VMware Site Recovery Administration

VMware Site Recovery
Site Recovery Manager 8.0
vSphere Replication 8.0

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

About VMware Site Recovery Administration

VMware Site Recovery is an extension to VMware vCenter Server that delivers a business continuity and disaster recovery solution that helps you plan, test, and run the recovery of vCenter Server virtual machines. VMware Site Recovery uses the host-based replication feature of vSphere Replication and the orchestration of Site Recovery Manager.

Intended Audience

This book is intended for VMware Site Recovery administrators who are familiar with vSphere and its replication technologies, such as host-based replication and replicated datastores. This solution serves the needs of administrators who want to configure protection for their vSphere inventory. It might also be appropriate for users who need to add virtual machines to a protected inventory or to verify that an existing inventory is properly configured for use with Site Recovery Manager.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Site Recovery Manager Privileges, Roles, and Permissions

1

Site Recovery Manager provides disaster recovery by performing operations for users. These operations involve managing objects, such as recovery plans or protection groups, and performing operations, such as replicating or powering off virtual machines. Site Recovery Manager uses roles and permissions so that only users with the correct roles and permissions can perform operations.

Site Recovery Manager adds several roles to vCenter Server, each of which includes privileges to complete Site Recovery Manager and vCenter Server tasks. You assign roles to users to permit them to complete tasks in Site Recovery Manager.

Privilege	The right to perform an action, for example to create a recovery plan or to modify a protection group.
Role	A collection of privileges. Default roles provide the privileges that certain users require to perform a set of Site Recovery Manager tasks, for example users who manage protection groups or perform recoveries. A user can have at most one role on an object, but roles can be combined if the user belongs to multiple groups that all have roles on the object.
Permission	A role granted to a particular user or user group on a specific object. A user or user group is also known as a principal. A permission is a combination of a role, an object, and a principal. For example, a permission is the privilege to modify a specific protection group.

For information about the roles that Site Recovery Manager adds to vCenter Server and the privileges that users require to complete tasks, see Site Recovery Manager Roles Reference.

This chapter includes the following topics:

How Site Recovery Manager Handles Permissions

Site Recovery Manager determines whether a user has permission to perform an operation, such as configuring protection or running the individual steps in a recovery plan. This permission check ensures the correct authentication of the user, but it does not represent the security context in which the operation is performed.

Site Recovery Manager performs operations in the security context of the user ID that is used to connect the sites, or in the context of the ID under which the Site Recovery Manager service is running, for example, the local system ID.

After Site Recovery Manager verifies that a user has the appropriate permissions on the target vSphere resources, Site Recovery Manager performs operations on behalf of users by using the vSphere administrator role.

For operations that configure protection on virtual machines, Site Recovery Manager validates the user permissions when the user requests the operation. Operations require two phases of validation.

1 During configuration, Site Recovery Manager verifies that the user configuring the system has the correct permissions to complete the configuration on the vCenter Server object. For example, a user must have permission to protect a virtual machine and use resources on the secondary vCenter Server instance that the recovered virtual machine uses.

2 The user performing the configuration must have the correct permissions to complete the task that they are configuring. For example, a user must have permissions to run a recovery plan. Site Recovery Manager then completes the task on behalf of the user as a vCenter Server administrator.

As a result, a user who completes a particular task, such as a recovery, does not necessarily require permissions to act on vSphere resources. The user only requires the permission to run a recovery in Site Recovery Manager. Site Recovery Manager performs the operations by using the user credentials that you provide when you connect the protected and recovery sites.

Site Recovery Manager maintains a database of permissions for internal Site Recovery Manager objects that uses a model similar to the one the vCenter Server uses. Site Recovery Manager verifies its own Site Recovery Manager privileges even on vCenter Server objects. For example, Site Recovery Manager checks for the **Resource.Recovery Use** permission on the target datastore rather than checking multiple low-level permissions, such as **Allocate space**. Site Recovery Manager also verifies the permissions on the remote vCenter Server instance.

To use Site Recovery Manager with vSphere Replication, you must assign vSphere Replication roles to users as well as Site Recovery Manager roles. For information about vSphere Replication roles, see *vSphere Replication Administration*.

Site Recovery Manager and the vCenter Server Administrator Role

If a user or user group has the vCenter Server administrator role on a vCenter Server instance when you install Site Recovery Manager, that user or user group obtains all Site Recovery Manager privileges.

If you assign the vCenter Server administrator role to users or user groups after you install Site Recovery Manager, you must manually assign the Site Recovery Manager roles to those users on Site Recovery Manager objects.

You can assign Site Recovery Manager roles to users or user groups that do not have the vCenter Server administrator role. In this case, those users have permission to perform Site Recovery Manager operations, but they do not have permission to perform all vCenter Server operations.

Site Recovery Manager and vSphere Replication Roles

When you install vSphere Replication with Site Recovery Manager, the vCenter Server administrator role inherits all of the Site Recovery Manager and vSphere Replication privileges.

If you manually assign a Site Recovery Manager role to a user or user group, or if you assign a Site Recovery Manager role to a user or user group that is not a vCenter Server administrator, these users do not obtain vSphere Replication privileges. The Site Recovery Manager roles do not include the privileges of the vSphere Replication roles. For example, the Site Recovery Manager Recovery Administrator role includes the privilege to run recovery plans, including recovery plans that contain vSphere Replication protection groups, but it does not include the privilege to configure vSphere Replication on a virtual machine. The separation of the Site Recovery Manager and vSphere Replication roles allows you to distribute responsibilities between different users. For example, one user with the VRM administrator role is responsible for configuring vSphere Replication on virtual machines, and another user with the Site Recovery Manager Recovery Administrator role is responsible for running recoveries.

In some cases, a user who is not vCenter Server administrator might require the privileges to perform both Site Recovery Manager and vSphere Replication operations. To assign a combination of Site Recovery Manager and vSphere Replication roles to a single user, you can add the user to two user groups.

Example: Assign Site Recovery Manager and vSphere Replication Roles to a User

By creating two user groups, you can grant to a user the privileges of both a Site Recovery Manager role and a vSphere Replication role, without that user being a vCenter Server administrator.

1 Create two user groups.

2 Assign a Site Recovery Manager role to one user group, for example Site Recovery Manager administrator.

3 Assign a vSphere Replication role to the other user group, for example VRM administrator.

4 Add the user to both user groups.

The user has all the privileges of the Site Recovery Manager administrator role and of the VRM administrator role.

Assign Site Recovery Manager Roles and Permissions

During installation of Site Recovery Manager, users with the vCenter Server administrator role are granted the administrator role on Site Recovery Manager. At this time, only vCenter Server administrators can log in to Site Recovery Manager, unless they explicitly grant access to other users.

To allow other users to access Site Recovery Manager, vCenter Server administrators must grant them permissions in the Site Recovery Manager user interface. You assign site-wide permission assignments on a per-site basis. You must add corresponding permissions on both sites.

Site Recovery Manager requires permissions on vCenter Server objects as well as on Site Recovery Manager objects. To configure permissions on the remote vCenter Server installation, start another instance of the vSphere Web Client. You can change Site Recovery Manager permissions from the same Site Recovery Manager user interface on both sites after you connect the protected and recovery sites.

Site Recovery Manager augments vCenter Server roles and permissions with additional permissions that allow detailed control over Site Recovery Manager specific tasks and operations. For information about the permissions that each Site Recovery Manager role includes, see Site Recovery Manager Roles Reference.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 On the left-hand pane click **Permissions**, select a site, and click **Add**.

   a From the **Domain** drop-down menu, select the domain that contains the user or group.

   b Select a name from the **User/Group** list.

   c Select a role from the **Role** drop-down menu to assign to the user or user group.

   The **Role** drop-down menu includes all of the roles that vCenter Server and its plug-ins make available. Site Recovery Manager adds several roles to vCenter Server.

Option	Action
Allow a user or user group to perform all Site Recovery Manager configuration and administration operations.	Assign the **SRM Administrator** role.
Allow a user or user group to manage and modify protection groups and to configure protection on virtual machines.	Assign the **SRM Protection Groups Administrator** role.
Allow a user or user group to perform recoveries and test recoveries.	Assign the **SRM Recovery Administrator** role.
Allow a user or user group to create, modify, and test recovery plans.	Assign the **SRM Recovery Plans Administrator** role.
Allow a user or user group to test recovery plans.	Assign the **SRM Recovery Test Administrator** role.

4 Click **Add** to assign the role and its associated privileges to the user or user group.

5 Repeat Step 3 through Step 4 to assign roles and privileges to the users or user groups on the other Site Recovery Manager site.

You assigned a given Site Recovery Manager role to a user or user group. This user or user group has privileges to perform the actions that the role defines on the objects on the Site Recovery Manager site that you configured.

Example: Combining Site Recovery Manager Roles

You can assign only one role to a user or user group. If a user who is not a vCenter Server administrator requires the privileges of more than one Site Recovery Manager role, you can create multiple user groups. For example, a user might require the privileges to manage recovery plans and to run recovery plans.

1 Create two user groups.

2 Assign the **SRM Recovery Plans Administrator** role to one group.

3 Assign the **SRM Recovery Administrator** role to the other group.

4 Add the user to both user groups.

By being a member of groups that have both the **SRM Recovery Plans Administrator** and the **SRM Recovery Administrator** roles, the user can manage recovery plans and run recoveries.

Site Recovery Manager Roles Reference

Site Recovery Manager includes a set of roles. Each role includes a set of privileges, which allow users with those roles to complete different actions.

Roles can have overlapping sets of privileges and actions. For example, the Site Recovery Manager Administrator role and the Site Recovery Manager Protection Groups Administrator have the **Create** privilege for protection groups. With this privilege, the user can complete one aspect of the set of tasks that make up the management of protection groups.

Assign roles to users on Site Recovery Manager objects consistently on both sites, so that protected and recovery objects have identical permissions.

All users must have at least the **System.Read** privilege on the root folders of vCenter Server and the Site Recovery Manager root nodes on both sites.

Note If you uninstall Site Recovery Manager Server, Site Recovery Manager removes the default Site Recovery Manager roles but the Site Recovery Manager privileges remain. You can still see and assign Site Recovery Manager privileges on other roles after uninstalling Site Recovery Manager. This is standard vCenter Server behavior. Privileges are not removed when you unregister an extension from vCenter Server.

Table 1-1. Site Recovery Manager Roles

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
Site Recovery Manager Administrator	The Site Recovery Manager Administrator grants permission to perform all Site Recovery Manager configuration and administration operations. ■ Configure advanced settings. ■ Configure connections. ■ Configure inventory preferences. ■ Configure placeholder datastores. ■ Configure array managers. ■ Manage protection groups. ■ Manage recovery plans. ■ Run recovery plans. ■ Perform reprotect operations. ■ Configure protection on virtual machines. ■ Edit protection groups. ■ Remove protection groups. ■ View storage policy objects.	**Site Recovery Manager.Advanced Settings.Modify** **Site Recovery Manager.Array Manager.Configure** **Site Recovery Manager.Diagnostics.Export** **Site Recovery Manager.Inventory Preferences.Modify** **Site Recovery Manager.Placeholder Datastores.Configure** **Site Recovery Manager.Protection Group.Assign to Plan** **Site Recovery Manager.Protection Group.Create** **Site Recovery Manager.Protection Group.Modify** **Site Recovery Manager.Protection Group.Remove** **Site Recovery Manager.Protection Group.Remove from Plan** **Site Recovery Manager.Recovery History .View Deleted Plans** **Site Recovery Manager.Recovery Plan.Configure** **Site Recovery Manager.Recovery Plan.Create** **Site Recovery Manager.Recovery Plan.Modify** **Site Recovery Manager.Recovery Plan.Recovery** **Site Recovery Manager.Recovery Plan.Remove** **Site Recovery Manager.Recovery Plan.Reprotect** **Site Recovery Manager.Recovery Plan.Test** **Site Recovery Manager.Remote Site.Modify** **Datastore.Replication.Protect** **Datastore.Replication.Unprotect.Stop** **Resource.Recovery Use** **Virtual Machine. SRM Protection.Protect** **Virtual Machine. SRM Protection.Stop** **Site Recovery Manager.Profile-driven storage.Profile-driven storage view**	■ Virtual machines ■ Datastores ■ vCenter Server folders ■ Resource pools ■ Site Recovery Manager service instances ■ Networks ■ Site Recovery Manager folders ■ Protection groups ■ Recovery plans ■ Array managers
Site Recovery Manager Protection Groups Administrator	The Site Recovery Manager Protection Groups Administrator role allows users to manage protection groups. ■ Create protection groups.	**Site Recovery Manager.Protection Group.Create** **Site Recovery Manager.Protection Group.Modify** **Site Recovery Manager.Protection Group.Remove** **Datastore.Replication.Protect** **Datastore.Replication.Unprotect.Stop** **Resource.Recovery Use** **Virtual Machine. SRM Protection.Protect** **Virtual Machine. SRM Protection.Stop**	■ Site Recovery Manager folders ■ Protection groups

Table 1-1. Site Recovery Manager Roles (Continued)

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
	■ Modify protection groups. ■ Add virtual machines to protection groups. ■ Delete protection groups. ■ Configure protection on virtual machines. ■ Remove protection from virtual machines. Users with this role cannot perform or test recoveries or create or modify recovery plans.		
Site Recovery Manager Recovery Administrator	The Site Recovery Manager Recovery Administrator role allows users to perform recoveries and reprotect operations. ■ Remove protection groups from recovery plans. ■ Test recovery plans. ■ Run recovery plans. ■ Run reprotect operations. ■ Configure custom command steps on virtual machines. ■ View deleted recovery plans. ■ Edit virtual machine recovery properties. Users with this role cannot configure protection on virtual machines, or create or modify recovery plans.	**Site Recovery Manager.Protection Group.Remove from plan** **Site Recovery Manager.Recovery Plan.Modify** **Site Recovery Manager.Recovery Plan.Test** **Site Recovery Manager.Recovery Plan.Recovery** **Site Recovery Manager.Recovery Plan.Reprotect** **Site Recovery Manager.Recovery Plan.Configure.Configure commands** **Site Recovery Manager.Recovery History.View deleted plans**	■ Protection groups ■ Recovery plans ■ Site Recovery Manager service instances

Table 1-1. Site Recovery Manager Roles (Continued)

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
Site Recovery Manager Recovery Plans Administrator	The Site Recovery Manager Recovery Plans Administrator role allows users to create and test recovery plans. ■ Add protection groups to recovery plans. ■ Remove protection groups from recovery plans. ■ Configure custom command steps on virtual machines. ■ Create recovery plans. ■ Test recovery plans. ■ Cancel recovery plan tests. ■ Edit virtual machine recovery properties. Users with this role cannot configure protection on virtual machines, or perform recoveries or reprotect operations.	**Site Recovery Manager.Protection Group.Assign to plan** **Site Recovery Manager.Protection Group.Remove from plan** **Site Recovery Manager.Recovery Plan.Configure Commands** **Site Recovery Manager.Recovery Plan.Create** **Site Recovery Manager.Recovery Plan.Modify** **Site Recovery Manager.Recovery Plan.Remove** **Site Recovery Manager.Recovery Plan.Test** **Resource.Recovery Use**	■ Protection groups ■ Recovery plans ■ vCenter Server folders ■ Datastores ■ Resource pools ■ Networks

Table 1-1. Site Recovery Manager Roles (Continued)

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
Site Recovery Manager Test Administrator	The Site Recovery Manager Test Administrator role only allows users to test recovery plans. ■ Test recovery plans. ■ Cancel recovery plan tests. ■ Edit virtual machine recovery properties. Users with this role cannot configure protection on virtual machines, create protection groups or recovery plans, or perform recoveries or reprotect operations.	**Site Recovery Manager.Recovery Plan.Modify** **Site Recovery Manager.Recovery Plan.Test**	Recovery plans
Site Recovery Manager Remote User	The Site Recovery Manager Remote User role grants users the minimum set of privileges needed for cross site Site Recovery Manager operations.	**Datastore.Browse datastore** **Datastore.Low level file operations** **Datastore.Replication.Update virtual machine files** **Datastore.Replication.Update virtual machine metadata** **Host.vSphere Replication.Manage replication** **Virtual Machine.Snapshot management.Remove snapshot** **Virtual Machine.vSphere Replication.Configure replication** **Virtual Machine.vSphere Replication.Manage replication** **Virtual Machine.vSphere Replication.Monitor replication**	■ Virtual machines ■ Datastores

Replicating Virtual Machines 2

Before you create protection groups, you must configure replication on the virtual machines to protect.

You replicate virtual machines by using vSphere Replication.

This chapter includes the following topics:

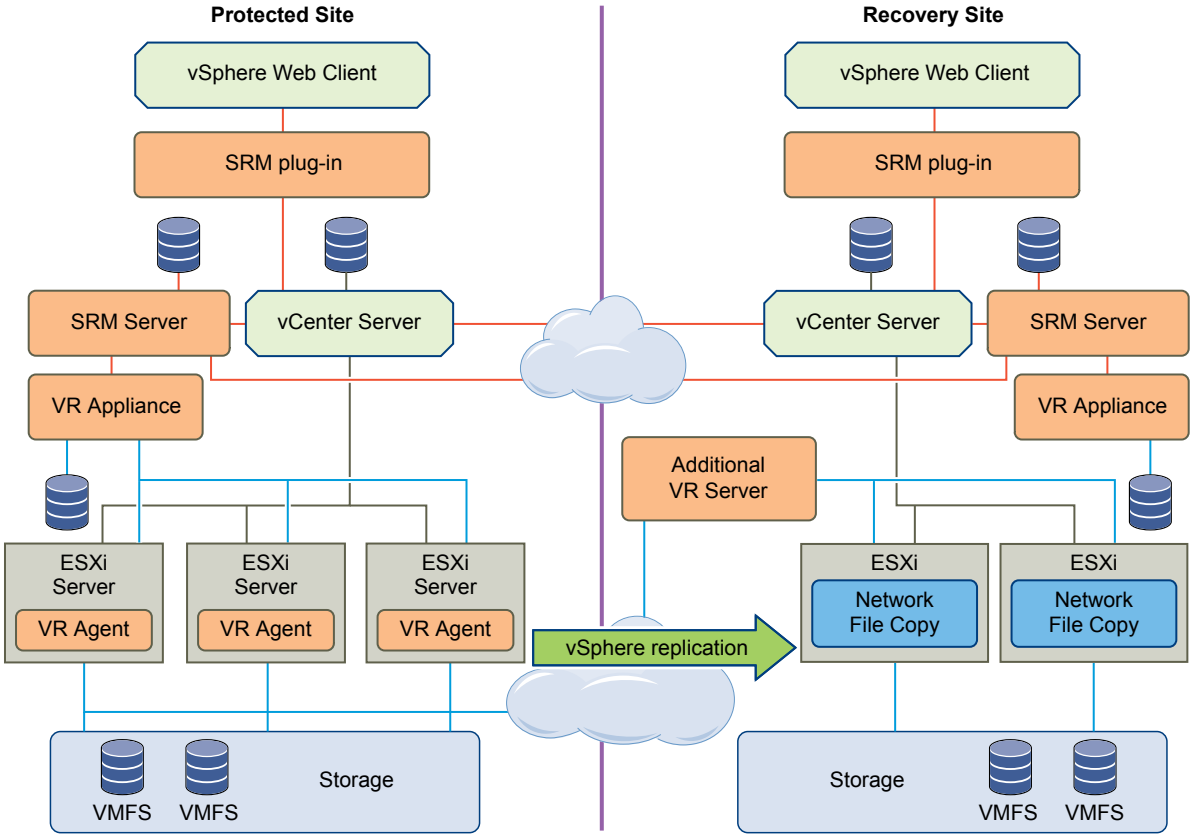
Using vSphere Replication with Site Recovery Manager

Site Recovery Manager can use vSphere Replication to replicate data to servers at the recovery site.

You deploy the vSphere Replication appliance and configure vSphere Replication on virtual machines independently of Site Recovery Manager. See *Install vSphere Replication* in the *VMware Site Recovery for VMware Cloud on AWS Installation and Configuration* guide for information about deploying and configuring vSphere Replication.

vSphere Replication does not require storage arrays. The vSphere Replication storage replication source and target can be any storage device, including, but not limited to, storage arrays.

Figure 2-1. Site Recovery Manager Architecture with vSphere Replication



How the Recovery Point Objective Affects Replication Scheduling

When you set a Recovery Point Objective (RPO) value during replication configuration, you determine the maximum data loss that you can tolerate.

The RPO value affects replication scheduling, but vSphere Replication does not adhere to a strict replication schedule. For example, when you set the RPO to 15 minutes, you instruct vSphere Replication that you can tolerate losing the data for up to 15 minutes. This does not mean that data is replicated every 15 minutes.

If you set an RPO of x minutes, and the RPO is not violated, the latest available replication instance can never reflect a state that is older than x minutes. A replication instance reflects the state of a virtual machine at the time the synchronization starts.

Assume that during replication configuration you set the RPO to 15 minutes. If the synchronization starts at 12:00 and it takes five minutes to transfer to the target site, the instance becomes available on the target site at 12:05, but it reflects the state of the virtual machine at 12:00. The next synchronization can start no later than 12:10. This replication instance is then available at 12:15 when the first replication instance that started at 12:00 expires.

If you set the RPO to 15 minutes and the replication takes 7.5 minutes to transfer an instance, vSphere Replication transfers an instance all the time. If the replication takes more than 7.5 minutes, the replication encounters periodic RPO violations. For example, if the replication starts at 12:00 and takes 10 minutes to transfer an instance, the replication finishes at 12:10. You can start another replication immediately, but it finishes at 12:20. During the time interval 12:15-12:20, an RPO violation occurs because the latest available instance started at 12:00 and is too old.

The replication scheduler tries to satisfy these constraints by overlapping replications to optimize bandwidth use and might start replications for some virtual machines earlier than expected.

To determine the replication transfer time, the replication scheduler uses the duration of the last few instances to estimate the next one.

How the 5 Minute Recovery Point Objective Works

You can use the 5 minute Recovery Point Objective (RPO) if the target and the source sites use VMFS 6.0, VMFS 5.x, NFS 4.1, NFS 3, VVOL, or VMware vSAN 6.2 Update 3 storage and later.

vSphere Replication 8.0 displays the 5 minute RPO setting when the target and the source site use VMFS 6.0, VMFS 5.x, NFS 4.1, NFS 3, VVOL, or VMware vSAN 6.2 Update 3 storage and later.

You can use the 5 minute RPO setting if you are using different datastore types between the source and the target site.

The 5 minute RPO can be applied to a maximum of 100 VMs on VMFS 6.0, VMFS 5.x, NFS 4.1, NFS 3 and VMware vSAN 6.2 Update 3 and later. The maximum for VVOL datastore is 50 VMs.

Note If you select the OS quiescing option while configuring replication, you cannot use an RPO value lower than 15 minutes.

Using vSphere Replication with VMware vSAN Storage

You can use VMware vSAN datastores as target datastores when configuring replications. Follow the guidelines when using vSphere Replication with vSAN storage.

Because user-friendly names of vSAN datastores might change and cause errors during replication or recovery operations, vSphere Replication automatically replaces the user-friendly name of a datastore with its UUID, which is constant. Therefore, the UUID is displayed everywhere in the vSphere Replication user interface, though you selected a human-readable name during replication configuration.

Limits of Using vSphere Replication with vSAN Storage

For reasons of load and I/O latency, vSAN storage is subject to limits in terms of the numbers of hosts that you can include in a vSAN cluster and the number of virtual machines that you can run on each host. See the Limits section in the *VMware vSAN Design and Sizing Guide* at https://www.vmware.com/products/vsan.html.

Using vSphere Replication adds to the load on the storage. Every virtual machine generates regular read and write operations. Configuring replications on those virtual machines adds another read operation to the regular read and write operations, which increases the I/O latency on the storage. The precise number of virtual machines that you can replicate to vSAN storage by using vSphere Replication depends on your infrastructure. If you notice slower response times when you configure replications for virtual machines in vSAN storage, monitor the I/O latency of the vSAN infrastructure. Potentially, reduce the number of virtual machines that you replicate in the vSAN datastore.

Note When you stop a replication, vSphere Replication does not delete the replica directory at the target datastore. As a result, stale directories remain on VMFS and NFS target datastores, and unused namespaces remain on Virtual SAN and Virtual Volume target datastores. Because the maximum number of directories and namespaces on a datastore is limited, you must manually clean them up to free resources on the datastore. See Clean Up the Target Datastore After You Stop a Replication.

Using vSphere Replication with vSphere Storage DRS

vSphere Replication can operate with target sites that have VMware vSphere® Storage DRS™ enabled.

Storage DRS can detect the data that vSphere Replication copies on the target site and can move replications without affecting the replication process.

How vSphere Replication Synchronizes Data Between vCenter Server Sites During Initial Configuration

When you configure a virtual machine for replication, vSphere Replication starts an initial configuration task during which a replica virtual machine is created on the target site, and data synchronization occurs between the source and the target vCenter Server site.

The speed of data synchronization depends on the availability of information about block allocation of the VMDK files. vSphere Replication uses this information to find empty regions of the disks and accelerate the sync operations by skipping these regions. The speed of data synchronization also depends on the site for which block allocation information is available.

- If the allocation information is available at both sites, data synchronization occurs at the highest possible speed.
- If the allocation information is available only at the source or the target site, vSphere Replication skips the empty regions on the VMDK disks at that site, but processes the entire disk at the site where allocation information is not available. Therefore, data synchronization is slower.
- If the allocation information is not available at either site, data synchronization is done by comparing all blocks between the source site and the target site, even if many of the blocks have not been allocated on the disk by the guest OS. This is the slowest method for data synchronization.

Note The availability of block allocation information has little effect on the speed of data synchronization for VMDK disks that are almost full.

Factors That Affect the Availability of Block Allocation Information

The availability of allocation information and the degree to which vSphere Replication can use it to accelerate data synchronization depend on the ESXi versions, the vSphere Replication Management server versions, the type of VMDK disks, and the type of volumes on which the disks reside.

Product Versions at the Source and the Target Site

The acceleration of initial synchronization is supported only on ESXi hosts 6.0.x or later.

If the ESXi and the vSphere Replication Server on the source site are 6.x or later, but the vSphere Replication Server or the hosts at the target site are not 6.x or later, the allocation information will be available only on the source site.

If the vSphere Replication Management servers at the source and at the target site are both 6.x, but one or more ESXi hosts at the target site are not 6.0 or later, if the vSphere Replication Management server selects a target host that is not 6.0 or later, there will be no allocation information available on the target site.

Note Because vSphere Replication Management server 6.x cannot select only ESXi 6.0 hosts for the initial synchronization, the acceleration of the operations might vary depending on the selected host. To achieve maximum acceleration, all ESXi hosts at the target site that act as storage servers for vSphere Replication should be ESXi 6.0 or later.

The Type of the Datastore

Disks on VMFS or VSAN datastores provide full allocation information.

NFS datastores cannot provide allocation information for the disks that are located on them.

Note Replication disks on the source and the target site can be on different datastore types. The acceleration of the initial synchronization depends on whether both sites can provide allocation information, or only one site. If none of the sites can provide allocation information, no acceleration occurs.

The Type of Virtual Disk

Lazy zeroed thick disks, thin disks, and vSAN sparse disks, Space-Efficient sparse disks, and VMDK sparse snapshots provide allocation information.

Eager zeroed thick disks do not provide allocation information.

Virtual disks that are based on VVOLs are native to the volume. vSphere Replication 6.x can get allocation information from them only when they are on the target site. For this reason, the acceleration of the initial synchronization will be partial.

vSphere Replication Roles Reference

vSphere Replication includes a set of roles. Each role includes a set of privileges, which enable users with those roles to complete different actions.

For information about how to assign roles, see *Assigning Roles in the vSphere Web Client* in *vSphere Security*.

Note When assigning permissions with no propagation, make sure that you have at least Read-only permission on all parent objects.

Table 2-1. vSphere Replication Roles

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
VRM replication viewer	■ View replications. ■ Cannot change replication parameters.	**VRM remote.View VR** **VRM remote.View VRM** **VRM datastore mapper.View** **Host.vSphere Replication.Manage replication** **Virtual machine.vSphere Replication.Monitor replication**	vCenter Server root folder with propagation, at source site (outgoing replications) and target site (incoming replications). Alternatively, vCenter Server root folder without propagation on both sites and virtual machine without propagation on the source site.
VRM virtual machine replication user	■ View replications. ■ Manage datastores. ■ Configure and unconfigure replications. ■ Manage and monitor replications. ■ View defined storage capabilities and storage profiles. Requires a corresponding user with the same role on the target site and additionally vSphere Replication target datastore user role on the target datacenter, or datastore folder or each target datastore.	**Datastore.Browse Datastore** **VRM remote.View VR** **VRM remote.View VRM** **VRM datastore mapper.Manage** **VRM datastore mapper.View** **Host.vSphere Replication.Manage replication** **Virtual machine.vSphere Replication.Configure replication** **Virtual machine.vSphere Replication.Manage replication** **Virtual machine.vSphere Replication.Monitor replication** **Profile-driven storage .Profile-driven storage view**	vCenter Server root folder with propagation on both sites. Alternatively, vCenter Server root folder without propagation on both sites, virtual machine without propagation on the source site, source datastores without propagation on the source site.

Table 2-1. vSphere Replication Roles (Continued)

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
VRM administrator	Incorporates all vSphere Replication privileges.	**VRM remote.Manage VR** **VRM remote.View VR** **VRM remote.Manage VRM** **VRM remote.View VRM** **VRM datastore mapper.Manage** **VRM datastore mapper.View** **VRM diagnostics .Manage** **VRM session .Terminate** **Datastore.Browse datastore** **Datastore.Low level file operations** **Host.vSphere Replication.Manage replication** **Resource.Assign virtual machine to resource pool** **Virtual machine.Configuration.Add existing disk** **Virtual machine.Configuration.Add or remove device** **Virtual machine.Interaction.Power On** **Virtual machine.Interaction.Device connection** **Virtual machine.Inventory.Register** **Virtual machine.vSphere Replication.Configure replication** **Virtual machine.vSphere Replication.Manage replication** **Virtual machine.vSphere Replication.Monitor replication** **Profile-driven storage .Profile-driven storage view**	vCenter Server root folder with propagation on both sites. Alternatively, vCenter Server root folder without propagation on both sites, virtual machine without propagation on the source site, target datastore, target virtual machine folder with propagation on the target site, target host or cluster with propagation on the target site.
VRM diagnostics	Generate, retrieve, and delete log bundles.	**VRM remote.View VR** **VRM remote.View VRM** **VRM diagnostics .Manage**	vCenter Server root folder on both sites.

Table 2-1. vSphere Replication Roles (Continued)

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
VRM target datastore user	Configure and reconfigure replications. Used on target site in combination with the VRM virtual machine replication user role on both sites.	**Datastore.Browse datastore** **Datastore.Low level file operations**	Datastore objects on target site, or datastore folder with propagation at target site, or target datacenter with propagation.
VRM virtual machine recovery user	Recover virtual machines.	**Datastore.Browse datastore** **Datastore.Low level file operations** **Host.vSphere Replication.Manage replication** **Virtual machine.Configuration.Add existing disk** **Virtual machine.Configuration.Add or remove device** **Virtual machine.Interaction.Power On** **Virtual machine.Interaction.Device connection** **Virtual machine.Inventory.Register** **Resource.Assign virtual machine to resource pool**	Secondary vCenter Server root folder with propagation. Alternatively, secondary vCenter Server root folder without propagation, target datastore without propagation, target virtual machine folder with propagation, target host or cluster with propagation.

Configure Replication

VMware Site Recovery uses vSphere Replication to protect individual virtual machines and their virtual disks by replicating them from one vCenter Server instance to another. With this procedure you can add the virtual machines to protection groups and recovery plans.

When you configure replication, you set a recovery point objective (RPO) to determine the maximum data loss that you can tolerate. For example, an RPO of 1 hour seeks to ensure that a virtual machine loses the data for no more than 1 hour during the recovery. For smaller RPO values, less data is lost in a recovery, but more network bandwidth is consumed keeping the replica up to date. The RPO value affects replication scheduling, but vSphere Replication does not adhere to a strict replication schedule. See How the Recovery Point Objective Affects Replication Scheduling and How the 5 Minute Recovery Point Objective Works.

Every time that a virtual machine reaches its RPO target, vSphere Replication records approximately 3800 bytes of data in the vCenter Server events database. If you set a low RPO period, this can quickly create a large volume of data in the database. To reduce the volume of data that is kept in the vCenter Server events database, limit the number of days that vCenter Server retains event data. See Configure Database Retention Policy in the *vCenter Server and Host Management Guide*. Alternatively, set a higher RPO value.

vSphere Replication guarantees crash consistency amongst all the disks that belong to a virtual machine. If you use quiescing, you might obtain a higher level of consistency. The available quiescing types are determined by the operating system of the virtual machine. See Compatibility Matrices for vSphere Replication 8.0 for quiescing support for Windows and Linux virtual machines.

You can configure virtual machines to replicate from and to Virtual SAN datastores. See Using vSphere Replication with VMware vSAN Storage for the limitations when using vSphere Replication with Virtual SAN.

Prerequisites

- Verify that the vSphere Replication appliance is deployed at the source and the target sites.
- Verify that the vSphere Replication appliances are paired.
- To enable the quiescing of virtual machines that run Linux guest OS, install the latest version of VMware Tools on each Linux machine that you plan to replicate.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Replications** tab, and click **New** to configure replication.
4. Select the virtual machines you want to replicate and click **Next.**
5. Accept the automatic assignment of a vSphere Replication server or select a particular server on the target site and click **Next**.
6. On the Target datastore page, select a datastore on which to replicate files and click **Next.**.

   When replicating multiple virtual machines, you can configure a different target datastore for each virtual machine.
7. On the Replication settings page, use the RPO slider to set the acceptable period for which data can be lost in the case of a site failure.

   The available RPO range is from 5 minutes to 24 hours.
8. (Optional) Select the quiescing method for the guest operating system of the source virtual machine.

   Note Quiescing options are available only for virtual machines that support quiescing. vSphere Replication does not support VSS quiescing on Virtual Volumes.
9. (Optional) Select **Enable network compression for VR data**.

   Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

10 (Optional) On the Protection group page, you can optionally add the virtual machine to a protection group.

Option	Description
Add to existing protection group	Adds the virtual machine to an existing protection group.
Add to new protection group	Adds the virtual machine to a new protection group. If you select this option, you must enter protection group name.
Do not add to protection group now	Select this option if you do not want to add the virtual machine to a protection group.

11 (Optional) On the Recovery plan page, you can optionally add the protection group to a recovery plan.

Option	Description
Add to existing recovery plan	Adds the protection group to an existing recovery plan.
Add to new recovery plan	Adds the protection group to a new recovery plan. If you select this option, you must enter recovery plan name.
Do not add to recovery plan now	Select this option if you do not want to add the protection group to a recovery plan.

12 On the Ready to complete page, review your settings, and click **Finish**.

Stop Replicating a Virtual Machine

If you do not need to replicate a virtual machine, you can stop the replication of that virtual machine.

Take a note of the target datastore and the name of the replication that you are about to stop. You need this information to clean up your environment after you stop the replication.

Prerequisites

Verify that you are logged in the vSphere Web Client as a VRM virtual machine replication user or a VRM administration user. See vSphere Replication Roles Reference.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 In the **Replications** tab, click **Forward Replications** or **Reverse Replications**.

4 Right-click a replication and select **Remove**.

vSphere Replication asks you if you want to permanently stop the replication for the selected virtual machine.

Note The hosts and vSphere Replication server used by the replication must be accessible to stop a replication on both sites. If a host or the server is not accessible, you can force stop the replication on the accessible site by selecting **Force stop replication**. If you force stop the replication from **Forward Replications**, you must also force stop the corresponding replication from **Outgoing Replications** if the source site is available. If you force stop the replication from **Reverse Replications**, you can only force stop the corresponding replication from **Incoming Replications**.

5 Click **Remove** to confirm that you want to stop replicating this virtual machine.

The virtual machine does not replicate to the target site.

When you stop a replication, the following operation is performed at the replication target site.

- VMDK files are deleted from the target site datastore if the VMDK files were created when the replication was first configured.

Note When you stop a replication, vSphere Replication does not delete the replica directory at the target datastore. As a result, stale directories remain on VMFS and NFS target datastores, and unused namespaces remain on Virtual SAN and Virtual Volume target datastores. Because the maximum number of directories and namespaces on a datastore is limited, you must manually clean them up to free resources on the datastore. See Clean Up the Target Datastore After You Stop a Replication.

Clean Up the Target Datastore After You Stop a Replication

When you stop a replication, vSphere Replication does not delete the replica directory at the target datastore.

As a result, stale directories remain on VMFS and NFS target datastores, and unused namespaces remain on Virtual SAN and Virtual Volume target datastores. Because the maximum number of directories and namespaces on a datastore is limited, you must manually clean them up to free resources on the datastore.

Prerequisites

Verify that you know the name of the replication that was stopped and its target datastore.

Procedure

1 Log in to the vSphere Web Client as and administrator user and navigate to the datastore that was the target for the stopped replication.

2 Enter the name of the stopped replication in the search text box and locate the folder that corresponds to this name.

3 Verify that the folder is empty and delete it.

Reconfiguring Replications

You can reconfigure a replication to modify its settings.

For example, you can reconfigure the replication to enable or disable a virtual machine disk file for replication, modify replication options, such as RPO or quiescing method.

To reconfigure replication parameters, select the replication from **Forward replications** or **Reverse replications**, and select **Reconfigure**.

Reconfigure Recovery Point Objective (RPO) in Replications

You can modify the settings for already configured replications to specify different recovery point objectives (RPOs).

Procedure

1. On the VMware Site Recovery home tab, select a site pair and click **Open**.
2. Click the **Replications** tab, and click **Forward replications** or **Reverse replications**. Right-click a replication and select **Reconfigure**.

   You might be prompted to provide login credentials for the target site.
3. Click **Next** until you reach **Replication settings**.
4. Modify the RPO settings for this replication and click **Next**.
5. Click **Finish** to save your changes.

Change the Target Datastore Location of a Replication

You can reconfigure a replication to change the datastore where replicated data is saved.

Note The old target datastore from which you want to move the replication data must be online. If the old datastore is inaccessible, the reconfiguration task fails. To change the target datastore when the old datastore is inaccessible, you must stop the replication to the old datastore and configure another replication to the new datastore.

Procedure

1. On the VMware Site Recovery home tab, select a site pair and click **Open**.
2. Click the **Replications** tab and click **Forward replications** or **Reverse replications**.
3. Right-click the replication for which you want to change the target datastore and select **Reconfigure**.

   The reconfiguration wizard open. You might be prompted to provide login credentials for the target site.
4. Click **Next** to reach the Target datastore page of the wizard.
5. Select **Change datastore**, and select the new datastore.

6 Click **Next** until you reach the Ready to complete page and click **Finish** to save your settings.

vSphere Replication moves all replicated instances and configuration files to the new target datastore according to your settings.

Replication States for Virtual Machines

vSphere Replication shows the replication states of virtual machines that you configured for replication.

State	Details for Each State
OK	OK, Moving, Recovering
Warning	Paused, OK(RPO violation), Not Active, Not Active(RPO violation), FullSync(RPO violation), Sync(RPO violation)
In Progress	FullSync, Sync, Initial Full Sync, Configuring
Error	Error, Error(RPO violation)
Recovered	Recovered

Note If a replication is in the Not Active replication state, you might have connected the source and target sites using network address translation (NAT). vSphere Replication does not support NAT. Use credential-based authentication and network routing without NAT when connecting the sites. Another cause for a Not Active replication state might be that the source virtual machine is powered off. Automatic replication works only on virtual machines that are powered on.

Monitor Replication for Virtual Machines

You can monitor the replication status and view information for virtual machines configured for replication.

For more information about how to identify replication errors, see Identifying Replication Problems in the Issues Tab.

Prerequisites

- Verify that vSphere Replication is running.
- Verify that the virtual machines are configured for replication.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 Select the **Replications** tab.

4 Select **Forward Replications** to see details of the virtual machines replicated from this site.

5 Select **Reverse Replications** to see details of the virtual machines replicated to this site.

According to the status of a selected replication, you can perform different actions on the replication.

Identifying Replication Problems in the Issues Tab

You can view and troubleshoot possible vSphere Replication problems that might occur during replication at the **Issues** tab of the corresponding Site Pair.

Table 2-2. Possible Replication Problems

Problem	Cause	Solution
Not Active	The replication is not active because the virtual machine is powered off and a warning icon appears. Replication is not running for that virtual machine.	Power on the virtual machine to resume replication.
Paused	If you paused the replication, a warning icon appears.	Resume the paused replication from the **Issues** tab.
Error	If you added a disk on a virtual machine which is already configured for replication, the replication pauses and goes to an error state.	Reconfigure the replication and enable or disable the newly added disk.
Error	While configuring replication, the replication fails with the incorrect UUID. For example, the replication seed found and intended for use has a different UUID from the original hard disk.	Reconfigure the replication.
Error	You do not use replication seeds during configuration, but a disk with the same name is found during configuration.	Reconfigure the replication.
RPO Violation	A replication contains an RPO violation.	See Change vSphere Replication Settings.

Configuring Mappings

3

Mappings allow you to specify how Site Recovery Manager maps virtual machine resources on the protected site to resources on the recovery site.

You can configure site-wide mappings to map objects in the vCenter Server inventory on the protected site to corresponding objects in the vCenter Server inventory on the recovery site.

- Networks, including the option to specify a different network to use for recovery plan tests
- Datacenters or virtual machine folders
- Compute resources, including resource pools, standalone hosts, vApps, or clusters

During a recovery, when virtual machines start on the recovery site, the virtual machines use the resources on the recovery site that you specify in the mappings. To enable bi-directional protection and reprotect, you can configure reverse mappings, to map the objects on the recovery site back to their corresponding objects on the protected site. You can also configure different mappings in the opposite direction, so that recovered virtual machines on a site use different resources to protected virtual machines on that site.

This chapter includes the following topics:

Inventory Mappings for vSphere Replication Protection Groups

For vSphere Replication protection, Site Recovery Manager applies inventory mappings to all virtual machines in a protection group when you create that group.

Site Recovery Manager creates a placeholder virtual machine when you create a vSphere Replication protection group. Site Recovery Manager derives the resource assignments for the placeholder from the site-wide inventory mappings.

If you configure site-wide inventory mappings, you can reapply the inventory mappings to a protection group whenever necessary, for example if you add new virtual machines to an existing protection group.

If you change the site-wide inventory mappings for a site, the changes do not affect virtual machines that Site Recovery Manager already protects in an existing protection group. Site Recovery Manager only applies the new mappings to previously protected virtual machines if you reconfigure protection on them.

Site Recovery Manager cannot protect a virtual machine unless it has valid inventory mappings. However, configuring site-wide inventory mappings is not mandatory for vSphere Replication protection groups. If you create a vSphere Replication protection group without having defined site-wide inventory mappings, you can configure each virtual machine in the group individually. You can override site-wide inventory mappings by configuring the protection of the virtual machines in a protection group. You can also create site-wide inventory mappings after you create a protection group, and then apply those site-wide mappings to that protection group.

- For information about configuring site-wide inventory mappings, see Configure Inventory Mappings.
- For information about configuring mappings on virtual machines individually, see Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group.
- For information about applying site-wide inventory mappings to an existing protection group, see Apply Inventory Mappings to All Members of a Protection Group.

Because placeholder virtual machines do not support NICs, you cannot change the network configurations of placeholder virtual machines. You can only change the network for a placeholder virtual machine in the inventory mappings. If no mapping for a network exists, you can specify a network when you configure protection for an individual virtual machine. Changes that you make to the placeholder virtual machine override the settings that you establish when you configure the protection of the virtual machine. Site Recovery Manager preserves these changes at the recovery site during the test and recovery.

Configure Inventory Mappings

Inventory mappings provide default objects in the inventory on the recovery site for the recovered virtual machines to use when you run recovery.

For vSphere Replication protection, if you configure site-wide inventory mappings before you create protection groups, you do not have to configure protection individually on each virtual machine when you create a protection group. Site Recovery Manager applies the site-wide mappings to all virtual machines in a vSphere Replication protection group at the moment that you create the protection group.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 On the left-hand pane expand **Configure**, and select the type of resource to configure.

Option	Action
Network Mappings	Map networks on the protected site to networks on the recovery site.
Folder Mappings	Map datacenters or virtual machine folders on the protected site to datacenters or virtual machine folders on the recovery site.
Resource Mappings	Map resource pools, standalone hosts, vApps, or clusters on the protected site to resource pools, standalone hosts, vApps, or clusters on the recovery site. You can map any type of resource on one site to any type of resource on the other site. **Note** You cannot map individual hosts that are part of clusters to other resource objects.

4 Click **New** to create a new mapping.

5 Select whether to create the mapping automatically or manually and click **Next**.

This step only applies to network mappings and folder mappings. Automatic mapping is only available for network and folder mappings. You must configure resource mappings manually.

Option	Description
Automatically	Site Recovery Manager automatically maps networks and folders on the protected site to networks and folders on the recovery site that have the same name.
Manually	To map specific networks and folders on the protected site to specific networks, folders, and resources on the recovery site.

6 Select the items on the protected site to map to items on the recovery site.

- If you selected automatic mapping, expand the inventory items on the left to select a parent node on the local site, for example a datacenter or a folder, then expand the inventory items on the right to select a parent node on the remote site.
- If you selected manual mapping, expand the inventory items on the left to select a specific object on the local site, then expand the inventory items on the right to select the object on the remote site to which to map this object.

If you select manual mapping, you can map multiple items on the local site to a single item on the remote site. You can select only one item at a time on the remote site.

7 Click **Add mappings**.

The mappings appear at the bottom of the page. If you selected automatic mapping, Site Recovery Manager automatically maps all of the items under the node that you selected on the protected site to items that have the same name under the node that you selected on the recovery site.

8 Click **Next**.

9 (Optional) On the **Reverse mappings** page, select the check box for a mapping.

Selecting this option creates corresponding mappings from the item on the remote site to the item on the local site. You require reverse mappings to establish bidirectional protection and to run reprotect operations.

10 (Optional) If you are configuring network mappings, in the **Test networks** page, click the network in the Test Network column and use the drop-down menu to select the network to use when you test recovery plans.

You can configure Site Recovery Manager to create an isolated network on the recovery site for when you test a recovery plan. Creating an isolated test network allows the test to proceed without adding extra traffic on the production network on the recovery site.

- Select **Isolated network (auto created)** to automatically create an isolated network on the recovery site to use for tests. This is the default option.
- Select an existing network on the recovery site to use for tests.

11 Click **Finish** to create the mappings.

12 Repeat Step 3 through Step 11 to establish mappings for the remaining resource types.

About Placeholder Virtual Machines

4

When you create a vSphere Replication protection group that contains individual virtual machines, Site Recovery Manager creates a placeholder virtual machine at the recovery site for each of the virtual machines in the protection group.

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

The files of the placeholder virtual machines are very small, and do not represent full copies of the protected virtual machines. The placeholder virtual machine does not have any disks attached to it. The placeholder virtual machine reserves compute resources on the recovery site, and provides the location in the vCenter Server inventory to which the protected virtual machine recovers when you run recovery.

The presence of placeholder virtual machines on the recovery site inventory provides a visual indication to vCenter Server administrators that the virtual machines are protected by Site Recovery Manager. The placeholders also indicate to vCenter Server administrators that the virtual machines can power on and start consuming local resources when Site Recovery Manager runs tests or runs a recovery plan.

When you recover a protected virtual machine by testing or running a recovery plan, Site Recovery Manager replaces the placeholder with the recovered virtual machine and powers it on according to the settings of the recovery plan. After a recovery plan test finishes, Site Recovery Manager restores the placeholders and powers off the recovered virtual machines as part of the cleanup process.

About Placeholder Datastores

If you use vSphere Replication to protect individual virtual machines, you must identify a datastore on the recovery site in which Site Recovery Manager can store the placeholder virtual machine files.

Placeholder virtual machine files are very small, so the placeholder datastore does not need to be large enough to accommodate the full virtual machines.

To enable planned migration and reprotect, you must select placeholder datastores on both sites.

This chapter includes the following topics:

What Happens to Placeholder Virtual Machines During Recovery

When you create vSphere Replication protection groups, Site Recovery Manager creates placeholder virtual machines on the recovery site. When you run a recovery plan that contains these protection groups, Site Recovery Manager replaces the placeholders with real virtual machines.

This example illustrates the process by which Site Recovery Manager replaces placeholder virtual machines on the recovery site with real virtual machines when you run recovery plans that contain vSphere Replication protection groups.

1 vSphere Replication replicates individual virtual machines by making copies of the virtual machines in the datastore that you configure as the vSphere Replication target. These virtual machine copies are not powered on.

2 You designate a datastore on the recovery site for Site Recovery Manager to use to store placeholder virtual machine files.

3 When you run a recovery plan, Site Recovery Manager shuts down the virtual machines on the protected site, and vSphere Replication powers on the copies of the virtual machines on the recovery site.

4 Site Recovery Manager sends a request to vCenter Server to swap the identity of the placeholder virtual machines for the replicated virtual machines that have surfaced on the recovery site.

Select a Placeholder Datastore

If you use vSphere Replication protection groups, you must specify a placeholder datastore on the recovery site for Site Recovery Manager to use to store placeholder virtual machines.

You must configure a placeholder datastore on both sites in the pair to establish bidirectional protection and to perform reprotect.

Prerequisites

- Verify that you connected and paired the protected and recovery sites.
- Placeholder datastores must meet certain criteria.
  - For clusters, the placeholder datastores must be visible to all hosts in the cluster.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 On the **Site Pair** tab, select **Configure > Placeholder Datastores**.

4 Select a site and click **New** to configure a placeholder datastore.

5 Select a datastore to designate as the location for placeholder virtual machines on the local site, and click **Add**.

Previously configured datastores appear but you cannot select them. Do not select replicated datastores that Site Recovery Manager does not manage.

Important If you use vSphere Replication, you can select a placeholder datastore that you already use as the target datastore for replications. If you use the same datastore, Site Recovery Manager creates placeholder VMs by using the names of the replication targets and adding the suffix (1). For information about the vSphere Replication protection groups, see vSphere Replication Protection Groups. Selecting the same datastore might lead to confusion when differentiating the replication targets from the placeholder VMs. To avoid confusion, the best practice is to use different datastores.

Make sure that placeholder datastores are not in the same Storage DRS cluster as the vSphere Replication replica target datastores.

Note When you configure or reconfigure a VM replication by using vSphere Replication, do not set the placeholder VM folder as a replication folder for the VM.

6 Select the other site in the pair.

7 Repeat Step 4 to Step 5 to configure a placeholder datastore on the other site.

Creating and Managing Protection Groups

5

After you configure a replication solution, you can create protection groups. A protection group is a collection of virtual machines that Site Recovery Manager protects together.

You can include one or more protection groups in a recovery plan. A recovery plan specifies how Site Recovery Manager recovers the virtual machines in the protection groups that it contains.

After you configure replication on virtual machines, you must assign each virtual machine to an existing resource pool, folder, and network on the recovery site. You can specify site-wide defaults for these assignments by selecting inventory mappings. For vSphere Replication protection groups, if you do not specify inventory mappings, you configure mappings individually for each virtual machine in the protection group.

After you create a vSphere Replication protection group, Site Recovery Manager creates placeholder virtual machines on the recovery site and applies the inventory mappings to each virtual machine in the group. If Site Recovery Manager cannot map a virtual machine to a folder, network, or resource pool on the recovery site, Site Recovery Manager sets the virtual machine to the Mapping Missing status, and does not create a placeholder for it.

Site Recovery Manager cannot protect virtual machines on which you did not configure or on which you incorrectly configured replication.

This chapter includes the following topics:

vSphere Replication Protection Groups

You can include virtual machines that you configured for vSphere Replication in vSphere Replication protection groups.

Virtual machines in the vCenter Server inventory that are configured for vSphere Replication are available for selection when you create or edit a vSphere Replication protection group.

You select a target location on a datastore on the remote site when you configure vSphere Replication on a virtual machine. When you include a virtual machine with vSphere Replication in a protection group, Site Recovery Manager creates a placeholder virtual machine for recovery. It is possible for the replication target for vSphere Replication and the placeholder virtual machine that Site Recovery Manager creates to both be on the same datastore on the recovery site because they are created in different datastore folders. When the replication target and the placeholder virtual machines are in the same datastore, Site Recovery Manager creates the placeholder virtual machine name by using the replication target name with the suffix `(1)`. To avoid confusion, the best practice is to use different datastores for the vSphere Replication replication target and for the Site Recovery Manager placeholder virtual machines. Site Recovery Manager applies the inventory mappings to the placeholder virtual machine on the recovery site.

Note When you configure or reconfigure a VM replication by using vSphere Replication, do not set the placeholder VM folder as a replication folder for the VM.

vSphere Replication synchronizes the disk files of the replication target virtual machine according to the recovery point objective that you set when you configured vSphere Replication on the virtual machine. When you perform a recovery with Site Recovery Manager, Site Recovery Manager powers on the replication target virtual machine and registers it with vCenter Server on the recovery site in the place of the placeholder virtual machine.

When using vSphere Replication protection groups, Site Recovery Manager is dependent on vSphere Replication, but vSphere Replication is not dependent on Site Recovery Manager. You can use vSphere Replication independently of Site Recovery Manager. For example, you can use vSphere Replication to replicate all of the virtual machines in the vCenter Server inventory, but only include a subset of those virtual machines in protection groups. Changes that you make to vSphere Replication configuration can affect the Site Recovery Manager protection of the virtual machines that you do include in protection groups.

- Site Recovery Manager monitors the vSphere Replication status of the virtual machines in vSphere Replication protection groups. If replication is not functioning for a virtual machine in a protection group, Site Recovery Manager cannot recover the virtual machine.
- If you unconfigure vSphere Replication on a virtual machine, Site Recovery Manager continues to include that virtual machine in protection groups in which you included it. Site Recovery Manager cannot recover that virtual machine until you reconfigure replication. If you unconfigure vSphere Replication on a virtual machine, you can remove it from the protection group manually.

If you remove a virtual machine with vSphere Replication from a protection group, vSphere Replication continues to replicate the virtual machine to the recovery site. The virtual machine does not recover with the rest of the virtual machines in the protection group if you run an associated recovery plan.

Create Protection Groups

You create protection groups to enable Site Recovery Manager to protect virtual machines.

You can organize protection groups in folders. Ensure that protection group names are unique across all folders.

When you create protection groups, wait to ensure that the operations finish as expected. Make sure that Site Recovery Manager creates the protection group and that the protection of the virtual machines in the group is successful.

Prerequisites

- Verify that you have configured vSphere Replication on virtual machines

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Protection Groups** tab, and click **New** to create a protection group.
4. On the Name and direction page, enter a name and description for the protection group, select a direction, and click **Next**.
5. Select virtual machines to add to the protection group, and click **Next**.
6. On the Recovery plan page, you can optionally add the protection group to a recovery plan.

Option	Description
Add to existing recovery plan	Adds the protection group to an existing recovery plan.
Add to new recovery plan	Adds the protection group to a new recovery plan. If you select this option, you must enter recovery plan name.
Do not add to recovery plan now	Select this option if you do not want to add the protection group to a recovery plan.

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

   You can monitor the progress of the creation of the protection group on the **Protection Group** tab.

What to do next

For vSphere Replication protection groups, if the protection status of the protection group is Not Configured, apply inventory mappings to the virtual machines:

- To apply site-wide inventory mappings, or to check that inventory mappings that you have already set are valid, see Configure Inventory Mappings. To apply these mappings to all of the virtual machines, see Apply Inventory Mappings to All Members of a Protection Group.

- To apply inventory mappings to each virtual machine in the protection group individually, see Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group.

Organize Protection Groups in Folders

You can create folders in which to organize protection groups.

Organizing protection groups into folders is useful if you have many protection groups.

Procedure

1. On the VMware Site Recovery home tab, select a site pair and click **Open**.
2. Select the **Protection Groups** tab, and in the left pane right-click on **Protection Groups** and select **New Folder**.
3. Enter a name for the folder to create, and click **Add**.
4. Add new or existing protection groups to the folder.

Option	Description
Create a new protection group	Right-click the folder and select **New Protection Group**.
Add an existing protection group	Right-click on a protection group from the inventory tree and select **Move**. Select a target folder and click **Move**.

5. (Optional) To rename or delete a folder, right-click the folder and select **Rename Folder** or **Delete Folder**.

   You can only delete a folder if it is empty.

Add or Remove Virtual Machines to or from a Protection Group

You can add or remove virtual machines in a vSphere Replication protection group. You can also change the name and description of a vSphere Replication protection group.

Prerequisites

You created a vSphere Replication protection group.

Procedure

1. On the VMware Site Recovery home tab, select a site pair and click **Open**.
2. Select the **Protection Groups** tab, right-click a protection group and select **Edit**.
3. (Optional) Change the name or description of the protection group and click **Next**.

   You cannot change the Direction or Location settings.
4. Modify the virtual machines that the protection group contains.
   - For vSphere Replication protection groups, select or deselect virtual machines to add them to or remove them from the protection group, and click **Next**.

5 Review the settings and click **Finish** to apply the settings.

You cannot revert or cancel the changes while Site Recovery Manager updates the protection group.

If you configured site-wide inventory mappings, Site Recovery Manager applies the mappings to the virtual machines that you added to the protection group. If successful, the status for the virtual machines is OK.

If you have not configured site-wide inventory mappings, the status for the protection group is Not Configured and the status for the new virtual machines is Mapping Missing.

What to do next

If the status of the protection group is Not Configured and the status for the new virtual machines is Mapping Missing, apply inventory mappings to the virtual machines:

- To apply site-wide inventory mappings, or to check that inventory mappings that you have already set are valid, see Configure Inventory Mappings. To apply these mappings to all of the virtual machines, see Apply Inventory Mappings to All Members of a Protection Group.
- To apply inventory mappings to each virtual machine in the protection group individually, see Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group.

Apply Inventory Mappings to All Members of a Protection Group

If the status of a vSphere Replication protection group is Not Configured, you can configure protection for all of the unconfigured virtual machines by using existing site-wide inventory mappings, in one step.

Site Recovery Manager applies site-wide inventory mappings to virtual machines in vSphere Replication protection groups when you create the protection group. If you change the site-wide inventory mappings after you create a vSphere Replication protection group or add virtual machines to a vSphere Replication protection group, the virtual machines continue to recover with the original inventory mappings. To apply new inventory mappings, you must reconfigure protection on the virtual machines in the protection group.

The status of a protection group can be Not Configured for several reasons:

- You did not configure site-wide inventory mappings before you created the protection group.
- You did not configure placeholder datastore mappings before you created the protection group.
- You added virtual machines to a protection group after you created it.
- Virtual machines lost their protection, possibly because you reconfigured them after you added them to a protection group. For example, you added or removed virtual disks or devices.

Prerequisites

- Configure or reconfigure site-wide inventory mappings. To select inventory mappings, see Configure Inventory Mappings.
- Configure or reconfigure placeholder datastore mappings. To configure a placeholder datastore, see Select a Placeholder Datastore.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Protection Groups** tab, select a protection group, and on the right pane, click the **Virtual Machines** tab.
4. Click the **Configure All VMs** icon.

   At least one virtual machine in the protection group must be in the Not Configured state for the **Configure All VMs** button to be activated.

   - If Site Recovery Manager successfully applied inventory mappings to the virtual machines, the status of the protection group is OK.
   - If Site Recovery Manager was unable to apply some or all of the inventory mappings, the status of the virtual machines is Not Configured or Mapping Missing.
   - If Site Recovery Manager applied the inventory mappings, but was unable to create placeholders for virtual machines, the status of the virtual machines is Placeholder VM creation error.
5. (Optional) If the status of the virtual machines is Not Configured or Mapping Missing, check the inventory mappings and click **Configure All VMs** again.
6. (Optional) If the status of the virtual machines is Placeholder VM creation error, check the placeholder datastore mapping and try to recreate the placeholder virtual machines.
   - To recreate the placeholder for an individual virtual machine, right-click a virtual machine and select **Recreate Placeholder**.
   - To recreate the placeholder for several virtual machines, right-click the protection group and select **Restore All Placeholder VMs**.

Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group

You can configure the mappings for the virtual machines in a vSphere Replication protection group individually. This ability allows you to use different resources on the recovery site for different virtual machines.

You can configure individual inventory mappings on virtual machines in a vSphere Replication protection group even if you configured site-wide inventory mappings. If you did configure site-wide inventory mappings, you can remove protection from an individual virtual machine and configure the folder and resource mappings to override the site-wide mappings. You can change the network mapping for an individual virtual machine without removing protection.

Prerequisites

You created a vSphere Replication protection group.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Protection Groups** tab, and select the protection group that includes the virtual machine to configure.
4. On the right pane, click the **Virtual Machines** tab.
5. Right-click the virtual machine and select **Configure Protection**.
6. Configure inventory mappings by expanding the resources, selecting the **Override site mappings** checkbox, and selecting resources on the recovery site.

   You can only change the folder, resource pool, and network mappings.
7. Click **OK**.
   - If Site Recovery Manager successfully applied inventory mappings to the virtual machine, the status of the virtual machine is OK.
   - If Site Recovery Manager was unable to apply some or all of the inventory mappings, the status of the virtual machine is Not Configured or Mapping Missing.
   - If Site Recovery Manager applied the inventory mappings but was unable to create a placeholder virtual machine, the status of the virtual machine is Placeholder VM creation error.
8. (Optional) If the status of the virtual machine is Not Configured or Mapping Missing, select **Configure Protection** again and check the inventory mappings.
9. (Optional) If the status of the virtual machine is Placeholder VM creation error, check the placeholder datastore mapping at the site level, right-click the virtual machine, and select **Recreate Placeholder**.

Modifying the Settings of a Protected Virtual Machine

Modifying the settings of a virtual machine that is included in a protection group, to add or change storage devices, such as hard disks or DVD drives, can affect the protection of that virtual machine.

If you add a device to a virtual machine that you protect by using vSphere Replication, you must reconfigure vSphere Replication on the virtual machine to select the replication options for the new device. For information about reconfiguring vSphere Replication settings, see Reconfiguring Replications.

After you modify virtual machines in a vSphere Replication protection group, you must reconfigure protection for any virtual machines that have a status of Not Configured, Device Not Found, Unresolved Devices, or Mapping Missing. See Apply Inventory Mappings to All Members of a Protection Group and Configure Inventory Mappings for an Individual Virtual Machine in a Protection Group.

Remove Protection from a Virtual Machine

You can temporarily remove protection from a replicated virtual machine in a vSphere Replication protection group without removing it from its protection group.

Removing protection deletes the placeholder virtual machine on the recovery site. If you remove protection from a virtual machine in a vSphere Replication protection group, the states of the virtual machine and the protection group are set to Not Configured. Running a recovery plan that contains the protection group succeeds for the protected virtual machines, but Site Recovery Manager does not recover the virtual machines or protection groups that are in the Not Configured state. If you ran planned migration, the plan enters the Recovery Incomplete state.

You might remove protection from a virtual machine when you want to exclude a protected virtual machine from a protection group.

If you disable vSphere Replication on a virtual machine that you included in a protection group, recovery fails for this virtual machine but succeeds for all of the correctly configured virtual machines in the protection group. You must remove protection from the virtual machine and remove the virtual machine from the protection group, either by editing the protection group or by clicking **Remove VM**. See Add or Remove Virtual Machines to or from a Protection Group.

Procedure

1. On the VMware Site Recovery home tab, select a site pair and click **Open**.
2. Select the **Protection Groups** tab, select a protection group, and on the right pane, click the **Virtual Machines** tab.
3. Right-click a virtual machine and select **Remove Protection**.
4. Click **Yes** to confirm the removal of protection from the virtual machine.

Protection Group Status Reference

You can monitor the status of a protection group and determine the operation that is allowed in each state.

Table 5-1. Protection Group States

State	Description
Loading	Appears briefly while the interface is loading until the protection group status appears.
OK	Group is idle. All virtual machines are in OK state. You can edit the group.
Not Configured	Group is idle. Some virtual machines might not be in OK state. You can edit the group.
Testing	Group is used in a plan running a test. You cannot edit the group.
Test Complete	Group is used in a plan running a test. You cannot edit the group. Group returns to the OK or Not Configured state when cleanup is successful.
Cleaning Up	Group is used in a plan that is cleaning up after a test. You cannot edit the group. Group returns to the OK or Not Configured state when cleanup is successful. If cleanup fails, the group goes to the Testing state.

Table 5-1. Protection Group States (Continued)

State	Description
Recovering	Group is used in a plan that is running a recovery. You cannot edit the group. If recovery succeeds, the group goes to Recovered state. If recovery fails, group status changes to Partially Recovered.
Partially Recovered	Group is in a plan that completed a recovery, but recovery failed for some virtual machines. You can remove virtual machines, but cannot configure or restore them.
Recovered	Group is in a plan that successfully completed a recovery. You can remove virtual machines, but cannot configure or restore them.
Reprotecting	Group is used in a plan running reprotect. You cannot edit the group. Group returns to OK or Not Configured state when reprotect is successful. If reprotect fails, the group goes to Partially Reprotected state.
Partially Reprotected	The group is in a plan that failed a reprotect. You can remove virtual machines, but cannot configure or restore them.
Configuring Protection	Protection operations are in progress on virtual machines in the group.
Removing Protection	Removing protection from virtual machines in the group is in progress.
Restoring Placeholders	Creation of placeholders is in progress for virtual machines in the group.
Operations in Progress	A combination of at least one Configure Protection and one Remove Protection operations are in progress in the group.

Virtual Machine Protection Status Reference

You can monitor the status of a virtual machine in a protection group and determine the operation that is allowed in each state.

Table 5-2. Virtual Machine Protection States

State	Description
Placeholder VM Not Found	You deleted the placeholder virtual machine. The Restore Placeholder icon is enabled.
Original protected VM not found	You deleted the original production virtual machine after failover and before reprotect. The Restore Placeholder icon is enabled.
Mapping missing: Folder *name*; Network *name* ; Resource pool *name*	Folder, resource pool, or network mappings are not configured for this VM. Fix the inventory mappings for the site or manually configure the virtual machine.
Placeholder VM creation error: *error string from server*	Error during placeholder virtual machine creation.
OK	The protected virtual machine exists, and both provider and placeholder status are clean.

Table 5-2. Virtual Machine Protection States (Continued)

State	Description
Invalid: *error*	The virtual machine is not valid because the home datastore is not replicated or the virtual machine has been deleted. The error string from the server contains the details. Remove protection from the virtual machine manually.
Not configured	You added a new virtual machine after creating the protection group. Use Configure All to configure protection on the virtual machine.
Error: *error*	Error can be one of the following: ■ Recovery site resource pool, folder, or network are not in the same datacenter. ■ Placeholder datastore not found. ■ Any vCenter Server error that occurred when creating placeholder, such as connection or permission problems.
Configuring protection	Virtual machine operation.
Removing protection	Virtual machine operation.
Restoring placeholder	Virtual machine operation.
Loading	Appears briefly while the interface is loading until the virtual machine status appears.
Mapping Conflict	Site Recovery Manager Server reported an inventory conflict. The resource pool and folder of the virtual machine are in different datacenters.
Replication Error	vSphere Replication reports an error about the virtual machine.
Replication Warning	vSphere Replication reports a warning about the virtual machine.

Creating, Testing, and Running Recovery Plans

6

After you configure Site Recovery Manager at the protected and recovery sites, you can create, test, and run a recovery plan.

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

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

You can run only one recovery plan at a time to recover a particular protection group. If you test or run a recovery plan with a replication group that is shared in other recovery plans, the other recovery plans change the state of the protection group to `Protection Group In Use` and you cannot run them.

This chapter includes the following topics:

Testing a Recovery Plan

When you create or modify a recovery plan, test it before you try to use it for planned migration or for disaster recovery.

By testing a recovery plan, you ensure that the virtual machines that the plan protects recover correctly to the recovery site. If you do not test recovery plans, an actual disaster recovery situation might not recover all virtual machines, resulting in data loss.

Testing a recovery plan exercises nearly every aspect of a recovery plan, although Site Recovery Manager makes several concessions to avoid disrupting ongoing operations on the protected and recovery sites. Recovery plans that suspend local virtual machines do so for tests as well as for actual recoveries. With this exception, running a test recovery does not disrupt replication or ongoing activities at either site.

If you use vSphere Replication, when you test a recovery plan, the virtual machine on the protected site can still synchronize with the replica virtual machine disk files on the recovery site. The vSphere Replication server creates redo logs on the virtual machine disk files on the recovery site, so that synchronization can continue normally. When you perform cleanup after running a test, the vSphere Replication server removes the redo logs from the disks on the recovery site and persists the changes accumulated in the logs to VM disks.

You can run test recoveries as often as necessary. You can cancel a recovery plan test at any time.

Before running a failover or another test, you must successfully run a cleanup operation. See Clean Up After Testing a Recovery Plan.

Permission to test a recovery plan does not include permission to run a recovery plan. Permission to run a recovery plan does not include permission to test a recovery plan. You must assign each permission separately. See Assign Site Recovery Manager Roles and Permissions.

Test Networks and Datacenter Networks

When you test a recovery plan, Site Recovery Manager can create a test network that it uses to connect recovered virtual machines. Creating a test network allows the test to run without potentially disrupting virtual machines in the production environment.

The isolated test network is managed by its own virtual switch, and in most cases recovered virtual machines can use the network without having to change network properties such as IP address, gateway, and so on. You use the isolated test network by selecting **Isolated network (auto created)** when you configure the test network settings while creating a recovery plan and there are no site-level mappings. An isolated test network does not span hosts. You must configure a test network for every network that a recovery plan uses during recovery.

You must recover any virtual machines that must interact with each other to the same test network. For example, if a Web server accesses information on a database, those Web server and database virtual machines should recover together to the same network.

A datacenter network is an existing network at the recovery site. You can select a datacenter network for use as a test network. To use it, recovered virtual machines must conform to its network address availability rules. These virtual machines must use a network address that the network's switch can serve and route, must use the correct gateway and DNS host, and so on. Recovered virtual machines that use DHCP can connect to this network without additional customization if the DHCP is properly configured. Other virtual machines might require IP customization and additional recovery plan steps to apply the customization.

Performing a Planned Migration or Disaster Recovery By Running a Recovery Plan

You can run a recovery plan under planned circumstances to migrate virtual machines from the protected site to the recovery site. You can also run a recovery plan under unplanned circumstances if the protected site suffers an unforeseen event that might result in data loss.

During a planned migration, Site Recovery Manager synchronizes the virtual machine data on the recovery site with the virtual machines on the protected site. Site Recovery Manager attempts to gracefully shut down the protected machines and performs a final synchronization to prevent data loss, then powers on the virtual machines on the recovery site. If errors occur during a planned migration, the plan stops so that you can resolve the errors and rerun the plan. You can reprotect the virtual machines after the recovery.

During disaster recoveries, Site Recovery Manager first attempts a storage synchronization. If it succeeds, Site Recovery Manager uses the synchronized storage state to recover virtual machines on the recovery site to their most recent available state, according to the recovery point objective (RPO) that you set when you configure your replication technology. When you run a recovery plan to perform a disaster recovery, Site Recovery Manager attempts to shut down the virtual machines on the protected site. If Site Recovery Manager cannot shut down the virtual machines, Site Recovery Manager still starts the copies at the recovery site. In case the protected site comes back online after disaster recovery, the recovery plan goes into an inconsistent state where production virtual machines are running on both sites, known as a split-brain scenario. Site Recovery Manager detects this state and allows you to run the plan once more to power off the virtual machines on the protected site. Then the recovery plan goes back to consistent state and you can run reprotect.

Site Recovery Manager uses VMware Tools heartbeat to discover when a virtual machine is running on the recovery site. In this way, Site Recovery Manager can ensure that all virtual machines are running on the recovery site. VMware Tools are also used to gracefully shutdown the guest operating system of protected virtual machines. For this reason, VMware recommends that you install VMware Tools on protected virtual machines. If you do not or cannot install VMware Tools on the protected virtual machines, you must configure Site Recovery Manager not to wait for VMware Tools to start in the recovered virtual machines and to skip the guest operating system shutdown step. See Change Recovery Settings.

After Site Recovery Manager completes the final replication, Site Recovery Manager makes changes at both sites that require significant time and effort to reverse. Because of this time and effort, you must assign the privilege to test a recovery plan and the privilege to run a recovery plan separately.

Running a Recovery with Forced Recovery

If the protected site is offline and Site Recovery Manager cannot perform its usual tasks in a timely manner which increases the RTO to an unacceptable level, you can run the recovery with the forced recovery option. Forced recovery starts the virtual machines on the recovery site without performing any operations on the protected site.

Caution Only use forced recovery in cases where the recovery time objective (RTO) is severely affected by a lack of connectivity to the protection site.

Forced recovery is for use in cases where infrastructure fails at the protected site and, as a result, protected virtual machines are unmanageable and cannot be shut down, powered off, or unregistered. In such a case, the system state cannot be changed for extended periods. To resolve this situation, you can force recovery. Forcing recovery does not complete the process of shutting down the virtual machines at the protected site. As a result, a split-brain scenario occurs, but the recovery might complete more quickly.

When running disaster recovery using vSphere Replication, Site Recovery Manager prepares vSphere Replication storage for reprotect and you do not have to verify mirroring.

To select forced recovery when running disaster recovery, you must enable the option `recovery.forceRecovery` in Advanced Settings on the Site Recovery Manager Server on the recovery site. That enables the option in the Run Recovery Plan wizard. You can only select the forced recovery option in disaster recovery mode. It is not available for planned migration.

After the forced recovery completes, you can resolve the issue that necessitated the forced recovery. After you resolve the underlying issue, run planned migration on the recovery plan again, resolve any problems that occur, and rerun the plan until it finishes successfully. Running the recovery plan again does not affect the recovered virtual machines at the recovery site.

Note When you run planned migration after running a forced recovery, virtual machines on the protected site might fail to shut down if the underlying datastores are read only or unavailable. In this case, log into vCenter Server on the protected site and power off the virtual machines manually. After you have powered off the virtual machines, run planned migration again.

Differences Between Testing and Running a Recovery Plan

Testing a recovery plan has no lasting effects on either the protected site or the recovery site, but running a recovery plan has significant effects on both sites.

You need different privileges when testing and running a recovery plan.

Table 6-1. How Testing a Recovery Plan Differs from Running a Recovery Plan

Area of Difference	Test a Recovery Plan	Run a Recovery Plan
Required privileges	Requires **Site Recovery Manager.Recovery Plans.Test** permission.	Requires **Site Recovery Manager.Recovery Plans.Recovery** permission.
Effect on virtual machines at protected site	None	Site Recovery Manager shuts down virtual machines in reverse priority order and restores any virtual machines that are suspended at the protected site.
Effect on virtual machines at recovery site	Site Recovery Manager suspends local virtual machines if the recovery plan requires this. Site Recovery Manager restarts suspended virtual machines after cleaning up the test.	Site Recovery Manager suspends local virtual machines if the recovery plan requires this.
Effect on replication	Site Recovery Manager creates temporary snapshots of replicated virtual machines at the recovery site.	During a planned migration, Site Recovery Manager synchronizes the replicated virtual machines, then stops replication, then makes the recovery site storage writable. During a disaster recovery, Site Recovery Manager attempts the same steps, but if they do not succeed, Site Recovery Manager ignores protected site errors.
Network	If you explicitly assign test networks, Site Recovery Manager connects recovered virtual machines to a test network. If virtual machine network assignment is **Isolated network (auto created)** and there are no site-level mappings, Site Recovery Manager assigns virtual machines to temporary networks that are not connected to any physical network.	Site Recovery Manager connects recovered virtual machines to the user-specified datacenter network.
Interruption of recovery plan	You can cancel a test at any time.	You can cancel the recovery at any time.

Performing Test Recovery of Virtual Machines Across Multiple Hosts on the Recovery Site

You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

With Site Recovery Manager, the vSwitches can be DVS based and span hosts. If you accept the default test network configured as **Isolated network (auto created)** and there are no site-level mappings, then virtual machines that are recovered across hosts are placed in their own test network during recovery plan tests. Each test switch is isolated between hosts. As a result, virtual machines in the same recovery

plan are isolated when the test recovery finishes. To allow the virtual machines to communicate, establish and select DVS switches or VLANs. With an isolated VLAN that connects all hosts to each other but not to a production network, you can more realistically test a recovery. To achieve connectivity among recovery hosts, but maintain isolation from the production network, follow these recommendations:

- Create DVS switches that are connected to an isolated VLAN that is private. Such a VLAN allows hosts and virtual machines to be connected, but to be isolated from production virtual machines. Use a naming convention that clearly designates that the DVS is for testing use, and select this DVS in the recovery plan test network column in the recovery plan editor.
- Create test VLANs on a physical network, providing no route back to the protected site. Trunk test VLANs to recovery site vSphere clusters and create virtual switches for test VLAN IDs. Use a clear naming convention to identify that these switches are for testing. Select these switches from the test recovery network column in the recovery plan editor.

Create, Test, and Run a Recovery Plan

You perform several sets of tasks to create, test, and run a recovery plan.

Create a Recovery Plan

You create a recovery plan to establish how Site Recovery Manager recovers virtual machines.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, and click **New** to create a recovery plan.
4. Enter a name, description and direction for the plan, select a folder, then click **Next**.
5. Select one or more protection groups for the plan to recover, and click **Next**.
6. From the **Test Network** drop-down menu, select a network to use during test recovery, and click **Next**.

   If there are no site-level mappings, the default option **Isolated network (auto created)** creates an isolated test network automatically.
7. Review the summary information and click **Finish** to create the recovery plan.

Organize Recovery Plans in Folders

You can create folders in which to organize recovery plans.

Organizing recovery plans into folders is useful if you have many recovery plans. You can limit the access to recovery plans by placing them in folders and assigning different permissions to the folders for different users or groups. For information about how to assign permissions to folders, see Assign Site Recovery Manager Roles and Permissions.

Procedure

1. On the VMware Site Recovery home tab, select a site pair and click **Open**.
2. Select the **Recovery Plans** tab, and in the left pane right-click on **Recovery Plans** and select **New Folder**.
3. Enter a name for the folder to create, and click **Add**.
4. Add new or existing recovery plans to the folder.

Option	Description
Create a new recovery plan	Right-click the folder and select **New Recovery Plan**.
Add an existing recovery plan	Right-click on a recovery plan from the inventory tree and select **Move**. Select a target folder and click **Move**.

5. (Optional) To rename or delete a folder, right-click the folder and select **Rename** or **Delete** .

   You can only delete a folder if it is empty.

Edit a Recovery Plan

You can edit a recovery plan to change the properties that you specified when you created it. You can edit recovery plans from the protected site or from the recovery site.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, right-click a recovery plan, and select **Edit Plan**.
4. (Optional) Change the name or description of the plan, and click **Next**.

   You cannot change the direction and the location of the recovery plan.
5. (Optional) Select or deselect one or more protection groups to add them to or remove them from the plan, and click **Next**.
6. (Optional) From the drop-down menu select a different test network on the recovery site, and click **Next**.
7. Review the summary information and click **Finish** to make the specified changes to the recovery plan.

   You can monitor the update of the plan in the Recent Tasks view.

Test a Recovery Plan

When you test a recovery plan, Site Recovery Manager runs the virtual machines of the recovery plan on a test network and on a temporary snapshot of replicated data at the recovery site.
Site Recovery Manager does not disrupt operations at the protected site.

Testing a recovery plan runs all the steps in the plan, except for powering down virtual machines at the protected site and forcing devices at the recovery site to assume mastership of replicated data. If the plan requires the suspension of local virtual machines at the recovery site, Site Recovery Manager suspends those virtual machines during the test. Running a test of a recovery plan makes no other changes to the production environment at either site.

Testing a recovery plan creates a snapshot on the recovery site of all of the disk files of the virtual machines in the recovery plan. The creation of the snapshots adds to the I/O latency on the storage. If you notice slower response times when you test recovery plans and you are using VMware Virtual SAN storage, monitor the I/O latency by using the monitoring tool in the Virtual SAN interface.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, right-click a recovery plan, and select **Test**.

   You can also run a test by clicking the **Test** icon in the **Recovery Steps** view of the recovery plan.
4. (Optional) Select **Replicate recent changes to recovery site**.

   Selecting this option ensures that the recovery site has the latest copy of protected virtual machines, but means that the synchronization might take more time.
5. Click **Next**.
6. Review the test information and click **Finish**.
7. Click the **Recovery Steps** tab in the recovery plan tab to monitor the progress of the test and respond to messages.

   The **Recovery Steps** tab displays the progress of individual steps. The Test task in Recent Tasks tracks overall progress.

What to do next

Run a cleanup operation after the recovery plan test finishes to restore the recovery plan to its original state from before the test.

Clean Up After Testing a Recovery Plan

After you test a recovery plan, you can return the recovery plan to the Ready state by running a cleanup operation. You must complete the cleanup operation before you can run a failover or another test.

Site Recovery Manager performs several cleanup operations after a test.

- Powers off the recovered virtual machines.
- Replaces recovered virtual machines with placeholders, preserving their identity and configuration information.
- Cleans up replicated storage snapshots that the recovered virtual machines used during the test.

Prerequisites

Verify that you tested a recovery plan.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, right-click a recovery plan, and select **Cleanup**.

   You can also run a test by clicking the **Cleanup** icon in the **Recovery Steps** view of the recovery plan.
4. Review the cleanup information and click **Next**.
5. Click **Finish**.
6. After the cleanup finishes, if it reports errors, run the cleanup again, selecting the **Force Cleanup** option.

   The **Force Cleanup** option forces the removal of virtual machines, ignoring any errors, and returns the plan to the Ready state. If necessary, run cleanup several times with the **Force Cleanup** option, until the cleanup succeeds.

Run a Recovery Plan

When you run a recovery plan, Site Recovery Manager migrates all virtual machines in the recovery plan to the recovery site. Site Recovery Manager attempts to shut down the corresponding virtual machines on the protected site.

Caution Running a recovery plan makes significant alterations in the configurations of the protected and recovery sites and it stops replication. Do not run any recovery plan that you have not tested. Reversing these changes might cost significant time and effort and can result in prolonged service downtime.

Prerequisites

- To use forced recovery, you must first enable this function. You enable forced recovery by enabling the **recovery.forceRecovery** setting as described in Change Recovery Settings.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, right-click a recovery plan, and select **Run**.

   You can also run the recovery plan by clicking the **Run** icon in the **Recovery Steps** view of the recovery plan.

4 Review the information in the confirmation prompt, and select **I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters**.

5 Select the type of recovery to run.

Option	Description
Planned Migration	Recovers virtual machines to the recovery site when both sites are running. If errors occur on the protected site during a planned migration, the planned migration operation fails.
Disaster Recovery	Recovers virtual machines to the recovery site if the protected site experiences a problem. If errors occur on the protected site during a disaster recovery, the disaster recovery continues and does not fail.

6 (Optional) Select the **Forced Recovery - recovery site operations only** check box.

This option is available if you enabled the forced recovery function and you selected **Disaster Recovery**.

7 Click **Next**.

8 Review the recovery information and click **Finish**.

9 Click the recovery plan and click **Recovery Steps**.

The **Recovery Steps** tab displays the progress of individual steps. The Recent Tasks area reports the progress of the overall plan.

Cancel a Test or Recovery

You can cancel a recovery plan test or recovery whenever the status is test in progress or failover in progress.

When you cancel a test or recovery, Site Recovery Manager does not start processes, and uses certain rules to stop processes that are in progress. Canceling a failover requires you to re-run the failover.

- Processes that can be stopped are stopped and flagged as errors.
- Processes that cannot be stopped, such as powering on or waiting for a heartbeat, run to completion before the cancellation finishes.

The time it takes to cancel a test or recovery depends on the type and number of processes that are currently in progress.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 Select the **Recovery Plans** tab, right-click a recovery plan, and select **Cancel**. You can also cancel the plan from the Recovery Steps tab.

What to do next

Run a cleanup after canceling a test.

Export Recovery Plan Steps

You can export the steps of a recovery plan in various formats for future reference, or to keep a hard copy backup of your plans.

You cannot export the recovery plan steps while a test recovery or a real recovery is in progress.

Prerequisites

Verify that you have a recovery plan.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 Select the **Recovery Plans** tab, and click a recovery plan.

4 Select the **Recovery Steps** tab and from the **View** drop-down menu select the recovery steps mode.

Option	Description
Test Steps	Exports the test recovery steps.
Recovery Steps	Exports the recovery steps.
Cleanup Steps	Exports the cleanup steps.
Reprotect Steps	Exports the reprotect steps.

Note Depending on the recovery plan status, the option to select the recovery steps mode might not be available.

5 Click **Export Steps**.

You can save the recovery plan steps as HTML, XML, CSV, or MS Excel or Word document.

6 Click **Download** and close the window.

Additionally, you can open the recovery plan steps report in a new tab

View and Export a Recovery Plan History

You can view and export reports about each run of a recovery plan, test of a recovery plan, test cleanup, or reprotect.

Recovery plan histories provide information about each run, test, cleanup, or reprotect of a recovery plan. The history contains information about the result and the start and end times for the whole plan and for each step in the plan. You can export history at any time, but history always contains entries only for completed operations. If an operation is in progress, the history appears after the operation completes.

SRM preserves history for deleted recovery plans. You can export history reports for existing and deleted plans.

To export a history report for an existing or a deleted plan, follow this procedure.

Prerequisites

You ran or tested a recovery plan, cleaned up after a test, or ran reprotect.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. On the Site Pair tab, select **Recovery Plans History**.
4. (Optional) Click **Export all** to export the entire recovery plans history list for a specific time period.
5. (Optional) Select an item from the recovery plans history list, and click **Export report** for the recovery plan history for a specific time period, recovery plan run, test, cleanup, or reprotect operation.
6. Select a format for the generated file and click **Download** or **Open in a new tab**.

   You can save the recovery plan history as HTML, XML, CSV, or MS Excel or Word document.

Delete a Recovery Plan

You can delete a recovery plan if you do not need it.

The recovery plan must be in a consistent state before you can delete it.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, right-click the recovery plan to delete, and select **Delete**.

Recovery Plan Status Reference

You can monitor the status of a recovery plan and determine the operation that is allowed in each state. The state of a recovery plan is determined by the states of the protection groups within the plan.

Table 6-2. Recovery States

State	Description
Ready	Recovery steps are cleared. You can verify protected virtual machines in a recovery plan in the **Virtual Machines** tab.
Test in progress	Canceling a test moves plan to Cancel in Progress state.
Test complete	Test completed with or without errors. If a failure occurs during the test, plan goes to Test Interrupted state.

Table 6-2. Recovery States (Continued)

State	Description
Test interrupted	Server failed while a test was running.
Cleanup in progress	After successful cleanup, plan state goes to Ready. If you set the Force Cleanup option, state goes to Ready after an error. If a failure occurs during cleanup, state goes to Cleanup Incomplete.
Cleanup incomplete	Errors occurred during cleanup. You can run the cleanup again. When running cleanup from this state, the cleanup wizard provides an option to ignore errors.
Cleanup interrupted	Site Recovery Manager failed during cleanup. You cannot change recovery options.
Recovery in progress	If you cancel recovery, the state goes to Cancel in progress.
Disaster recovery complete	During recovery at the protected site, VM shutdown encountered errors, possibly because the sites were not connected, the step before split brain.
Recovery started	A recovery started on the peer site, but if the sites are not connected, the exact state is unknown. Log in to the recovery site or reconnect the sites to get the current state.
Recovery required (split brain)	Sites were disconnected during recovery. Split brain scenario detected when sites reconnect. System prompts you to run recovery again to synchronize the sites. You can verify protected virtual machines in a recovery plan in the **Virtual Machines** tab.
Recovery complete	The recovery plan goes to this state after the split brain recovery is resolved. The recovery plan goes to this state after a successful planned migration. You can see the recover steps of the last recovery run. You can verify protected virtual machines in a recovery plan in the **Virtual Machines** tab.
Incomplete recovery	Canceled recovery or any recovery error. Run recovery again. You need to either resolve errors and rerun recovery, or remove protection for VMs in error. The plan detects the resolution of errors in either of these ways and updates state to Recovery Complete.
Partial recovery	Some but not all protection groups are recovered by an overlapping plan.
Recovery interrupted	A failure during recovery causes the recovery to pause. Click **Run** to continue. You cannot change recovery options.

Table 6-2. Recovery States (Continued)

State	Description
Cancel in progress	Canceling a test results in Test Complete with last result canceled. Canceling a recovery results in Incomplete Recovery with last result canceled. If the operation is canceled early enough, may result in a Ready state.
Reprotect in progress	If the server fails during this state, it goes to Reprotect Interrupted.
Partial reprotect	Overlapping plan was reprotected. The already reprotected groups go to Ready state, but this is valid, since the other groups are in the Recovered state.
Incomplete reprotect	Reprotect did not complete the storage operations. Sites must be connected for the reportect to succeed on the new run. Reprotect completed the storage operations but did not complete creating shadow virtual machines. You can run reprotect again even if the site running the virtual machines is disconnected, then proceed to recovery immediately after.
Reprotect interrupted	If the Site Recovery Manager Server fails during reprotect, run reprotect again to continue and properly clean up the state.
Waiting for user input	Test is paused. Dismiss the prompt to resume the test. Recovery is paused. Dismiss the prompt to resume recovery.
Protection groups in use	Plan contains groups that are being used for a test or failover by another plan. This state also occurs when the other plan has completed a Test operation on the groups, but has not run Cleanup. Wait for the other plan to complete the test or cleanup or edit the plan to remove the groups.
Direction error	Groups are in a mixed state, which is an invalid state. The plan contains different groups that are Ready in opposite directions. Choose one direction as correct and remove the protection groups that are in the opposite direction. For this error to occur, overlapping plans have run and reprotected some of the groups in the plan already.
Deleting	Plan enters this brief state while waiting for deletion of a peer plan. Plan automatically completes when the other plan is deleted.

Table 6-2. Recovery States (Continued)

State	Description
Plan out of sync	This state can occur under different circumstances: ■ Between a successful test recovery and a cleanup operation. If you cannot edit the plan in this state, run cleanup to return the plan to the Ready state. To allow cleanup, it might be required to open the plan in the VMware Site Recovery UI for the other site. If the plan remains in the Plan Out of Sync state, edit the plan. ■ During regular operation You can edit the plan. Opening the plan for editing and saving the changes after edit causes Site Recovery Manager to force synchronization of Site Recovery Manager internal data about the plan between protection and recovery Site Recovery Manager servers, which clears the Plan Out Of Sync status .
No protection groups	The plan contains no protection groups and the plan cannot run. You can edit the plan including the recovery site. You can create empty plans through the API or UI, or by deleting protection groups.
Internal error	A protection group with an unknown state is in the plan, or some other unexpected error occurred. You cannot run the plan but you can delete it.

Configuring a Recovery Plan

7

You can configure a recovery plan to run commands on Site Recovery Manager Server or on a virtual machine, display messages that require a response when the plan runs on the Site Recovery Manager Server or in the guest OS, suspend non-essential virtual machines during recovery, configure dependencies between virtual machines, customize virtual machine network settings, and change the recovery priority of protected virtual machines.

A simple recovery plan that specifies only a test network to which the recovered virtual machines connect and timeout values for waiting for virtual machines to power on and be customized can provide an effective way to test a Site Recovery Manager configuration. Most recovery plans require configuration for use in production. For example, a recovery plan for an emergency at the protected site might be different from a recovery plan for the planned migration of services from one site to another.

Note A recovery plan always reflects the current state of the protection groups that it recovers. If any members of a protection group show a status other than OK, you must correct the problems before you can make any changes to the recovery plan. When a recovery plan is running, its state reflects the state of the recovery plan run, rather than the state of the protection groups that it contains.

This chapter includes the following topics:

Recovery Plan Steps

A recovery plan runs a series of steps that must be performed in a specific order for a given workflow such as a planned migration or reprotect. You cannot change the order or purpose of the steps, but you can insert your own steps that display messages and run commands.

Site Recovery Manager runs different recovery plan steps in different ways.

- Some steps run during all recoveries.
- Some steps run only during test recoveries.
- Some steps run only during real recoveries.

Understanding recovery steps, their order, and the context in which they run is important when you customize a recovery plan.

Recovery Order

When you run a recovery plan, it starts by powering off the virtual machines at the protected site. Site Recovery Manager powers off virtual machines according to the priority that you set, with high-priority machines powering off last. Site Recovery Manager omits this step when you test a recovery plan.

Site Recovery Manager powers on groups of virtual machines on the recovery site according to the priority that you set. Before a priority group starts, all of the virtual machines in the next-higher priority group must recover or fail to recover. Dependencies between virtual machines within different priority groups are ignored. If dependencies exist between virtual machines in the same priority group, Site Recovery Manager first powers on the virtual machines on which other virtual machines depend. If Site Recovery Manager can meet the virtual machine dependencies, Site Recovery Manager attempts to power on as many virtual machines in parallel as vCenter Server supports.

Recovery Plan Timeouts and Pauses

Several types of timeouts can occur during the running of recovery plan steps. Timeouts cause the plan to pause for a specified interval to allow the step time to finish.

Message steps force the plan to pause until the user acknowledges the message. Before you add a message step to a recovery plan, make sure that it is necessary. Before you test or run a recovery plan that contains message steps, make sure that a user can monitor the progress of the plan and respond to the messages as needed.

Creating Custom Recovery Steps

You can create custom recovery steps that present messages to the user during a recovery.

Site Recovery Manager can run custom steps in a virtual machine that is part of the recovery plan. The custom recovery steps are shared between the Test workflow and Run workflow. If you add a custom recovery step before testing a recovery plan, it is available and executed when you run the actual recovery plan and the reverse. You cannot run custom steps on virtual machines that are to be suspended.

During reprotect, Site Recovery Manager preserves all custom recovery steps in the recovery plan. If you perform a recovery or test after a reprotect, custom recovery steps are run on the new recovery site, which was the original protected site.

After reprotect, you can usually use custom recovery steps that show messages directly without modifications. You might need to modify some custom recovery steps after a reprotect, if these steps run commands that contain site-specific information, such as network configurations.

You can configure commands and prompts in recovery plan steps that signify completion of a particular operation. You cannot add commands and prompts before the Configure Test networks step.

Types of Custom Recovery Steps

You can create different types of custom recovery steps to include in recovery plans.

Custom recovery steps are either command recovery steps or message prompt steps.

Command Recovery Steps

Command recovery steps contain per-virtual machine commands.

Per-Virtual Machine Commands

Site Recovery Manager associates per-virtual machine commands with newly recovered virtual machines during the recovery process. You can use these commands to complete configuration tasks after powering on a virtual machine. Commands that you configure to run after the virtual machine is powered on run in the newly recovered virtual machine. Commands that run on the newly recovered virtual machine are run in the context of the user account that VMware Tools uses on the recovered virtual machine. Depending on the function of the command that you write, you might need to change the user account that VMware Tools uses on the recovered virtual machine.

Message Prompt Recovery Steps

Present a message in the Site Recovery Manager user interface during the recovery. You can use this message to pause the recovery and provide information to the user running the recovery plan. For example, the message can instruct users to perform a manual recovery task or to verify steps. The only action users can take in direct response to a prompt is to dismiss the message, which allows the recovery to continue.

Execution of Commands and Prompt Steps

For vSphere Replication protection groups, the first command or prompt step added between **Create Writeable Storage Snapshot** and the first non-empty VM priority group starts in parallel with the step **Create Writeable Storage Snapshot** to address restart failure scenarios.

How Site Recovery Manager Handles Custom Recovery Step Failures

Site Recovery Manager handles custom recovery step failures differently based on the type of recovery step.

Site Recovery Manager attempts to complete all custom recovery steps, but some command recovery steps might fail to finish.

Command Recovery Steps

By default, Site Recovery Manager waits for 5 minutes for command recovery steps to finish. You can configure the timeout for each command. If a command finishes within this timeout period, the next recovery step in the recovery plan runs. How Site Recovery Manager handles failures of custom commands depends on the type of command.

Type of Command	Description
Per-virtual machine commands	Run in a batch after a virtual machine powers on. If a command fails, the remaining per-virtual machine commands in the batch do not run. For example, if you add five commands to run after power on, and the third command in the batch fails, the remaining two commands to run after power on do not run.

Message Prompt Recovery Steps

Custom recovery steps that issue a message prompt cannot fail. The recovery plan pauses until the user dismisses the prompt.

Create Top-Level Message Prompts

You can add steps that display message prompts that a user must acknowledge during a recovery.

Prerequisites

- You have a recovery plan to which to add custom steps.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. On the **Recovery Plans** tab, select a recovery plan, and click **Recovery Steps**.
4. Use the **View** drop-down menu to select the type of recovery plan run to which to add a step.

Option	Description
Test Steps	Add a step to run when you test a recovery plan.
Recovery Steps	Add a step to run when you perform planned migration or disaster recovery

You cannot add steps in the cleanup or reprotect operations.

5 Select where to add the step.
   - To add a step before a step, right click the step and select **Add Step Before**.
   - To add a step after the last step, right click the last step and select **Add Step After**.
6 In the **Name** text box, enter a name for the step.

   The step name appears in the list of steps in the **Recovery Steps** view.
7 In the **Content** text box, enter the message to display during the recovery plan run.
8 Click **Add** to add the step to the recovery plan.

What to do next

You can right click the newly created step and select options to edit, delete or add steps before and after it.

Create Command Steps for Individual Virtual Machines

You can create custom recovery steps for Site Recovery Manager to perform tasks on a virtual machine after Site Recovery Manager powers it on.

Site Recovery Manager associates command steps with a protected or recovered virtual machine in the same way as customization information. If multiple recovery plans contain the same virtual machine, Site Recovery Manager includes the commands in all of the recovery plans .

Prerequisites

- You have a recovery plan to which to add custom steps.
- For information about writing the commands to add to command steps, see Guidelines for Writing Command Steps and Environment Variables for Command Steps.

Procedure

1 In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2 On the VMware Site Recovery home tab, select a site pair and click **Open**.
3 On the **Recovery Plans** tab, select a recovery plan, and click **Recovery Steps**.
4 Right-click a virtual machine and click **Configure Recovery**.
5 On the **Recovery Properties** tab, click **Post Power On Steps**.
6 Click **New** to add a step.
7 In the **Name** text box, enter a name for the step.

   The step name appears in the list of steps in the **Recovery Steps** view.
8 In the Content text box, enter the command or script to run.
9 Modify the **Timeout** setting for the command to run on the virtual machine.
10 Click **Add** to add the step to the recovery plan.

11 Click **OK** to reconfigure the virtual machine to run the command after it powers on.

Guidelines for Writing Command Steps

All batch files or commands for custom recovery steps that you add to a recovery plan must meet certain requirements.

When you create a command step to add to a recovery plan, make sure that it takes into account the environment in which it must run. Errors in a command step affect the integrity of a recovery plan.

- You must start the Windows command shell using its full path on the local host. For example, to run a script located in `c:\alarmscript.bat`, use the following command line:

  ```
  c:\windows\system32\cmd.exe /c c:\alarmscript.bat
  ```

- Batch files and commands must finish within 300 seconds. Otherwise, the recovery plan terminates with an error. To change this limit, see Change Recovery Settings.
- Batch files or commands that produce output that contains characters with ASCII values greater than 127 must use UTF-8 encoding. Site Recovery Manager records only the final 4KB of script output in log files and in the recovery history. Scripts that produce more output should redirect the output to a file rather than sending it to the standard output to be logged.

Environment Variables for Command Steps

Site Recovery Manager makes environment variables available that you can use in commands for custom recovery steps.

In the default configuration, command steps on a recovered VM run with the identity of the VMware Tools service account. You can change the default configuration of the VMs that are compatible with the recovery.autoDeployGuestAlias setting. For information about the recovery.autoDeployGuestAlias setting, see Change Recovery Settings.

Site Recovery Manager sets the environment variables only for the duration of the command step. The specific environment variables do not exist in the guest OS of the recovered VM if the command is completed.

Table 7-1. Environment Variables Available to All Command Steps

Name	Value	Example
VMware_RecoveryName	Name of the recovery plan that is running.	Plan A
VMware_RecoveryMode	Recovery mode.	Test or recovery
VMware_VC_Host	Host name of the vCenter Server at the recovery site.	vc_hostname.example.com
VMware_VC_Port	Network port used to contact vCenter Server.	443

Site Recovery Manager makes additional environment variables available for per-virtual machine command steps that run on the recovered virtual machine.

Table 7-2. Environment Variables Available to Per-Virtual Machine Command Steps

Name	Value	Example
VMware_VM_Uuid	UUID used by vCenter to uniquely identify this virtual machine.	4212145a-eeae-a02c-e525-ebba70b0d4f3
VMware_VM_Name	Name of this virtual machine, as set at the protected site.	My New Virtual Machine
VMware_VM_Ref	Managed object ID of the virtual machine.	vm-1199
*VMware_VM_Guest*Name	Name of the guest OS as defined by the VIM API.	otherGuest
*VMware_VM_Guest*Ip	IP address of the virtual machine, if known.	192.168.0.103
VMware_VM_Path	Path to the VMX file of this virtual machine.	`[datastore-123] jquser-vm2/jquser-vm2.vmx`

Table 7-3. Environment Variables Available to Per-Virtual Machine Command Steps That Run on Recovered Virtual Machines

Name	Value and Description	Example
VMware_GuestOp_OutputFile	The value is the path to a command output file. If the command creates the file, Site Recovery Manager downloads the content of the file and adds it as a result to the recovery plan history and server logs. Site Recovery Manager adds the final 4 KB of the command output file to the recovery plan history and server logs. If the scripts generate an output greater than 4 KB, the output must be recorded in a custom location. When the command finishes, Site Recovery Manager deletes the command output file.	`C:\Windows\TEMP\vmware0\srmStdOut.log`

Example: Content for Command That Runs on a Recovered Virtual Machine

For Windows guest OS, you can create a `myGuestScript.bat` file that has the following content.

```
@echo off
echo %DATE% %TIME% : VM %VMware_VM_Name% recovered by RP %VMware_RecoveryName% ran in
%VMware_RecoveryMode% mode
echo %DATE% %TIME% : Configured with the following FQDN: %VMware_VM_GuestName% and IP:
%VMware_VM_GuestIp%
:: some more custom actions
```

To run the `myGuestScript.bat`, use the following command content.

```
C:\Windows\System32\cmd.exe /c C:\myScripts\myGuestScript.bat > %VMware_GuestOp_OutputFile% 2>&1
```

For Linux or Unix guest OS, you can create a `myGuestScript.sh` file that has the following content.

```
echo $(date) : VM $VMWare_VM_Name recovered by $VMWare_RecoveryName ran
echo $(date) : Configured with the following FQDN: $VMWare_VM_GuestName and IP: $VMWare_VM_GuestIp
# some more custom actions
```

To run the `myGuestScript.sh` file, use the following command content.

```
/bin/bash myGuestScript.sh &>$VMWare_GuestOp_OutputFile
```

Suspend Virtual Machines When a Recovery Plan Runs

Site Recovery Manager can suspend virtual machines on the recovery site during a recovery and a test recovery.

Suspending virtual machines on the recovery site is useful in active-active datacenter environments and where non-critical workloads run on recovery sites. By suspending any virtual machines that host non-critical workloads on the recovery site, Site Recovery Manager frees capacity for the recovered virtual machines. Site Recovery Manager resumes virtual machines that are suspended during a failover operation when the failover runs in the opposite direction.

You can only add virtual machines to suspend at the recovery site.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, click on a recovery plan, and select **Recovery Steps**.
4. Right-click **Suspend Non-critical VMs at recovery site** and select **Add Non-Critical VM**.
5. Select virtual machines on the recovery site to suspend during a recovery.
6. Click **Save**.

Site Recovery Manager suspends the virtual machines on the recovery site when the recovery plan runs.

Specify the Recovery Priority of a Virtual Machine

By default, Site Recovery Manager sets all virtual machines in a new recovery plan to recovery priority level 3. You can increase or decrease the recovery priority of a virtual machine. The recovery priority specifies the shutdown and power on order of virtual machines.

If you change the priority of a virtual machine, Site Recovery Manager applies the new priority to all recovery plans that contain this virtual machine.

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

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, click on a recovery plan, and select **Virtual Machines**.
4. Right-click a virtual machine and select **Priority Group**.
5. Select a new priority for the virtual machine.

   The highest priority is 1. The lowest priority is 5.
6. Click **Yes** to confirm the change of priority.

Configure Virtual Machine Dependencies

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

When a recovery plan runs, Site Recovery Manager starts the virtual machines that other virtual machines depend on before it starts the virtual machines with the dependencies. If Site Recovery Manager cannot start a virtual machine that another virtual machine depends on, the recovery plan continues with a warning. You can only configure dependencies between virtual machines that are in the same recovery priority group. If you configure a virtual machine to be dependent on a virtual machine that is in a lower priority group, Site Recovery Manager overrides the dependency and first starts the virtual machine that is in the higher priority group.

If you remove a protection group that contains the dependent virtual machine from the recovery plan the status of the protection group is set to `Not in this Plan` in the dependencies for the virtual machine with the dependency. If the configured virtual machine has a different priority than the virtual machine that it depends on, the status of the dependent virtual machine is set to Lower Priority or Higher Priority.

Prerequisites

- Verify that the virtual machine with the dependency and the virtual machine that it depends on are in the same recovery plan.
- Verify that the virtual machine with the dependency and the virtual machine that it depends on are in the same recovery priority group.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, click on a recovery plan, and select **Virtual Machines**.
4. Right-click a virtual machine that depends on one or more other virtual machines and select **Configure Recovery**.
5. Expand **VM Dependencies**.
6. From the drop-down menu select **View all**.

   A dialog opens listing all virtual machines in the selected recovery plan.
7. Select one or more virtual machines from the list and click **OK**.

   The selected virtual machines are added to the list of dependencies.
8. Verify the virtual machines in the **VM Dependencies** list are on and verify the status of the dependencies is **OK**.
9. (Optional) To remove a dependency, select **View VM Dependencies** from the drop-down menu, select a virtual machine from the list of virtual machines that this virtual machine depends on and click **Remove**.
10. Click **OK**.

Configure Virtual Machine Startup and Shutdown Options

You can configure how a virtual machine starts up and shuts down on the recovery site during a recovery.

You can configure whether to shut down the guest operating system of a virtual machine before it powers off on the protected site. You can configure whether to power on a virtual machine on the recovery site. You can also configure delays after powering on a virtual machine to allow VMware Tools or other applications to start on the recovered virtual machine before the recovery plan continues.

Prerequisites

You created a recovery plan.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, click on a recovery plan, and select **Virtual Machines**.
4. Right-click a virtual machine and select **Configure Recovery**.

5 Expand **Shutdown Action** and select the shutdown method for this virtual machine.

Option	Description
Shutdown guest OS before power off	Gracefully shuts down the virtual machine before powering it off. You can set a timeout period for the shutdown operation. Setting the timeout period to 0 is equivalent to the Power off option. This option requires that VMware Tools are running on the virtual machine. **Note** The virtual machine powers off when the timeout expires. If the OS of the virtual machine has not completed its shutdown tasks when the timeout expires, data loss might result. For a large virtual machine that requires a long time to shut down gracefully, set an appropriately long power-off timeout.
Power off	Powers off the virtual machine without shutting down the guest operating system.

6 Expand **Startup Action** and select whether to power on the virtual machine after a recovery.

Option	Description
Power on	Powers on the virtual machine on the recovery site.
Do not power on	Recovers the virtual machine but does not power it on.

7 (Optional) Select or deselect the **Wait for VMware tools** check box.

This option is only available if you selected **Power on** in Step 6.

If you select **Wait for VMware tools**, Site Recovery Manager waits until VMware Tools starts after powering on the virtual machine before the recovery plan continues to the next step. You can set a timeout period for VMware Tools to start.

8 (Optional) Select or deselect the **Additional Delay before running Post Power On steps and starting dependent VMs** check box and specify the time for the additional delay.

This option is only available if you selected **Power on** in Step 6.

For example, you might specify an additional delay after powering on a virtual machine to allow applications to start up that another virtual machine depends on.

Limitations to Protection and Recovery of Virtual Machines

The protection and recovery by Site Recovery Manager of virtual machines is subject to limitations.

Protection and Recovery of Suspended Virtual Machines

When you suspend a virtual machine, vSphere creates and saves its memory state. When the virtual machine resumes, vSphere restores the saved memory state to allow the virtual machine to continue without any disruption to the applications and guest operating systems that it is running.

Protection and Recovery of Linked Clone Virtual Machines

vSphere Replication does not support the protection and recovery of virtual machines that are linked clones.

Protection and Recovery of Virtual Machines with Reservations, Affinity Rules, or Limits

When Site Recovery Manager recovers a virtual machine to the recovery site, it does not preserve any reservations, affinity rules, or limits that you have placed on the virtual machine. Site Recovery Manager does not preserve reservations, affinity rules, and limits on the recovery site because the recovery site might have different resource requirements to the protected site. The only exception is the **Reserve all guest memory (All locked)** setting, if it was enabled on the protected VM.

You can set reservations, affinity rules, and limits for recovered virtual machines by configuring reservations and limits on the resource pools on the recovery site and setting up the resource pool mapping accordingly. Alternatively, you can set reservations, affinity rules, or limits manually on the placeholder virtual machines on the recovery site.

Customizing IP Properties for Virtual Machines

8

You can customize IP settings for virtual machines for the protected site and the recovery site. Customizing the IP properties of a virtual machine overrides the default IP settings when the recovered virtual machine starts at the destination site.

If you do not customize the IP properties of a virtual machine, Site Recovery Manager uses the IP settings for the recovery site during a recovery or a test from the protection site to the recovery site. Site Recovery Manager uses the IP settings for the protection site after reprotect during the recovery or a test from the original recovery site to the original protection site.

Site Recovery Manager supports different types of IP customization.

- Use IPv4 and IPv6 addresses.
- Configure different IP customizations for each site.
- Use DHCP, Static IPv4, or Static IPv6 addresses.
- Customize addresses of Windows and Linux virtual machines.
- Customize multiple NICs for each virtual machine.

Note You only configure one IP address per NIC.

For the list of guest operating systems for which Site Recovery Manager supports IP customization, see the *Compatibility Matrixes for Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.html.

You associate customization settings with protected virtual machines. As a result, if the same protected virtual machine is a part of multiple recovery plans, then all recovery plans use a single copy of the customization settings. You configure IP customization as part of the process of configuring the recovery properties of a virtual machine.

If you do not customize a NIC on the recovery site, the NIC continues to use the IP settings from the protected site, and vice versa, and Site Recovery Manager does not apply IP customization to the virtual machine during recovery.

You can apply IP customizations to individual or to multiple virtual machines.

If you configure IP customization on virtual machines, Site Recovery Manager adds recovery steps to those virtual machines.

Guest OS Startup	The Guest Startup process happens in parallel for all virtual machines for which you configure IP customization.
Customize IP	Site Recovery Manager pushes the IP customizations to the virtual machine.
Guest OS Shutdown	Site Recovery Manager shuts down the virtual machine and reboots it to ensure that the changes take effect and that the guest operating system services apply them when the virtual machine restarts.

After the IP customization process finishes, virtual machines power on according to the priority groups and any dependencies that you set.

Note To customize the IP properties of a virtual machine, you must install VMware Tools or the VMware Operating System Specific Packages (OSP) on the virtual machine. See http://www.vmware.com/download/packages.html.

This chapter includes the following topics:

Manually Customize IP Properties for an Individual Virtual Machine

You can customize IP settings manually for individual virtual machines for both the protected site and the recovery site.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, click on a recovery plan, and select **Virtual Machines**.
4. Right-click a virtual machine and click **Configure Recovery**.
5. Click the **IP Customization** tab and select **Manual IP customization**.
6. Select the NIC for which you want to modify IP Settings.
7. Click **Configure** for the protected site or **Configure** for the recovery site, depending on whether you want to configure IP settings on the protected site or on the recovery site.

8 Click the **IPv4** tab to configure IPv4 settings, and select DHCP, or for static addresses, enter an IP address, subnet information, and gateway server addresses.

   Alternately, if the virtual machine is powered on and has VMware Tools installed, you can click **Retrieve** to import current settings configured on the virtual machine.

9 Click the **IPv6** tab to configure IPv6 settings, and select DHCP, or for static addresses, enter an IP address, subnet information, and gateway server addresses.

   Alternately, if the virtual machine is powered on and has VMware Tools installed, you can click **Retrieve** to import current settings configured on the virtual machine.

10 Click the **DNS** tab to configure DNS settings.

   a Choose how DNS servers are found.

      You can use DHCP to find DNS servers or you can specify primary and alternate DNS servers.

   b Enter a DNS suffix and click **Add** or select an existing DNS suffix and click **Remove**, **Move Up**, or **Move Down**.

      Alternately, if the virtual machine is powered on and has VMware Tools installed, you can click **Retrieve** to import current settings configured on the virtual machine.

11 Click the **WINS** tab to enter primary and secondary WINS addresses.

   The WINS tab is available only when configuring DHCP or IPv4 addresses for Windows virtual machines.

12 Repeat Step 7 through Step 10 to configure recovery site or protected site settings, if required.

   For example, if you configured IP settings for the recovery site, you might want to configure IP settings for the protected site. Recovery site settings are applied during recovery. Protected site settings are applied during failback.

13 Repeat the configuration process for other NICs, as required.

Note Virtual machines with manually defined IP customization are not subject to the IP Mapping Rule evaluation during recovery. Manually-specified IP configuration takes precedence over IP mapping rules.

Customizing IP Properties for Multiple Virtual Machines

You can customize the IP properties for multiple virtual machines on the protected and recovery sites by using the DR IP Customizer tool and by defining subnet-level IP mapping rules.

Note You can use the DR IP Customizer tool only on your on-premises environment.

In previous releases of Site Recovery Manager, you customized IP properties for multiple virtual machines by using the DR IP Customizer tool. In addition to DR IP Customizer, you can customize IP properties for multiple virtual machines by defining subnet-level IP customization rules.

You can use subnet-level IP customization rules in combination with DR IP Customizer.

- Using DR IP Customizer is a fast way to define explicit IP customization settings for multiple virtual machines by using a CSV file.
- You apply subnet-level IP customization rules to virtual machines by using the vSphere Web Client.

Virtual machines that you configure by using DR IP Customizer are not subject to subnet-level IP customization rules. You can achieve the same IP customization results by using either DR IP Customizer or IP subnet rules.

Customizing IP Properties for Multiple Virtual Machines By Using the DR IP Customizer Tool

The DR IP Customizer tool allows you to define explicit IP customization settings for multiple protected virtual machines on the protected and recovery sites.

In addition to defining subnet IP mapping rules, you can use the DR IP Customizer tool to apply customized networking settings to virtual machines when they start on the recovery site. You provide the customized IP settings to the DR IP Customizer tool in a comma-separated value (CSV) file.

Rather than manually creating a CSV file, you can use the DR IP Customizer tool to export a CSV file that contains information about the networking configurations of the protected virtual machines. You can use this file as a template for the CSV file to apply on the recovery site by customizing the values in the file.

1. Run DR IP Customizer to generate a CSV file that contains the networking information for the protected virtual machines.
2. Modify the generated CSV file with networking information that is relevant to the recovery site.
3. Run DR IP Customizer again to apply the CSV with the modified networking configurations to apply when the virtual machines start up on the recovery site.

You can run the DR IP Customizer tool on either the protected site or on the recovery site. Virtual machine IDs for protected virtual machines are different at each site, so whichever site you use when you run the DR IP Customizer tool to generate the CSV file, you must use the same site when you run DR IP Customizer again to apply the settings.

You can customize the IP settings for the protected and the recovery sites so that Site Recovery Manager uses the correct configurations during reprotect operations.

For the list of guest operating systems for which Site Recovery Manager supports IP customization, see the *Compatibility Matrixes for Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.html.

Report IP Address Mappings for Recovery Plans

The IP address map reporter generates an XML document describing the IP properties of protected virtual machines and their placeholders, grouped by site and recovery plan. This information can help you understand the network requirements of a recovery plan.

Because the IP address mapping reporter must connect to both sites, you can run the command at either site. You are prompted to supply the vCenter login credentials for each site when the command runs.

Procedure

1. Open a command shell on the Site Recovery Manager Server host at either the protected or recovery site.
2. Change to the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin` directory.
3. Run the `dr-ip-reporter.exe` command.
   - If you have a Platform Services Controller with a single vCenter Server instance, run the following command:

     ```
     dr-ip-reporter.exe --cfg ..\config\vmware-dr.xml
     --out path_to_report_file.xml
     --uri https://Platform_Services_Controller_address[:port]/lookupservice/sdk
     ```

     This example points `dr-ip-reporter.exe` to the `vmware-dr.xml` file of the Site Recovery Manager Server and generates the report file for the vCenter Server instance that is associated with the Platform Services Controller at https://*Platform_Services_Controller_address*.
   - If you have a Platform Services Controller that includes multiple vCenter Server instances, you must specify the vCenter Server ID in the `--vcid` parameter.

     ```
     dr-ip-reporter.exe --cfg ..\config\vmware-dr.xml
     --out path_to_report_file.xml
     --uri https://Platform_Services_Controller_address[:port]/lookupservice/sdk
     --vcid vCenter_Server_ID
     ```

     This example points `dr-ip-reporter.exe` to the `vmware-dr.xml` file of the Site Recovery Manager Server and generates the report file for the vCenter Server instance with the ID *vCenter_Server_ID*.

     Note The vCenter Server ID is not the same as the vCenter Server name.
   - To restrict the list of networks to just the ones that a specific recovery plan requires, include the `-plan` option on the command line:

     ```
     dr-ip-reporter.exe --cfg ..\config\vmware-dr.xml
     --out path_to_report_file.xml
     --uri https://Platform_Services_Controller_address[:port]/lookupservice/sdk
     --plan recovery_plan_name
     ```

Syntax of the DR IP Customizer Tool

The DR IP Customizer tool includes options that you can use to gather networking information about the virtual machines that Site Recovery Manager protects. You can also use the options to apply customizations to virtual machines when they start up on the recovery site.

Note This release of Site Recovery Manager allows you to define subnet-level IP mapping rules to customize IP settings on virtual machines, as well as by using the DR IP Customizer tool. You can use subnet-level IP mapping rules in combination with DR IP Customizer. For information about how you can use subnet-level IP mapping rules and DR IP Customizer together, see Customizing IP Properties for Multiple Virtual Machines.

You find the `dr-ip-customizer.exe` executable file in `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin` on the Site Recovery Manager Server host machine. When you run `dr-ip-customizer.exe`, you specify different options depending on whether you are generating or applying a comma-separated value (CSV) file.

```
dr-ip-customizer.exe
--cfg SRM Server configuration XML
--cmd apply/drop/generate
[--csv Name of existing CSV File]
[--out Name of new CSV file to generate]
--uri https://host[:port]/lookupservice/sdk
--vcid UUID
[--ignore-thumbprint]
[--extra-dns-columns]
[--verbose]
```

You can run the DR IP Customizer tool on either the protected site or on the recovery site. Virtual machine IDs for protected virtual machines are different at each site, so whichever site you use when you run the DR IP Customizer tool to generate the CSV file, you must use the same site when you run DR IP Customizer again to apply the settings.

Some of the options that the DR IP Customizer tool provides are mandatory, others are optional.

Table 8-1. DR IP Customizer Options

Option	Description	Mandatory
`-h [ --help ]`	Displays usage information about `dr-ip-customizer.exe`.	No
`-c [ --cfg ] arg`	Path to the application XML configuration file, `vmware-dr.xml`.	Yes

Table 8-1. DR IP Customizer Options (Continued)

Option	Description	Mandatory
`--cmd arg`	You specify different commands to run DR IP Customizer in different modes. ■ The `apply` command applies the network customization settings from an existing CSV file to the recovery plans on the Site Recovery Manager Server instances. ■ The `generate` generates a basic CSV file for the all virtual machines in the recovery plans on the Site Recovery Manager servers. ■ The `drop` command removes the recovery settings from virtual machines specified by the input CSV file. Always provide the same vCenter Server instance for the `apply` and `drop` commands as the one that you used to generate the CSV file.	Yes
`--csv arg`	Path to the CSV file.	Yes, when running the `apply` and `drop` commands.
`-o [ --out ] arg`	Name of the new CSV output file that the `generate` command creates. If you provide the name of an existing CSV file, the `generate` command overwrites its current contents.	Yes, when you run the `generate` command.
`--uri arg`	Lookup Service URL on the Platform Service Controller with the form `https://host[:port]/lookupservice/sdk`. Specify the port if it is not 443 . Use the same vCenter Server instance for the `apply` and `drop` commands as the one that you used to generate the CSV file.	Yes
`--vcid arg`	The vCenter Server instance UUID.	Optional, unless the infrastructure contains more than one vCenter Server instance.
`-i [ --ignore-thumbprint ]`	Ignore the vCenter Server thumbprint confirmation prompts.	No
`-e [ --extra-dns-columns ]`	Must be specified if the input CSV file contains extra columns for DNS information.	No
`-v [ --verbose ]`	Enable verbose output. You can include a `--verbose` option on any `dr-ip-customizer.exe` command line to log additional diagnostic messages.	No

The tool can print the UUID to the Lookup Service whenever the `--vcid` value is unspecified as in this example:

```
dr-ip-customizer.exe --cfg testConfig.xml -i --cmd generate -o c: \tmp\x.csv --uri
https://service.company.com:443/lookupservice/sdk --vcid ?
```

```
ERROR: Failed to locate VC instance. Use one of the following known VC instances:
e07c907e-cd41-4fe7-b38a-f4c0e677a18c vc.company.com
```

The result is the vCenter Server instance UUID followed by the vCenter Server DNS hostname for each vCenter Server registered with the Lookup Service.

Structure of the DR IP Customizer CSV File

The DR IP Customizer comma-separated value (CSV) file consists of a header row that defines the meaning of each column in the file, and one or more rows for each placeholder virtual machine in a recovery plan.

Note This release of Site Recovery Manager allows you to define subnet-level IP mapping rules to customize IP settings on virtual machines, as well as by using the DR IP Customizer tool. You can use subnet-level IP mapping rules in combination with DR IP Customizer. For information about how you can use subnet-level IP mapping rules and DR IP Customizer together, see Customizing IP Properties for Multiple Virtual Machines.

Configuring IP settings for both sites is optional. You can provide settings for only the protected site, or settings for only the recovery site, or settings for both sites. You can configure each site to use a different set of network adapters in a completely different way.

Certain fields in the CSV file must be completed for every row. Other fields can be left blank if no customized setting is required.

Table 8-2. Columns of the DR IP Customizer CSV File

Column	Description	Customization Rules
VM ID	Unique identifier that DR IP Customizer uses to collect information from multiple rows for application to a single virtual machine. This ID is internal to DR IP Customizer and is not the same as the virtual machine ID that vCenter Server uses.	Not customizable. Cannot be blank.
VM Name	The human-readable name of the virtual machine as it appears in the vCenter Server inventory.	Not customizable. Cannot be blank.

Table 8-2. Columns of the DR IP Customizer CSV File (Continued)

Column	Description	Customization Rules
vCenter Server	Address of a vCenter Server instance on either the protected site or the recovery site. You set the IP settings for a virtual machine on each site in the vCenter Server column.	Not customizable. Cannot be blank. This column can contain both vCenter Server instances. Each vCenter Server instance requires its own row. You can configure one set of IP settings to use on one site and another set of IP settings to use on the other site. You can also provide IP settings to be used on both sites, for reprotect operations.
Adapter ID	ID of the adapter to customize. Adapter ID 0 sets global settings on all adapters for a virtual machine. Setting values on Adapter ID 1, 2, 3, and so on, configures settings for specific NICs on a virtual machine.	Customizable. Cannot be left blank. The only fields that you can modify for a row in which the Adapter ID is 0 are DNS Server(s) and DNS Suffix(es). These values, if specified, are inherited by all other adapters in use by that VM ID. You can include multiple DNS servers on multiple lines in the CSV file. For example, if you require two global DNS hosts, you include two lines for Adapter ID 0. ■ One line that contains all the virtual machine information plus one DNS host. ■ One line that contains only the second DNS host. To add another DNS server to a specific adapter, add the DNS server to the appropriate Adapter line. For example, add the DNS server to Adapter ID 1.
DNS Domain	DNS domain for this adapter.	Customizable. Can be left blank. If you do enter a value, it must be in the format **`example.company.com`**.
Net BIOS	Select whether to activate NetBIOS on this adapter.	Customizable. Can be left blank. If not left empty, this column must contain one of the following strings: `disableNetBIOS`, `enableNetBIOS`, or `enableNetBIOSViaDhcp`.
Primary WINS	DR IP Customizer validates that WINS settings are applied only to Windows virtual machines, but it does not validate NetBIOS settings.	Customizable. Can be left blank.
Secondary WINS	DR IP Customizer validates that WINS settings are applied only to Windows virtual machines, but it does not validate NetBIOS settings.	Customizable. Can be left blank.

Table 8-2. Columns of the DR IP Customizer CSV File (Continued)

Column	Description	Customization Rules
IP Address	IPv4 address for this virtual machine.	Customizable. Cannot be blank. Virtual machines can have multiple virtual network adapters. You can configure each virtual network adapter with one static IPv4 address. If the field is not set to a specific static address you must set it to DHCP.
Subnet Mask	Subnet mask for this virtual machine.	Customizable. Can be left blank.
Gateway(s)	IPv4 gateway or gateways for this virtual machine.	Customizable. Can be left blank.
IPv6 Address	IPv6 address for this virtual machine.	Customizable. Can be left blank if you do not use IPv6. Virtual machines can have multiple virtual network adapters.You can configure each virtual network adapter with one static IPv6 address. If the field is not set to a specific static address you must set it to DHCP. If you run Site Recovery Manager Server on Windows Server 2003 and you customize IPv6 addresses for a virtual machine, you must enable IPv6 on the Site Recovery Manager Server instances. Site Recovery Manager performs validation of IP addresses during customization, which requires IPv6 to be enabled on the Site Recovery Manager Server if you are customizing IPv6 addresses. Later versions of Windows Server have IPv6 enabled by default.
IPv6 Subnet Prefix length	Ipv6 subnet prefix length to use.	Customizable. Can be left blank.
IPv6 Gateway(s)	IPv4 gateway or gateways for this adapter.	Customizable. Can be left blank.

Table 8-2. Columns of the DR IP Customizer CSV File (Continued)

Column	Description	Customization Rules
DNS Server(s)	Address of the DNS server or servers.	Customizable. Can be left blank. If you enter this setting in an Adapter ID 0 row, it is treated as a global setting. On Windows virtual machines, this setting applies for each adapter if you set it in the Adapter ID rows other than Adapter ID 0. On Linux virtual machines, this is always a global setting for all adapters. This column can contain one or more IPv4 or IPv6 DNS servers for each NIC.
DNS Suffix(es)	Suffix or suffixes for DNS servers.	Customizable. Can be left blank. These are global settings for all adapters on both Windows and Linux virtual machines.

Modifying the DR IP Customizer CSV File

You modify the DR IP Customizer comma-separated value (CSV) file to apply customized networking settings to virtual machines when they start on the recovery site.

Note This release of Site Recovery Manager allows you to define subnet-level IP mapping rules to customize IP settings on virtual machines, as well as by using the DR IP Customizer tool. You can use subnet-level IP mapping rules in combination with DR IP Customizer. For information about how you can use subnet-level IP mapping rules and DR IP Customizer together, see Customizing IP Properties for Multiple Virtual Machines.

One challenge of representing virtual machine network configurations in a CSV file is that virtual machine configurations include hierarchical information. For example, a single virtual machine might contain multiple adapters, and each adapter might have multiple listings for elements such as gateways. The CSV format does not provide a system for hierarchical representations. As a result, each row in the CSV file that the DR IP Customizer generates might provide some or all of the information for a specific virtual machine.

For a virtual machine with a simple network configuration, all the information can be included in a single row. In the case of a more complicated virtual machine, multiple rows might be required. Virtual machines with multiple network cards or multiple gateways require multiple rows. Each row in the CSV file includes identification information that describes to which virtual machine and adapter the information applies. Information is aggregated to be applied to the appropriate virtual machine.

Follow these guidelines when you modify the DR IP Customizer CSV file.

- Omit values if a setting is not required.
- Use the minimum number of rows possible for each adapter.
- Do not use commas in any field.

- Specify Adapter ID settings as needed. DR IP Customizer applies settings that you specify on Adapter ID 0 to all NICs. To apply settings to individual NICs, specify the values in the Adapter ID 1, 2, ..., *n* fields.
- To specify more than one value for a column, create an additional row for that adapter and include the value in the column in that row. To ensure that the additional row is associated with the intended virtual machine, copy the VM ID, VM Name, vCenter Server, and Adapter ID column values.
- To specify an IP address for a network adapter on each of the protected and recovery sites, or to specify multiple DNS server addresses, add a new row for each address. Copy the VM ID, VM Name, and Adapter ID values to each row.

Run DR IP Customizer to Customize IP Properties for Multiple Virtual Machines

You can use the DR IP Customizer tool to customize the IP properties for multiple virtual machines that Site Recovery Manager protects.

Note This release of Site Recovery Manager allows you to define subnet-level IP mapping rules to customize IP settings on virtual machines, as well as by using the DR IP Customizer tool. You can use subnet-level IP mapping rules in combination with DR IP Customizer. For information about how you can use subnet-level IP mapping rules and DR IP Customizer together, see Customizing IP Properties for Multiple Virtual Machines.

Prerequisites

- Use the DR IP Customizer tool on a computer with access to vCenter Server instances in your environment.
- The user account that you use to run the DR IP Customizer tool requires at least the Site Recovery Manager Recovery Plans Administrator role.

Procedure

1. Open a command shell on the Site Recovery Manager Server host.
2. Change directory to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.
3. Run the `dr-ip-customizer.exe` command to generate a comma-separated value (CSV) file that contains information about the protected virtual machines.
   - If you have a Platform Services Controller with a single vCenter Server instance, run the following command:

     ```
     dr-ip-customizer.exe --cfg SRM_install_dir\config\vmware-dr.xml
     --cmd generate --out "path_to_CSV_file.csv"
     --uri https://Platform_Services_Controller_address[:port]/lookupservice/sdk
     ```

This example points `dr-ip-customizer.exe` to the `vmware-dr.xml` file of the Site Recovery Manager Server and generates the CSV file for the vCenter Server instance that is associated with the Platform Services Controller at https://*Platform_Services_Controller_address*.

- If you have a Platform Services Controller that includes multiple vCenter Server instances, you must specify the vCenter Server ID in the `--vcid` parameter. If you do not specify `--vcid`, or if you provide an incorrect ID, the tool lists all available vCenter Server instances.

```
dr-ip-customizer.exe --cfg SRM_install_dir\config\vmware-dr.xml
--cmd generate --out "path_to_CSV_file.csv"
--uri https://Platform_Services_Controller_address[:port]/lookupservice/sdk
--vcid vCenter_Server_ID
```

This example points `dr-ip-customizer.exe` to the `vmware-dr.xml` file of the Site Recovery Manager Server and generates the CSV file for the vCenter Server instance with the ID *vCenter_Server_ID*.

Note The vCenter Server ID is not the same as the vCenter Server name.

4. (Optional) Check the vCenter Server thumbprint and enter **y** to confirm that you trust this vCenter Server instance.

   If you specified the `--ignore-thumbprint` option, you are not prompted to check the thumbprint.

5. Enter the login credentials for the vCenter Server instance.

   You might be prompted again to confirm that you trust this vCenter Server instance.

6. Edit the generated CSV file to customize the IP properties for the virtual machines in the recovery plan.

   You can use a spread sheet application to edit the CSV file. Save the modified CSV file under a new name.

7. Run `dr-ip-customizer.exe` to apply the customized IP properties from the modified CSV file.

   You can run the DR IP Customizer tool on either the protected site or on the recovery site. Virtual machine IDs for protected virtual machines are different at each site, so whichever site you use when you run the DR IP Customizer tool to generate the CSV file, you must use the same site when you run DR IP Customizer again to apply the settings.

   - If you have a Platform Services Controller with a single vCenter Server instance, run the following command:

```
dr-ip-customizer.exe --cfg SRM_install_dir\config\vmware-dr.xml
--cmd apply --csv "path_to_CSV_file.csv"
--uri https://Platform_Services_Controller_address[:port]/lookupservice/sdk
```

This example points `dr-ip-customizer.exe` to the `vmware-dr.xml` file of the Site Recovery Manager Server and applies the customizations in the CSV file to the vCenter Server that is associated with the Platform Services Controller at https://*Platform_Services_Controller_address*.

- If you have a Platform Services Controller that includes multiple vCenter Server instances, you must specify the vCenter Server ID in the `--vcid` parameter.

```
dr-ip-customizer.exe --cfg SRM_install_dir\config\vmware-dr.xml
--cmd apply --csv "path_to_CSV_file.csv"
--uri https://Platform_Services_Controller_address[:port]/lookupservice/sdk
--vcid vCenter_Server_ID
```

This example points `dr-ip-customizer.exe` to the `vmware-dr.xml` file of the Site Recovery Manager Server and applies the customizations in the CSV file to the vCenter Server instance with the ID *vCenter_Server_ID*.

The specified customizations are applied to all of the virtual machines named in the CSV file during a recovery. You do not need to manually configure IP settings for these machines when you edit their recovery plan properties.

Customize IP Properties for Multiple Virtual Machines by Defining IP Customization Rules

You can specify a single subnet-level IP mapping rule for a selected configured virtual network mapping on the protected and recovery sites.

Subnet-level mapping eliminates the need to define exact adapter-level IP mapping. Instead, you specify an IP customization rule that Site Recovery Manager applies to relevant adapters. The IP customization rule is used for test and recovery workflows. You cannot reuse IP customization rules between different network mappings.

Important

- IP subnet mapping rules support IPv4 only.
- Rule-based IPv6 customization is not supported in Site Recovery Manager.
- When you apply IP subnet mapping rules to Windows virtual machines with IPv6 enabled, the IPv6 settings, DHCP or static, remain unaffected after recovery. For Linux virtual machines, IPv6 settings are reset to DHCP.
- Site Recovery Manager does not evaluate IP mapping rules for virtual machines configured to use manual IP customization.

The IP customization rule applies to virtual machines failing over from a protected site IPv4 subnet to a recovery site IPv4 subnet, for example, from 10.17.23.0/24 to 10.18.22.0/24. The IP customization rule states that during recovery Site Recovery Manager evaluates the existing IP configuration of the recovered virtual machine's NICs and reconfigures static NICs found on the 10.17.23.0/24 subnet for the 10.18.22.0/24 subnet.

If the rule matches, Site Recovery Manager derives the new static IPv4 address from the old one by preserving the host bits of the original IPv4 address and placing it to the target subnet. For example, if the original protected site address is 10.17.23.55/24, the new address is 10.18.22.55/24.

If the default gateway text box is empty, Site Recovery Manager derives the new gateway parameter from the original one by preserving the host bits of the original IPv4 address and placing it in the target subnet. For example, if the original protected site gateway is 10.17.23.1, the new gateway is 10.18.22.1. If you specify an explicit gateway parameter, Site Recovery Manager checks that the IPv4 address syntax is correct and applies it exactly.

Site Recovery Manager applies DNS and other parameters as specified. DHCP-enabled NICs are not subject to customization as their network configuration remains unchanged during recovery.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. In the left pane click **Configure > Network Mappings**.
4. Select a network mapping for which to define a customization rule.
5. To define a rule, right-click on the mapping and select **Add IP Customization Rule**.
6. Specify the subnet IP ranges that map to the protected and recovery sites.
7. Specify the network settings for the recovery site network.
8. Click **Add** to save your changes.

Apply IP Customization Rules to a Virtual Machine

You can apply an IP customization rule to the recovery settings of a protected virtual machine.

When you apply an IP customization rule, you specify a single subnet IP mapping rule for each network mapping.

If you set the advanced setting option `recovery.useIpMapperAutomatically` to True and configure the IP mapping rule for virtual networks, then Site Recovery Manager evaluates the subnet IP mapping rules during recovery to customize the virtual machines. If you set this option to False, Site Recovery Manager does not evaluate the IP mapping rules during recovery. You can override the effect of this option for each virtual machine by using the **IP Customization** option.

The `recovery.useIpMapperAutomatically` default option is True. If you set it to Auto, Site Recovery Manager customizes the virtual machine by using the IP Customization rule.

Prerequisites

For the list of guest operating systems for which Site Recovery Manager supports IP customization, see the *Compatibility Matrixes for Site Recovery Manager 8.0* at https://www.vmware.com/support/srm/srm-compat-matrix-8-0.html.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, click on a recovery plan and select **Virtual Machines**.
4. Right-click a virtual machine and click **Configure Recovery**.
5. Click **IP Customization**.
6. From the IP customization mode list, select **Use IP customization rules if applicable** and click **OK**.

Reprotecting Virtual Machines After a Recovery

9

After a recovery, the recovery site becomes the primary site, but the virtual machines are not protected yet. If the original protected site is operational, you can reverse the direction of protection to use the original protected site as a new recovery site to protect the new protected site.

Manually reestablishing protection in the opposite direction by recreating all protection groups and recovery plans is time consuming and prone to errors. Site Recovery Manager provides the reprotect function, which is an automated way to reverse protection.

After Site Recovery Manager performs a recovery, the virtual machines start up on the recovery site. By running reprotect when the protected site comes back online, you reverse the direction of replication to protect the recovered virtual machines on the recovery site back to the original protected site.

Reprotect uses the protection information that you established before a recovery to reverse the direction of protection. You can initiate the reprotect process only after recovery finishes without any errors. If the recovery finishes with errors, you must fix all errors and rerun the recovery, repeating this process until no errors occur.

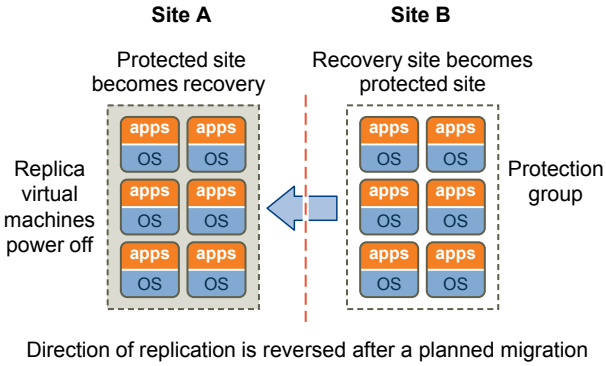
You can conduct tests after a reprotect operation completes, to confirm that the new configuration of the protected and recovery sites is valid.

Example: Performing a Reprotect Operation

Site A is the protected site and site B is the recovery site. If site A goes offline, run the disaster recovery workflow on the recovery plan to bring the virtual machines online on site B. After the recovery, the protected virtual machines from site A start up on site B without protection.

When site A comes back online, complete recovery by doing a planned migration because site A virtual machines and datastores need to be powered down and unmounted before reversing protection. Then initiate a reprotect operation to protect the recovered virtual machines on site B. Site B becomes the protected site, and site A becomes the recovery site. Site Recovery Manager reverses the direction of replication from site B to site A.

Figure 9-1. Site Recovery Manager Reprotect Process



- How Site Recovery Manager Reprotects Virtual Machines with vSphere Replication

  In the reprotect process using vSphere Replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

- Preconditions for Performing Reprotect

  You can perform reprotect only if you meet certain preconditions.

- Reprotect Virtual Machines

  Reprotect results in the reconfiguration of Site Recovery Manager protection groups and recovery plans to work in the opposite direction. After a reprotect operation, you can recover virtual machines back to the original site using a planned migration workflow.

- Reprotect States

  The reprotect process can pass through several states that you can observe in the recovery plan in the VMware Site Recovery user interface.

How Site Recovery Manager Reprotects Virtual Machines with vSphere Replication

In the reprotect process using vSphere Replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

When performing reprotection with vSphere Replication, Site Recovery Manager uses the original VMDK files as initial copies during synchronization. The full synchronization that appears in the recovery steps mostly performs checksums, and only a small amount of data is transferred through the network.

Forcing synchronization of data from the new protection site to the new recovery site ensures that the recovery site has a current copy of the protected virtual machines running at the protection site. Forcing this synchronization ensures that recovery is possible immediately after the reprotect process finishes.

If you want to manually set up reverse replication on a vSphere Replication protected virtual machine, use the VMware Site Recovery user interface to force stop the incoming replication group on the old recovery site, which is the new protected site. If you just delete the virtual machine on the original protected site, the reprotect will fail.

Preconditions for Performing Reprotect

You can perform reprotect only if you meet certain preconditions.

You can perform reprotect on recovery plans that contain vSphere Replication protection groups.

Before you can run reprotect, you must satisfy the preconditions.

1 Run a planned migration and make sure that all steps of the recovery plan finish successfully. If errors occur during the recovery, resolve the problems that caused the errors and rerun the recovery. When you rerun a recovery, operations that succeeded previously are skipped. For example, successfully recovered virtual machines are not recovered again and continue running without interruption.

2 The original protected site must be available. The vCenter Server instances, ESXi Servers, Site Recovery Manager Server instances, the vSphere Replication servers and corresponding databases must be available.

3 If you performed a disaster recovery operation, you must perform a planned migration when both sites are running again. If errors occur during the attempted planned migration, you must resolve the errors and rerun the planned migration until it succeeds.

Reprotect is not available under certain circumstances.

- Recovery plans cannot finish without errors. For reprotect to be available, all steps of the recovery plan must finish successfully.
- You cannot restore the original site, for example if a physical catastrophe destroys the original site.

Reprotect Virtual Machines

Reprotect results in the reconfiguration of Site Recovery Manager protection groups and recovery plans to work in the opposite direction. After a reprotect operation, you can recover virtual machines back to the original site using a planned migration workflow.

Prerequisites

See Preconditions for Performing Reprotect.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 Select the **Recovery Plans** tab, right-click a recovery plan and select **Reprotect**.

4 Select the check box to confirm that you understand that the reprotect operation is irreversible.

5 (Optional) Select the **Force Cleanup** check box to ignore errors during the cleanup operation on the recovery site, and click **Next**.

The **Force Cleanup** option is only available after you have performed an initial reprotect operation that has experienced errors.

6 Review the reprotect information and click **Finish**.

7 Select the recovery plan and click **Recovery Steps** tab to monitor the progress of the reprotect operation.

8 When the reprotect operation finishes, select the recovery plan, click **History**, and click the **Export report for selected history item** button.

   The recovery plan can return to the ready state even if errors occurred during the reprotect operation. Check the history report for the reprotect operation to make sure that no errors occurred. If errors did occur during reprotect, attempt to fix the errors and run a test recovery to make sure that the errors are fixed. If you do not fix errors that occurred during reprotect and you subsequently attempt to run planned migration or disaster recovery without fixing them, some virtual machines might fail to recover.

Site Recovery Manager reverses the recovery site and protected sites. Site Recovery Manager creates placeholder copies of virtual machines from the new protected site at the new recovery site.

Reprotect States

The reprotect process can pass through several states that you can observe in the recovery plan in the VMware Site Recovery user interface.

If reprotect fails, or succeeds partially, you can perform remedial actions to complete the reprotect.

Table 9-1. Reprotect States

State	Description	Remedial Action
Reprotect In Progress	Site Recovery Manager is running reprotect.	None
Partial Reprotect	Occurs if multiple recovery plans share the same protection groups and some of the protection groups were successfully reprotected in another plan.	Run reprotect again on the partially reprotected plans.
Incomplete Reprotect	Occurs because of failures during reprotect. For example, this state might occur because of a failure to perform reverse replication or a failure to create placeholder virtual machines.	■ If a reprotect operation fails to perform reverse replication, make sure that sites are connected, review the reprotect progress in the VMware Site Recovery UI, and start the reprotect task again. If reprotect still does not succeed, run the reprotect task with the **Force Cleanup** option. ■ If Site Recovery Manager fails to create placeholder virtual machines, recovery from the reprotect error is still possible. Review the reprotect steps in the VMware Site Recovery UI, resolve any open issues, and run reprotect again.

Table 9-1. Reprotect States (Continued)

State	Description	Remedial Action
Reprotect Interrupted	Occurs if one of the Site Recovery Manager Servers stops unexpectedly during the reprotect process.	Ensure that both Site Recovery Manager Servers are running and start the reprotect task again.
Ready	Occurs when the reprotect finishes successfully.	None.

Restoring the Pre-Recovery Site Configuration By Performing Failback

10

To restore the original configuration of the protected and recovery sites after a recovery, you can perform a sequence of optional procedures known as failback.

After a planned migration or a disaster recovery, the former recovery site becomes the protected site. Immediately after the recovery, the new protected site has no recovery site to which to recover. If you run reprotect, the new protected site is protected by the original protection site, reversing the original direction of protection. See Chapter 9 Reprotecting Virtual Machines After a Recovery for information about reprotect.

To restore the configuration of the protected and recovery sites to their inital configuration before the recovery, you perform failback.

To perform failback, you run a sequence of reprotect and planned migration operations.

1. Perform a reprotect. The recovery site becomes the protected site. The former protected site becomes the recovery site.
2. Perform a planned migration to shut down the virtual machines on the protected site and start up the virtual machines on the recovery site. To avoid interruptions in virtual machine availability, you might want to run a test before you start the planned migration. If the test identifies errors, you can resolve them before you perform the planned migration.
3. Perform a second reprotect, to revert the protected and recovery sites to their original configuration before the recovery.

You can configure and run a failback when you are ready to restore services to the original protected site, after you have brought it back online after an incident.

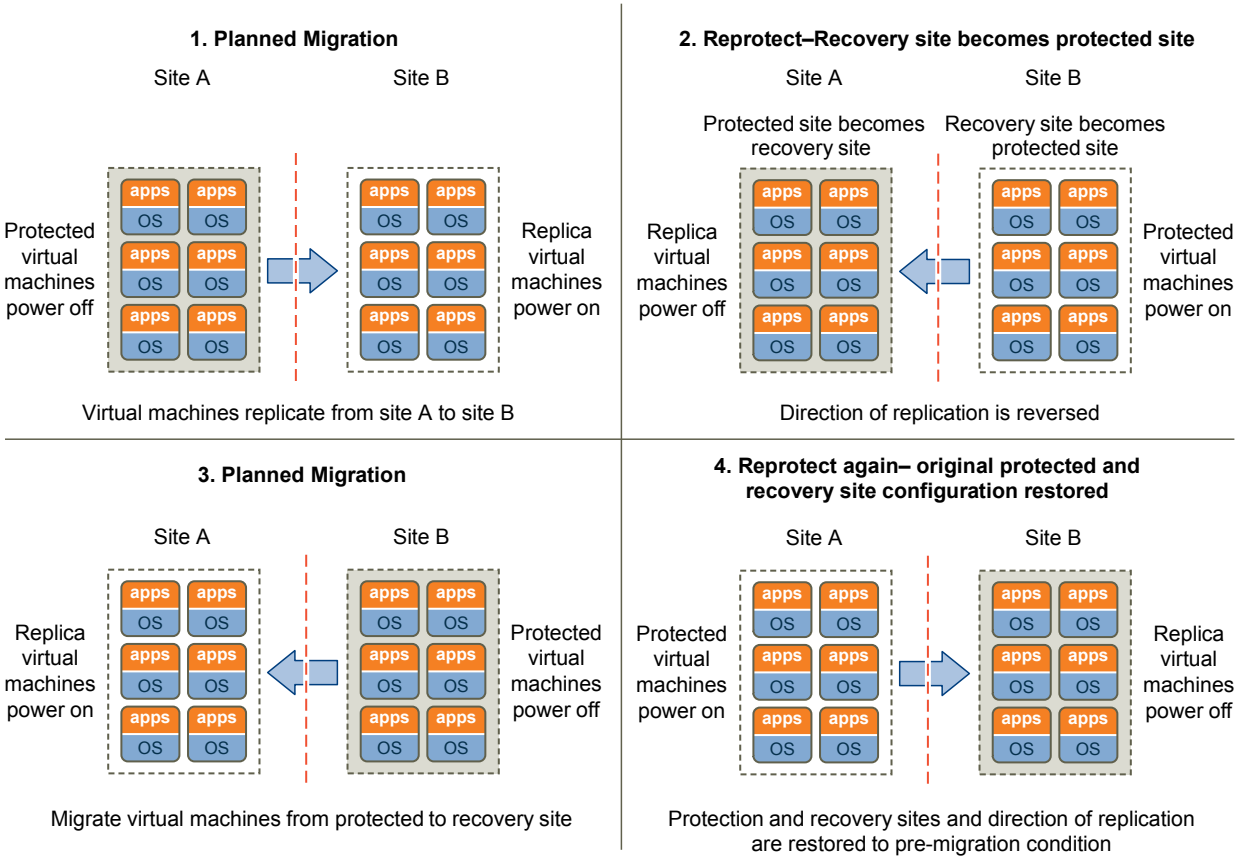
Example: Performing a Failback Operation

Site A is the protected site and B is the recovery site. A recovery occurs, migrating the virtual machines from site A to site B. To restore site A as the protected site, you perform a failback.

1. Virtual machines replicate from site A to site B.
2. Perform a reprotect. Site B, the former recovery site, becomes the protected site.
   Site Recovery Manager uses the protection information to establish the protection of site B. Site A becomes the recovery site.
3. Perform a planned migration to recover the protected virtual machines on site B to site A.

4 Perform a second reprotect. Site A becomes the protected site and site B becomes the recovery site.

Figure 10-1. Site Recovery Manager Failback Process



Perform a Failback

After Site Recovery Manager performs a recovery, you can perform a failback to restore the original configuration of the protected and recovery sites.

To aid comprehension, the original protected site from before a recovery is site A. The original recovery site is site B. After a recovery from site A to site B, the recovered virtual machines are running on site B without protection.

Prerequisites

Verify that the following conditions are in place.

- You have performed a recovery, either as part of a planned migration or as part of a disaster recovery.
- The original protected site, site A, is running.
- If you performed a disaster recovery, you must perform a planned migration recovery when the hosts and datastores on the original protected site, site A, are running again.
- You did not run reprotect since the recovery.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. Select the **Recovery Plans** tab, right-click a recovery plan and select **Reprotect**.
4. Select the check box to confirm that you understand that the reprotect operation is irreversible and determine whether to enable **Force Cleanup**, and click **Next**.

   Force Cleanup is only available after you have run reprotect once and errors occured. Enabling this option forces the removal of virtual machines, ignoring errors, and returns the recovery plan to the ready state.
5. Review the reprotect information and click **Finish**.
6. Select the recovery plan and click **Recovery Steps** to monitor the reprotect operation until it finishes.
7. (Optional) If necessary, rerun reprotect until it finishes without errors.

   At the end of the reprotect operation, Site Recovery Manager has reversed replication, so that the original recovery site, site B, is now the protected site.
8. (Optional) After the test completes, right-click the recovery plan and select **Cleanup** to clean up the recovery plan.
9. Right-click the recovery plan and select **Run** to run the recovery plan as a planned migration.
10. Select the recovery plan and click **Recovery Steps** to monitor the planned migration until it finishes.

    The planned migration shuts down the virtual machines on the new protected site, site B, and starts up the virtual machines on the new recovery site, site A. If necessary, rerun the planned migration until it finishes without errors.

    When the planned migration completes, the virtual machines are running on the original protected site, site A, but the virtual machines are not protected. The virtual machines on the original recovery site, site B, are powered off.
11. Right-click the recovery plan and select **Reprotect** and follow the instructions of the wizard to perform a second reprotect operation.

    Running reprotect again reestablishes protection in the original direction from before the recovery.

You restored the protected and recovery sites to their original configuration before the recovery. The protected site is site A, and the recovery site is site B.

Interoperability of Site Recovery Manager with Other Software

11

Site Recovery Manager Server operates as an extension to the vCenter Server at a site. Site Recovery Manager is compatible with other VMware solutions, and with third-party software.

You can run other VMware solutions such as vCenter Update Manager, vCenter Server Heartbeat, VMware Fault Tolerance, vSphere Storage vMotion, and vSphere Storage DRS in deployments that you protect using Site Recovery Manager. Use caution before you connect other VMware solutions to the vCenter Server instance to which the Site Recovery Manager Server is connected. Connecting other VMware solutions to the same vCenter Server instance as Site Recovery Manager might cause problems when you upgrade Site Recovery Manager or vSphere. Check the compatibility and interoperability of the versions of these solutions with your version of Site Recovery Manager by consulting *VMware Product Interoperability Matrixes*.

This chapter includes the following topics:

Site Recovery Manager and vCenter Server

Site Recovery Manager takes advantage of vCenter Server services, such as storage management, authentication, authorization, and guest customization. Site Recovery Manager also uses the standard set of vSphere administrative tools to manage these services.

Because the Site Recovery Manager Server depends on vCenter Server for some services, you must install and configure vCenter Server at a site before you install Site Recovery Manager.

You can use Site Recovery Manager and vSphere Replication with the vCenter Server Appliance or with a standard vCenter Server installation. You can have vCenter Server Appliance on one site and a standard vCenter Server installation on the other.

How Changes to vCenter Server Inventory Affect Site Recovery Manager

Because Site Recovery Manager protection groups apply to a subset of the vCenter Server inventory, changes to the protected inventory made by vCenter Server administrators and users can affect the integrity of Site Recovery Manager protection and recovery. Site Recovery Manager depends on the availability of certain objects, such as virtual machines, folders, resource pools, and networks, in the vCenter Server inventory at the protected and recovery sites. Deletion of resources such as folders or networks that are referenced by recovery plans can invalidate the plan. Renaming or relocating objects in the vCenter Server inventory does not affect Site Recovery Manager, unless it causes resources to become inaccessible during test or recovery.

In the case of VR, Site Recovery Manager can tolerate certain changes at the protected site without disruption.

- Deleting protected virtual machines.
- Deleting an object for which an inventory mapping exists.

Site Recovery Manager can tolerate certain changes at the recovery site without disruption.

- Moving placeholder virtual machines to a different folder or resource pool.
- Deleting an object for which an inventory map exists.

Site Recovery Manager and the vCenter Server Database

If you update the vCenter Server installation that Site Recovery Manager extends, do not reinitialize the vCenter Server database during the update. Site Recovery Manager stores identification information about all vCenter Server objects in the Site Recovery Manager database. If you reinitialize the vCenter Server database, the identification data that Site Recovery Manager has stored no longer matches identification information in the new vCenter Server instance and objects are not found.

Using Site Recovery Manager with VMware Virtual SAN Storage and vSphere Replication

You can use VMware Virtual SAN storage with Site Recovery Manager and vSphere Replication.

Site Recovery Manager supports vSphere Replication with Virtual SAN.

For information about the compatible versions of vSphere Replication and Virtual SAN, see *VMware Product Interoperability Matrixes* at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

For information about using vSphere Replication with Virtual SAN, see Using vSphere Replication with VMware vSAN Storage.

How Site Recovery Manager Interacts with DPM and DRS During Recovery

Distributed Power Management (DPM) and Distributed Resource Scheduler (DRS) are not mandatory, but Site Recovery Manager supports both services and enabling them provides certain benefits when you use Site Recovery Manager.

DPM is a VMware feature that manages power consumption by ESX hosts. DRS is a VMware facility that manages the assignment of virtual machines to ESX hosts.

Site Recovery Manager temporarily disables DPM for the clusters on the recovery site and ensures that all hosts in the cluster are powered on when recovery or test recovery starts. This allows for sufficient host capacity while recovering virtual machines. After the recovery or test is finished, Site Recovery Manager restores the DPM settings on the cluster on the recovery site to their original values.

For planned migration and reprotect operations, Site Recovery Manager also disables DPM on the affected clusters on the protected site and ensures that all of the hosts in the cluster are powered on. This allows Site Recovery Manager to complete host level operations, for example unmounting datastores or cleaning up storage after a reprotect operation. After the planned migration or reprotect operation has finished, Site Recovery Manager restores the DPM settings on the cluster on the protected site to their original values.

The hosts in the cluster are left in the running state so that DPM can power them down as needed. Site Recovery Manager registers virtual machines across the available ESX hosts in a round-robin order, to distribute the potential load as evenly as possible. Site Recovery Manager always uses DRS placement to balance the load intelligently across hosts before it powers on recovered virtual machines on the recovery site, even if DRS is disabled on the cluster.

If DRS is enabled and in fully automatic mode, DRS might move other virtual machines to further balance the load across the cluster while Site Recovery Manager is powering on the recovered virtual machines. DRS continues to balance all virtual machines across the cluster after Site Recovery Manager has powered on the recovered virtual machines.

How Site Recovery Manager Interacts with Storage DRS or Storage vMotion

You can use Site Recovery Manager when protecting virtual machines on sites that are configured for Storage DRS or Storage vMotion if you follow certain guidelines.

For information about how Site Recovery Manager handles datastore tagging for Storage DRS, see http://kb.vmware.com/kb/2108196.

Using Site Recovery Manager with vSphere Replication on Sites with Storage DRS or Storage vMotion

Follow the guidelines if you use vSphere Replication to protect or recover virtual machines on sites that use Storage DRS or Storage vMotion.

- vSphere Replication is compatible with vSphere Storage DRS on both protected and recovery sites. On the protected site, you can use Storage DRS to move the disk files of virtual machines that vSphere Replication protects, with no impact on the ongoing replication. On the recovery site, you must register the vSphere Replication appliance with the vCenter Single Sign-On service so that Storage DRS can identify the replica disk files on the Storage DRS cluster and generate migration recommendations. You can use Storage DRS to migrate replica disk files with no impact on subsequent recovery. See *Register the vSphere Replication Appliance with vCenter Single Sign-On* from the vSphere Replication documentation for details.
- vSphere Replication is compatible with Storage vMotion on the protected site. You can use Storage vMotion to move the disk files of replicated virtual machines on the protected site with no impact on the ongoing replication.
- Site Recovery Manager detects the changes and fails over the virtual machine successfully.
- Site Recovery Manager supports Storage DRS clusters on the recovery site with datastores containing the vSphere Replication replica disks.
- vSphere Replication is compatible with Storage vMotion and saves the state of a disk or virtual machine when the home directory of a disk or virtual machine moves. Replication of the disk or virtual machine continues normally after the move.
- A full sync causes Storage DRS to generate migration recommendations or directly trigger Storage vMotion if Storage DRS running in fully-automated mode. This happens if the DRS rules are very aggressive, or if a large number of virtual machines perform a full sync at the same time. The default I/O latency threshold for Storage DRS is 15ms. By default, Storage DRS performs loading balancing operations every 8 hours. Storage DRS also waits until it has collected sufficient statistics about the I/O load before it generates Storage vMotion recommendations. Consequently, a full sync only affects Storage DRS recommendations if the full sync lasts for a long time and if, during that time, the additional I/O that the full sync generates causes the latency to exceed the I/O latency threshold.
- When you use Storage DRS in manual mode on protected virtual machine datastores, stale recommendations might exist after a failover. After reprotecting the failed over virtual machines to the original site, if you apply these stale Storage DRS recommendations, the Site Recovery Manager placeholder VM becomes corrupted, causing a subsequent recovery to the original site to fail for the VMs for which the Storage DRS recommendations were applied. If you apply stale updates, unregister the placeholder VM and use the Site Recovery Manager repair operation to recreate a valid placeholder. To avoid this issue, clear any stale recommendations from a prior failover from that site by regenerating Storage DRS recommendations for the affected Storage DRS storage cluster after reprotect successfully completes.

How Site Recovery Manager Interacts with vSphere High Availability

You can use Site Recovery Manager to protect virtual machines on which vSphere High Availability (HA) is enabled.

HA protects virtual machines from ESXi host failures by restarting virtual machines from hosts that fail on new hosts within the same site. Site Recovery Manager protects virtual machines against full site failures by restarting the virtual machines at the recovery site. The key difference between HA and Site Recovery Manager is that HA operates on individual virtual machines and restarts the virtual machines automatically. Site Recovery Manager operates at the recovery plan level and requires a user to initiate a recovery manually.

To transfer the HA settings for a virtual machine onto the recovery site, you must set the HA settings on the placeholder virtual machine before performing recovery, at any time after you have configured the protection of the virtual machine.

You can replicate HA virtual machines by using vSphere Replication. If HA restarts a protected virtual machine on another host on the protected site, vSphere Replication will perform a full sync after the virtual machine restarts.

Site Recovery Manager does not require HA as a prerequisite for protecting virtual machines. Similarly, HA does not require Site Recovery Manager.

Site Recovery Manager and vSphere PowerCLI

VMware vSphere PowerCLI provides a Windows PowerShell interface for command-line access to Site Recovery Manager tasks.

vSphere PowerCLI exposes the Site Recovery Manager APIs. You can use vSphere PowerCLI to administrate Site Recovery Manager or to create scripts that automate Site Recovery Manager tasks.

For information about how to manage Site Recovery Manager by using vSphere PowerCLI, see the vSphere PowerCLI documentation at https://www.vmware.com/support/developer/PowerCLI/.

Site Recovery Manager and vRealize Orchestrator

The vRealize Orchestrator plug-in for Site Recovery Manager allows you to automate certain Site Recovery Manager operations by including them in vRealize Orchestrator workflows.

The vRealize Orchestrator plug-in for Site Recovery Manager includes actions and workflows that run Site Recovery Manager operations. If you are a vRealize Orchestrator administrator, you can create workflows that include the actions and workflows from the Site Recovery Manager plug-in. By including Site Recovery Manager actions and workflows in vRealize Orchestrator workflows, you can combine Site Recovery Manager operations with the automated operations that other vRealize Orchestrator plug-ins provide.

For example, you can create a workflow that uses the actions and workflows of the vRealize Orchestrator plug-in for vCenter Server to create and configure virtual machines and register them with vCenter Server. In the same workflow, you can use the actions and workflows from the Site Recovery Manager plug-in to create protection groups and protect the virtual machines as soon as they are created. You can also use Site Recovery Manager actions and workflows to configure some of the recovery settings for the protected virtual machines. Combining the vCenter Server and Site Recovery Manager actions and workflows in a vRealize Orchestrator workflow thus allows you to automate the process of creating and protecting virtual machines.

You can use the vRealize Orchestrator plug-in for Site Recovery Manager in a shared recovery site configuration, in which you connect multiple Site Recovery Manager instances to a single vCenter Server instance. You can also use the vRealize Orchestrator plug-in for Site Recovery Manager with multiple Site Recovery Manager instances on multiple vCenter Server instances that are connected to the same vCenter Single Sign-On server.

For information about creating workflows by using vRealize Orchestrator, see the vRealize Orchestrator documentation.

For information about how to use the vRealize Orchestrator plug-in for Site Recovery Manager, see the *Using the vRealize Orchestrator Plug-In for Site Recovery Manager* documentation.

Using Site Recovery Manager with SIOC Datastores

Site Recovery Manager fully supports storage I/O control (SIOC).

Planned Migration of Virtual Machines on Datastores that Use SIOC

In previous releases of Site Recovery Manager you had to disable storage I/O control (SIOC) on datastores that you included in a recovery plan before you ran a planned migration. This release of Site Recovery Manager fully supports SIOC, so you do not have to disable SIOC before you run a planned migration.

Disaster Recovery and Reprotect of Virtual Machines on Datastores that Use SIOC

In previous releases of Site Recovery Manager, if you ran a disaster recovery with SIOC enabled, the recovery would succeed with errors. After the recovery, you had to manually disable SIOC on the protected site and run a planned migration recovery again. You could not run reprotect until you successfully ran a planned migration. This release of Site Recovery Manager fully supports SIOC, so recovery succeeds without errors and you can run planned migration and reprotect after a disaster recovery without disabling SIOC.

Using Site Recovery Manager with Admission Control Clusters

You can use Admission Control on a cluster to reserve resources on the recovery site.

However, using Admission Control can affect disaster recovery by preventing Site Recovery Manager from powering on virtual machines when running a recovery plan. Admission Control can prevent virtual machines from powering on if powering them on would violate the relevant Admission Control constraints.

You can add a command step to a recovery plan to run a PowerCLI script that disables Admission Control during the recovery. See Creating Custom Recovery Steps for information about creating command steps.

1 Create a pre-power on command step in the recovery plan that runs a PowerCLI script to disable Admission Control.

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$false
```

2 Create a post-power on command step in the recovery plan to reenable Admission Control after the virtual machine powers on.

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$true
```

If you disable Admission Control during recovery, you must manually reenable Admission Control after you perform cleanup following a test recovery. Disabling Admission Control might affect the ability of High Availability to restart virtual machines on the recovery site. Do not disable Admission Control for prolonged periods.

Site Recovery Manager and Virtual Machines Attached to RDM Disk Devices

Protection and recovery of virtual machines that are attached to a raw disk mapping (RDM) disk device is subject to certain limitations when you use vSphere Replication.

- vSphere Replication supports RDM devices in virtual mode only, for both the source and target device. If you use vSphere Replication, you cannot protect and recover virtual machines that use RDM in physical compatibility mode.

Site Recovery Manager and Active Directory Domain Controllers

Active Directory provides its own replication technology and restore mode.

Do not use Site Recovery Manager to protect Active Directory domain controllers. Use the Active Directory replication technology and restore mode technologies to handle disaster recovery situations.

Advanced Site Recovery Manager Configuration

12

The Site Recovery Manager default configuration enables some simple recovery scenarios. Advanced users can customize Site Recovery Manager to support a broader range of site recovery requirements.

This chapter includes the following topics:

Reconfigure Site Recovery Manager Settings

Using the **Advanced Settings**, you can view or change many custom settings for the Site Recovery Manager service. Advanced Settings provide a way for a user with adequate privileges to change default values that affect the operation of various Site Recovery Manager features.

Important During an upgrade, Site Recovery Manager does not retain any advanced settings that you configured in the previous installation. This is by design. Due to changes in default values or improvements in performance, advanced settings that you set in a previous version of Site Recovery Manager might not be required by or compatible with the new version. Similarly, if you uninstall then reinstall the same version of Site Recovery Manager, reusing the database from the previous installation, advanced settings are not retained.

Change Connections Settings

Site Recovery Manager communicates with other services.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. In the left pane click **Configure > Advanced Settings > Connections**.

4 Select a site, and click **Edit** to change the settings.

Option	Action
Change the number of failed pings before raising a site down event. The default value is 5.	Enter a new value in the **connections.hmsPanicDelay** text box.
Change the number of status checks (pings) to try before declaring the check a failure. The default value is 2.	Enter a new value in the **connections.hmsPingFailedDelay** text box.
Change the timeout value for the wait time for updates from servers. The default value is 900 seconds.	Enter a new value in the **connections.waitForUpdatesTimeout** text box.

5 Click **OK** to save your changes.

Change Site Recovery Manager History Report Collection Setting

Site Recovery Manager history reports are useful to diagnose Site Recovery Manager Server behavior before and after a failure. You can change the number of history reports to export.

When you run failover, test, cleanup, and reprotect operations with site A as the protected site and site B as recovery site, you can export history reports for these operations when you collect a support bundle for Site B, the recovery site. The most recent history is fetched directly from the Site Recovery Manager database.

After reprotect occurs, site A is the new recovery site and site B is the protected site. When you run failover, test, cleanup, and reprotect operations, you can export history reports when you collect a support bundle for site A, the recovery site.

Prerequisites

- Verify that you have Administrator credentials.
- Site Recovery Manager must be connected to a Site Recovery Manager database that you can access with valid database credentials.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 In the left pane click **Configure > Advanced Settings > Export History**.

4 Select a site and click **Edit** to change the settings.

5 Change the value for **exportHistory.numReports** as needed.

You can enter a value from 0 to 50. The default value is 5.

6 To choose not to export reports, change the value to zero (0).

7 Click **OK** to save your changes.

Change Local Site Settings

Site Recovery Manager monitors consumption of resources on the Site Recovery Manager Server host and raises an alarm if a resource threshold is reached. You can change the thresholds and the way that Site Recovery Manager raises the alarms.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 In the left pane click **Configure > Advanced Settings > Local Site Status**.

4 Select a site and click **Edit** to change the settings.

Option	Action
Change the time difference at which Site Recovery Manager checks the CPU usage, disk space, and free memory at the local site. The default value is 60 seconds.	Enter a new value in the **localSiteStatus.checkInterval** text box.
Change the timeout during which Site Recovery Manager waits between raising alarms about CPU usage, disk space, and free memory at the local site. The default value is 600 seconds.	Enter a new value in the **localSiteStatus.eventFrequency** text box.
Change the maximum allowed time difference between server clocks. The default is 20 seconds.	Enter a new value in the**localSiteStatus.maxClockSkew** textbox. If the detected server clock time is off by more than the set number of seconds to the Site Recovery Manager Server clock, Site Recovery Manager raises an event.
Change the percentage of CPU usage that causes Site Recovery Manager to raise a high CPU usage event. The default value is 70.	Enter a new value in the **localSiteStatus.maxCpuUsage** text box.
Change the number of days before the Site Recovery Manager certificate expires before raising a certificate expiring event. The default value is 30 days.	Enter a new value in the **localSiteStatus. minCertRemainingTime** text box.
Change the percentage of free disk space that causes Site Recovery Manager to raise a low disk space event. The default value is 100 Mb.	Enter a new value in the **localSiteStatus.minDiskSpace** text box.
Change the amount of free memory that causes Site Recovery Manager to raise a low memory event. The default value is 32 MB.	Enter a new value in the **localSiteStatus.minMemory** text box.

5 Click **OK** to save your changes.

Change Logging Settings

You can change the levels of logging that Site Recovery Manager provides for the Site Recovery Manager Server components.

Site Recovery Manager Server operates log rotation. When you restart Site Recovery Manager Server, or when a log file becomes large, Site Recovery Manager Server creates a new log file and writes subsequent log messages to the new log file. When Site Recovery Manager Server creates new log files, it compresses the old log files to save space.

You might reduce the logging levels for some Site Recovery Manager Server components because log files become too large too quickly. You might increase logging levels for certain components to help diagnose problems. The list of available logging levels is the same for all Site Recovery Manager Server components.

none	Turns off logging.
quiet	Records minimal log entries.
panic	Records only panic log entries. Panic messages occur in cases of complete failure.
error	Records panic and error log entries. Error messages occur in cases of problems that might or might not result in a failure.
warning	Records panic, error, and warning log entries. Warning messages occur for behavior that is undesirable but that might be part of the expected course of operation.
info	Records panic, error, warning, and information log entries. Information messages provide information about normal operation.
verbose	Records panic, error, warning, information, and verbose log entries. Verbose messages provide more detailed information than information messages.
trivia	Records panic, error, warning, information, verbose, and trivia log entries. Trivia messages provide all available information. This level of logging is useful for debugging but it can produce so much data that it might affect performance. **Note** Set this logging level only when instructed by VMware Support to help resolve a problem.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 In the left pane click **Configure > Advanced Settings > Log Manager**.

4 Select a site and click **Edit** to modify the logging settings.

By default, all components record verbose level logs, unless stated otherwise in the description of the logging level.

Option	Description
Set logging level for all components that do not have an entry in logManager. The default is verbose.	Select a logging level from the **logManager.Default** drop-down menu.
Set logging level for the external API module. The default is verbose.	Select a logging level from the **logManager.ExternalAPI** drop-down menu.
Set logging level for vSphere Replication. The default is verbose.	Select a logging level from the **logManager.HbrProvider** drop-down menu.
Set logging level for the IP Customizer tool. The default is verbose.	Select a logging level from the **logManager.IPCustomizer** drop-down menu.
Set logging level for inventory mapping. The default is verbose.	Select a logging level from the **logManager.InventoryMapper** drop-down menu.
Set logging level for licensing issues. The default is verbose.	Select a logging level from the **logManager.Licensing** drop-down menu.
Set logging level for persistence issues. The default is verbose.	Select a logging level from the **logManager.Persistence** drop-down menu.
Set logging level for recovery operations. The default is verbose.	Select a logging level from the **logManager.Recovery** drop-down menu. By default, recovery logging is set to **verbose**.
Set logging level for recovery configuration operations. The default is verbose.	Select a logging level from the **logManager.RecoveryConfig** drop-down menu.
Set logging level for replication operations. The default is verbose.	Select a logging level from the **logManager.Replication** drop-down menu.
Set logging level for authorization issues between Site Recovery Manager Server and vCenter Server. The default is verbose.	Select a logging level from the **logManager.ServerAuthorization** drop-down menu.
Set logging level for session management. The default is verbose.	Select a logging level from the **logManager.SessionManager** drop-down menu.
Set logging level for the SOAP Web Services adapter. The default is info.	Select a logging level from the **logManager.SoapAdapter** drop-down menu. Due to the levels of traffic that the SOAP adapter generates, setting the logging level to **trivia** might affect performance. By default, SOAP adapter logging is set to **info**.
Set logging level for storage issues. The default is verbose.	Select a logging level from the **logManager.Storage** drop-down menu. **Note** The setting is not supported in Site Recovery Manager 8.0.
Set logging level for storage provider issues. The default is verbose.	Select a logging level from the **logManager.StorageProvider** drop-down menu. **Note** The setting is not supported in Site Recovery Manager 8.0.

5 Click **OK** to save your changes.

The new logging levels apply as soon as you click **OK**. You do not need to restart the Site Recovery Manager service. If you restart Site Recovery Manager Server, logging remains set to the level that you chose.

Change Recovery Settings

You can adjust default values for timeouts that occur when you test or run a recovery plan. You might adjust default values if tasks fail to finish because of timeouts.

Several types of timeouts can occur during recovery plan steps. These timeouts cause the plan to pause for a specified interval to give the step time to finish.

Site Recovery Manager applies some advanced settings to a virtual machine when you configure protection on that virtual machine:

- `recovery.autoDeployGuestAlias`
- `recovery.defaultPriority`
- `recovery.powerOnTimeout`
- `recovery.powerOnDelay`
- `recovery.customizationShutdownTimeout`
- `recovery.customizationTimeout`
- `recovery.skipGuestShutdown`
- `recovery.powerOffTimeout`

Site Recovery Manager keeps a copy of virtual machine recovery settings on each Site Recovery Manager site. If recovery advanced settings are different on the protection and recovery sites,Site Recovery Manager initializes recovery settings for a virtual machine to different values at each site . When Site Recovery Manager recovers the virtual machine from site A to site B, it applies the local recovery settings for site B. When recovering from site B to site A, Site Recovery Manager applies the local recovery settings for site A. This condition exists until you explicitly edit and save individual virtual machine recovery settings from the recovery plan Virtual Machines tab. Recovery settings for the affected virtual machine synchronize and become identical on both Site Recovery Manager sites.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 In the left pane click **Configure > Advanced Settings > Recovery**.

4 Select a site and click **Edit** to modify the recovery site settings.

Option	Action
Enable or disable the automatic configuration of guest user mappings. This option is available only for VMs that use a compatible version of VMware Tools. The default value is true. **For information about the compatible versions of VMware Tools, see *Compatibility Matrixes for Site Recovery Manager 8.0*.**	Select the value of **recovery.autoDeployGuestAlias** to enable or disable the automatic configuration of guest user mappings. If the value is true, Site Recovery Manager creates guest user mappings in the guest OS of all VMs during the recovery and removes them when the recovery finishes. To use this option, you must install a compatible version of VMware Tools and must configure the IP customization or in-guest callout operations on the VMs that you want to recover. Before you run the recovery process, you must ensure the time synchronization between the ESXi hosts and the vCenter Single Sign-On server on the recovery site. If the value is false, you must manually map the local Site Recovery Manager solution user on the recovery site to a guest user account on the protected VM. The guest OS user must have permissions to run commands and access to files in the gust OS. If you configure an IP customization or in-guest callout operations, you must ensure the time synchronization between the guest OS of the protected VM and the vCenter Single Sign-On servers on the recovery site. If your Site Recovery Manager sites are in enhanced linked mode, you can use vSphere Web Client to configure the guest user mappings. For information about how to configure guest user mappings, see the *Configuring User Mappings on Guest Operating Systems* chapter in the *VMware vSphere ESXi and vCenter Server* documentation. If your Site Recovery Manager sites are not in enhanced linked mode, you must use a vSphere API to configure the guest user mappings and to ensure that the alias certificate is mapped. The best practice is to use the signing certificates of the vCenter Single Sign-On server. For information about the vSphere API, see the *VMware vSphere API Reference* documentation.
Change the virtual machine power off timeout in IP customization. The default value is 300 seconds.	Enter a new value in the **recovery.customizationShutdownTimeout** text box. This value is the minimal virtual machine power off timeout in seconds used in IP customization workflow only. If you specify power off timeout in virtual machine recovery settings, the greater value of the two takes precedence.
Change the IP customization timeout. The default value is 600 seconds.	Enter a new value in the **recovery.customizationTimeout** text box. This value is the timeout used in preparation of IP customization scripts on the Site Recovery Manager Server. You rarely need to change this value.
Change the default priority for recovering a virtual machine. The default value is 3.	Enter a new value in the **recovery.defaultPriority** text box.
Enable or disable forced recovery. The default value is false.	Select or deselect the **recovery.forceRecovery** check box. Activate forced recovery in cases where a lack of connectivity to the protected site severely affects RTO. This setting only removes the restriction to select forced recovery when running a recovery plan. To actually enable forced recovery, select it when you run a plan.
Change the timeout for hosts in a cluster to power on. The default value is 1200 seconds.	Enter a new value in the **recovery.hostPowerOnTimeout** text box.

Option	Action
Change the default timeout value to wait for guest shutdown to complete before powering off VMs. The default value is 300 seconds.	Enter a new value in the **recovery.powerOffTimeout** text box. This value defines the guest operating system timeout before power-off is attempted as a last resort to shutting down the virtual machines. **Note** The virtual machines power off when the timeout expires. If the OS of the virtual machine has not completed its shutdown tasks when the timeout expires, data loss might result. For a large virtual machine that requires a longer time to shut down gracefully, set the guest OS power-off timeout individually for that virtual machine as described in Configure Virtual Machine Startup and Shutdown Options.
Change the delay after powering on a virtual machine before starting dependent tasks. The default value is 0.	Enter a new value in the **recovery.powerOnDelay** text box. The new value applies to power-on tasks for virtual machines at the recovery site.
Change the timeout to wait for VMware Tools when powering on virtual machines. The default value is 300 seconds.	Enter a new value in the **recovery.powerOnTimeout** text box. The new power-on value applies to power-on tasks for virtual machines at the recovery site. If protected virtual machines do not have VMware Tools installed, set this value to 0 to skip waiting for VMware Tools when powering on those VMs and avoid a timeout error in SRM.
Enable or disable skipping the shutdown of the guest OS. The default value is false.	Select or deselect the **recovery.skipGuestShutdown** check box. If skipGuestShutdown=true, Site Recovery Manager does not attempt guest OS shutdown on protection site VMs, but directly powers them off instead. In this case, the value set for recovery.powerOffTimeout has no effect together with this setting. If VMware Tools are not installed in the virtual machine, enable this setting to avoid a guest OS shutdown error in Site Recovery Manager. You can also enable the option to directly power off virtual machines without a shutdown timeout, bypassing the guest OS. See Configure Virtual Machine Startup and Shutdown Options.
Enable or disable automatic VM IP customization during recovery. The default value is true.	Select or deselect the **recovery.useIpMapperAutomatically** check box. If you select the option and IP mapping rules are configured for virtual networks, then Site Recovery Manager evaluates these rules during recovery to customize the VMs. If you deselect the option, the IP mapping rules are not evaluated during recovery. You can override the option for each VM in VM Recovery Settings IP Customization mode.

5 Click **OK** to save your changes.

What to do next

To apply the changes to virtual machines that you have previously protected, you must reconfigure those virtual machines. For example, if you reconfigure the `defaultPriority` setting, you can manually reconfigure the priority of a previously protected virtual machine to match the new `defaultPriority` setting. You can apply changes from either Recovery Plans or from Protection Groups.

See Apply Recovery Settings to Virtual Machines in a Recovery Plan and Apply Recovery Settings to Virtual Machines in a Protection Group.

Apply Recovery Settings to Virtual Machines in a Recovery Plan

If you change advanced recovery settings on a protected virtual machine, you must reconfigure the virtual machine for the settings to take effect.

You can more efficiently configure recovery settings in a recovery plan if you target a single setting or a single virtual machine. In some cases, you can apply a setting only this way, for example, if you change settings in a disaster recovery or incomplete recovery scenario.

Procedure

1. On the VMware Site Recovery home tab, select a site pair and click **Open**.
2. Select the **Recovery Plans** tab and click on the recovery plan to which the virtual machine belongs.
3. On the **Virtual Machines** tab, right-click a virtual machine and click **Configure Recovery**.
4. Make the changes you want to the recovery properties settings.
5. Click **OK**.

What to do next

To apply recovery settings to virtual machines in a Protection Group, see Apply Recovery Settings to Virtual Machines in a Protection Group.

Apply Recovery Settings to Virtual Machines in a Protection Group

If you change advanced recovery settings for protected virtual machines, the new settings do not take effect until the virtual machines are reconfigured.

You can more conveniently update recovery settings by using the Protection Groups feature when you apply settings to multiple virtual machines, although it can be used for a single virtual machine. You can select all of the virtual machines in a protection group and update the settings all at once.

Procedure

1. On the VMware Site Recovery home tab, select a site pair and click **Open**.
2. Select the **Protection Groups** tab and click on the protection group to which the virtual machine belongs.
3. On the **Virtual Machines** tab, right-click a virtual machine and click **Remove Protection**.

   The virtual machine status changes to Not Configured.
4. Click **Configure All VMs** to reconfigure all virtual machines in the protection group, or select a virtual machine and click **Configure Protection** to reconfigure only that virtual machine.

What to do next

To apply recovery settings to a virtual machine in a recovery plan, see Apply Recovery Settings to Virtual Machines in a Recovery Plan.

Change Remote Manager Settings

If you run tasks that take a long time to complete, the default timeout period on the remote site might elapse before the task completes. You can configure additional timeouts to allow long-running tasks to finish.

A long-running task might be the test recovery or cleanup of a large virtual machine. If a virtual machine has large disks, it can take a long time to perform a test recovery or to perform a full recovery. The default timeout period monitors the connectivity between the sites, so if a task takes a longer time to complete than the default timeout period and does not send notifications to the other site while it is running, timeouts can result. In this case, you can change the remote manager settings so that Site Recovery Manager does not time out before a long-running task finishes.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. In the left pane click **Configure > Advanced Settings > Remote Manager**.
4. Select a site and click **Edit** to modify the remote manager settings.

Option	Action
Configure the maximum time to wait for a remote operation to complete. The default value is 900 seconds.	Enter a value for **remoteManager.defaultTimeout**.
Mark a virtual machine as protected by Site Recovery Manager. The default value is true.	Select the checkbox to enable the value **remoteManager.enableCustomFields**.
Set a time period to wait for requests to aggregate at the remote site. The default value is 2000 milliseconds.	Enter a value for **remoteManager.powerOnAggregationInterval**.
Configure the maximum time to wait for cancelled tasks to stop. The default value is 300 seconds.	Enter a value for **remoteManager.taskCancelDefaultTimeout**.
Configure an additional timeout period for tasks to complete on the remote site. The default value is 900 seconds.	Enter a value for **remoteManager.taskDefaultTimeout**.
Configure the number of seconds to wait for a timed out task to report progress. The default value is 180 seconds.	Enter a value for **remoteManager.taskProgressDefaultTimeout**. The task is allowed more time to complete if progress update is received within that time.
Configure the number of seconds to wait for a timeout of xVC-vMotion. The default value is 3600 seconds.	Enter a value for **remoteManager.xVcVMotionTimeout**. **Note** The setting is not supported in Site Recovery Manager 8.0.

5. Click **OK** to save your changes.

Change Remote Site Settings

You can modify the default values that the Site Recovery Manager Server at the protected site uses to determine whether the Site Recovery Manager Server at the remote site is available.

Site Recovery Manager monitors the connection between the protected site and the recovery site and raises alarms if the connection breaks. You can change the criteria that cause Site Recovery Manager to raise a connection event and change the way that Site Recovery Manager raises alarms.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. In the left pane click **Configure > Advanced Settings > Remote Site Status**.
4. Select a site and click **Edit** to modify the settings.

Option	Action
Change the number of failed pings before raising a site down event. The default value is 5.	Enter a new value in the **remoteSiteStatus.drPanicDelay** text box.
Change the number of remote site status checks (pings) to try before declaring the check a failure. The default value is 2.	Enter a new value in the **remoteSiteStatus.drPingFailedDelay** text box.

5. Click **OK** to save your changes.

Change Replication Settings

You can edit replication settings to modify how long Site Recovery Manager waits for the creation of virtual machine placeholders to finish.

Procedure

1. In the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the VMware Site Recovery home tab, select a site pair and click **Open**.
3. In the left pane click **Configure > Advanced Settings > Replication**.
4. Click **Edit** to change the settings.

Option	Action
Skip the check for non-protected replica virtual machines while deactivating the protection site during Planned Migration. The default value is false.	Move the slider to enable the value **replication.disablePiggybackVmsCheckDuringDeactivate**. **Note** The setting is not supported in Site Recovery Manager 8.0.
Change the timeout in seconds to wait when creating a placeholder virtual machine. The default value is 300 seconds.	Enter a new value in the **replication.placeholderVmCreationTimeout** text box.
Periodically poll the virtual machines in storage policy protection groups for missing mappings and report a warning if any mappings are missing that can cause the storage policy protection group recovery to fail. The default value is false.	Move the slider to change the value **replication.pollForMissingInventoryMappings** to true. **Note** The setting is not supported in Site Recovery Manager 8.0.

Option	Action
Change the timeout in seconds to wait for consistency group information to be replicated to the remote site before starting an online sync on that site. The default is 900 seconds.	Enter a new value in the **replication.protectionInfoSyncTimeout** textbox. **Note** The setting is not supported in Site Recovery Manager 8.0.
Change the interval in seconds to poll the storage policy protection groups and missing inventory mappings. The default value is 120 seconds.	Enter a new value in the **replication.protectionPollInterval** textbox. **Note** The setting is not supported in Site Recovery Manager 8.0.

5 Click **OK** to save your changes.

Change SSO Setting

You can modify the Single Sign On setting for Site Recovery Manager to renew SSO tokens.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 In the left pane click **Configure > Advanced Settings > SSO**.

4 Click **Edit** to change the **sso.sts.tokenLifetime** setting to specify the number of seconds to use SSO tokens before they are renewed.

The default value is 28800 seconds (8 hours).

5 Click **OK** to save your changes.

Change vSphere Replication Settings

You can adjust global settings to change how Site Recovery Manager interacts with vSphere Replication.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 In the left pane click **Configure > Advanced Settings > vSphere Replication**.

4 Click **Edit** to modify the vSphere Replication settings.

Option	Description
Allow Site Recovery Manager to recover virtual machines that are managed by other solutions. The default value is false.	vSphere Replication allows solutions to manage the replication of virtual machines. By default, Site Recovery Manager only recovers the virtual machines that it manages. To allow Site Recovery Manager to recover virtual machines whose replications are managed by other solutions, select the **allowOtherSolutionTagInRecovery** check box.
Keep older multiple point in time (PIT) snapshots during recovery. The default value is true.	If you configure vSphere Replication to take PIT snapshots of protected virtual machines, Site Recovery Manager only recovers the most recent snapshot when you perform a recovery. To recover older PIT snapshots during recovery, select the **preserveMpitImagesAsSnapshots** check box. **Note** The setting is not supported in Site Recovery Manager 8.0.
Change the timeout period for vSphere Replication synchronization operations. The default value is 7200.	Enter a new value in the **synchronizationTimeout** text box. The value that you enter must be half of the timeout time that you want to set. The default value is 7200 and corresponds to a working synchronization timeout period of 14400 seconds. Change this value if you experience timeout errors when vSphere Replication synchronizes virtual machines on the recovery site.
Change the default RPO setting for replications. The default value is 240.	Enter a new value in the **vrReplication.timeDefault** text box. The default value is 240 minutes (4 hours). This value is selected when you configure replications, but you can specify a different RPO in the **Configure Replication** wizard when you configure replication for an individual virtual machine or for a group of virtual machines.

5 Click **OK** to save your changes.

Change Telemetry Settings

You can edit the telemetry settings of Site Recovery Manager to specify a proxy host to use when sending telemetry reports.

Procedure

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

2 On the VMware Site Recovery home tab, select a site pair and click **Open**.

3 In the left pane click **Configure > Advanced Settings > Telemetry**.

4 Click **Edit** to change the settings.

Option	Description
Specify the host name of the HTTP proxy to use when sending telemetry reports.	Enter the name of the HTTP proxy in the **telemetry.proxyHost** text box.
Specify the port for the HTTP proxy to use when sending telemetry reports.	Enter the port number in the **telemetry.proxyPort** box.
Specify whether to use SSL to connect to the HTTP proxy when sending telemetry reports. The default value is false.	Move the slider to change the value **telemetry.proxyUseSsl** to true.

5 Click **OK** to save your changes.

Modify Settings to Run Large Site Recovery Manager Environments

If you use Site Recovery Manager to test or recover a large number of virtual machines, you might need to modify the default Site Recovery Manager settings to achieve the best possible recovery times in your environment or to avoid timeouts.

In large environments, Site Recovery Manager might simultaneously power on or power off large numbers of virtual machines. Simultaneously powering on or powering off large numbers of virtual machines can create a heavy load on the virtual infrastructure, which might lead to timeouts. You can modify certain Site Recovery Manager settings to avoid timeouts, either by limiting the number of power on or power off operations that Site Recovery Manager performs concurrently, or by increasing the timeout periods.

The limits that you set on power on or power off operations depend on how many concurrent power on or power off operations your infrastructure can handle.

You modify certain options in the **Advanced Settings** menus in the vSphere Web Client or in the Site Recovery Manager client plug-in. To modify other settings, you edit the `vmware-dr.xml` configuration file on the Site Recovery Manager Server. Always modify settings by using the client menus when an option exists. If you modify settings, you must make the same modifications on the Site Recovery Manager Server and vCenter Server instances on both the protected and recovery sites.

For descriptions of the settings that you can change, see Settings for Large Site Recovery Manager Environments.

Procedure

1 In the vSphere Web Client, select a cluster.

2 On the **Configure** tab, select **Services > vSphere DRS**.

If you are using vCenter Server 6.0 Update 3, on the **Manage** tab, select **Services > vSphere DRS**

3 Click **Edit**.

4 In **Advanced Options**, set the `srmMaxBootShutdownOps` setting.

Option	Description
Option text box	Enter `srmMaxBootShutdownOps`.
Value text box	Enter the maximum number of boot and shutdown operations, for example 32. If you set the value to 32, the next guest starts booting or shutting down as soon as one of the first batch of 32 has finished, namely. VMs 1 to 32 all start together, then VM 33 starts once one of the first batch has finished, VM 34 starts when the second one of the first batch has finished, and so on.

5 Click **OK** to save your changes.

6 Log in to the Site Recovery Manager Server host.

7 Open the `vmware-dr.xml` file in a text editor.

   You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder.

8 Change the `defaultMaxBootAndShutdownOpsPerCluster` and `defaultMaxBootAndShutdownOpsPerHost` settings in the `vmware-dr.xml` file:

```
<config>
...
   <defaultMaxBootAndShutdownOpsPerCluster>24</defaultMaxBootAndShutdownOpsPerCluster>
   <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
...
</config>
```

   If these elements do not already exist in the `vmware-dr.xml` file, you can add them anywhere in the `<config>` section. If you set the `<defaultMaxBootAndShutdownOpsPerCluster>` value to 24, the next guest starts booting or shutting down as soon as one of the first batch of 24 has finished, namely VMs 1 to 24 all start together, then VM 25 starts once one of the first batch has finished, VM 26 starts when the second one of the first batch has finished, and so on.

9 Restart the Site Recovery Manager Server to apply the new settings.

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

11 On the VMware Site Recovery home tab, select a site pair and click **Open**.

12 In the left pane select **Configure > Advanced Settings > vSphere Replication**, select a site and increase the `vrReplication.synchronizationTimeout` setting.

   The default value is 7200 and corresponds to a working synchronization timeout period of 14400 seconds.

13 Select **Advanced Settings > Storage** and increase the `storage.commandTimeout` setting.

   The default value is 300 seconds.

14 Click **OK** to save your changes.

Settings for Large Site Recovery Manager Environments

To protect a large number of virtual machines, you can modify the default Site Recovery Manager settings to achieve the best possible recovery times in your environment or to avoid timeouts.

You modify certain options in the **Advanced Settings** menu in the VMware Site Recovery user interface. To modify other settings, you edit the `vmware-dr.xml` configuration file on the Site Recovery Manager Server. Always modify settings by using the client menus when an option exists. If you modify settings, you must make the same modifications on the Site Recovery Manager Server and vCenter Server instances on both the protected and recovery sites.

To modify the settings, see Modify Settings to Run Large Site Recovery Manager Environments.

Table 12-1. Settings that Modify the Number of Simultaneous Power On or Power Off Operations

Option	Description
srmMaxBootShutdownOps	Specifies the maximum number of concurrent power-on operations for any given cluster. Guest shutdowns, but not forced power offs, are throttled according to this value. Guest shutdowns occur during primary site shutdowns (planned failover) and IP customization workflows. Modify this option per cluster in the vSphere Web Client by right-clicking a cluster and selecting **Settings**. Click **vSphere DRS**, then **Edit > Advanced Options**. Type the option to override the **defaultMaxBootAndShutdownOpsPerCluster** value that you can set in the `vmware-dr.xml` file. You can set a global value **defaultMaxBootAndShutdownOpsPerCluster** in the `vmware-dr.xml` file, and then set different **srmMaxBootShutdownOps** values for individual clusters in the vSphere Web Client. By default, throttling is turned off.
defaultMaxBootAndShutdownOpsPerCluster	Specifies the maximum number of concurrent power-on operations for all clusters that Site Recovery Manager protects. Guest shutdowns, but not forced power offs, are throttled according to this value. Guest shutdowns occur during primary site shutdowns (planned failover) and IP customization workflows. You modify this setting in the `vmware-dr.xml` file. The **srmMaxBootShutdownOps** value that you can set in the vSphere Web Client overrides the **defaultMaxBootAndShutdownOpsPerCluster** value. You can set a global value **defaultMaxBootAndShutdownOpsPerCluster** in the `vmware-dr.xml` file, and then set different **srmMaxBootShutdownOps** values for individual clusters in the vSphere Web Client. By default, throttling is turned off.
defaultMaxBootAndShutdownOpsPerHost	Specifies the maximum number of concurrent power-on operations on any standalone host. You can only set the option in the `vmware-dr.xml` file. By default, throttling is turned off.

Table 12-2. Settings that Modify Timeout Periods

Option	Description
vrReplication.synchronizationTimeout	Site Recovery Manager enforces a timeout to complete an online or offline synchronization for virtual machines replicated by vSphere Replication during a test or failover. If a synchronization does not finish within the given timeout, for example, because of a slow network or a large virtual machine, Site Recovery Manager reports a failure during a test or failover. Modify this option in the vSphere Web Client. In **Site Recovery**, select a site. On the **Manage** tab, select **Advanced Settings > vSphere Replication**. The default value is 7200 and corresponds to a working synchronization timeout period of 14400 seconds.

Site Recovery Manager Events and Alarms

13

Site Recovery Manager supports event logging. Each event includes a corresponding alarm that Site Recovery Manager can trigger if the event occurs. This provides a way to track the health of your system and to resolve potential issues before they affect the protection that Site Recovery Manager provides.

This chapter includes the following topics:

How Site Recovery Manager Monitors Connections Between Sites

Site Recovery Manager monitors the connection between the protected and recovery sites and logs events if the remote site stops responding.

When Site Recovery Manager establishes the connection between two paired Site Recovery Manager Server instances, the Site Recovery Manager Server that initiated the connection sends a `RemoteSiteUpEvent`.

If Site Recovery Manager detects that a monitored connection has broken, it starts periodic connection checks by sending a `ping` request to the remote site. Site Recovery Manager monitors the connection checks and logs events.

- Site Recovery Manager sends pings at regular intervals. You can configure this interval by setting the `remoteSiteStatus.pingInterval` value. The default is 300 seconds.
- The connection monitor skips a number of failed pings. You can configure this number by setting the `remoteSiteStatus.pingFailedDelay` value. The default is 2.
- When the number of skipped failed pings exceeds the value of the `remoteSiteStatus.pingFailedDelay` setting, Site Recovery Manager sends a `RemoteSitePingFailedEvent` event.
- When the number of skipped failed pings exceeds a higher limit Site Recovery Manager sends a `RemoteSiteDownEvent` event for every failed ping and stops sending `RemoteSitePingFailedEvent` events. You can configure this higher limit of failed pings by setting the `remoteSiteStatus.panicDelay` setting. The default is 5.

- Site Recovery Manager continues to send `RemoteSiteDownEvent` events until the connection is reestablished.
- When a connection to the remote site Site Recovery Manager Server is reestablished, Site Recovery Manager sends `RemoteSiteUpEvent` events.

Site Recovery Manager Events Reference

Site Recovery Manager monitors different types of events.

Site Status Events

Site status events provide information about the status of the protected and recovery sites and the connection between them.

Table 13-1. Site Status Events

Event Name	Event Type	Event Description	Category
Unknown status	`UnknownStatusEvent`	Site Recovery Manager Server status is not available	Info
Remote site down	`RemoteSiteDownEvent`	Site Recovery Manager Server has lost its connection with the remote Site Recovery Manager Server.	Error
Remote site ping failed	`RemoteSitePingFailedEvent`	Failures at the remote site or network connectivity problems.	Warning
Remote site created	`RemoteSiteCreatedEvent`	Local site has been successfully paired with the remote site.	Info
Remote site up	`RemoteSiteUpEvent`	Site Recovery Manager Server re-establishes its connection with the remote Site Recovery Manager Server.	Info
Remote site deleted	`RemoteSiteDeletedEvent`	Remote Site Recovery Manager site has been deleted.	Info
vSphere Replication replicated virtual machine is added to a protection group	`HbrGroupVmAssociatedEvent`	A virtual machine replicated by vSphere Replication is added to a protection group.	Info
vSphere Replication replicated virtual machine is removed from a protection group	`HbrGroupVmDisassociatedEvent`	A virtual machine replicated by vSphere Replication is removed from a protection group.	Info
Local vSphere Replication Server is down	`LocalHmsConnectionDownEvent`	Repeated connection attempts to vSphere Replication fail.	Error
The connection to the local vSphere Replication Server has been restored	`LocalHmsConnectionUpEvent`	Connection to vSphere Replication is successful.	Info
The local vSphere Replication Server is not responding	`LocalHmsPingFailedEvent`	Failure to establish connection to the local vSphere Replication Server	Warning
Low disk space	`LowDiskSpaceEvent`	Free disk space on the local site is low.	Warning

Table 13-1. Site Status Events (Continued)

Event Name	Event Type	Event Description	Category
Low memory	LowMemoryEvent	Available memory on the local site is low.	Warning
SRM Server certificate not yet valid	SrmCertificateNotValidEvent	The SSL/TLS certificate for the specified SRM Server is in the future.	Error
SRM Server certificate expiring	SrmCertificateExpiringEvent	The SSL/TLS certificate for the specified SRM Server expires in the specified number of days.	Info
SRM Server certificate has expired	SrmCertificateExpiredEvent	The SSL/TLS certificate for the specified SRM Server has expired.	Error

Protection Group Events

Protection Group events provide information about actions and status related to protection groups.

Table 13-2. Protection Group Replication Events

Event	Description	Cause	Category
CreatedEvent	Created protection group.	Posted on both vCenter Servers in the completion of the Commit phase of creating a protection group.	Info
RemovedEvent	Removed protection group.	Posted on both vCenter Servers in the completion of the Commit phase of removing a protection group.	Info
ReconfiguredEvent	Reconfigured protection group.	Posted on both vCenter Servers in the completion of the Commit phase of reconfiguring a protection group.	Info
ProtectedVmCreatedEvent	Virtual machine in group is configured for protection.	Posted on both vCenter Servers in the completion of the Commit phase of the protection of a virtual machine.	Info
ProtectedVmRemovedEvent	Virtual machine in group is no longer configured for protection.	Posted on both vCenter Servers in the completion of the Commit phase of unprotecting a virtual machine.	Info
ProtectedVmReconfiguredProtectionSettingsEvent	Reconfigured protection settings for virtual machine.	Posted on both vCenter Servers in the completion of the Commit phase of reconfiguring virtual machine protection settings.	Info
ProtectedVmReconfiguredRecoveryLocationSettingsEvent	Reconfigured recovery location settings for virtual machine.	Posted on the protected site vCenter Server only on the successful completion of reconfiguring the recovery location settings for a protected virtual machine.	Info
PlaceholderVmCreatedEvent	The placeholder virtual machine was created in the vCenter Server inventory.	Posted on the recovery site vCenter Server placeholder virtual machine is created as a result of protection, repair operation.	Info

Table 13-2. Protection Group Replication Events (Continued)

Event	Description	Cause	Category
PlaceholderVmCreatedFromOldProductionVmEvent	The placeholder virtual machine was created in the vCenter Server inventory using the identity of the old protected virtual machine.	Posted on the recovery site vCenter Server placeholder virtual machine is created as a result of swapping the old protected virtual machine with a placeholder virtual machine during or after reprotect operation .	Info
VmFullyProtectedEvent	Virtual machine in group: Unresolved devices have all been resolved.	A protected virtual machine's previously unresolved devices have all been resolved.	Warning
VmNotFullyProtectedEvent	Virtual machine in group: One or more devices need to be configured for protection.	Posted on the protected site vCenter Server only upon device handling updating the recovery location settings with a non-empty unresolvedDevices set. This can be triggered by changes to the protected virtual machine or during reprotect of a virtual machine.	Warning
PlaceholderVmUnexpectedlyDeletedEvent	Virtual machine in group: The placeholder virtual machine was removed from the vCenter Server inventory.	Posted on the recovery site vCenter Server when Site Recovery Manager detects that the placeholder virtual machine was unexpectedly deleted or removed from the vCenter Server inventory.	Warning
ProductionVmDeletedEvent	Virtual machine in group: The protected virtual machine has been removed from the virtual machine vCenter Server inventory.	Posted when a protected virtual machine is deleted or removed from the vCenter Server inventory.	Error
ProductionVmInvalidEvent	Virtual machine in group: Cannot resolve the file locations of the protected virtual machine for replication.	Posted when the replication provider cannot find the protected virtual machine files in order to replicate them.	Error

Recovery Events

Recovery events provide information about actions and status related to the Site Recovery Manager recovery processes.

Table 13-3. Recovery Events

Event Name	Event Type	Event Description	Category
Recovery plan has begun recovering the specified virtual machine.	RecoveryVmBegin	Signaled when the recovery virtual machine was successfully created. If some error occurred before the virtual machine ID is known the event is not fired.	Info
Recovery plan has completed recovering the virtual machine.	RecoveryVmEnd	Signaled after the last post-power on script has completed, or after a recovery-stopping error has occurred for the virtual machine.	Info

Table 13-3. Recovery Events (Continued)

Event Name	Event Type	Event Description	Category
Recovery plan *hostname*has been created.	`PlanCreated`	Signaled when a new plan is created. It is sent to each vCenter Server instance where the plan is hosted.	Info
Recovery plan has been destroyed.	`PlanDestroy`	Signaled when a plan has been deleted from the site. Note that on the site where the plan has been requested to be deleted there can be a significant delay, while it waits for the plan to be deleted at the other site. It will be sent to each vCenter Server instance where the plan is hosted.	Info
Recovery plan was changed.	`PlanEdit`	Signaled when an existing plan is edited.	Info
Recovery plan has begun a test.	`PlanExecTestBegin`	Signaled on the recovery site when a recovery test is initiated.	Info
Recovery plan has completed a test.	`PlanExecTestEnd`	Signaled on the recovery site when a recovery test has completed.	Info
Recovery plan has begun a test cleanup.	`PlanExecCleanupBegin`	Signaled on the recovery site when a test cleanup is initiated.	Info
Recovery plan has completed a test cleanup.	`PlanExecCleanupEnd`	Signaled on the recovery site when a test cleanup has completed.	Info
Recovery plan has begun a recovery.	`PlanExecBegin`	Signaled on the recovery site when a recovery is initiated.	Info
Recovery plan has completed a recovery.	`PlanExecEnd`	Signaled on the recovery site when a recovery has completed.	Info
Recovery plan has begun a reprotect operation.	`PlanExecReprotectBegin`	Signaled on the recovery site when a reprotect is initiated.	Info
Recovery plan has completed a reprotect operation.	`PlanExecReprotectEnd`	Signaled on the recovery site when a reprotect has completed.	Info
Recovery plan is displaying a prompt and is waiting for user input.	`PlanPromptDisplay`	Signaled on the recovery site when a prompt step is encountered. The key is a unique identifier for the prompt.	Info
Recovery plan has received an answer to its prompt.	`PlanPromptResponse`	Signaled on the recovery site when a prompt step is closed.	Info

Table 13-3. Recovery Events (Continued)

Event Name	Event Type	Event Description	Category
Recovery plan has started to run a command on a recovered virtual machine.	PlanVmCommandBegin	Signaled on the recovery site when Site Recovery Manager has started to run a callout command on a recovered virtual machine.	Info
Recovery plan has completed executing a command on a recovered virtual machine.	PlanVmCommandEnd	Signaled on the recovery site when Site Recovery Manager has finished running a callout command on a recovered virtual machine.	Info

Licensing Events

Licensing events provide information about changes in Site Recovery Manager licensing status.

Table 13-4. Licensing Events

Event	Description	Cause
LicenseExpiringEvent	The Site Recovery Manager License at the specified site expires in the specified number of days.	Every 24 hours, non-evaluation, expiring licenses are checked for the number of days left. This event is posted with the results.
EvaluationLicenseExpiringEvent	The Site Recovery Manager Evaluation License at the specified site expires in the specified number of days.	Every 24 hours, evaluation licenses are checked for the number of days left. This event is posted with the results.
LicenseExpiredEvent	The Site Recovery Manager license at the specified site license has expired.	Every 30 minutes, expired (non-evaluation) licenses will post this event.
EvaluationLicenseExpiredEvent	The Site Recovery Manager Evaluation License at the specified site license has expired.	Every 30 minutes, evaluation licenses will post this event.
UnlicensedFeatureEvent	The Site Recovery Manager license at the specified site is overallocated by the specified number of licenses.	Every 24 hours and upon the protection or unprotection of a virtual machine, this event will be posted if the total number of licenses exceeds the capacity in the license.
LicenseUsageChangedEvent	The Site Recovery Manager license at the specified site is using the specified number out of the total number licenses.	Every 24 hours and upon the protection or unprotection of a virtual machine, this event will be posted if the total number of licenses does not exceed the capacity in the license.

Permissions Events

Permission events provide information about changes to Site Recovery Manager permissions.

Table 13-5. Permissions Events

Event	Description	Cause
PermissionsAddedEvent	Permission created for the entity on Site Recovery Manager.	A permission for the entity was created using the role specified. The IsPropagate flag indicates whether the permission is propagated down the entity hierarchy.
PermissionsDeletedEvent	Permission rule removed for the entity on Site Recovery Manager.	A permission for the entity was deleted.
PermissionsUpdatedEvent	Permission changed for the entity on Site Recovery Manager.	A permission for the indicated entity was modified.

SNMP Traps

Site Recovery Manager sends SNMP traps to community targets defined in vCenter Server. You can configure them using the vSphere Web Client. When you enter localhost or 127.0.0.1 as a target host for SNMP traps, Site Recovery Manager uses the IP address or host name of the vSphere server as configured by the Site Recovery Manager installer.

Table 13-6. SNMP Traps

Event	Description	Cause
RecoveryPlanExecuteTestBeginTrap	This trap is sent when a recovery plan starts a test.	Site Recovery Manager site name, recovery plan name, recovery type, execution state.
RecoveryPlanExecuteTestEndTrap	This trap is sent when a recovery plan ends a test.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, result status.
RecoveryPlanExecuteCleanupBeginTrap	This trap is sent when a recovery plan starts a test cleanup.	Site Recovery Manager site name, recovery plan name, recovery type, execution state.
RecoveryPlanExecuteCleanupEndTrap	This trap is sent a recovery plan ends a test cleanup.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, result status.
RecoveryPlanExecuteBeginTrap	This trap is sent when a recovery plan starts a recovery.	Site Recovery Manager site name, recovery plan name, recovery type, execution state.
RecoveryPlanExecuteEndTrap	This trap is sent when a recovery plan ends a recovery.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, result status.
RecoveryPlanExecuteReprotectBeginTrap	This trap is sent when Site Recovery Manager starts the reprotect workflow for a recovery plan.	Site Recovery Manager site name, recovery plan name, recovery type, execution state.
RecoveryPlanExecuteReprotectEndTrap	This trap is sent when Site Recovery Manager has finished the reprotect workflow for a recovery plan.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, result status.

Table 13-6. SNMP Traps (Continued)

Event	Description	Cause
RecoveryVmBeginTrap	This trap is sent when a recovery plan starts recovering a virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, virtual machine name, virtual machine UUID.
RecoveryVmEndTrap	This trap is sent when a recovery plan has finished recovering a virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, virtual machine name, virtual machine UUID, result status.
RecoveryPlanVmCommandBeginTrap	This trap is sent when a recovery plan starts the execution of a command callout on a recovered virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name, virtual machine name, virtual machine UUID.
RecoveryPlanVmCommandEndTrap	This trap is sent when a recovery plan has finished the execution of a command callout on a recovered virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name, virtual machine name, virtual machine UUID, result status.
RecoveryPlanPromptDisplayTrap	This trap is sent when a recovery plan requires user input before continuing.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, prompt string.
RecoveryPlanPromptResponseTrap	This trap is sent when a recovery plan no longer requires user input before continuing.	Site Recovery Manager site name, recovery plan name, recovery type, and execution state.

Collecting Site Recovery Manager Log Files

14

To help identify the cause of any problems you encounter during the day-to-day running of Site Recovery Manager, you might need to collect Site Recovery Manager log files to review or send to VMware Support.

Site Recovery Manager creates several log files that contain information that can help VMware Support diagnose problems. You can collect the log files for your on-premises installation of Site Recovery Manager manually.

The Site Recovery Manager Server and client use different log files.

The Site Recovery Manager Server log files contain information about the server configuration and messages related to server operations. The Site Recovery Manager Server log bundle also contains system information and history reports of the latest recovery plan executions.

The Site Recovery Manager client log files contain information about the client configuration and messages related to Site Recovery Manager standalone user interface.

Log files from vCenter Server instances and ESXi Server instances that are part of your Site Recovery Manager system might also include information useful for diagnosing Site Recovery Manager problems.

The Site Recovery Manager log file collects or retrieves the files and compresses them in a zipped file that is placed in a location that you choose.

Errors that you encounter during Site Recovery Manager operations appear in error dialog boxes or appear in the **Recent Tasks** window. Most errors also generate an entry in a Site Recovery Manager log file. Check the recent tasks and log files for the recovery site and the protected site.

This chapter includes the following topics:

Collect Site Recovery Manager Log Files Manually

You can download Site Recovery Manager Server log files for your on-premises Site Recovery Manager installation in a log bundle that you generate manually.

Use this information to understand and resolve issues.

Procedure

- Initiate the collection of Site Recovery Manager Server log files from the **Start** menu:
  a Log in to the Site Recovery Manager Server host.
  b Select **Start > Programs > VMware > VMware Site Recovery Manager > Generate VMware vCenter Site Recovery Manager log bundle**.
- Initiate the collection of Site Recovery Manager Server log files from the Windows command line:
  a Start a Windows command shell on the Site Recovery Manager Server host.
  b Change directory to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.
  c Run the following command.

```
cscript srm-support.wsf
```

The individual log files are collected in a file named `srm-support-`*`MM-DD-YYYY-HH-MM`*`.zip`, where *MM-DD-YYYY-HH-MM* indicates the month, day, year, hour, and minute when the log files were created. The log bundle is saved on the desktop by default.

Change Size and Number of Site Recovery Manager Server Log Files

You can change the size, number, and location of Site Recovery Manager Server log files.

You can modify the Site Recovery Manager log settings in the `vmware-dr.xml` configuration file on the Site Recovery Manager Server.

Procedure

1. Log in to the Site Recovery Manager Server host.
2. Open the `vmware-dr.xml` file in a text editor.

   You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder.
3. Find the `<log>` section in the `vmware-dr.xml` file.
4. Set the maximum size in bytes of the logs to retain.

   You set the maximum log size by adding a `<maxFileSize>` section to the `<log>` section. The default is 10485760 bytes.

```
<log>

   <maxFileSize>10485760</maxFileSize>

</log>
```

5 Set the maximum number of log files to retain.

You set the maximum number of logs by adding a <maxFileNum> section to the <log> section. The default is 20 log files.

```
<log>

   <maxFileNum>20</maxFileNum>

</log>
```

6 Change the location on the Site Recovery Manager Server in which to store the logs.

You change the log location by modifying the <directory> section in the <log> section.

```
<log>

   <directory>C:\ProgramData\VMware\VMware vCenter Site Recovery
    Manager\Logs</directory>

</log>
```

7 Change the default prefix for log files.

You change the default prefix by modifying the <name> section in the <log> section.

```
<log>

   <name>vmware-dr</name>

</log>
```

8 Change the logging level.

You change the logging level by modifying the <level> section in the <log> section. The possible logging levels are error, warning, info, verbose, and trivia. If you set the level to trivia, you will see a noticeable negative effect on performance.

```
<log>

   <level>info</level>

</log>
```

9 (Optional) Set the level of logging for Site Recovery Manager Server components.

You can set specific logging levels for components by modifying the appropriate `<level>` sections. For example, you can set the logging level for the recovery component to trivia.

```
<level id="Recovery">
   <logName>Recovery</logName>
   <logLevel>trivia</logLevel>
</level>
```

10 Restart the Site Recovery Manager Server service for changes to take effect.

Configure Site Recovery Manager Core Dumps

You can configure Site Recovery Manager core dump settings to change the location of the core dump files and compress them.

You can modify the Site Recovery Manager core dump settings in the `vmware-dr.xml` configuration file on the Site Recovery Manager Server.

The Site Recovery Manager Server `rundll32.exe` child process monitors the primary Site Recovery Manager Server process for panic exits and is then responsible for generating the core dump.

Procedure

1 Log in to the Site Recovery Manager Server host.

2 Open the `vmware-dr.xml` file in a text editor.

You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder.

3 Change the location on the Site Recovery Manager Server in which to store core dumps.

You change the core dump location by modifying the `<coreDump>` section.

```
<coreDump>C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles</coreDump>
```

The default path is `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles` unless this location does not exist or is not writable. In that case, Site Recovery Manager Server uses `C:\ProgramData\VMware`.

4 Use the core dump system parameters to limit the number of created and compressed dump files.

```
<debug>
  <dumpCoreCompression>true,false</dumpCoreCompression>
  <dumpFullCore>true,false</dumpFullCore>
</debug>
```

Option	Description
dumpCoreCompression	If unspecified, the default value is false. Site Recovery Manager Server does not compress previous core dump files as it creates core dump files. If you specify true, then Site Recovery Manager Server compresses all older core dumps when it generates a new core dump.
dumpFullCore	If unspecified, the default value is false. Site Recovery Manager Server generates a core dump file several MB in size and provides some assistance to support when a problem occurs. If you set this value to true, Site Recovery Manager Server generates a full core dump file that might be several GBs in size, depending on the workload at the time the core dump occurs. This larger file can provide greater assistance to support when a problem occurs. If disk space allows, set this value to true.

5 To modify the maximum number of core dump files, add a row to the `<debug>` section.

```
<maxCoreDumpFiles>max files</maxCoreDumpFiles>
```

If unspecified, the default value is 4. This value specifies the maximum number of core dump files that are retained in the core dump directory. When Site Recovery Manager Server creates core dumps, Site Recovery Manager Server deletes older files as necessary to avoid exceeding the maximum and consuming excessive disk space, especially when `dumpFullCore` is true.

Troubleshooting Site Recovery Manager

15

If you encounter problems with creating protection groups and recovery plans, recovery, or guest customization, you can troubleshoot the problem.

When searching for the cause of a problem, also check the VMware knowledge base at http://kb.vmware.com/.

This chapter includes the following topics:

Powering on Many Virtual Machines Simultaneously on the Recovery Site Can Lead to Errors

When many virtual machines perform boot operations at the same time, you might see errors during array-based and vSphere Replication recovery.

Problem

When powering on many virtual machines simultaneously on the recovery site, you might see these errors in the recovery history reports:

- `The command 'echo "Starting IP customization on Windows ..." > > % VMware_GuestOp_OutputFile%.`
- `Cannot complete customization, possibly due to a scripting runtime error or invalid script parameters.`
- `An error occurred when uploading files to the guest VM.`
- `Timed out waiting for VMware Tools after 600 seconds.`

Cause

By default, Site Recovery Manager does not limit the number of power-on operations that can be performed simultaneously. If you encounter errors while virtual machines power on on the recovery site, you can modify the `vmware-dr.xml` file to set a limit on the number of virtual machines that power on simultaneously.

If you encounter these errors, limit the number of power-on operations on the recovery site according to the capacity of your environment for a standalone host or for a cluster.

Solution

1. On the recovery server, go to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config`.
2. Open the `vmware-dr.xml` file in a text editor.
3. Update the `defaultMaxBootAndShutdownOpsPerCluster` and `defaultMaxBootAndShutdownOpsPerHost` values to limit the number of power-on operations at the recovery site.

   The following example shows how to limit the number of power-on operations to a maximum of 32 per cluster and 4 per standalone host.

   ```
   <config>
     <defaultMaxBootAndShutdownOpsPerCluster>32</defaultMaxBootAndShutdownOpsPerCluster>
     <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
   </config>
   ```

4. Restart the Site Recovery Manager Server service.

LVM.enableResignature=1 Remains Set After a Site Recovery Manager Test Recovery

Site Recovery Manager does not support ESXi environments in which the `LVM.enableResignature` flag is set to 0.

Problem

During a test recovery or an actual recovery, Site Recovery Manager sets `LVM.enableResignature` to 1 if the flag is not already set. Site Recovery Manager sets this flag to resignature snapshot volumes and mounts them on ESXi hosts for recovery. After the operation finishes, the flag remains set to 1.

Cause

Site Recovery Manager does not check how snapshot volumes are presented to ESXi hosts.
Site Recovery Manager does not support setting the `LVM.enableResignature` flag to 0. If you set the flag from 1 to 0, a virtual machine outage might occur each time you perform a test recovery or an actual recovery occurs.

Setting the `LVM.enableResignature` flag on ESXi hosts is a host-wide operation. When this flag is set to 1, during the host rescan or the next host reboot, all snapshot LUNs that are visible to the ESXi host, and that can be resignatured, are resignatured.

If snapshot volumes unrelated to Site Recovery Manager are forcefully mounted to ESXi hosts on the recovery site, these LUNs are resignatured as part of a host rescan during a test recovery or an actual recovery process. As a result, all the virtual machines in these volumes become inaccessible.

Solution

To prevent outages, make sure that no snapshot LUNs that are unrelated to Site Recovery Manager, and that are forcefully mounted, are visible to ESXi hosts on the recovery site.

Adding Virtual Machines to a Protection Group Fails with an Unresolved Devices Error

Adding virtual machines to a protection group fails with an error if you did not map the devices of the virtual machine.

Problem

When you add a virtual machine to a protection group, you see the error `Unable to protect VM '`*`virtual machine name`*`' due to unresolved devices`.

Cause

You did not map the devices of the virtual machine on the protected site to the corresponding devices on the recovery site.

Solution

Configure the protection settings of the virtual machine as described in Modifying the Settings of a Protected Virtual Machine.

Configuring Protection fails with Placeholder Creation Error

When you configure protection on multiple virtual machines, the configuration fails with a placeholder creation error.

Problem

Configuring protection on a large number of virtual machines at the same time fails with either a placeholder creation timeout error or a placeholder creation naming error:

- `Placeholder VM creation error:Operation timed out:300 seconds`
- `Placeholder VM creation error:The name 'placeholder_name' already exists`

This problem occurs when you configure protection in different ways:

- You create a protection group that contains a datastore or datastores that contain a large number of virtual machines.
- You use the **Protection Groups > Virtual Machines > Restore All** option in the Site Recovery Manager interface on a large number of virtual machines.
- You use the Site Recovery Manager API to protect a large number of virtual machines manually.

Cause

The infrastructure on the recovery site is unable to handle the volume of concurrent creations of placeholder virtual machines.

Solution

Increase the `replication.placeholderVmCreationTimeout` setting from the default of 300 seconds. See Change Replication Settings.

You do not need to restart Site Recovery Manager Server after changing this setting. Site Recovery Manager applies the setting the next time that you configure protection on a virtual machine.

Rapid Deletion and Recreation of Placeholders Fails

If you delete all of the placeholder virtual machines from a datastore, unmount the datastore, and remount the datastore, recreation of the placeholder virtual machines might fail.

Problem

Recreating the placeholders too rapidly after unmounting the datastore can fail with the error `NoCompatibleHostFound`.

Cause

The associations between ESXi hosts and datastores are updated at 10-minute intervals. If you recreate the placeholders after unmounting and remounting the datastore but before the next update, the host cannot be found.

Solution

Wait for more than 10 minutes after unmounting and remounting the datastore before you recreate the placeholder virtual machines.

Planned Migration Fails Because Host is in an Incorrect State

If you put the ESXi host on the recovery site into maintenance mode during a planned migration, the planned migration fails.

Problem

Planned migration fails with the error `Error – The operation is not allowed in the current state of the host`.

Cause

Site Recovery Manager cannot power on virtual machines on the recovery site when the ESXi host on the recovery site is in maintenance mode.

Solution

Exit maintenance mode on the ESXi host on the recovery site and rerun the planned migration.

Recovery Fails with a Timeout Error During Network Customization for Some Virtual Machines

During a recovery some virtual machines do not recover and show a timeout error during network customization.

Problem

During recovery some virtual machines do not recover within the default timeout period of 120 seconds.

Cause

This problem can occur for one of the following reasons.

- The VMware Tools package is not installed on the virtual machine that you are recovering.
- The cluster on the recovery site is experiencing heavy resource use while trying to simultaneously recover multiple virtual machines. In this case you can increase certain timeout settings to allow more time for tasks to complete. See Change Recovery Settings.

Solution

1 Verify that VMware Tools is installed on the virtual machine that you are recovering.

2 Check the available capacity on the recovery site.

If the recovery site is experiencing heavy resource use, increasing the timeout period for guest customization can resolve the issue.

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

b On the VMware Site Recovery home tab, select a site pair and click **Open**.

c Select **Advanced Settings > Recovery**, select a site, and click **Edit**.

d Increase the `recovery.customizationTimeout` parameter from the default of 600 seconds.

e Increase the `recovery.powerOnTimeout` parameter from the default of 300 seconds.

3 Run the recovery again.

Recovery Fails with Unavailable Host and Datastore Error

Recovery or test recovery fails with an error about host hardware and datastores being unavailable if you run the recovery or test shortly after changes occur in the vCenter Server inventory.

Problem

Recovery or test recovery fails with the error `No host with hardware version '7' and datastore 'ds_id' which are powered on and not in maintenance mode are available....`

Cause

Site Recovery Manager Server keeps a cache of the host inventory state. Sometimes when recent changes occur to the inventory, for example if a host becomes inaccessible, is disconnected, or loses its connection to some of the datastores, Site Recovery Manager Server can require up to 15 minutes to update its cache. If Site Recovery Manager Server has the incorrect host inventory state in its cache, a recovery or test recovery might fail.

Solution

Wait for 15 minutes before running a recovery if you change the host inventory. If you receive the error again, wait for 15 minutes and rerun the recovery.

Reprotect Fails with a vSphere Replication Timeout Error

When you run reprotect on a recovery plan that contains vSphere Replication protection groups, the operation times out with an error.

Problem

Reprotect operations on recovery plans that contain vSphere Replication protection groups fail with the error `Operation timed out: 7200 seconds VR synchronization failed for VRM group <Unavailable>. Operation timed out: 7200 seconds`.

Cause

When you run reprotect, Site Recovery Manager performs an online sync for the vSphere Replication protection group, which might cause the operation to timeout. The default timeout value is 2 hours and corresponds to a working synchronization timeout of 4 hours.

Solution

Increase the `synchronizationTimeout` timeout value in Advanced Settings. See Change vSphere Replication Settings.

Recovery Plan Times Out While Waiting for VMware Tools

Running a recovery plan fails with a timeout error while waiting for VMware Tools to start.

Problem

Recovery operations fail at the Shutdown VMs step or Waiting for VMware Tools step of a recovery plan.

Cause

Site Recovery Manager uses VMware Tools heartbeat to discover when recovered virtual machines are running on the recovery site. Recovery operations require that you install VMware Tools on the protected virtual machines. Recovery fails if you did not install VMware Tools on the protected virtual machines, or if you did not configure Site Recovery Manager to start without waiting for VMware Tools to start.

Solution

Install VMware Tools on the protected virtual machines. If you do not or cannot install VMware Tools on the protected virtual machines, you must configure Site Recovery Manager not to wait for VMware Tools to start in the recovered virtual machines and to skip the guest operating system shutdown step. See Change Recovery Settings.

Synchronization Fails for vSphere Replication Protection Groups

During test recovery, planned migration, and reprotect of recovery plans that contain vSphere Replication protection groups, the virtual machine synchronization step fails with an error.

Problem

Synchronization of virtual machines in a vSphere Replication protection group fails with the error message `Error – VR synchronization failed for VRM group <Unavailable>. The object has already been deleted or has not been completely created.`

Cause

Excessive I/O traffic on one or more of the virtual machines in the protection group causes the synchronization to time out before it can finish. This might occur because of heavy traffic. For example, setting the logging level to trivia mode can generate heavy I/O traffic.

Solution

1. Log in to the Site Recovery Manager Server host.
2. Open the `vmware-dr.xml` file in a text editor.

   You find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder.
3. Add a `<topology><drTaskCleanupTime>` element to the `vmware-dr.xml` file.

   You can add the `<topology>` element anywhere at the top level in the `<Config>` tags. Set the value of `<drTaskCleanupTime>` to at least 300 seconds. If you set the logging level to trivia, set `<drTaskCleanupTime>` to 1000 seconds.

   ```
   <topology>
      <drTaskCleanupTime>1000</drTaskCleanupTime>
   </topology>
   ```
4. Save and close the `vmware-dr.xml` file.
5. Restart the Site Recovery Manager Server service to apply the new settings.

Recovery Sticks at 36% During Planned Migration

If you stop the Site Recovery Manager service on the protected site during a planned migration, the operation sticks at 36%.

Problem

During a planned migration, if you stop the Site Recovery Manager service on the protected site, when the workflow proceeds to step 15 **Unmount protected site storage**, it might not fail gracefully, but instead remains at 36%.

Solution

Click **Cancel** to cancel the workflow, then re-run the workflow.

Recovery Fails Due to Restricted User Permissions

You might receive an error during the recovery process if the Site Recovery Manager solution user does not have permissions to perform an IP customization or in-guest OS callout operations.

Problem

If the Site Recovery Manager solution user does not have appropriate permissions to the guest OS of the recovered VM, you might receive one of the following error messages during the recovery process.

```
GuestPermissionDenied
```

```
CannotAccessFile
```

Cause

The problem appears if the Site Recovery Manager solution user is mapped to a guest OS user that does not have access to a file in the guest OS or permissions to run commands.

Solution

1. If you use Site Recovery Manager to configure the guest user mappings, ensure that the guest OS user who runs the VMware Tools service has access to a file or has permissions to run commands.

   For information about how to enable or disable the automatic configuration of the guest user mappings, see Change Recovery Settings.
2. (Optional) If you manually configure the guest user mappings, map the local Site Recovery Manager solution user on the recovery site to the guest OS user with appropriate permissions.
3. Rerun the recovery plan.

Recovery Fails Due to an Unsupported Combination of VMware Tools and ESXi

The recovery process might fail if the version of VMware Tools installed on your VM and the version of the ESXi host on the recovery site are incompatible with Site Recovery Manager.

Problem

You might receive the following error during the recovery process.

```
OperationNotSupportedByGuest
```

Cause

The problem might appear if you use incompatible versions of VMware Tools and ESXi. For information about the compatibility between Site Recovery Manager, VMware Tools, and ESXi, see *Compatibility Matrixes for Site Recovery Manager 8.0*.

Solution

- Ensure that the versions of VMware Tools and ESXi are compatible with your Site Recovery Manager.

Troubleshooting vSphere Replication

16

Known troubleshooting information can help you diagnose and correct problems that occur while replicating and recovering virtual machines with vSphere Replication.

If you have problems with deploying vSphere Replication, replicating or recovering virtual machines, or connecting to databases, you can troubleshoot them. To help identify the problem, you might need to collect and review vSphere Replication logs and send them to VMware Support.

See Replication States for Virtual Machines and Identifying Replication Problems in the Issues Tab to learn about replication states and how to identify replication issues.

You can also search for solutions to problems in the VMware knowledge base at http://kb.vmware.com.

- Generate vSphere Replication Support Bundle

  You can use the vSphere Replication virtual appliance management interface (VAMI) to generate a support bundle for system monitoring and troubleshooting. A VMware support engineer might request the bundle during a support call.

- vSphere Replication Events and Alarms

  vSphere Replication supports event logging. You can define alarms for each event that can trigger if the event occurs. This feature provides a way to monitor the health of your system and to resolve potential problems, ensuring reliable virtual machine replication.

- Solutions for Common vSphere Replication Problems

  Known troubleshooting information can help you diagnose and correct problems with vSphere Replication.

Generate vSphere Replication Support Bundle

You can use the vSphere Replication virtual appliance management interface (VAMI) to generate a support bundle for system monitoring and troubleshooting. A VMware support engineer might request the bundle during a support call.

To access and download the vSphere Replication logs, you need access to the vSphere Replication VAMI. vSphere Replication rotates its logs when the log file reaches 50MB and keeps at most 12 compressed log files.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
2. Click the **VRM** tab and click **Support**.
3. Click **Generate** to generate a `.zip` package of the current vSphere Replication logs.

   A link to the package containing the replication and system logs appears. Log files from the vSphere Replication appliance and all connected Additional vSphere Replication Servers are included in the same package.
4. Click the link to download the package.
5. (Optional) Click **Delete** next to existing log packages to delete them individually.

Manually Access the vSphere Replication Logs

You can copy and use the vSphere Replication logs for system monitoring and troubleshooting. A VMware support engineer might request these logs during a support call.

Use SCP or Win SCP to copy log folders and files from the vSphere Replication appliance and all Additional vSphere Replication Servers.

- `/opt/vmware/hms/logs/`
- `/opt/vmware/var/log/lighttpd/`
- `/var/log/vmware/`
- `/var/log/boot.msg`

vSphere Replication Events and Alarms

vSphere Replication supports event logging. You can define alarms for each event that can trigger if the event occurs. This feature provides a way to monitor the health of your system and to resolve potential problems, ensuring reliable virtual machine replication.

- Configure vSphere Replication Alarms

  You can define and edit alarms to alert you when a specific vSphere Replication event occurs.
- List of vSphere Replication Events

  vSphere Replication Replication monitors replications and the underlying replication infrastructure, and generates different types of events.

Configure vSphere Replication Alarms

You can define and edit alarms to alert you when a specific vSphere Replication event occurs.

You can create an alarm that triggers when a specific event occurs, such as after you configure a virtual machine for replication. See *View and Edit Alarm Settings in the vSphere Web Client* in the vSphere Web Client documentation.

List of vSphere Replication Events

vSphere Replication Replication monitors replications and the underlying replication infrastructure, and generates different types of events.

Table 16-1. vSphere Replication Events

Event Name	Event Description	Event Type	Category	Event Target
vSphere Replication configured	Virtual machine is configured for vSphere Replication	com.vmware.vcHms.replicationConfiguredEvent	Info	Virtual Machine
vSphere Replication unconfigured	Virtual machine was unconfigured for vSphere Replication	com.vmware.vcHms.replicationUnconfiguredEvent	Info	Virtual Machine
Host configured for vSphere Replication	Host is configured for vSphere Replication	com.vmware.vcHms.hostConfiguredForHbrEvent	Info	Host System
Host unconfigured for vSphere Replication	Host with managed object id <Host Moid> was unconfigured for vSphere Replication	com.vmware.vcHms.hostUnconfiguredForHbrEvent	Info	Folder
Virtual machine is not configured for vSphere Replication	Virtual machine is experiencing problems with vSphere Replication and must be reconfigured	com.vmware.vcHms.vmMissingReplicationConfigurationEvent	Error	Virtual Machine
VM cleaned up from vSphere Replication	Virtual machine cleaned up from vSphere Replication configuration	com.vmware.vcHms.vmReplicationConfigurationRemovedEvent	Info	Virtual Machine
RPO violated	Virtual machine vSphere Replication RPO is violated by <x> minutes	com.vmware.vcHms.rpoViolatedEvent	Error	Virtual Machine
RPO restored	Virtual machine vSphere Replication RPO is not longer violated	com.vmware.vcHms.rpoRestoredEvent	Info	Virtual Machine

Table 16-1. vSphere Replication Events (Continued)

Event Name	Event Description	Event Type	Category	Event Target
Remote vSphere Replication site is disconnected	Connection to the remote vSphere Replication site <siteName> is down	com.vmware.vcHms.remoteSiteDownEvent	Error	Folder
Remote vSphere Replication site is connected	Connection to the remote vSphere Replication site <siteName> is established	com.vmware.vcHms.remoteSiteUpEvent	Info	Folder
VR Server disconnected	vSphere Replication server <VR Server> disconnected	com.vmware.vcHms.hbrDisconnectedEvent	Info	Folder
VR Server reconnected	vSphere Replication server <VR Server> reconnected	com.vmware.vcHms.hbrReconnectedEvent	Info	Folder
Invalid vSphere Replication cleaned up	Virtual machine <VM name> was removed from vCenter Server and its vSphere Replication state was cleaned up	com.vmware.vcHms.replicationCleanedUpEvent	Info	Folder
Virtual machine recovered from replica	Recovered virtual machine <VM Name> from vSphere Replication image	com.vmware.vcHms.vmRecoveredEvent	Info	Virtual Machine
vSphere Replication cannot access datastore	Datastore is not accessible for vSphere Replication Server	com.vmware.vcHms.datastoreInaccessibleEvent	Error	Datastore
vSphere Replication handled a disk addition on a virtual machine	vSphere Replication detected and handled the addition of a disk to virtual machine <VM name>. Disks added are <Disk name>	com.vmware.vcHms.handledVmDiskAddEvent	Info	Virtual Machine
vSphere Replication handled a disk removal on a virtual machine	vSphere Replication detected and handled the addition of a disk to virtual machine <VM name>. Disks added are <Disk name>	com.vmware.vcHms.handledVmDiskRemoveEvent	Info	Virtual Machine

Table 16-1. vSphere Replication Events (Continued)

Event Name	Event Description	Event Type	Category	Event Target
Failed to resolve storage policy	Failed to resolve a specific storage policy for the provided storage profile ID <profile ID> and datastore with managed object ID <Moid>	com.vmware.vcHms.failedResolvingStoragePolicyEvent	Error	Datastore
vSphere Replication paused	vSphere Replication was paused as a result of a configuration change, such as a disk being added or reverting to a snapshot where disk states are different	hbr.primary.SystemPausedReplication	Error	Virtual Machine
Invalid vSphere Replication configuration	Invalid vSphere Replication configuration	hbr.primary.InvalidVmReplicationConfigurationEvent	Error	Virtual Machine
Sync started	Sync started	hbr.primary.DeltaStartedEvent	Info	Virtual Machine
Application consistent sync completed	Application consistent sync completed	hbr.primary.AppQuiescedDeltaCompletedEvent	Info	Virtual Machine
File-system consistent sync completed	File-system consistent sync completed	hbr.primary.FSQuiescedDeltaCompletedEvent	Info	Virtual Machine
Unquiesced crash consistent sync completed	Quiescing failed or the virtual machine is powered off. Unquiesced crash consistent sync completed.	hbr.primary.UnquiescedDeltaCompletedEvent	Warning	Virtual Machine
Crash consistent sync completed	Crash consistent sync completed	hbr.primary.DeltaCompletedEvent	Info	Virtual Machine
Sync failed to start	Sync failed to start	hbr.primary.FailedToStartDeltaEvent	Error	Virtual Machine
Full-sync started	Full-sync started	hbr.primary.SyncStartedEvent	Info	Virtual Machine
Full-sync completed	Full-sync completed	hbr.primary.SyncCompletedEvent	Info	Virtual Machine
Full-sync failed to start	Full-sync failed to start	hbr.primary.FailedToStartSyncEvent	Error	Virtual Machine

Table 16-1. vSphere Replication Events (Continued)

Event Name	Event Description	Event Type	Category	Event Target
Sync aborted	Sync aborted	hbr.primary.DeltaAbortedEvent	Warning	Virtual Machine
No connection to VR Server	No connection to vSphere Replication Server	hbr.primary.NoConnectionToHbrServerEvent	Warning	Virtual Machine
Connection to VR Server restored	Connection to VR Server has been restored	hbr.primary.ConnectionRestoredToHbrServerEvent	Info	Virtual Machine
vSphere Replication configuration changed	vSphere Replication configuration has been changed	hbr.primary.VmReplicationConfigurationChangedEvent	Info	Virtual Machine

Solutions for Common vSphere Replication Problems

Known troubleshooting information can help you diagnose and correct problems with vSphere Replication.

Solution

- Error at vService Bindings When Deploying the vSphere Replication Appliance

  When you deploy the vSphere Replication appliance, you get an error at vService bindings in the Deploy OVF Template wizard.

- OVF Package is Invalid and Cannot be Deployed

  When you attempt to deploy OVF for the vSphere Replication appliance, an OVF package error might occur.

- Connection Errors Between vSphere Replication and SQL Server Cannot be Resolved

  You cannot resolve a connection error between the vSphere Replication appliance and SQL Server.

- Configuring Replication Fails for Virtual Machines with Two Disks on Different Datastores

  If you try to configure vSphere Replication on a virtual machine that includes two disks that are contained in different datastores, the configuration fails.

- vSphere Replication Service Fails with Unresolved Host Error

  If the address of vCenter Server is not set to a fully qualified domain name (FQDN) or to a literal address, the vSphere Replication service can stop unexpectedly or fail to start after a reboot.

- vSphere Replication RPO Violations

  You might encounter RPO violations even if vSphere Replication is running successfully at the recovery site.

- vSphere Replication Does Not Start After Moving the Host

  If you move the ESXi Server on which the vSphere Replication appliance runs to the inventory of another vCenter Server instance, vSphere Replication operations are not available. vSphere Replication operations are also unavailable if you reinstall vCenter Server.
- Unexpected vSphere Replication Failure Results in a Generic Error

  vSphere Replication includes a generic error message in the logs when certain unexpected failures occur.
- vSphere Replication is Inaccessible After Changing vCenter Server Certificate

  If you change the SSL certificate of vCenter Server, you cannot access vSphere Replication.
- Configuring Replication Fails Because Another Virtual Machine has the Same Instance UUID

  You cannot configure a replication because another virtual machine already exists at the target site.
- Unable to Establish an SSH Connection to the vSphere Replication Appliance

  SSH connections to the vSphere Replication appliance are disabled.
- The vSphere Replication Appliance Root File System Switches to Read-only Mode and Login Fails

  The vSphere Replication appliance root file system switches to `read–only` mode, and you cannot log in.

Error at vService Bindings When Deploying the vSphere Replication Appliance

When you deploy the vSphere Replication appliance, you get an error at vService bindings in the Deploy OVF Template wizard.

Problem

When you deploy the vSphere Replication, an error appears at vService bindings in the Deploy OVF Template wizard.

```
Unsupported section '{http://www.vmware.com/schema/ovf}vServiceDependencySection'(A vService
dependency)
```

Cause

This error is typically the result of the vCenter Management Web service being paused or stopped.

Solution

Attempt to start the vCenter Management Web service. If vCenter Server is running as a Linux virtual appliance, reboot the appliance.

OVF Package is Invalid and Cannot be Deployed

When you attempt to deploy OVF for the vSphere Replication appliance, an OVF package error might occur.

Problem

The error `OVF package is invalid and cannot be deployed` might appear while you attempt to deploy the vSphere Replication appliance.

Cause

This problem is due to the vCenter Server port being changed from the default of 80.

Solution

If possible, change the vCenter Server port back to 80.

Connection Errors Between vSphere Replication and SQL Server Cannot be Resolved

You cannot resolve a connection error between the vSphere Replication appliance and SQL Server.

Problem

vSphere Replication might not be able to connect to SQL Server, and you have insufficient information to solve this problem.

Cause

Several issues can cause this problem, and initially available information about the problem is insufficient to affect a resolution.

Solution

1. Use a file management tool to connect to the vSphere Replication appliance.

   For example, you might use SCP or WinSCP. Connect using the root account, which is the same account used to connect to the VAMI.
2. Delete any files you find in `/opt/vmware/hms/logs`.
3. Connect to the VAMI and attempt to save the vSphere Replication configuration.

   This action recreates the SQL error.
4. Connect to the vSphere Replication appliance again and find the `hms-configtool.log` file which is in `/opt/vmware/hms/logs`.

   This log file contains information about the error that just occurred. Use this information to troubleshoot the connection issue, or provide the information to VMware for further assistance. For more details, see*Reconfigure vSphere Replication to Use an External Database* in the *VMware Site Recovery Installation and Configuration* guide.

Configuring Replication Fails for Virtual Machines with Two Disks on Different Datastores

If you try to configure vSphere Replication on a virtual machine that includes two disks that are contained in different datastores, the configuration fails.

Problem

Configuration of replication fails with the following error:

```
Multiple source disks with device keys device_keys point to the same destination datastore and file
path disk_path.
```

Cause

This problem occurs because vSphere Replication does not generate a unique datastore path or file name for the destination virtual disk.

Solution

If you select different datastores for the VMDK files on the protected site, you must also select different datastores for the target VMDK files on the secondary site.

Alternatively, you can create a unique datastore path by placing the VMDK files in separate folders on a single target datastore on the secondary site.

vSphere Replication Service Fails with Unresolved Host Error

If the address of vCenter Server is not set to a fully qualified domain name (FQDN) or to a literal address, the vSphere Replication service can stop unexpectedly or fail to start after a reboot.

Problem

The vSphere Replication service stops running or does not start after a reboot. The error `unable to resolve host: non-fully-qualified-name` appears in the vSphere Replication logs.

Solution

1. In the vSphere Web Client, select the vCenter Server instance and click **Manage > Settings > Advanced Settings** to check that the `VirtualCenter.FQDN` key is set to either a fully qualified domain name or to a literal address.
2. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
3. Review and confirm the browser security exception, if applicable, to proceed to the login page.
4. Type the root user name and password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication appliance.
5. Enter the same FQDN or literal address for vCenter Server as you set for the `VirtualCenter.FQDN` key.
6. Click **Save and Restart Service** to apply the changes.

vSphere Replication RPO Violations

You might encounter RPO violations even if vSphere Replication is running successfully at the recovery site.

Problem

When you replicate virtual machines, you might encounter RPO violations.

Cause

RPO violations might occur for one of the following reasons:

- Network connectivity problems between source hosts and vSphere Replication servers at the target site.
- As a result of changing the IP address, the vSphere Replication server has a different IP address.
- The vSphere Replication server cannot access the target datastore.
- Slow bandwidth between the source hosts and the vSphere Replication servers.

Solution

- Search the `vmkernel.log` at the source host for the vSphere Replication server IP address to see any network connectivity problems.
- Verify that the vSphere Replication server IP address is the same. If it is different, reconfigure all the replications, so that the source hosts use the new IP address.
- Check `/var/log/vmware/*hbrsrv*` at the vSphere Replication appliance at the target site for problems with the server accessing a target datastore.
- To calculate bandwidth requirements, see http://kb.vmware.com/kb/2037268.

vSphere Replication Does Not Start After Moving the Host

If you move the ESXi Server on which the vSphere Replication appliance runs to the inventory of another vCenter Server instance, vSphere Replication operations are not available. vSphere Replication operations are also unavailable if you reinstall vCenter Server.

Problem

If the ESXi Server instance on which vSphere Replication runs is disconnected from vCenter Server and is connected to another vCenter Server instance, you cannot access vSphere Replication functions. If you try to restart vSphere Replication, the service does not start.

Cause

The OVF environment for the vSphere Replication appliance is stored in the vCenter Server database. When the ESXi host is removed from the vCenter Server inventory, the OVF environment for the vSphere Replication appliance is lost. This action disables the mechanisms that the vSphere Replication appliance uses to authenticate with vCenter Server.

Solution

1 (Optional) If possible, redeploy the vSphere Replication appliance and configure all replications and if possible, reuse the existing .vmdk files as initial copies.

   a Power off the old vSphere Replication appliances.

   b Remove any temporary `hbr*` files from the target datastore folders.

   c Deploy new vSphere Replication appliances and connect the sites.

   d Configure all replications, reusing the existing replica .vmdk files as initial copies.

2 (Optional) If you cannot redeploy the vSphere Replication appliance, use the VAMI to connect vSphere Replication to the original vCenter Server instance.

   a Reconnect the ESXi host to vCenter Server.

   b Connect to the VAMI of the vSphere Replication server at https://*vr-server-address*:5480 .

   c Select the **Configuration** tab.

   d Type **`username:password@vcenter_server_address`** in **vCenter Server Address**, where username and password are credentials of the vCenter Server administrator.

   e Type the correct managed object id of the appliance VM in **Appliance VM MO value**. Use the vCenter Server MOB to obtain the appliance id.

   f Click **Save and Restart Service**.

   If you use the VAMI solution, you must repeat the steps each time that you change the vSphere Replication certificate.

Unexpected vSphere Replication Failure Results in a Generic Error

vSphere Replication includes a generic error message in the logs when certain unexpected failures occur.

Problem

Certain unexpected vSphere Replication failures result in the error message

```
A generic error occurred in the vSphere Replication Management Server.
```

In addition to the generic error, the message provides more detailed information about the problem, similar to the following examples.

- `A generic error occurred in the vSphere Replication Management Server. Exception details: 'org.apache.http.conn.HttpHostConnectException: Connection to https://vCenter_Server_address refused'`. This error relates to problems connecting to vCenter Server.
- `Synchronization monitoring has stopped. Please verify replication traffic connectivity between the source host and the target vSphere Replication Server. Synchronization monitoring will resume when connectivity issues are resolved.` This problem relates to a synchronization operation error.

- `Error – Unable to reverse replication for the virtual machine 'virtual machine name'. VRM Server generic error. Please check the documentation for any troubleshooting information. Exception details: 'org.hibernate.exception.LockAcquisitionException: Transaction (Process ID 57) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Rerun the transaction.` This problem relates to a deadlock in Microsoft SQL Server.

Cause

vSphere Replication sends this message when it encounters configuration or infrastructure errors. For example, network issues, database connection issues, or host overload.

Solution

Check the `Exception details` message for information about the problem. Depending on the details of the message, you can choose to retry the failed operation, restart vSphere Replication, or correct the infrastructure.

vSphere Replication is Inaccessible After Changing vCenter Server Certificate

If you change the SSL certificate of vCenter Server, you cannot access vSphere Replication.

Problem

vSphere Replication uses certificate-based authentication to connect to vCenter Server. If you change the vCenter Server certificate, vSphere Replication is inaccessible.

Cause

The vSphere Replication database contains the old vCenter Server certificate.

Solution

- Log into the virtual appliance management interface (VAMI) of the vSphere Replication appliance and click **Configuration > Save and Restart Service**.

  Do not change any configuration information before clicking **Save and Restart Service**.

  vSphere Replication restarts with the new vCenter Server certificate.

Configuring Replication Fails Because Another Virtual Machine has the Same Instance UUID

You cannot configure a replication because another virtual machine already exists at the target site.

Problem

You might see the following error message:

```
Unable to configure replication for virtual machine VM_name because group group_name cannot be created.
Another virtual machine configured_VM_name}' that has the same instance UUID instance_UUID already
exists on protection site source_site_name.
```

Cause

This error message might appear on the following occasions.

- If, due to a connectivity issue or some other problem, an orphaned replication remains on one of the sites while it is deleted from the other site, the orphaned replication prevents you from configuring a new replication for the same virtual machine.
- If you have paired two sites and reinstall the vSphere Replication Management server appliance or reset its database on one of the sites, the other site contains information about the old appliance and database, and prevents you from configuring new replications.

Solution

- If you have not reinstalled the vSphere Replication Management server, an orphaned replication exists in your environment, and you know the GID value of that replication, use the Managed Object Browser (MOB) of the vSphere Replication Management server to delete the replication.
  a Navigate to https://*vrms_address*:8043/mob/?moid=GID-*orphaned_replication_GID*&vmodl=1

    Where *vrms_address* is the IP address of the vSphere Replication Management server.

  b Invoke the destroy method to remove the replication from the site on which the vSphere Replication Management server runs.
- If you have not reinstalled the vSphere Replication Management server and orphaned replication exists in your environment, but you do not know the GID value of that replication, the value can be retrieved from the log files or the vSphere Replication Management server database. Contact VMware Global Support Services for assistance.
- If the vSphere Replication Management server on one of the sites was reinstalled or otherwise reset:
  a Reinstall the vSphere Replication Management server at the other site or reset its database.
  b Connect the sites and register any additional vSphere Replication server appliances.
  c Remove any temporary `hbr*` files left over from the target datastore folders.
  d Configure all replications, reusing the existing replica .vmdk files as replication seeds.

Unable to Establish an SSH Connection to the vSphere Replication Appliance

SSH connections to the vSphere Replication appliance are disabled.

Problem

To apply custom settings to vSphere Replication, you need to establish an SSH connection to the vSphere Replication appliance, and modify certain configuration files.

To transfer files from and to the vSphere Replication appliance, you use SCP or SFTP protocol.

Because the SSH connections are disabled, you cannot apply the changes that you need, and you cannot transfer files.

Cause

By default, SSH connections to the vSphere Replication appliance are disabled to strengthen the security in your environment.

Solution

Prerequisites

Verify that you have the root user credentials to log in to the vSphere Replication appliance.

Procedure

1. In the vSphere Web Client, right-click the vSphere Replication Management (HMS) virtual machine, and select **Open Console**.
2. Log in as the root user, and run the following script.

   ```
   /usr/bin/enable-sshd.sh
   ```

Procedure

The script configures the vSphere Replication appliance to enable SSH connections.

The vSphere Replication Appliance Root File System Switches to Read-only Mode and Login Fails

The vSphere Replication appliance root file system switches to `read-only` mode, and you cannot log in.

Problem

vSphere Replication server cannot update its database and becomes unresponsive. Login through vSphere Replication virtual appliance management interface (VAMI) UI, ssh, or console fails. Attempts to use the appliance console to log in result in the following error message:

`Read-only file system`.

Cause

To prevent data corruption the vSphere Replication appliance is configured to put its root file system in `read-only` mode when it detects a problem with the underlying storage.

Solution

1. Resolve the storage problem or use Storage vMotion to migrate the vSphere Replication appliance to another storage.
2. Reboot the vSphere Replication appliance.
3. Verify that you can log in by using the VAMI UI and the appliance console.