Site Recovery Manager Administration

Site Recovery Manager 5.5

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

Contents

About VMware vCenter Site Recovery Manager Administration

VMware vCenter Site Recovery Manager (Site Recovery Manager) 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. Site Recovery Manager can discover and manage replicated datastores, and automate migration of inventory from one vCenter Server instance to another.

Intended Audience

This book is intended for Site Recovery Manager 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.

Updated Information

Site Recovery Manager Administration is updated with each release of the product or when necessary.

This table provides the update history of *Site Recovery Manager Administration*.

Revision	Description
001112-07	■ Clarified the operation of `defaultMaxBootAndShutdownOpsPerCluster` and `defaultMaxBootAndShutdownOpsPerHost` in Modify Settings to Run Large Site Recovery Manager Environments. ■ Updated the maximum log size of Site Recovery Manager Server in Change Size and Number of Site Recovery Manager Server Log Files. ■ Updated the information about the synchronization timeout period for vSphere Replication in the following topics ■ Change vSphere Replication Settings ■ Settings for Large Site Recovery Manager Environments ■ Modify Settings to Run Large Site Recovery Manager Environments ■ Reprotect Fails with a vSphere Replication Timeout Error ■ Updated the description of the **allowOtherSolutionTagInRecovery** setting in Change vSphere Replication Settings.
001112-06	Included instruction to check recovery plan history for errors after running reprotect in Reprotect Virtual Machines.
001112-05	■ Corrected the syntax of the DR IP Reporter tool in Report IP Address Mappings for Recovery Plans. ■ Added that advanced settings are not retained during upgrade or after uninstalling and reinstalling the same product version in Reconfigure Site Recovery Manager Settings.
001112-04	Corrected Using vSphere Replication with Virtual SAN Storage, Configure Replication for a Single Virtual Machine, and Configure Replication for Multiple Virtual Machines to state that using vSphere Replication with Virtual SAN storage is supported on both the source and target sites.
001112-03	■ Clarified what happens to Site Recovery Manager privileges when you uninstall Site Recovery Manager in Site Recovery Manager Roles Reference. ■ Clarified what happens when per-virtual machine command steps fail in How Site Recovery Manager Handles Custom Recovery Step Failures. ■ Corrected the event names in Recovery Events and Storage and Storage Provider Events.

Revision	Description
001112-02	■ Added statements of full support for VMware Virtual SAN in vSphere 5.5u1 and vSphere Replication 5.5.1. ■ Added that Site Recovery Manager applies IP customization only to the most recent point-in-time snapshot in Replicating a Virtual Machine and Enabling Multiple Point in Time Instances and Recover a Point-in-Time Snapshot of a Virtual Machine. ■ Added sections on limits and point-in-time snapshots to Using vSphere Replication with Virtual SAN Storage. ■ Added that you must use the vSphere Web Client to configure vSphere Replication to Virtual SAN storage in Configure Replication for a Single Virtual Machine and Configure Replication for Multiple Virtual Machines. ■ Added recommendation to configure vSphere Replication in batches of 30 virtual machines when using Virtual SAN storage in Configure Replication for Multiple Virtual Machines. ■ Added information about I/O latency when using vSphere Replication with Virtual SAN storage in Test a Recovery Plan. ■ Clarified descriptions of command recovery steps in Types of Custom Recovery Steps. ■ Listed the settings that are applied to a virtual machine at the moment that you configure protection in Change Recovery Settings. ■ Added new advanced settings for Site Recovery Manager 5.5.1 in Change Storage Provider Settings.
001112-01	Added information about the user account in which command steps run in Types of Custom Recovery Steps.
001112-00	Initial release.

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.

- 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 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.

- 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.

- Managing Permissions in a Shared Recovery Site Configuration

  You can configure Site Recovery Manager to use with a shared recovery site. The vCenter Server administrator on the shared recovery site must manage permissions so that each customer has sufficient privileges to configure and use Site Recovery Manager, but no customer has access to resources that belong to another customer.

- Assign Site Recovery Manager Roles and Permissions

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

- 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.

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. The role authorizes the action, but the action is performed by Site Recovery Manager acting as an administrator. Site Recovery Manager performs the operations by using the administrator 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.

Site Recovery Manager does not perform verification of roles or permissions after installation. 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.

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.

Managing Permissions in a Shared Recovery Site Configuration

You can configure Site Recovery Manager to use with a shared recovery site. The vCenter Server administrator on the shared recovery site must manage permissions so that each customer has sufficient privileges to configure and use Site Recovery Manager, but no customer has access to resources that belong to another customer.

In the context of a shared recovery site, a customer is the owner of a pair of Site Recovery Manager Server instances. Customers with adequate permissions must be able to access the shared recovery site to create, test, and run the recovery plans for their own protected site. The vCenter Server administrator at the shared recovery site must create a separate user group for each customer. No customer's user accounts can be a member of the vCenter Server Administrators group. The only supported configuration for a shared recovery site is for one organization to manage all of the protected sites and the recovery site.

Caution Certain Site Recovery Manager roles allow users to run commands on Site Recovery Manager Server, so you should assign these roles to trusted administrator-level users only. See Site Recovery Manager Roles Reference for the list of Site Recovery Manager roles that run commands on Site Recovery Manager Server.

On a shared recovery site, multiple customers share a single vCenter Server instance. In some cases, multiple customers can share a single ESXi host on the recovery site. You can map the resources on the protected sites to shared resources on the shared recovery site. You might share resources on the recovery site if you do not need to keep all of the customers' virtual machines separate, for example if all of the customers belong to the same organization.

You can also create isolated resources on the shared recovery site and map the resources on the protected sites to their own dedicated resources on the shared recovery site. You might use this configuration if you must keep all of the customers' virtual machines separate from each other, for example if all of the customers belong to different organizations.

Guidelines for Sharing Customer Resources

Follow these guidelines when you configure permissions for sharing customer resources on the shared recovery site:

- All customers must have read access to all folders of the vCenter Server on the shared recovery site.
- Do not give a customer the permission to rename, move, or delete the datacenter or host.
- Do not give a customer the permission to create virtual machines outside of the customer’s dedicated folders and resource pools.
- Do not allow a customer to change roles or assign permissions for objects that are not dedicated to the customer’s own use.
- To prevent unwanted propagation of permissions across different organizations’ resources, do not propagate permissions on the root folder, datacenters, and hosts of the vCenter Server on the shared recovery site.

Guidelines for Isolating Customer Resources

Follow these guidelines when you configure permissions for isolating customer resources on the shared recovery site:

- Assign to each customer a separate virtual machine folder in the vCenter Server inventory.
  - Set permissions on this folder to prevent any other customer from placing their virtual machines in it. For example, set the Administrator role and activate the propagate option for a customer on that customer's folder. This configuration prevents duplicate name errors that might otherwise occur if multiple customers protect virtual machines that have identical names.
  - Place all of the customer's placeholder virtual machines in this folder, so that they can inherit its permissions.
  - Do not assign permissions to access this folder to other customers.
- Assign dedicated resource pools, datastores, and networks to each customer, and configure the permissions in the same way as for folders.

Viewing Tasks and Events in a Shared Recovery Site Configuration

In the Recent Tasks panel of the vSphere Client, users who have permissions to view an object can see tasks that other users start on that object. All customers can see all of the tasks that other users perform on a shared resource. For example, all users can see the tasks that run on a shared host, datacenter, or the vCenter Server root folder.

Events that all of the instances of Site Recovery Manager Server generate on a shared recovery site have identical permissions. All users who can see events from one instance of Site Recovery Manager Server can see events from all Site Recovery Manager Server instances that are running on the shared recovery site.

Assign Site Recovery Manager Roles and Permissions

During installation, Site Recovery Manager administrator rights are assigned to the vCenter Server administrator role. 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 interface. Permission assignments apply 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 Client. You can change Site Recovery Manager permissions from the same 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. Click **Sites** in the Site Recovery Manager interface, and select the site on which to assign permissions.
2. Click the **Permissions** tab.
3. Right-click anywhere in the panel for either the local or remote sites and select **Add Permission**.
4. Click **Add**.
5. Identify a user or group for the role.
   a. From the **Domain** drop-down menu, select the domain that contains the user or group.
   b. Enter a user or user group name in the **Search** text box or select a name from the **Name** list.
   c. Click **Add** and click **OK**.

6 Select a role from the **Assigned Role** drop-down menu to assign to the user or user group that you selected.

The **Assigned 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 Site Recovery Manager Administrator role.
Allow a user or user group to manage and modify protection groups and to configure protection on virtual machines.	Assign the Site Recovery Manager Protection Groups Administrator role.
Allow a user or user group to perform recoveries and test recoveries.	Assign the Site Recovery Manager Recovery Administrator role.
Allow a user or user group to create, modify, and test recovery plans.	Assign the Site Recovery Manager Recovery Plans Administrator role.
Allow a user or user group to test recovery plans.	Assign the Site Recovery Manager Recovery Test Administrator role.

When you select a role, the hierarchical list displays the privileges that the role includes. Click a privilege in the hierarchical list to see a description of that privilege. You cannot modify the list of privileges that each role includes.

7 Select **Propagate to Child Objects** to apply the selected role to all of the child objects of the inventory objects that this role can affect.

For example, if a role contains privileges to modify folders, selecting this option extends the privileges to all the virtual machines in a folder. You might deselect this option to create a more complex hierarchy of permissions. For example, deselect this option to override the permissions that are propagated from the root of a certain node from the hierarchy tree, but without overriding the permissions of the child objects of that node.

8 Click **OK** to assign the role and its associated privileges to the user or user group.

9 Repeat Step 1 through Step 8 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 Site Recovery Manager Recovery Plans Administrator role to one group.

3 Assign the Site Recovery Manager 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 Site Recovery Manager Recovery Plans Administrator and the Site Recovery Manager 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. ■ Perform reprotect operations. ■ Configure protection on virtual machines. ■ Edit protection groups. ■ Remove protection groups. Users with this role cannot run recoveries. Only users with the Site Recovery Manager Recovery Administrator role can perform recoveries.	**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.DiagnosticsExport** **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**	■ Virtual machines ■ Datastores ■ vCenter Server folders ■ Resource pools ■ Site Recovery Manager service instances ■ Networks ■ Site Recovery Manager folders ■ Protection groups ■ Recovery plans ■ Array managers

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 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** **Resource.Recovery Use** **Virtual Machine. SRM Protection.Protect** **Virtual Machine. SRM Protection.Stop**	
Site Recovery Manager Protection Groups Administrator	The Site Recovery Manager Protection Groups Administrator role allows users to manage protection groups. - Create protection groups. - 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.Protection Group.Create** **Site Recovery Manager.Protection Group.Modify** **Site Recovery Manager.Protection Group.Remove** **Datastore.Replication.Protect** **Datastore.Replication.Unprotect** **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
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 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
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

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.

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

Table 1-2. 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. 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**	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 1-2. 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**	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 1-2. 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.

Replicating Virtual Machines 2

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

You can replicate virtual machines by using either array-based replication, vSphere Replication, or a combination of both.

This information concerns replication using vSphere Replication. To configure array-based replication on virtual machines, consult the documentation from your storage array manager (SRA) vendor.

This chapter includes the following topics:

How the Recovery Point Objective Affects Replication Scheduling

The Recovery Point Objective (RPO) value you set during replication configuration affects replication scheduling.

If you set an RPO of x minutes, 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 replication starts.

You set the RPO during replication configuration to 15 minutes. If the replication 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 replication 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.

Replicating a Virtual Machine and Enabling Multiple Point in Time Instances

You can recover virtual machines at specific points in time (PIT) such as the last known consistent state.

Note You cannot use the Site Recovery Manager interface to configure replication that uses point in time (PIT) snapshots. To enable PIT snapshots, configure replication of a virtual machine by using the vSphere Web Client. See Configure Replication for a Single Virtual Machine in *vSphere Replication Administration*.

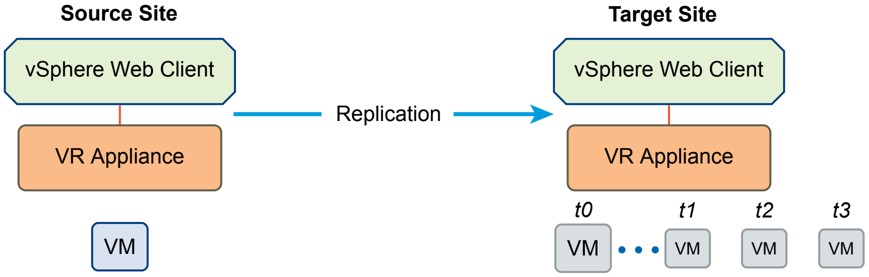
When you configure replication of a virtual machine, you can enable multiple point in time (PIT) instances in the recovery settings in the Configure Replication wizard. vSphere Replication retains a number of snapshot instances of the virtual machine on the target site based on the retention policy that you specify. vSphere Replication supports maximum of 24 snapshot instances. After you recover a virtual machine, you can revert it to a specific snapshot.

During replication, vSphere Replication replicates all aspects of the virtual machine to the target site, including any potential viruses and corrupted applications. If a virtual machine suffers from a virus or corruption and you have configured vSphere Replication to keep PIT snapshots, you can recover the virtual machine and then revert it to a snapshot of the virtual machine in its uncorrupted state.

You can also use the PIT instances to recover the last known good state of a database.

Note vSphere Replication does not replicate virtual machine snapshots.

Figure 2-1. Recovering a Virtual Machine at Points in Time (PIT)



Site Recovery Manager only recovers the most recent PIT snapshot during a recovery. To recover older snapshots, you must enable the **vrReplication > preserveMpitImagesAsSnapshots** option in **Advanced Settings** in the Site Recovery Manager interface. See Change vSphere Replication Settings.

To recover a virtual machine from an older PIT snapshot, you must manually revert the virtual machine to that snapshot after the recovery. See Recover a Point-in-Time Snapshot of a Virtual Machine.

If you recover a PIT snapshot of a virtual machine for which you have configured IP customization, Site Recovery Manager only applies the customization to the most recent PIT snapshot. If you recover an older PIT snapshot of a virtual machine with IP customization, you must configure the IP settings manually.

Using vSphere Replication with Virtual SAN Storage

You can use VMware Virtual SAN datastores as the source and target datastores when configuring replications. Follow the guidelines when using vSphere Replication with Virtual SAN storage.

Note VMware Virtual SAN is a fully supported feature of vSphere 5.5u1.

- You can use Virtual SAN in production environments with vSphere Replication 5.5.1 and vSphere 5.5u1.
- Virtual SAN is an experimental feature in vSphere 5.5. You can perform testing with Virtual SAN with vSphere Replication 5.5.0 and vSphere 5.5, but it is not supported for use in production environments. See the release notes for the vSphere Replication 5.5.0 release for information about how to enable Virtual SAN in vSphere 5.5.

vSphere Replication does not support replicating or recovering virtual machines to the root folders with user-friendly names on Virtual SAN datastores. These names can change, which causes replication errors. When selecting Virtual SAN datastores, always select folders with UUID names, which do not change.

Configuring Replications

When configuring replications for a single virtual machine, vSphere Replication creates the destination folder that you choose, obtains the UUID reference for that folder, and then uses the UUID name rather than the user-friendly name. The UUID name is visible when vSphere Replication displays the target folders when reconfiguring replications.

When configuring replication for multiple virtual machines, create a root folder in the Virtual SAN datastore, obtain its UUID name, and use the folder that is identified by the UUID in the replication wizard.

Configure vSphere Replication on batches of a maximum of 30 virtual machines at a time.

Configuring Replications by Using Replication Seeds

When copying replication seed files to the target datastore, you can use the vSphere Web Client to create a new root folder on a Virtual SAN datastore, or place the files in an existing folder. When you configure replications that use replication seeds, you must select the folder by using its UUID name. Selecting the user-friendly folder names is not supported.

Reconfiguring Replications

If you want to change the destination folder for a disk or the virtual machine config files, you must use the following options:

- Select the UUID name of an existing folder.
- Allow vSphere Replication to create a new folder and obtain its UUID name.

Limits of Using vSphere Replication with Virtual SAN Storage

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

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

Retaining Point-in-Time Snapshots when Using Virtual SAN Storage

Virtual SAN storage stores virtual machine disk files as a set of objects and components. Each disk object in Virtual SAN storage has mirror and witness objects. In the default Virtual SAN storage policy, a disk object has 2 mirrors and one witness. The number of mirror components is determined by the size of the virtual machine disk and the number of failures to tolerate that you set in your Virtual SAN storage policy. A mirror object is divided into components of a maximum size of 256 GB each.

- If a virtual machine has one 256 GB disk and you use the default Virtual SAN storage policy, the disk object will have 2 mirror components of 256 GB each and 1 witness, to make a total of 3 components.
- If a virtual machine has one 512 GB disk and you use the default Virtual SAN storage policy, the disk object will have 4 mirror components of 256 GB each and 1 witness, to make a total of 5 components.

See the *VMware Virtual SAN Design and Sizing Guide* at http://www.vmware.com/products/virtual-san/resources.html for explanations of objects, components, mirrors, witnesses, and Virtual SAN storage policies.

If you enable multiple point-in-time (PIT) snapshots, you must make allowances for the additional components that each snapshot creates in the Virtual SAN storage, based on the number of disks per virtual machine, the size of the disks, the number of PIT snapshots to retain, and the number of failures to tolerate. When retaining PIT snapshots and using Virtual SAN storage, you must calculate the number of extra components that you require for each virtual machine:

Number of disks x *number of PIT snapshots* x *number of mirror and witness components*

Examples of using this formula demonstrate that retaining PIT snapshots rapidly increases the number of components in the Virtual SAN storage for every virtual machine that you configure for vSphere Replication:

- You have a virtual machine with two 256 GB disks for which you retain 10 MPIT snapshots, and you set the default Virtual SAN storage policy:
  - 2 (number of disks) x 10 (number of PIT snapshots) x 3 (2 mirror components + 1 witness) = 60 components for this one virtual machine.
- You have a virtual machine with two 512 GB disks for which you retain 10 PIT snapshots, and you set the default Virtual SAN storage policy:
  - 2 (number of disks) x 10 (number of PIT snapshots) x 5 (4 mirror components of 256 GB each + 1 witness) = 100 components for this one virtual machine.

The number of PIT snapshots that you retain can increase I/O latency on the Virtual SAN storage.

Configure Replication for a Single Virtual Machine

vSphere Replication can protect individual virtual machines and their virtual disks by replicating them to another location.

When you configure replication, you set a recovery point objective (RPO) to determine the period of time between replications. For example, an RPO of 1 hour seeks to ensure that a virtual machine loses no more than 1 hour of data during the recovery. For smaller RPOs, less data is lost in a recovery, but more network bandwidth is consumed keeping the replica up to date.

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 avoid creating large volumes of data 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.

Note You cannot use the Site Recovery Manager interface to configure replication that uses point in time (PIT) snapshots. To enable PIT snapshots, configure replication of a virtual machine by using the vSphere Web Client. See Configure Replication for a Single Virtual Machine in *vSphere Replication Administration*.

To recover a virtual machine from an older PIT snapshot, you must manually revert the virtual machine to that snapshot after the recovery. See Recover a Point-in-Time Snapshot of a Virtual Machine.

vSphere Replication guarantees crash consistency amongst all the disks that belong to a virtual machine. If you use VSS quiescing, you might obtain a higher level of consistency. The available quiescing types are determined by the virtual machine's operating system. See Compatibility Matrixes for vSphere Replication 5.5 for Microsoft Volume Shadow Copy Service (VSS) quiescing support for Windows virtual machines.

You can use vSphere Replication with a Virtual SAN datastore on the source and target sites. However, you must use the vSphere Web Client to configure vSphere Replication when replicating to Virtual SAN storage. The Site Recovery Manager client does not allow you to select Virtual SAN storage when you select the target datastore.

Note VMware Virtual SAN is a fully supported feature of vSphere 5.5u1.

- You can use Virtual SAN in production environments with vSphere Replication 5.5.1 and vSphere 5.5u1.
- Virtual SAN is an experimental feature in vSphere 5.5. You can perform testing with Virtual SAN with vSphere Replication 5.5.0 and vSphere 5.5, but it is not supported for use in production environments. See the release notes for the vSphere Replication 5.5.0 release for information about how to enable Virtual SAN in vSphere 5.5.

Prerequisites

Verify that you have deployed and connected vSphere Replication appliances and Site Recovery Manager Server instances at each site.

Procedure

1. On the vSphere Client Home page, click **VMs and Templates**.
2. Browse the inventory to find the single virtual machine to replicate using vSphere Replication.
3. Right-click the virtual machine and select **vSphere Replication**.
4. Use the RPO slider or enter a value to configure the maximum amount of data that can be lost in the case of a site failure.

   The available RPO range is from 15 minutes to 24 hours.
5. Select a Guest OS Quiescing configuration, if applicable to the source virtual machine operating system.

6 If no target file location is specified or to override the default determined by the datastore mappings, click **Browse** to select a target location for the virtual machine.

Option	Description
Place virtual machine in a datastore directly	Select a datastore and click **OK**.
Place virtual machine in a specific folder in a datastore	Select **Specify datastore folder**, click **Browse** to locate the folder, then double-click the desired folder.

7 Select a replication destination for each media device for the virtual machine.

The next pages are created dynamically depending on the media devices installed on the virtual machine. They might include multiple virtual drives, all of which you can configure individually. Configurable settings include whether the virtual drive is replicated, the virtual drive's replication destination, and information about how the replicated virtual drive is configured. If the disk is to be replicated, select a replication destination for the disk before proceeding.

8 Accept the automatic assignment of a vSphere Replication server or select a particular server on the target site.

9 Review the settings and click **Finish** to establish replication.

vSphere Replication starts an initial full synchronization of the virtual machine files to the designated datastore on the target site.

10 (Optional) Select the vSphere Replication view in the Site Recovery Manager interface.

11 (Optional) Select the remote vSphere Replication site and click the **Virtual Machines** tab.

You can monitor the progress of the initial full synchronization of the virtual machine files to the target site.

Configure Replication for Multiple Virtual Machines

You can configure replication for multiple virtual machines using the configure multiple replications wizard.

When you configure replication, you set a recovery point objective (RPO) to determine the period of time between replications. For example, an RPO of 1 hour seeks to ensure that a virtual machine loses no more than 1 hour of data during the recovery. For smaller RPOs, less data is lost in a recovery, but more network bandwidth is consumed keeping the replica up to date.

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 avoid creating large volumes of data 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.

Note You cannot use the Site Recovery Manager interface to configure replications that use point in time (PIT) snapshots. To enable PIT snapshots, configure replication of virtual machines by using the vSphere Web Client. See Configure Replication for Multiple Virtual Machines in *vSphere Replication Administration*.

To recover a virtual machine from an older PIT snapshot, you must manually revert the virtual machine to that snapshot after the recovery. See Recover a Point-in-Time Snapshot of a Virtual Machine.

vSphere Replication guarantees crash consistency amongst all the disks that belong to a virtual machine. If you use VSS quiescing, you might obtain a higher level of consistency. The available quiescing types are determined by the virtual machine's operating system. See Compatibility Matrixes for vSphere Replication 5.5 for Microsoft Volume Shadow Copy Service (VSS) quiescing support for Windows virtual machines.

You can use vSphere Replication with a Virtual SAN datastore on the source and target sites. However, you must use the vSphere Web Client to configure vSphere Replication when replicating to Virtual SAN storage. The Site Recovery Manager client does not allow you to select Virtual SAN storage when you select the target datastore.

Note VMware Virtual SAN is a fully supported feature of vSphere 5.5u1.

- You can use Virtual SAN in production environments with vSphere Replication 5.5.1 and vSphere 5.5u1.
- Virtual SAN is an experimental feature in vSphere 5.5. You can perform testing with Virtual SAN with vSphere Replication 5.5.0 and vSphere 5.5, but it is not supported for use in production environments. See the release notes for the vSphere Replication 5.5.0 release for information about how to enable Virtual SAN in vSphere 5.5.

Configuring vSphere Replication on a large number of virtual machines simultaneously when using Virtual SAN storage can cause the initial full synchronization of the virtual machine files to run very slowly. Initial full synchronization operations generate heavy I/O traffic and configuring too many replications at the same time can overload the Virtual SAN storage. Configure vSphere Replication on batches of a maximum of 30 virtual machines at a time.

Prerequisites

To replicate virtual machines using vSphere Replication, you must deploy the vSphere Replication appliance at the source and target sites. You must power on the virtual machines to begin replication.

Before you replicate multiple machines, configure datastore mappings in the Site Recovery Manager user interface. You configure the mappings so that information is available to Site Recovery Manager regarding the target datastore destinations for replication.

Procedure

1. On the vSphere Web Client Home page, click **VMs and Templates**.
2. Select a folder or datacenter in the left pane and click the **Virtual Machines** tab.
3. Select the virtual machines to replicate using the Ctrl or Shift keys.
4. Right-click the virtual machines and select **vSphere Replication**.
5. Use the RPO slider or enter a value to configure the maximum amount of data that can be lost in the case of a site failure.

   The available RPO range is from 15 minutes to 24 hours.
6. Select a Guest OS Quiescing configuration, if applicable to the source virtual machine operating system.
7. (Optional) Choose whether to enable **Initial copies of .vmdk files have been placed on the target datastore**.

   Select this option if you have physically copied VMDK files to the target site for use as replication seeds. Site Recovery Manager uses datastore mappings and source virtual machine information to find and use initial copies. Site Recovery Manager shows progress and status as it searches for initial copies. You can stop the search process or start it again.
8. Accept the automatic assignment of a vSphere Replication server or select a particular server on the target site.
9. Review the settings and click **Finish** to establish replication.

   vSphere Replication starts an initial full synchronization of the virtual machine files to the designated datastore on the target site.
10. (Optional) Select the vSphere Replication view in the Site Recovery Manager interface.
11. (Optional) Select the remote vSphere Replication site and click the **Virtual Machines** tab.

    You can monitor the progress of the initial full synchronization of the virtual machine files to the target site.

What to do next

If you did not configure the datastore mappings for vSphere Replication before configuring replication, the virtual machines appear in the **vSphere Replication > Virtual Machines** tab in red with the status `Datastore mappings were not configured`. Configure the datastore mappings and reconfigure vSphere Replication on the virtual machines.

Replicate Virtual Machines By Using Replication Seeds

You can make the initial replication of VDMK files more efficient by physically moving files onto a storage device. vSphere Replication uses the physically moved files as replication seeds.

You might need to use replication seeds if it is not practical to copy the files over the network because the amount of data is too large, the bandwidth available is too small, or some combination of the two.

When replicating virtual machines, ensure that virtual machines are replicated to subdirectories in datastores. Copied disks work if the transfer method preserves the identity information stored in the VMDK file.

Prerequisites

- You deployed the vSphere Replication appliance at both sites.
- You paired the Site Recovery Manager Server instances at each site, and you paired the vSphere Replication appliances.
- Power off the source virtual machine before downloading the VMDK files to use as seeds for the replication. Replication begins when the virtual machine is powered on.

Procedure

1. Use the vSphere Client to connect to a vCenter Server that can manage the virtual machines to be physically moved.
2. Click **Datastores**.
3. In the left pane, browse to the datastore that contains the files for the virtual machine, select the datastore, and in the right pane, click **Browse this datastore**.
4. Select the folders for all virtual machines to be physically moved, right-click the selection, and click **Download**.
5. Select a destination to which to copy the files and click **OK**.
6. Click **Yes**.
7. After the download finishes, transfer the files to a location on the paired site to upload them.
8. On the vSphere Client Home page at the paired site, click **Datastores**.
9. In the left pane, browse to the datastore to contain the files for the virtual machine, select the datastore, and in the right pane, click **Browse this datastore**.
10. Select the folder to contain the copies of the virtual machines, right-click the selection, and click **Upload Folder**.
11. Select the folder containing the virtual machines, and click **OK.**
12. On the protected site, right-click the virtual machine to replicate and select **vSphere Replication**.
13. Set the recovery point objective and target file location as normal and click **Next**.

14 Click **Browse** in the Target Disk File Location panel.

15 Select the target datastore, select the **Specify datastore folder** check box, and click **Browse**.

16 Select the target datastore and click **Open**.

17 Select the datastore folder that contains the seed files, change the file type to All Files, select the VMDK file to use as a replication seed, and click **OK**.

18 Click Yes to confirm that you want to use this file as an initial copy.

19 Follow the prompts to select a vSphere Replication server and click **Finish** to complete the configuration.

Reconfigure Replications

You can reconfigure the replication to enable or disable a virtual machine disk file for replication, modify replication options, such as RPO or the quiescing method. You can also specify a different target datastore for replica configuration and disk files and move the virtual machine to a different vSphere Replication server.

Prerequisites

You configured vSphere Replication on one or more virtual machines.

Procedure

1 Select the vSphere Replication view of the Site Recovery Manager interface.

2 Select a vSphere Replication server and click the **Virtual Machines** tab.

3 Select a virtual machine or use the Ctrl or Shift keys to select multiple virtual machines, right-click and select **Configure Replication**.

4 (Optional) Use the RPO slider or enter a value to reconfigure the maximum amount of data that can be lost in the case of a site failure.

The available RPO range is from 15 minutes to 24 hours.

5 (Optional) Change the Guest OS Quiescing configuration, if applicable to the virtual machine guest operating system

6 (Optional) Change the target location for the virtual machine files.

Option	Description
Reconfigure replication of a single virtual machine	Click **Browse** to change the target location for the virtual machine files.
Reconfigure replication of multiple virtual machines	Select **Initial copies of .vmdk files have been placed on the target datastore** if you have copied replication seeds to a new target datastore.

7 (Optional) Change the replication destination for each media device for the virtual machine.

   The next pages are created dynamically depending on the media devices installed on the virtual machine. They might include multiple virtual drives, all of which you can configure individually. Configurable settings include whether the virtual drive is replicated, the virtual drive's replication destination, and information about how the replicated virtual drive is configured. If the disk is to be replicated, select a replication destination for the disk before proceeding.

8 (Optional) Select a different vSphere Replication server to manage the replication of this virtual machine.

9 Review the settings and click **Finish** to establish replication.

   vSphere Replication starts an initial full synchronization of the virtual machine files to the designated datastore on the target site.

Stop Replicating a Virtual Machine

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

Stopping replication of a virtual machine does not remove it from any protection groups of which it is a member.

Prerequisites

You have configured vSphere Replication on a virtual machine that you no longer need to protect.

Procedure

1 Select the vSphere Replication view of the Site Recovery Manager interface.

2 Select a vSphere Replication server and click the **Virtual Machines** tab.

3 Select a virtual machine and click **Remove Replication**.

4 Click **Yes** to confirm that you want to stop replicating this virtual machine.

5 Select the Protection Groups view of the Site Recovery Manager interface.

6 Select the protection group of which the virtual machine is a member, and click the **Virtual Machines** tab.

7 Select the virtual machine on which you stopped replication and click **Remove Protection**.

8 Click **Yes** to confirm that you want to stop protecting this virtual machine.

The virtual machine does not replicate to the target site.

The virtual machine is no longer included in a protection group.

Creating Protection Groups

3

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

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

You must configure the virtual machines in a protection group so that Site Recovery Manager can add them to the vCenter Server inventory at the recovery site.

You configure virtual machines and create protection groups differently depending on whether you use array-based replication or vSphere Replication. You cannot create protection groups that combine virtual machines for which you configured array-based replication with virtual machines for which you configured vSphere Replication. However, you can include array-based protection groups and vSphere Replication protection groups in the same recovery plan.

- About Array-Based Protection Groups and Datastore Groups

  When you create a protection group for array-based replication, you specify array information and then Site Recovery Manager computes the set of virtual machines into a datastore group. Datastore groups contain all the files of the protected virtual machines.

- Create vSphere Replication Protection Groups

  You can create protection groups that contain virtual machines that vSphere Replication protects.

- Apply Inventory Mappings to All Members of a Protection Group

  If you add virtual machines to a protection group, or if virtual machines lose their protection, you can configure protection for all unconfigured virtual machines by using the existing inventory mappings, in one step.

About Array-Based Protection Groups and Datastore Groups

When you create a protection group for array-based replication, you specify array information and then Site Recovery Manager computes the set of virtual machines into a datastore group. Datastore groups contain all the files of the protected virtual machines.

You can add virtual machines to a protection group by creating them on one of the datastores that belong to the datastore groups that Site Recovery Manager associates with the protection group. You can also add virtual machines to the protection group by using Storage vMotion to move their storage to one of the datastores in the datastore group. You can remove a member from a protection group by moving the virtual machine's files to another datastore.

If you disable protection on a virtual machine, you must move the files of that virtual machine to an unprotected datastore. If you leave the files of an unprotected virtual machine in a protected datastore, recovery fails for all the virtual machines in that datastore.

To configure array-based replication, you must assign each virtual machine to a resource pool, folder, and network that exist at the recovery site. You can specify defaults for these assignments by selecting inventory mappings. Site Recovery Manager applies inventory mappings when you create the protection group. If you do not specify inventory mappings, you must configure them individually for each member of the protection group. Site Recovery Manager does not protect virtual machines that you did not configure or that you incorrectly configured for replication, even if they reside on a protected datastore.

If your storage array supports consistency groups, Site Recovery Manager is compatible with vSphere Storage DRS and vSphere Storage vMotion. You can use Storage DRS and Storage vMotion to move virtual machine files within a consistency group that Site Recovery Manager protects. If your storage array does not support consistency groups, you cannot use Storage DRS and Storage vMotion in combination with Site Recovery Manager.

- How Site Recovery Manager Computes Datastore Groups

  Site Recovery Manager determines the composition of a datastore group by the set of virtual machines that have files on the datastores in the group, and by the devices on which those datastores are stored.

- Create Array-Based Protection Groups

  You create array-based protection groups to enable the protection of virtual machines in datastore groups that you configure to use array-based replication.

- Edit Array-Based Protection Groups

  You can change the name and description of an array-based protection group and add or remove datastore groups that are part of the protection group.

How Site Recovery Manager Computes Datastore Groups

Site Recovery Manager determines the composition of a datastore group by the set of virtual machines that have files on the datastores in the group, and by the devices on which those datastores are stored.

When you use array-based replication, each storage array supports a set of replicated datastores. On storage area network (SAN) arrays that use connection protocols such as Fibre Channel and iSCSI, these datastores are called logical storage units (LUN) and are composed of one or more physical datastores. On network file system (NFS) arrays, the replicated datastores are typically referred to as volumes. In every pair of replicated storage devices, one datastore is the replication source and the other is the replication target. Data written to the source datastore is replicated to the target datastore on a schedule controlled by the replication software of the array. When you configure Site Recovery Manager to work with a storage replication adapter (SRA), the replication source is at the protected site and the replication target is at the recovery site.

A datastore provides storage for virtual machine files. By hiding the details of physical storage devices, datastores simplify the allocation of storage capacity and provide a uniform model for meeting the storage needs of virtual machines. Because any datastore can span multiple devices, Site Recovery Manager must ensure that all devices backing the datastore are replicated before it can protect the virtual machines that use that datastore. Site Recovery Manager must ensure that all datastores containing protected virtual machine files are replicated. During a recovery or test, Site Recovery Manager must handle all such datastores together.

To achieve this goal, Site Recovery Manager aggregates datastores into datastore groups to accommodate virtual machines that span multiple datastores. Site Recovery Manager regularly checks and ensures that datastore groups contain all necessary datastores to provide protection for the appropriate virtual machines. When necessary, Site Recovery Manager recalculates datastore groups. For example, this can occur when you add new devices to a virtual machine, and you store those devices on a datastore that was not previously a part of the datastore group.

A datastore group consists of the smallest set of datastores required to ensure that if any of a virtual machine's files is stored on a datastore in the group, all of the virtual machine's files are stored on datastores that are part of the same group. For example, if a virtual machine has disks on two different datastores, then Site Recovery Manager combines both datastores into a datastore group. Site Recovery Manager combines devices into datastore groups according to set criteria.

- Two different datastores contain files that belong to the same virtual machine.
- Datastores that belong to two virtual machines share a raw disk mapping (RDM) device on a SAN array, as in the case of a Microsoft cluster server (MSCS) cluster.
- Two datastores span extents corresponding to different partitions of the same device.
- A single datastore spans two extents corresponding to partitions of two different devices. The two extents must be in a single consistency group and the SRA must report consistency group information from the array in the device discovery stage. Otherwise, the creation of protection groups based on this datastore is not possible even though the SRA reports that the extents that make up this datastore are replicated.
- Multiple datastores belong to a consistency group. A consistency group is a collection of replicated datastores where every state of the target set of datastores existed at a specific time as the state of the source set of datastores. Informally, the datastores are replicated together such that when recovery happens using those datastores, software accessing the targets does not see the data in a state that the software is not prepared to deal with.

Protecting Virtual Machines on VMFS Datastores that Span Multiple LUNs or Extents

Not all SRAs report consistency group information from the storage array, because not all storage arrays support consistency groups. If an SRA reports consistency group information from the array following a datastore discovery command, the LUNs that constitute a multi-extent VMFS datastore must be in the same storage array consistency group. If the array does not support consistency groups and the SRA does not report any consistency group information, Site Recovery Manager cannot protect virtual machines located on the multi-extent datastore.

Create Array-Based Protection Groups

You create array-based protection groups to enable the protection of virtual machines in datastore groups that you configure to use array-based replication.

Site Recovery Manager computes the datastore groups when you configure the array pair or when you refresh the list of devices.

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

You can organize protection groups in folders. Different views in the Recovery interface display the names of the protection groups, but they do not display the folder names. If you have two protection groups with the same name in different folders, it might be difficult to tell them apart in some views in the Recovery interface. Consequently, ensure that protection group names are unique across all folders. In environments in which not all users have view privileges for all folders, to be sure of the uniqueness of protection group names, do not place protection groups in 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.

Procedure

1. Click **Protection Groups** in the Site Recovery Manager interface, and click **Create Protection Group**.
2. On the Select a Site and Protection Group Type page, select which site to protect and select **Array Based Replication**.
3. Select an array pair, and click **Next**.
4. Select a datastore group from the list, and click **Next**.

   When you select a datastore group, the virtual machines in that datastore group appear in the Virtual Machines on the Selected Datastore Group pane, and are marked for inclusion in the protection group after you create the protection group.
5. Type a name and optional description for the protection group, and click **Next**.

6 Click **Finish** to create the protection group and begin the protection of the specified virtual machines.

   You can monitor the progress of the tasks to create the protection group and protect the virtual machines in the Recent Tasks panel of the vSphere Client.

What to do next

Create a recovery plan with which to associate your protection groups. See Create a Recovery Plan.

Edit Array-Based Protection Groups

You can change the name and description of an array-based protection group and add or remove datastore groups that are part of the protection group.

Procedure

1 Click **Protection Groups**, right-click an array-based protection group and select **Edit Protection Group**.

2 Click **Next**.

3 Add or remove datastore groups in the protection group and click **Next**.

4 Edit the name or description of the protection group and click **Next**.

5 Click **Finish**.

Create vSphere Replication Protection Groups

You can create protection groups that contain virtual machines that vSphere Replication protects.

You can organize protection groups in folders. Different views in the Recovery interface display the names of the protection groups, but they do not display the folder names. If you have two protection groups with the same name in different folders, it might be difficult to tell them apart in some views in the Recovery interface. Consequently, ensure that protection group names are unique across all folders. In environments in which not all users have view privileges for all folders, to be sure of the uniqueness of protection group names, do not place protection groups in folders.

When you create a vSphere Replication protection group, you can add to the protection group any virtual machines that you configured for vSphere Replication.

Prerequisites

Use the vSphere Client to configure vSphere Replication for virtual machines. See Configure Replication for a Single Virtual Machine or Configure Replication for Multiple Virtual Machines.

Procedure

1 Click **Protection Groups** in the Site Recovery Manager interface and click **Create Protection Group**.

2 Select the site to be the protected site, select **vSphere Replication**, and click **Next**.

3 Select virtual machines from the list and click **Next**.

Only virtual machines that you configured for vSphere Replication and that are not already in a protection group appear in the list.

4 Type a name and optional description for the protection group, and click **Next**.

5 Click **Finish** to create the protection group.

What to do next

Create a recovery plan with which to associate your protection groups. See Create a Recovery Plan.

Edit vSphere Replication Protection Groups

You can edit a vSphere Replication protection group to change its name and to add or remove virtual machines to the group.

Procedure

1 Click **Protection Groups** in the left pane and right-click a vSphere Replication protection group.

2 Select **Edit Protection Group** and click **Next**.

You cannot change the **Protected Site** or **Protection Group Type** settings.

3 Add virtual machines to the protection group and click **Next**.

4 Edit the name or description of the protection group and click **Next**.

5 Click **Finish**.

6 (Optional) To remove a virtual machine from a vSphere Replication protection group, click the **Virtual Machines** tab, select a virtual machine and click **Remove Protection**.

Apply Inventory Mappings to All Members of a Protection Group

If you add virtual machines to a protection group, or if virtual machines lose their protection, you can configure protection for all unconfigured virtual machines by using the existing inventory mappings, in one step.

Procedure

1 Click **Protection Groups** in the left pane, select a protection group, and click the **Virtual Machines** tab.

2 Click **Configure All**.

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

Creating, Testing, and Running Recovery Plans

4

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, and another plan to handle an unplanned event such as a power failure or natural disaster. Having these different recovery plans allows you to decide how to perform recovery.

Testing a recovery plan runs the plan without affecting services at the protected or recovery sites, apart from suspending non-critical virtual machines on the recovery site if you configure the recovery plan to do so. You can perform planned migrations from the protected site to the recovery site or disaster recoveries by running a recovery plan.

You can run only one recovery plan at a time to recover a particular protection group. If you simultaneously test or run multiple recovery plans that specify the same protection group, only one recovery plan can operate on the protection group. Other running recovery plans that specify the same protection group report warnings for that protection group and the virtual machines it contains. The warnings explain that the virtual machines were recovered, but do not report other protection groups that the other recovery plans cover.

- 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.

- 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.

- 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.

- Protecting Microsoft Cluster Server and Fault Tolerant Virtual Machines

  You can use Site Recovery Manager to protect Microsoft Cluster Server (MSCS) and fault tolerant virtual machines, with certain limitations.

- Create, Test, and Run a Recovery Plan

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

- 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.

- View and Export Recovery Plan History

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

- Cancel a Test or Recovery

  You can cancel a recovery plan test at any time during its run. You can cancel a planned migration or disaster recovery at certain times during its run.

- Delete a Recovery Plan

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

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.

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

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 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 test network by selecting **Auto** when you configure the network settings when you run a test.

A datacenter network is a network that typically supports existing virtual machines at the recovery site. 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. Other virtual machines require IP customization and additional recovery plan steps to apply the customization.

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.

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 machines on the recovery site with the virtual machines on the protected site, then stops replication. Site Recovery Manager attempts to replicate all virtual machines and gracefully shut down the protected machines. 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 restores virtual machines on the recovery site to their most recent available state, according to the recovery point objective (RPO). 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, and automatic reprotect might not be possible.

If Site Recovery Manager detects that a datastore on the protected site is in the all paths down (APD) state and is preventing a virtual machine from shutting down, Site Recovery Manager waits for a period before attempting to shut down the virtual machine again. The APD state is usually transient, so by waiting for a datastore in the APD state to come back online, Site Recovery Manager can gracefully shut down the protected virtual machines on that datastore.

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. For this reason, 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, 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.

Forced recovery is for use in cases where storage arrays fail 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.

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.

Running forced recovery with array-based replication can affect the mirroring between the protected and the recovery storage arrays. After you run forced recovery, you must check that mirroring is set up correctly between the protected array and the recovery array before you can perform further replication operations. If mirroring is not set up correctly, you must repair the mirroring by using the storage array software.

When you enable forced recovery, any outstanding changes on the protection site are not replicated to the recovery site before the sequence begins. Replication of the changes occurs according to the recovery point objective (RPO) period of the storage array. If a new virtual machine or template is added on the protection site and recovery is initiated before the storage RPO period has elapsed, the new virtual machine or template does not appear on the replicated datastore and is lost. To avoid losing the new virtual machine or template, wait until the end of the RPO period before running the recovery plan with forced recovery.

After the forced recovery completes and you have verified the mirroring of the storage arrays, 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.

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 4-1. 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**.
Effect on virtual machines at protected site	None	Site Recovery Manager shuts down virtual machines in reverse priority order.
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 storage at the recovery site. For array-based replication, Site Recovery Manager rescans the arrays to discover them.	During a planned migration, Site Recovery Manager synchronizes replicated datastores, then stops replication, then makes the target devices at the recovery site writable. During a disaster recovery, Site Recovery Manager attempts the same steps , but if they do not succeed, Site Recovery Manager ignores the errors.

Table 4-1. How Testing a Recovery Plan Differs from Running a Recovery Plan (Continued)

Area of Difference	Test a Recovery Plan	Run a Recovery Plan
Network	If you explicitly assign test networks, Site Recovery Manager connects recovered virtual machines to a test network. If virtual machine network assignment is **Auto**, 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 a datacenter network.
Interruption of recovery plan	You can cancel a test at any time.	You can cancel the recovery in some cases.

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 cluster and ensures that all hosts in it are powered on before recovery begins. After the recovery or test is complete, Site Recovery Manager reenables DPM for the cluster. The hosts in it 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.

The behavior of Storage DRS or Storage vMotion depends on whether you use Site Recovery Manager with array-based replication or with vSphere Replication.

Using Site Recovery Manager with Array-Based Replication on Sites with Storage DRS or Storage vMotion

You must follow the guidelines if you use array-based replication to protect virtual machines on sites that use Storage DRS or Storage vMotion.

- If your storage array supports consistency groups, Site Recovery Manager is compatible with vSphere Storage DRS and vSphere Storage vMotion. You can use Storage DRS and Storage vMotion to move virtual machine files within a consistency group that Site Recovery Manager protects. If your storage array does not support consistency groups, you cannot use Storage DRS and Storage vMotion in combination with Site Recovery Manager.
- If you enable Storage DRS on the protection site, a datastore cluster must contain one and only one consistency group. Do not include any datastore that does not belong to the consistency group in the cluster. Placing multiple consistency groups into the same cluster might result in virtual machines being lost during a recovery. This guideline also applies on the recovery site if Storage DRS is enabled on the recovery site.
- Do not use Storage DRS or Storage vMotion to move virtual machines regularly. Do not accept recommendations to manually move virtual machines regularly. You can move virtual machines occasionally, but excessive movement of virtual machines can cause problems. Moving virtual machines requires the array to replicate virtual machines over the network, which takes time and consumes bandwidth. When Storage DRS or Storage vMotion moves virtual machines, you might encounter problems during a recovery:
  - If Storage DRS or Storage vMotion moves a virtual machine to a different consistency group within the same protection group, there is a short period between Site Recovery Manager propagating the new location of the virtual machine to the recovery site and the array replicating the changes to the recovery site. In addition, there is another period during which the arrays replicate the source and target consistency groups to a consistent state on the recovery site. While the array is propagating all of the changes to the recovery site, disaster recovery of this virtual machine might fail.
  - If Storage DRS or Storage vMotion moves a virtual machine to a different protection group, Site Recovery Manager generates a protection error for this virtual machine. You must unconfigure protection of the virtual machine in the old protection group and configure protection of the virtual machine in the new protection group. Until you configure protection in the new protection group, planned migration or disaster recovery of this virtual machine fails.
- Adding a disk to a protected virtual machine results in the same problems as for moving an entire virtual machine. Site Recovery Manager does not prevent you from doing this, but if a virtual machine contains an unreplicated disk and you do not exclude the disk from protection, powering on the virtual machine fails after the move.

- Moving a protected disk to a different consistency group results in the same problems as for moving an entire virtual machine. These problems occur if you move a disk to a different consistency group within the same protection group or if you move it into a different protection group.
  Site Recovery Manager does not prevent you from doing this, but if a disk has moved to a different consistency group, powering on the virtual machine fails after the move.

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

You must follow the guidelines if you use vSphere Replication to protect virtual machines on sites that use Storage DRS or Storage vMotion.

- vSphere Replication is compatible with vSphere Storage vMotion and vSphere Storage DRS on the protected site. You can use Storage vMotion and Storage DRS to move the disk files of a virtual machine that vSphere Replication protects, with no impact on replication.
- 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 trigger Storage vMotion only if you set the Storage DRS rules to be 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.

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 array-based replication or vSphere Replication. If HA restarts a protected virtual 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.

Protecting Microsoft Cluster Server and Fault Tolerant Virtual Machines

You can use Site Recovery Manager to protect Microsoft Cluster Server (MSCS) and fault tolerant virtual machines, with certain limitations.

To use Site Recovery Manager to protect MSCS and fault tolerant virtual machines, you might need to change your environment.

General Limitations to Protecting MSCS and Fault Tolerant Virtual Machines

Protecting MSCS and fault tolerant virtual machines is subject to the following limitations.

- You can use array-based replication only to protect MSCS virtual machines. Protecting MSCS virtual machines with vSphere Replication is not supported.
- Reprotect of MSCS or fault tolerant virtual machines requires VMware High Availability (HA) and VMware Distributed Resource Scheduler (DRS). When you move MSCS or fault tolerant virtual machines across their primary and secondary sites during reprotect, you must enable HA and DRS, and set the affinity and antiaffinity rules as appropriate. See DRS Requirements for Protection of MSCS Virtual Machines.
- vSphere does not support vSphere vMotion for MSCS virtual machines.

ESXi Host Requirements for Protection of MSCS Virtual Machines

To protect MSCS or fault tolerant virtual machines, the ESXi host machines on which the virtual machines run must meet certain criteria.

- You must run a fault tolerant virtual machine and its shadow on two separate ESXi Server instances.
- You can run a cluster of MSCS virtual machines in the following possible configurations.

  Cluster-in-a-box
  The MSCS virtual machines in the cluster run on a single ESXi Server. You can have a maximum of five MSCS nodes on one ESXi Server.

  Cluster-across-boxes
  You can spread the MSCS cluster across a maximum of five ESXi Server instances. You can protect only one virtual machine node of any MSCS cluster on a single ESXi Server instance. You can have multiple MSCS node virtual machines running on an ESXi host, as long as they do not participate in the same MSCS cluster. This configuration requires shared storage on a Fibre Channel SAN for the quorum disk.

DRS Requirements for Protection of MSCS Virtual Machines

To use DRS on sites that contain MSCS virtual machines, you must configure the DRS rules to allow Site Recovery Manager to protect the virtual machines. By following the guidelines, you can protect MSCS virtual machines on sites that run DRS if the placeholder virtual machines are in either a cluster-across-boxes MSCS deployment or in a cluster-in-a-box MSCS deployment.

- Because vSphere does not support vSphere vMotion for MSCS virtual machines, you must set the `VM to Host` DRS rule so that DRS does not perform vMotion on MSCS nodes. Set the `VM to Host` rule for the virtual machines on the protected site and for the shadow virtual machines on the recovery site.
- Set the DRS rules on the virtual machines on the protected site before you configure MSCS in the guest operating systems. Set the DRS rules immediately after you deploy, configure, or power on the virtual machines.
- Set the DRS rules on the virtual machines on the recovery site immediately after you create a protection group of MSCS nodes, as soon as the placeholder virtual machines appear on the recovery site.
- DRS rules that you set on the protected site are not transferred to the recovery site after a recovery. For this reason, you must set the DRS rules on the placeholder virtual machines on the recovery site.
- Do not run a test recovery or a real recovery before you set the DRS rules on the recovery site.

If you do not follow the guidelines on either the protected site or on the recovery site, vSphere vMotion might move MSCS virtual machines to a configuration that Site Recovery Manager does not support.

- In a cluster-in-a-box deployment on either the protected or recovery site, vSphere vMotion might move MSCS virtual machines to different ESXi hosts.
- In a cluster-in-a-box deployment on either the protected or recovery site, vSphere vMotion might move some or all of the MSCS virtual machines to a single ESXi host.

Create, Test, and Run a Recovery Plan

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

Procedure

1. Create a Recovery Plan

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

2. 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.

3. 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.

4 Test a Recovery Plan

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

5 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.

6 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.

7 Recover a Point-in-Time Snapshot of a Virtual Machine

With vSphere Replication, you can retain point-in-time snapshots of a virtual machine. You can configure Site Recovery Manager to recover a number of point-in-time (PIT) snapshots of a virtual machine when you run a recovery plan.

Create a Recovery Plan

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

During tests, isolate the virtual machines that Site Recovery Manager recovers. If Site Recovery Manager brings duplicate machines on line and they begin to interact with unprotected virtual machines in your production network, errors can occur.

Procedure

1 Click **Recovery Plans**, click the **Summary** tab, and click **Create Recovery Plan**.

2 Select the recovery site.

3 Select one or more protection groups for the plan to recover, and click **Next**.

4 Select a recovery site network to which recovered virtual machines connect during recovery plan tests, and click **Next**.

You can isolate virtual machine Site Recovery Manager restorations during test recoveries by selecting **Auto**, which is an isolated network, or by selecting a manually created network that is not connected to other networks.

5 Type a name for the plan in the **Recovery Plan Name** text box, add an optional description, and click **Next**.

6 Review the summary information and click **Finish** to create the recovery plan.

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

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 Click **Recovery Plans**, right-click a recovery plan, and select **Edit Recovery Plan**.

2 Click **Next**.

  You cannot change the recovery site.

3 Select one or more protection groups for the plan to recover, and click **Next**.

4 Select a recovery site network to which recovered virtual machines connect during recovery plan tests, and click **Next**.

5 Change the name of the plan in the **Recovery Plan Name** text box and add an optional description.

6 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.

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.

You can only add virtual machines to suspend at the recovery site. To suspend virtual machines at both the protected and recovery sites, you must perform a recovery and then reverse protection by performing a reprotect operation before you can add virtual machines to suspend at the original protected site. If you configure virtual machines to suspend at both sites, the plan starts virtual machines at one site and suspends them at the other with each recovery that you run.

Procedure

1 On the recovery site, click **Recovery Plans** in the left pane and select the recovery plan to edit.

2 Click the **Recovery Steps** tab and click **Add Non-Critical VM**.

3 Expand the hierarchical list to select virtual machines on the recovery site to suspend during a recovery.

4 Click **OK**.

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

Test a Recovery Plan

When you test a recovery plan, Site Recovery Manager runs the recovery plan on a test network and 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 with the exception of 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 testing 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. Click **Recovery Plans** in the Site Recovery Manager interface.
2. Select the recovery plan to test, and click **Test**.
3. (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 the synchronization might take more time.
4. Click **Next**.
5. Review the test information and click **Start**.
6. Click the **Recovery Steps** tab to monitor the progress of the test and respond to messages.

   The **Recovery Steps** tab displays the progress of individual steps. The **Summary** tab reports the progress of the overall plan.

   Note Site Recovery Manager initiates recovery steps in the prescribed order, with one exception. It does not wait for the Prepare Storage step to finish for all protection groups before continuing to the next steps.

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.

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. Click **Recovery Plans** in the Site Recovery Manager interface, select the recovery plan that you tested, and click **Cleanup**.
2. Review the cleanup information and click **Next**.
3. Click **Start**.
4. 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 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. In the case of array-based replication, recovered virtual machines and services might need to be supported at the recovery site for a period of time. 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. Click **Recovery Plans** in the left pane, select the recovery plan to run, and click **Recovery**.
2. 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**.

3 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.

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

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

5 Click **Next**.

6 Review the recovery information and click **Start**.

7 Click the **Recovery Steps** tab.

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

Recover a Point-in-Time Snapshot of a Virtual Machine

With vSphere Replication, you can retain point-in-time snapshots of a virtual machine. You can configure Site Recovery Manager to recover a number of point-in-time (PIT) snapshots of a virtual machine when you run a recovery plan.

You configure the retention of PIT snapshots when you configure vSphere Replication on a virtual machine. For more information about PIT snapshots, see Replicating a Virtual Machine and Enabling Multiple Point in Time Instances.

Note You cannot use the Site Recovery Manager interface to configure replication that uses point in time (PIT) snapshots. To enable PIT snapshots, configure replication of a virtual machine by using the vSphere Web Client. See Configure Replication for a Single Virtual Machine in *vSphere Replication Administration*.

Site Recovery Manager only recovers the most recent PIT snapshot during a recovery. To recover older snapshots, you must enable the **vrReplication > preserveMpitImagesAsSnapshots** option in **Advanced Settings** in the Site Recovery Manager interface. See Change vSphere Replication Settings.

If you recover a PIT snapshot of a virtual machine for which you have configured IP customization, Site Recovery Manager only applies the customization to the most recent PIT snapshot. If you recover an older PIT snapshot of a virtual machine with IP customization, you must configure the IP settings manually.

Point-in-time recovery is not available with array-based replication.

Procedure

1 Configure Site Recovery Manager to retain older PIT snapshots by setting the **vrReplication > preserveMpitImagesAsSnapshots** option.

2 Use the vSphere Web Client to configure replication of a virtual machine, selecting the option to retain a number of PIT snapshots.

3 In the Site Recovery Manager interface, add the virtual machine to a vSphere Replication protection group.

4 Include the vSphere Replication protection group in a recovery plan.

5 Run the recovery plan.

When the recovery plan is finished, the virtual machine is recovered to the recovery site, with the number of PIT snapshots that you configured.

6 In the **VMs and Templates** view, right-click the recovered virtual machine and select **Snapshot > Snapshot Manager**.

7 Select one of the PIT snapshots of this virtual machine and click **Go to**.

The recovered virtual machine reverts to the PIT snapshot that you selected.

8 (Optional) If you have configured the virtual machine for IP customization, and if you select an older PIT snapshot than the most recent one, manually configure the IP settings on the recovered virtual machine.

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 Click **Recovery Plans** in the Site Recovery Manager interface, select a recovery plan, and click the **Recovery Steps** tab.

2 Click **Export Steps**.

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

View and Export Recovery Plan History

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

Recovery plan histories provide information about each run, test, or cleanup 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 cannot export the recovery plan history while a test recovery, real recovery, or test cleanup is in progress.

Prerequisites

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

Procedure

1. Click **Recovery Plans** in the Site Recovery Manager interface, select a recovery plan, and click the **History** tab.
2. (Optional) Click **View** for a recovery plan run, test, or cleanup operation.

   The history opens in a browser.
3. (Optional) Click **Export** for a recovery plan run, test, or cleanup operation.

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

Cancel a Test or Recovery

You can cancel a recovery plan test at any time during its run. You can cancel a planned migration or disaster recovery at certain times during its run.

When you cancel a test or recovery, Site Recovery Manager does not start steps, and uses certain rules to stop steps that are in progress.

- Steps that cannot be stopped, such as powering on or waiting for a heartbeat, run to completion before the cancellation finishes.
- Steps that add or remove storage devices are undone by cleanup operations if you cancel.

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

Procedure

- ◆ To cancel a test or recovery, click **Cancel** on the recovery plan toolbar.

Delete a Recovery Plan

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

Deleting a recovery plan does not delete the history of the plan, which you can still view in the **All Recovery Plans > All History** tab.

Procedure

1. Click **Recovery Plans** and select the recovery plan to delete.
2. (Optional) Click the **History** tab and click **Export List** to download the history of the plan.

3 Right-click the recovery plan to delete, and select **Delete Recovery Plan**.

Reprotecting Virtual Machines After a Recovery

5

After a recovery, the recovery site becomes the new protected site, but it is 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 protected virtual machines start up on the recovery site. Because the former protected site might be offline, these virtual machines are not protected. 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 complete the reprotect process only after a recovery finishes. 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.

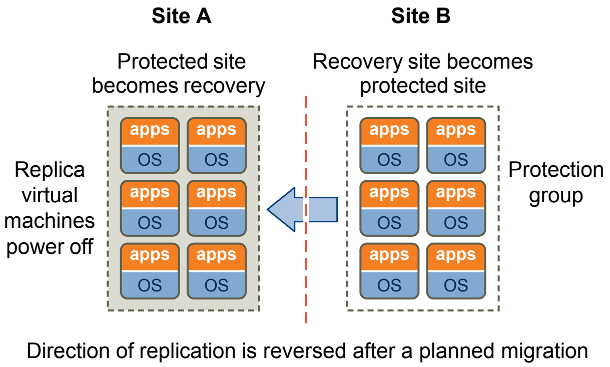
You can perform reprotect on protection groups that contain virtual machines that are configured for both array-based replication and for vSphere Replication.

Example: Performing a Reprotect Operation

Site A is the protected site and site B is the recovery site. If site A goes offline, Site Recovery Manager recovers the protected virtual machines to 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, you can run 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 5-1. Site Recovery Manager Reprotect Process


Site A
Site B
Protected site becomes recovery
Recovery site becomes protected site
Replica virtual machines power off
Protection group
apps
OS
Direction of replication is reversed after a planned migration

- How Site Recovery Manager Performs Reprotect

  The reprotect process involves two stages. Site Recovery Manager reverses the direction of protection, then forces a 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. With reprotect, you can recover virtual machines back to the original site after a recovery.

- Reprotect States

  The reprotect process passes through several states that you can observe in the recovery plan in the Site Recovery Manager plug-in in the vSphere Client.

How Site Recovery Manager Performs Reprotect

The reprotect process involves two stages. Site Recovery Manager reverses the direction of protection, then forces a synchronization of the storage from the new protected site to the new recovery site.

When you initiate the reprotect process, Site Recovery Manager instructs the underlying storage arrays or vSphere Replication to reverse the direction of replication. After reversing the replication, Site Recovery Manager creates placeholder virtual machines at the new recovery site, which was the original protected site before the reprotect.

When creating placeholder virtual machines on the new protected site, Site Recovery Manager uses the location of the original protected virtual machine to determine where to create the placeholder virtual machine. Site Recovery Manager uses the identity of the original protected virtual machine to create the placeholder and any subsequent recovered virtual machines. If the original protected virtual machines are no longer available, Site Recovery Manager uses the inventory mappings from the original recovery site to the original protected site to determine the resource pools and folders for the placeholder virtual machines. You must configure inventory mappings on both sites before running reprotect, or reprotect might fail.

When performing reprotect with array-based replication, Site Recovery Manager places the files for the placeholder virtual machines in the placeholder datastore for the original protected site, not in the datastore that held the original protected virtual machines.

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 finishes.

When performing reprotect 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.

Preconditions for Performing Reprotect

You can perform reprotect only if you meet certain preconditions.

You can perform reprotect on protection groups that contain virtual machines that are configured for both array-based replication and for vSphere Replication.

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, and corresponding databases must all be recoverable.
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. To unpair and recreate the pairing of protected and recovery sites, both sites must be available. If you cannot restore the original protected site, you must reinstall Site Recovery Manager on the protected and recovery sites.

Reprotect Virtual Machines

Reprotect results in the reconfiguration of Site Recovery Manager protection groups and recovery plans to work in the opposite direction. With reprotect, you can recover virtual machines back to the original site after a recovery.

Prerequisites

See Preconditions for Performing Reprotect.

Procedure

1. Click **Recovery Plans** in the Site Recovery Manager interface, select a recovery plan, and click **Reprotect**.
2. Select the check box to confirm that you understand that the reprotect operation is irreversible.
3. Review the reprotect information and click **Start**.
4. Click the **Recovery Steps** tab to monitor the progress of the reprotect operation.

   Certain steps do not apply to all virtual machines. For example, virtual machines that you configured for array-based replication appear under **Configure Storage to Reverse Direction > Protection Group > Configure VR Replication**, even though this step does not perform any actions on them. These virtual machines are marked Not Applicable when the step runs.
5. When the reprotect operation finishes, select the recovery plan, click **History**, and click **View** for the reprotect operation.

   The history report for the reprotect operation opens in a browser. 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 passes through several states that you can observe in the recovery plan in the Site Recovery Manager plug-in in the vSphere Client.

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

Table 5-1. 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 reprotect succeeds for some groups in some plans, but not for others.	Run reprotect again on the partially reprotected plans.

Table 5-1. Reprotect States (Continued)

State	Description	Remedial Action
Incomplete Reprotect	Occurs because of failures during reprotect. For example, this state might occur because of a failure to synchronize storage or a failure to create placeholder virtual machines.	■ If a reprotect operation fails to synchronize storage, make sure that sites are connected, review the reprotect progress in the vSphere Client , and start the reprotect task again. If reprotect still won't complete, run the reprotect task with the **Force Cleanup** option. ■ If Site Recovery Manager fails to create placeholder virtual machines, recoveries are still possible. Review the reprotect steps in the vSphere Client, resolve any open issues, and start the reprotect task again.
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.

Restoring the Pre-Recovery Site Configuration By Performing Failback

6

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 5 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 complete 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

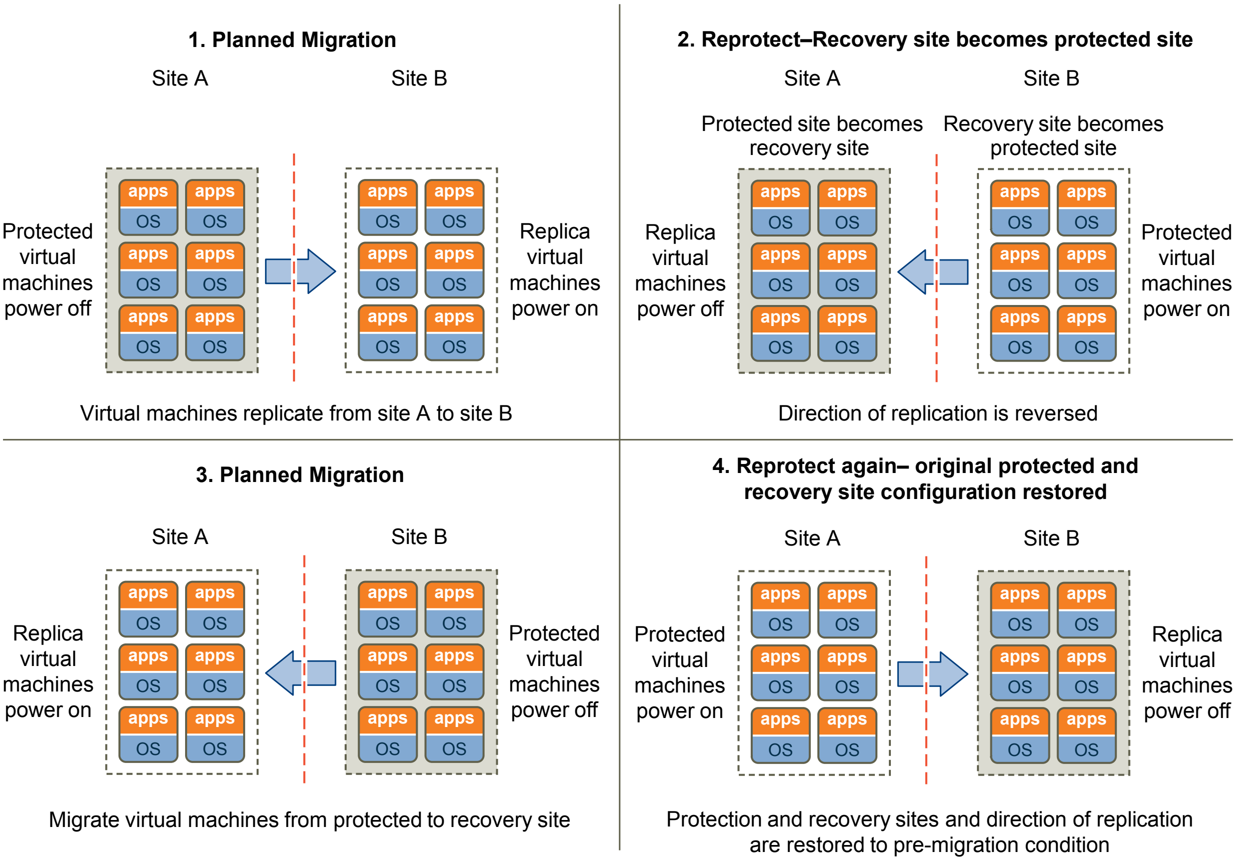
Site A is the protected site and B is the recovery site. A recovery occurs, migrating the virtual machines from site A to site B. To restore site A as the protected site, you perform a failback.

- 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.

- Perform a planned migration to recover the protected virtual machines on site B to site A.

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

Figure 6-1. Site Recovery Manager Failback Process


1. Planned Migration
Site A
Site B
Protected virtual machines power off
Replica virtual machines power on
apps
OS
Virtual machines replicate from site A to site B
2. Reprotect–Recovery site becomes protected site
Site A
Site B
Protected site becomes recovery site
Recovery site becomes protected site
Replica virtual machines power off
Protected virtual machines power on
Direction of replication is reversed
3. Planned Migration
Site A
Site B
Replica virtual machines power on
Protected virtual machines power off
Migrate virtual machines from protected to recovery site
4. Reprotect again– original protected and recovery site configuration restored
Site A
Site B
Protected virtual machines power on
Replica virtual machines power off
Protection and recovery sites and direction of replication are restored to pre-migration condition

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 protected site, site A, are running again.
- You did not run reprotect since the recovery.

Procedure

1 Click **Recovery Plans** in the Site Recovery Manager interface, select a recovery plan, and click **Reprotect**.

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

3 Review the reprotect information and click **Start**.

4 Monitor the reprotect operation on the **Recovery Steps** tab until it finishes.

5 (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.

6 (Optional) Click **Test** and follow the prompts to test the recovery plan.

Testing the recovery plan verifies that the recovery plan works after the reprotect operation.

7 Click **Recovery** to run the recovery plan as a planned migration.

8 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**.

9 Select **Planned Migration**, click **Next**, and click **Start**.

10 Monitor the planned migration operation on the **Recovery Steps** tab 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 Click **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.

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, 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.

- Recovery Plan Steps

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

- 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.

- Creating Custom Recovery Steps

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

- Customize the Recovery of an Individual Virtual Machine

  You can configure a virtual machine in a recovery plan to use a prescribed customization specification, or to run message or command steps when it is recovered.

Recovery Plan Steps

A recovery plan runs a series of steps that must be performed in a specific order. 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 are always skipped during test 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. 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.

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.

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. Click **Recovery Plans** in the left pane, select a recovery plan, and click the **Virtual Machines** tab or the **Recovery Steps** tab.
2. Right-click a virtual machine and select **Priority**.
3. Select a new priority for the virtual machine.

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

Creating Custom Recovery Steps

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

Site Recovery Manager can run custom steps either on the Site Recovery Manager Server or in a virtual machine that is part of the recovery plan.

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.

- Types of Custom Recovery Steps

  You can create different types of custom recovery steps to include in recovery plans.
- 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.
- Create Top-Level Command Steps

  You can add top-level commands anywhere in the recovery plan.
- Create Top-Level Message Prompt Steps

  You can add top-level message prompts anywhere in the recovery plan.
- Create Command Steps for Individual Virtual Machines

  You can configure custom recovery steps to perform tasks for a virtual machine before and after Site Recovery Manager powers them on.

- Create Message Prompt Steps for Individual Virtual Machines

  You can configure custom recovery steps to prompt users to perform tasks for a virtual machine before and after the virtual machine 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.

- Environment Variables for Command Steps

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

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 either top-level commands or per-virtual machine commands.

Top-Level Commands

Run on the Site Recovery Manager Server. For example, you might use these commands to power on physical devices or to redirect network traffic.

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. You can run the commands either before or after powering on a virtual machine. Commands that you configure to run after the virtual machine is powered on can run either on the Site Recovery Manager Server or 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 click **OK**, which dismisses the message and allows the recovery to continue.

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
Top-level commands	If a recovery step fails, Site Recovery Manager logs the failure and shows a warning on the **Recovery Steps** tab. Subsequent custom recovery steps continue to run.
Per-virtual machine commands	Run in batches either before or 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 before power on and five commands to run after power on, and the third command in the batch before power on fails, the remaining two commands to run before power on do not run. Site Recovery Manager does not power on the virtual machine and so cannot run any post-power on commands.

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 Command Steps

You can add top-level commands anywhere in the recovery plan.

Prerequisites

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

Procedure

1. Click **Recovery Plans** in the Site Recovery Manager interface, and select a recovery plan.
2. Click the **Recovery Steps** tab.
3. Right-click a step before or after which to add a custom step, and select **Add Step**.
4. Select **Command on SRM Server**.
5. In the **Name** text box, type a name for the step.
6. In the **Content** text box, type the commands for the step to run.

7 (Optional) Modify the **Timeout** setting.

8 Select where in the sequence of steps to insert the new step.

- **Before selected step**
- **After selected step**

9 Click **OK** to add the step to the recovery plan.

Create Top-Level Message Prompt Steps

You can add top-level message prompts anywhere in the recovery plan.

Prerequisites

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

Procedure

1 Click **Recovery Plans** in the Site Recovery Manager interface, and select a recovery plan.

2 Click the **Recovery Steps** tab.

3 Right-click a step before or after which to add a custom step, and select **Add Step**.

4 Select **Prompt**.

5 In the **Name** text box, type a name for the step.

6 In the **Content** text box, type the prompt message.

7 Select where in the sequence of steps to insert the new step.

- **Before selected step**
- **After selected step**

8 Click **OK** to add the step to the recovery plan.

Create Command Steps for Individual Virtual Machines

You can configure custom recovery steps to perform tasks for a virtual machine before and after Site Recovery Manager powers them on.

Site Recovery Manager associates command steps with a protected or recovered virtual machine in the same way as customization information. If different recovery plans contain the same virtual machine, the commands and prompts are the same.

Prerequisites

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

Procedure

1 Click **Recovery Plans** in the Site Recovery Manager interface, and select a recovery plan.

2 Click the **Virtual Machines** tab.

3 Right-click a virtual machine and click **Configure**.

4 Select **Pre-Power On Steps** or **Post Power On Steps** in the left pane, and click **Add**.

5 Select **Command on SRM Server** or **Command on Recovered VM**.

6 In the **Name** text box, type a name for the step.

7 In the **Content** text box, type the commands for the step to run.

8 (Optional) Modify the **Timeout** setting.

9 Click **OK** to add the step to the recovery plan.

10 Click **OK** to reconfigure the virtual machine to run the command before or after it powers on.

Create Message Prompt Steps for Individual Virtual Machines

You can configure custom recovery steps to prompt users to perform tasks for a virtual machine before and after the virtual machine powers on.

Site Recovery Manager associates message prompt steps with a protected virtual machine in the same way as customization information. If different recovery plans contain the same virtual machine, the commands and prompts are the same.

Prerequisites

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

Procedure

1 Click **Recovery Plans** in the Site Recovery Manager interface, and select a recovery plan.

2 Click the **Virtual Machines** tab.

3 Right-click a virtual machine and click **Configure**.

4 Select **Pre-Power On Steps** or **Post Power On Steps** in the left pane, and click **Add**.

5 Select **Prompt**.

6 In the **Name** text box, type a name for the step.

7 In the **Content** text box, type the prompt message.

8 Click **OK** to add the step to the recovery plan.

9 Click **OK** to reconfigure the virtual machine to prompt the user with a message before or 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. Test the command on the recovery site Site Recovery Manager Server before you add it to the 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
  ```

- You must install batch files and commands on the Site Recovery Manager Server at the recovery site.
- 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.

Command steps run with the identity of the LocalSystem account on the Site Recovery Manager Server host at the recovery site. When a command step runs, Site Recovery Manager makes environment variables available for it to use.

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 either on Site Recovery Manager Server or 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

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

Name	Value	Example
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 this VMDK of this virtual machine.	`[datastore-123] jquser-vm2/jquser-vm2.vmdk`

Customize the Recovery of an Individual Virtual Machine

You can configure a virtual machine in a recovery plan to use a prescribed customization specification, or to run message or command steps when it is recovered.

Message and command steps added to the recovery steps for a virtual machine operate like message and command steps added to a recovery plan. See Guidelines for Writing Command Steps.

Procedure

1 Connect the vSphere Client to the vCenter Server instance on the recovery site.

2 In the Site Recovery Manager interface, click **Recovery Plans** in the left pane, and click the plan to customize.

3 Click the **Recovery Steps** tab or the **Virtual Machines** tab.

4 Right-click a virtual machine in the list, and click **Configure**.

5 Click **IP Settings**.

You can also type a description of the specification you apply. Only the IP properties from the selected specification are applied. If you used the `dr-ip-customizer.exe` command to customize virtual machines in the recovery plan, you do not need to specify that customization here.

6 Select the appropriate entry to add a message or command step that runs before the machine is powered on.

7 Select the appropriate entry to add a message or command step that runs after the machine is powered on.

The customizations that you specify become associated with the protected virtual machine. As a result, the settings are shared between all recovery plans that apply to this virtual machine.

Note If you remove the protection of a virtual machine, all recovery customizations are lost.

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.

See the Compatibility Matrix for vCenter Site Recovery Manager 5.5 for the list of guest operating systems for which Site Recovery Manager supports IP customization.

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 one site, the NIC uses the IP settings from the other site.

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. The power on process happens immediately before the Wait for VMTools process for each virtual machine.

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.

- Customize IP Properties For an Individual Virtual Machine

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

- 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.

- Customizing IP Properties for Multiple Virtual Machines

  Manually configuring IP settings for many virtual machines at a recovery site can be time consuming and can lead to errors in configuration. To facilitate the configuration process for multiple virtual machines, Site Recovery Manager includes the DR IP Customizer tool.

Customize IP Properties For an Individual Virtual Machine

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

Procedure

1. Click **Recovery Plans**, and click the plan that you want to customize.
2. Click the **Virtual Machines** tab, right-click a virtual machine, and select **Configure**.
3. Select the NIC for which you will modify IP Settings.
4. To customize settings, enable the **Customize IP settings during recovery** option.

5 Click **Configure Protection** or **Configure Recovery**, depending on which set of IP settings you want to configure.

6 Click the **General** tab to configure settings.

   a Choose the type of addressing to be used.

      Available options include DHCP, static IPv4, or static IPv6.

   b 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 **Update** to import current settings configured on the virtual machine.

7 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**.

8 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.

9 Repeat Step 5 through Step 8 to configure recovery or protection settings, if required.

   For example, if you configured IP settings for the protected site, you might want to configure settings for the recovery site.

10 Repeat the configuration process for other NICs, as required, beginning by choosing another NIC as described in Step 3.

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, as shown in this example.

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out path_to_report_file.xml
--vc vcenter_server_address
```

To restrict the list of networks to just the ones required by a specific recovery plan, include the `-plan` option on the command line, as shown in this example.

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out path_to_report_file.xml
--vc vcenter_server_address
--plan recovery_plan_name
```

Note The command normally asks you to verify the thumbprints presented by the certificates at each site. You can suppress the verification request by including the `-I` option.

Customizing IP Properties for Multiple Virtual Machines

Manually configuring IP settings for many virtual machines at a recovery site can be time consuming and can lead to errors in configuration. To facilitate the configuration process for multiple virtual machines, Site Recovery Manager includes the DR IP Customizer tool.

You 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 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.

See the Compatibility Matrix for vCenter Site Recovery Manager 5.5 for the list of guest operating systems for which Site Recovery Manager supports IP customization.

- 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.

- 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.

- 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.

- 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.

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.

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]
[--vc vCenter Server address]
[--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
`--cfg arg`	Path to the XML configuration file of the Site Recovery Manager Server, `vmware-dr.xml` file.	Yes
`--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` command generates a basic CSV file for all virtual machines that Site Recovery Manager protects for a vCenter Server instance. ■ 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 to use as input.	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.
`--vc arg`	vCenter Server host name. Virtual machine IDs for the protected virtual machines are different at each site. Use the same vCenter Server instance when you generate the CSV file and when you apply it.	Yes
`-i [ --ignore-thumbprint ]`	Ignore the vCenter Server thumbprint confirmation prompt.	No

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

Option	Description	Mandatory
`-e [ --extra-dns-columns ]`	Obsolete.	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

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.

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.
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.

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

Column	Description	Customization Rules
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.
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 or one static IPv6 address. For example, if you set a static address for IPv4, you must set the IPv6 address 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.

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

Column	Description	Customization Rules
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 IPv4 address or one static IPv6 address. For example, if you set a static address for IPv6, you must set the IPv4 address 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.
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.

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 multiple IP addresses for a network adapter 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.

Examples of DR IP Customizer CSV Files

You obtain a CSV file that contains the networking information for the protected virtual machines on the vCenter Server by running `dr-ip-customizer.exe` with the `--cmd generate` command. You edit the CSV file to customize the IP settings of the protected virtual machines.

You can download a bundle of the example CSV files that this section describes.

Example: A Generated DR IP Customizer CSV File

For a simple setup with only two protected virtual machines, the generated CSV file might contain only the virtual machine ID, the virtual machine name, the names of the vCenter Server instances on both sites, and a single adapter.

```
VM ID,VM Name,vCenter Server,Adapter ID,DNS Domain,Net BIOS,
Primary WINS,Secondary WINS,IP Address,Subnet Mask,Gateway(s),
IPv6 Address,IPv6 Subnet Prefix length,IPv6 Gateway(s),
DNS Server(s),DNS Suffix(es)
```

```
protected-vm-10301,vm-3-win,vcenter-server-site-B,0,,,,,,,,,,,,
protected-vm-10301,vm-3-win,vcenter-server-site-A,0,,,,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-B,0,,,,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-A,0,,,,,,,,,,,,
```

This generated CSV file shows two virtual machines, vm-3-win and vm-1-linux. The virtual machines are present on the protected site and on the recovery site, vcenter-server-site-B, and vcenter-server-site-A. DR IP Customizer generates an entry for each virtual machine and each site with Adapter ID 0. You can add additional lines to customize each NIC, once you are aware of how many NICs are on each virtual machine.

Example: Setting Static IPv4 Addresses

You can modify the generated CSV file to assign two network adapters with static IPv4 addresses to one of the virtual machines, vm-3-win, on the protected site and the recovery site.

For readability, the example CSV file in the following table omits empty columns. The DNS Domain, NetBIOS, IPv6 Address, IPv6 Subnet Prefix length, and IPv6 Gateway(s) columns are all omitted.

Table 8-3. Setting Static IPv4 Addresses in a Modified CSV File

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com

Table 8-3. Setting Static IPv4 Addresses in a Modified CSV File (Continued)

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301		vcenter-server-site-A	1			192.168.0.21	255.255.255.0	192.168.0.1		
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

The information in this CSV file applies different static IPv4 settings to vm-3-win on the protected site and on the recovery site.

- On the vcenter-server-site-B site:
  - Sets the DNS suffixes example.com and eng.example.com for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, a static IPv4 address 192.168.1.21, and DNS server 1.1.1.1.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, a static IPv4 address 192.168.1.22, and DNS server 1.1.1.2.
- On the vcenter-server-site-A site:
  - Sets the DNS suffixes example.com and eng.example.com for all NICs for this virtual machine.
  - Sets the DNS servers 1.1.0.1 and 1.1.0.2 for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, with a static IPv4 address 192.168.0.21.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 1.2.3.4 and 1.2.3.5 and a static IPv4 address 192.168.0.22.

Example: Setting Static and DHCP IPv4 Addresses

You can modify the generated CSV file to assign multiple NICs to one of the virtual machines, vm-3-win, that use a combination of static and DHCP IPv4 addresses. The settings can be different on the protected site and the recovery site.

For readability, the example CSV file in the following table omits empty columns. The DNS Domain, NetBIOS, IPv6 Address, IPv6 Subnet Prefix length, and IPv6 Gateway(s) columns are all omitted.

Table 8-4. Setting Static and DHCP IPv4 Addresses in a Modified CSV File

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
protected-vm-10301		vcenter-server-site-A	1			dhcp				
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

The information in this CSV file applies different static and dynamic IPv4 settings to vm-3-win on the protected site and on the recovery site.

- On site vcenter-server-site-B:
  - Sets the DNS suffixes example.com and eng.example.com for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, that uses DHCP to obtain an IP address and sets the static DNS server 1.1.1.1.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, with a static IPv4 address 192.168.1.22 and DNS server 1.1.1.2.

- On site vcenter-server-site-A:
  - Sets the DNS suffixes to example.com and eng.example.com for all NICs for this virtual machine.
  - Sets the DNS servers 1.1.0.1 and 1.1.0.2 for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, that uses DHCP to obtain an IPv4 address and the globally assigned DNS server information.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 1.2.3.4 and 1.2.3.5, and a static IPv4 address 192.168.0.22.

Example: Setting Static and DHCP IPv4 and IPv6 Addresses

You can modify the generated CSV file to assign multiple NICs to vm-3-win, one of the virtual machines. The NICs can use a combination of static and DHCP IPv4 and IPv6 addresses. The settings can be different on both the protected site and the recovery site.

For readability, the example CSV file in the following table omits empty columns. The DNS Domain and NetBIOS columns are omitted.

Table 8-5. Setting Static and DHCP IPv4 and IPv6 Addresses in a Modified CSV File

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	IPv6 Address	IPv6 Subnet Prefix length	IPv6 Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301	vm-3-win	vcenter-server-site-B	0										example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0										eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	dhcp			1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	dhcp			::ffff:192.168.1.22	32	::ffff:192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0										example.com

Table 8-5. Setting Static and DHCP IPv4 and IPv6 Addresses in a Modified CSV File (Continued)

VM ID	VM Name	vCenter Server	Adapter ID	Primary WINS	Secondary WINS	IP Address	Subnet Mask	Gateway(s)	IPv6 Address	IPv6 Subnet Prefix length	IPv6 Gateway(s)	DNS Server(s)	DNS Suffix(es)
protected-vm-10301	vm-3-win	vcenter-server-site-A	0										eng.example.com
protected-vm-10301		vcenter-server-site-A	1			dhcp			::ffff:192.168.0.22	32	::ffff:192.168.0.1	::ffff:192.168.0.250	
protected-vm-10301		vcenter-server-site-A	1									::ffff:192.168.0.251	
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1				1.1.1.1	

The information in this CSV file applies different IP settings to vm-3-win on the protected site and on the recovery site.

- On site vcenter-server-site-B:
  - Sets the DNS suffixes example.com and eng.example.com for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, that sets a static IPv4 address 192.168.1.21, uses DHCP to obtain an IPv6 address, and uses DNS server 1.1.1.1.
  - Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 2.2.3.4 and 2.2.3.5, that uses DHCP to obtain an IPv4 address, sets a static IPv6 address ::ffff:192.168.1.22, and uses DNS server 1.1.1.2.
- On site vcenter-server-site-A:
  - Sets the DNS suffixes to example.com and eng.example.com for all NICs for this virtual machine.
  - Adds a NIC, Adapter ID 1, that uses DHCP to obtain an IPv4 address and sets a static IPv6 address ::ffff:192.168.1.22. Adapter ID 1 uses static IPv6 DNS servers ::ffff:192.168.0.250 and ::ffff:192.168.0.251.

- Adds a NIC, Adapter ID 2, with primary and secondary WINS servers 1.2.3.4 and 1.2.3.5, a static IPv4 address 192.168.0.22, and DNS server 1.1.1.1. By leaving the IPv6 column blank, Adapter ID 2 uses DHCP for IPv6 addresses.

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.

Prerequisites

Use the DR IP Customizer tool on a computer with access to vCenter Server instances in your environment.

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.

```
dr-ip-customizer.exe --cfg ..\config\vmware-dr.xml --cmd generate --out
"C:\MassIPCustCSVs\MassIPCust-generate-output.csv" --vc vc04.eng.example.com
```

This example points `dr-ip-customizer.exe` to the `vmware-dr.xml` file of the Site Recovery Manager Server and generates the file `MassIPCust-generate-output.csv` for the vCenter Server instance `vc04.eng.example.com`.

4 (Optional) Check the vCenter Server thumbprint and type **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.

   ```
   dr-ip-customizer.exe --cfg ..\config\vmware-dr.xml --cmd apply --csv
   "C:\MassIPCustCSVs\MassIPCust-ipv6.csv" --vc vc04.eng.example.com
   ```

   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 file `MassIPCustCSVs\MassIPCust-ipv6.csv` to the vCenter Server instance `vc04.eng.example.com`.

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.

Advanced Site Recovery Manager Configuration 9

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:

Configure Protection for a Virtual Machine or Template

You can edit the protection properties of any virtual machine or template in a protection group. You can change the resource mappings, attached storage devices and their datastores, and other properties that control the configuration with which Site Recovery Manager recovers the virtual machine.

You must configure protection for virtual machines that have a status of Not Configured or Mapping Missing.

If you are using array-based replication, editing the properties of a virtual machine to add or change storage devices, such as hard disks or DVD drives, can affect the protection of that machine if the device that you add is stored on a datastore that is not replicated, or that is protected by a different protection group.

- If the new device is created on a replicated datastore that is not part of any protection group, the datastore is added to the virtual machine's protected datastore group and the protection of the virtual machine is unaffected.
- If the new device is created on a replicated datastore that is protected by a different protection group, this invalidates the protection of the virtual machine.
- If the new device is created on a nonreplicated datastore, this invalidates the protection of the virtual machine.

- If you use Storage vMotion to move a virtual machine to a nonreplicated datastore, or to a replicated datastore on an array that Site Recovery Manager has not been configured to manage (through an SRA), this invalidates the protection of the virtual machine. You can use Storage vMotion to move a virtual machine to datastore that is part of another protection group.

Procedure

1. Click **Protection Groups** in the Site Recovery Manager interface and select the protection group that includes the virtual machine to configure.
2. On the **Virtual Machines** tab, right-click a virtual machine and select **Configure Protection**.
3. In the **Virtual Machine Properties** window, review and configure properties as needed.

   a. Click **Folder** to specify an alternate destination folder.

   b. Click **Recovery Pool** to specify an alternate resource pool in which to place the recovered virtual machine.

   c. If configuring protection for a template, click **Recovery Host** to specify an alternate host to which to recover the virtual machine.

      This step only applies to templates.

   d. Click **Network** to specify an alternate recovery network to which to restore the virtual machine.
4. Click **OK** to apply the new configuration to the selected virtual machine.

Configure Resource Mappings for a Virtual Machine

If you have not specified inventory mappings for your site, you must configure resource mappings for individual virtual machines. You can configure resource mappings only if site-wide inventory mappings have not been established.

If inventory mappings have been established for a site, you cannot override them by configuring the protection of individual virtual machines. If you need to override inventory mappings for a few members of a protection group, use the vSphere Client to connect to the recovery site and edit the settings of the placeholders or move them to a different folder or resource pool.

Procedure

1. Click **Protection Groups**, and navigate to the protection group that includes the virtual machine that you want to configure.
2. On the Virtual Machines page, right-click a virtual machine and click **Configure Protection**.

   If you established inventory mappings, they are applied.
3. Configure mappings as needed.

   For most virtual machines, you can change the Folder and Compute Resource mappings. For more information, see Configure Protection for a Virtual Machine or Template.

Specify a Nonreplicated Datastore for Swap Files

Every virtual machine requires a swap file. By default, vCenter Server creates swap files in the same datastore as the other virtual machine files. To prevent Site Recovery Manager from replicating swap files you can configure virtual machines to create them in a nonreplicated datastore.

Caution Under normal circumstances, you should keep the swap files in the same datastore as the other virtual machine files. However, you might need to prevent replication of swap files to avoid excessive consumption of network bandwidth. Also, some storage vendors recommend that you do not replicate swap files. Only prevent replication of swap files if it is absolutely necessary.

If you are using a nonreplicated datastore for swap files, you must create a nonreplicated datastore for all protected clusters at both the protected and recovery sites. The nonreplicated datastore must be visible to all hosts in the cluster, otherwise vMotion will not work.

Procedure

1. In the vSphere Client, right-click an ESXi cluster and click **Edit Settings**.
2. In the Settings page for the cluster, click **Swapfile Location**, select **Store the swapfile in the datastore specified by the host**, and click **OK**.
3. For each host in the cluster, select a nonreplicated datastore.

    a. Select a host and click the **Configuration** tab.

    b. In the Software panel, click **Virtual Machine Swapfile Location**, and click **Edit** at the top right of the main panel.

    c. On the Virtual Machine Swapfile Location page, select a nonreplicated datastore and click **OK**.
4. For standalone hosts that are not part of a cluster, select the host and click the **Configuration** tab.
5. In the Software panel, click **Virtual Machine Swapfile Location**, and click **Edit** at the top right of the main panel.
6. Select **Store the swapfile in a swapfile datastore selected below**, select the datastore, and click **OK**.
7. Power off and power on all of the virtual machines in the cluster.

    Resetting the guest operating system is not sufficient. The change of swapfile location takes effect after you power off then power on the virtual machines.
8. Browse the datastore that you selected for swapfiles and verify that VSWP files are present for the virtual machines in the cluster.

Recovering 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 **Auto**, then virtual machines that are recovered across hosts are placed in their own test network. Each test switch is isolated between hosts. As a result, virtual machines in the same plan are isolated when the 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.

Resize Virtual Machine Disk Files During Replication Using Replication Seeds

vSphere Replication prevents you from resizing the virtual machine disk file during replication. If you used replication seeds for the target disk, you can resize the disk manually.

Procedure

1. Unconfigure replication on the virtual machine.
2. Resize the disk on the source site.
3. Resize the target disk that is left over after you unconfigure replication.
4. Reconfigure replication on the virtual machine.

Resize Virtual Machine Disk Files During Replication Without Using Replication Seeds

vSphere Replication prevents you from resizing the virtual machine disk file during replication. If you did not use replication seeds during configuration of the target disk, vSphere Replication deletes the target disk when you stop the replication.

To resize a virtual machine disk if you did not initially use replication seeds, you must perform a test recovery, clone the recovered virtual machine, and reconfigure the disk manually using replication seeds.

Procedure

1. Run a test recovery for the virtual machine.
2. Clone the recovered virtual machine on the same datastore where the replication occurs after you reconfigure the replication.
3. Revert the test recovery.
4. Unconfigure the replication.
5. Resize the disk on the source site.
6. Resize the disk on the cloned virtual machine on the target site.
7. Unregister the cloned virtual machine on the target site, but do not delete the disks.
8. Enable replication by using the disks of the cloned virtual machine as seeds.

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 Local Site Settings

Site Recovery Manager monitors consumption of resources on the Site Recovery Manager Server host, and it 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. Click **Sites** in the Site Recovery Manager interface, right-click the site on which to change settings, and select **Advanced Settings**.
2. Click **localSiteStatus**.

3 Change the settings as needed.

Option	Action
Change the interval at which Site Recovery Manager checks the CPU usage, disk space, and free memory at the local site	Type a new value in the **localSiteStatus.checkInterval** text box.
Change the name of the local site	Type a new value in the **localSiteStatus.displayName** 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	Type a new value in the **localSiteStatus.eventFrequency** text box.
Change the percentage of CPU usage that causes Site Recovery Manager to raise a high CPU usage event	Type a new value in the **localSiteStatus.maxCpuUsage** text box.
Change the percentage of free disk space that causes Site Recovery Manager to raise a low disk space event	Type 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	Type a new value in the **localSiteStatus.minMemory** text box.

4 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.

Procedure

1 Click **Sites** in the Site Recovery Manager interface, right-click the site on which to change settings, and select **Advanced Settings**.

2 Click **logManager**.

3 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	Select a logging level from the **logManager.Default** drop-down menu.
Set logging level for the external API module	Select a logging level from the **logManager.ExternalAPI** drop-down menu.
Set logging level for vSphere Replication	Select a logging level from the **logManager.HbrProvider** drop-down menu.
Set logging level for the IP Customizer tool	Select a logging level from the **logManager.IPCustomizer** drop-down menu.
Set logging level for inventory mapping	Select a logging level from the **logManager.InventoryMapper** drop-down menu.
Set logging level for licensing issues	Select a logging level from the **logManager.Licensing** drop-down menu.
Set logging level for persistence issues	Select a logging level from the **logManager.Persistence** drop-down menu.
Set logging level for recovery operations	Select a logging level from the **logManager.Recovery** drop-down menu. By default, recovery logging is set to **trivia**.
Set logging level for recovery configuration operations	Select a logging level from the **logManager.RecoveryConfig** drop-down menu.
Set logging level for array-based replication operations	Select a logging level from the **logManager.Replication** drop-down menu.

Option	Description
Set logging level for authorization issues between Site Recovery Manager Server and vCenter Server	Select a logging level from the **logManager.ServerAuthorization** drop-down menu.
Set logging level for session management	Select a logging level from the **logManager.SessionManager** drop-down menu.
Set logging level for the SOAP Web Services adapter	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	Select a logging level from the **logManager.Storage** drop-down menu.
Set logging level for messages from the array-based storage provider	Select a logging level from the **logManager.StorageProvider** drop-down menu.

4 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 choose.

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 when recovery plan steps run. 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 at the moment that you configure protection on that virtual machine:

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

If you change any of these advanced settings after you have configured the protection of a virtual machine, the new settings do not apply to that virtual machine. Modifications to these advanced settings apply only to virtual machines that you protect after you changed the settings. This is by design, because if Site Recovery Manager were to apply changed advanced settings to virtual machines on which you have already configured protection, this could lead to unwanted changes in the protection of those virtual machines.

To apply the changes that you make in these advanced settings to virtual machines that you have previously protected, you must reconfigure those virtual machines individually. 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 also apply all of the new advanced settings by removing the protection from a virtual machine by removing it from a protection group and then adding it back in the protection group. Adding the virtual machine back in the protection group will apply the newer advanced settings to the virtual machine.

Procedure

1 Click **Sites** in the Site Recovery Manager interface, right-click the site on which to change settings, and select **Advanced Settings**.

2 Click **recovery**.

3 Modify the recovery site settings.

Option	Action
Change the IP customization timeout	Type a new value in the **recovery.customizationTimeout** text box.
Change the default priority for recovering a virtual machine	Type a new value in the **recovery.defaultPriority** text box.
Enable or disable forced recovery	Select or deselect the **recovery.forceRecovery** check box. You should only activate forced recovery in cases where a lack of connectivity to the protected site severely affects RTO.
Change the timeout for hosts in a cluster to power on	Type a new value in the **recovery.hostPowerOnTimeout** text box.
Change the timeout for guest OS to power off	Type a new value in the **recovery.powerOffTimeout** text box. The new time-out value applies to power-off tasks for virtual machines at the recovery site.
Change the delay after powering on a virtual machine before starting dependent tasks	Type 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	Type 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.
Enable or disable skipping the shutdown of the guest OS	Select or deselect the **recovery.skipGuestShutdown** check box. If protected virtual machines do not have VMware Tools installed and the guest shutdown timeout is not set to 0, you must select this option. If you do not select this option and VMware Tools is not installed, a recovery cannot progress past the step Shutdown VMs at the recovery site.

4 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 Click **Sites** in the Site Recovery Manager interface, right-click the site on which to change settings, and select **Advanced Settings**.

2 Click **remoteSiteStatus**.

3 Modify the settings.

Option	Action
Change the number of remote site status checks (pings) to try before declaring the check a failure	Type a new value in the **remoteSiteStatus.pingFailedDelay** text box.
Change the number of failed pings before raising a site down event	Type a new value in the **remoteSiteStatus.panicDelay** text box.
Change the interval at which Site Recovery Manager checks whether the Site Recovery Manager Server at the remote site is available	Type a new value in the **remoteSiteStatus.pingInterval** text box.

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

Change the Timeout for the Creation of Placeholder Virtual Machines

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

Procedure

1 Click **Sites** in the Site Recovery Manager interface, right-click the site on which to change settings, and select **Advanced Settings**.

2 Click **replication**.

3 Change the **replication.placeholderVmCreationTimeout** setting to modify the number of seconds to wait when creating a placeholder virtual machine.

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

Change Storage Settings

You can adjust the settings of your storage array, to modify how Site Recovery Manager and vCenter Server communicate with the storage replication adapter (SRA).

Procedure

1 Click **Sites** in the Site Recovery Manager interface, right-click the site on which to change settings, and select **Advanced Settings**.

2 Click **storage**.

3 Modify the storage settings.

Option	Action
Change SRA update timeout	Type a new value in the **storage.commandTimeout** text box.
Change the maximum number of concurrent SRA operations	Type a new value in the **storage.maxConcurrentCommandCnt** text box.
Change the minimum amount of time in seconds between datastore group computations	Type a new value in the **storage.minDsGroupComputationInterval** text box.
Change the interval between status updates for ongoing data synchronization operations	Type a new value in the **storage.querySyncStatusPollingInterval** text box.
Change the interval between storage array discovery checks	Type a new value in the **storage.storagePingInterval** text box.
Change the maximum amount of time permitted for data synchronization operations to complete	Type a new value in the **storage.syncTimeout** text box.

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

Change Storage Provider Settings

For array-based replication, the SAN provider is the interface between Site Recovery Manager and your storage replication adapter (SRA). Some SRAs require you to change default SAN provider values. You can change the default timeout values and other behaviors of the Site Recovery Manager SAN provider.

You can change settings for resignaturing, fixing datastore names, host rescan counts, and timeouts. For more information about these values, see the SRA documentation from your array vendor.

Procedure

1 Click **Sites** in the Site Recovery Manager interface, right-click the site on which to change settings, and select **Advanced Settings**.

2 Click **storageProvider**.

3 Modify the SAN provider settings.

Option	Action
Make Site Recovery Manager attempt to detach and reattach LUNs with duplicate volumes	Select the **storageProvider.autoDetachLUNsWithDuplicateVolume** check box.
Set the `LVM.EnableResignature` flag on ESXi hosts during test and recovery	In the **storageProvider.autoResignatureMode** text box, type **`0`** to disable, **`1`** to enable, or **`2`** to ignore the flag. The default setting is 0. If you set this flag to 1, Site Recovery Manager resignatures all known VMFS snapshot volumes, including any volumes that Site Recovery Manager does not manage. If you leave the flag set to 0, Site Recovery Manager only resignatures the VMFS snapshot volumes that it manages.
Force removal, upon successful completion of a recovery, of the `snap-`*`xx`* prefix applied to recovered datastore names	Select the **storageProvider.fixRecoveredDatastoreNames** check box.
Delay host scans during testing and recovery	SRAs can send responses to Site Recovery Manager before a promoted storage device on the recovery site is available to the ESXi hosts. When Site Recovery Manager receives a response from an SRA, it rescans the storage devices. If the storage devices are not fully available yet, ESXi Server does not detect them and Site Recovery Manager does not find the replicated devices when it rescans. Datastores are not created and recovered virtual machines cannot be found. To delay the start of storage rescans until they are available on the ESXi hosts, type a new value in the **storageProvider.hostRescanDelaySec** text box. Only change this value if you experience problems with unavailable datastores.
Repeat host scans during testing and recovery	Type a new value in the **storageProvider.hostRescanRepeatCnt** text box. Some storage arrays require more than one rescan, for example to discover the snapshots of failed-over LUNs. In previous releases, you might have used the `storageProvider.hostRescanRepeatCnt` parameter to introduce a delay in recoveries. Use the `storageProvider.hostRescanDelaySec` parameter instead.
Change the interval that Site Recovery Manager waits for each HBA rescan to complete	Type a new value in the **storageProvider.hostRescanTimeoutSec** text box.
Set the number of times that Site Recovery Manager attempts to resignature a VMFS volume	Type a new value in the **storageProvider.resignatureFailureRetryCount** text box.
Set a timeout for resignaturing a VMFS volume	Type a new value in the **storageProvider.resignatureTimeoutSec** text box. If you change the **storageProvider.hostRescanTimeoutSec** setting, increase the **storageProvider.resignatureTimeoutSec** setting to the same timeout that you use for **storageProvider.hostRescanTimeoutSec**.
Search for VMX files in recovered datastores to identify virtual machines that Storage vMotion has moved before or during a test or a recovery	The option is selected by default. Deselect the **storageProvider.storageVmotionVmxSearch** check box to disable this option.

Option	Action
Identify VMX file paths that Site Recovery Manager should not consider as potential VMX file candidates after Storage vMotion	Some arrays create VMX file paths that the `storageProvider.storageVmotionVmxSearch` search algorithm should ignore. Type a comma-separated list of strings in the **storageProvider.storageVmotionVmxFilePathsToSkip** text box to identify VMX file paths to ignore after Storage vMotion. Site Recovery Manager does not consider VMX file paths that contain one or more of these strings as potential candidate VMX files after Storage vMotion.
Change the interval that Site Recovery Manager waits for recovered datastores to become accessible	Type a new value in the **storageProvider.waitForAccessibleDatastoreTimeoutSec** text box. Change this value if you experience timeouts caused by Site Recovery Manager checking for datastores that are not available yet. This setting is available in Site Recovery Manager 5.5.1 and later.
Change the interval that Site Recovery Manager waits for recovered datastores to be added to vCenter Server	Type a new value in the **storageProvider.waitForRecoveredDatastoreTimeoutSec** text box. Change this value if you experience timeouts caused by Site Recovery Manager checking for datastores that have not been detected by vCenter Server yet. This setting is available in Site Recovery Manager 5.5.1 and later.
Change the interval that Site Recovery Manager waits for VMFS volumes to be mounted	Type a new value in the **storageProvider.waitForVmfsVolumesMountedStateTimeoutSec** text box. Change this value if you experience timeouts caused by Site Recovery Manager checking for VMFS volumes that take a long time to mount. This setting is available in Site Recovery Manager 5.5.1 and later.

4 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 Click **Sites** in the Site Recovery Manager interface, right-click the site on which to change settings, and select **Advanced Settings**.

2 Click **vrReplication**.

3 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	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.

Option	Description
Change the timeout period for reverse replication during reprotect operations	Type a new value in the **reverseReplicationTimeout** 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 reverses replication during reprotect operations.
Change the timeout period for vSphere Replication synchronization operations	Type a new value in the **synchronizationTimeout** text box. 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	Type 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.

4 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 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 Right-click a cluster in the vCenter Server Inventory and select **Edit Settings > vSphere DRS > Advanced Options**.

2 Set the srmMaxBootShutdownOps setting.

Option	Description
Option text box	Type srmMaxBootShutdownOps.
Value text box	Type the maximum number of boot 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.

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

4 Log into the Site Recovery Manager Server host.

5 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.

6 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.

7 Restart the Site Recovery Manager Server to apply the new settings.

8 Click **Sites** in the Site Recovery Manager interface, right-click the site on which to change settings, and select **Advanced Settings**.

9 Select **vrReplication** and increase the synchronizationTimeout setting.

The default value is 7200 and corresponds to a working synchronization timeout period of 14400 seconds.

10 Select **storage** and increase the commandTimeout setting.

For example, increase the commandTimeout value to 3600 seconds.

11 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** menus in the vSphere 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.

To modify the settings, see Modify Settings to Run Large Site Recovery Manager Environments.

Table 9-1. 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 Client by right-clicking a cluster and selecting **Edit Settings > vSphere DRS > Advanced Options**. This setting overrides 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 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 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 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 9-2. Settings that Modify Timeout Periods

Option	Description
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 **Advanced Settings > vrReplication** in the Site Recovery Manager client plug-in. The default value is 7200 and corresponds to a working synchronization timeout period of 14400 seconds.
commandTimeout	The timeout for running SRA commands in ABR-related workflows. In some cases, such as surfacing LUNs and snapshots, some arrays take longer than the default time to respond. Modify this option in **Advanced Settings > storage** in the Site Recovery Manager client plug-in. The default value is 5 minutes.

Troubleshooting Site Recovery Manager

10

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:

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 Virtual Machines with Snapshots

Array-based replication supports the protection and recovery of virtual machines with snapshots, but with limitations.

You can specify a custom location for storing snapshot delta files by setting the `workingDir` parameter in VMX files. Site Recovery Manager does not support the use of the `workingDir` parameter.

Limitations also apply if you are running versions of ESX or ESXi Server older than version 4.1.

- If the virtual machine has multiple VMDK disk files, all the disk files must be contained in the same folder as the VMX file itself.
- If a virtual machine is attached to a Raw Disk Mapping (RDM) disk device, you must store the mapping file in the same folder as the VMX file. RDM snapshots are only available if you create the RDM mapping using Virtual Compatibility Mode.

If you are running a ESX or ESXi Server 4.1 or later, these limitations do not apply.

vSphere Replication supports the protection of virtual machines with snapshots, but you can only recover the latest snapshot. vSphere Replication erases the snapshot information in the recovered virtual machine, so snapshots are no longer available after recovery.

Protection and Recovery of Virtual Machines with Memory State Snapshots

When protecting virtual machines with memory state snapshots, the ESXi hosts at the protection and recovery sites must have compatible CPUs, as defined in the VMware knowledge base articles VMotion CPU Compatibility Requirements for Intel Processors and VMotion CPU Compatibility Requirements for AMD Processors. The hosts must also have the same BIOS features enabled. If the BIOS configurations of the servers do not match, they show a compatibility error message even if they are otherwise identical. The two most common features to check are Non-Execute Memory Protection (NX / XD) and Virtualization Technology (VT / AMD-V).

Protection and Recovery of Linked Clone Virtual Machines

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

Array-based replication supports the protection and recovery of virtual machines that are linked clones if all the nodes in the snapshot tree are replicated.

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.

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.

Protection and Recovery of Virtual Machines Attached to RDM Disk Devices

The protection and recovery of virtual machines that are attached to a raw disk mapping (RDM) disk device is subject to different support depending on whether you use array-based replication or vSphere Replication.

- Array-based replication supports RDM devices in physical mode and in virtual mode.
- vSphere Replication supports RDM devices in virtual mode only, for both the source and target device.

Planned Migration of Virtual Machines on Datastores that Use SIOC

You cannot use Site Recovery Manager to perform a planned migration of virtual machines on datastores that have storage I/O control (SIOC) enabled. Datastores with SIOC enabled cannot be unmounted, so cannot be part of a planned migration. You must disable SIOC on datastores included in a recovery plan before running a planned migration.

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

If you run a recovery with SIOC enabled, the recovery will succeed with errors. After the recovery, you must manually disable SIOC on the protected site and run a planned migration recovery again. You cannot run reprotect until you have successfully run a planned migration.

Protection and Recovery of Virtual Machines with Components on Multiple Arrays

Array-based replication in Site Recovery Manager depends on the concept of an array pair. Site Recovery Manager defines groups of datastores that it recovers as units. As a consequence, limitations apply to how you can store the components of virutal machines that you protect using array-based replication.

- Site Recovery Manager does not support storing virtual machine components on multiple arrays on the protected site that replicate to a single array on the recovery site.
- Site Recovery Manager does not support storing virtual machine components on multiple arrays on the protected site that replicate to mulitple arrays on the recovery site, if the virtual machine components span both arrrays.

If you replicate virtual machine components from multiple arrays to a single array or to a span of arrays on the recovery site, the VMX configurations of the UUID of the datastores on the protected site do not match the configurations on the recovery site.

The location of the VMX file of a virtual machine determines which array pair a virtual machine belongs to. A virtual machine cannot belong to two array pairs, so if it has more than one disk and if one of those disks is in an array that is not part of the array pair to which the virtual machine belongs, Site Recovery Manager cannot protect the whole virtual machine. Site Recovery Manager handles the disk that is not on the same array pair as the virtual machine as a non-replicated device.

As a consequence, store all the virtual disks, swap files, RDM devices, and the working directory for the virtual machine on LUNs in the same array so that Site Recovery Manager can protect all the components of the virtual machine.

Protection and Recovery of Active Directory Domain Controllers

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

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.

vSphere Replication Limitations

vSphere Replication is subject to some limitations when replicating virtual machines.

Replicating Large Volumes

vSphere Replication can replicate virtual machines greater than 2TB with the following limitations:

- If you move a virtual machine with replicated disks over 2032GB back to a machine on an older release, vSphere Replication cannot replicate or power on the virtual machine.
- Full sync of very large disks can take days.
- vSphere Replication must track changed blocks and consumes more memory on larger disks.
- vSphere Replication tracks larger blocks on disks over 2TB. Replication performance on a disk over 2TB might be different on a disk over 2TB for the same workload depending on how much of the disk goes over the network for a particular set of changed blocks.
- Replication might consume more or less bandwidth depending on the workload and how it changes blocks on the disk during the RPO interval.

Shared Disk Support

vSphere Replication cannot replicate virtual machines that share vmdk files in this release.

Site Recovery Manager Events and Alarms

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.

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 five minutes.
- The connection monitor skips a number of failed pings. You can configure this number by setting the `remoteSiteStatus.pingFailedDelay` value.
- 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.
- Site Recovery Manager continues to send `RemoteSiteDownEvent` events until the connection is reestablished.

Configure Site Recovery Manager Alarms

Site Recovery Manager adds alarms to the alarms that vCenter Server supports. You can configure Site Recovery Manager alarms to send an email notification, send an SNMP trap, or to run a script on the vCenter Server host.

The **Alarms** tab in the Site Recovery Manager interface lists all of the Site Recovery Manager alarms. You can edit the settings for each alarm to specify the action for Site Recovery Manager to take when an event triggers the alarm. By default, none of the Site Recovery Manager alarms act until you configure the alarm.

Prerequisites

For alarms to send email notifications, you must configure the **Mail** settings in the **vCenter Server Settings** menu.

Procedure

1 In the left pane, click **Sites**, and select a site.

2 Click the **Alarms** tab to display the list of Site Recovery Manager alarms.

3 Right-click an alarm and click **Edit Settings**.

4 Click the **Actions** tab.

5 Click **Add** to add an action to perform when this alarm is triggered.

6 Select an action from the drop-down list.

Option	Description
Send Email	The default action. Type an email address in the **Value** text box.
Send SNMP Trap	Type the name of an SNMP trap in the **Value** text box.
Run Script	Type the path to the script to run in the **Value** text box.

7 Click the **General** tab.

8 Select the **Enable this alarm** check box to enable the action for this alarm.

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 10-1. Site Status Events

Event Key	Event Description	Cause
`UnknownStatusEvent`	Unknown Status	Site Recovery Manager Server status is not available
`RemoteSiteDownEvent`	Remote Site Down	Site Recovery Manager Server has lost its connection with the remote Site Recovery Manager Server.
`RemoteSitePingFailedEvent`	Remote Site Ping Failed	Failures at the remote site or network connectivity problems.
`RemoteSiteCreatedEvent`	Remote Site Created	Remote site is created.
`RemoteSiteUpEvent`	Remote Site Up	Site Recovery Manager Server re-establishes its connection with the remote Site Recovery Manager Server.
`RemoteSiteDeletedEvent`	Remote Site Deleted	Remote site has been deleted.

Protection Group Events

Protection Group events provide information about actions and status related to protection groups.

These events have three categories:

- Protection Group Replication Informational Events
- Protection Group Replication Warning Events
- Protection Group Replication Error Events

Table 10-2. Protection Group Replication Informational Events

Event Key	Event Description	Cause
ProtectionGroup > CreatedEvent	Created protection group.	Posted on both vCenter Servers in the completion of the Commit phase of creating a protection group.
ProtectionGroup > RemovedEvent	Removed protection group.	Posted on both vCenter Servers in the completion of the Commit phase of removing a protection group.
ProtectionGroup > ReconfiguredEvent	Reconfigured protection group.	Posted on both vCenter Servers in the completion of the Commit phase of reconfiguring a protection group.
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.

Table 10-2. Protection Group Replication Informational Events (Continued)

Event Key	Event Description	Cause
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.
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.
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.
PlaceholderVmCreatedEvent	The placeholder virtual machine was created in the VMware vCenter Server inventory.	Posted on the Recovery site vCenter Server only when we create the placeholder virtual machine as a result of protection, repair.
PlaceholderVmCreatedFromOldProductionVmEvent	The placeholder virtual machine was created in the VMware vCenter Server inventory using the identity of the old protected virtual machine.	Posted on the Recovery site vCenter Server only when we create the placeholder virtual machine as a result of swapping for the old protected virtual machine during or after reprotect.

Table 10-3. Protection Group Replication Warning Events

Event Key	Event Description	Cause
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.
PlaceholderVmUnexpectedlyDeletedEvent	Virtual machine in group: The placeholder virtual machine was removed from the VMware vCenter Server inventory.	Posted on the Recovery site vCenter Server only when we detect that the placeholder virtual machine was unexpectedly deleted or removed from the vCenter inventory.

Table 10-4. Protection Group Replication Error Events

Event Key	Event Description	Cause
ProductionVmDeletedEvent	Virtual machine in group: The protected virtual machine has been removed from the virtual machineware vCenter Server inventory.	Posted when we detect that the protected virtual machine's protected virtual machine has been deleted or removed from the vCenter inventory.
ProductionVmInvalidEvent	Virtual machine in group: Cannot resolve the file locations of the protected virtual machine for replication.	Posted whenever we handle device or recovery location changes but notice that the provider cannot find the protected virtual machine files in order to replicate them.

Recovery Events

Recovery events provide information about actions and status related to the Site Recovery Manager recovery processes.

Table 10-5. Recovery Events

Event	Description	Cause
`RecoveryVmBegin`	Recovery plan has begun recovering the specified virtual machine.	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.
`RecoveryVmEnd`	Recovery plan has completed recovering the virtual machine.	Signaled after the last post-power on script has completed, or after a recovery-stopping error has occurred for the virtual machine.
`PlanCreated`	Recovery plan *hostname*has been created.	Signaled when a new plan is created. It is sent to each vCenter Server instance where the plan is hosted.
`PlanDestroy`	Recovery plan has been destroyed.	Signaled when a plan has been deleted from the site. Note that on the site where the plan has been requested to 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.
`PlanEdit`	Recovery plan was changed.	Signaled when an existing plan is edited.
`PlanExecTestBegin`	Recovery plan has begun a test.	Signaled on the recovery site when a recovery test is initiated.
`PlanExecTestEnd`	Recovery plan has completed a test.	Signaled on the recovery site when a recovery test has completed.
`PlanExecCleanupBegin`	Recovery plan has begun a test cleanup.	Signaled on the recovery site when a test cleanup is initiated.
`PlanExecCleanupEnd`	Recovery plan has completed a test cleanup.	Signaled on the recovery site when a test cleanup has completed.

Table 10-5. Recovery Events (Continued)

Event	Description	Cause
`PlanExecBegin`	Recovery plan has begun a recovery.	Signaled on the recovery site when a recovery is initiated.
`PlanExecEnd`	Recovery plan has completed a recovery.	Signaled on the recovery site when a recovery has completed.
`PlanExecReprotectBegin`	Recovery plan has begun a reprotect operation.	Signaled on the recovery site when a reprotect is initiated.
`PlanExecReprotectEnd`	Recovery plan has completed a reprotect operation.	Signaled on the recovery site when a reprotect has completed.
`PlanPromptDisplay`	Recovery plan is displaying a prompt and is waiting for user input.	Signaled on the recovery site when a prompt step is encountered. The key is a unique identifier for the prompt.
`PlanPromptResponse`	Recovery plan has received an answer to its prompt.	Signaled on the recovery site when a prompt step is closed.
`PlanServerCommandBegin`	Recovery plan has started to run a command on the Site Recovery Manager Server machine.	Signaled on the recovery site when Site Recovery Manager has started to run a callout command on the Site Recovery Manager Server machine.
`PlanServerCommandEnd`	Recovery plan has completed executing a command on the Site Recovery Manager Server machine.	Signaled on the recovery site when Site Recovery Manager has finished running a callout command on the Site Recovery Manager Server machine.
`PlanVmCommandBegin`	Recovery plan has started to run a command on a recovered virtual machine.	Signaled on the recovery site when Site Recovery Manager has started to run a callout command on a recovered virtual machine.
`PlanVmCommandEnd`	Recovery plan has completed executing a command on a recovered virtual machine.	Signaled on the recovery site when Site Recovery Manager has finished running a callout command on a recovered virtual machine.

Storage and Storage Provider Events

Storage and storage provider events provide information about actions and status related storage or storage providers.

Table 10-6. SRA Events

Event	Description	Cause
`StorageAdaptLoadEvent`	Loaded the specified SRA.	Site Recovery Manager detected new SRA either during startup or during user-initiated SRAs reload.
`StorageAdaptReloadFailEvent`	Failed to load SRA from the specified path.	Site Recovery Manager failed to reload previously known SRA either during startup or during user-initiated SRAs reload.
`StorageAdaptChangeEvent`	Loaded new version of the specified SRA.	Site Recovery Manager detected that previously known SRA was upgraded.

Table 10-7. Array Manager Events

Event	Description	Cause
`SAManagerAddedEvent`	Created the specified array manager using the specified SRA.	User added an Array Manager.
`SAManagerRemovedEvent`	Deleted the specified array manager.	User removed an Array Manager.
`SAManagerReconfigEvent`	Reconfigured the specified array manager.	User edited Array Manager properties.
`SAManagerPingOkEvent`	Ping for the specified array manager succeeded.	Site Recovery Manager Server successfully pinged an Array Manager.
`SAManagerPingFailEvent`	Failed to ping the specified array manager.	An error occurred during Array Manager ping.

Table 10-8. Array Pair Events

Event	Description	Cause
`SAPairDiscoveredEvent`	Discovered replicated array pair with Array Manager.	User created Array Manager which discovered replicated array pairs.
`SAPairEnabledEvent`	Enabled replicated array pair with Array Manager.	User enabled an Array Pair.
`SAPairDisabledEvent`	Disabled replicated array pair with Array Manager.	User disabled an Array Pair.
`SAPairPingOkEvent`	Ping for replicated array pair succeeded.	Site Recovery Manager Server successfully pinged the array pair.
`SAPairPingFailEvent`	Failed to ping replicated array pair.	An error occurred during Array Pair ping.

Table 10-9. Datastore Events

Event	Description	Cause
`StorageDsDiscoveredEvent`	Discovered replicated datastore.	Site Recovery Manager Server discovered replicated datastore.
`StorageDsLostEvent`	Specified datastore is no longer replicated.	User turned off replication of storage devices backing the datastore.

Table 10-9. Datastore Events (Continued)

Event	Description	Cause
`StorageRdmDiscoveredEvent`	Discovered replicated RDM attached to specified virtual machine.	Site Recovery Manager Server discovered replicated RDM. This is raised when you add an RDM disk to a protected virtual machine.
`StorageRdmLostEvent`	RDM attached to specified virtual machine is no longer replicated.	User turned off replication of the LUN backing the RDM.

Table 10-10. Protection Events

Event	Description	Cause
`SPDsProtEvent`	Protected datastore in specified protection group.	User included datastore in new or existing protection group.
`SPDsUnprotEvent`	Unprotected specified datastore.	User removed datastore from protection group or deleted protection group which contained this datastore. This is raised if you unprotect a datastore either by removing it from a protection group or by removing the protection group.
`SPVmDiscoveredEvent`	Discovered replicated virtual machine.	User created virtual machine on a replicated datastore.
`SPVmLostEvent`	Specified virtual machine is no longer replicated	User migrated virtual machine off of the replicated datastore.
`SPDsProtMissingEvent`	Replicated datastore needs to be included in specified protection group but is included in an alternate protection group.	This is raised if you have a datastore that needs to be merged and is still not protected. At the conflict event, the datastore is already protected.
`SPDsProtConflictEvent`	Replicated datastore needs to be included in specified protection group.	This is raised if you have a datastore that needs to be merged and is still not protected. At the conflict event, the datastore is already protected.
`SPDsReplicationLostEvent`	Datastore included in specified protection group is no longer replicated.	User turned off replication for devices backing the datastore.
`SPGroupProtRestoredEvent`	Protection has been restored for specified protection group.	The previous (non-empty) issues of a protection group are cleared.
`SPVmDsProtMissingEvent`	Datastore used by virtual machine needs to be included in specified protection group.	If you add a datastore to a VM that is already protected by a protection group and this datastore is not part of this protection group, you need to add it.
`SPVmDsProtConflictEvent`	Datastore used by specified virtual machine needs to be added to specified protection group, but is currently in use by an alternate protection group.	If you add a datastore to a VM that is already protected by a protection group and this datastore is not part of this protection group, you need to add it.
`SPVmDsReplicationLostEvent`	Datastore used by specified virtual machine and included in specified protection group is no longer replicated.	See description.

Table 10-10. Protection Events (Continued)

Event	Description	Cause
`SPVmProtRestoredEvent`	Protection for specified virtual machine in specified protection group has been restored.	The previous (non-empty) issues for a protected virtual machine are cleared. The event will not be posted when issues related to non-protected virtual machine are cleared
`SPCgSpansProtGroupsEvent`	Specified consistency group spans specified protection groups.	This is raised if you have two datastores protected in different protection groups but then later you merge them into a single consistency group on the array.
`SPCgDsMissingProtEvent`	Datastore from specified consistency group needs to be included in specified protection group.	See description.
`SPDsSpansConsistGroupsEvent`	Datastore spans devices from different consistency groups.	This is raised if you have a datastore on top of multiple LUNs but these LUNs do not belong to the same consistency group.
`SPNfsDsUrlConflictEvent`	NFS datastores mounted from specified volume have different URLs mounted from the remote host. The remote path has the specified URL, while the datastore mounted from the other host has the specified URL.	The same NFS volume is mounted using the different IP addresses of the same NFS server in two different datastores.

Licensing Events

Licensing events provide information about changes in Site Recovery Manager licensing status.

Table 10-11. Licensing Events

Type	Description	Content
`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.

Table 10-11. Licensing Events (Continued)

Type	Description	Content
`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 10-12. Permissions Events

Type	Description	Content
`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.

SNMP traps for Site Recovery Manager 5.x are backward compatible with Site Recovery Manager 4.0 and later releases.

Table 10-13. 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.

Table 10-13. SNMP Traps (Continued)

Event	Description	Cause
`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.
`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.
`RecoveryPlanServerCommandBeginTrap`	This trap is sent when a recovery plan starts the execution of a command callout on Site Recovery Manager Server machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name.
`RecoveryPlanServerCommandEndTrap`	This trap is sent when a recovery plan has finished the execution of a command callout on Site Recovery Manager Server machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name, 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.

Table 10-13. SNMP Traps (Continued)

Event	Description	Cause
`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.

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.

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 10-14. 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

Table 10-14. vSphere Replication Events (Continued)

Event Name	Event Description	Event Type	Category	Event Target
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
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

Table 10-14. vSphere Replication Events (Continued)

Event Name	Event Description	Event Type	Category	Event Target
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
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	Warning	Virtual Machine

Table 10-14. vSphere Replication Events (Continued)

Event Name	Event Description	Event Type	Category	Event Target
Unquiesced crash consistent sync completed	Unquiesced crash consistent sync completed. Quiescing failed or virtual machine is powered off.	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
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

Collecting Site Recovery Manager Log Files

Site Recovery Manager creates several log files that contain information that can help VMware Support diagnose problems. You can use the Site Recovery Manager log collector to simplify log file collection.

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 client log files contain information about the client configuration and messages related to client plug-in operations. 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.

Site Recovery Manager also provides for the collection of vSphere Replication log files as part of the Site Recovery Manager log bundle. 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.

- Collect Site Recovery Manager Log Files By Using the Site Recovery Manager Interface

  You can download logs for Site Recovery Manager, the vSphere Replication appliance, and vSphere Replication servers to a user-specified location.

- Collect Site Recovery Manager Log Files Manually

  You can download Site Recovery Manager Server log files in a log bundle that you generate manually. This is useful if you are unable to access the vSphere Client.

Collect Site Recovery Manager Log Files By Using the Site Recovery Manager Interface

You can download logs for Site Recovery Manager, the vSphere Replication appliance, and vSphere Replication servers to a user-specified location.

Use this information to understand and resolve issues. For best results, collect logs from each site.

Procedure

1. Click **Sites**, and select a site.
2. Click the **Summary** tab, and click **Export System Logs**.
3. In the **Download Location** text box, enter a path or click **Browse** to browse to a location.
4. (Optional) Deselect the **Include VR system logs** check box to disable the download of vSphere Replication log data.

   vSphere Replication system logs are downloaded by default. These logs include information about vSphere Replication management server (VRMS), vSphere Replication server, and replication events.
5. Click **OK** to download the logs.

The **Downloading System Logs Bundles** window provides information about the log bundles.

- A list of each host system, the status of their log bundle download, and other details.
- Download Details provides information on the log bundle file name and destination for the log bundle file.

This process does not collect client logs. You must collect client logs separately.

Collect Site Recovery Manager Log Files Manually

You can download Site Recovery Manager Server log files in a log bundle that you generate manually. This is useful if you are unable to access the vSphere Client.

The bundle of logs that these procedures generate is identical to the logs that you generate by using the vSphere Client.

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 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.

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 into 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 5242880 bytes.

```
<log>

   <maxFileSize>5242880</maxFileSize>

</log>
```

5 Set the maximum number of log files to retain.

You set the maximum number of logs by adding a `<maxFileSize>` section to the `<log>` section. The default is 10 log files.

```
<log>

   <maxFileNum>50</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, trivia, and verbose.

```
<log>

   <level>verbose</level>

</log>
```

9. 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 in the `<log>` section.

   ```
   <log>

      <coreDump>C:\ProgramData\VMware\VMware vCenter Site Recovery
       Manager\DumpFiles</coreDump>

   </log>
   ```

10. (Optional) Set the level of logging for specific Site Recovery Manager Server components.

    You can set specific logging levels for the `SoapAdapter`, `SanConfigManager`, `Recovery`, `Folders`, `Libs`, and `HttpConnectionPool` components by modifying the appropriate `<level>` sections. The possible logging levels are error, warning, info, trivia, and verbose.

    ```
    <level id="Recovery">
       <logName>Recovery</logName>
       <logLevel>trivia</logLevel>
    </level>
    ```

11. (Optional) Set the level of logging for storage replication adapters.

    Setting the Site Recovery Manager logging level does not set the logging level for SRAs. You change the SRA logging level by adding a `<level id="SraCommand">` section to `vmware-dr.xml` to set the SRA logging level. The possible logging levels are error, warning, info, trivia, and verbose.

    ```
    <level id="SraCommand">
       <logName>SraCommand</logName>
       <logLevel>trivia</logLevel>
    </level>
    ```

12. Restart the Site Recovery Manager Server service for changes to take effect.

Access the vSphere Replication Logs

You can use the vSphere Replication logs for system monitoring and troubleshooting. A VMware support engineer might request these logs during a support call.

To access and download the vSphere Replication logs, you need access to the vSphere Replication virtual appliance management interface (VAMI). vSphere Replication rotates its logs when the log file reaches 50MB and keeps at most 12 compressed log files.

To manually copy log files, see Manually Access the vSphere Replication Logs.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.

Procedure

1 Connect to the VAMI of the vSphere Replication appliance in a Web browser.

The URL for the VAMI is https://*vr-appliance-address*:5480.

You can also access the VAMI by clicking **Configure VR Appliance** in the **Summary** tab in the vSphere Replication view of the Site Recovery Manager interface.

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`

Resolve Site Recovery Manager Operational Problems

If you encounter problems with creating protection groups and recovery plans, failover, recovery, or guest customization, you can troubleshoot the problem.

Site Recovery Manager Doubles the Number of Backslashes in the Command Line When Running Callouts

When a backslash is a part of the callout command line, Site Recovery Manager doubles all backslashes.

Problem

The command-line system interpreter treats double backslashes as a single backslash only in file paths. If the callout command requires a backslash in a parameter other than a file path and the command does not convert double backslashes to a single backslash, the callout command might fail with an error.

For example, you can add a callout step to the workflow and enter the following text as a command:

```
c:\Windows\system32\cmd.exe /C "C:\myscript.cmd" a/b/c \d\e\f \\g\\h c:\myscript.log
```

As result of the callout step, Site Recovery Manager runs the following command:

```
c:\\Windows\\system32\\cmd.exe /C "C:\\myscript.cmd" a/b/c \\d\\e\\f \\\\g\\\\h c:\\myscript.log
```

If `myscript.cmd` does not change the double backslash to a single backslash, and parameters `\d\e\f` and `\\g\\h` are sensitive to the number of back slashes, `myscript.cmd` can fail.

Solution

1 Create an additional command-line batch file to contain commands and all required parameters. The callout step runs this additional batch file without any argument. For the example, the solution is as follows:

   a In a text editor such as Notepad, create a file `c:\SRM_callout.cmd` with the following content: **`C:\myscript.cmd a/b/c \d\e\f \\g\\h c:\myscript.log`**

   b In a recovery plan callout step, type the command to run: **`c:\\Windows\\system32\\cmd.exe /C c:\SRM_callout.cmd`**

2 Add a code to the original script file that replaces double back slashes with a single back slash.

   a Add code similar to the following sample in the beginning of the script file `c:\myscript.cmd`.

   ```
   @echo off
   set arg2=%2
   set arg3=%3
   set fixed_arg2=%arg2:\\=\%
   set fixed_arg3=%arg3:\\=\%
   ```

   If you use the shift command in a script, all backslash-sensitive parameters are handled this way.

   b If you do not use the shift command in a script, make the following changes:

   Replace `%2` with `%fixed_arg2%`.

   Replace `%3` with `%fixed_arg3%`.

   c Do not change the callout step command.

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 Failover

Site Recovery Manager does not support ESXi environments in which the `LVM.enableResignature` flag is set to 0.

Problem

During a test failover or an actual failover, 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 failover or an actual failover 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 failover or an actual failover 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 configure the appropriate inventory mappings.

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 configure the inventory mappings to map the devices of the virtual machine on the protected site to the corresponding devices on the recovery site.

Solution

Configure the inventory mappings as described in *Site Recovery Manager Installation and Configuration*.

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 the Timeout for the Creation of Placeholder Virtual Machines.

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.

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 failover 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 datastore on the recovery site is full.

Solution

1. Verify that VMware Tools is installed on the virtual machine that you are recovering.
2. Check the available capacity of the datastore on the recovery site.

   If the datastore is full or almost full, increasing the timeout period for guest customization can resolve the issue.

   a. In the vSphere Client, select the host and select **Configuration > Advanced Settings**.

   b. Update the customization timeout parameter to 1200 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.

Reprotect Fails After Restarting vCenter Server

After you restart vCenter Server, when you use vSphere Replication, reprotect operations sometimes fail.

Problem

After you restart vCenter Server, when you use vSphere Replication, reprotect operations fail with the error

```
Error – Unable to reverse replication for the virtual machine
     'virtual_machine'. The session is not authenticated.
```

Cause

After vCenter Server restarts, it fails to refresh some sessions that Site Recovery Manager uses to communicate with vSphere Replication and causes reprotect to fail.

Solution

Restart the Site Recovery Manager services on both of the sites.

Rescanning Datastores Fails Because Storage Devices are Not Ready

When you start a test recovery or a recovery, some SRAs send responses to Site Recovery Manager before a promoted storage device on the recovery site is available to the ESXi hosts.
Site Recovery Manager rescans the storage devices and the rescan fails.

Problem

If storage devices are not fully available yet, ESXi Server does not detect them and
Site Recovery Manager does not find the replicated devices when it rescans. This can cause several problems.

- Datastores are not created and recovered virtual machines cannot be found.
- ESXi hosts become unresponsive to vCenter Server heartbeat and disconnect from vCenter Server. If this happens,vCenter Server sends an error to Site Recovery Manager and a test recovery or real recovery fails.
- The ESXi host is available, but rescanning and disk resignaturing exceed the Site Recovery Manager or vCenter Server timeouts, resulting in a Site Recovery Manager error.

Cause

The storage devices are not ready when Site Recovery Manager starts the rescan.

Solution

To delay the start of storage rescans until the storage devices are available on the ESXi hosts, increase the `storageProvider.hostRescanDelaySec` setting to a value between 20 and 180 seconds. See Change Storage Provider Settings.

Note In Site Recovery Manager 5.1 and earlier, you might have used the `storageProvider.hostRescanRepeatCnt` parameter to introduce a delay in recoveries. Use the `storageProvider.hostRescanDelaySec` parameter instead.

Scalability Problems when Replicating Many Virtual Machines with a Short RPO to a Shared VMFS Datastore on ESXi Server 5.0

Performance might be slow if you replicate a large number of virtual machines with a short Recovery Point Objective (RPO) to a single virtual machine file store (VMFS) datastore that is accessible by multiple hosts on the recovery site.

Problem

This problem occurs when running ESXi Server 5.0 on the recovery site. It can result in missed RPO targets.

The number of virtual machines that can successfully replicate to a single, shared VMFS datastore increases if the RPO targets are longer.

Follow the guidelines when calculating the number of virtual machines that you should replicate to a single VMFS volume on the recovery site.

- If all your virtual machines have an RPO of 15 minutes, performance is affected when replicating 50 to 100 virtual machines to the same VMFS datastore.
- If all your virtual machines have an RPO of 30 minutes, performance is affected when replicating 100 to 200 virtual machines to the same VMFS datastore.

If you have heterogeneous RPO targets in a protection group, calculate the harmonic mean of the RPO targets when calculating the number of virtual machines that you can replicate to a single VMFS volume. For example, if you have 100 virtual machines with an RPO of 20 minutes and 50 virtual machines with an RPO of 600 minutes, you calculate the harmonic mean of the RPO as follows:

150/(100/20 + 50/600) = ~30

In this example, the configuration is similar to a setup with 150 virtual machines, each having an RPO of approximately 30 minutes. In this case, performance is affected if these 150 virtual machines replicate to a single VMFS volume.

Cause

This problem affects only VMFS datastores that are shared by multiple hosts. It does not occur on datastores that are local to one host or on other datastore types, such as NFS. This problem affects only installations that are running ESXi Server 5.0.

The number of vSphere Replication servers is not relevant. These limits apply to the number of virtual machines that you can replicate to a single VMFS datastore.

Solution

1 Upgrade ESXi Server to version 5.1 or later on the recovery site.

2 If you cannot upgrade ESXi Server to version 5.1 or later, redistribute the replicated virtual machines or adjust their RPO.

   - Reduce the number of virtual machines with a short RPO that replicate to a single VMFS volume, for example by using a larger number of smaller datastores.
   - Increase the RPO of the virtual machines replicating to a single VMFS volume to create a longer harmonic mean RPO.

Application Quiescing Changes to File System Quiescing During vMotion to an Older Host

vSphere Replication can create an application quiesced replica for virtual machines with Windows Server 2008 and Windows 8 guest operating systems running on an ESXi 5.1 or newer host.

Problem

The ESXi 5.1 or newer host is in a cluster with hosts from older versions and you use vMotion to move the replicated virtual machine to an older host. vSphere Replication then creates a file system quiesced replica.

Cause

A mix of ESXi 5.1 (or newer) and older hosts in the cluster creates a file system quiesced replica during vMotion to an older host. The process should instead create an application quiesced replica.

Solution

Make sure that all hosts in the cluster are running ESXi 5.1 or newer before you use vMotion to move a Windows Server 2008 and Windows 8 virtual machine with application quiescing.

Reconfigure Replication on Virtual Machines with No Datastore Mapping

If you did not configure the datastore mappings before configuring vSphere Replication on multiple virtual machines, the replication configuration fails.

Problem

On the **Virtual Machines** tab for a vSphere Replication site, virtual machines appear in red with the status `Datastore mappings were not configured`.

Cause

You did not configure datastore mappings before configuring replication on multiple virtual machines. You must reconfigure replication on the virtual machines individually.

Solution

1. Select the vSphere Replication view in the Site Recovery Manager interface.
2. Select the remote vSphere Replication site and click the **Virtual Machines** tab.
3. Right-click a virtual machine with the status `Datastore mappings were not configured` and select **Configure Replication**.

   The RPO value and any quiescing methods that you set when you attempted to configure the multiple virtual machines are already set.
4. Click **Browse** to select the target datastore for the VMX file and click **Next**.
5. Click **Browse** to select the target datastore for the VMDK file and click **Next**.
6. Select a vSphere Replication server on the target site and click **Next**.
7. Click **Finish**.

   When the reconfiguration is finished, the virtual machine synchronizes with the target site.
8. Repeat Step 3 through Step 7 for all virtual machines that show the status `Datastore mappings were not configured`.

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 error `Multiple source disks, with device keys` *`device_keys`*`, point to the same destination datastore and file path.`

The replication group remains in the error state.

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 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 KB 2037268 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 `VRM Server generic error. Please check the documentation for any troubleshooting information.`.

In addition to the generic error, the message provides more detailed information about the problem, similar to the following examples.

- `VRM Server generic error. Please check the documentation for any troubleshooting information. The detailed exception is: 'org.apache.http.conn.HttpHostConnectException: Connection to https://`*`vCenter_Server_address`*` refused'`. This error relates to problems connecting to vCenter Server.
- `Error – VR synchronization failed for VRM group `*`virtual machine name`*`. Sync monitoring aborted. Please verify replication traffic connectivity between source host and target VR server. Sync will automatically 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. The detailed exception is: '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 `detailed exception` message for information about the problem. Depending on the details of the message, you can try to retry the failed operation, restart vSphere Replication, or correct the infrastructure.

Generating Support Bundles Disrupts vSphere Replication Recovery

If you generate a vSphere Replication log bundle and at the same time attempt to run a recovery, the recovery might fail.

Problem

In heavily loaded environments, generating log bundles can cause vSphere Replication connection problems during recovery operations. Recovery fails with the error

```
VRM Server generic error. Please check the documentation for any
     troubleshooting information. The detailed exception is: 'Failed write-locking
     object:
     object_ID'.
```

Cause

vSphere Replication server is blocked when the log bundle is generated. This situation occurs if the storage for the vSphere Replication virtual machine is overloaded.

Solution

Rerun the recovery. If the recovery still fails, reevaluate the storage bandwidth requirements of the cluster on which vSphere Replication is running, and the network bandwidth if the storage is NAS.

Initial Full Synchronization of Virtual Machine Files to VMware Virtual SAN Storage Is Slow

When using VMware Virtual SAN storage and configuring vSphere Replication on multiple virtual machines, the initial full synchronization takes a long time to complete.

Problem

Configuring vSphere Replication on a large number of virtual machines simultaneously when using vSphere Replication with Virtual SAN storage causes the initial full synchronization of the virtual machine files to run very slowly.

Cause

Initial full synchronization operations generate heavy I/O traffic. Configuring too many replications at the same time can overload the Virtual SAN storage.

Solution

Configure vSphere Replication in batches of a maximum of 30 virtual machines at a time.

vSphere Replication Operations Run Slowly as the Number of Replications Increases

As you increase the number of virtual machines that you replicate, vSphere Replication operations can run more slowly.

Problem

Response times for vSphere Replication operations can increase as you replicate more virtual machines. You possibly experience recovery operation timeouts or failures for a few virtual machines, and RPO violations.

Cause

Every virtual machine in a datastore generates regular read and write operations. Configuring vSphere Replication on those virtual machines adds another read operation to the regular read and write operations, which increases the I/O load on the storage. The performance of vSphere Replication depends on the I/O load of the virtual machines that you replicate and on the capabilities of the storage hardware. If the load generated by the virtual machines, combined with the extra I/O operations that vSphere Replication introduces, exceeds the capabilities of your storage hardware, you might experience slow response times.

Solution

When running vSphere Replication, if response times are greater than 30 ms, reduce the number of virtual machines that you replicate to the datastore. Alternatively, increase the capabilities of your hardware. If you suspect that the I/O load on the storage is an issue and you are using VMware Virtual SAN storage, monitor the I/O latency by using the monitoring tool in the Virtual SAN interface.