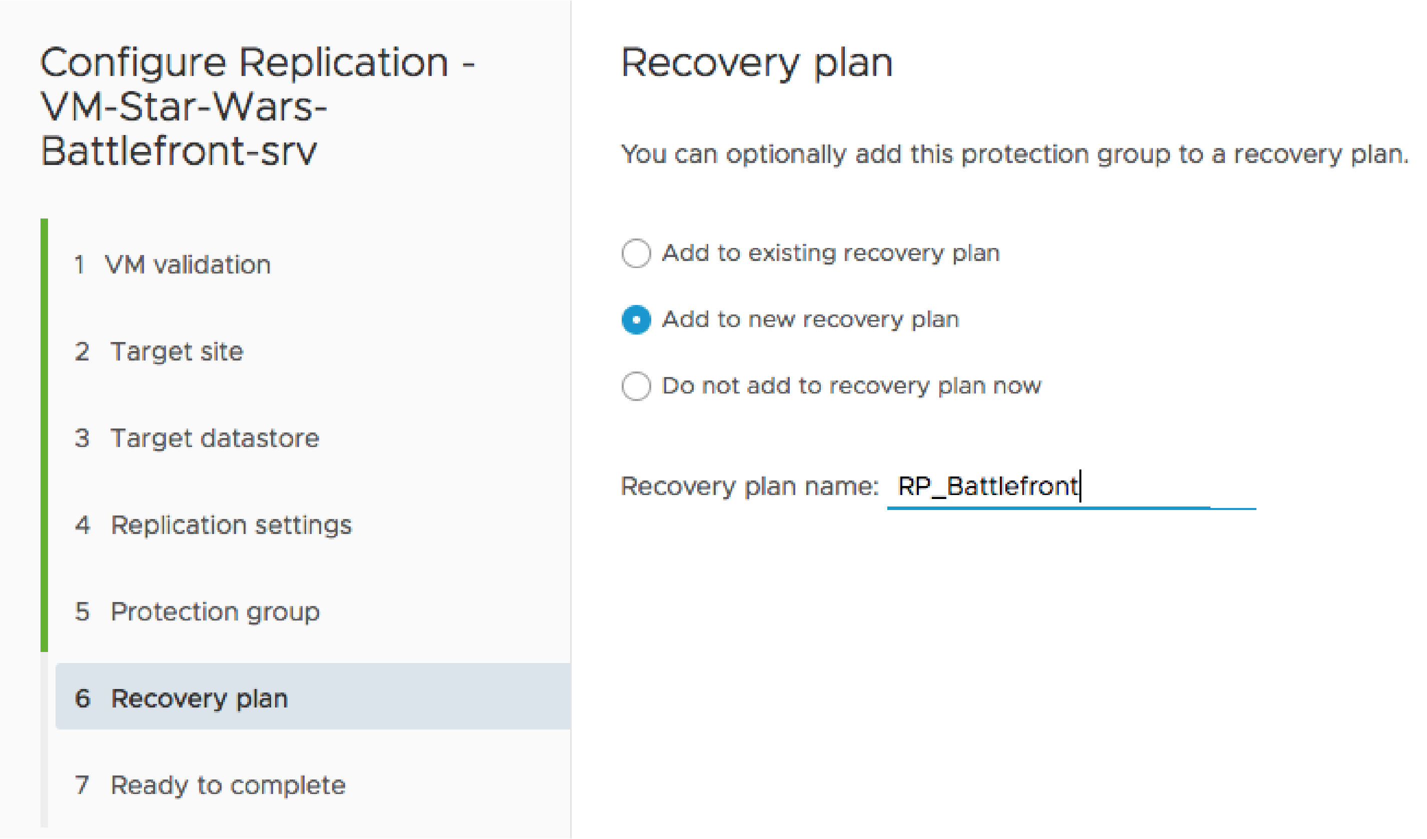
VNX 5500 Sofia
SRA version: 5.0.2
Address: 10.26.231.149

VNX 5500 B
SRA version: 5.0.2
Address: 10.26.231.151

DISCOVER DEVICES

Device (VC Boston)	Datastore	Status	Device (VC Las Vegas)	Protection Group
AM-10GB-RP-LUN-1		→ Forward	AM-10GB-RP-LUN-1	
AM-10GB-RP-LUN-2		→ Forward	AM-10GB-RP-LUN-2	
AM-3GB-RP-LUN-6		→ Forward	AM-3GB-RP-LUN-6	
AM-5GB-RP-LUN-3		→ Forward	AM-5GB-RP-LUN-3	

For vSphere Replication, the vSphere Replication virtual appliance must be deployed and the virtual machines to be protected by Site Recovery Manager must be configured for replication.



Configure Replication - VM-Star-Wars-Battlefront-srv

1 VM validation

2 Target site

3 Target datastore

4 Replication settings

5 Protection group

6 Recovery plan

7 Ready to complete

Recovery plan

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

○ Add to existing recovery plan

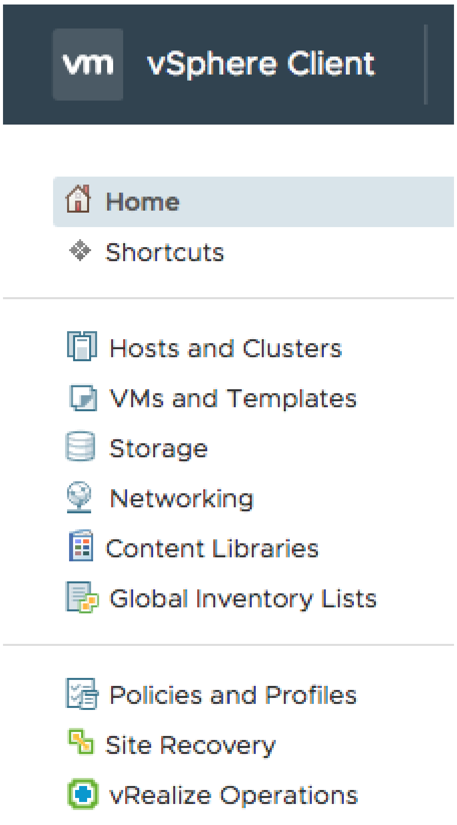
● Add to new recovery plan

○ Do not add to recovery plan now

Recovery plan name: RP_Battlefront

Site Recovery Manager 8.4 and VMware vCenter Server as well as the workloads they are protecting require infrastructure services like DNS, DHCP, and Active Directory. These must be in place at both the protected and recovery sites.

Site Recovery Manager is managed using an HTML5 based UI. During the installation of Site Recovery Manager, a plugin labeled “Site Recovery Manager” is installed in the vSphere HTML5 UI or Web Client and an icon labeled “Site Recovery” is displayed.



Site Recovery Manager supports protection for up to 5,000 virtual machines and is able to simultaneously run up to 10 recovery plans containing up to 2,000 virtual machines. Up to 500 virtual machines can be included in a single protection group and Site Recovery Manager provides support for up to 500 protection groups.

Use Cases

Though the most obvious use case for Site Recovery Manager is disaster recovery from one site to another it can handle a number of different use cases

Overview

Though the most obvious use case for Site Recovery Manager 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 Site Recovery Manager 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 Site Recovery Manager was specifically designed to accomplish. This is the most critical but least frequently used use case for Site Recovery Manager. Unexpected site failures don’t happen often but when they do fast recovery is critical to business. Site Recovery Manager 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 Site Recovery Manager. This can be anything from an oncoming storm to the threat of power issues. When utilized with a supported stretched storage solution, Site Recovery Manager can orchestrate the cross-vCenter vMotion of virtual machines allowing for zero-downtime disaster avoidance.

Without stretched storage, Site Recovery Manager 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.

Planned Migration

The most common way Site Recovery Manager is used on a regular basis is for movement of virtual machines and applications between sites. This can be for datacenter relocation, global load balancing or planned site maintenance.

Site Recovery Manager has all the capabilities to ensure a smooth site migration. It supports full testing of the migration in a manner completely non-disruptive to production systems. It also supports using stretched storage for zero-downtime migrations. Additionally, in planned migration mode it will pause if any issues are discovered during the migration, providing an opportunity to correct them.

Upgrade and Patch Testing

The Site Recovery Manager 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.

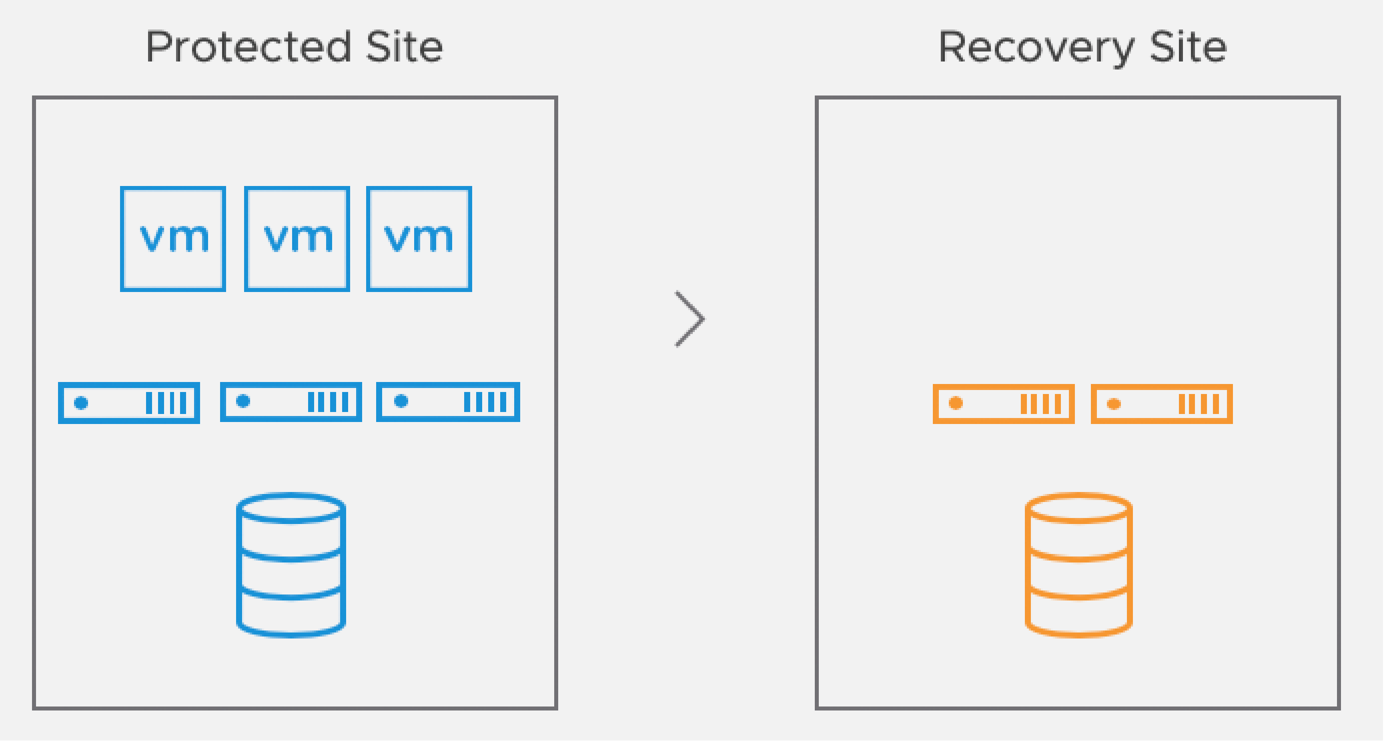
Topologies

Site Recovery Manager can be used in a number of different failover scenarios depending on customer requirements, constraints and objectives.

Overview

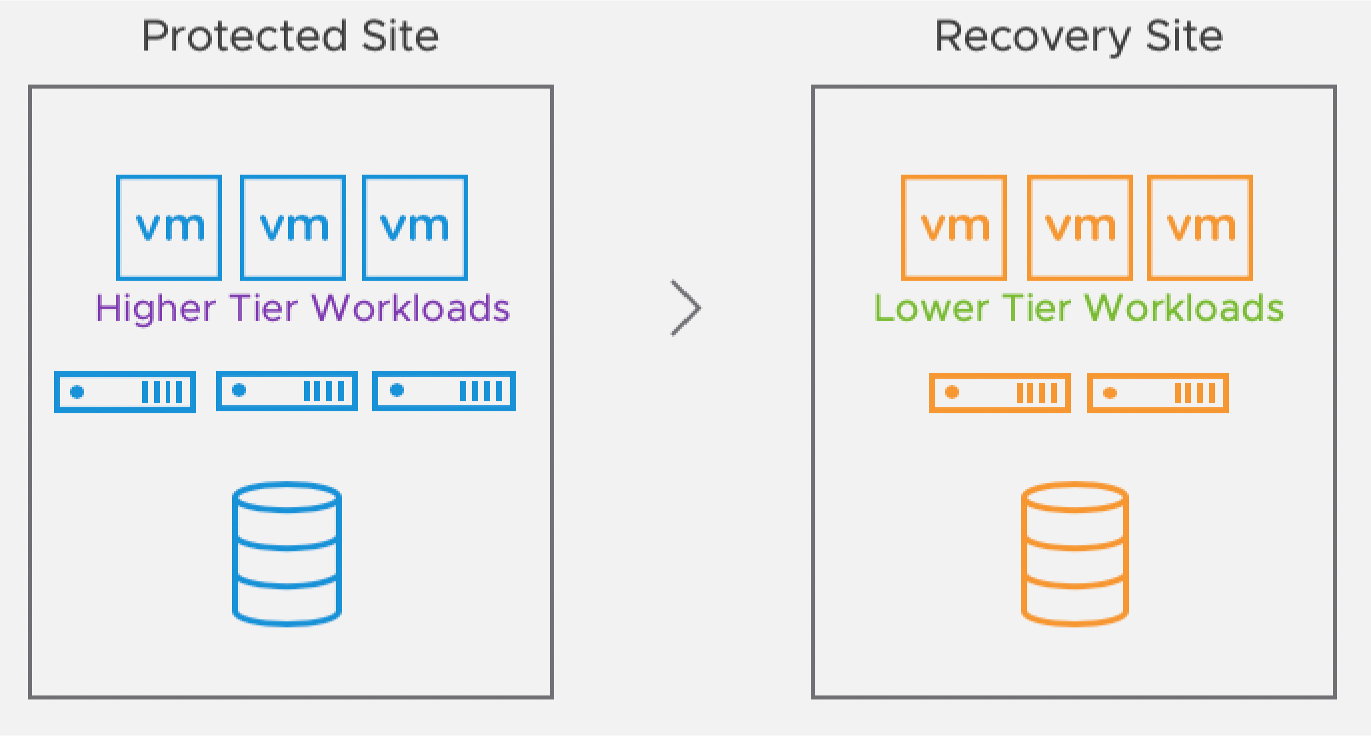
Site Recovery Manager can be used in a number of different failover scenarios depending on customer requirements, constraints and objectives. All of these arrangements are supported and easily configured. Additionally, Site Recovery Manager's integration with the vSphere Client makes multiple site topologies easy to manage.

Active-Passive



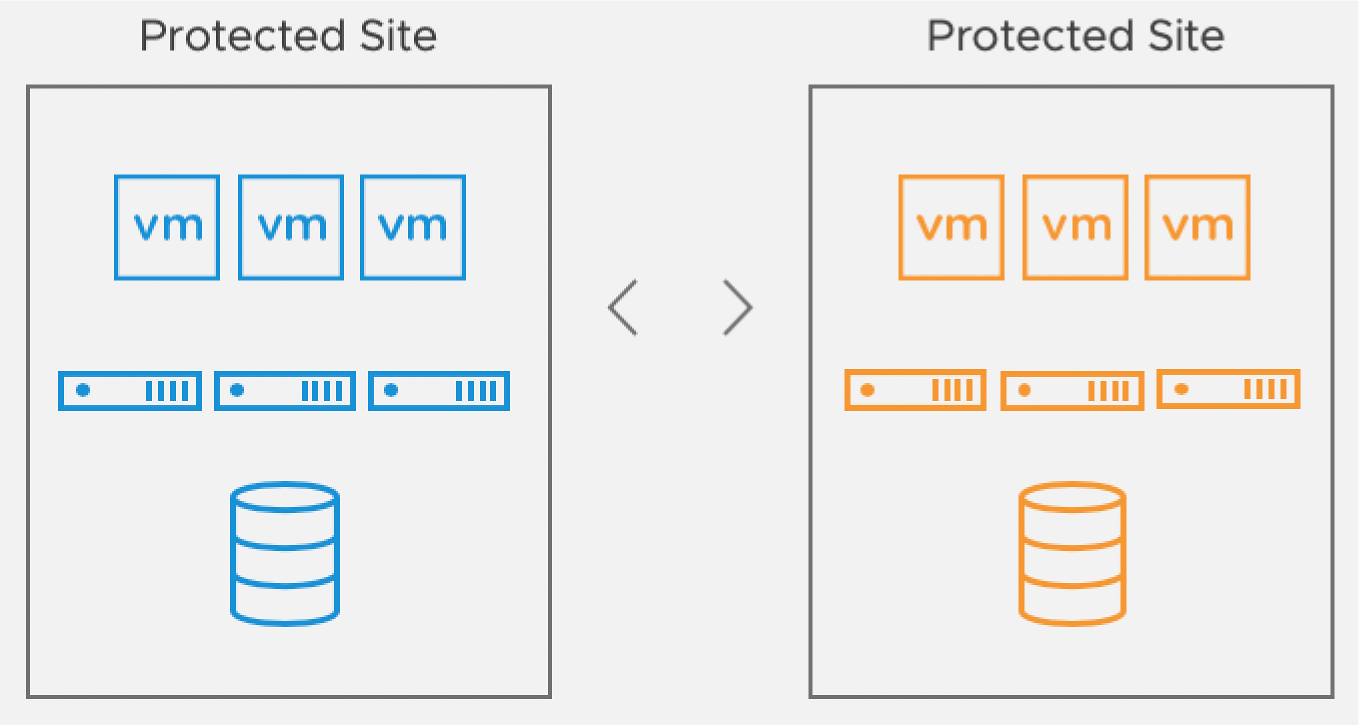
In the traditional active-passive scenario there is a production site running applications and services and a secondary or recovery site that is idle until needed for recovery. This topology is common and though it provides dedicated recovery resources it means paying for a site, servers and storage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

Active-Active



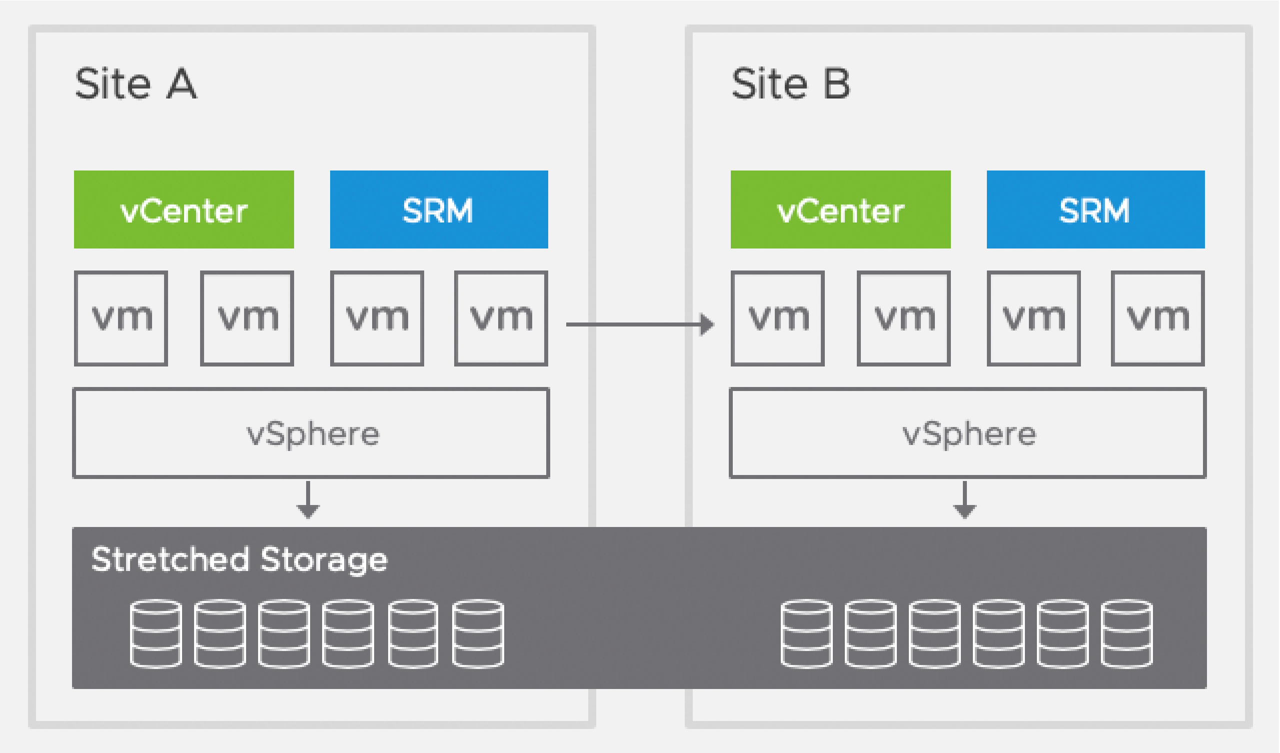
Site Recovery Manager can be used in a configuration where low-priority workloads such as test and development run at the recovery site and are powered off as part of the recovery plan. This allows for the utilization of recovery site resources as well as sufficient capacity for critical systems in case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

Bi-Directional



In situations where production applications are operating at both sites Site Recovery Manager 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).

Stretched Storage



Site Recovery Manager supports using stretched storage, thereby combining the benefits of Site Recovery Manager with the advantages of stretched storage. This allows Site Recovery Manager customers to achieve what was previously only possible with vSphere Metro Storage Clusters, namely:

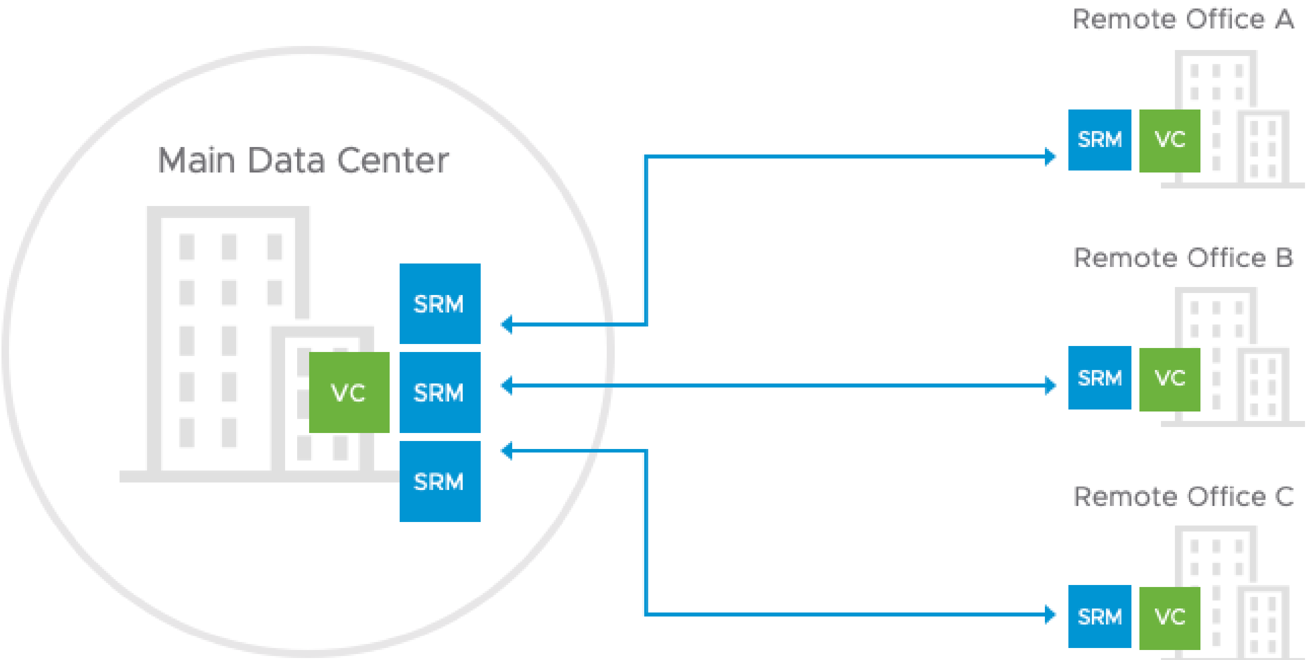
- Zero-downtime disaster avoidance
- Planned maintenance downtime

As well as all of the pre-existing benefits of Site Recovery Manager, most of which are not available when using stretched storage by itself.

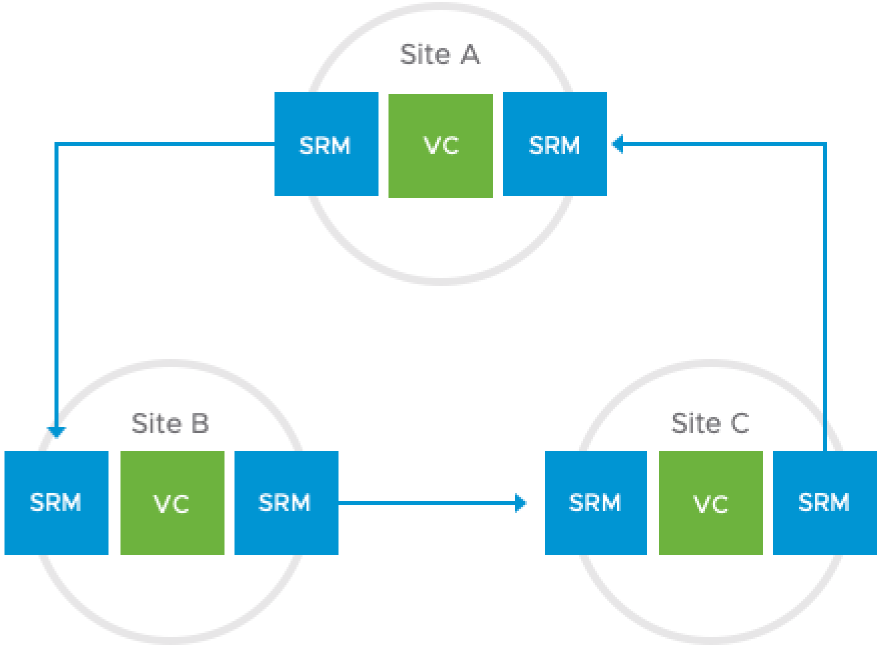
To fully utilize stretched storage and the vMotion of protected virtual machines, stretched layer two network connectivity between sites must be in place as it isn't possible to non-disruptively change the IP address of a running virtual machine. VMware NSX is an excellent solution to this and provides a host of additional benefits as well.

Multi-Site

While Site Recovery Manager is designed for the most common protection use case, one site protected by another, it is also capable of supporting additional configurations. These can be:



- Shared Recovery: where multiple remote sites are protected by a single recovery site.
- Shared Protection: where a single site fails over some applications/virtual machines to one remote site and others to one or more additional remote sites.



- Other topologies such as a three-site configuration where site A’s workloads are protected at site B, site B’s are protected at site C and site C’s are protected at site A.

Any of these and other multi-site topologies are supported provided these limits are taken into account:

- Each virtual machine is only protected by a single Site Recovery Manager pair.
- Site Recovery Manager doesn’t currently support the failover of the same virtual machine to different or multiple recovery sites.

More details about Site Recovery Manager topologies and configurations are available in the documentation center.

© VMware LLC.

Deployment and Configuration

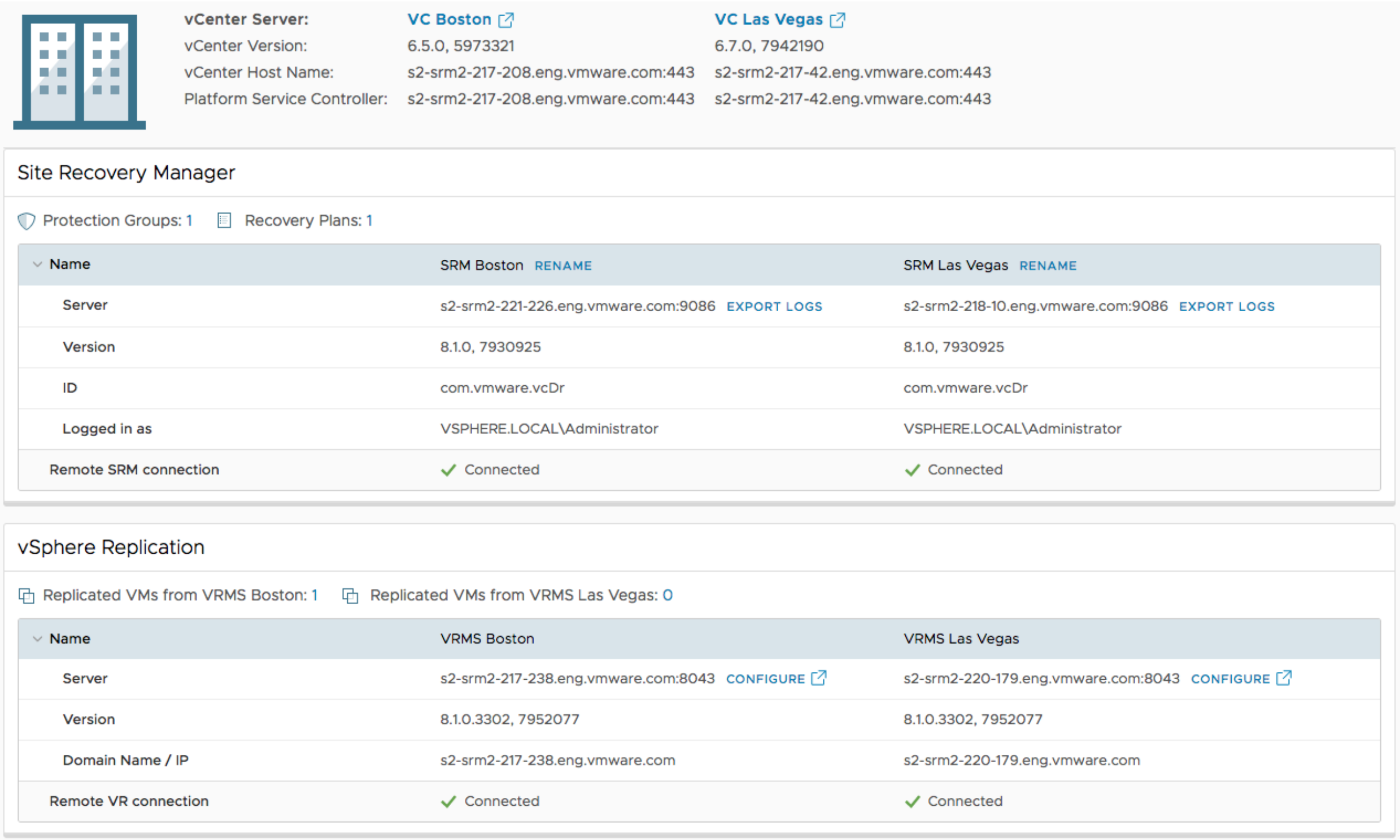
The process of deploying and configuring Site Recovery Manager is simple and logical.

Overview

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

Site Pairing

Site pairing is the first step in configuring Site Recovery Manager. The most common configuration is pairing two sites, though as was outlined in the previous section on topologies, other arrangements are supported.



vCenter Server:	VC Boston	VC Las Vegas
vCenter Version:	6.5.0, 5973321	6.7.0, 7942190
vCenter Host Name:	s2-srm2-217-208.eng.vmware.com:443	s2-srm2-217-42.eng.vmware.com:443
Platform Service Controller:	s2-srm2-217-208.eng.vmware.com:443	s2-srm2-217-42.eng.vmware.com:443

Site Recovery Manager

Protection Groups: 1 Recovery Plans: 1

Name	SRM Boston RENAME	SRM Las Vegas RENAME
Server	s2-srm2-221-226.eng.vmware.com:9086 EXPORT LOGS	s2-srm2-218-10.eng.vmware.com:9086 EXPORT LOGS
Version	8.1.0, 7930925	8.1.0, 7930925
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
Remote SRM connection	✓ Connected	✓ Connected

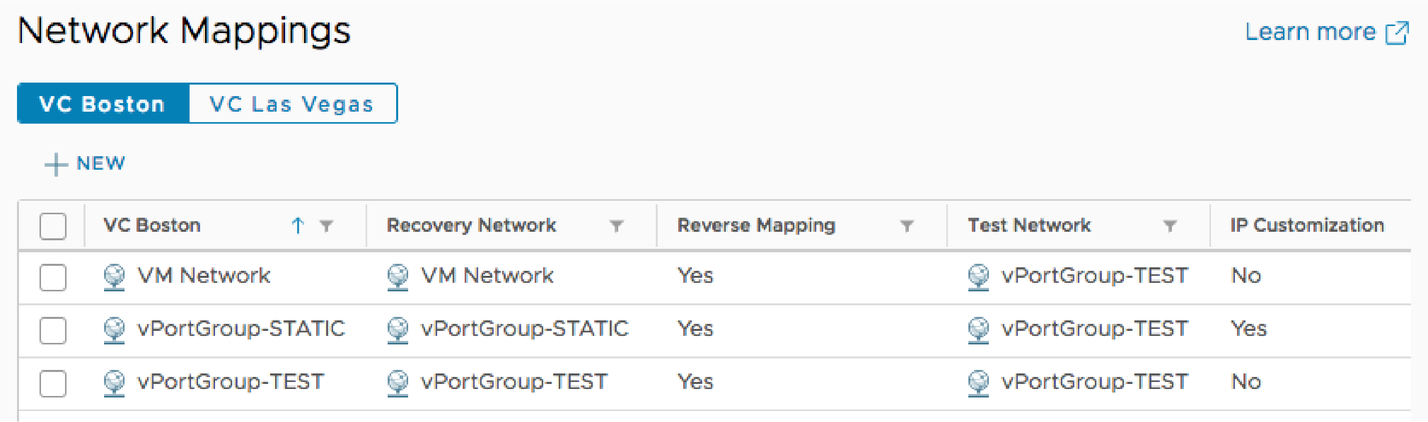
vSphere Replication

Replicated VMs from VRMS Boston: 1 Replicated VMs from VRMS Las Vegas: 0

Name	VRMS Boston	VRMS Las Vegas
Server	s2-srm2-217-238.eng.vmware.com:8043 CONFIGURE	s2-srm2-220-179.eng.vmware.com:8043 CONFIGURE
Version	8.1.0.3302, 7952077	8.1.0.3302, 7952077
Domain Name / IP	s2-srm2-217-238.eng.vmware.com	s2-srm2-220-179.eng.vmware.com
Remote VR connection	✓ Connected	✓ Connected

Inventory Mappings

There are multiple types of inventory mappings in Site Recovery Manager: 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 “Production-100” at the protected site and a network port group named “Production-200” at the recovery site. As a result of this mapping, virtual machines connected to “Production-100” at the protected site will, by default, automatically be connected to “Production-200” at the recovery site. Networks to be used during testing can also be configured in the same area.



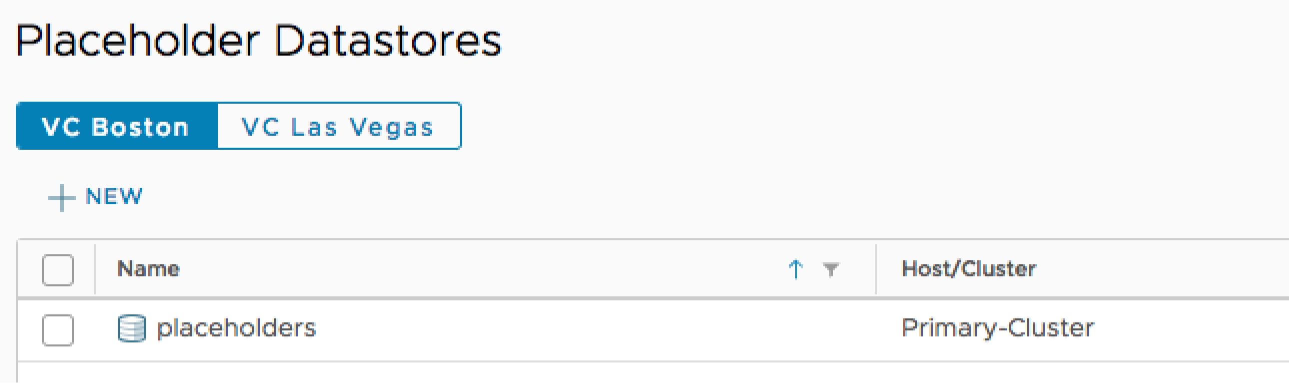
Network Mappings

□	VC Boston	Recovery Network	Reverse Mapping	Test Network	IP Customization
□	VM Network	VM Network	Yes	vPortGroup-TEST	No
□	vPortGroup-STATIC	vPortGroup-STATIC	Yes	vPortGroup-TEST	Yes
□	vPortGroup-TEST	vPortGroup-TEST	Yes	vPortGroup-TEST	No

Placeholder Virtual Machines and Datastores

For each protected virtual machine Site Recovery Manager creates a placeholder virtual machine at the recovery site. Placeholder virtual machines are contained in a datastore and registered with the vCenter Server at the recovery site. This datastore is called the “placeholder datastore”. Since placeholder virtual machines do not have virtual disks they consume a minimal amount of storage (1.25 MB/VM).

The protected and recovery sites will each require that a small datastore that is accessible by all hosts at that site be created or allocated for use as the placeholder datastore. Each site requires at least one placeholder datastore to allow for failover as well as failback. Site Recovery Manager will automatically select the placeholder datastore if it isn't chosen by the administrator.



Placeholder Datastores

□	Name	Host/Cluster
□	placeholders	Primary-Cluster

When utilizing Storage Policy-Based Protection Groups, placeholder datastores are not required and placeholder VMs are not created as they are not needed for this new type of protection group.

Replication Options

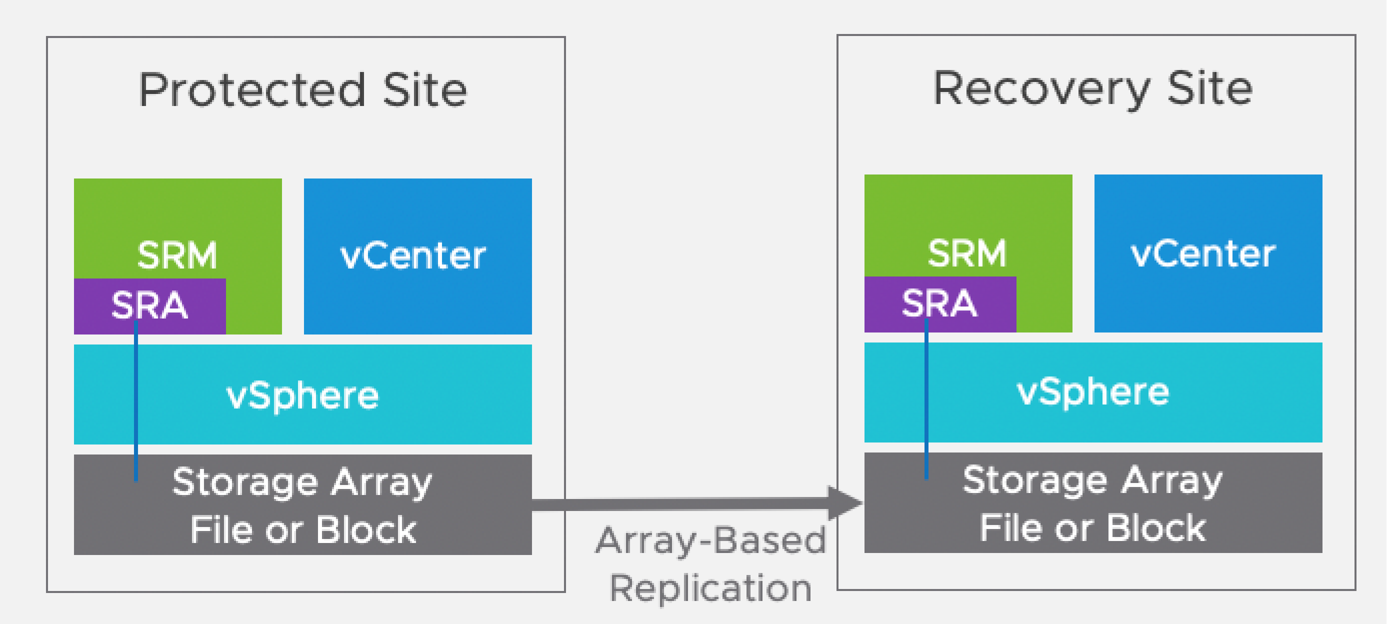
As mentioned previously, Site Recovery Manager offers a choice of replication technologies.

Overview

As mentioned previously, Site Recovery Manager offers a choice of replication technologies. Virtual machines can be replicated with vSphere Replication, array-based replication, or Virtual Volumes replication and the same virtual machine cannot be protected by more than one replication type. The virtual machine must be configured for replication before or as part of being protected by Site Recovery Manager. For a full comparison between array-based replication and vSphere replication see Site Recovery Manager – Array-Based Replication vs. vSphere Replication.

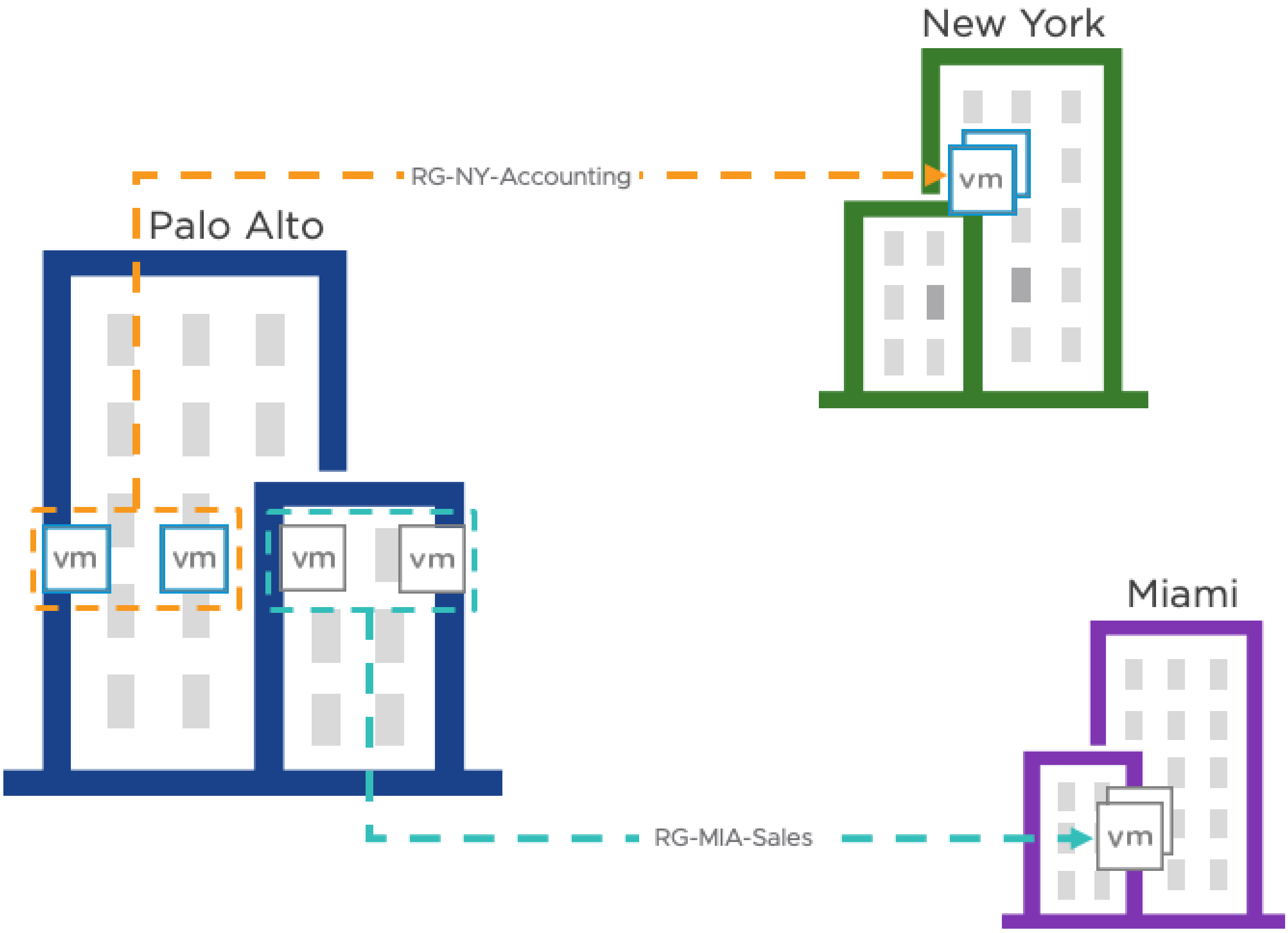
Array-Based and Virtual Volume Replication

When using array-based replication, one or more storage arrays at the protected site replicate data to peer array(s) at the recovery site. A storage replication adaptor (SRA) is required for the specific array and replication solution to be used with Site Recovery Manager. Storage replication adaptors are software components that are created and supported by the array replication vendors using guidelines from VMware. The storage replication adaptor is what Site Recovery Manager uses for communicating with the storage array. They are therefore installed on the Site Recovery Manager servers at both sites and are able to monitor and control array functions related to migrations, failovers, re-protections, failbacks, and tests.



When using Virtual Volumes (vVols) replication, the concept of Replication Groups is introduced. Replication Groups bringing more efficient, accurate, and responsive recovery of your virtual machines. A Replication Group is a group of replicated storage devices to provide atomic failover for an application. In other words, a Replication Group is the minimum unit of failover. Replication Groups are created and managed by a storage administrator using the storage vendor’s tools or created on the fly (if the array supports so-called "automatic" RG group selection).

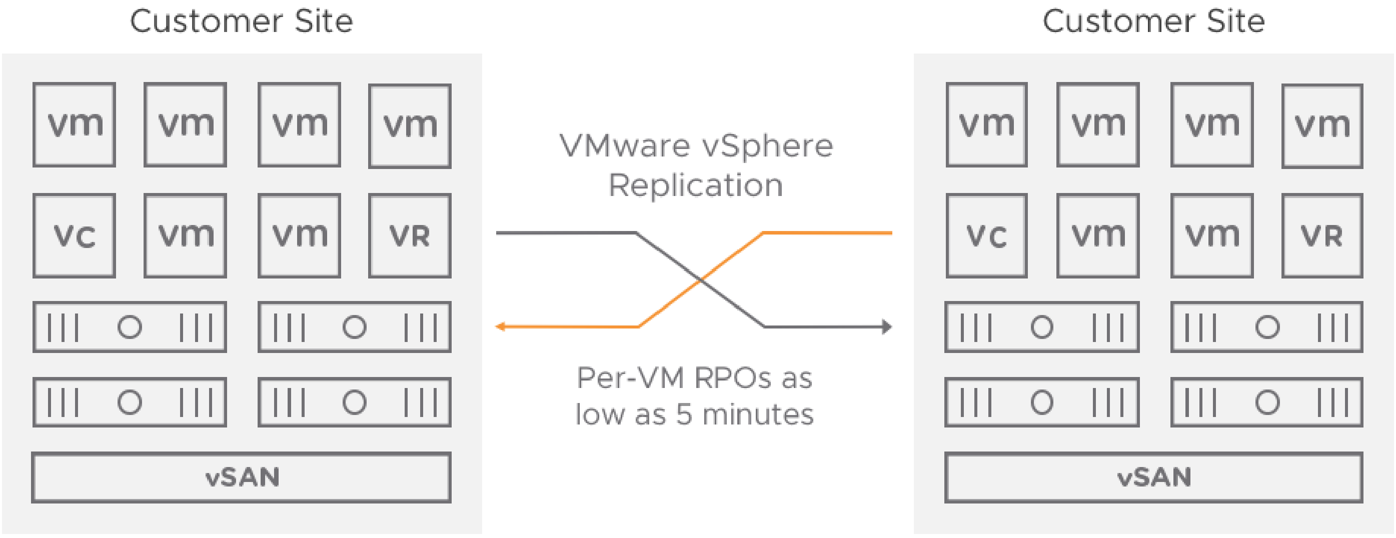
Replication Groups also define the set of vVols that are maintained in write-order fidelity where writes are replicated on the destination site in the exact same order they're generated at the source site to ensure at any time the destination site represents at least a crash-consistent version of the data on the source site.



vSphere Replication

To use vSphere replication requires deployment and configuration of the vSphere Replication appliance. This is done independently of Site Recovery Manager. 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.

For details about installing and configuring vSphere Replication see the vSphere Replication documentation.



© VMware LLC.

Protection Groups

Protection groups are a way of grouping virtual machines that will be recovered together.

Overview

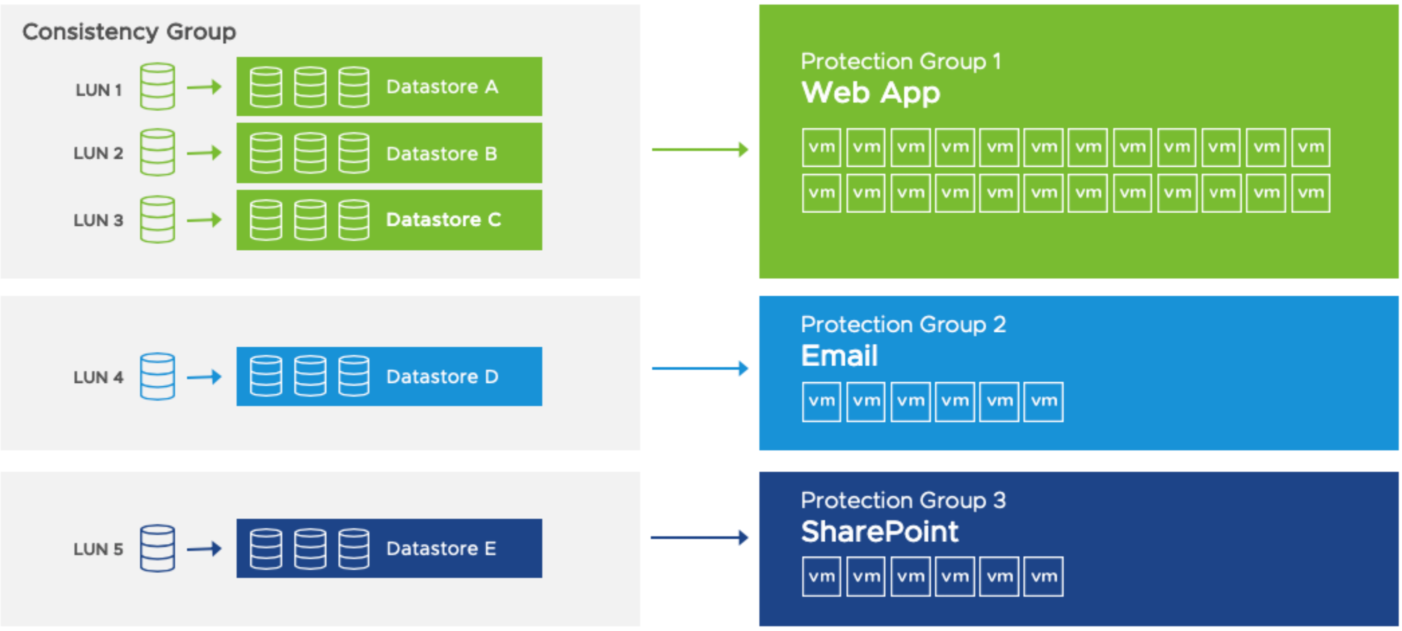
Protection groups are a way of grouping virtual machines that will be recovered together. In many cases, a protection group will consist of the virtual machines that support a service or application such as email or an accounting system. For example, an application might consist of a two-server database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

A protection group contains virtual machines whose data has been replicated by array-based replication, Virtual Volumes or vSphere replication. Before a protection group can be created, replication must be configured. A protection group cannot contain virtual machines replicated by more than one replication solution (e.g. same virtual machine protected by both vSphere replication and array-based replication) and, a virtual machine can only belong to a single protection group.

Array-Based Replication

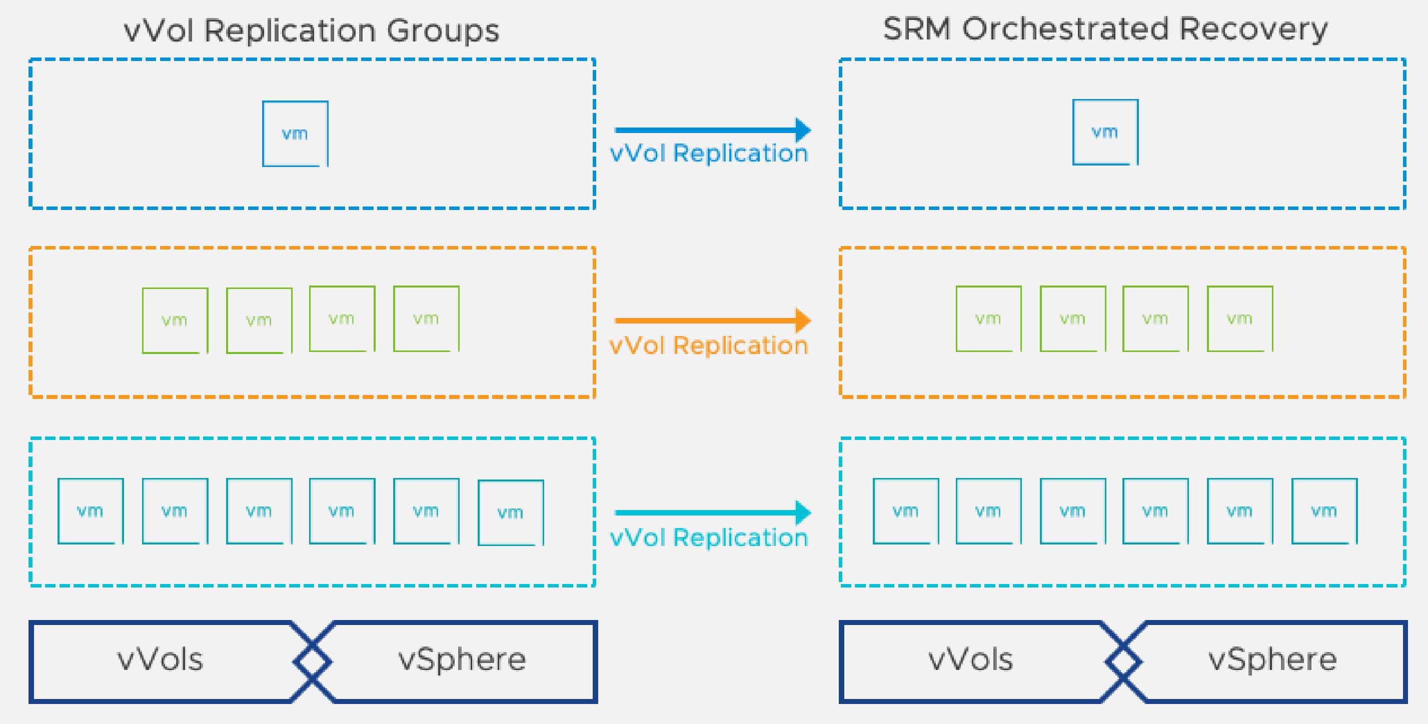
The virtual machines included in array-based replication protection groups are determined by the storage where the virtual machines are located. All the virtual machines on a datastore have to be protected by Site Recovery Manager and they all have to belong to the same protection group. It is not supported, advisable or recommended to protect a subset of virtual machines on a datastore. Doing this will trigger alarms within the Site Recovery Manager user interface and can result in significant issues with those unprotected virtual machines. In the example below, we have virtual machines located on multiple datastores that map to LUNs and consistency groups and protection groups.



Within the storage array, the multiple LUNs can be configured in a consistency group to ensure write order consistency. These datastores are said to be in a datastore group, which contains all the datastores associated with the virtual machines in the protection group.

Virtual Volumes

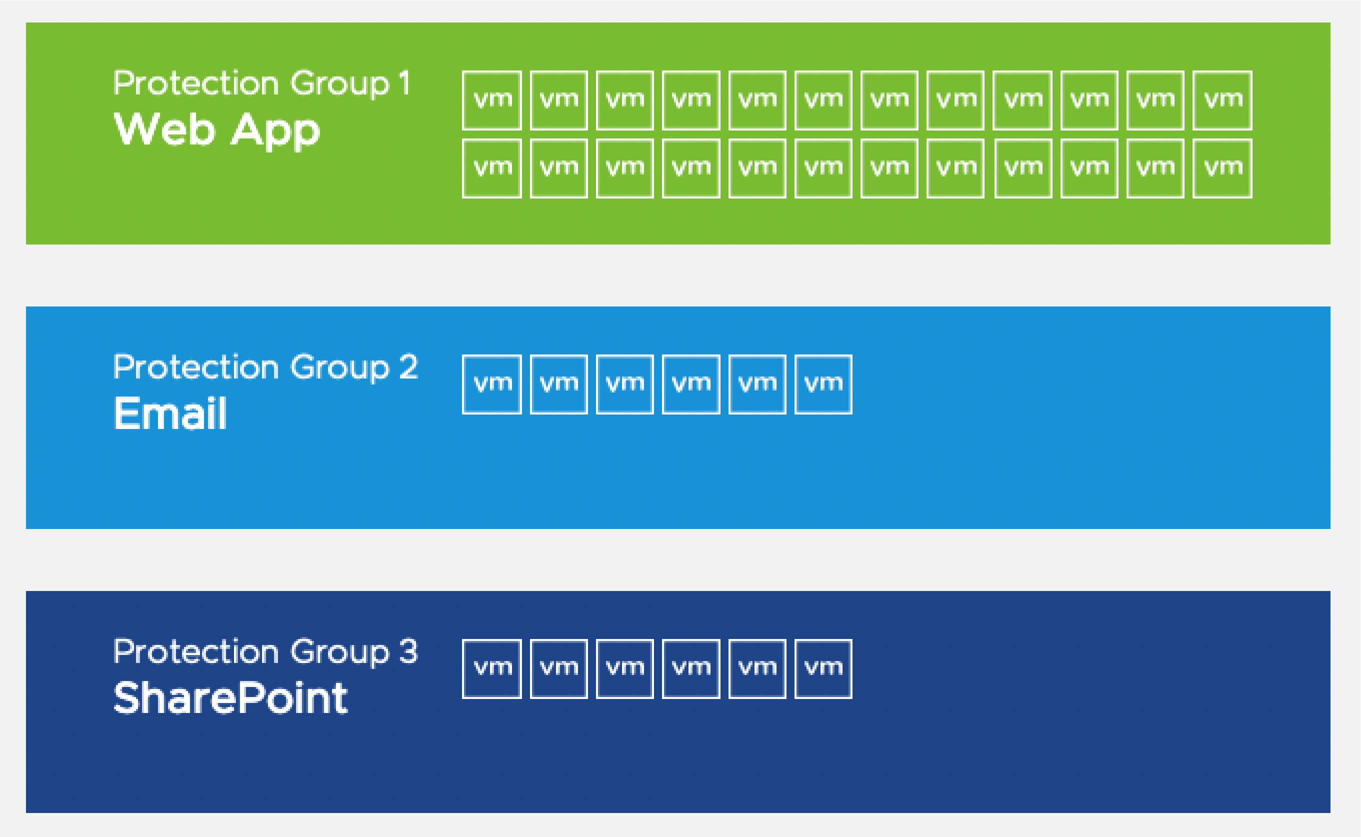
The integration of Site Recovery Manager with virtual volumes is built on top of the replication capability that was introduced in virtual volumes 2.0. This implementation introduced the concepts of replication groups and fault domains, which the Site Recovery Manager integration builds on. A fault domain roughly translates to a site or an array replication pair. A replication group, also known as a consistency group, is made up of one or more virtual machines that are replicated in a consistent state. A vVol protection group can consist of one or more replication groups. All of a replicated virtual machines disks must belong to the same replication group.



Virtual Machines are added to a virtual volume protection group by associating them with the storage policy that is configured for replication. This allows for the protection of virtual machines to be automated and policy-based.

vSphere Replication

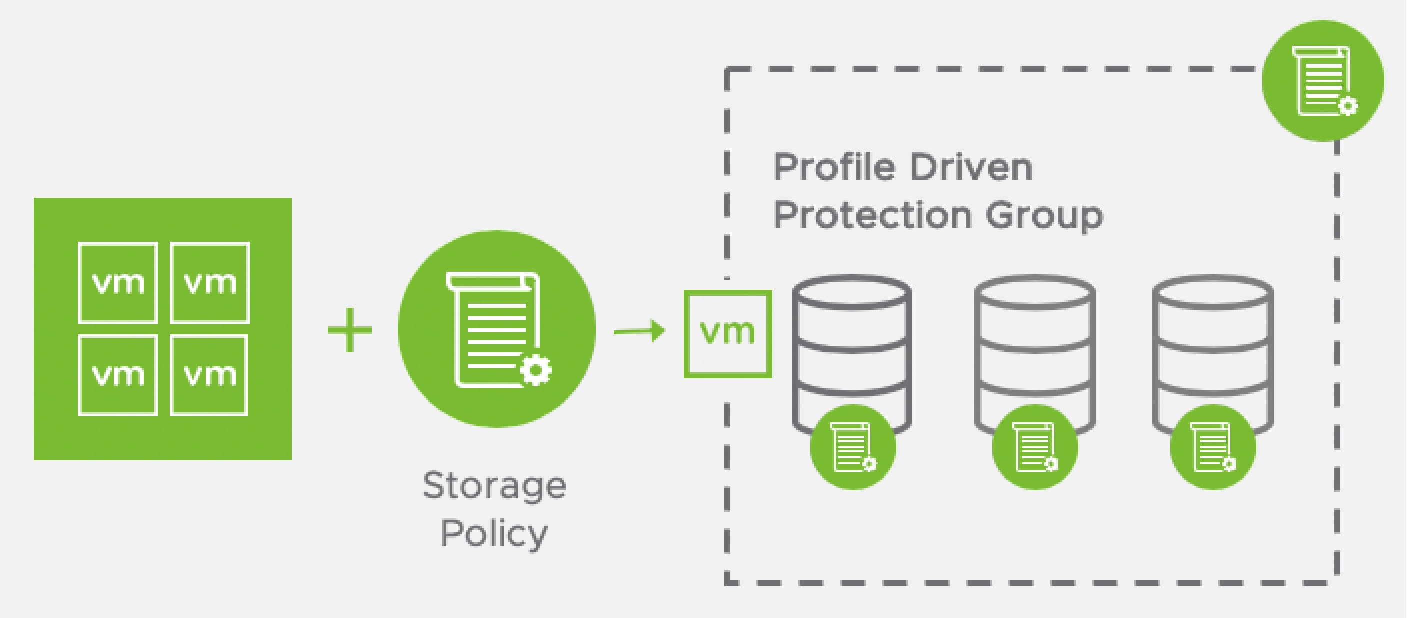
For virtual machines protected by Site Recovery Manager using vSphere replication deciding what virtual machines are going to belong to what protection group is simple since virtual machines are replicated on an individual basis, whatever makes sense from a recovery standpoint. vSphere replication protection groups are not tied to storage type or configuration other than they cannot be located on array-based replication replicated storage.



Storage Policy-Based

Storage policy-based protection groups use vSphere storage profiles to identify protected datastores and virtual machines. They automate the process of protecting and unprotecting virtual machines and adding and removing datastores from protection groups. Storage profile-based protection groups enable deep integration with virtual machine provisioning tools like VMware vRealize Automation. This combination makes it easier than ever to deploy and protect virtual machines.

Storage policy-based protection groups utilize vSphere tags in combination with vSphere storage policy-based management to enable automated policy-based protection for virtual machines. Storage policy-based management enables vSphere administrators to automate the provisioning and management of virtual machines storage to meet requirements like performance, availability, and protection. vSphere tags allow for the ability to attach metadata to vSphere inventory, in this case, datastores, which makes these objects more sortable, searchable and possible to associate with storage policies.



© VMware LLC.

Here is how tags and storage-policy based management are used together with storage policy-based protection groups:

- A tag is created and associated with all the datastores in each desired protection group
- A tag-based storage policy is created for each protection group utilizing the tag
- A storage policy-based protection group is created and associated with the storage policy

When any virtual machine, new or existing, is associated with that policy and placed on the replicated datastore, Site Recovery Manager protection is automatic. If a virtual machine is disassociated from that policy and/or moved off the datastore it is automatically unprotected. The same happens for datastores and the virtual machines on them.

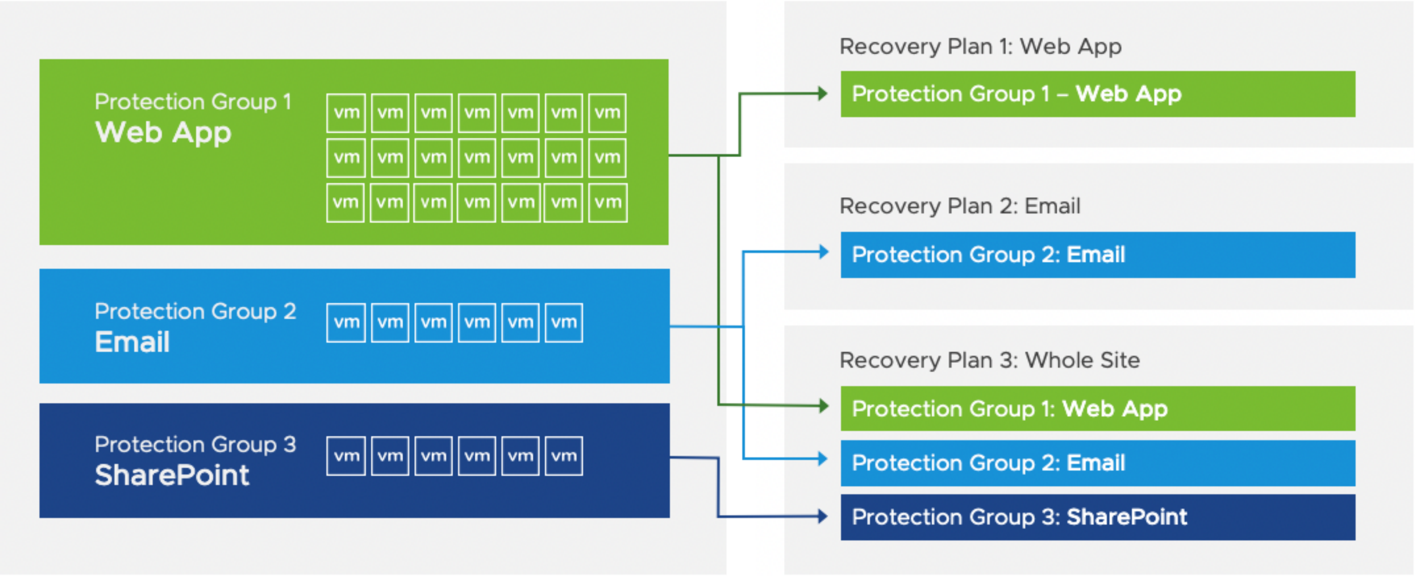
Recovery Plans

Recovery Plans in Site Recovery Manager are like an automated run book, controlling all the steps in the recovery process.

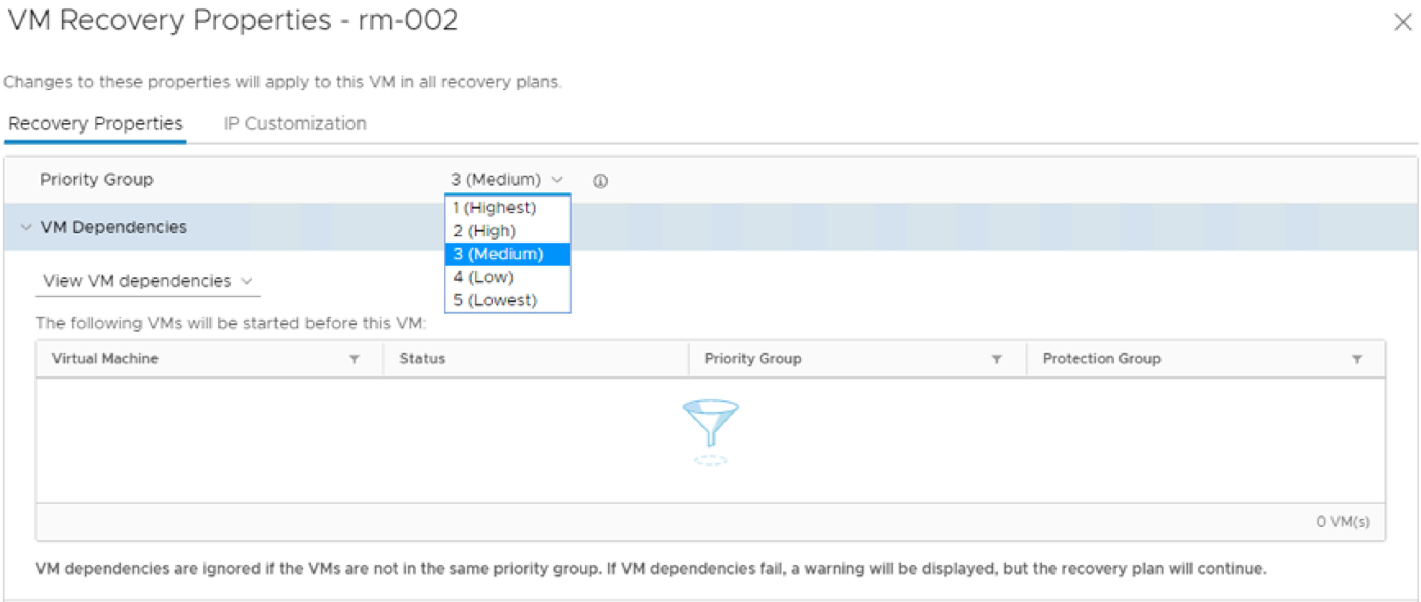
Overview

Recovery Plans in Site Recovery Manager are like an automated run book, 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 below there are three protection groups: Web App, Email and SharePoint. And there are three recovery plans: The Web App recovery plan containing the Web App protection group, the Email recovery plan containing the Email protection group, and the Whole Site recovery plan containing all three protection groups.


Protection Group 1
Web App
vm
Protection Group 2
Email
Protection Group 3
SharePoint
Recovery Plan 1: Web App
Protection Group 1 – Web App
Recovery Plan 2: Email
Protection Group 2: Email
Recovery Plan 3: Whole Site
Protection Group 1: Web App
Protection Group 2: Email
Protection Group 3: SharePoint

Priority Groups



VM Recovery Properties - rm-002

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

Priority Group: 3 (Medium)

The following VMs will be started before this VM:

Virtual Machine	Status	Priority Group	Protection Group

0 VM(s)

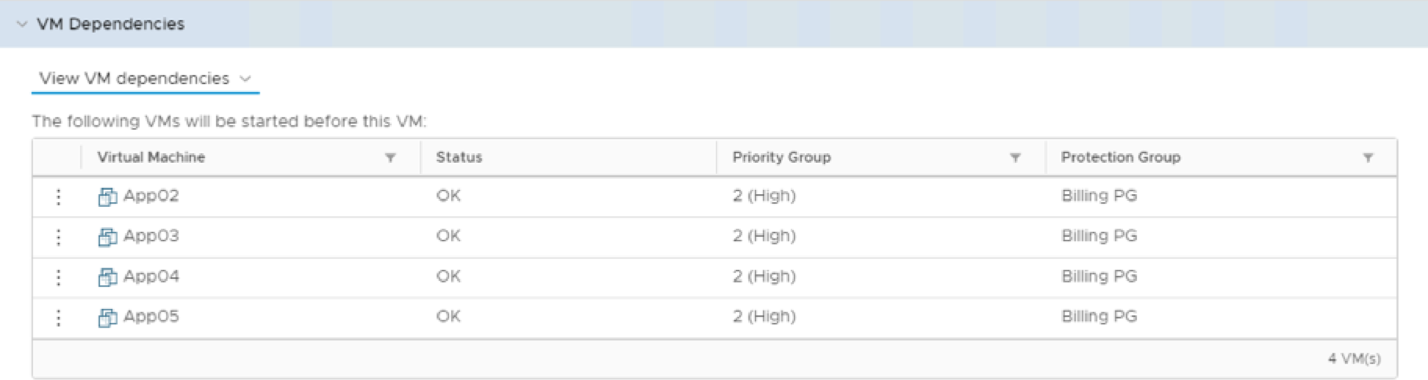
VM dependencies are ignored if the VMs are not in the same priority group. If VM dependencies fail, a warning will be displayed, but the recovery plan will continue.

There are five priority groups in Site Recovery Manager. 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 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, a specific other 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” - Site Recovery Manager will wait until “acct01” starts before powering on “acct02”. VMware Tools heartbeats are used to validate when a virtual machine has started successfully.



The following VMs will be started before this VM:

Virtual Machine	Status	Priority Group	Protection Group
App02	OK	2 (High)	Billing PG
App03	OK	2 (High)	Billing PG
App04	OK	2 (High)	Billing PG
App05	OK	2 (High)	Billing PG

4 VM(s)

Shutdown and Startup Actions

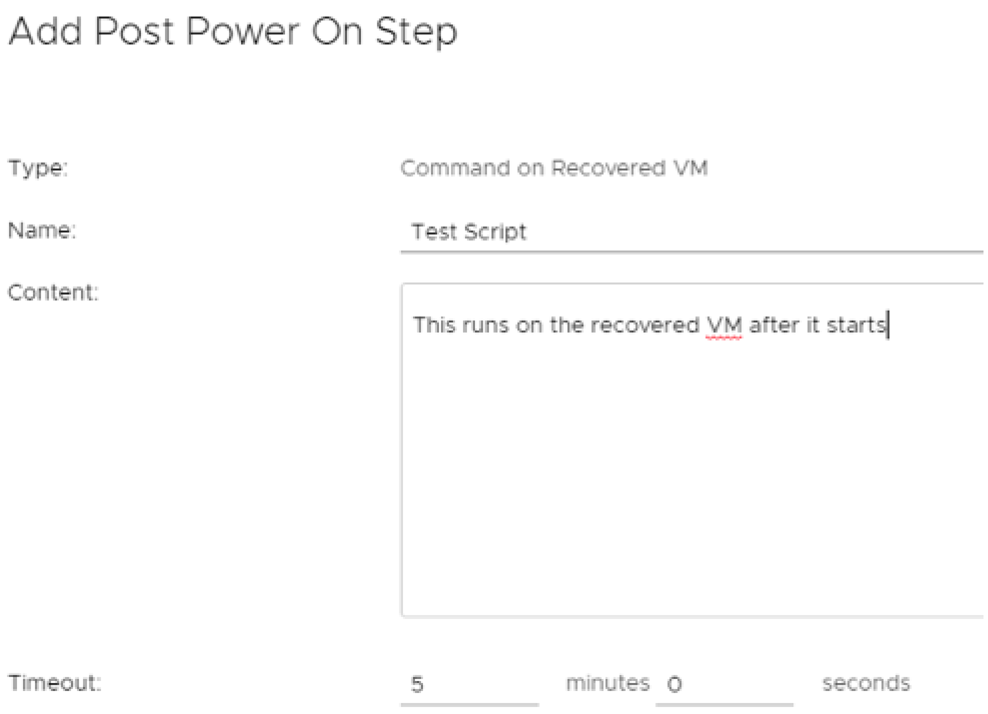
Shutdown actions apply to the protected virtual machines at the protected site during the run of a recovery plan. Shutdown actions are not used during the test of a recovery plan. By default, Site Recovery Manager will issue a guest OS shutdown, which requires VMware Tools and there is a time limit of 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.

A startup action applies to a virtual machine that is recovered by Site Recovery Manager. 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.

Pre and Post Power On Steps

Site Recovery Manager can run a command from the Site Recovery Manager server at the recovery site before and after powering on a virtual machine. 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. Running a script inside of a virtual machine is also supported as a post power on step. Site Recovery Manager 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.



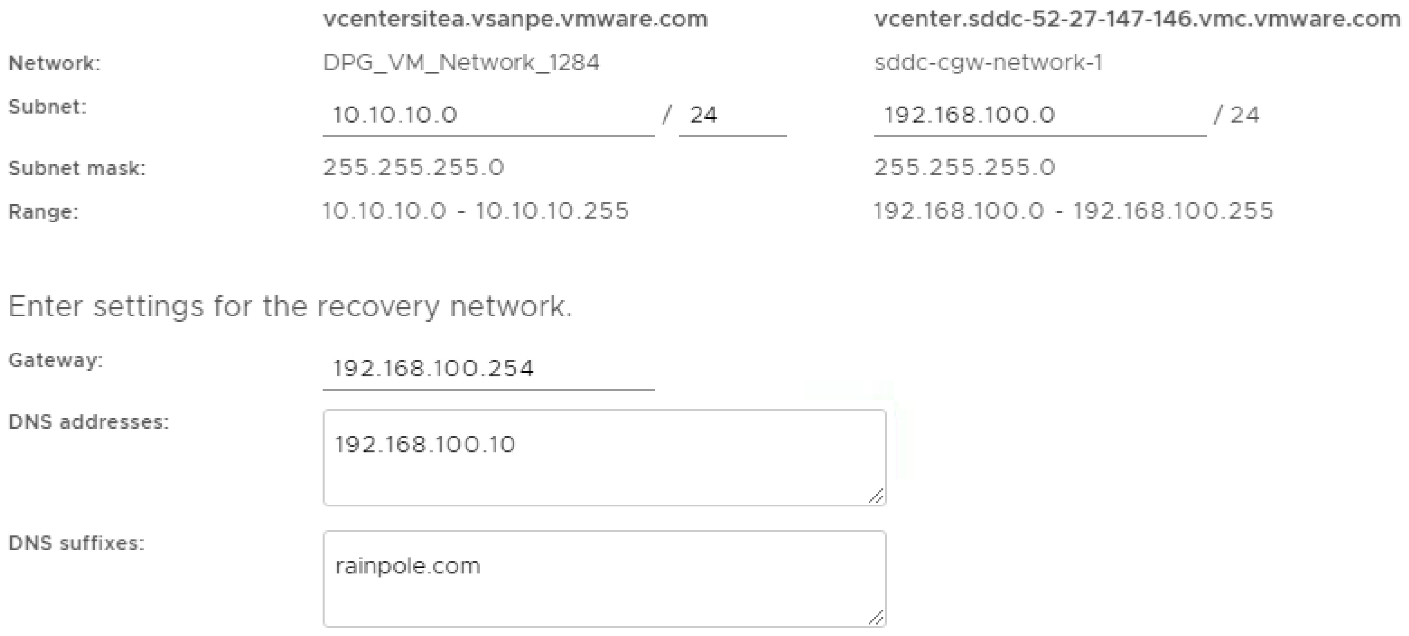
Add Post Power On Step

Type:	Command on Recovered VM
Name:	Test Script
Content:	This runs on the recovered VM after it starts
Timeout:	5 minutes 0 seconds

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, Site Recovery Manager 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 Site Recovery Manager. 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 198.168.100/24.



	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.

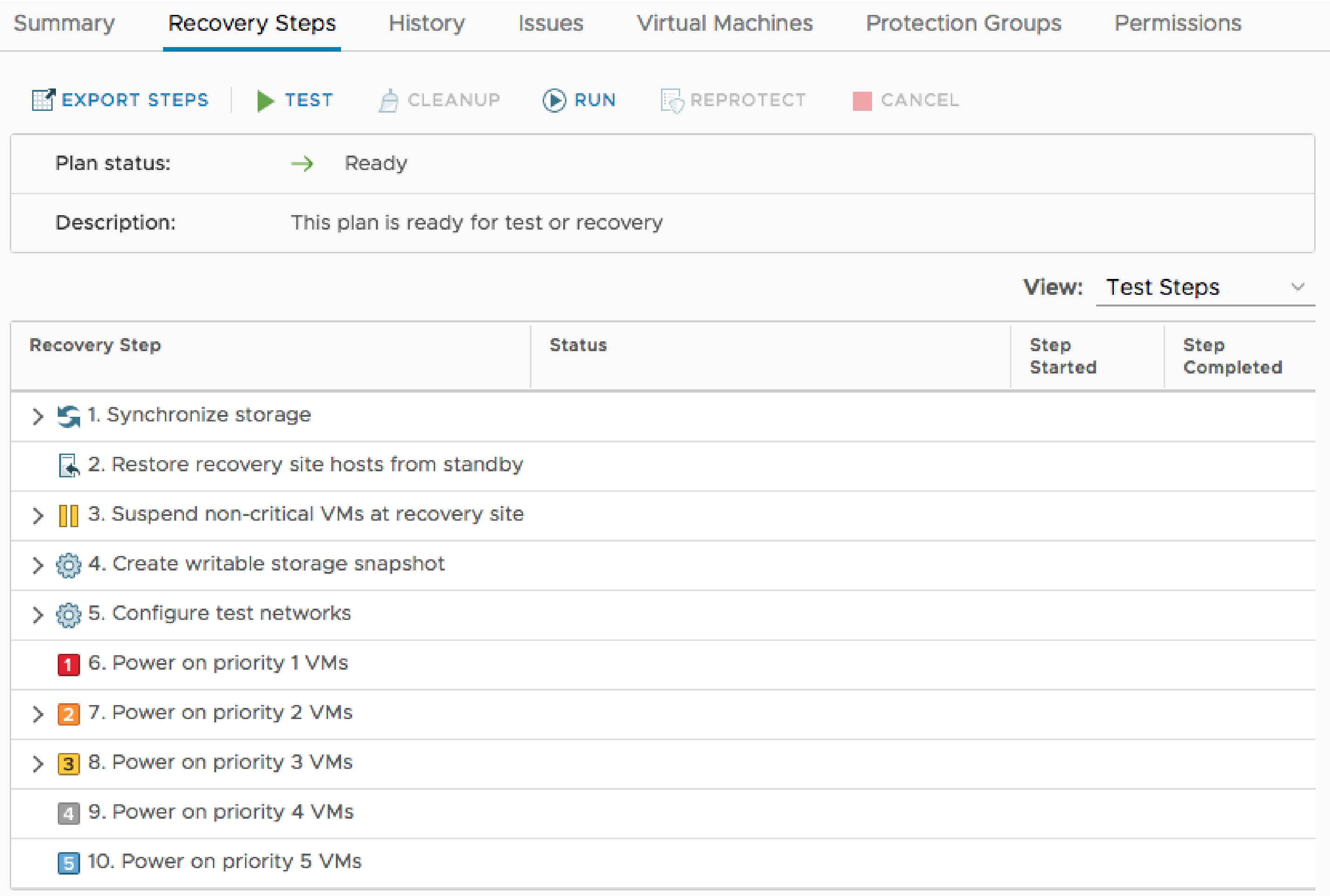
Gateway:	192.168.100.254
DNS addresses:	192.168.100.10
DNS suffixes:	rainpole.com

Workflows

After creating a recovery plan, it is beneficial to test the recovery plan to verify it works as expected.

Testing and Cleanup

After creating a recovery plan, it is beneficial to test the recovery plan to verify it works as expected. Site Recovery Manager 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.



Plan status: → Ready

Description: This plan is ready for test or recovery

View: Test Steps

Recovery Step	Status	Step Started	Step Completed
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			
10. Power on priority 5 VMs			

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.

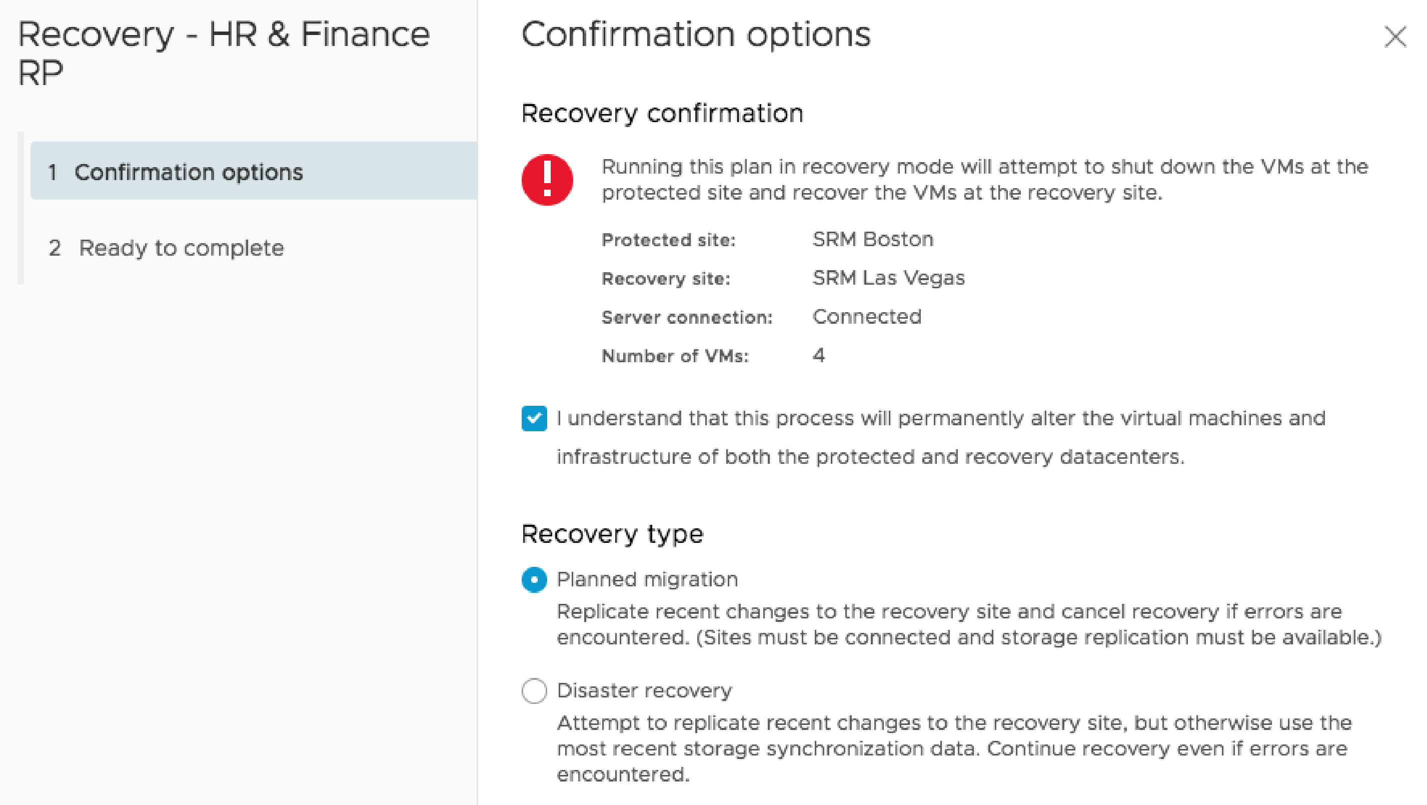
A question often asked is whether replication continues during the test of a recovery plan. The answer is yes. VMware Site Recovery Manager utilizes snapshots - either array snapshots (or clones) with array replication or virtual machine snapshots with vSphere Replication - as part of the recovery plan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

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. Site Recovery Manager 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.

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, Site Recovery Manager will attempt to shut down virtual machines at the protected site, or cross-vCenter vMotion them, if conducting a planned migration and utilizing stretched storage, 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.



Recovery - HR & Finance RP

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:	SRM Boston
Recovery site:	SRM Las Vegas
Server connection:	Connected
Number of VMs:	4

☑ 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.

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, Site Recovery Manager 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. If utilizing stretched storage, when conducting a planned migration, compatible virtual machines will be relocated utilizing cross-vCenter vMotion.

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 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.

This process is slightly different when running a recovery plan in planned migration mode when utilizing stretched storage. In this case, virtual machines that are capable of being vMotioned to the second site will be migrated first then the plan will proceed as above. This allows for a completely non-disruptive migration of production workloads from site to site.

If the protected site is offline due to a disaster, for example, the disaster recovery type should be selected. Site Recovery Manager will still attempt to synchronize storage as described in the previous paragraph. Since the protected site is offline, Site Recovery Manager will begin recovering virtual machines at the recovery site using the most recently replicated data.

Re-protect and Failback

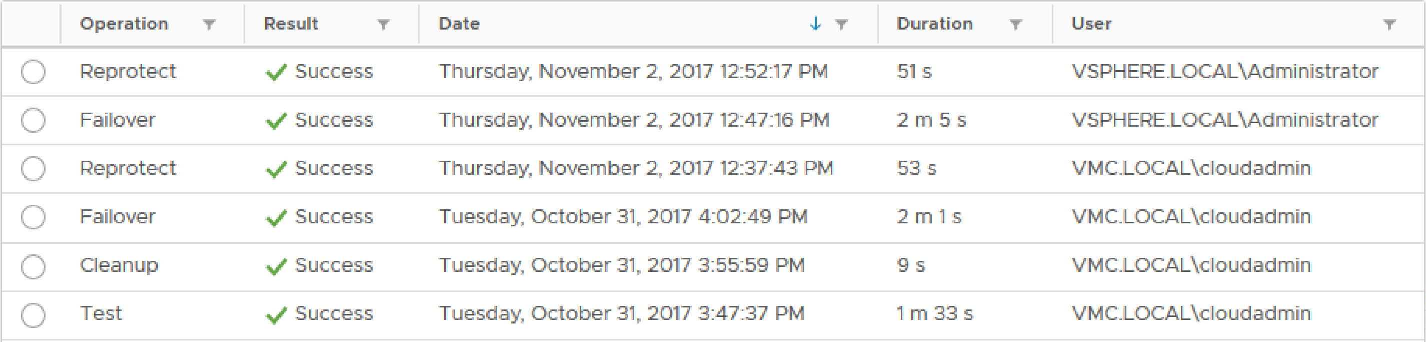
Site Recovery Manager features the ability to not only fail over virtual machine workloads, but also fail them back to their original site. However, this assumes that the original protected site is still intact and operational. An example of this is a disaster avoidance situation: The threat could be rising floodwaters from a major storm and Site Recovery Manager 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 re-protect workflow. This operation involves reversing replication and setting up the recovery plan to run in the opposite direction.

History Reports

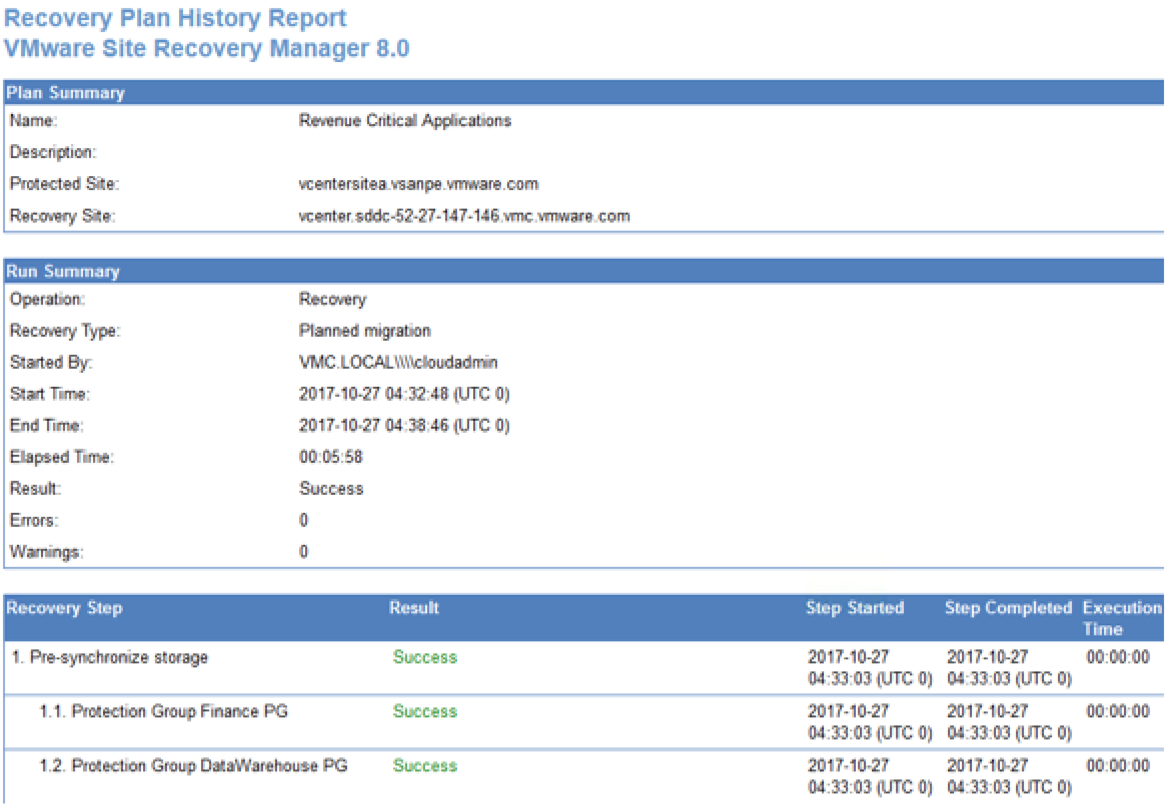
When workflows such as a recovery plan test and cleanup are performed in Site Recovery Manager, history reports are automatically generated. These reports document items such as the workflow name, execution times, successful operations, failures, and error messages. History reports are useful for a number 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.

Here is an example of the summary report:



	Operation	Result	Date	Duration	User
○	Reprotect	✓ Success	Thursday, November 2, 2017 12:52:17 PM	51 s	VSPHERE.LOCAL\Administrator
○	Failover	✓ Success	Thursday, November 2, 2017 12:47:16 PM	2 m 5 s	VSPHERE.LOCAL\Administrator
○	Reprotect	✓ Success	Thursday, November 2, 2017 12:37:43 PM	53 s	VMC.LOCAL\cloudadmin
○	Failover	✓ Success	Tuesday, October 31, 2017 4:02:49 PM	2 m 1 s	VMC.LOCAL\cloudadmin
○	Cleanup	✓ Success	Tuesday, October 31, 2017 3:55:59 PM	9 s	VMC.LOCAL\cloudadmin
○	Test	✓ Success	Tuesday, October 31, 2017 3:47:37 PM	1 m 33 s	VMC.LOCAL\cloudadmin

And an example of the detailed report:



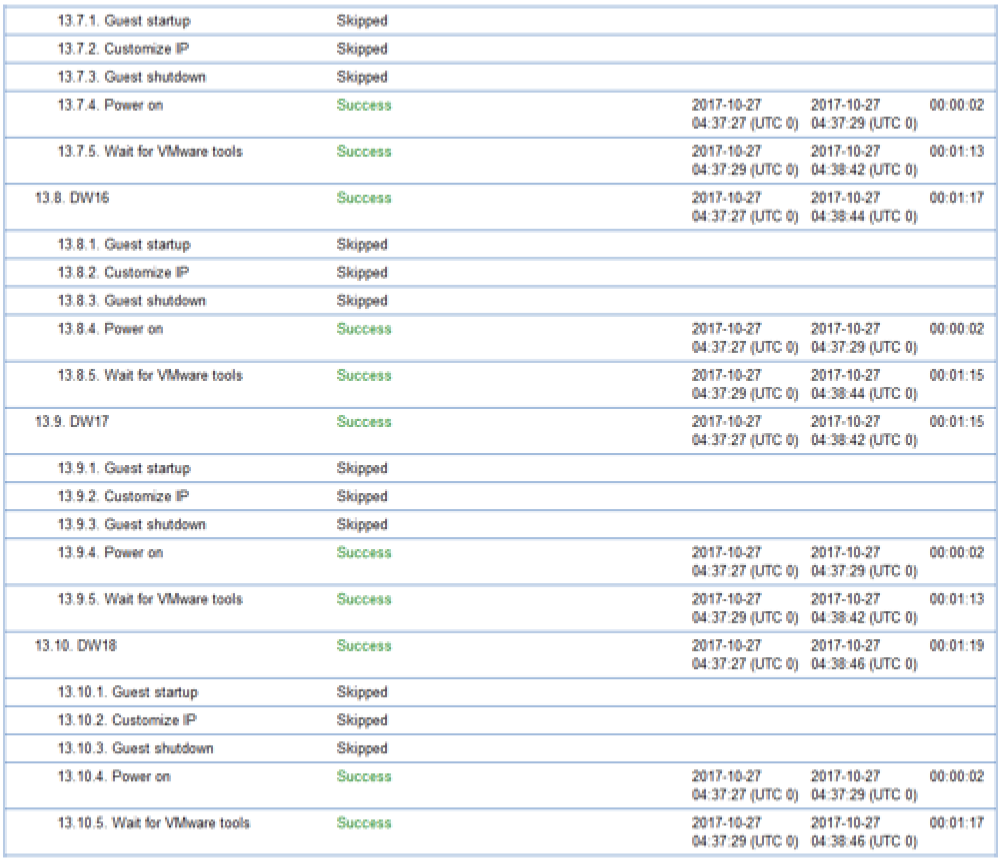
Recovery Plan History Report
VMware Site Recovery Manager 8.0

Plan Summary	
Name:	Revenue Critical Applications
Description:	
Protected Site:	vcentersitea.vsanpe.vmware.com
Recovery Site:	vcenter.sddc-52-27-147-146.vmc.vmware.com

Run Summary	
Operation:	Recovery
Recovery Type:	Planned migration
Started By:	VMC.LOCAL\\\\cloudadmin
Start Time:	2017-10-27 04:32:48 (UTC 0)
End Time:	2017-10-27 04:38:46 (UTC 0)
Elapsed Time:	00:05:58
Result:	Success
Errors:	0
Warnings:	0

Recovery Step	Result	Step Started	Step Completed	Execution Time
1. Pre-synchronize storage	Success	2017-10-27 04:33:03 (UTC 0)	2017-10-27 04:33:03 (UTC 0)	00:00:00
1.1. Protection Group Finance PG	Success	2017-10-27 04:33:03 (UTC 0)	2017-10-27 04:33:03 (UTC 0)	00:00:00
1.2. Protection Group DataWarehouse PG	Success	2017-10-27 04:33:03 (UTC 0)	2017-10-27 04:33:03 (UTC 0)	00:00:00

VM Detail:



13.7.1. Guest startup	Skipped			
13.7.2. Customize IP	Skipped			
13.7.3. Guest shutdown	Skipped			
13.7.4. Power on	Success	2017-10-27 04:37:27 (UTC 0)	2017-10-27 04:37:29 (UTC 0)	00:00:02
13.7.5. Wait for VMware tools	Success	2017-10-27 04:37:29 (UTC 0)	2017-10-27 04:38:42 (UTC 0)	00:01:13
13.8. DW16	Success	2017-10-27 04:37:27 (UTC 0)	2017-10-27 04:38:44 (UTC 0)	00:01:17
13.8.1. Guest startup	Skipped			
13.8.2. Customize IP	Skipped			
13.8.3. Guest shutdown	Skipped			
13.8.4. Power on	Success	2017-10-27 04:37:27 (UTC 0)	2017-10-27 04:37:29 (UTC 0)	00:00:02
13.8.5. Wait for VMware tools	Success	2017-10-27 04:37:29 (UTC 0)	2017-10-27 04:38:44 (UTC 0)	00:01:15
13.9. DW17	Success	2017-10-27 04:37:27 (UTC 0)	2017-10-27 04:38:42 (UTC 0)	00:01:15
13.9.1. Guest startup	Skipped			
13.9.2. Customize IP	Skipped			
13.9.3. Guest shutdown	Skipped			
13.9.4. Power on	Success	2017-10-27 04:37:27 (UTC 0)	2017-10-27 04:37:29 (UTC 0)	00:00:02
13.9.5. Wait for VMware tools	Success	2017-10-27 04:37:29 (UTC 0)	2017-10-27 04:38:42 (UTC 0)	00:01:13
13.10. DW18	Success	2017-10-27 04:37:27 (UTC 0)	2017-10-27 04:38:46 (UTC 0)	00:01:19
13.10.1. Guest startup	Skipped			
13.10.2. Customize IP	Skipped			
13.10.3. Guest shutdown	Skipped			
13.10.4. Power on	Success	2017-10-27 04:37:27 (UTC 0)	2017-10-27 04:37:29 (UTC 0)	00:00:02
13.10.5. Wait for VMware tools	Success	2017-10-27 04:37:29 (UTC 0)	2017-10-27 04:38:46 (UTC 0)	00:01:17

Next Steps

Automate and Orchestrate Your DR Plans with Site Recovery Manager

Make Site Recovery Manager a part of your vSphere deployments and improve your virtual machine availability and reduce your risk. Take the Site Recovery Manager Hands-on Lab today and register for a free trial of Site Recovery Manager and enjoy the benefits of automated and orchestrated protection of your critical virtual machines as an
an integrated part of your IT platform.

Additional Resources

For more information about VSphere Site Recovery Manager, please visit the product pages. Below are links to documentation and other resources:

- Product Documentation (includes Install Guide, Administration Guide, API Guide, and more)
- VMTN Community Forums
- FAQ
- Evaluation Guide
- Hands-on Lab

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 Manager 8.2 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 group. 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 blogs here: https://blogs.vmware.com/virtualblocks
- Follow Cato on Twitter: @vCatoGrace

© VMware LLC.

Copyright © 2005-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.