Site Recovery Manager Administration

Site Recovery Manager 8.3

vmware®
by **Broadcom**

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

https://docs.vmware.com/

Contents

About VMware Site Recovery Manager Administration

VMware 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

This *Site Recovery Manager 8.3 Administration* guide is updated with each release of the product or when necessary.

This table provides the update history of the *Site Recovery Manager 8.3 Administration* guide.

Revision	Description
05 AUG 2020	At VMware, we value inclusion. To foster this principle with our customer, partner, and internal community, we are replacing some of the terminology in our content. We have updated this guide to remove instances of non-inclusive language.
02 APR 2020	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 permissions on Site Recovery Manager to use a shared recovery site. The vCenter Server administrator on the shared recovery site must manage permissions so that each user has sufficient privileges to configure and use Site Recovery Manager, but no user has access to resources that belong to another user.

- **Assign Site Recovery Manager Roles and Permissions**

  During the installation of Site Recovery Manager, users with the vCenter Server administrator role are granted the administrator role on Site Recovery Manager. Currently, 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. Site Recovery Manager performs the operations by using the user credentials that you provide when you connect the protected and recovery sites.

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

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

Site Recovery Manager and the vCenter Server Administrator Role

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

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

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

Site Recovery Manager and vSphere Replication Roles

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

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

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

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

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

1   Create two user groups.

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

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

4   Add the user to both user groups.

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

Managing Permissions in a Shared Recovery Site Configuration

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

In the context of a shared recovery site, a user is the owner of a pair of Site Recovery Manager Server instances. Users 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 user. No user'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 User Resources

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

- All users must have read access to all folders of the vCenter Server on the shared recovery site.

- Do not give a user the permission to rename, move, or delete the data center or host.

- Do not give a user the permission to create virtual machines outside of the user's dedicated folders and resource pools.

- Do not allow a user to change roles or assign permissions for objects that are not dedicated to the user's own use.

- To prevent unwanted propagation of permissions across different organizations' resources, do not propagate permissions on the root folder, data centers, and hosts of the vCenter Server on the shared recovery site.

Guidelines for Isolating User Resources

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

- Assign to each user a separate virtual machine folder in the vCenter Server inventory.

  - Set permissions on this folder to prevent any other user from placing their virtual machines in it. For example, set the Administrator role and activate the propagate option for a user on that user's folder. This configuration prevents duplicate name errors that might otherwise occur if multiple users protect virtual machines that have identical names.

  - Place all of the user's placeholder virtual machines in this folder, so that they can inherit its permissions.

  - Do not assign permissions to access this folder to other users.

- Assign dedicated resource pools, datastores, and networks to each user, and configure the permissions in the same way as for folders.

Caution   A deployment in which you isolate user resources still assumes trust between the vSphere sites. Even though you can isolate user resources, you cannot isolate the users themselves. This is not a suitable deployment if you must keep all users completely separate.

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

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

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

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

Procedure

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

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

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

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

   b   Enter the name of the specific User/Group or search for a User/Group from the **User/ Group** list, and select it.

   By default the vCenter Single Sign-On returns a maximum of 5000 rows, distributed in two halves. One half for the user and the other half for the Solution Users and Groups. You can change that setting from the vCenter Server advance settings.

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

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

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

4   Select **Propagate to Children** to apply the selected role to all 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.

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

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

Results

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

Example: Combining Site Recovery Manager Roles

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

1   Create two user groups.

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

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

4   Add the user to both user groups.

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

Site Recovery Manager Roles Reference

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

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

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

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

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

Table 1-1. Site Recovery Manager Roles

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
Site Recovery Manager Administrator	The Site Recovery Manager Administrator grants permission to perform all Site Recovery Manager configuration and administration operations. ■ Configure advanced settings. ■ Configure connections. ■ Configure inventory preferences. ■ Configure placeholder datastores. ■ Configure array managers. ■ Manage protection groups. ■ Manage recovery plans. ■ Run recovery plans. ■ Perform reprotect operations. ■ Configure protection on virtual machines. ■ Edit protection groups. ■ Remove protection groups. ■ View storage policy objects. The Site Recovery Manager Administrator user cannot edit inherited permissions. To restrict the access of a specific user or to	**Site Recovery Manager.Advanced Settings.Modify** **Site Recovery Manager.Array Manager.Configure** **Site Recovery Manager.Diagnostics.Export** **Site Recovery Manager.Internal.Internal Access** **Site Recovery Manager.Inventory Preferences.Modify** **Site Recovery Manager.Placeholder Datastores.Configure** **Site Recovery Manager.Protection Group.Assign to Plan** **Site Recovery Manager.Protection Group.Create** **Site Recovery Manager.Protection Group.Modify** **Site Recovery Manager.Protection Group.Remove** **Site Recovery Manager.Protection Group.Remove from Plan** **Site Recovery Manager.Recovery History.Delete History** **Site Recovery Manager.Recovery History .View Deleted Plans** **Site Recovery Manager.Recovery Plan.Configure commands** **Site Recovery Manager.Recovery Plan.Create** **Site Recovery Manager.Recovery Plan.Modify** **Site Recovery Manager.Recovery Plan.Recovery** **Site Recovery Manager.Recovery Plan.Remove** **Site Recovery Manager.Recovery Plan.Reprotect** **Site Recovery Manager.Recovery Plan.Test** **Site Recovery Manager.Remote Site.Modify** **Datastore.Replication.Protect** **Datastore.Replication.Unprotect.Stop** **Resource.Recovery Use** **Virtual Machine. SRM Protection.Protect** **Virtual Machine. SRM Protection.Stop** **Site Recovery Manager.Profile-driven storage.Profile-driven storage view**	■ Virtual machines ■ Datastores ■ vCenter Server folders ■ Resource pools ■ Site Recovery Manager service instances ■ Networks ■ Site Recovery Manager folders ■ Protection groups ■ Recovery plans ■ Array managers

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
	grant access to a user, the Site Recovery Manager Administrator must add a new role.		
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.Stop** **Resource.Recovery Use** **Virtual Machine. SRM Protection.Protect** **Virtual Machine. SRM Protection.Stop**	■ Site Recovery Manager folders ■ Protection groups

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

Role	Actions that this Role Permits	Privileges that this Role Includes	Objects in vCenter Server Inventory that this Role Can Access
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 remove 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

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

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

Replicating Virtual Machines

2

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

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

Read the following topics next:

- Using Array-Based Replication with Site Recovery Manager
- Using vSphere Replication with Site Recovery Manager
- Using Virtual Volumes with Site Recovery Manager
- Using Array-Based Replication and vSphere Replication with Site Recovery Manager

Using Array-Based Replication with Site Recovery Manager

When you use array-based replication, one or more storage arrays at the protected site replicate data to peer arrays at the recovery site. With storage replication adapters (SRAs), you can integrate Site Recovery Manager with a wide variety of arrays.

To use array-based replication with Site Recovery Manager, you must configure replication first before you can configure Site Recovery Manager to use it.

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.

You can protect virtual machines that contain disks that use VMware vSphere Flash Read Cache storage. Since the host to which a virtual machine recovers might not be configured for Flash Read Cache, Site Recovery Manager disables Flash Read Cache on disks when it starts the virtual machines on the recovery site. Site Recovery Manager sets the reservation to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take a note of virtual machine's cache reservation from the vSphere Web Client. After the recovery, you can migrate the virtual machine to a host with Flash Read Cache storage and manually restore the original Flash Read Cache setting on the virtual machine.

If you protect virtual machines by using storage policy protection groups, you must replicate those virtual machines by using array-based replication.

Storage Replication Adapters

Storage replication adapters are not part of a Site Recovery Manager release. Your array vendor develops and supports them. You must install an SRA specific to each array that you use with Site Recovery Manager on the Site Recovery Manager Server host. Site Recovery Manager supports the use of multiple SRAs.

Figure 2-1. Site Recovery Manager Architecture with Array-Based Replication
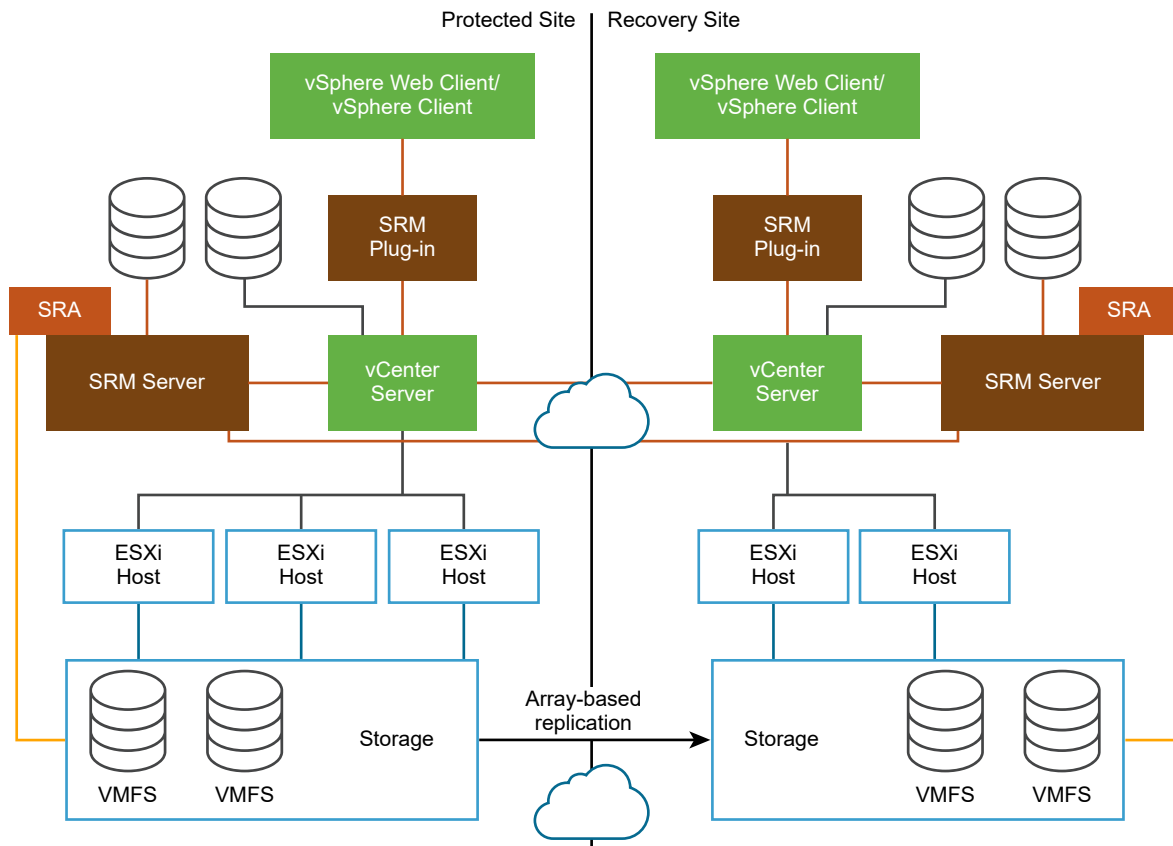
Configure Array-Based Replication

To protect virtual machines that you replicate by using array-based replication, including virtual machines that you protect by using storage policy protection groups, you must configure storage replication adapters (SRAs) at each site.

Install Storage Replication Adapters

If you protect virtual machines by using array-based replication or by using array-based replication with storage policy protection, you must install a Storage Replication Adapter (SRA) specific to each storage array that you use with Site Recovery Manager. An SRA is a program

that an array vendor provides that enables Site Recovery Manager to work with a specific kind of array.

You must install an appropriate SRA on the Site Recovery Manager Server hosts at the protected and recovery sites. If you use more than one type of storage array, you must install the SRA for each type of array on both of the Site Recovery Manager Server hosts.

Note   You can configure Site Recovery Manager to use more than one type of storage array, but you cannot store the virtual machine disks for a single virtual machine on multiple arrays from different vendors. You must store all of the disks for a virtual machine on the same array.

Storage replication adapters come with their own installation instructions. You must install the version of an SRA that corresponds to a specific Site Recovery Manager version. Install the same version of the SRA at both sites. Do not mix SRA versions.

If you are using vSphere Replication, you do not require an SRA.

Prerequisites

- Check the availability of an SRA for your type of storage by consulting the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.

- Download the SRA by going to https://my.vmware.com/web/vmware/downloads, selecting **VMware Site Recovery Manager > Download Product**, then selecting **Drivers & Tools > Storage Replication Adapters > Go to Downloads**.

- If you obtain an SRA from a different vendor site, verify that it has been certified for the Site Recovery Manager release you are using by checking the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.

- Read the documentation provided with your SRA. SRAs do not support all features that storage arrays support. The documentation that your SRA provides details what the SRA supports and requires. For example, HP and EMC have detailed physical requirements which must be met for the SRA to perform as expected.

- Install Site Recovery Manager Server before you install the SRAs.

- Your SRA might require the installation of other vendor-provided components. You might need to install some of these components on the Site Recovery Manager Server host. Other components might require only network access by the Site Recovery Manager Server. For the latest information on such requirements, review the release notes and readme files for the SRAs you are installing.

- Enable the storage array's capability to create snapshot copies of the replicated devices. See your SRA documentation.

Procedure

1 Install the SRA on each Site Recovery Manager Server host.

The installer installs the SRA in `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra`.

2 In the vSphere Client, click **Site Recovery > Open Site Recovery**, select a site pair, and click **View Details**.

3 In the **Site Pair** tab, go to **Configure > Array Based Replication > Storage Replication Adapters** , and click the **Rescan Adapters** button.

This action refreshes SRA information, allowing Site Recovery Manager to discover the SRAs.

Add Storage Replication Adapters to the Site Recovery Manager Appliance

If you plan to use Site Recovery Manager for array-based replication, you must add Storage Replication Adapters (SRA) to the Site Recovery Manager Server. The SRA files are distributed as `.tar.gz` archives.

You must install an appropriate SRA on the Site Recovery Manager Server hosts at the protected and recovery sites. If you use more than one type of storage array, you must install the SRA for each type of array on both of the Site Recovery Manager Server hosts.

Prerequisites

▪ Download the SRA. Go to https://my.vmware.com/web/vmware/downloads, select **VMware Site Recovery Manager > Download Product**, and then select **Drivers & Tools > Storage Replication Adapters > Go to Downloads**.

▪ If you obtain an SRA from a different vendor site, verify that it is certified for the Site Recovery Manager release you are using. See the *VMware Compatibility Guide* for Site Recovery Manager at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.

▪ Enable the storage array's capability to create snapshot copies of the replicated devices. See your SRA documentation.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 In the Site Recovery Manager Appliance Management Interface, click **Storage Replication Adapters**, and click **New Adapter**.

3 Click **Upload**, navigate to the directory where you saved the SRA file, and select it.

4 When the process finishes, click **Close**.

The Storage Replication Adapter card appears in the Site Recovery Manager Appliance Management Interface.

5 Log in to the vSphere Client or the vSphere Web Client.

6 Click **Site Recovery > Open Site Recovery**, select a site pair, and click **View Details**.

7 In the **Site Pair** tab, go to **Configure > Array Based Replication > Storage Replication Adapters** , and click the **Rescan Adapters** button.

Download and Upload Configuration Archives for Storage Replication Adapters

If you use Site Recovery Manager Appliance with array-based replication and you need to replace a Storage Replication Adapter (SRA), you can download the configuration archive for this SRA and then import the configuration into the replacement SRA.

Prerequisites

To download an SRA configuration file and import it into another SRA, you must use SRAs obtained from the same vendor.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 Click the **Storage Replication Adapters** tab.

3 Select the appropriate Storage Replication Adapter card and click the drop-down menu (⋮).

Option	Description
Download Configuration Archive	Download the configuration archive for the selected SRA.
Upload Configuration Archive	Import a configuration for the selected SRA. a Navigate to the directory where you saved the SRA configuration archive file and select it. The configuration files are distributed as `.tar.gz` archives. b Click **Open**.

Delete Storage Replication Adapters

You use the Site Recovery Manager Appliance Management Interface to delete Storage Replication Adapters (SRA) from the Site Recovery Manager Server.

Note If you delete an SRA, any currently running operations involving storage arrays controlled by this adapter are interrupted. This includes, but is not limited to, Recover, Test, Cleanup, Reprotect operations.

Procedure

1 Log in to the Site Recovery Manager Appliance Management Interface as admin.

2 In the Site Recovery Manager Appliance Management Interface, click **Storage Replication Adapters**.

3 Select the appropriate Storage Replication Adapter card, and from the drop-down menu

(⋮) , click **Delete**.

4   Confirm that you are aware of the results of deleting the adapter and click **Delete**.

Rescan Arrays to Detect Configuration Changes

By default, Site Recovery Manager checks arrays for changes to device configurations by rescanning arrays every 24 hours. However, you can force an array rescan at any time.

You can reconfigure the frequency with which Site Recovery Manager performs regular array scans by changing the `storage.minDsGroupComputationInterval` option in Advanced Settings. See Change Storage Settings.

Configuring array managers causes Site Recovery Manager to compute datastore groups based on the set of replicated storage devices that it discovers. If you change the configuration of the array at either site to add or remove devices, Site Recovery Manager must rescan the arrays and recompute the datastore groups.

Procedure

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

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

3   On the Site Pair tab, click **Configure > Array Based Replication > Array Pairs**.

4   Select an array pair and click **Array Manager Pair > Discover Array Pairs** to rescan the arrays, or **Discover Devices** to recompute the storage devices and consistency groups.

When you select an array pair, the **Array Pairs** tab provides detailed information about all the storage devices in the array, including the local device name, the device it is paired with, the direction of replication, the protection group to which the device belongs, whether the datastore is local or remote, and the consistency group ID for each SRA device.

Configure Array Managers

After you pair the protected site and recovery site, configure their respective array managers so that Site Recovery Manager can discover replicated devices, compute datastore groups, and initiate storage operations.

You typically configure array managers only once after you connect the sites. You do not need to reconfigure them unless array manager connection information or credentials change, or you want to use a different set of arrays.

Prerequisites

- Connect the sites as described in Connect the Protected and Recovery Sites in *Site Recovery Manager Installation and Configuration*.

- Install SRAs at both sites as described in Install Storage Replication Adapters.

Procedure

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

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

3 On the Site Pair tab, click **Configure > Array Based Replication > Array Pairs**.

4 Click the **Add** button to add an array manager.

5 Select the storage replication adapter that you want Site Recovery Manager to use and click **Next**.

If no manager type appears, rescan for SRAs or check that you have installed an SRA on the Site Recovery Manager Server host.

6 Enter a name for the local array manager, provide the required information for the type of SRA you selected, and click **Next**.

Use a descriptive name that makes it easy for you to identify the storage associated with this array manager.

For more information about how to fill in the text boxes, see the documentation that your SRA vendor provides. Text boxes vary between SRAs, but common text boxes include IP address, protocol information, mapping between array names and IP addresses, and user name and password.

7 (Optional) If you do not want to create an array pair, select the **Do not create a remote array manager now** check box and click **Finish**.

8 Enter a name for the remote array manager, provide the required information for the type of SRA you selected, and click **Next**.

9 On the **Array pairs** page, select the array pair to enable, then click **Next**.

10 Review the configuration and click **Finish**.

Edit Array Managers

Use the Edit Local Array Manager wizard or the Edit Remote Array Manager wizard to modify an array manager's name or other settings, such as the IP address or user name and password.

For more information about how to fill in the adapter fields, see the documentation that your SRA vendor provides. While fields vary among SRAs, common fields include IP address, protocol information, mapping between array names and IP addresses, and user names and passwords.

Procedure

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

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

3 On the Site Pair tab, click **Configure > Array Based Replication > Array Pairs**.

4 Select an array pair, click **Array Manager Pair**, and click **Edit Local Array Manager** or **Edit Remote Array Manager**.

5 Modify the name for the array.

Use a descriptive name that makes it easy for you to identify the storage associated with this array manager. You cannot modify the array manager type.

6 Modify the adapter information.

These fields are created by the SRA.

7 Click **Save** to complete the modification of the array manager.

Specify an Unreplicated 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 an unreplicated datastore.

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

Note If you are using an unreplicated datastore for swap files, you must create an unreplicated datastore for all protected hosts and clusters at both the protected and recovery sites. All hosts in a cluster must have access to the unreplicated datastore, otherwise vMotion does not work.

Procedure

1 In the vSphere Client, select **Hosts and Clusters**, select a host, and click **Configure**.

2 Under **Virtual Machines**, select **Swap file location**, and click **Edit**.

3 Select **Use a specific datastore**, and select an unreplicated datastore.

4 Click **OK**.

5 Power off and power on all virtual machines on the host.

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.

6 Browse the datastore that you selected for swapfiles and verify that VSWP files are present for the virtual machines.

Isolating Devices for Stretched Storage During Disaster Recovery

In a disaster recovery with stretched storage, the failover command must isolate devices at the recovery site.

If some hosts at the protected site are still operational and continue running virtual machines when you initiate a disaster recovery, Site Recovery Manager cannot power on the corresponding virtual machines at the recovery site due to file locks. If the storage array isolates the devices at the recovery site, the ESX hosts at the recovery site can break the necessary locks and power on the virtual machines.

Site Recovery Manager must use `isolation="true"` in the failover SRA command for the stretched devices that were not deactivated at the protected site.

If there are VMs running at the recovery site from the same device, and the recovery site ESXi is mounting the storage from the protected site, during isolation there is a risk of failing write operations. It is recommended that all VMs on stretched storage are running on the protected site.

Implementation details of isolation for stretched storage are specific to array vendors. Some array vendors might make the devices inaccessible at the protected site after running the failover SRA command with isolation. Some array vendors might break the communication between source and target site for that particular device.

Using vSphere Replication with Site Recovery Manager

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

You deploy the vSphere Replication appliance and configure vSphere Replication on virtual machines independently of Site Recovery Manager. See the vSphere Replication documentation at https://www.vmware.com/support/pubs/vsphere-replication-pubs.html for information about deploying and configuring vSphere Replication.

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

You can configure vSphere Replication to regularly create and retain snapshots of protected virtual machines on the recovery site. Taking multiple point-in-time (PIT) snapshots of virtual machines allows you to retain more than one replica of a virtual machine on the recovery site. Each snapshot reflects the state of the virtual machine at a certain point in time. You can select which snapshot to recover when you use vSphere Replication to perform a recovery.

Figure 2-2. Site Recovery Manager Architecture with vSphere Replication
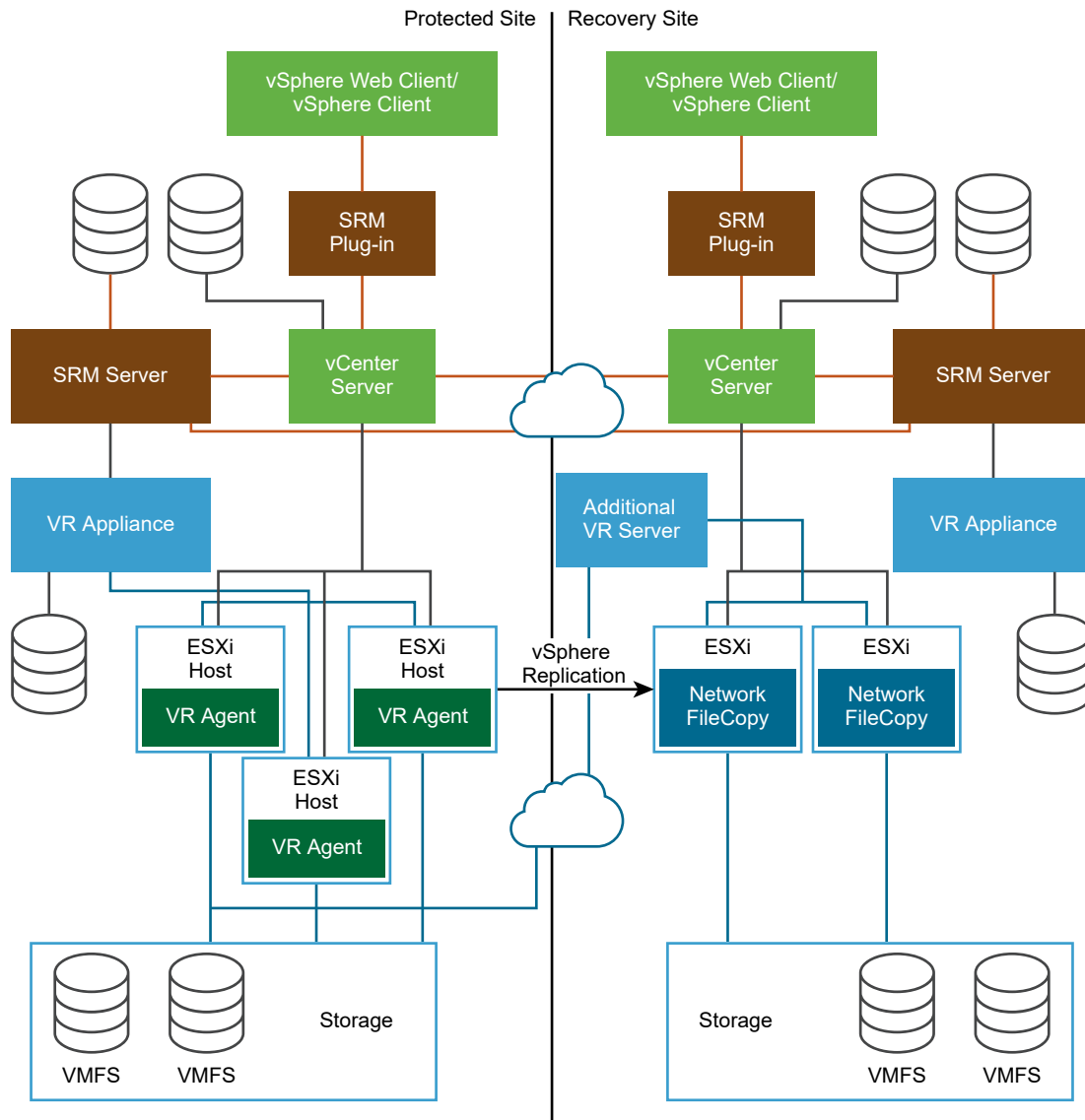
Replicating a Virtual Machine and Enabling Multiple Point in Time Instances

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

When you configure replication of a virtual machine, you can enable multiple point in time (MPIT) 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 a 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 2-3. Recovering a Virtual Machine at Points in Time (PIT)
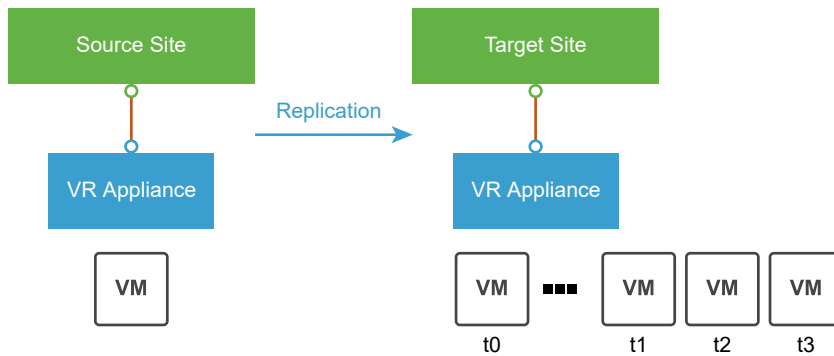
Using Virtual Volumes with Site Recovery Manager

Virtual Volumes supports replication, test recovery, test cleanup, planned migration, disaster recovery and reprotect. With the array-based replication, you can off-load replication of virtual machines to your storage array and use full replication capabilities of the array. You can group several virtual machines to replicate them as a single unit.

Virtual Volumes replication is policy driven. After you configure your Virtual Volumes storage for replication, information about replication capabilities and replication groups is delivered from the array by the storage provider. This information shows in the VM Storage Policy interface of vCenter Server.

You use the VM storage policy to describe replication requirements for your virtual machines. The parameters that you specify in the storage policy depend on how your array implements replication. For example, your VM storage policy might include such parameters as the replication schedule, replication frequency, or recovery point objective (RPO). The policy might also indicate the replication target, a secondary site where your virtual machines are replicated, or specify whether replicas must be deleted.

By assigning the replication policy during VM provisioning, you request replication services for your virtual machine. After that, the array takes over the management of all replication schedules and processes. For additional information how to create and assign Virtual Volumes replication policies, see *Virtual Volumes and Replication* in the *vSphere Storage* guide.

Configure Virtual Volumes

To use Virtual Volumes with Site Recovery Manager, you must configure your Virtual Volumes environment first.

Prerequisites

Follow the guidelines in *Before you enable Virtual Volumes* in the *vSphere Storage* guide.

Procedure

1 Register Storage Providers for Virtual Volumes

   Your Virtual Volumes environment must include storage providers, also called VASA providers. Typically, third-party vendors develop storage providers through the VMware APIs for Storage Awareness (VASA). Storage providers facilitate communication between vSphere and the storage side. You must register the storage provider in vCenter Server to be able to work with Virtual Volumes.

2 Create a Virtual Volumes Datastore

   You use the **New Datastore** wizard to create a Virtual Volumes datastore.

3 Review and Manage Protocol Endpoints

   ESXi hosts use a logical I/O proxy, called protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. Protocol endpoints are exported, along with associated storage containers, by the storage system through a storage provider. Protocol endpoints become visible in the vSphere Client after you map a storage container to a Virtual Volumes datastore. You can review properties of protocol endpoints and modify specific settings.

4 Change the Path Selection Policy for a Protocol Endpoint

   If your ESXi host uses SCSI-based transport to communicate with protocol endpoints representing a storage array, you can modify default multipathing policies assigned to protocol endpoints. Use the **Edit Multipathing Policies** dialog box to change a path selection policy.

Register Storage Providers for Virtual Volumes

Your Virtual Volumes environment must include storage providers, also called VASA providers. Typically, third-party vendors develop storage providers through the VMware APIs for Storage Awareness (VASA). Storage providers facilitate communication between vSphere and the storage side. You must register the storage provider in vCenter Server to be able to work with Virtual Volumes.

After registration, the Virtual Volumes provider communicates with vCenter Server. The provider reports characteristics of underlying storage and data services, such as replication, that the storage system provides. The characteristics appear in the VM Storage Policies interface and can be used to create a VM storage policy compatible with the Virtual Volumes datastore. After you

apply this storage policy to a virtual machine, the policy is pushed to Virtual Volumes storage. The policy enforces optimal placement of the virtual machine within Virtual Volumes storage and guarantees that storage can satisfy virtual machine requirements. If your storage provides extra services, such as caching or replication, the policy enables these services for the virtual machine.

Prerequisites

Verify that an appropriate version of the Virtual Volumes storage provider is installed on the storage side. Obtain credentials of the storage provider.

Procedure

1 Navigate to vCenter Server.

2 Click the **Configure** tab, and click **Storage Providers**.

3 Click the **Add** icon.

4 Enter connection information for the storage provider, including the name, URL, and credentials.

5 Specify the security method.

Action	Description
Direct vCenter Server to the storage provider certificate	Select the **Use storage provider certificate** option and specify the certificate's location.
Use a thumbprint of the storage provider certificate	If you do not guide vCenter Server to the provider certificate, the certificate thumbprint is displayed. You can check the thumbprint and approve it. vCenter Server adds the certificate to the truststore and proceeds with the connection.

The storage provider adds the vCenter Server certificate to its truststore when vCenter Server first connects to the provider.

6 To complete the registration, click **OK**.

Results

vCenter Server discovers and registers the Virtual Volumes storage provider.

Create a Virtual Volumes Datastore

You use the **New Datastore** wizard to create a Virtual Volumes datastore.

Procedure

1 In the vSphere Client object navigator, browse to a host, a cluster, or a data center.

2 From the right-click menu, select **Storage > New Datastore**.

3 Select **vVol** as the datastore type.

4 Enter the datastore name and select a backing storage container from the list of storage containers.

Make sure to use the name that does not duplicate another datastore name in your data center environment.

If you mount the same Virtual Volumes datastore to several hosts, the name of the datastore must be consistent across all hosts.

5 Select the hosts that require access to the datastore.

6 Review the configuration options and click **Finish**.

What to do next

After you create the Virtual Volumes datastore, you can perform such datastore operations as renaming the datastore, browsing datastore files, unmounting the datastore, and so on.

You cannot add the Virtual Volumes datastore to a datastore cluster.

Review and Manage Protocol Endpoints

ESXi hosts use a logical I/O proxy, called protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. Protocol endpoints are exported, along with associated storage containers, by the storage system through a storage provider. Protocol endpoints become visible in the vSphere Client after you map a storage container to a Virtual Volumes datastore. You can review properties of protocol endpoints and modify specific settings.

Procedure

1 Navigate to the host.

2 Click the **Configure** tab.

3 Under **Storage**, click **Protocol Endpoints**.

4 To view details for a specific item, select this item from the list.

5 Use tabs under Protocol Endpoint Details to access additional information and modify properties for the selected protocol endpoint.

Tab	Description
Properties	View the item properties and characteristics. For SCSI (block) items, view and edit multipathing policies.
Paths (SCSI protocol endpoints only)	Display paths available for the protocol endpoint. Disable or enable a selected path. Change the Path Selection Policy.
Datastores	Display a corresponding Virtual Volumes datastore. Perform datastore management operations.

Change the Path Selection Policy for a Protocol Endpoint

If your ESXi host uses SCSI-based transport to communicate with protocol endpoints representing a storage array, you can modify default multipathing policies assigned to protocol endpoints. Use the **Edit Multipathing Policies** dialog box to change a path selection policy.

Procedure

1   Navigate to the host.

2   Click the **Configure** tab.

3   Under **Storage**, click **Protocol Endpoints**.

4   Select the protocol endpoint whose path you want to change and click the **Properties** tab.

5   Under Multipathing Policies, click **Edit Multipathing**.

6   Select a path policy and configure its settings. Your options change depending on the type of storage device you use.

    The path policies available for your selection depend on the storage vendor support.

    ▪   For information about path policies for SCSI devices, see Path Selection Plug-Ins and Policies.

    ▪   For information about path mechanisms for NVMe devices, see VMware High Performance Plug-In and Path Selection Schemes.

7   To save your settings and exit the dialog box, click **OK**.

Using Array-Based Replication and vSphere Replication with Site Recovery Manager

You can use a combination of array-based replication and vSphere Replication in your Site Recovery Manager deployment.

To create a mixed Site Recovery Manager deployment that uses array-based replication and vSphere Replication, you must configure the protected and recovery sites for both types of replication.

▪   Set up and connect the storage arrays and install the appropriate storage replication adapters (SRA) on both sites.

▪   Deploy vSphere Replication appliances on both sites and configure the connection between the appliances.

▪   Configure virtual machines for replication using either array-based replication or vSphere Replication, as appropriate.

    Note   Do not attempt to configure vSphere Replication on a virtual machine that resides on a datastore that you replicate by using array-based replication.

You create array-based protection groups for virtual machines that you configure with array-based replication, and vSphere Replication protection groups for virtual machines that you configure with vSphere Replication. You cannot mix replication types in a protection group. You can mix array-based protection groups and vSphere Replication protection groups in the same recovery plan.

Figure 2-4. Site Recovery Manager Architecture with Array-Based Replication and vSphere Replication
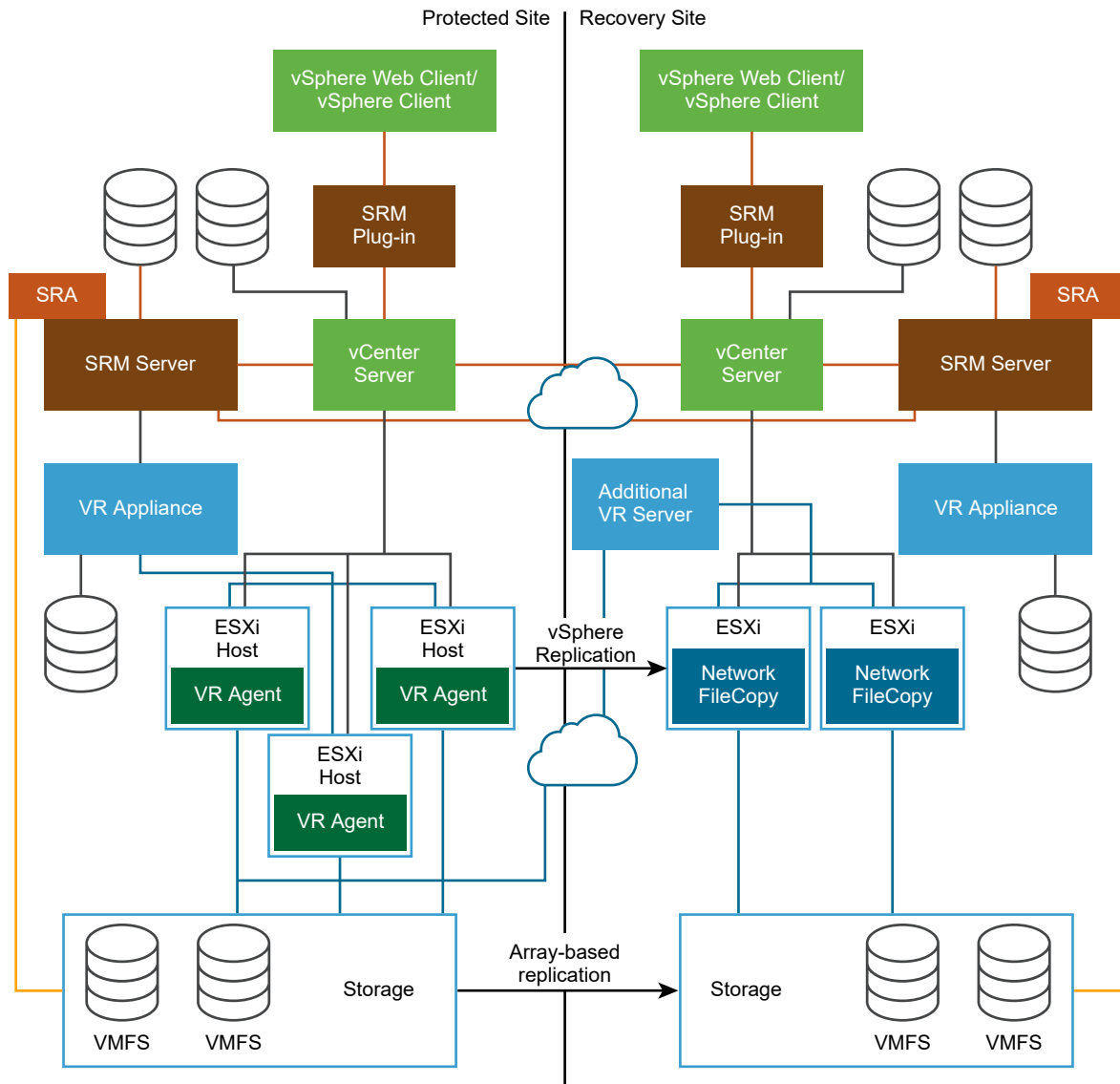
Configuring Mappings

3

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

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

- Networks, including the option to specify a different network to use for recovery plan tests

- Data centers or virtual machine folders

- Compute resources, including resource pools, standalone hosts, vApps, or clusters

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

Site Recovery Manager applies inventory mappings differently depending on whether you use array-based protection groups and vSphere Replication protection groups, or storage policy protection groups. For information about the differences between how Site Recovery Manager applies inventory mappings to the different types of protection group, see Inventory Mappings for Array-Based Replication Protection Groups and vSphere Replication Protection Groups and Inventory Mappings for Storage Policy Protection Groups .

If you use storage policy protection groups, in addition to mapping inventory objects, you map storage policies on the protected site to storage policies on the recovery site.

Read the following topics next:

- Inventory Mappings for Array-Based Replication Protection Groups and vSphere Replication Protection Groups

- Inventory Mappings for Storage Policy Protection Groups

- Configure Inventory Mappings

- About Storage Policy Mappings

- Select Storage Policy Mappings

Inventory Mappings for Array-Based Replication Protection Groups and vSphere Replication Protection Groups

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

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

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

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

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

- For information about configuring site-wide inventory mappings, see Configure Inventory Mappings.

- For information about configuring mappings on virtual machines individually, see Configure Inventory Mappings for an Individual Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

- For information about applying site-wide inventory mappings to an existing protection group, see Apply Inventory Mappings to All Members of an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

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

Inventory Mappings for Storage Policy Protection Groups

For storage policy protection, Site Recovery Manager applies inventory mappings to virtual machines when you run a recovery plan that contains a storage policy protection group.

With array-based and vSphere Replication protection groups, Site Recovery Manager applies inventory mappings at the moment that you configure protection on a virtual machine. With storage policy protection groups, because storage policy protection is dynamic, Site Recovery Manager only applies the inventory mappings at the moment that you run a recovery plan. Virtual machine placement decisions are made according to the inventory mappings when a recovery plan runs, so Site Recovery Manager does not create placeholder virtual machines on the recovery site.

Because Site Recovery Manager applies inventory mappings for storage policy protection groups when you run a recovery plan, you cannot configure individual mappings on virtual machines in storage policy protection groups. Site Recovery Manager always uses the site-wide inventory mappings when you run a recovery with storage policy protection. If inventory mappings are missing, test recovery, planned migration, and disaster recovery of recovery plans that contain storage policy protection groups fail. You can configure Site Recovery Manager to periodically poll the virtual machines in storage policy protection groups for missing mappings and report a warning if any mappings are missing that can cause the storage policy protection group recovery to fail. For information about how to configure periodic polling for missing mappings, see Change Replication Settings.

Note If the network mapping is missing but the other mappings are present and you run a test recovery, Site Recovery Manager uses the auto-generated test network and the test succeeds with a warning. If a test recovery succeeds with a warning about the missing network mapping, configure the network mapping and run the test again. Planned migration and disaster recovery do not use the test network and fail if the network mapping is missing.

If a recovery plan fails due to missing mappings and the protected site is available, configure the missing mappings and run the plan again. For information about how to configure site-wide inventory mappings, see Configure Inventory Mappings.

Resource Inventory Mappings and Storage Policy Protection Groups

As a result of the dynamic virtual machine protection, storage policy protection groups have specific requirements and limitations on how to set resource inventory mappings.

- Site Recovery Manager requires existing resource inventory mappings for all top-level compute resources (clusters or unmanaged hosts) on the protection site that have mounted the datastores protected by a storage policy protection group.

- Site Recovery Manager determines the desired visibility of the recovered datastore based on top-level compute resource mappings and does not consider resource mappings for resource pools.

  - If there is no resource mapping for its parent top-level compute resource, Site Recovery Manager cannot apply an existing mapping for a resource pool.

  - An existing mapping of a protection site resource pool to a different recovery compute resource hierarchy compared to its parent, does not expose the storage of virtual machines under that resource pool to the mapped compute resource.

For a successful storage policy protection group recovery, you must observe the following rules when creating resource mappings.

- Create resource mappings for all protected top-level compute resources (clusters or unmanaged hosts) which have mounted datastores protected by a storage policy protection group.

- If you must create additional mappings for resource pools, map them to a target under the same top-level recovery compute resource, to which their parent top-level protected compute resource is mapped. For example, when the protected host or cluster P is mapped to a recovery host or cluster R or a recovery resource pool under R, then all protected resource pools under P must also be mapped to R or a recovery resource pool under R.

Temporary Placeholder Mappings for Storage Policy Protection

Site Recovery Manager applies inventory mappings for storage policy protection at the moment that you run a recovery plan. If you run a recovery plan that contains storage policy protection groups and you have not configured inventory mappings, or if the objects that you mapped are missing, test recovery, planned migration, and disaster recovery fail.

You can usually only configure inventory mappings when both the protected site and the recovery site are available. If a recovery plan with storage policy protection groups fails due to missing mappings and the protected site is not available, you cannot configure the missing mappings in the normal way. To mitigate this situation, when a recovery fails due to missing mappings and the protected site is not available, Site Recovery Manager creates temporary placeholder mappings. Temporary placeholder mappings allow you to configure the missing mappings so that you can run the recovery successfully when the protected site is offline. Temporary placeholder mappings are incomplete mappings that identify inventory objects on the protected site that contain virtual machines that are included in the recovery plan. The temporary placeholder mappings do not include target objects on the recovery site. When a recovery fails due to missing mappings, the protected site is unavailable, and Site Recovery Manager creates temporary placeholder mappings, you can complete the temporary placeholder mappings and rerun the recovery successfully.

For information about how to configure temporary placeholder mappings, see Configure Temporary Placeholder Mappings.

Configure Temporary Placeholder Mappings

If a recovery plan that contains a storage policy protection group fails due to missing mappings and the protected site is unavailable, Site Recovery Manager creates temporary placeholder mappings. You complete these temporary placeholder mappings so that the recovery can succeed.

Because Site Recovery Manager applies inventory mappings to virtual machines in storage policy protection groups at the moment that you run a recovery plan, storage policy protection groups require site-wide inventory mappings. If site-wide inventory mappings are missing, recovery tests, planned migrations, and disaster recovery of recovery plans that contain storage policy protection groups fail.

If a recovery plan that contains a storage policy protection group fails due to missing mappings and the protected site is available, configure the missing mappings in the normal way and run the recovery again. For information about how to configure site-wide inventory mappings, see Configure Inventory Mappings.

If a recovery plan that contains a storage policy protection group fails due to missing mappings and the protected site is unavailable, you cannot configure the missing mappings normally. To allow the recovery to succeed, you must complete the temporary placeholder mappings that Site Recovery Manager creates when a recovery plan fails due to missing mappings.

Prerequisites

- The protected site is unavailable.

- You ran a disaster recovery on a recovery plan that contains a storage policy protection group.

- The recovery failed due to missing inventory mappings.

Procedure

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

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

3 Click the **Recovery Plans** tab, and select the recovery plan that failed.

4 Select **Recovery Steps** and expand the steps that are in an error state.

5 Hover your pointer over an error message to see the full message.

    If inventory mappings are missing, you see an error about missing mappings.

    For example, if resource mappings are missing, you see `Cannot fetch hosts associated with placeholder VMs. Mapping for resourcePool` *`address`* `missing in resource mappings.`

6 Select the **Site Pair** tab and check the remote SRM connection for the recovery site.

    You see a message informing you that the protected site is offline and that Site Recovery Manager has created temporary placeholder mappings.

7   Select each of the **Network Mappings**, **Folder Mappings**, **Resource Mappings**, and **Storage Policy Mappings** tabs.

Where mappings are missing, Site Recovery Manager has selected a resource on the protected site. The corresponding resource on the recovery site shows `Mapping is missing`.

8   Select the temporary placeholder mapping and click the icon to edit the mapping.

9   Select a resource on the recovery site to map to from the resource on the protected site that Site Recovery Manager selected, and click **OK**.

10 Click the **Recovery Plans** tab, select the recovery plan that failed, and run the recovery plan again.

If you configured all of the missing mappings, the recovery succeeds. If there are still missing mappings, the recovery fails.

11 If the recovery fails again, repeat steps Step 4 to Step 10 until the recovery succeeds.

What to do next

When the protected site is available again, configure site-wide inventory mappings in the normal way and run recovery again so that Site Recovery Manager can complete the recovery steps on the protected site.

Note   Site Recovery Manager does not retain temporary placeholder mappings. The temporary placeholder mappings that you configured are lost if you restart Site Recovery Manager Server on the recovery site. Always configure normal inventory mappings after you have run a recovery in which you had to configure temporary placeholder mappings.

Users Gain Access to Virtual Machines After Configuring Temporary Placeholder Mappings

Users who complete temporary placeholder mappings when the protected site is unavailable might gain access to virtual machines that they should not.

Problem

The protected site is unavailable during a disaster recovery and Site Recovery Manager creates temporary placeholder mappings. The user who runs the recovery plan completes the temporary placeholder mappings and reruns the plan. After the recovery, the user has access to virtual machines on the recovery site that they did not have permission to access on the protected site.

- A user runs a disaster recovery when the protected site is unavailable.

- The user does not have permission to access all of the inventory objects on the protected site.

- Site Recovery Manager detects missing mappings, and creates temporary placeholder mappings that include objects on the protected site that the user does not have permission to access.

- The user configures the target mappings from the objects on the protected site to objects on the recovery site to which they do have access.

- After the recovery, because the recovered virtual machines use resources on the recovery site that the user has permission to access, the user can access virtual machines that they did not have permission to access when those virtual machines were on the protected site.

Cause

If the protected site is unavailable, Site Recovery Manager cannot perform permission checks on inventory objects on the protected site before it uses them to create temporary placeholder mappings.

Solution

Verify that users who have permission to run recovery plans also have permission to access all of the objects on both sites.

Configure Inventory Mappings

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

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

When you use storage policy protection, Site Recovery Manager applies inventory mappings at the moment that a recovery plan runs. You cannot configure protection individually on the virtual machines in a storage policy protection group. As a consequence, you must configure site-wide inventory mappings if you use storage policy protection.

Procedure

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

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

3 On the **Site Pair** tab expand **Configure**, and select the type of resource to configure.

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

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

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

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

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

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

   ▪ If you selected automatic mapping, expand the inventory items on the left to select a parent node on the local site, for example a data center or a folder, then expand the inventory items on the right to select a parent node on the remote site.

   ▪ If you selected manual mapping, expand the inventory items on the left to select a specific object on the local site, then expand the inventory items on the right to select the object on the remote site to which to map this object.

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

   Note Auto-mapping for NSX universal wires is only supported with storage policy protection groups. If you are using virtual machine protection groups, you must explicitly configure network mapping between the two ends of the universal wire to ensure that the virtual machines recover on the same universal wire. See Using Site Recovery Manager with NSX Data Center for vSphere.

7   Click **Add mappings**.

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

8   Click **Next**.

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

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

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

- Select an existing network on the recovery site to use for tests.

10   (Optional) On the **Prepare reverse mappings** page, select the check box for a mapping.

Selecting this option creates corresponding mappings from the item on the remote site to the item on the local site. You require reverse mappings to establish bidirectional protection and to run reprotect operations. You cannot select this option if two or more mappings have the same target on the remote site.

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

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

About Storage Policy Mappings

You can protect virtual machines that you have associated with storage policies by including them in storage policy protection groups.

Storage policies place virtual machines in the vCenter Server inventory and on datastores according to rules and tags that you define in vCenter Server. Storage policies can move virtual machines in the inventory or to different datastores, to accommodate changes in the vCenter Server environment.

If you map storage policies on the protected site to storage policies on the recovery site, when you run a recovery plan, Site Recovery Manager places the recovered virtual machines in the vCenter Server inventory and on datastores on the recovery site according to the storage policy that you mapped to on the recovery site.

Select Storage Policy Mappings

If you map storage policies on the protected site to storage policies on the recovery site, when you run a recovery plan, Site Recovery Manager can place the recovered virtual machines in the vCenter Server inventory and on datastores on the recovery site according to the storage policy that you mapped to on the recovery site.

Prerequisites

You created storage policies on both the protected site and the recovery site.

Procedure

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

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

3. On the **Site Pair** tab, click **Configure > Storage Policy Mappings**.

4. Select a site and click **New** to create a mapping.

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

Option	Description
Automatically prepare mappings for storage policies with matching names	Site Recovery Manager automatically maps storage policies on the protected site to storage policies on the recovery site that have the same name.
Prepare mappings manually	To map specific storage policies on the protected site to specific storage policies on the recovery site.

6. Select the storage policies on the protected site to map to storage policies on the recovery site.

   - If you selected automatic mapping, Site Recovery Manager selects any storage policies on the protected site for which a storage policy with the same name exists on the recovery site.

   - If you selected manual mapping, select a specific storage policy on the protected site, then select the storage policy on the recovery site to which to map this storage policy.

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

7. Click **Add mappings**.

   The mappings appear at the bottom of the page.

8. Click **Next**.

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

    Selecting this option creates corresponding mappings from the storage policy on the remote
    site to the storage policy on the local site. You require reverse mappings to establish
    bidirectional protection and to run reprotect operations. You cannot select this option if two
    or more mappings have the same target on the remote site.

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

About Placeholder Virtual Machines

<div style="text-align: right">

4

</div>

When you create an array-based replication protection group that contains datastore groups or a vSphere Replication protection group that contains individual virtual machines, Site Recovery Manager creates a placeholder virtual machine at the recovery site for each of the virtual machines in the protection group.

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

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

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

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

Note Site Recovery Manager does not create placeholder virtual machines for storage policy protection groups. For information about how Site Recovery Manager places virtual machines on the recovery site when you use storage policy protection groups, see Inventory Mappings for Storage Policy Protection Groups and About Storage Policy Mappings.

About Placeholder Virtual Machine Templates

When you protect a template on the protected site, Site Recovery Manager creates the placeholder template by creating a virtual machine in the default resource pool of a compute resource and then by marking that virtual machine as a template. Site Recovery Manager selects the compute resource from the set of available compute resources in the data center on the

recovery site to which the folder of the virtual machine on the protected site is mapped. All the hosts in the selected compute resource must have access to at least one placeholder datastore. At least one host in the compute resource must support the hardware version of the protected virtual machine template.

About Placeholder Datastores

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

Note Site Recovery Manager does not create placeholder virtual machines for storage policy protection groups. You do not need to identify a placeholder datastore if you only use storage policy protection groups.

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

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

Read the following topics next:

- What Happens to Placeholder Virtual Machines During Recovery
- Select a Placeholder Datastore

What Happens to Placeholder Virtual Machines During Recovery

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

Note Site Recovery Manager does not create placeholder virtual machines for storage policy protection groups. This example applies to array-based protection groups and to vSphere Replication protection groups. It does not apply to storage policy protection groups. For information about how Site Recovery Manager recovers virtual machines when you use storage policy protection groups, see About Storage Policy Protection Groups.

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

1   Virtual machines replicate to the recovery site independently of Site Recovery Manager, according to the type of replication that you use.

    ■   For datastore-based replication, the storage array replicates datastores that contain virtual machine files as raw storage in the target storage array.

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

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

3   When you configure Site Recovery Manager protection on a virtual machine by adding a datastore group or an individual virtual machine to a protection group, Site Recovery Manager creates a placeholder for that virtual machine in the placeholder datastore on the recovery site.

4   When you run a recovery plan, Site Recovery Manager shuts down the virtual machines on the protected site, and activates the virtual machines on the recovery site according to the type of replication that you use.

    ■   For datastore-based replication, Site Recovery Manager surfaces the raw storage on the recovery site that contains the replicated virtual machines as a vCenter Server datastore. Site Recovery Manager registers the recovered datastore with the ESXi host or cluster with which the placeholder datastore is registered.

    ■   vSphere Replication powers on the copies of the virtual machines on the recovery site.

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

Select a Placeholder Datastore

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

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

Note   Site Recovery Manager does not create placeholder virtual machines for storage policy protection groups. You do not need to select a placeholder datastore if you only use storage policy protection groups.

Prerequisites

▪ Verify that you connected and paired the protected and recovery sites.

▪ Placeholder datastores must meet certain criteria.

    ▪ For clusters, the placeholder datastores must be visible to all hosts in the cluster.

    ▪ You cannot select as placeholder datastores any datastores that are replicated by using array-based replication.

Procedure

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

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

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

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

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

Previously configured datastores appear but you cannot select them. If a datastore is replicated, but Site Recovery Manager does not have an array manager for that datastore, the option to select the replicated datastore might be available. Do not select replicated datastores that Site Recovery Manager does not manage.

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

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

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

Important If you use Virtual Volumes replication, do not use Virtual Volumes datastore as a placeholder datastore. Use a local VMFS datastore as the placeholder datastore.

6 Select the other site in the pair.

7 Repeat Step 3 to Step 5 to configure a placeholder datastore on the other site.

Creating and Managing Protection Groups

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

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

You configure virtual machines and create protection groups differently depending on whether you use array-based replication, vSphere Replication, Virtual Volumes replication, or storage policy protection. 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, Virtual Volumes replication, or storage policy protection. You can include a combination of array-based replication protection groups, Virtual Volumes replication protection groups, and vSphere Replication protection groups in the same recovery plan. You cannot include storage policy protection groups in the same recovery plan as array-based replication protection groups, Virtual Volumes replication protection groups, and vSphere Replication protection groups.

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

After you create an array-based replication protection group, Virtual Volumes protection group, or a vSphere Replication protection group, Site Recovery Manager creates placeholder virtual machines on the recovery site and applies the inventory mappings to each virtual machine in the group. If Site Recovery Manager cannot map a virtual machine to a folder, network, or resource pool on the recovery site, Site Recovery Manager sets the virtual machine to the Mapping Missing status, and does not create a placeholder for it. For storage policy protection groups, Site Recovery Manager applies inventory mappings when you run a recovery plan. Site Recovery Manager does not create placeholder virtual machines for storage policy protection groups.

Site Recovery Manager cannot protect virtual machines on which you did not configure or on which you incorrectly configured replication. In the case of array-based replication, this is true even if the virtual machines reside on a protected datastore.

Read the following topics next:

- About Array-Based Replication Protection Groups and Datastore Groups

- vSphere Replication Protection Groups

- About Virtual Volumes Protection Groups

- About Storage Policy Protection Groups

- Protect an Encrypted VM

- Automatic Protection of Virtual Machines

- Overview of Protection Group States

- Overview of Virtual Machine Protection States

- Creating Protection Groups

- Organize Protection Groups in Folders

- Add and Remove Datastore Groups or Virtual Machines to or from a Protection Group

- Apply Inventory Mappings to All Members of an Array-Based, Virtual Volumes, or vSphere Replication Protection Group

- Configure Inventory Mappings for an Individual Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group

- Modifying the Settings of a Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group

- Removing Protection from a Virtual Machine

About Array-Based Replication Protection Groups and Datastore Groups

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

You add virtual machines to an array-based replication protection group by placing them in a datastore that belongs to a datastore group that Site Recovery Manager associates with a protection group. Site Recovery Manager recomputes the datastore groups when it detects a change in a protected virtual machine. For example, if you add a hard disk that is on another LUN to a protected virtual machine, Site Recovery Manager adds the LUN to the datastore group of that protection group. You must reconfigure the protection to protect the new LUN. Site Recovery Manager computes consistency groups when you configure an array pair or when you refresh the list of devices.

You can also add virtual machines to the protection group by using Storage vMotion to move their files to one of the datastores in the datastore group. You can remove a virtual machine from an array-based replication protection group by moving the virtual machine's files to another datastore.

You can protect and recover encrypted virtual machines by using array-based replication protection groups. The protection and recovery of encrypted virtual machines with array-based replication requires VMware vSphere 6.7 and later.

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.

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.

vSphere Replication Protection Groups

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

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

You select a target location on a datastore on the remote site when you configure vSphere Replication on a virtual machine. When you include a virtual machine with vSphere Replication in a protection group, Site Recovery Manager creates a placeholder virtual machine for recovery. It is possible for the replication target for vSphere Replication and the placeholder virtual machine that Site Recovery Manager creates to both be on the same datastore on the recovery site

because they are created in different datastore folders. When the replication target and the placeholder virtual machines are in the same datastore, Site Recovery Manager creates the placeholder virtual machine name by using the replication target name with the suffix `(1)`. To avoid confusion, the best practice is to use different datastores for the vSphere Replication replication target and for the Site Recovery Manager placeholder virtual machines. Site Recovery Manager applies the inventory mappings to the placeholder virtual machine on the recovery site.

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

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

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

- Site Recovery Manager monitors the vSphere Replication status of the virtual machines in vSphere Replication protection groups. If replication is not functioning for a virtual machine in a protection group, Site Recovery Manager cannot recover the virtual machine.

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

- If you configured vSphere Replication on a virtual machine that resides on a datastore that Site Recovery Manager already protects with array-based replication, Site Recovery Manager reports an error if you try to include that virtual machine in a vSphere Replication protection group.

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

About Virtual Volumes Protection Groups

You can include virtual machines that you configured for a Virtual Volumes replication in Virtual Volumes protection groups.

When using Virtual Volumes protection groups, Site Recovery Manager checks both the recovery and the protection site and matches the Virtual Volumes configurations that can be used. That includes paired fault domains, direction of replication, and so on. To use Virtual Volumes protection groups, you must have a registered Virtual Volumes datastore at both the protected and the recovery site.

There are certain limitations to Virtual Volumes protection groups.

- Site Recovery Manager does not support protection of virtual machines that have non-replicated virtual disks with Virtual Volumes protection groups.

- Site Recovery Manager does not support the protection of virtual machines with different vVols-based disks, replicated by different storage policies or different Virtual Volumes replication groups.

- Virtual Volumes does not support the recovery of template virtual machines.

For additional information about Virtual Volumes, see Using Virtual Volumes with Site Recovery Manager and Change the Virtual Volumes Replication Settings.

About Storage Policy Protection Groups

Storage policy protection groups enable the automatic protection of virtual machines that are associated with a storage policy.

You use array-based replication to replicate the datastores from the protected site to the recovery site. If you tag a datastore and you create a storage policy that maps to that tag, the datastore is automatically associated with that storage policy. A storage policy protection group that includes that storage policy automatically protects any virtual machines that have been tagged appropriately that reside on the datastore. If you disassociate a virtual machine from the storage policy or move it off the datastore, Site Recovery Manager automatically unprotects it.

When you create a storage policy protection group, Site Recovery Manager performs the following operations:

- Creates a managed object that represents the storage policy protection group on the local Site Recovery Manager Server instance.

- Associates the storage policies that you select with the storage policy protection group. Site Recovery Manager protects all compliant storage policies that you include in the storage policy protection group.

- The local storage policy protection group actively protects the appropriate vSphere entities on the local vCenter Server instance and determines the compliance of the storage policies that it contains. The initial protection of the newly created storage policy protection group includes protecting all the virtual machines that are associated with the storage policies in the protection group, based on the latest known state of the vSphere inventory.

  Note   The initial protection does not include any storage synchronization for the associated consistency groups. You must replicate the storage according to its regular schedule, independently of vSphere and Site Recovery Manager.

- Starts vSphere inventory monitoring to detect any vSphere entities that are added to the inventory after the initial protection. If Site Recovery Manager fails to protect any vSphere entities, the creation of the storage policy protection group does not fail, but errors appear in the protection group properties.

- Creates a peer managed object to represent the storage policy protection group on the Site Recovery Manager Server instance on the recovery site. This object is ready for recovery immediately after creation, even if the underlying storage is not yet ready for recovery.

After you create a storage policy protection group, you might need to synchronize the underlying storage to make sure that the protected vSphere entities are recoverable. Run a test recovery with the option to replicate recent changes as soon as possible after you create the protection group.

Prerequisites for Storage Policy Protection Groups

When you create storage policy protection groups, you must first create storage policies and ensure that your environment meets certain prerequisites.

Prerequisites

- Create datastore tags and assign them to datastores to associate with a storage policy:

  - If your environment does not use Enhanced Linked Mode, create tag categories and tags on both the protected site and the recovery site, and assign them to the datastores to protect on the protected site.

  - If your environment uses Enhanced Linked Mode, create tag categories and tags only on the protected site. The tags are replicated to other vCenter Server instances in Enhanced Linked Mode environments.

- Create virtual machine storage policies in vCenter Server on both sites, that include the tags that you assigned to the datastores to protect. Create virtual machine policies on both sites even if your environment uses Enhanced Linked Mode. The storage policies can have different names on each site.

- Associate virtual machines to protect with the appropriate storage policy on the protected site. You must associate all the virtual machine's disks with the same storage policy.

- Configure array-based replication of the datastores from the protected site to the recovery site by using the replication technology that your array vendor provides.

- Configure inventory mappings in Site Recovery Manager. Storage policy protection groups have specific behavior concerning the application of inventory mappings, and requirements on how to set the resource inventory mappings. For example, if you use storage policy protection groups and you do not configure mappings, planned migration or disaster recovery fail, but Site Recovery Manager finishes successfully your operation with temporary placeholder mappings.

- When Site Recovery Manager Server starts, Site Recovery Manager queries the storage policy-based management and tag manager services in vCenter Server to find virtual machines that are associated with a storage policy. These services and vCenter Server must be running when you start or restart Site Recovery Manager Server. If they are not running, Site Recovery Manager Server does not start.

For information about how to create storage policies, see Virtual Machine Storage Policies in the *VMware vSphere ESXi and vCenter Server 6.7 Documentation*.

For information about how to create inventory mappings, see Configure Inventory Mappings.

For information about storage policy protection groups and inventory mappings, see Inventory Mappings for Storage Policy Protection Groups .

For information about known limitations of storage policy protection groups, see Limitations of Storage Policy Protection Groups.

Limitations of Storage Policy Protection Groups

Storage policy protection groups are subject to limitations.

Protecting Virtual Machine Templates

Datastores that are compliant with protected storage policies should not contain virtual machine templates.

Protecting Virtual Machines with RDM Disks

Datastores that are compliant with protected storage policies should not contain virtual machines with RDM disks.

Protecting Virtual Machines and Licensing Limits

- Virtual machines that are not initially protected due to licensing limits are not protected even after you modify consistency groups and virtual machines to meet the licensing limit.

- Virtual machines that are not initially protected due to licensing limits are not protected even after you install a license for a larger number of virtual machines.

Duplicate Tags in Enhanced Linked Mode Environments

In an environment that uses Enhanced Linked Mode, if a temporary network partition occurs between vCenter Server instances, it is possible to create a tag on one site and to create another tag with the same name on another site. You might then tag one set of datastores on one site with the first tag, and another set of datastores on the other site with the second, identical tag. Because Site Recovery Manager looks up tags by name rather than by ID, when the network partition is removed, the datastores on both sites appear to be tagged with the same tag. If you delete one of the duplicate tags, Site Recovery Manager might remove protection from the consistency groups that reside in the datastore that bore that tag. The virtual machines in those consistency groups lose their protection and the recovery settings for the virtual machines are deleted.

To avoid this situation, resolve tag conflicts before creating storage policy protection groups and configuring virtual machine recovery settings. If you encounter this situation after you have already created storage policy protection groups, shut down the protected site temporarily and resolve the tag conflict.

Changing Array States Between Recovery and Reprotect

After running a recovery plan but before running reprotect, if you change the state of an array device, for example to fix issues with reversal of replication, and you initiate a rescan of the storage devices, Site Recovery Manager can stop unexpectedly. If this occurs, you must recreate the corresponding protection groups and recovery plans.

Associating Nonreplicated Datastores with Storage Policies

It is possible to associate a nonreplicated datastore with a storage policy that you include in a storage policy protection group. However, Site Recovery Manager does not protect the virtual machines that reside on a nonreplicated datastore, even if that datastore is associated with a storage policy that is included in a storage policy protection group. If you run a recovery plan that includes that protection group, any virtual machines that have files on a nonreplicated datastore appear with errors in the protection group and are not recovered.

Datastores Spanning Multiple Consistency Groups

Do not configure datastores to span multiple consistency groups. Site Recovery Manager cannot protect such datastores or virtual machines that use multiple consistency groups and operations can fail.

- If no other datastores backed by the consistency group are part of the storage policy, the protection group might skip the consistency group.

- The protection group might not report problems related to the datastores.

- Virtual machines using datastores that span consistency groups are in a nonprotected state even if the virtual machines use the correct storage policy.

- The datastores that span multiple consistency groups will appear to be nonreplicated and are not protected by the storage policy protection group. Those datastores might disappear when Site Recovery Manager migrates the protection group to the recovery site.

Protecting the Same Consistency Groups in Both Array-Based Replication and Storage Policy Protection Groups

If you tag a replicated datastore and associate it with a storage policy, you can include the storage policy and its associated consistency groups in a storage policy protection group. It is also possible to include a datastore group that contains the tagged datastore in an array-based replication protection group. Therefore, consistency groups can end up being included in both an array-based replication protection group and in a storage policy protection group.

When a storage policy protection group and an array-based replication protection group both attempt to protect the same consistency group, the array-based replication protection group takes the ownership of the consistency group and the virtual machines that it contains. The storage policy protection group marks the consistency group and virtual machines in an error state. In this situation, you must remove the consistency group from one of the protection groups.

- To keep the consistency group in the array-based replication protection group, disassociate the affected virtual machines from the storage policy. Also disassociate the consistency group from the storage policy. This removes them from the storage policy protection group.

- To keep the consistency group in the storage policy protection group, edit the array-based replication protection group to remove the datastore and virtual machines. This automatically resolves the error in the storage policy protection group.

Changing the Protection Status of Consistency Groups and VMs During and After a Recovery

You can change the protection status of the consistency groups and VMs that are part of a storage policy protection group by tagging and untagging the datastores, or associating and disassociating VMs with storage policies. When you change the protection status of the VMs and consistency groups and a planned migration or disaster recovery are not running, Site Recovery Manager updates the protection status of the VMs and consistency groups in the SPPG.

If you change the protection status of the VMs and consistency groups during a planned migration or disaster recovery that uses the storage policy protection group, the Site Recovery Manager user interface might show changes on the protection site, but the recovery workflow cannot be updated properly, and the recovery might fail.

To ensure a successful recovery process, you must not change the protection status of the VMs and consistency groups in an SPPG during a planned migration or disaster recovery of the SPPG. More precisely, the window when protection changes are not supported starts from the first time a recovery plan containing the SPPG enters Recovery In Progress state, until the same plan reaches Recovery Complete state.

You cannot add consistency groups or virtual machines to a storage policy protection group if you have successfully or unsuccessfully run a recovery plan that contains that protection group. Do not add new consistency groups or virtual machines to a storage policy protection group in the Recovered or Partially Recovered states. You can add new consistency groups or virtual machines to an existing storage policy protection group that has never been included in a recovery plan run, or that has only been included in test recoveries.

When you have run a recovery plan that contains a storage policy protection group, you must include any new consistency groups or virtual machines in a new storage policy protection group. Remove new consistency groups or virtual machines from the recovered storage policy protection group before you add them to a new storage policy protection group. Site Recovery Manager only supports the protection of an object in a single protection group.

Requirements for Resource Inventory Mappings

Storage policy protection groups have specific requirements and limitations on how to set the resource inventory mappings. For more information, see Inventory Mappings for Storage Policy Protection Groups .

Storage Policy Protection Groups and Nonprotected Virtual Machines

Your environment, the implementation of your storage policies, and the configuration of the datastores and virtual machines to protect must meet the prerequisites for storage policy protection groups. If they do not meet the prerequisites, Site Recovery Manager might not protect all of the virtual machines in a storage policy protection group.

For the prerequisites that you must satisfy for storage policy protection, see Prerequisites for Storage Policy Protection Groups.

For example, virtual machines that are not associated with a storage policy can reside in a tagged datastore alongside virtual machines that are associated with a storage policy. If you include the storage policy in a storage policy protection group, because these virtual machines are not associated with that storage policy, Site Recovery Manager does not protect them.

Nonprotected virtual machines can appear in storage policy protection groups for reasons other than the non-association of virtual machines with the correct storage policy. For descriptions of other circumstances in which nonprotected virtual machines can appear in storage policy protection groups, see Limitations of Storage Policy Protection Groups.

If a storage policy protection group includes nonprotected virtual machines, these virtual machines appear in the **Related Objects > Virtual Machines** view for the storage policy protection group. The protection group appears in an error state.

How Site Recovery Manager handles nonprotected virtual machines depends on the type of recovery that you run.

Note You can only attempt to protect nonprotected virtual machines in storage policy protection groups on which you have never run recovery. If you have successfully or unsuccessfully run recovery on a storage policy protection group that contains nonprotected virtual machines, you must remove those virtual machines from the storage policy protection group.

- If you run a test recovery on a storage policy protection group that contains nonprotected virtual machines, the operation fails with errors. If a test recovery fails due to nonreplicated virtual machines, run cleanup before you attempt to protect or remove the nonprotected virtual machines, then run the test again. After you have run cleanup, if you have never run a recovery on this protection group, attempt to fix the protection of the affected virtual machines, for example by associating them with the correct storage policy, or by moving virtual machine files from a nonreplicated datastore to a replicated datastore.

- If you run planned migration on a storage policy protection group that contains nonprotected virtual machines, the operation fails and the recovery plan shows the Incomplete Recovery state. During the deactivation step of planned migration, nonprotected virtual machines on the protected site can prevent Site Recovery Manager from making the storage read-only, or virtual machines might lose access to their data. If a protection group is in the Incomplete Recovery state, you must remove the nonprotected virtual machines out of the protected datastore and disassociate them from the storage policy.

- If you run disaster recovery on a storage policy protection group that contains nonprotected virtual machines, the operation succeeds but Site Recovery Manager does not recover the nonprotected virtual machines. When the protected site comes back online and you attempt to run planned migration to complete the recovery, the planned migration fails if nonprotected virtual machines are still present on the protected site. If a protection group is in the Incomplete Recovery state, you must remove the nonprotected virtual machines out of the protected datastore and disassociate them from the storage policy.

Protect an Encrypted VM

You can protect and recover encrypted VMs by using, an array-based replication protection group, a vSphere Replication protection group, or a Storage Policy Protection Group (SPPG).

After you create a storage policy, you must edit the rule set of your storage policy by using the following procedure.

Prerequisites

- If you are using an SPPG, complete the prerequisites in Prerequisites for Storage Policy Protection Groups

- Ensure that the recovery and protected sites use a common Key Management Server (KMS) or that the Key Management Server clusters at both sites use common encryption keys. For information about how to set up a Key Management Server cluster, see the *VMware vSphere ESXi and vCenter Server 6.7* documentation.

Procedure

1 On the **Rule set** page of the **VM Storage Policy** wizard, select **Use rule-sets in the storage policy** and ensure that the Tag based replacement option is selected for the Storage Type.

2 Click **<Add rule>** and click **Tags from category**.

3 In the <Select category>, click your category.

4 Ensure that Tagged with any one of … is selected for Tags from category.

5 Click **Add tags…** and select your tag.

What to do next

1 Create a storage policy mapping and ensure that the storage policy on the recovery site is the same as the policy on the protected site. For information about how to create a storage policy mapping, see Select Storage Policy Mappings.

2 Create an array-based replication protection group, a vSphere Replication protection group, or a storage policy protection group. For information about how to create an array-based replication protection group, see Create Array-Based Replication Protection Groups. For information about how to create a vSphere Replication protection group, see Create vSphere Replication Protection Groups. For information about how to create a storage policy protection group, see Create Storage Policy Protection Groups.

Automatic Protection of Virtual Machines

Site Recovery Manager supports the automatic protection of virtual machines in array-based protection groups, Virtual Volumes protection groups, and storage policy protection groups.

This topic provides information about automatic protection of array-based protection groups and Virtual Volumes protection groups only. Automatic protection mechanism for storage policy protection groups is different. See About Storage Policy Protection Groups.

Array-Based Replication Automatic Protection

When you create a new virtual machine or use vMotion to move a virtual machine on a datastore that is replicated and protected in Site Recovery Manager, the virtual machine is automatically added to and protected in an existing protection group.

Virtual Volumes Automatic Protection

Site Recovery Manager applies automatic protection to new or existing virtual machines for which the SPBM policy is changed to a Virtual Volumes policy for replication and to a replication group protected with Site Recovery Manager.

Note If a protected virtual machine is deleted, Site Recovery Manager does not provide an automatic unprotection. The virtual machine must be explicitly unprotected. If an already protected virtual machine is Storage vMotioned to a datastore protected in a different array-based replication protection group or the Virtual Volumes replication policy is changed to refer it to a different Virtual Volumes protection group, the virtual machine protection is not automatically migrated in the new protection group. The virtual machine must be explicitly unprotected from the previous protection groups first.

Multi-Tenancy Considerations and Configuration

Protecting virtual machines and virtual machine templates is a cross-site operation. During this operation, the Site Recovery Manager servers on both sites perform permission checks for the local user that is logged in. For automatic protection each Site Recovery Manager site uses a pre-configured local vCenter Server account to perform the permission checks with. By default Site Recovery Manager uses its local solution user as automatic protection user. The user can be changed with an advanced setting to another vCenter Server account. This vCenter Server account cannot be a user group or a user with global vCenter Server administrator privileges.

For successful protection, the vCenter Server account that you use for automatic protection must have the following privileges.

- **VcDr.ProtectionProfile.com.vmware.vcDr.Edit** privilege in the permission assigned in the Site Recovery Manager inventory on the protection group where the virtual machine will be added.

- **VirtualMachine.Replication.com.vmware.vcDr.Protect** privilege in the permission assigned on the production virtual machine or the virtual machine template in the vCenter Server inventory.

When assigning permissions to the automatic protection user or the user groups that the automatic protection user is a member of, the administrators can choose **SrmAdministrator** or **SrmProtectionGroupsAdministrator** roles.

For multiple Site Recovery Manager deployments on a single vCenter Server, the administrators must configure different automatic protection accounts per Site Recovery Manager instance and assign appropriate permissions that split the vCenter Server inventory to simulate a multi-tenant environment.

You can modify how Site Recovery Manager handles the automatic protection of virtual machines. See, Change the Automatic Protection Settings. The required privilege to edit those settings is **VcDr.Protection.com.vmware.vcDr.AutoProtection.Edit** part of the **SrmAdministrator** role.

Overview of Protection Group States

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

Table 5-1. Protection Group States

State	Description
Loading	Appears briefly while the interface is loading until the protection group status appears.
OK	Group is idle. All virtual machines are in `OK` state. You can edit the group.
Not Configured	Group is idle. Some virtual machines might not be in `OK` state. You can edit the group.
Testing	Group is used in a plan running a test. You cannot edit the group.
Test Complete	Group is used in a plan running a test. You cannot edit the group. Group returns to the `OK` or `Not Configured` state when cleanup is successful.
Cleaning Up	Group is used in a plan that is cleaning up after a test. You cannot edit the group. Group returns to the `OK` or `Not Configured` state when cleanup is successful. If cleanup fails, the group goes to the `Testing` state.
Recovering	Group is used in a plan that is running a recovery. You cannot edit the group. If recovery succeeds, the group goes to `Recovered` state. If recovery fails, group status changes to `Partially Recovered`.
Partially Recovered	Group is in a plan that completed a recovery, but recovery failed for some virtual machines. You can remove virtual machines, but cannot configure or restore them.
Recovered	Group is in a plan that successfully completed a recovery. You can remove virtual machines, but cannot configure or restore them.
Reprotecting	Group is used in a plan running reprotect. You cannot edit the group. Group returns to `OK` or `Not Configured` state when reprotect is successful. If reprotect fails, the group goes to `Partially Reprotected` state.

Table 5-1. Protection Group States (continued)

State	Description
Partially Reprotected	The group is in a plan that failed a reprotect. You can remove virtual machines, but cannot configure or restore them.
Configuring Protection	Protection operations are in progress on virtual machines in the group.
Removing Protection	Removing protection from virtual machines in the group is in progress.
Restoring Placeholders	Creation of placeholders is in progress for virtual machines in the group.
Operations in Progress	A combination of at least one **Configure Protection** and one **Remove Protection** operations are in progress in the group.

Overview of Virtual Machine Protection States

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

Table 5-2. Virtual Machine Protection States

State	Description
Placeholder VM Not Found	You deleted the placeholder virtual machine. The **Restore Placeholder** icon is enabled.
Original protected VM not found	You deleted the original production virtual machine after failover and before reprotect. The **Restore Placeholder** icon is enabled.
Datastore *name* used by VM is missing from group	The virtual machine requires a datastore that is not in the protection group. Edit the protection group to include the datastore.
Datastore *name* used by VM is protected in a different group	The virtual machine requires a datastore that is in a different protection group. Remove the datastore from the other protection group and edit the current protection group to include the datastore. You cannot include a datastore in two protection groups.
Device not found: *device name*	You added an unreplicated disk or device to a protected virtual machine. You must edit the replication of the virtual machine to either include or remove the device from protection.
Mapping missing: Folder *name*; Network *name* ; Resource pool *name*	Folder, resource pool, or network mappings are not configured for this VM. Fix the inventory mappings for the site or manually configure the virtual machine.

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

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

Creating Protection Groups

You create protection groups so that Site Recovery Manager can protect virtual machines.

When you create protection groups, wait until 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.

You can organize the protection groups in folders.

Note The name of the protection group must be different than the name of the selected folder.

Create vSphere Replication Protection Groups

Create vSphere Replication protection groups to protect virtual machines for which you configured vSphere Replication.

Prerequisites

Verify that you configured vSphere Replication on virtual machines.

Procedure

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

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

3 Click the **Protection Groups** tab, and click **New** to create a protection group.

4 On the **Name and direction** page, enter a name and description for the protection group, select a direction, and click **Next**.

5 On the **Protection group type** pane, select **Individual VMs (vSphere Replication)**, and click **Next**.

6 Select virtual machines from the list to add to the protection group 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.

7 On the **Recovery plan** page, you can optionally add the protection group to a recovery plan.

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

8 Review your settings and click **Finish**.

Results

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

- If Site Recovery Manager successfully applied inventory mappings to the protected virtual machines, the protection status of the protection group is OK.

- If you did not configure inventory mappings, or if Site Recovery Manager was unable to apply them, the protection status of the protection group is Not Configured.

What to do next

If the protection status of the protection group is Not Configured, apply inventory mappings to the virtual machines:

- To apply site-wide inventory mappings, or to check whether inventory mappings that you have already set are valid, see Configure Inventory Mappings. To apply these mappings to all the virtual machines, see Apply Inventory Mappings to All Members of an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

- To apply inventory mappings to each virtual machine in the protection group individually, see Configure Inventory Mappings for an Individual Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

Create Storage Policy Protection Groups

Create storage policy protection groups to protect virtual machines that are associated with a storage policy.

Prerequisites

Verify that you satisfied the requirements in Prerequisites for Storage Policy Protection Groups and reviewed the Limitations of Storage Policy Protection Groups .

Procedure

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

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

3   Click the **Protection Groups** tab, and click **New** to create a protection group.

4   On the **Name and direction** page, enter a name and description for the protection group, select a direction, and click **Next**.

5   On the **Protection group type** page, select the **Storage Policies (array-based replication)**, and click **Next**.

6   Select storage policies to add to the protection group and click **Next**.

7   On the **Recovery plan** page, you can optionally add the protection group to a recovery plan.

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

8   Review your settings and click **Finish**.

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

- If Site Recovery Manager successfully protected all the virtual machines associated with the storage policy, the protection status of the protection group is `OK`.

- If Site Recovery Manager cannot protect all the virtual machines associated with the storage policy, the protection status of the protection group is `Not Configured`.

What to do next

If the protection status of the protection group is `Not Configured`, verify that you satisfied the prerequisites in Prerequisites for Storage Policy Protection Groups, review Limitations of Storage Policy Protection Groups, modify the storage policy implementation accordingly, and attempt to recreate the protection group.

Create Array-Based Replication Protection Groups

Create array-based replication protection groups to protect virtual machines for which you configured array-based replication.

Prerequisites

- Verify that you have included virtual machines in datastores for which you configured array-based replication.

- Verify that you have configured the resource pool mappings for the replicated datastores.

Procedure

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

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

3   Click the **Protection Groups** tab, and click **New** to create a protection group.

4   On the **Name and direction** page, enter a name and description for the protection group, select a direction, and click **Next**.

5   On the **Protection group type** pane, select **Datastore groups (array-based replication)**, select an array pair, and click **Next**.

6   Select datastore groups to add to the protection group and click **Next**.

When you select a datastore group, the virtual machines that the group contains appear in the **Virtual machines** table.

7 On the **Recovery plan** page, you can optionally add the protection group to a recovery plan.

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

8 Review your settings and click **Finish**.

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

- If Site Recovery Manager successfully applied inventory mappings to the protected virtual machines, the protection status of the protection group is `OK`.

- If you did not configure inventory mappings, or if Site Recovery Manager was unable to apply them, the protection status of the protection group is `Not Configured`.

What to do next

If the protection status of the protection group is Not Configured, apply inventory mappings to the virtual machines:

- To apply site-wide inventory mappings, or to check whether inventory mappings that you have already set are valid, see Configure Inventory Mappings. To apply these mappings to all the virtual machines, see Apply Inventory Mappings to All Members of an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

- To apply inventory mappings to each virtual machine in the protection group individually, see Configure Inventory Mappings for an Individual Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

Create Virtual Volumes Protection Groups

Create Virtual Volumes protection groups to protect virtual machines for which you configured Virtual Volumes replication.

Prerequisites

Verify that you have included virtual machines in datastores for which you configured Virtual Volumes replication.

Procedure

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

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

3 Click the **Protection Groups** tab, and click **New** to create a protection group.

4 On the **Name and direction** page, enter a name and description for the protection group, select a direction, and click **Next**.

5 On the **Protection group type** pane, select **Virtual Volumes (vVol replication)**, select a specific fault domain, and click **Next**.

A fault domain can contain more than one Storage Container. When you select a fault domain, Site Recovery Manager enumerates all storage containers in the fault domain. For each storage container, Site Recovery Manager collects all the replication groups and VMs. Only one fault domain is associated to a particular Site Recovery Manager protection group. You cannot have replication groups from different fault domains in one protection group, but you can have replication groups from multiple storage containers part of one fault domain in one protection group. For example, if Fault Domain A to Fault Domain B has a replication group 1 with 1 VM called Test_AB and Fault Domain A to Fault Domain C has a replication group 2 with 1 VM called Test_AC, you can create a protection group containing both replication groups.

6 Select replication groups to add to the protection group and click **Next**.

You can expand each replication group row to see the virtual machines that the group contains.

Virtual machines that have replication errors are listed separately. You can see them by enabling **Show virtual machines which cannot be protected**.

Note Virtual Volumes does not support the recovery of template virtual machines.

7 On the **Recovery plan** page, you can optionally add the protection group to a recovery plan.

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

8 Review your settings and click **Finish**.

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

■ If Site Recovery Manager successfully applied inventory mappings to the protected virtual machines, the protection status of the protection group is OK.

■ If you did not configure inventory mappings, or if Site Recovery Manager was unable to apply them, the protection status of the protection group is Not Configured.

What to do next

If the protection status of the protection group is Not Configured, apply inventory mappings to the virtual machines:

- To apply site-wide inventory mappings, or to check whether inventory mappings that you have already set are valid, see Configure Inventory Mappings. To apply these mappings to all the virtual machines, see Apply Inventory Mappings to All Members of an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

- To apply inventory mappings to each virtual machine in the protection group individually, see Configure Inventory Mappings for an Individual Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

Organize Protection Groups in Folders

You can create folders in which to organize protection groups.

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

Procedure

1   On the **Site Recovery** home tab, select a site pair, and click **View Details**.

2   Click the **Protection Groups** tab, and in the left pane right-click **Protection Groups**, and click **New Folder**.

3   Enter a name for new folder, and click **Add**.

4   Add new or existing protection groups to the folder.

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

Add and Remove Datastore Groups or Virtual Machines to or from a Protection Group

You can add and remove datastore groups to and from an array-based replication protection group, or add and remove virtual machines to and from a vSphere Replication protection group.

You can also change the name and description of an array-based replication, Virtual Volumes replication, or vSphere Replication protection group.

Note You cannot edit storage policy protection groups after their initial creation. You add virtual machines to or remove virtual machines from an existing storage policy protection group by modifying the storage policy associations of virtual machines in protected datastores. You can only add or remove virtual machines in a storage policy protection group if recovery has never been run on that protection group. For more information, see Limitations of Storage Policy Protection Groups.

Prerequisites

You created an array-based replication protection group, Virtual Volumes replication protection group, or a vSphere Replication protection group.

Procedure

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

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

3   Click the **Protection Groups** tab, right-click a protection group, and click **Edit**.

4   (Optional) Change the name or description of the protection group and click **Next**.

5   Click **Next**.

6   Modify the datastore groups or virtual machines that the protection group contains.

   ■   For array-based protection groups, select or deselect datastore groups to add them to or remove them from the protection group, and click **Next**.

   ■   For vSphere Replication protection groups, select or deselect virtual machines to add them to or remove them from the protection group, and click **Next**.

   ■   For Virtual Volumes protection groups, select or deselect replication groups to add them to or remove them from the protection group, and click **Next**

7   Review the settings and click **Next** to apply the changes.

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

8   Click **Finish**.

Results

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

Note When you add datastores or virtual machines to a protection group, inventory mappings only apply to the new virtual machines. For example, if you change inventory mappings, then add a datastore to a protection group that is in the `OK` state, Site Recovery Manager applies the new mappings to the newly protected virtual machines that reside in the new datastore. The previously protected virtual machines continue to use the old mappings.

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

What to do next

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

- To apply site-wide inventory mappings, or to check that inventory mappings that you have already set are valid, see Configure Inventory Mappings. To apply these mappings to all virtual machines, see Apply Inventory Mappings to All Members of an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

- To apply inventory mappings to each virtual machine in the protection group individually, see Configure Inventory Mappings for an Individual Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

Apply Inventory Mappings to All Members of an Array-Based, Virtual Volumes, or vSphere Replication Protection Group

If the protection status of an array-based, Virtual Volumes, or vSphere Replication protection group is `Not Configured`, you can configure protection for all the unconfigured virtual machines by using existing site-wide inventory mappings.

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

- You did not configure site-wide inventory mappings before you created the protection group.

- You did not configure placeholder datastore mappings before you created the protection group.

- You added virtual machines to a protection group after you created it.

- Virtual machines lost their protection, possibly because you reconfigured them after you added them to a protection group. For example, you added or removed virtual disks or devices.

Prerequisites

■ Configure or reconfigure site-wide inventory mappings. To select inventory mappings, see Configure Inventory Mappings.

■ Configure or reconfigure placeholder datastore mappings. To configure a placeholder datastore, see Select a Placeholder Datastore.

Procedure

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

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

3 Click the **Protection Groups** tab, click a protection group, and on the right pane, click the **Virtual Machines** tab.

4 Click the **Configure All VMs** button.

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

5 Click **Yes** to confirm that you want to apply inventory mappings to all unconfigured virtual machines.

6 Monitor the status of the virtual machines. If Site Recovery Manager was unable to apply some or all inventory mappings, or if it was unable to create placeholders for virtual machines, you can perform remedial actions.

Status	Action
OK	No action required
Not Configured or Mapping Missing	Check the inventory mappings and click **Configure All VMs** again
Placeholder VM creation error	Check the placeholder datastore mapping and try to recreate the placeholder virtual machines. ■ To recreate the placeholder for an individual virtual machine, right-click a virtual machine and select **Recreate Placeholder**. ■ To recreate the placeholder for several virtual machines, right-click the protection group and select **Restore Placeholder VMs**.

Configure Inventory Mappings for an Individual Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group

You can configure the mappings for the virtual machines in an array-based, Virtual Volumes, or vSphere Replication protection group individually. This way, you can use different resources on the recovery site for different virtual machines.

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

You cannot specify placeholder datastores for individual virtual machines. You must map datastores on the protected site to placeholder datastores on the recovery site at the site level. To configure a placeholder datastore, see Select a Placeholder Datastore.

Prerequisites

You created an array-based, Virtual Volumes, or vSphere Replication protection group.

Procedure

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

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

3   Click the **Protection Groups** tab, and click the protection group that includes the virtual machine to configure.

4   In the right pane, click the **Virtual Machines** tab.

5   Right-click the virtual machine and click **Configure Protection**.

6   Configure inventory mappings by expanding the resources, selecting the **Override site mappings** check box, and selecting resources on the recovery site. Click **OK**.

    You can only change the folder, resource pool, and network mappings.

7   Monitor the status of the virtual machines. If Site Recovery Manager was unable to apply some or all the inventory mappings, or if it was unable to create placeholders for virtual machines, you can perform remedial actions.

Status	Action
OK	No action required
Not Configured or Mapping Missing	Click **Configure Protection** again and check the inventory mappings.
Placeholder VM creation error	Check the placeholder datastore mapping at the site level, right-click the virtual machine, and click **Recreate Placeholder**.

Modifying the Settings of a Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group

Modifying the settings of a protected virtual machine, and adding or changing storage devices, such as hard disks or DVD drives, can affect the protection of that virtual machine.

Note   You cannot modify the settings of a virtual machine that you protect in a storage policy protection group.

If you use array-based replication or Virtual Volumes replication, adding or changing devices on a protected virtual machine affects protection depending on how you create the new device.

- If the new device is on a replicated datastore that is not part of a protection group, the protection group that contains the virtual machine goes into the `Not Configured` state. Reconfigure the protection group to add the datastore that contains the new device to the protection group.

- If the new device is on a replicated datastore that a different protection group protects, the protection of the virtual machine is invalid.

- If the new device is on an unreplicated datastore, you must replicate the datastore or remove protection from the device.

- If you use Storage vMotion to move a virtual machine to an unreplicated datastore, or to a replicated datastore on an array for which Site Recovery Manager does not have a storage replication adapter (SRA), the protection of the virtual machine is invalid. You can use Storage vMotion to move a virtual machine to a datastore that is part of another protection group.

If you add a device to a virtual machine that you protect by using vSphere Replication, you must reconfigure vSphere Replication on the virtual machine to select the replication options for the new device. For information about reconfiguring vSphere Replication settings, see the vSphere Replication documentation at https://docs.vmware.com/en/vSphere-Replication/index.html.

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

Removing Protection from a Virtual Machine

You might want to remove protection from a virtual machine for different reasons. Removing protection from a virtual machine affects protection groups differently.

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

Note You cannot temporarily remove protection from virtual machines in storage policy protection groups.

In array-based replication and Virtual Volumes replication, a distinction exists between the Site Recovery Manager protection of a virtual machine and the Site Recovery Manager storage management for that virtual machine. If you remove protection from a virtual machine in an array-based replication or Virtual Volumes replication protection group, Site Recovery Manager no longer recovers the virtual machine, but it continues to monitor and manage the storage of the virtual machine files.

You might remove protection from a virtual machine for different reasons:

- You use vSphere Replication and you want to exclude a protected virtual machine from a protection group.

- You use array-based replication or Virtual Volumes replication, and someone moves a virtual machine that you do not want to protect to a replicated datastore. If you remove protection from the virtual machine, the protection group shows the `Not Configured` state. Test recovery and planned migration fail for the whole group. Disaster recovery succeeds, but only for the protected virtual machines in the group, and certain operations on the protected site are skipped. The recovery plan enters the `Recovery required` state. In this case, move the virtual machine off the protected datastore.

- You use array-based replication and a virtual machine has devices that are stored on an unreplicated datastore. You can remove protection from the virtual machine so that disaster recovery succeeds for all the other virtual machines in the group while you relocate the device files.

Removing protection from a virtual machine affects protection groups differently, according to whether you use array-based replication, Virtual Volumes replication, or vSphere Replication.

- If you remove protection from a virtual machine that is part of an array-based replication protection group, 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 datastore that Site Recovery Manager has included in a datastore group, test recovery and planned migration fail for the entire datastore group. Disaster recovery succeeds, but only for the protected virtual machines in the datastore group, and you must move the unprotected virtual machine before you can run planned migration to finish the recovery.

- If a Virtual Volumes replication policy is changed to refer it to a different Virtual Volumes protection group, the virtual machine protection is not automatically migrated in the new protection group. The virtual machine must be explicitly unprotected from the previous protection groups first.

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

Remove Protection from a Virtual Machine

You can temporarily remove protection from a replicated virtual machine in an array-based replication, Virtual Volumes replication, or vSphere Replication protection group without removing it from its protection group.

Note You cannot temporarily remove protection from virtual machines in storage policy protection groups.

Procedure

1 On the **Site Recovery** home tab, select a site pair, and click **View Details**.

2 Click the **Protection Groups** tab, select a protection group, and on the right pane, click the **Virtual Machines** tab.

3 Right-click a virtual machine and click **Remove Protection**.

4 Click **Yes** to confirm the removal of protection from the virtual machine.

Creating, Testing, and Running Recovery Plans

<div style="text-align:right">6</div>

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

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

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

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

- 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.

- 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. If the protected site suffers an unforeseen event that might result in data loss, you can also run a recovery plan under unplanned circumstances.

- 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.

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

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

- **Create, Test, and Run a Recovery Plan**

  You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

- **Disable the Recovery of a Virtual Machine in a Storage Policy Protection Group**

  You can disable the recovery of a virtual machine in a storage policy protection group without removing it from the protection group.

- **Disable the Recovery of a Consistency Group in a Storage Policy Protection Group**

  You can disable the recovery of a consistency group in a storage policy protection group without removing it from the protection group.

- **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 a Recovery Plan History Report**

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

- **Delete a Recovery Plan**

  If you do not need a recovery plan, you can delete it.

- **Overview of Recovery Plan States**

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

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 and for actual recoveries. With this exception, running a test recovery does not disrupt replication or ongoing activities at either site.

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

If you use array-based replication, when you test a recovery plan, the virtual machines on the protected site are still replicated to the replica virtual machines' disk files on the recovery site. During a test recovery, the array creates a snapshot of the volumes hosting the virtual machines' disk files on the recovery site. Array replication continues normally while the test is in progress. When you perform cleanup after running a test, the array removes the snapshots that were created earlier as part of the test recovery workflow.

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

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

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

Test Networks and Data Center Networks

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

The isolated test network is managed by its own virtual switch, and in most cases recovered virtual machines can use the network without having to change network properties such as IP address, gateway, and so on. An isolated test network does not span hosts. You must configure a test network for every network that a recovery plan uses during recovery.

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

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

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

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

Note When you run a recovery plan to perform planned migration and disaster recovery, 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.

Planned Migration

During a planned migration, Site Recovery Manager synchronizes the virtual machine data on the recovery site with the virtual machines on the protected site.

Site Recovery Manager attempts to shut down the protected virtual machines gracefully and performs a final synchronization to prevent data loss, then powers on the virtual machines on the recovery site.

If errors occur during a planned migration, the plan stops so that you can resolve the errors and rerun the plan. You can reprotect the virtual machines after the recovery.

Disaster Recovery

During a disaster recovery, Site Recovery Manager first attempts a storage synchronization. If it succeeds, Site Recovery Manager uses the synchronized storage state to recover virtual machines on the recovery site to their most recent available state, according to the recovery point objective (RPO) that you set when you configure replication.

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 powers on the copies at the recovery site.

In case the protected site comes back online after disaster recovery, the recovery plan goes into an inconsistent state, where production virtual machines are running on both sites, known as a split-brain scenario. Site Recovery Manager detects this state and you can run the plan again to power off the virtual machines on the protected site. Then the recovery plan goes back to a consistent state and you can run reprotect.

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.

Use of VMware Tools

Site Recovery Manager uses VMware Tools heartbeat to discover when a virtual machine is running on the recovery site. In this way, Site Recovery Manager can ensure that all virtual machines are running on the recovery site. VMware Tools are also used to shut down the guest operating system of protected virtual machines gracefully. For this reason, it is a best practice to install 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.

Running a Recovery with Forced Recovery

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

When to Use Forced Recovery

You can use forced recovery in cases where infrastructure fails at the protected site and, as a result, protected virtual machines are unmanageable and cannot be shut down, powered off, or unregistered. In such a case, the system state cannot be changed for extended periods.

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 can finish more quickly.

Forced Recovery with vSphere Replication

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

Forced Recovery with Array-Based Replication

Running disaster recovery with array-based replication when the storage array of the protected site is offline or unavailable can affect the mirroring between the protected and the recovery storage arrays.

After you run forced recovery, you must check whether 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 while the protected site storage is still available, 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 finishes 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.

Enabling Forced Recovery

To select forced recovery when running disaster recovery, you must enable the option `recovery.forceRecovery` in Advanced Settings on the Site Recovery Manager Server on the recovery site. For more information, see Change Recovery Settings.

In the **Run Recovery Plan** wizard, you can only select the forced recovery option in disaster recovery mode. This option is not available for planned migration.

Planned Migration after Forced Recovery

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

Differences Between Testing and Running a Recovery Plan

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

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

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

Area of Difference	Test a Recovery Plan	Run a Recovery Plan
Required privileges	Requires **Site Recovery Manager.Recovery Plans.Test** permission.	Requires **Site Recovery Manager.Recovery Plans.Recovery** permission.
Effect on virtual machines at the protected site	None	Site Recovery Manager shuts down virtual machines in reverse priority order and restores any virtual machines that are suspended at the protected site.

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

Area of Difference	Test a Recovery Plan	Run a Recovery Plan
Effect on virtual machines at the recovery site	If the recovery plan requires it, Site Recovery Manager suspends local virtual machines. Site Recovery Manager restarts suspended virtual machines after cleaning up the test.	If the recovery plan requires it, Site Recovery Manager suspends local virtual machines.
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 protected site errors.
Network	If you explicitly assign test networks, Site Recovery Manager connects recovered virtual machines to a test network. If the virtual machine network assignment is **Isolated network (auto created)** and there are no site-level mappings, Site Recovery Manager assigns virtual machines to temporary networks that are not connected to any physical network.	Site Recovery Manager connects recovered virtual machines to the user-specified data center network.
Interruption of recovery plan	You can cancel a test at any time.	You can cancel the recovery at any time.

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

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

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

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

- Create DVS switches that are connected to an isolated VLAN that is private. Such a VLAN allows hosts and virtual machines to be connected, but to be isolated from production virtual machines. Use a naming convention that clearly designates that the DVS is for testing use, and select this DVS in the recovery plan test network column in the recovery plan editor.

- Create test VLANs on a physical network, providing no route back to the protected site. Trunk test VLANs to recovery site vSphere clusters and create virtual switches for test VLAN IDs. Use a clear naming convention to identify that these switches are for testing. Select these switches from the test recovery network column in the recovery plan editor.

Create, Test, and Run a Recovery Plan

You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

Procedure

1 Create a Recovery Plan

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

2 Organize Recovery Plans in Folders

   To control the access of different users or groups to recovery plans, you can organize your recovery plans in folders.

3 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.

4 Test a Recovery Plan

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

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. You must finish the cleanup operation before you can run a failover or another test.

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 configure Site Recovery Manager to recover a number of point-in-time (PIT) snapshots of a virtual machine when you run a recovery plan.

8 Cancel a Test or Recovery

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

Create a Recovery Plan

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

Procedure

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

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

3 Click the **Recovery Plans** tab, and click **New** to create a recovery plan.

4 Enter a name, description, and direction for the plan, select a folder, and click **Next**.

Note The name of the recovery plan must be different than the name of the selected folder.

5 Select the group type from the menu.

Option	Action
Protection groups for individual VMs or datastore groups	Select this option to create a recovery plan that contains array-based replication and vSphere Replication protection groups.
Storage policy protection groups	Select this option to create a recovery plan that contains storage policy protection groups. If you are using stretched storage, select this option.

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

7 From the **Test Network** drop-down menu, select a network to use during test recovery, and click **Next**.

If there are no site-level mappings, the default option **Use site-level mapping** creates an isolated test network.

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

Organize Recovery Plans in Folders

To control the access of different users or groups to recovery plans, you can organize your recovery plans in folders.

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

Procedure

1   On the **Site Recovery** home tab, select a site pair, and click **View Details**.

2   Click the **Recovery Plans** tab, and in the left pane right-click **Recovery Plans** and click **New Folder**.

3   Enter a name for the folder to create, and click **Add**.

4   Add new or existing recovery plans to the folder.

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

Edit a Recovery Plan

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

Procedure

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

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

3   Click the **Recovery Plans** tab, right-click a recovery plan, and click **Edit**.

4   (Optional) Change the name or description of the plan, and click **Next**.

    You cannot change the direction and the location of the recovery plan.

5   (Optional) Select or deselect one or more protection groups to add them to or remove them from the plan, and click **Next**.

6   (Optional) From the drop-down menu select a different test network on the recovery site, and click **Next**.

7   Review the summary information and click **Finish** to make the specified changes to the recovery plan.

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

Test a Recovery Plan

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

Testing a recovery plan runs all the steps in the plan, except for powering down virtual machines at the protected site and forcing devices at the recovery site to assume control 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 the disk files of the virtual machines in the recovery plan. The creation of the snapshots adds to the I/O latency on the storage. If you notice slower response times when you test recovery plans and you are using VMware Virtual SAN storage, monitor the I/O latency by using the monitoring tool in the Virtual SAN interface.

Procedure

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

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

3   Click the **Recovery Plans** tab, right-click a recovery plan, and click **Test**.

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

4   (Optional) Select **Replicate recent changes to recovery site**.

    Selecting this check box ensures that the recovery site has the latest copy of protected virtual machines, but means that the synchronization might take more time.

5   Click **Next**.

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

7   Click the **Recovery Steps** tab in the recovery plan tab to monitor the progress of the test and respond to messages.

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

What to do next

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

Clean up After Testing a Recovery Plan

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

Site Recovery Manager performs several cleanup operations after a test.

- Powers off the recovered virtual machines.

- Replaces recovered virtual machines with placeholders, preserving their identity and configuration information.

- Cleans up replicated storage snapshots that the recovered virtual machines used during the test.

Prerequisites

Verify that you tested a recovery plan.

Procedure

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

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

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

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

4   Review the cleanup information and click **Next**.

5   Click **Finish**.

6   (Optional) If the cleanup finishes with errors, select the **Force Cleanup** check box to ignore errors during the cleanup operation, and run the cleanup again. If necessary, run cleanup several times, until it finishes without errors.

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 stops replication. Do not run any recovery plan that you have not tested. Reversing these changes might cost significant time and effort and can result in prolonged service downtime.

Prerequisites

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

Site Recovery Manager Administration

- Ensure that you have configured full inventory mappings. If you have only configured temporary placeholder inventory mappings and you run a planned migration with the **Enable vMotion of eligible VMs** option, planned migration fails, even though both sites are running.

- To use the **Enable vMotion of eligible VMs** option with planned migration, enable vMotion on the virtual machines. For instructions about enabling vMotion on virtual machines, see Enable vSphere vMotion for Planned Migration.

Procedure

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

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

3 Click the **Recovery Plans** tab, right-click a recovery plan, and click **Run**.

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

5 Select the type of recovery to run.

Option	Description
Planned Migration	Recovers virtual machines to the recovery site when both sites are running. If errors occur on the protected site during a planned migration, the planned migration operation fails. If your array supports stretched storage, select the **Enable vMotion of eligible VMs** check box.
Disaster Recovery	Recovers virtual machines to the recovery site if the protected site experiences a problem. If errors occur on the protected site during a disaster recovery, the disaster recovery continues and does not fail.

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

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

7 Click **Next**.

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

9 To monitor the progress of the individual steps, click the recovery plan and click the **Recovery Steps** tab.

Results

The **Recent Tasks** panel reports the progress of the overall plan.

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

With vSphere Replication, 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.

Prerequisites

1   Configure Site Recovery Manager to retain older PIT snapshots by setting the value of the **vrReplication.preserveMpitImagesAsSnapshots** option in **Advanced Settings** to `true`. For more information, see Change vSphere Replication Settings and Replicating a Virtual Machine and Enabling Multiple Point in Time Instances.

2   Configure replication of the virtual machine with vSphere Replication.

3   Add the virtual machine to a vSphere Replication protection group and include the protection group in a recovery plan.

Procedure

1   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.

2   In the **VMs and Templates** view, right-click the recovered virtual machine and select **Snapshots > Manage Snapshots**.

3   Select one of the PIT snapshots of this virtual machine and click **Revert To**.

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

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

Cancel a Test or Recovery

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

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

■   Processes that cannot be stopped, such as powering on or waiting for a heartbeat, run to completion before the cancellation finishes.

■   Processes that add or remove storage devices are undone by cleanup operations.

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

Procedure

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

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

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

What to do next

Run a cleanup after canceling a test.

Disable the Recovery of a Virtual Machine in a Storage Policy Protection Group

You can disable the recovery of a virtual machine in a storage policy protection group without removing it from the protection group.

If you run a recovery plan that cannot finish without errors, you can disable the recovery of the virtual machine or virtual machines causing the errors. You must repeat the procedure for each individual virtual machine.

Prerequisites

To use the Disable Recovery functionality, the storage policy protection group must be in partially recovered state.

Procedure

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

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

3   Click the **Protection Groups** tab, click a storage policy protection group, and click the **Virtual Machines** tab.

4   Select a virtual machine and click the **Disable Recovery** button.

5   Click **Yes** to confirm.

Results

Next time you run the recovery plan, the virtual machine is skipped for recovery.

What to do next

Run the recovery plan again.

Disable the Recovery of a Consistency Group in a Storage Policy Protection Group

You can disable the recovery of a consistency group in a storage policy protection group without removing it from the protection group.

If a consistency group is causing errors when you run a recovery plan of an SPPG, you can disable the recovery of the consistency group. You must repeat the procedure for each individual consistency group.

Prerequisites

To use the Disable Recovery functionality, the storage policy protection group must be in partially recovered state, and one of the following conditions must be met:

- The consistency group does not appear on the recovery site.

- The consistency group appears on the recovery site but is empty.

- The consistency group appears on the recovery site but all virtual machines in the group have errors.

Procedure

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

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

3   Select the **Protection Groups** tab, click a storage policy protection group, and select the **Consistency Groups** tab.

4   Select a consistency group and click the **Disable Recovery** button.

5   Click **Yes** to confirm.

Results

Next time you run the recovery plan, the consistency group is skipped for recovery.

What to do next

Run the recovery plan again. See 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.

Prerequisites

Verify that no test recovery or real recovery is in progress.

Procedure

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

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

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

4 (Required) Click the **Recovery Steps** tab and from the **View** drop-down menu select the recovery steps mode.

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

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

5 Click the **Export Steps** icon.

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

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

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

View and Export a Recovery Plan History Report

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

Recovery plan history reports 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 can export a history report at any time, but history reports always contain entries only for completed operations. If an operation is in progress, the history report appears after the operation finishes.

Site Recovery Manager preserves history for deleted recovery plans. You can export history reports for existing and deleted plans.

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

Prerequisites

You ran or tested a recovery plan, or performed a cleanup after a test.

Procedure

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

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

3 On the **Site Pair** tab, click **Recovery Plans History**.

4 (Optional) To export the entire recovery plans history list for a specific time period, click **Export all**.

5 (Optional) Select an item from the recovery plans history list, and click **Export report** for the recovery plan history for a specific time period, recovery plan run, test, cleanup, or reprotect operation.

6 Select a format for the generated file, and click **Download** or **Open in a new tab**.

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

Delete a Recovery Plan

If you do not need a recovery plan, you can delete it.

Prerequisites

Verify that the recovery plan is in a consistent state.

Procedure

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

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

3 Click the **Recovery Plans** tab, right-click the recovery plan to delete, and click **Delete**.

Overview of Recovery Plan States

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

Table 6-2. Recovery States

State	Description
Ready	Recovery steps are cleared.
	For storage policy protection groups, recovery steps do not show virtual machines and consistency groups when a recovery plan is in this state.
	You can verify protected virtual machines in a recovery plan in the **Virtual Machines** tab.
Test in progress	Canceling a test moves plan to Cancel in progress state.
Test complete	Test completed with or without errors. If a failure occurs during the test, plan goes to Test Interrupted state.
Test interrupted	Server failed while a test was running.
Cleanup in progress	After successful cleanup, plan state goes to Ready.
	If cleanup is incomplete, state goes to Cleanup Incomplete.
	If you set the **Force Cleanup** option, state goes to Ready after an error.
	If a failure occurs during cleanup, state goes to Cleanup Incomplete.

Table 6-2. Recovery States (continued)

State	Description
Cleanup incomplete	Errors occurred during cleanup.
	You can run the cleanup again.
	When running cleanup from this state, the cleanup wizard provides an option to ignore errors.
Cleanup interrupted	Site Recovery Manager failed during cleanup.
	You cannot change recovery options.
Recovery in progress	If you cancel recovery, the state goes to Cancel in progress.
Disaster recovery complete	During recovery at the protected site, VM shutdown encountered errors, possibly because the sites were not connected, the step before split brain.
	System prompt warns of split brain and to run recovery again when sites reconnect.
	When sites are connected, state goes to Recovery required (split brain).
Recovery started	A recovery started on the peer site, but if the sites are not connected, the exact state is unknown.
	Log in to the recovery site or reconnect the sites to get the current state.
Recovery required (split brain)	Sites were disconnected during recovery. Split-brain scenario detected when sites reconnect.
	System prompts you to run recovery again to synchronize the sites.
	For storage policy protection groups, recovery steps do not show virtual machines and consistency groups when a recovery plan is in this state.
	You can verify protected virtual machines in a recovery plan in the **Virtual Machines** tab.
Recovery complete	If errors, VMs are all recovered but with errors. Running recovery again does not fix the errors.
	Plan goes to this state after the split brain recovery is resolved.
	You can see the recover steps of the last recovery run.
	For storage policy protection groups, recovery steps do not show virtual machines and consistency groups when a recovery plan is in this state.
	You can verify protected virtual machines in a recovery plan in the **Virtual Machines** tab.
	Sites were disconnected during recovery. The connection status is the only property that triggers this state.
Incomplete recovery	Canceled recovery or datastore error. Run recovery again.
	You must either resolve errors and rerun recovery, or remove protection for VMs in error. The plan detects the resolution of errors in either of these ways and updates state to Recovery complete.

Table 6-2. Recovery States (continued)

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

Table 6-2. Recovery States (continued)

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

Configuring a Recovery Plan

7

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

A simple recovery plan that specifies only a test network to which the recovered virtual machines connect and timeout values for waiting for virtual machines to power on and be customized can provide an effective way to test a Site Recovery Manager configuration.

Most recovery plans require configuration for use in production. For example, a recovery plan for an emergency at the protected site might be different from a recovery plan for the planned migration of services from one site to another.

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

When a recovery plan is running, its state reflects the state of the recovery plan run, rather than the state of the protection groups that it contains.

Recovery Plan Steps

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

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

- Some steps run during all recoveries.

- Some steps run only during test recoveries.

- Some steps are always skipped during test recoveries.

- Some steps run only with stretched storage.

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, Site Recovery Manager performs the following operations:

1 Site Recovery Manager powers off virtual machines according to the priority that you set, with high-priority virtual machines powering off last. Site Recovery Manager skips this step when you test a recovery plan.

2 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 the virtual machines in the next-higher priority group must recover or fail to recover.

During recovery, dependencies between virtual machines within different priority groups are ignored. If dependencies exist between virtual machines in the same priority group, Site Recovery Manager first powers on the virtual machines on which other virtual machines depend.

If Site Recovery Manager can meet the virtual machine dependencies, Site Recovery Manager attempts to power on as many virtual machines in parallel as vCenter Server supports.

Recovery Plan Timeouts and Pauses

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

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

Recovery Steps for Stretched Storage

The recovery plan wizard provides an option to use cross vSphere vMotion to perform failover for all protected, powered-on virtual machines residing on stretched storage at the protected site. When this option is selected, two additional steps occur during recovery immediately before powering off the protected site virtual machines.

- **Preparing storage for VM migration**. Site Recovery Manager changes the preference to the recovery site for each consistency group.

- **Migrating VMs**. If the production virtual machine is not powered on, the step fails. If the production virtual machine is powered on, Site Recovery Manager initiates vSphere vMotion to migrate the virtual machine to the recovery site.

Caution   Virtual machines that are eligible for migration are not migrated if they are lower priority than non-eligible VMs, or if they have dependencies on non-eligible VMs.

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.

When you add custom recovery steps, the steps are shared between the Test workflow and Run workflow. You cannot run custom steps on virtual machines that are to be suspended.

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

After reprotect, you can usually use custom recovery steps that show messages directly without modifications.

However, if there are custom steps that run commands containing site-specific information, such as network configurations, you might need to modify these steps after a reprotect.

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

You cannot add commands and prompts to these top-level steps relevant to storage policy protection groups:

- Complete test recovery of storage consistency groups

- Complete test recovery of VMs

- Complete test recovery of protection groups

- Complete live migration of protection groups

- Complete protection group operations on protected site

- Complete recovery of storage consistency groups

- Complete recovery of VMs

- Complete recovery of protection groups

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

Top-level commands run on the Site Recovery Manager Server. 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 perform 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 close the message, which allows the recovery to continue.

Execution of Commands and Prompt Steps

For storage policy protection groups, if you add a command or prompt before the first-priority virtual machines, Site Recovery Manager runs the command or prompt after the step **Apply VM policies** finishes for all virtual machines.

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

How Site Recovery Manager Handles Custom Recovery Step Failures

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

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

Command Recovery Steps

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

Type of Command	Description
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. Instead, the recovery plan pauses until you close the prompt.

Guidelines for Writing Command Steps

All batch files, scripts, 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 Site Recovery Manager Server on the recovery site before you add it to the plan.

Site Recovery Manager for Windows

- 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 ends 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 4 KB 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.

Site Recovery Manager Appliance

- You must copy the script in the home directory of the **admin** user `/home/admin`.

- You must change the access permission of the script so that the **srm** user can run it. For example, for a bash script, use the following command line:

  ```
  chmod 755 Myscript.sh
  ```

- When you run the script, you must use the full path on the local host. For example, to run a bash script, use the following command:

```
/bin/sh /home/admin/Myscript.sh
```

Environment Variables for Command Steps

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

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

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

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

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

Site Recovery Manager makes additional environment variables available for per-virtual machine command steps that run 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 Server to uniquely identify this virtual machine.	4212145a-eeae-a02c-e525-ebba70b0d4f3
VMware_VM_Name	Name of this virtual machine, as set at the protected site.	My New Virtual Machine
VMware_VM_Ref	Managed object ID of the virtual machine.	vm-1199
VMware_VM_GuestName	Name of the guest OS as defined by the VIM API.	otherGuest

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

Name	Value	Example
*VMware_VM_Guest*Ip	IP address of the virtual machine, if known.	192.168.0.103
VMware_VM_Path	Path to the VMX file of this virtual machine.	`[datastore-123] jquser-vm2/jquser-vm2.vmx`

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

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

Example: Commands That Can Run on Site Recovery Manager

For Site Recovery Manager for Windows, you can create a `myServerScript.bat` file that has the following content.

```
@echo off
echo %DATE% %TIME% : Recovery Plan %VMware_RecoveryName% ran in %VMware_RecoveryMode% mode"
:: some more custom actions
```

To run the `myServerScript.bat` file, use the following command content.

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

For the Site Recovery Manager Appliance, you can create a `myServerScript.sh` script that has the following content.

```
clear
echo "$(date "+%Y-%m-%d %H:%M:%S") : Recovery Plan $VMware_RecoveryName ran in
$VMware_RecoveryMode mode"
# some more custom actions
```

Note Do not use the vertical bar (|) and the single quote (') symbols when writing the commands in the script.

To run the `myServerScript.sh` script, use the following command content.

```
/bin/sh /home/admin/myServerScript.sh
```

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

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

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

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

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

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

```
echo $(date) : VM $VMware_VM_Name recovered by $VMware_RecoveryName ran
echo $(date) : Configured with the following FQDN: $VMware_VM_GuestName and IP:
$VMware_VM_GuestIp
# some more custom actions
```

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

```
/bin/sh myGuestScript.sh &>$VMware_GuestOp_OutputFile
```

Create Top-Level Message Prompts or Command Steps

You can add top-level recovery steps anywhere in the recovery plan. Top-level command steps are commands or scripts that you run on Site Recovery Manager Server during a recovery. You can also add steps that display message prompts that a user must acknowledge during a recovery.

Prerequisites

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

Procedure

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

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

3   On the **Recovery Plans** tab, select a recovery plan, and click **Recovery Steps**.

4 Use the **View** drop-down menu to select the type of step that you want to add.

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

You cannot add steps in the cleanup or reprotect operations.

5 Select where to add the step.

- To add a step before a step, right-click the step, and select **Add Step Before**.

- To add a step after the last step, right-click the last step, and select **Add Step After**.

6 Select **Command on SRM Server** or **Prompt**.

7 In the **Name** text box, enter a name for the step.

The step name appears in the list of steps in the **Recovery Steps** view.

8 In the **Content** text box, enter a command, script, or message prompt.

- If you selected **Command on SRM Server**, enter the command or script to run.

- If you selected **Prompt**, enter the text of the message to display during the recovery plan run.

9 (Optional) Modify the **Timeout** setting for the command to run on Site Recovery Manager Server.

This option is not available if you create a prompt step.

10 Click **Add** to add the step to the recovery plan.

What to do next

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

Create Message Prompts or Command Steps for Individual Virtual Machines

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

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

Prerequisites

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

- Verify that you have VMware Tools installed on the virtual machines where you are going to run custom scripts.

Procedure

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

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

3 On the **Recovery Plans** tab, select a recovery plan, and click **Recovery Steps**.

4 Right-click a virtual machine and click **Configure Recovery**.

5 On the **Recovery Properties** tab, click **Pre-Power On Steps** or **Post-Power On Steps**.

6 Click the plus icon to add a step.

7 Select the type of step to create.

Option	Description
Prompt	Prompts users to perform a task or to provide information that the user must acknowledge before the plan continues to the next step. This option is available for both pre-power on steps and post-power on steps.
Command on SRM Server	Runs a command on Site Recovery Manager Server. This option is available for both pre-power on steps and post-power on steps.
Command on Recovered VM	Runs a command on the recovered virtual machine. This option is only available for post-power on steps.

8 In the **Name** text box, enter a name for the step.

The step name appears in the list of steps in the **Recovery Steps** view.

9 In the **Content** text box, enter a command, script, or message prompt.

- If you selected **Command on SRM Server** or **Command on Recovered VM**, enter the command or script to run.

- If you selected **Prompt**, enter the text of the message to display during the recovery plan run.

10 (Optional) Modify the **Timeout** setting for the command to run on Site Recovery Manager Server.

This option is not available if you create a prompt step.

11 To add the step to the recovery plan, click **Add**.

12 To reconfigure the virtual machine to run the command before or after it powers on, click **OK**.

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

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

Procedure

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

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

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

4 Right-click **Suspend non-critical VMs at recovery site** and click **Add or Remove Non-Critical VM**.

5 Select virtual machines on the recovery site to suspend during a recovery.

6 Click **Save**.

Results

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

Specify the Recovery Priority of a Virtual Machine

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

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

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

Caution If a virtual machine that is eligible for stretched storage migration has a lower priority than a virtual machine that is not eligible for stretched storage migration, the eligible virtual machine is not be migrated.

Procedure

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

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

3   Click the **Recovery Plans** tab, click a recovery plan, and click **Virtual Machines**.

4   Right-click a virtual machine and click **Priority Group**.

5   Select a new priority for the virtual machine.

The highest priority is 1. The lowest priority is 5.

6   To confirm the change of priority, click **Yes**.

Configure Virtual Machine Dependencies

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

Caution   Virtual machines that are eligible for stretched storage migration are not migrated if they depend on VMs that are non-eligible for stretched storage migration.

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

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

Prerequisites

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

Procedure

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

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

3   Click the **Recovery Plans** tab, click a recovery plan, and click **Virtual Machines**.

4   Right-click a virtual machine that depends on one or more other virtual machines and click **Configure Recovery**.

5   Expand **VM Dependencies**.

6   From the drop-down menu, select **View all**.

7   Select one or more virtual machines from the list of all virtual machines in the selected recovery plan.

    The selected virtual machines are added to the list of dependencies.

8   Verify the virtual machines in the **VM Dependencies** list are on and verify the status of the dependencies is **OK**.

9   (Optional) To remove a dependency, select **View VM Dependencies** from the drop-down menu, select a virtual machine from the list of virtual machines that this virtual machine depends on, and click **Remove**.

10 Click **OK**.

Enable vSphere vMotion for Planned Migration

vSphere vMotion migration of a virtual machine is available only for a planned migration. You can enable or disable vSphere vMotion from the **Recovery Properties** dialog box.

Prerequisites

■   Before performing a vSphere vMotion migration, confirm that the virtual machine belongs to a storage policy protection group, is placed on stretched storage, and is powered on.

■   Ensure that you have configured full inventory mappings. If you have only configured temporary placeholder inventory mappings and you run a planned migration with the **Enable vMotion of eligible VMs** option, planned migration fails, even though both sites are running.

Procedure

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

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

3   Click the **Recovery Plans** tab, click a recovery plan, and click the **Virtual Machines** tab.

4   Right-click a virtual machine and click **Configure Recovery**.

    Select **Use vMotion for planned migration (VM should be powered on)**.

5   Click **OK**.

Results

There is no power cycle during the planned migration. Configured shutdown or startup actions or steps configured before power on are ignored. Steps configured after power on are run.

Configure Virtual Machine Startup and Shutdown Options

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

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

Prerequisites

You created a recovery plan.

Procedure

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

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

3   Click the **Recovery Plans** tab, click a recovery plan, and click **Virtual Machines**.

4   Right-click a virtual machine and click **Configure Recovery**.

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

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

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

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

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

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

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

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

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

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

Limitations to Protection and Recovery of Virtual Machines

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

Protection and Recovery of Suspended Virtual Machines

When you suspend a virtual machine, vSphere creates and saves its memory state. When the virtual machine resumes, vSphere restores the saved memory state so that the virtual machine can continue to operate 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.

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. As a consequence, snapshots are no longer available after recovery, unless you configure vSphere Replication to retain multiple point-in-time snapshots. For information about recovering older snapshots by using multiple point-in-time snapshots with vSphere Replication, see Replicating a Virtual Machine and Enabling Multiple Point in Time Instances.

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. The only exception is the **Reserve all guest memory (All locked)** setting, if it was enabled on the protected VM.

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

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 virtual 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 multiple arrays on the recovery site, if the virtual machine components span both arrays.

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 an unreplicated 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.

Customizing IP Properties for Virtual Machines

<div align="right">

8
</div>

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

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

Site Recovery Manager supports different types of IP customization.

- Use IPv4 and IPv6 addresses.

- Configure different IP customizations for each site.

- Use DHCP, Static IPv4, or Static IPv6 addresses.

- Customize addresses of Windows and Linux virtual machines.

- Customize multiple NICs for each virtual machine.

   Note You only configure one IP address per NIC.

For the list of guest operating systems for which Site Recovery Manager supports an IP customization, see the *Compatibility Matrices for Site Recovery Manager 8.3* at https://docs.vmware.com/en/Site-Recovery-Manager/8.3/rn/srm-compat-matrix-8-3.html.

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

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

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

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

Guest OS Startup

The Guest Startup process happens in parallel for all virtual machines for which you configure IP customization.

Customize IP

Site Recovery Manager pushes the IP customizations to the virtual machine.

Guest OS Shutdown

Site Recovery Manager shuts down the virtual machine and reboots it to ensure that the changes take effect and that the guest operating system services apply them when the virtual machine restarts.

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

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

- Manually Customize IP Properties for an Individual Virtual Machine

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

- Customizing IP Properties for Multiple Virtual Machines

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

Manually Customize IP Properties for an Individual Virtual Machine

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

Procedure

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

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

3   Click the **Recovery Plans** tab, click a recovery plan, and click **Virtual Machines**.

4   Right-click a virtual machine and click **Configure Recovery**.

5   Click the **IP Customization** tab and select **Manual IP customization** from the drop-down menu.

6   Select the NIC for which you want to modify IP Settings.

7   Click **Configure** for the protected site or the recovery site, depending on which set of IP settings you want to configure.

8   To configure IPv4 settings, click the **IPv4** tab.

- Select DHCP, or for static addresses, enter an IP address, subnet information, and gateway server addresses.

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

9   To configure IPv6 settings, click the **IPv6** tab.

- Select DHCP, or for static addresses, enter an IP address, subnet information, and gateway server addresses.

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

10   To configure DNS settings, click the **DNS** tab.

- Table 8-1. DNS Settings

Setting	Options
DNS Server	Choose how DNS servers are found: ■ Use DHCP to obtain a DNS address automatically. ■ Specify a preferred and an alternate DNS server.
DNS Suffix	Enter a DNS suffix and click **Add** or select an existing DNS suffix and click **Remove**, **Move Up**, or **Move Down**.

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

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

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

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

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

Results

Recovery site settings are applied during recovery. Protected site settings are applied during failback.

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

Apply IP Customization Rules to a Virtual Machine

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

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

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

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

Prerequisites

For the list of guest operating systems for which Site Recovery Manager supports an IP customization, see the *Compatibility Matrices for Site Recovery Manager 8.3* at https://docs.vmware.com/en/Site-Recovery-Manager/8.3/rn/srm-compat-matrix-8-3.html.

Procedure

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

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

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

4 Right-click a virtual machine and click **Configure Recovery**.

5 From the **IP Customization** mode list, select **Use IP customization rules if applicable** and click **OK**.

Option	Description
Auto	Depends on the advanced setting for `recovery.useIpMapperAutomatically`.
	If you have configured IP mapping rules for virtual networks and `recovery.useIpMapperAutomatically` is set to True, Site Recovery Manager evaluates the subnet IP mapping rules during a recovery to customize the virtual machines.
	If `recovery.useIpMapperAutomatically` is set to False, Site Recovery Manager does not evaluate the IP mapping rules during recovery.
Use IP customization rules if applicable	Overrides the effect of the Auto option. If you have configured IP mapping rules for virtual networks, during recovery Site Recovery Manager customizes the virtual machines .
Manual IP customization	Overrides the effect of the Auto option. You must set up manually the new recovery IP per virtual machine.
No IP customization	Overrides the effect of the Auto option. No changes in the recovery virtual machine IP.

Customizing IP Properties for Multiple Virtual Machines

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

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

- Using DR IP Customizer is a fast way to define explicit IP customization settings for multiple virtual machines by using a CSV file.

- You apply subnet-level IP customization rules to virtual machines by using the vSphere Web Client or the vSphere Client.

Virtual machines that you configure by using DR IP Customizer are not subject to subnet-level IP customization rules.

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

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

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

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

1 Run DR IP Customizer to generate a CSV file that contains the networking information for the protected virtual machines.

2 Modify the generated CSV file with networking information that is relevant to the recovery site.

3 Run DR IP Customizer on the protected machines again to apply the CSV with the modified networking configurations to apply when the virtual machines start up on the recovery site.

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

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

For the list of guest operating systems for which Site Recovery Manager supports an IP customization, see the *Compatibility Matrices for Site Recovery Manager 8.3* at https:// docs.vmware.com/en/Site-Recovery-Manager/8.3/rn/srm-compat-matrix-8-3.html.

What to read next

- 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.

- 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.

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 Server login credentials for each site when the command runs.

Procedure

1 Log in to the Site Recovery Manager Server host at either the protected or recovery site and open a command prompt.

2 Change the working directory to:

   - For Windows `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.

- For Linux `/opt/vmware/srm/bin/`.

3 Run the `dr-ip-reporter` command.

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

  - For Windows:

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

  - For Linux:

    ```
    /opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
    --out path_to_report_file.xml
    --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
    ```

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

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

  - For Windows:

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

  - For Linux:

    ```
    /opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
    --out "path_to_report_file.xml"
    --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
    --vcid vCenter_Server_ID
    ```

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

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

- To restrict the list of networks to just the ones that a specific recovery plan requires, include the `--plan` option in the command line:

  - For Windows:

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

  - For Linux:

    ```
    /opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
    --out "path_to_report_file.xml"
    --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
    --plan recovery_plan_name
    ```

Syntax of the DR IP Customizer Tool

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

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

- If you are using Site Recovery Manager for Windows, 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.

- If you are using the Site Recovery Manager Virtual Appliance, the `dr-ip-customizer` is located in the `/opt/vmware/srm/bin/` directory on the appliance.

When you run `dr-ip-customizer.exe` or `dr-ip-customizer`, you specify different options depending on whether you are generating or applying a comma-separated value (CSV) file.

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

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

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

Table 8-2. DR IP Customizer Options

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

Table 8-2. DR IP Customizer Options (continued)

Option	Description	Mandatory
`--uri arg`	Lookup Service URL on the Platform Service Controller with the form `https://host[:port]/lookupservice/sdk`. Specify the port if it is not 443 . The Site Recovery Manager instance associates this address with the primary site's infranode. Use the same vCenter Server instance for the `apply` and `drop` commands as the one that you used to generate the CSV file.	Yes
`--vcid arg`	The primary sitevCenter Server instance UUID.	Optional, unless the primary site infrastructure contains more than one vCenter Server instance.
`-i [ --ignore-thumbprint ]`	Ignore the vCenter Server thumbprint confirmation prompt.	No
`-e [ --extra-dns-columns ]`	Must be specified if the input CSV file contains extra columns for DNS information.	No
`-v [ --verbose ]`	Enable verbose output. You can include a `--verbose` option on any `dr-ip-customizer.exe` or `dr-ip-customizer` command line to log additional diagnostic messages.	No

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

■ For Windows:

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

■ For Linux:

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg testConfig.xml -i --cmd generate -o "/home/
admin/x.csv" --uri
https://service.company.com:443/lookupservice/sdk --vcid ?
```

The resulting error message includes the vCenter Server instance UUID followed by the vCenter Server DNS host name for each vCenter Server registered with the Lookup Service:

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

Structure of the DR IP Customizer CSV File

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

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

You 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 8-3. 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. It is the same as the virtual machine ID that vCenter Server uses if present, or the BIOS id if not.	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 8-3. 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. If the field is not set to a specific static address you must set it to DHCP.

Table 8-3. Columns of the DR IP Customizer CSV File (continued)

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

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

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

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

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

- Omit values if a setting is not required.

- Use the minimum number of rows possible for each adapter.

- Do not use commas in any field.

- Specify Adapter ID settings as needed. DR IP Customizer applies settings that you specify on Adapter ID 0 to all NICs. To apply settings to individual NICs, specify the values in the Adapter ID 1, 2, ..., *n* fields.

- To specify more than one value for a column, create an additional row for that adapter and include the value in the column in that row. To ensure that the additional row is associated with the intended virtual machine, copy the VM ID, VM Name, vCenter Server, and Adapter ID column values.

- To specify an IP address for a network adapter on each of the protected and recovery sites, or to specify multiple DNS server addresses, add a new row for each address. Copy the VM ID, VM Name, and Adapter ID values to each row.

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` or `dr-ip-customizer` with the --

`cmd generate` command. You edit the CSV file to customize the IP settings of the protected virtual machines.

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

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)
103b9e8b-1f90-faca-8028-13820b8f236e,vm-3-win,vcenter-server-site-B,0,,,,,,,,,,,,
103b9e8b-1f90-faca-8028-13820b8f236e,vm-3-win,vcenter-server-site-A,0,,,,,,,,,,,,
834c1a9b-1f91-fbca-1028-43820d8f236d,vm-1-linux,vcenter-server-site-B,0,,,,,,,,,,,,
834c1a9b-1f91-fbca-1028-43820d8f236d,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 8-4. 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)
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e	vm-3- win	vcenter -server -site-B	0							example. com
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e	vm-3- win	vcenter -server -site-B	0							eng.exa mple.co m
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e		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	
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e		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	
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e	vm-3- win	vcenter -server -site-A	0						1.1.0.1	example. com
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e	vm-3- win	vcenter -server -site-A	0						1.1.0.2	eng.exa mple.co m

Table 8-4. 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)
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e		vcenter -server -site-A	1			192.168.0 .21	255.255. 255.0	192.168.0 .1		
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e		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 8-5. 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)
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e	vm-3-win	vcenter -server -site-B	0							example. com
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e	vm-3-win	vcenter -server -site-B	0							eng.exa mple.co m
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e		vcenter -server -site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e		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	
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e	vm-3-win	vcenter -server -site-A	0						1.1.0.1	example. com
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e	vm-3-win	vcenter -server -site-A	0						1.1.0.2	eng.exa mple.co m

Table 8-5. Setting Static and DHCP 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)
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e		vcenter -server -site-A	1			dhcp				
103b9e 8b-1f90 -faca-8 028-13 820b8f 236e		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 8-6. 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)
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0										example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0										eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		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	
103b9e8b-1f90-faca-8028-13820b8f236e		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 8-6. 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)
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0										eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1			dhcp			::ffff:192.168.0.22	32	::ffff:192.168.0.1	::ffff:192.168.0.250	
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1									::ffff:192.168.0.251	
103b9e8b-1f90-faca-8028-13820b8f236e		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.

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

Prerequisites

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

- If you are using Site Recovery Manager for Windows, the user account that you use to run the DR IP Customizer tool requires at least the Site Recovery Manager Recovery Plans Administrator role.

- If you are using the Site Recovery Manager Virtual Appliance, you must SSH with the admin user.

Procedure

1 Log in to the Site Recovery Manager Server host and open a command shell.

2 Change the working directory to:

- For Windows `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.

- For Linux `/opt/vmware/srm/bin/`.

3. Run the `dr-ip-customizer` command to generate a comma-separated value (CSV) file that contains information about the protected virtual machines.

   - If you have a Platform Services Controller with a single vCenter Server instance

     For Windows, run the following command:

     ```
     dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
     Manager\config\vmware-dr.xml"
     --cmd generate --out "C:\tmp\output.csv"
     --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
     ```

     For Linux, run the following command:

     ```
     /opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
     --cmd generate --out "/home/admin/output.csv"
     --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
     ```

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

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

     For Windows, run the following command:

     ```
     dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
     Manager\config\vmware-dr.xml"
     --cmd generate --out "C:\tmp\output.csv"
     --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
     --vcid vCenter_Server_ID
     ```

     For Linux, run the following command:

     ```
     /opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
     --cmd generate --out "/home/admin/output.csv"
     --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
     --vcid vCenter_Server_ID
     ```

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

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

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

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

5 Enter the login credentials for the vCenter Server instance.

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

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

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

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

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

- If you have a Platform Services Controller with a single vCenter Server instance

  For Windows, run the following command:

  ```
  dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
  Manager\config\vmware-dr.xml"
  --cmd apply --csv "C:\tmp\output.csv"
  --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
  ```

  For Linux, run the following command:

  ```
  /opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
  --cmd apply --csv "/home/admin/output.csv"
  --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
  ```

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

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

  For Windows, run the following command:

  ```
  dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery
  Manager\config\vmware-dr.xml"
  --cmd apply --csv "C:\tmp\output.csv"
  --uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
  --vcid vCenter_Server_ID
  ```

For Linux, run the following command:

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd apply --csv "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

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

Results

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

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

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

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

Important

- IP subnet mapping rules support IPv4 only.

- Rule-based IPv6 customization is not supported in Site Recovery Manager.

- When you apply IP subnet mapping rules to Windows virtual machines with IPv6 enabled, the IPv6 settings, DHCP or static, remain unaffected after recovery. For Linux virtual machines, IPv6 settings are reset to DHCP.

- Site Recovery Manager does not evaluate IP mapping rules for virtual machines configured to use manual IP customization.

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

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

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

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

Procedure

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

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

3   On the **Site Pair** tab, click **Configure > Network Mappings**.

4   Select a network mapping for which to define a customization rule.

5   To define a rule, click **Add IP Customization Rule**.

6   Specify the subnet IP ranges that map to the protected and recovery sites.

7   Specify the network settings for the recovery site network.

8   Click **Add** to save your changes.

Reprotecting Virtual Machines After a Recovery

9

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

Manually re-establishing 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 the protection.

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

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

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

You can perform reprotect on recovery plans that contain array-based replication protection groups, vSphere Replication protection groups, and storage policy protection groups.

Note If you change the disk size of a virtual machine replicated with vSphere Replication after it was recovered, and then run reprotect, the reprotect operation will fail.

Performing a Reprotect Operation

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

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

Figure 9-1. Site Recovery Manager Reprotect Process

- How Site Recovery Manager Reprotects Virtual Machines with Array-Based Replication

  In the reprotect process with array-based replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

- How Site Recovery Manager Reprotects Virtual Machines with vSphere Replication

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

- How Site Recovery Manager Reprotects Virtual Machines with Storage Policy Protection

  In the reprotect process using storage policy protection, Site Recovery Manager reverses the direction of replication and protects the virtual machines that are associated with the relevant storage policies on what was previously the recovery site. Site Recovery Manager reestablishes vSphere entity protection and monitoring on the new protected site.

- Preconditions for Performing Reprotect

  You can perform reprotect only if you meet certain preconditions.

- Reprotect Virtual Machines

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

- Overview of Reprotect States

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

How Site Recovery Manager Reprotects Virtual Machines with Array-Based Replication

In the reprotect process with array-based replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

When you initiate the reprotect process, Site Recovery Manager instructs the underlying storage arrays 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 operation.

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. 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 the reprotect process, or the process might fail.

When reprotecting virtual machines 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 process finishes.

How Site Recovery Manager Reprotects Virtual Machines with vSphere Replication

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

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

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

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

How Site Recovery Manager Reprotects Virtual Machines with Storage Policy Protection

In the reprotect process using storage policy protection, Site Recovery Manager reverses the direction of replication and protects the virtual machines that are associated with the relevant storage policies on what was previously the recovery site. Site Recovery Manager reestablishes vSphere entity protection and monitoring on the new protected site.

Reversing the replication of a storage policy protection group is the same as reversing the replication of an array-based replication protection group because it only affects the underlying storage. When you perform reprotect on a recovery plan that includes a storage policy protection group, the replication technology that your storage arrays provide reverses the replication of all of the consistency groups that are associated with the storage policies that the protection group contains.

If the storage arrays fail to reverse replication for any consistency groups in the protection group, the recovery plan goes into the Incomplete Reprotect state. In this state, you must resolve the storage issues and run reprotect again. Rerunning reprotect on a storage policy protection group only affects the direction of replication of consistency groups for which a previous reprotect operation did not complete successfully.

When the storage arrays have reversed the direction of replication, Site Recovery Manager reestablishes vSphere entity protection and monitoring. The conditions for reestablishment of vSphere entity protection and monitoring during reprotect are less strict than the conditions for establishing vSphere entity protection and monitoring during the creation of a storage policy protection group:

- Site Recovery Manager checks the storage policies on the new protected site for compliance. If storage policies on the new protected site are non-compliant, reprotect does not fail but Site Recovery Manager cannot protect the virtual machines that are associated with that storage policy. For information about compliance, see Prerequisites for Storage Policy Protection Groups and Limitations of Storage Policy Protection Groups.

- Site Recovery Manager restarts vSphere entity monitoring on the new protected site.

- Site Recovery Manager starts protecting all compliant virtual machines. This might not be the same set of virtual machines as was recovered when you ran the recovery plan initially because you or another user might have associated more virtual machines with the storage policy on the new protected site. Reprotect does not fail if Site Recovery Manager fails to protect a virtual machine on the new protected site.

- The storage policy protection group is ready for recovery from the new protected site to the new recovery site.

Preconditions for Performing Reprotect

You can perform reprotect only if you meet certain preconditions.

You can perform reprotect on recovery plans that contain array-based replication protection groups, vSphere Replication protection groups, and storage policy protection groups.

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

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

2   The original protected site must be available. The vCenter Server instances, ESXi Servers, Site Recovery Manager Server instances, 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. After a reprotect operation, you can recover virtual machines back to the original site using a planned migration workflow.

Prerequisites

See Preconditions for Performing Reprotect.

Procedure

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

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

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

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

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

The **Force Cleanup** option is only available after you perform an initial reprotect operation that experiences errors.

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

7 To monitor the progress of the reprotect operation, select the recovery plan and click **Recovery Steps** tab.

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

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

Results

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.

Overview of Reprotect States

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

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

Table 9-1. Reprotect States

State	Description	Remedial Action
Reprotect In Progress	Site Recovery Manager is running reprotect.	None
Partial Reprotect	Occurs if multiple recovery plans share the same protection groups and some of the protection groups were successfully reprotected in another plan.	Run reprotect again on the partially reprotected plans.

Table 9-1. 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 perform a reverse replication or a failure to create a placeholder virtual machines.	■ If a reprotect operation fails to perform a reverse replication, make sure that sites are connected, review the reprotect progress in the Site Recovery UI, and start the reprotect task again. If reprotect still does not succeed, run the reprotect task with the **Force Cleanup** option. ■ If Site Recovery Manager fails to create placeholder virtual machines, recovery is still possible. Review the reprotect steps in the Site Recovery user interface, resolve any problems, and run reprotect 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.
Ready	Occurs when the reprotect finishes successfully.	None.

Restoring the Pre-Recovery Site Configuration by Performing Failback

10

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

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

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

To perform a 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   To shut down the virtual machines on the protected site and start up the virtual machines on the recovery site, perform a planned migration. To avoid interruptions in virtual machine availability, you might want to run a test before you start the planned migration. If the test identifies errors, you can resolve them before you perform the planned migration.

3   Perform a second reprotect, to revert the protected and recovery sites to their original configuration before the recovery.

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

Performing a Failback Operation

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

1   Virtual machines replicate from site A to site B.

2   Perform a reprotect. Site B, the former recovery site, becomes the protected site. Site Recovery Manager uses the protection information to establish the protection of site B. Site A becomes the recovery site.

3   To recover the protected virtual machines on site B to site A, perform a planned migration.

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

Figure 10-1. Site Recovery Manager Failback Process
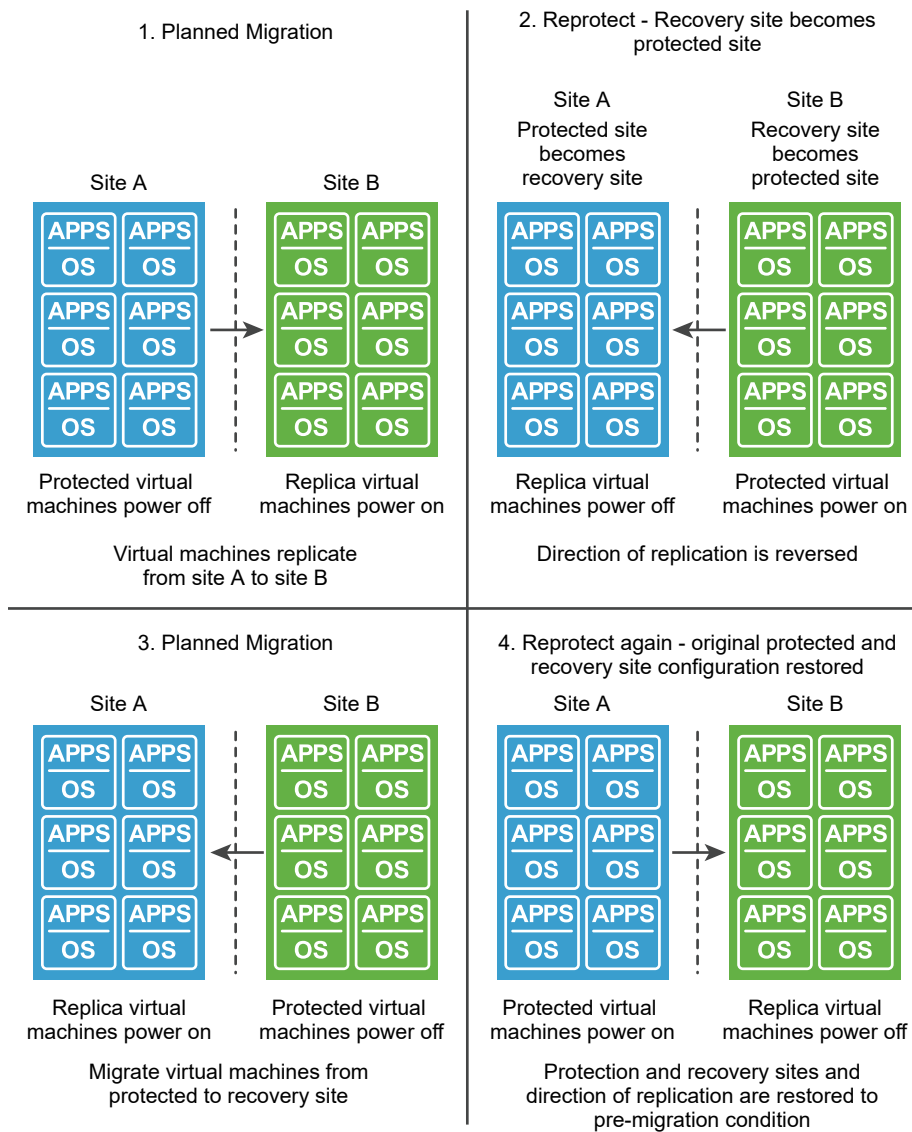
Read the following topics next:

■ Perform a Failback

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.

After a recovery from site A to site B, the recovered virtual machines are running on site B without protection.

Prerequisites

- You 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.

- You did not run reprotect since the recovery.

- If you performed a disaster recovery, you must perform a planned migration when the hosts and datastores on the original protected site are running again.

Procedure

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

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

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

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

5 Determine whether to enable **Force Cleanup**, and click **Next**.

   Force Cleanup is only available after you run reprotect once and errors occur. Enabling this option forces the removal of virtual machines, ignoring errors, and returns the recovery plan to the `ready` state.

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

7 Select the recovery plan and click **Recovery Steps** to monitor the reprotect operation until it finishes.

8 (Required) If necessary, rerun reprotect until it finishes without errors.

   At the end of the reprotect operation, Site Recovery Manager reverses replication, so that the original recovery site, site B, is now the protected site.

9 To run the recovery plan as a planned migration, right-click the recovery plan and click **Recovery**.

10 Select the recovery plan and click **Recovery Steps** to monitor the planned migration until it finishes.

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

   When the planned migration completes, the virtual machines are running on the original protected site, site A, but the virtual machines are not protected. The virtual machines on the original recovery site, site B, are powered off.

11 Right-click the recovery plan, click **Reprotect**, and follow the instructions of the wizard to perform a second reprotect operation.

Results

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

Interoperability of Site Recovery Manager with Other Software

<div style="text-align: right">11</div>

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

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

Read the following topics next:

- Site Recovery Manager and vCenter Server
- Using Site Recovery Manager with VMware vSAN Storage and vSphere Replication
- How Site Recovery Manager Interacts with DPM and DRS During Recovery
- How Site Recovery Manager Interacts with Storage DRS or Storage vMotion
- How Site Recovery Manager Interacts with vSphere High Availability
- How Site Recovery Manager Interacts with Stretched Storage
- How Site Recovery Manager Interacts with vSphere Cluster Services
- Using Site Recovery Manager with NSX Data Center for vSphere
- Site Recovery Manager and vSphere PowerCLI
- Site Recovery Manager and Virtual Machine Encryption
- Site Recovery Manager and VMware vSphere Virtual Volumes
- VMware HCX Integration with Site Recovery Manager
- Site Recovery Manager and vRealize Orchestrator
- VMware Site Recovery Manager and VMware vRealize Operations Manager
- Protecting Windows Server Failover Clustering and Fault Tolerant Virtual Machines
- Using Site Recovery Manager with SIOC Datastores

- Using Site Recovery Manager with Admission Control Clusters

- Site Recovery Manager and Virtual Machines Attached to RDM Disk Devices

- Site Recovery Manager and Active Directory Domain Controllers

Site Recovery Manager and vCenter Server

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

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

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

How Changes to vCenter Server Inventory Affect Site Recovery Manager

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

In the case of array-based replication and vSphere Replication, Site Recovery Manager can tolerate certain changes at the protected site without disruption.

- Deleting protected virtual machines.

- Deleting an object for which an inventory mapping exists.

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

- Moving placeholder virtual machines to a different folder or resource pool.

- Deleting an object for which an inventory mapping exists.

Note Storage Policy Protection Groups handle changes differently. See Inventory Mappings for Storage Policy Protection Groups .

Site Recovery Manager and the vCenter Server Database

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

Using Site Recovery Manager with VMware vSAN Storage and vSphere Replication

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

Site Recovery Manager supports vSphere Replication with vSAN. You cannot use vSAN storage with array-based replication.

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

For information about using vSphere Replication with vSAN, see Using vSphere Replication with VMware vSAN Storage in *vSphere Replication Administration*.

How Site Recovery Manager Interacts with DPM and DRS During Recovery

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

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

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

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

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

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

How Site Recovery Manager Interacts with Storage DRS or Storage vMotion

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

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

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

Using Site Recovery Manager with 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.

- Storage DRS considers the protection and the replication status of datastores while calculating placement recommendations to perform automatic or manual migration. Storage DRS checks if the datastore is replicated or not, part of a consistency group or protection group, then tags the datastore accordingly. For more information on how Site Recovery Manager handles datastore tagging, see http://kb.vmware.com/kb/2108196.

- Site Recovery Manager supports Storage DRS clusters containing datastores from different consistency groups. If you migrate a virtual machine to a datastore that is not part of a protection group, then you have to reconfigure the protection group to include that datastore.

- Site Recovery Manager supports Storage vMotion without limitation between non-replicated datastores and between replicated datastores in the same consistency group. In those cases, Storage DRS can perform automatic Storage vMotion in clusters in automatic mode, or issue recommendations for Storage vMotion in clusters in manual mode.

■ Special considerations apply to Storage vMotion between a replicated and a non-replicated datastore, or between replicated datastores in different consistency groups. In those cases, Storage DRS does not automatically initiate or recommend Storage vMotion. Manually initiated Storage vMotion results in a warning detailing the possible impact.

■ 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.

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

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

■ vSphere Replication is compatible with vSphere Storage DRS on both protected and recovery sites. On the protected site, you can use Storage DRS to move the disk files of virtual machines that vSphere Replication protects, with no impact on the ongoing replication. On the recovery site, you must register the vSphere Replication appliance with the vCenter Single Sign-On service so that Storage DRS can identify the replica disk files on the Storage DRS cluster and generate migration recommendations. You can use Storage DRS to migrate replica disk files with no impact on subsequent recovery. See *Register the vSphere Replication Appliance with vCenter Single Sign-On* from the vSphere Replication documentation for details.

- vSphere Replication is compatible with Storage vMotion on the protected site. You can use Storage vMotion to move the disk files of replicated virtual machines on the protected site with no impact on the ongoing replication.

- Site Recovery Manager detects the changes and fails over the virtual machine successfully.

- Site Recovery Manager supports Storage DRS clusters on the recovery site with datastores containing the vSphere Replication replica disks.

- vSphere Replication is compatible with Storage vMotion and saves the state of a disk or virtual machine when the home directory of a disk or virtual machine moves. Replication of the disk or virtual machine continues normally after the move.

- A full sync causes Storage DRS to generate migration recommendations or directly trigger Storage vMotion if Storage DRS running in fully-automated mode. This happens if the DRS rules are very aggressive, or if a large number of virtual machines perform a full sync at the same time. The default I/O latency threshold for Storage DRS is 15ms. By default, Storage DRS performs loading balancing operations every 8 hours. Storage DRS also waits until it has collected sufficient statistics about the I/O load before it generates Storage vMotion recommendations. Consequently, a full sync only affects Storage DRS recommendations if the full sync lasts for a long time and if, during that time, the additional I/O that the full sync generates causes the latency to exceed the I/O latency threshold.

- When you use Storage DRS in manual mode on protected virtual machine datastores, stale recommendations might exist after a failover. After reprotecting the failed over virtual machines to the original site, if you apply these stale Storage DRS recommendations, the Site Recovery Manager placeholder VM becomes corrupted, causing a subsequent recovery to the original site to fail for the VMs for which the Storage DRS recommendations were applied. If you apply stale updates, unregister the placeholder VM and use the Site Recovery Manager repair operation to recreate a valid placeholder. To avoid this issue, clear any stale recommendations from a prior failover from that site by regenerating Storage DRS recommendations for the affected Storage DRS storage cluster after reprotect successfully completes.

How Site Recovery Manager Interacts with vSphere High Availability

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

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

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

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

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

How Site Recovery Manager Interacts with Stretched Storage

Stretched storage support is available for array-based replication.

Site Recovery Manager supports active-active stretched storage between protected and recovery sites by using Cross vCenter Server vMotion to perform planned migrations, eliminating service downtime. Disaster recovery and test recovery continue to use the existing LUN-based recovery functionality.

Important   Stretched storage is supported only on vCenter Single Sign-On Enhanced Linked Mode environments. Planned migration with Cross vCenter Server vMotion fails if the sites are not Enhanced Linked Mode. Stretched storage is required when using Cross vCenter Server vMotion during a planned migration.

Protection Groups

Important   Protection groups for stretched storage must be created as storage policy protection groups. You must create and use storage profiles to protect and recover stretched storage devices.

- Protection groups with stretched devices must have a preferred direction from the protected site to the recovery site. The preferred direction must match the site preference that the array maintains for the corresponding devices. If the array supports site preference, then the protected site must have the site preference.

- Stretched and nonstretched virtual machines and consistency groups can be in the same protection groups and the same recovery plan.

- The stretched virtual machines must be on a stretched datastore and must be powered on at the protected site.

- You cannot create two protection groups in opposite directions by using the same stretched device pair. You can place virtual machines on the stretched devices at the recovery site that correspond to protected devices at the protected site, but if the recovery site ESXi is mounting the protected site storage there is a risk of data corruption. You cannot protect these virtual machines, but they are automatically protected during the reprotect process.

Planned Migration

- The **Run Recovery Plan** wizard has an option to use Cross vCenter Server vMotion to perform a planned migration. If the option is selected, Cross vCenter Server vMotion is used for all protected, powered-on virtual machines on the stretched storage at the protected site. If the option is not selected, the regular recovery workflow is used for replicated LUNs, including stretched storage.

- If Cross vCenter Server vMotion fails for any reason, the recovery plan stops at the "Migrating VMs" step and does not continue. If you cannot resolve the problem that is preventing Site Recovery Manager from using Cross vCenter Server vMotion, rerun the recovery plan with the vSphere vMotion option turned off. The migration can then use the regular recovery workflow for replicated LUNs.

- During the deactivate step the stretched devices stay mounted at the protected site even if vMotion is not used. Site Recovery Manager ignores non-protected replica virtual machines on the stretched devices at the protected site and does not unregister them.

Test Recovery

- Test recovery is performed by using the regular test recovery workflow for replicated devices, including stretched devices. vMotion compatibility checks are performed for each virtual machine on the stretched devices.

- If the array does not support creating read-write snapshots for stretched devices, Site Recovery Manager does not allow you to perform a test recovery for these devices.

Cross vCenter Server vMotion

Cross vCenter Server vMotion is not supported for migration from a vSphere Distributed Switch port group to a standard switch network. In this instance, attempting to Cross vCenter Server vMotion a virtual machine results in these error messages.

- Unable to find a host in the cluster <cluster-name> that is compatible with the Cross vCenter Server vMotion of the virtual machine <vm-name> from the protection group <PG-name>.

- Currently connected network interface <network-adapter-name> cannot use network <network-name>, because the type of the destination network is not supported for vMotion based on the source network type.

Cross vCenter Server vMotion does not work in these situations.

- If the distributed resource scheduler is disabled for the cluster

- If the virtual machine has snapshots

- If the virtual machine is a linked clone

Cross vCenter Server vMotion requirements in vSphere are discussed in the *ESXi and vCenter Server 7.0* documentation.

How Site Recovery Manager Interacts with vSphere Cluster Services

vSphere Cluster Services (vCLS) ensures that if vCenter Server becomes unavailable, cluster services remain available to maintain the resources and health of the workloads that run in the clusters.

vCLS uses agent virtual machines to maintain the cluster services health. The vCLS agent virtual machines (vCLS VMs) are created when you add hosts to clusters. Up to three vCLS VMs are required to run in each vSphere cluster, distributed within a cluster. vCLS is also enabled on clusters which contain only one or two hosts. In these clusters, the number of vCLS VMs is one and two, respectively.

The vCLS agent virtual machines cannot be stored on a replicated datastore managed by Site Recovery Manager. You must have a non-replicated datastore with a minimum free capacity of 6 GB.

Using Site Recovery Manager with NSX Data Center for vSphere

Site Recovery Manager can protect virtual machines that are attached to NSX networks present on the protected and recovery site without having to configure inventory mappings.

NSX Data Center for vSphere supports Universal Logical Switches which allow for the creation of layer-2 networks that span vCenter Server boundaries. When using Universal Logical Switches with NSX, there is a virtual port group at both the protected and recovery site that connects to the same layer-2 network. This means that when using storage policy protection groups and a Universal Logical Switch, you do not need to specify any network mapping. Site Recovery Manager works with NSX Data Center for vSphere to automatically map the virtual machine to the correct network at the recovery site.

You can override auto-mapping by manually configuring network mappings on stretched networks. Enhanced Linked Mode and non- Enhanced Linked Mode topologies are supported.

Limitations

- Auto-mapping for NSX universal wires is **only** supported with storage policy protection groups and Universal Logical Switches.

- Network auto-mapping for storage policy protection groups is not supported on VMware NSX-T™ Data Center.

- For virtual machine protection groups, you must explicitly configure network mapping between the two ends of the universal wire to ensure that the virtual machines recover on the same universal wire.

- This feature is only supported for a full recovery. Test failover must be done manually.

See Configure Inventory Mappings for details.

Site Recovery Manager and vSphere PowerCLI

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

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

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

Site Recovery Manager and Virtual Machine Encryption

You can use Site Recovery Manager to protect and recover encrypted virtual machines with array-based protection groups, storage policy protection groups, and vSphere Replication protection groups.

Encryption protects not only your virtual machine but also virtual machine disks and other files. You set up a trusted connection between vCenter Server and a key management server (KMS). vCenter Server can then retrieve keys from the KMS as needed. You must use a KMS cluster registered with the same name on the protected and the recovery sites. For more information, see *Set Up the KMS Cluster* in the *Administering VMware vSAN* guide.

To perform a guest customization of encrypted virtual machines, Site Recovery Manager requires ESXi 6.5 or later.

For more information on virtual machine encryption, see Virtual Machine Encryption in the *vSphere Security* documentation.

For more information about storage policy protection groups and encrypted virtual machines, see Protect an Encrypted VM.

For more information about vSphere Replication and encrypted virtual machines, see Replicating Encrypted Virtual Machines in the *vSphere Replication Administration* documentation.

Site Recovery Manager and VMware vSphere Virtual Volumes

You can use Site Recovery Manager to protect virtual machines on VMware vSphere Virtual Volumes storage.

The Virtual Volumes functionality helps to improve granularity. It helps you to differentiate virtual machine services on a per application level by offering a new approach to storage management. Rather than arranging storage around features of a storage system, Virtual Volumes arrange storage around the needs of individual virtual machines, making storage virtual machine centric. Virtual Volumes maps virtual disks and their derivatives, clones, snapshots, and replicas, directly to objects, called virtual volumes, on a storage system. This mapping allows vSphere to offload intensive storage operations such as snapshot, cloning, and replication to the storage system.

A Virtual Volumes storage provider, also called a VASA provider, is a software component that acts as a storage awareness service for vSphere. The provider mediates out-of-band communication between vCenter Server and ESXi hosts on one side and a storage system on the other. The storage provider is implemented through VMware APIs for Storage Awareness (VASA) and is used to manage all aspects of Virtual Volumes storage. The storage provider integrates with the Storage Monitoring Service (SMS), included in vSphere, to communicate with vCenter Server and ESXi hosts. The storage provider delivers information from the underlying storage container. The storage container capabilities appear in vCenter Server and the vSphere Client. Then, in turn, the storage provider communicates virtual machine storage requirements, which you can define in the form of a storage policy, to the storage layer. This integration process ensures that a virtual volume created in the storage layer meets the requirements outlined in the policy. Site Recovery Manager supports VASA 3.0 and later.

VMware HCX Integration with Site Recovery Manager

With the HCX integration with Site Recovery Manager, you can use the features and tools of VMware Site Recovery Manager for virtual machines, which are protected by HCX.

To integrate HCX with Site Recovery Manager, you need HCX Private Cloud (HCX Enterprise Plus) and Site Recovery Manager version 8.2 or above. For more information, see the *VMware HCX Product Documentation*.

Note   You can integrate Site Recovery Manager with either HCX or vSphere Replication, but not both at the same time, in the same Site Recovery Manager instance.

Site Recovery Manager and vRealize Orchestrator

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

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

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

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

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

VMware Site Recovery Manager and VMware vRealize Operations Manager

The vRealize Operations Management Pack for Site Recovery Manager allows VMware administrators to monitor the local Site Recovery Manager Windows services in VMware vRealize Operations Manager.

The vRealize Operations Management Pack for VMware Site Recovery Manager provides capabilities for monitoring the connectivity between Site Recovery Manager instances, the availability of a remote Site Recovery Manager instance, and the status of protection groups and recovery plans. Alarms are generated when there are Site Recovery Manager connectivity issues encountered or protection groups and recovery plans are in an error state. The user interface provides statistics for the number of Site Recovery Manager-related objects and how many of them have errors.

The vRealize Operations Management Pack for VMware Site Recovery Manager requires certain ports to be open. If you are connecting to the Site Recovery Manager virtual appliance, the management pack uses port 443 (HTTPS protocol). If you are connecting to Site Recovery Manager for Windows, by default the management pack uses port 9086 (HTTPS protocol).

Protecting Windows Server Failover Clustering and Fault Tolerant Virtual Machines

You can use Site Recovery Manager to protect Windows Server Failover Clustering (WSFC) and fault tolerant virtual machines, with certain limitations.

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

General Limitations to Protecting WSFC and Fault Tolerant Virtual Machines

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

- Site Recovery Manager supports protecting and recovering WSFC virtual machines with shared disks with array-based replication only.

- Site Recovery Manager supports protecting and recovering WSFC virtual machines without shared disks with array-based replication and vSphere Replication.

- Protect and reprotect of WSFC or fault tolerant virtual machines requires VMware High Availability (HA) and VMware Distributed Resource Scheduler (DRS) at both the protected and the recovery sites. When you move WSFC 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 WSFC Virtual Machines.

- You can use array-based replication to protect multiple vCPU fault tolerance (SMP-FT) virtual machines. Both the primary and the secondary fault tolerant virtual machine disk files must reside on replicated LUNs, and all LUNs must be part of the same consistency group.

- Site Recovery Manager attempts to fail over only the primary SMP-FT virtual machine and does not try to fall back on the secondary SMP-FT virtual machine, if something is wrong with the files of the primary SMP-FT virtual machine.

- Site Recovery Manager shows a warning when an SMP-FT VM virtual machine is protected and its storage does not meet the replication requirements.

- One SMP-FT virtual machine can be protected by only one Protection Group.

- Site Recovery Manager does not support for SMP-FT virtual machines replicated by vSphere Replication.

- Site Recovery Manager does not support SMP-FT virtual machines in storage policy protection groups. SMP-FT does not support storage profiles.

- Site Recovery Manager does not support recovery of SMP-FT virtual machines with Virtual Volumes protection groups. SMP-FT does not support storage profiles.

- When doing reprotect, Site Recovery Manager does not preserve SMP-FT configuration on the original protected site.

- When performing failover, the destination virtual machine is powered on as non-FT virtual machine. It can be configured as an SMP-FT virtual machine after failover by using tools outside Site Recovery Manager.

- Fault tolerant virtual machines are not supported on NFS datastores.

ESXi Host Requirements for Protection of WSFC Virtual Machines

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

- You can run a cluster of WSFC virtual machines in the following possible configurations.

  ### Cluster-in-a-box

  The WSFC virtual machines in the cluster run on a single ESXi host. You can have a maximum of five WSFC nodes on one ESXi host.

  ### Cluster-across-boxes

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

DRS Requirements for Protection of WSFC Virtual Machines

To use DRS on sites that contain WSFC 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 WSFC virtual machines on sites that run DRS if the placeholder virtual machines are in either a cluster-across-boxes WSFC deployment or in a cluster-in-a-box WSFC deployment.

- 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 WSFC 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 WSFC 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 WSFC virtual machines to different ESXi hosts.

- In a cluster-across-boxes deployment on either the protected or recovery site, vSphere vMotion might move some or all of the WSFC virtual machines to a single ESXi host.

Support for WSFC with Clustered VMDKs

Site Recovery Manager can protect WSFC with clustered virtual machine disk files. vSphere 7.0 introduces support for the use of VMDKs on a clustered datastore as shared disk resources for a WSFC. Using VMDKs reduces the extra overhead to manage the virtual disks compared to pRDMs. For additional information about the supported configurations for a WSFC with shared disk resources, see *Setup for Windows Server Failover Clustering* in the *VMware vSphere Product Documentation*.

Using Site Recovery Manager with SIOC Datastores

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

Planned Migration of Virtual Machines on Datastores that Use SIOC

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

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

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

Using Site Recovery Manager with Admission Control Clusters

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

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

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

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

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

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

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

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

Site Recovery Manager and Virtual Machines Attached to RDM Disk Devices

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

Note   Site Recovery Manager does not support the protection of virtual machines attached to RDM devices in storage policy protection groups.

- Array-based replication supports RDM devices in physical compatibility mode and in virtual compatibility mode. If you use Site Recovery Manager with array-based replication, you can protect and recover virtual machines that use RDM in either physical compatibility mode or virtual compatibility mode.

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

- If you use both array-based replication and vSphere Replication, you can only protect and recover virtual machines that use RDM in physical compatibility mode by using array-based replication. You can protect and recover virtual machines that use RDM in virtual compatibility mode by using either array-based replication or vSphere Replication.

Site Recovery Manager and Active Directory Domain Controllers

Site Recovery Manager can support the protection of virtual machines that are serving as Active Directory domain controllers like any other application supported with Site Recovery Manager.

As an alternative to the native Active Directory replication technology and restores mode, you can use Site Recovery Manager to protect an Active Directory infrastructure in a disaster scenario. If you experience any problems, they might be related to specific network configurations and domain controller interdependencies.

Advanced Site Recovery Manager Configuration

12

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

Read the following topics next:

- Reconfigure Site Recovery Manager Settings
- Modify Settings to Run Large Site Recovery Manager Environments

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 If you previously installed Site Recovery Manager for Windows and you upgrade to Site Recovery Manager for Windows, during an upgrade, Site Recovery Manager for Windows 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 for Windows might not be required by or compatible with the new version. Similarly, if you uninstall then reinstall the same version of Site Recovery Manager for Windows, reusing the database from the previous installation, advanced settings are not retained.

Change Connections Settings

Site Recovery Manager communicates with other services.

Procedure

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

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

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

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

Option	Action
Change the number of failed pings before raising a site down event. The default value is 5.	Enter a new value in the **connections.hmsPanicDelay** text box.
Change the number of status checks (pings) to try before declaring the check a failure. The default value is 2.	Enter a new value in the **connections.hmsPingFailedDelay** text box.
Configure the maximum number of replication groups in a single VASA provider call. If set to zero, the replication group operations are not split in batches.	Enter a new value in the **connections.smsGroupBatchSize** text box.
Configure the number of times to retry the VASA provider calls. The default value is 30.	Enter a new value in the **connections.smsGroupOpRetryCount** text box.
Change the timeout value for the wait time for updates from servers. The default value is 900 seconds.	Enter a new value in the **connections.waitForUpdatesTimeout** text box.

5   To save your changes, click **OK**.

Change Site Recovery Manager History Report Collection Setting

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

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

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

Prerequisites

▪   Verify that you have Administrator credentials.

▪   Site Recovery Manager must be connected to a Site Recovery Manager database that you can access with valid database credentials.

Procedure

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

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

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

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

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

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

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

7   To save your changes, click **OK**.

Change Local Site Settings

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

Procedure

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

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

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

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

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

Option	Action
Change the percentage of free disk space that causes Site Recovery Manager to raise a low disk space event. The default value is 100 Mb.	Enter a new value in the **localSiteStatus.minDiskSpace** text box.
Change the amount of free memory that causes Site Recovery Manager to raise a low memory event. The default value is 32 MB.	Enter a new value in the **localSiteStatus.minMemory** text box.

5   To save your changes, click **OK**.

Change Logging Settings

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

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

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

none

Turns off logging.

quiet

Records minimal log entries.

panic

Records only panic log entries. Panic messages occur in cases of complete failure.

error

Records panic and error log entries. Error messages occur in cases of problems that might or might not result in a failure.

warning

Records panic, error, and warning log entries. Warning messages occur for behavior that is undesirable but that might be part of the expected course of operation.

info

Records panic, error, warning, and information log entries. Information messages provide information about normal operation.

verbose

Records panic, error, warning, information, and verbose log entries. Verbose messages provide more detailed information than information messages.

trivia

Records panic, error, warning, information, verbose, and trivia log entries. Trivia messages provide all available information. This level of logging is useful for debugging but it can produce so much data that it might affect performance.

Note Set this logging level only when instructed by VMware Support to help resolve a problem.

Procedure

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

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

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

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

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

Option	Description
Set logging level for all components that do not have an entry in logManager. The default is verbose.	Select a logging level from the **logManager.Default** drop-down menu.
Set logging level for the external API module. The default is verbose.	Select a logging level from the **logManager.ExternalAPI** drop-down menu.
Set logging level for vSphere Replication. The default is verbose.	Select a logging level from the **logManager.HbrProvider** drop-down menu.
Set logging level for the IP Customizer tool. The default is verbose.	Select a logging level from the **logManager.IPCustomizer** drop-down menu.
Set logging level for inventory mapping. The default is verbose.	Select a logging level from the **logManager.InventoryMapper** drop-down menu.
Set logging level for licensing issues. The default is verbose.	Select a logging level from the **logManager.Licensing** drop-down menu.
Set logging level for persistence issues. The default is verbose.	Select a logging level from the **logManager.Persistence** drop-down menu.
Set logging level for recovery operations. The default is trivia.	Select a logging level from the **logManager.Recovery** drop-down menu. By default, recovery logging is set to **trivia**.

Option	Description
Set logging level for recovery configuration operations. The default is verbose.	Select a logging level from the **logManager.RecoveryConfig** drop-down menu.
Set logging level for array-based replication operations. The default is verbose.	Select a logging level from the **logManager.Replication** drop-down menu.
Set logging level for authorization issues between Site Recovery Manager Server and vCenter Server. The default is verbose.	Select a logging level from the **logManager.ServerAuthorization** drop-down menu.
Set logging level for session management. The default is verbose.	Select a logging level from the **logManager.SessionManager** drop-down menu.
Set logging level for the SOAP Web Services adapter. The default is info.	Select a logging level from the **logManager.SoapAdapter** drop-down menu. Due to the levels of traffic that the SOAP adapter generates, setting the logging level to **trivia** might affect performance. By default, SOAP adapter logging is set to **info**.
Set logging level for storage issues. The default is verbose.	Select a logging level from the **logManager.Storage** drop-down menu.
Set logging level for messages from the array-based storage provider. The default is verbose.	Select a logging level from the **logManager.StorageProvider** drop-down menu.
Set logging level for messages from the Virtual Volumes storage provider. The default is verbose.	Select a logging level from the **logManager.VvolProvider** drop-down menu.

5   To save your changes, click **OK**.

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

Change Recovery Settings

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

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

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

- `recovery.autoDeployGuestAlias`

- `recovery.defaultPriority`

- `recovery.powerOnTimeout`

- `recovery.powerOnDelay`

- `recovery.customizationShutdownTimeout`

- `recovery.customizationTimeout`

- `recovery.skipGuestShutdown`

- `recovery.powerOffTimeout`

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

Procedure

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

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

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

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

Option	Action
Enable or disable the automatic configuration of guest user mappings. This option is available only for VMs that use a compatible version of VMware Tools. The default value is true. **For information about the compatible versions of VMware Tools, see** *Compatibility Matrices for Site Recovery Manager 8.3.*	Select the value of **recovery.autoDeployGuestAlias** to enable or disable the automatic configuration of guest user mappings. If the value is true, Site Recovery Manager creates guest user mappings in the guest OS of all VMs during the recovery and removes them when the recovery finishes. To use this option, you must install a compatible version of VMware Tools and must configure the IP customization or in-guest callout operations on the VMs that you want to recover. Before you run the recovery process, you must ensure the time synchronization between the ESXi hosts and the vCenter Single Sign-On server on the recovery site. If the value is false, you must manually map the local Site Recovery Manager solution user on the recovery site to a guest user account on the protected VM. The guest OS user must have permissions to run commands and access to files in the gust OS. If you configure an IP customization or in-guest callout operations, you must ensure the time synchronization between the guest OS of the protected VM and the vCenter Single Sign-On servers on the recovery site. If your Site Recovery Manager sites are in enhanced linked mode, you can use vSphere Web Client to configure the guest user mappings. For information about how to configure guest user mappings, see the *Configuring User Mappings on Guest Operating Systems* chapter in the *VMware vSphere ESXi and vCenter Server* documentation. If your Site Recovery Manager sites are not in enhanced linked mode, you must use a vSphere API to configure the guest user mappings and to ensure that the alias certificate is mapped. The best practice is to use the signing certificates of the vCenter Single Sign-On server. For information about the vSphere API, see the *VMware vSphere API Reference* documentation.
Change the virtual machine power off timeout in IP customization. The default value is 300 seconds.	Enter a new value in the **recovery.customizationShutdownTimeout** text box. This value is the minimal virtual machine power off timeout in seconds used in IP customization workflow only. If you specify power off timeout in virtual machine recovery settings, the greater value of the two takes precedence.
Change the IP customization timeout. The default value is 600 seconds.	Enter a new value in the **recovery.customizationTimeout** text box. This value is the timeout used in preparation of IP customization scripts on the Site Recovery Manager Server. You rarely need to change this value.
Change the default priority for recovering a virtual machine. The default value is 3.	Enter a new value in the **recovery.defaultPriority** text box.
Enable or disable forced recovery. The default value is false.	Move the slider to change the value of **recovery.forceRecovery** to true. Activate forced recovery in cases where a lack of connectivity to the protected site severely affects RTO. This setting only removes the restriction to select forced recovery when running a recovery plan. To actually enable forced recovery, select it when you run a plan.
Change the timeout for hosts in a cluster to power on. The default value is 1200 seconds.	Enter a new value in the **recovery.hostPowerOnTimeout** text box.

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

5 To save your changes, click **OK**.

What to do next

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

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

Apply Recovery Settings to Virtual Machines in a Recovery Plan

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

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

Procedure

1 On the **Site Recovery** home tab, select a site pair, and click **View Details**.

2 Select the **Recovery Plans** tab, and click on the recovery plan to which the virtual machine belongs.

3 On the **Virtual Machines** tab, right-click a virtual machine and click **Configure Recovery**.

4 Make the changes you want to the recovery properties settings.

5 Click **OK**.

What to do next

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

Apply Recovery Settings to Virtual Machines in a Protection Group

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

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

Procedure

1 On the **Site Recovery** home tab, select a site pair, and click **View Details**.

2 Select the **Protection Groups** tab, and click on the protection group to which the virtual machine belongs.

3 On the **Virtual Machines** tab, right-click a virtual machine and click **Remove Protection**.

The virtual machine status changes to Not Configured.

4 Click **Configure All VMs** to reconfigure all virtual machines in the protection group, or select a virtual machine and click **Configure Protection** to reconfigure only that virtual machine.

What to do next

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

Change Remote Manager Settings

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

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

Procedure

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

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

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

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

Option	Action
Configure the maximum time to wait for a remote operation to complete. The default value is 900 seconds.	Enter a new value in the **remoteManager.defaultTimeout** text box.
Mark a virtual machine as protected by Site Recovery Manager. The default value is true.	Move the slider to change the value of **remoteManager.enableCustomFields**.
Set a time period to wait for requests to aggregate at the remote site. The default value is 2000 milliseconds.	Enter a new value in the **remoteManager.powerOnAggregationInterval** text box.
Configure the maximum time to wait for canceled tasks to stop. The default value is 300 seconds.	Enter a new value in the **remoteManager.taskCancelDefaultTimeout** text box.
Configure an additional timeout period for tasks to complete on the remote site. The default value is 900 seconds.	Enter a new value in the **remoteManager.taskDefaultTimeout** text box.

Option	Action
Configure the number of seconds to wait for a remote task to report progress. For each remote task, the specified timeout is the minimum amount of time that Site Recovery Manager waits for the remote task to complete. If progress update is received within that time, the task is allowed more time to complete. The default value is 180 seconds.	Enter a new value in the **remoteManager.taskProgressDefaultTimeout** text box.
Configure the number of attempts to power on a virtual machine in case of failure. The default value is 5 times.	Enter a new value in the **remoteManager.vmPowerOnRetryCount** text box.
Configure the number of attempts to shut down the guest OS of a virtual machine in case of failure. The default value is 5 times.	Enter a new value in the **remoteManager.vmGuestShutDownRetryCount** text box.
Configure the number of attempts to reconfigure a virtual machine's settings in case of failure. The default value is 5 times.	Enter a new value in the **remoteManager.vmReconfigureRetryCount** text box
Configure the number of seconds to wait for a timeout of xVC-vMotion. The default value is 3600 seconds.	Enter a new value in the **remoteManager.xVcVMotionTimeout** text box.

5 To save your changes, click **OK**.

Change Remote Site Settings

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

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

Procedure

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

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

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

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

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

5 To save your changes, click **OK**.

Change Replication Settings

You can edit replication settings to modify how long Site Recovery Manager waits for the creation of virtual machine placeholders to finish. You can modify the protection polling interval of virtual machines in storage policy protection groups.

Procedure

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

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

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

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

Option	Action
Skip the check for non-protected replica virtual machines while deactivating the protection site during Planned Migration. The default value is false.	Move the slider to change the value **replication.disablePiggybackVmsCheckDuringDeactivate**.
Change the timeout in seconds to wait when creating a placeholder virtual machine. The default value is 300 seconds.	Enter a new value in the **replication.placeholderVmCreationTimeout** text box.
Periodically poll the virtual machines in storage policy protection groups for missing mappings and report a warning if any mappings are missing that can cause the storage policy protection group recovery to fail. The default value is false.	Move the slider to change the value **replication.pollForMissingInventoryMappings** to true.
Enable or disable the preservation of VM Tags on the recovery site for recovered virtual machines. The default value is true.	Move the slider to change the value **replication.preserveVmTags** to false. **Note** To attach tags to recovered virtual machines on the recovery site, the setting must be set to true on the recovery site.

Option	Action
Change the timeout in seconds to wait for consistency group information to be replicated to the remote site before starting an online sync on that site. The default is 900 seconds.	Enter a new value in the **replication.protectionInfoSyncTimeout** text box.
Change the interval in seconds to poll the storage policy protection groups and missing inventory mappings. The default value is 120 seconds.	Enter a new value in the **replication.protectionPollInterval** text box. **Note** Before you update the polling interval, estimate the changes in your environment, their frequency, and the performance of the environment.

5   To save your changes, click **OK**.

Change SSO Setting

You can modify the Single Sign On setting for Site Recovery Manager to renew SSO tokens.

Procedure

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

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

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

4   Select a site, and click **Edit** to change the **sso.sts.tokenLifetime** setting to specify the number of seconds to use SSO tokens before they are renewed.

The default value is 28800 seconds (8 hours).

5   To save your changes, click **OK**.

Change Storage Settings

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

Procedure

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

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

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

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

Option	Action
Change the time in seconds to wait before attempting to attach tags to recovered datastores. The default value is 30 seconds.	Enter a new value in the **storage.attachTagsDelaySec** text box.
Change timeout in seconds for running an SRA command. The default value is 300 seconds.	Enter a new value in the **storage.commandTimeout** text box.
Change timeout in seconds between datastore monitoring related operations. The default value is 30 seconds.	Enter a new value in the **storage.datastoreMonitoringPollingInterval** text box.
Allow Site Recovery Manager to create tag categories and the Replicated tag that Storage DRS compatibility requires. The default value is true.	Move the slider to change the value of **storage.enableSdrsStandardTagCategoryCreation**.
Allow Site Recovery Manager to automatically create and attach tags to replicated or protected datastores for Storage DRS compatibility. The default value is true.	Move the slider to change the value of **storage.enableSdrsTagging**. If you change the value to false, Site Recovery Manager deletes all the tags and tag categories and breaks compatibility with Storage DRS.
Allow Site Recovery Manager to repair missing or incorrect tags on replicated or protected datastores for Storage DRS compatibility. The default value is true.	Move the slider to change the value of **storage.enableSdrsTaggingRepair** check box.
Change the maximum number of concurrent SRA operations. The default value is 5.	Enter a new value in the **storage.maxConcurrentCommandCnt** text box.
Change the maximum length in bytes of the SRA command console output to log. The default value is 1048576 bytes (1 MB).	Enter a new value in the **storage.maxSraCommandOutputLength** text box. ■ A value of 0 means no SRA output log. ■ A value of -1 means unlimited length. ■ If you enter a value that is different from 0, -1, and it is not within the interval between 512 bytes and 10 MB, the value is automatically set to the default 1 MB.
Change the minimum amount of time in seconds between datastore group computations. The default value is 0.	Enter a new value in the **storage.minDsGroupComputationInterval** text box.
Change the interval between status updates for ongoing data synchronization operations. The default value is 30 seconds.	Enter a new value in the **storage.querySyncStatusPollingInterval** text box.

Option	Action
Change the interval between Storage DRS tagging-related operations. The default value is 50 seconds.	Enter a new value in the **storage.sdrsTaggingPollInterval** text box.
Change the interval between storage array discovery checks. The default value is 86400 seconds (24 hours).	Enter a new value in the **storage.storagePingInterval** text box.
Change the maximum amount of time permitted for data synchronization operations to complete. The default value is 86400 seconds (24 hours).	Enter a new value in the **storage.syncTimeout** text box.

5   To save your changes, click **OK**.

Change ABR Storage Policy Setting

You can modify the ABR Storage Policy setting to specify the interval (in seconds) to perform auto-discovery of datastores that match a virtual machine storage policy.

Procedure

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

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

3   In the left pane, click **Configure > Advanced Settings > ABR Storage Policy**.

4   Select a site, and click **Edit**.

5   Change the value for **storagePolicyAbrReplication.policyDatastorePollInterval** as needed. The default value is 20 seconds.

6   To save your changes, click **OK**.

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 in seconds. For more information about these values, see the SRA documentation from your array vendor.

Procedure

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

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

3 In the left pane, click **Configure > Advanced Settings > Storage Provider**.

4 Select a site, and click **Edit** to modify the storage provider settings.

Option	Action
Make Site Recovery Manager attempt to detach and reattach LUNs with duplicate volumes. The default value is true.	Move the slider to change the value of **storageProvider.autoDetachLUNsWithDuplicateVolume**.
Set the `LVM.EnableResignature` flag on ESXi hosts during test and recovery. The default value is 0.	In the **storageProvider.autoResignatureMode** text box, enter **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.
Change the timeout in seconds to wait for Batch Attach LUN operation to complete on each ESXi host. The default value is 3600 seconds.	Enter a value in the **storageProvider.batchAttachTimeoutSec** text box.
Change the timeout in seconds to wait for Batch Detach LUN operation to complete on each ESXi host. The default value is 3600 seconds.	Enter a value in the **storageProvider.batchDetachTimeoutSec** text box.
Change the interval that Site Recovery Manager waits for VMFS volumes to be mounted. The default value is 3600 seconds.	Enter a new value in the **storageProvider.batchMountTimeoutSec** 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.
Change the interval that Site Recovery Manager waits for VMFS volumes to be unmounted. The default value is 3600 seconds.	Enter a new value in the **storageProvider.batchUnmountTimeoutSec** text box. Change this value if you experience timeouts caused by Site Recovery Manager checking for VMFS volumes that take a long time to unmount. This setting is available in Site Recovery Manager 5.5.1 and later.
Set number of retries for batch unmount of VMFS/NFS volumes. The default is 3 tries.	Enter a new value in the **storageProvider.datastoreUnmountRetryCount** text box.
Change the interval that Site Recovery Manager waits before attempting to unmount the datastore. The default is 1 second.	Enter a new value in the **storageProvider.datastoreUnmountRetryDelaySec** text box.
Change the time in seconds to wait before fetching datastores on the ESXi hosts after receiving an SRA response during test and recovery. This setting applies only when there are no SCSI devices. The default value is 0.	Enter a new value in the **storageProvider.fetchDatastoreDelaySec** text box.

Option	Action
Force removal, upon successful completion of a recovery, of the `snap-xx` prefix applied to recovered datastore names. The default value is false.	Move the slider to change the value of **storageProvider.fixRecoveredDatastoreNames**.
Change the time that Site Recovery Manager waits before removing the `snap-xx` prefix applied to recovered datastore names. The default value is 0 seconds.	Enter a new value in the **storageProvider.fixRecoveredDatastoreNamesDelaySec** text box.
Change the time interval between SMP-FT VM datastore compliance checks. The default value is 300 seconds.	Enter a new value in the **storageProvider.ftVmComplianceCheckInterval** text box.
Delay host scans during testing and recovery. The default value is 0 seconds.	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, enter 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. The default value is 1.	Enter 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. The default value is 300 seconds.	Enter a new value in the **storageProvider.hostRescanTimeoutSec** text box.
Set the number of times that Site Recovery Manager attempts to resignature a VMFS volume. The default value is 1.	Enter a new value in the **storageProvider.resignatureFailureRetryCount** text box.
Set a timeout for resignaturing a VMFS volume. The default value is 900 seconds.	Enter 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**.

Option	Action
Identify VMX file paths that Site Recovery Manager should not consider as potential VMX file candidates after Storage vMotion. The default value is .snapshot,	Enter 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.
Set the timeout in seconds for local stretched devices to be matched to the corresponding remote stretched devices. The default is 300 seconds.	Enter the new value in the **storageProvider.stretchedDevicesMatchTimeout** text box.
Set the number of parallel xVC-vMotion requests per host. This limit applies to both source and target hosts. The default value is 2.	Enter the new value in the **storageProvider.vmMigrationLimitPerHost** text box.
Set the timeout in seconds to wait for newly discovered datastores to become accessible. The default value is 60 seconds.	Enter the new value in the **storageProvider.waitForAccessibleDatastoreTimeoutSec** text box.
Enable Site Recovery Manager to wait to discover datastores after recovery. The default value is false.	Move the slider to change the value of **storageProvider.waitForDeviceRediscovery** to true.
Enable Site Recovery Manager to wait to discover datastores after failover. The default value is true.	Move the slider to change the value of **storageProvider.waitForDeviceRediscoveryAfterPrepareFailover** to false.
Set the timeout in seconds to wait for the Virtual Center to report newly discovered datastores. The default value is 30 seconds.	Enter the new value in the **storageProvider.waitForRecoveredDatastoreTimeoutSec** text box.
Set the time interval in seconds that Site Recovery Manager waits for VMFS volumes to become mounted. The default value is 30 seconds.	Enter the new value in the **storageProvider.waitForVmfsVolumesMountedStateTimeoutSec** text box.

5   To save your changes, click **OK**.

Change vSphere Replication Settings

You can adjust global settings to change how Site Recovery Manager interacts with vSphere Replication.

Procedure

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

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

3   In the left pane, click **Configure > Advanced Settings > vSphere Replication**.

4 Select a site, and click **Edit** to modify the vSphere Replication settings.

Option	Description
Allow Site Recovery Manager to recover virtual machines that are managed by other solutions. The default value is false.	vSphere Replication allows solutions to manage the replication of virtual machines. By default, Site Recovery Manager only recovers the virtual machines that it manages. To allow Site Recovery Manager to recover virtual machines whose replications are managed by other solutions, move the slider of **vrReplication.allowOtherSolutionTagInRecovery** to true.
Keep older multiple point in time (PIT) snapshots during recovery. The default value is true.	If you configure vSphere Replication to take PIT snapshots of protected virtual machines, Site Recovery Manager only recovers the most recent snapshot when you perform a recovery. To recover older PIT snapshots during recovery, use the slider to set the value of **vrReplication.preserveMpitImagesAsSnapshots** to true.
Change the timeout period for reverse replication during reprotect operations	Type a new value in the **vrReplication.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. The default value is 7200.	Enter a new value in the **vrReplication.synchronizationTimeout** text box. The value that you enter must be half of the timeout time that you want to set. The default value is 7200 and corresponds to a working synchronization timeout period of 14400 seconds. Change this value if you experience timeout errors when vSphere Replication synchronizes virtual machines on the recovery site.

5 To save your changes, click **OK**.

Change the Automatic Protection Settings

You can adjust the automatic protection settings to modify how Site Recovery Manager handles the automatic protection of virtual machines.

Procedure

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

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

3 In the left pane, click **Configure > Advanced Settings > Automatic Protection**.

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

Option	Action
Enable or disable the automatic protection for array-based replication protection groups. The default value is true.	Move the slider to change the value of **autoprotect.abrEnabled**.
Configure the backoff delay value in seconds. The default value is 60 seconds. This setting determines the interval between two automatic protection attempts equal to currentRetryAttempt * retryBackOffDelay.	Enter a new value in the **autoprotect.retryBackoffDelay** text box.
Configure the number of retry attempts for a failed automatic protection operation. The default number is 5.	Enter a new value in the **autoprotect.retryCount** text box.
Set the local account that Site Recovery Manager uses to check the local vCenter Server and Site Recovery Manager permissions when applying automatic protection to virtual machines and virtual machine templates.	Enter a new value in the **autoprotect.username** text box. When left empty, Site Recovery Manager uses a default user.
Enable or disable the automatic protection for Virtual Volumes protection groups. The default value is true.	Move the slider to change the value of **autoprotect.vvolEnabled**.

5 To save your changes, click **OK**.

Change the Virtual Volumes Replication Settings

You can adjust the Virtual Volumes Replication settings to modify how Site Recovery Manager handles the replication of virtual machines on a Virtual Volumes storage.

Procedure

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

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

3 In the left pane, click **Configure > Advanced Settings > Virtual Volumes Replication**.

4 Select a site and click **Edit** to modify the Virtual Volumes replication settings.

Option	Action
Configure the time between Virtual Volumes configuration updates. The default value is 60 seconds.	Enter a new value in the **vvolReplication.agentScanTimerSeconds** text box.
Configure the timeout in seconds for Virtual Volumes storage synchronization operations. The default value is 0.	Enter a new value in the **vvolReplication.syncReplicationGroupTimeoutSeconds** text box.
Configure the timeout to wait for updating the virtual machine files on Virtual Volumes storage. The default value is 7200.	Enter a new value in the **vvolReplication.updateVirtualMachineFilesTimeout** text box.

5 To save your changes, click **OK**.

Change Telemetry Settings

You can edit the Site Recovery Manager telemetry settings to specify a proxy host to use when sending telemetry reports.

Procedure

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

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

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

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

Option	Description
Specify the host name of the HTTP proxy to use when sending telemetry reports.	Enter the name of the HTTP proxy in the **telemetry.proxyHost** text box.
Specify the port for the HTTP proxy to use when sending telemetry reports.	Enter the port number in the **telemetry.proxyPort** box.
Specify whether to use SSL to connect to the HTTP proxy when sending telemetry reports. The default value is false.	Move the slider to change the value **telemetry.proxyUseSsl** to true.

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

Modify Settings to Run Large Site Recovery Manager Environments

If you use Site Recovery Manager to test or recover a large number of virtual machines, you might need to modify the default Site Recovery Manager settings to achieve the best possible recovery times in your environment or to avoid timeouts.

In large environments, Site Recovery Manager might simultaneously power on or power off large numbers of virtual machines. Simultaneously powering on or powering off large numbers of virtual machines can create a heavy load on the virtual infrastructure, which might lead to timeouts. You can modify certain Site Recovery Manager settings to avoid timeouts, either by limiting the number of power on or power off operations that Site Recovery Manager performs concurrently, or by increasing the timeout periods.

The limits that you set on power on or power off operations depend on how many concurrent power on or power off operations your infrastructure can handle.

You modify certain options in the **Advanced Settings** menus in the vSphere Web Client or in the Site Recovery Manager client plug-in. To modify other settings, you edit the `vmware-dr.xml` configuration file on the Site Recovery Manager Server or on the Site Recovery Manager Virtual Appliance. Always modify settings by using the client menus when such option exists. If you modify settings, you must make the same modifications on the Site Recovery Manager and the vCenter Server instances on both the protected and recovery sites.

For descriptions of the settings that you can change, see Settings for Large Site Recovery Manager Environments.

Procedure

1 In the vSphere Web Client or the vSphere Client, select a cluster.

2 On the **Configure** tab, select **Services > vSphere DRS**.

   If you are using vCenter Server 6.0 Update 3, on the **Manage** tab, select **Services > vSphere DRS**

3 Click **Edit**.

4 In **Advanced Options**, set the `srmMaxBootShutdownOps` setting.

Option	Description
Option text box	Enter `srmMaxBootShutdownOps`.
Value text box	Enter the maximum number of concurrent startup and shutdown operations. If you set the value to 32, for example, this means that VMs 1 to 32 start up or shut down together, and that VM 33 starts up or shuts down as soon as one of the first-batch VMs has finished. VM 34 starts up when the second VM of the first batch has finished, and so on.

5 To save your changes, click **OK**.

6   Log in to the Site Recovery Manager Server host.

7   Open the `vmware-dr.xml` file in a text editor.

- If you are using Site Recovery Manager for Windows, you find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder on the Site Recovery Manager Server host machine.

- If you are using the Site Recovery Manager Virtual Appliance, you find the `vmware-dr.xml` file in the `/opt/vmware/srm/conf/` directory on the appliance.

8   Change the `defaultMaxBootAndShutdownOpsPerCluster` and `defaultMaxBootAndShutdownOpsPerHost` settings in the `vmware-dr.xml` file:

```
<config>
...
   <defaultMaxBootAndShutdownOpsPerCluster>24</defaultMaxBootAndShutdownOpsPerCluster>
   <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
...
</config>
```

If these elements do not already exist in the `vmware-dr.xml` file, you can add them anywhere in the `<config>` section.

If you set the `<defaultMaxBootAndShutdownOpsPerCluster>` value to 24, the next guest starts up or shuts down as soon as one of the first batch of 24 has finished. This means that VMs 1 to 24 all start together, then VM 25 starts once one of the first-batch VMs has finished. VM 26 starts when the second VM of the first batch has finished, and so on.

9   To apply the new settings, restart Site Recovery Manager Server.

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

11   On the **Site Recovery** home tab, select a site pair, and click **View Details**.

12   In the left pane, click **Configure > Advanced Settings > vSphere Replication** and increase the `vrReplication.synchronizationTimeout` and `vrReplication.reverseReplicationTimeout` settings.

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

13   Select **Advanced Settings > Storage**, select a site, and increase the `storage.commandTimeout` setting.

The default value is 300 seconds.

14   To save your changes, click **OK**.

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 Web Client or in the Site Recovery Manager client plug-in. To modify other settings, you edit the `vmware-dr.xml` configuration file on the Site Recovery Manager Server or on the Site Recovery Manager Virtual Appliance. Always modify settings by using the client menus when such option exists. If you modify settings, you must make the same modifications on the Site Recovery Manager and the vCenter Server instances on both the protected and recovery sites.

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

Table 12-1. Settings that Modify the Number of Simultaneous Power On or Power Off Operations

Option	Description
srmMaxBootShutdownOps	Specifies the maximum number of concurrent power-on operations for any given cluster. Guest shutdowns, but not forced power offs, are throttled according to this value. Guest shutdowns occur during primary site shutdowns (planned failover) and IP customization workflows. Modify this option per cluster in the vSphere Web Client or the vSphere Client by right-clicking a cluster and selecting **Settings**. Click **vSphere DRS**, then **Edit > Advanced Options**. Type the option to override the **defaultMaxBootAndShutdownOpsPerCluster** value that you can set in the `vmware-dr.xml` file. You can set a global value **defaultMaxBootAndShutdownOpsPerCluster** in the `vmware-dr.xml` file, and then set different **srmMaxBootShutdownOps** values for individual clusters in the vSphere Web Client or 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 Web Client overrides the **defaultMaxBootAndShutdownOpsPerCluster** value. You can set a global value **defaultMaxBootAndShutdownOpsPerCluster** in the `vmware-dr.xml` file, and then set different **srmMaxBootShutdownOps** values for individual clusters in the vSphere Web Client. By default, throttling is turned off.
defaultMaxBootAndShutdownOpsPerHost	Specifies the maximum number of concurrent power-on operations on any standalone host. You can only set the option in the `vmware-dr.xml` file. By default, throttling is turned off.

Table 12-2. Settings that Modify Timeout Periods

Option	Description
vrReplication.synchronizationTimeout	Site Recovery Manager enforces a timeout to complete an online or offline synchronization for virtual machines replicated by vSphere Replication during a test or failover. If a synchronization does not finish within the given timeout, for example, because of a slow network or a large virtual machine, Site Recovery Manager reports a failure during a test or failover. Modify this option in the Site Recovery user interface. On the Site Recovery home tab, select a site pair and click **View Details**. In the left pane, select **Configure > Advanced Settings > vSphere Replication**. The default value is 7200 and corresponds to a working synchronization timeout period of 14400 seconds.
vrReplication.reverseReplicationTimeout	The timeout period for reverse replication during reprotect operations. Modify this option in the Site Recovery user interface. On the Site Recovery home tab, select a site pair and click **View Details**. In the left pane, select **Configure > Advanced Settings > vSphere Replication**. The default value is 7200 and corresponds to a working synchronization timeout period of 14400 seconds.
storage.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 the Site Recovery user interface. On the Site Recovery home tab, select a site pair and click **View Details**. In the left pane, select **Configure > Advanced Settings > Storage**. The default value is 300 seconds.

Site Recovery Manager Events and Alarms

13

Site Recovery Manager supports event logging. Each event includes a corresponding alarm that Site Recovery Manager can trigger if the event occurs. This provides a way to track the health of your system and to resolve potential issues before they affect the protection that Site Recovery Manager provides.

Read the following topics next:

- How Site Recovery Manager Monitors Connections Between Sites
- Create Site Recovery Manager Alarms

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` event.

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.

- The connection monitor skips a number of failed pings. You can configure this number by setting the `remoteSiteStatus.drPingFailedDelay` value. The default is 2.

- When the number of skipped failed pings exceeds the value of the `remoteSiteStatus.drPingFailedDelay` 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.drPanicDelay` setting. The default is 5.

- Site Recovery Manager continues to send `RemoteSiteDownEvent` events until the connection is reestablished.

■ When a connection to the remote site Site Recovery Manager Server is reestablished, Site Recovery Manager sends `RemoteSiteUpEvent` events.

Create 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 **Alarm Definitions** tab lists all 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.

Note In an environment with more than one vCenter Server, Site Recovery Manager displays all events from the Site Recovery Manager Servers that are registered as extensions, even if you select events for a specific vCenter Server.

Prerequisites

For alarms to send email notifications, configure the **Mail** settings in the **vCenter Server Settings** menu. See *ESXi and vCenter Server Documentation*.

Procedure

1 In the vSphere Client, click a vCenter Server.

2 In the **Configure** tab, expand **More** and click **Alarm Definitions** to display the list of vCenter Server alarms.

3 Click **Add** to add a new alarm.

4 On the **Name** page, enter an alarm name, description, and click **Next**.

5 On the **Targets** page, select a target from the drop-down menu, and click **Next**.

6 On the **Alarm Rule** page, select an event from the drop-down menu and the corresponding status.

If you see repeated events in the list, each event represents a single Site Recovery Manager instance and triggers an alarm for the extension with which it is registered. For example, in a scenario with multiple Site Recovery Manager instances, you can use `RecoveryPlanCreated (SRM 1)` and `RecoveryPlanCreated (SRM 2)` for the same event on both extensions.

7 To add a condition that triggers the alarm, click **Add Argument**, select an argument from the drop-down menu, the operator, and the transition from warning to critical condition.

8 (Optional) Select to send email notifications, SNMP traps, or to run a script.

9 Click **Next**.

10 On the **Review** page, select whether to enable the alarm, and click **Create**.

Site Recovery Manager Events Reference

Site Recovery Manager monitors different types of events.

Site Status Events

Site status events provide information about the status of the protected and recovery sites and the connection between them.

Table 13-1. Site Status Events

Event Name	Event Type	Event Description	Category
Unknown status	UnknownStatusEvent	Site Recovery Manager Server status is not available	Info
Remote site down	RemoteSiteDownEvent	Site Recovery Manager Server has lost its connection with the remote Site Recovery Manager Server.	Error
Remote site ping failed	RemoteSitePingFailedEvent	Failures at the remote site or network connectivity problems.	Warning
Remote site created	RemoteSiteCreatedEvent	Local site has been successfully paired with the remote site.	Info
Remote site up	RemoteSiteUpEvent	Site Recovery Manager Server re-establishes its connection with the remote Site Recovery Manager Server.	Info
Remote site deleted	RemoteSiteDeletedEvent	Remote Site Recovery Manager site has been deleted.	Info
vSphere Replication replicated virtual machine is added to a protection group	HbrGroupVmAssociatedEvent	A virtual machine replicated by vSphere Replication is added to a protection group.	Info
vSphere Replication replicated virtual machine is removed from a protection group	HbrGroupVmDisassociatedEvent	A virtual machine replicated by vSphere Replication is removed from a protection group.	Info
Local vSphere Replication Server is down	LocalHmsConnectionDownEvent	Repeated connection attempts to vSphere Replication fail.	Error
The connection to the local vSphere Replication Server has been restored	LocalHmsConnectionUpEvent	Connection to vSphere Replication is successful.	Info
The local vSphere Replication Server is not responding	LocalHmsPingFailedEvent	Failure to establish connection to the local vSphere Replication Server	Warning
Low disk space	LowDiskSpaceEvent	Free disk space on the local site is low.	Warning

Table 13-1. Site Status Events (continued)

Event Name	Event Type	Event Description	Category
Low memory	`LowMemoryEvent`	Available memory on the local site is low.	Warning
SRM Server certificate not yet valid	`SrmCertificateNotValidEvent`	The SSL/TLS certificate for the specified SRM Server is in the future.	Error
SRM Server certificate expiring	`SrmCertificateExpiringEvent`	The SSL/TLS certificate for the specified SRM Server expires in the specified number of days.	Info
SRM Server certificate has expired	`SrmCertificateExpiredEvent`	The SSL/TLS certificate for the specified SRM Server has expired.	Error

Protection Group Events

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

Table 13-2. Protection Group Replication Events

Event	Description	Cause	Category
`ProtGroupCreatedEvent`	Created protection group.	Posted on both vCenter Servers in the completion of the Commit phase of creating a protection group.	Info
`ProtGroupRemovedEvent`	Removed protection group.	Posted on both vCenter Servers in the completion of the Commit phase of removing a protection group.	Info
`ProtGroupReconfiguredEvent`	Reconfigured protection group.	Posted on both vCenter Servers in the completion of the Commit phase of reconfiguring a protection group.	Info
`ProtectedVmCreatedEvent`	Virtual machine in group is configured for protection.	Posted on both vCenter Servers in the completion of the Commit phase of the protection of a virtual machine.	Info
`ProtectedVmRemovedEvent`	Virtual machine in group is no longer configured for protection.	Posted on both vCenter Servers in the completion of the Commit phase of unprotecting a virtual machine.	Info
`ProtVmReconfigProtEvent`	Reconfigured protection settings for virtual machine.	Posted on both vCenter Servers in the completion of the Commit phase of reconfiguring virtual machine protection settings.	Info
`ProtVmReconfigRecoLocEvent`	Reconfigured recovery location settings for virtual machine.	Posted on the protected site vCenter Server only on the successful completion of reconfiguring the recovery location settings for a protected virtual machine.	Info
`PholderVmCreatedEvent`	The placeholder virtual machine was created in the vCenter Server inventory.	Posted on the recovery site vCenter Server placeholder virtual machine is created as a result of protection, repair operation.	Info

Table 13-2. Protection Group Replication Events (continued)

Event	Description	Cause	Category
`PholderVmFromOldProdVmEvent`	The placeholder virtual machine was created in the vCenter Server inventory using the identity of the old protected virtual machine.	Posted on the recovery site vCenter Server placeholder virtual machine is created as a result of swapping the old protected virtual machine with a placeholder virtual machine during or after reprotect operation .	Info
`VmFullyProtectedEvent`	Virtual machine in group: Unresolved devices have all been resolved.	A protected virtual machine's previously unresolved devices have all been resolved.	Warning
`VmNotFullyProtectedEvent`	Virtual machine in group: One or more devices need to be configured for protection.	Posted on the protected site vCenter Server only upon device handling updating the recovery location settings with a non-empty unresolvedDevices set. This can be triggered by changes to the protected virtual machine or during reprotect of a virtual machine.	Warning
`PholderVmUnexpectDeleteEvent`	Virtual machine in group: The placeholder virtual machine was removed from the vCenter Server inventory.	Posted on the recovery site vCenter Server when Site Recovery Manager detects that the placeholder virtual machine was unexpectedly deleted or removed from the vCenter Server inventory.	Warning
`ProductionVmDeletedEvent`	Virtual machine in group: The protected virtual machine has been removed from the virtual machine vCenter Server inventory.	Posted when a protected virtual machine is deleted or removed from the vCenter Server inventory.	Error
PholderVmRemoveFailedEvent	Virtual machine in group: The placeholder virtual machine cannot be removed from the vCenter Server inventory.	Posted when the deletion of a placeholder virtual machine from the vCenter Server inventory during unprotect fails.	Error
`ProductionVmInvalidEvent`	Virtual machine in group: Cannot resolve the file locations of the protected virtual machine for replication.	Posted when the replication provider cannot find the protected virtual machine files in order to replicate them.	Error

Recovery Events

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

Table 13-3. Recovery Events

Event Name	Event Type	Event Description	Category
Recovery plan has begun recovering the specified virtual machine.	RecoveryVmBegin	Signaled when the recovery virtual machine was successfully created. If some error occurred before the virtual machine ID is known the event is not fired.	Info
Recovery plan has completed recovering the virtual machine.	RecoveryVmEnd	Signaled after the last post-power on script has completed, or after a recovery-stopping error has occurred for the virtual machine.	Info
Recovery Plan [data.Plan] failed registering virtual machine [data.Vm].	RecoveryVmRegisterFailed	Signaled in the case of SPPGs after a recovered VM has failed registration with the recovery site VC. If the plan is run against the local VC, then [data.local] will be true.	Info
Recovery plan *hostname* has been created.	PlanCreated	Signaled when a new plan is created. It is sent to each vCenter Server instance where the plan is hosted.	Info
Recovery plan has been destroyed.	PlanDestroy	Signaled when a plan has been deleted from the site. Note that on the site where the plan has been requested to be deleted there can be a significant delay, while it waits for the plan to be deleted at the other site. It will be sent to each vCenter Server instance where the plan is hosted.	Info
Recovery plan was changed.	PlanEdit	Signaled when an existing plan is edited.	Info
Recovery plan has begun a test.	PlanExecTestBegin	Signaled on the recovery site when a recovery test is initiated.	Info
Recovery plan has completed a test.	PlanExecTestEnd	Signaled on the recovery site when a recovery test has completed.	Info
Recovery plan has begun a test cleanup.	PlanExecCleanupBegin	Signaled on the recovery site when a test cleanup is initiated.	Info
Recovery plan has completed a test cleanup.	PlanExecCleanupEnd	Signaled on the recovery site when a test cleanup has completed.	Info
Recovery plan has begun a recovery.	PlanExecBegin	Signaled on the recovery site when a recovery is initiated.	Info
Recovery plan has completed a recovery.	PlanExecEnd	Signaled on the recovery site when a recovery has completed.	Info
Recovery plan has begun a reprotect operation.	PlanExecReprotectBegin	Signaled on the recovery site when a reprotect is initiated.	Info
Recovery plan has completed a reprotect operation.	PlanExecReprotectEnd	Signaled on the recovery site when a reprotect has completed.	Info

Table 13-3. Recovery Events (continued)

Event Name	Event Type	Event Description	Category
Recovery plan is displaying a prompt and is waiting for user input.	PlanPromptDisplay	Signaled on the recovery site when a prompt step is encountered. The key is a unique identifier for the prompt.	Info
Recovery plan has received an answer to its prompt.	PlanPromptResponse	Signaled on the recovery site when a prompt step is closed.	Info
Recovery plan has started to run a command on the Site Recovery Manager Server machine.	PlanServerCommandBegin	Signaled on the recovery site when Site Recovery Manager has started to run a callout command on the Site Recovery Manager Server machine.	Info
Recovery plan has completed executing a command on the Site Recovery Manager Server machine.	PlanServerCommandEnd	Signaled on the recovery site when Site Recovery Manager has finished running a callout command on the Site Recovery Manager Server machine.	Info
Recovery plan has started to run a command on a recovered virtual machine.	PlanVmCommandBegin	Signaled on the recovery site when Site Recovery Manager has started to run a callout command on a recovered virtual machine.	Info
Recovery plan has completed executing a command on a recovered virtual machine.	PlanVmCommandEnd	Signaled on the recovery site when Site Recovery Manager has finished running a callout command on a recovered virtual machine.	Info

Automatic Protection Events

Automatic Protection events provide information about actions and status related to automatic protection.

Automatic Protection Events

Table 13-4.

Event	Description	Cause	Category
`AutomaticProtectionOffEvent`	Event to indicate that Automatic Protection is disabled.	The Site Recovery Manager server has lost the network connection to the remote Site Recovery Manager server or the remote Site Recovery Manager server does not support Automatic Protection.	Warning
`AutomaticProtectionOnEvent`	Event to indicate that Automatic Protection is on.	The Site Recovery Manager server establishes healthy network connection to the remote Site Recovery Manager server and both servers support Automatic Protection.	Info
`AutoprotectDisabledPgEvent`	Event to indicate that Automatic Protection is disabled for a particular protection group.	Automatic Protection is disabled for a particular protection group.	Info
`AutoprotectDisabledRpEvent`	Event to indicate that Automatic Protection is disabled for a particular replication provider.	Automatic Protection is disabled for a particular replication provider.	Info
`AutoprotectEnabledPgEvent`	Event to indicate that Automatic Protection is enabled for a particular protection group.	Automatic Protection is enabled for a particular protection group.	Info
`AutoprotectEnabledRpEvent`	Event to indicate that Automatic Protection is enabled for a particular replication provider.	Automatic Protection is enabled for a particular replication provider.	Info
`VmAutoprotectErrorEvent`	Event to indicate that the Automatic Protection operation failed.	Automatic Protection operation failed.	Error
`VmAutoprotectEvent`	Event to indicate that the Automatic Protection operation completed successfully.	Automatic Protection operation completed successfully.	Info

Virtual Volumes Events

Virtual Volumes events provide information about actions and status related to Virtual Volumes.

Virtual Volumes Events

Table 13-5.

Event	Description	Cause	Category
VvolGroupErrorEvent	Event to indicate that there are errors in a Virtual Volumes protection group.	Errors in a Virtual Volumes protection group.	Error
VvolGroupWarningEvent	Event to indicate that there are warnings in a Virtual Volumes protection group.	Warnings in a Virtual Volumes protection group.	Warning
VvolVmErrorEvent	Event to indicate that there are errors in a Virtual Volumes protected virtual machine.	Errors in a Virtual Volumes protected virtual machine.	Error
VvolVmWarningEvent	Event to indicate that there are warnings in a Virtual Volumes protected virtual machine.	Warnings in a Virtual Volumes protected virtual machine.	Warning

Storage and Storage Provider Events

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

Table 13-6. SRA Events

Event	Description	Cause	Category
StorageAdaptLoadEvent	Loaded the specified SRA.	Site Recovery Manager detected new SRA either during startup or during user-initiated SRAs reload.	Info
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.	Error
StorageAdaptChangeEvent	Loaded new version of the specified SRA.	Site Recovery Manager detected that previously known SRA was upgraded.	Info

Table 13-7. Array Manager Events

Event	Description	Cause	Category
SAManagerAddedEvent	Created the specified array manager using the specified SRA.	User added an Array Manager.	Info
SAManagerRemovedEvent	Deleted the specified array manager.	User removed an Array Manager.	Info
SAManagerReconfigEvent	Reconfigured the specified array manager.	User edited Array Manager properties.	Info

Table 13-7. Array Manager Events (continued)

Event	Description	Cause	Category
SAManagerPingOkEvent	Ping for the specified array manager succeeded.	Site Recovery Manager Server successfully pinged an Array Manager.	Info
SAManagerPingFailEvent	Failed to ping the specified array manager.	An error occurred during Array Manager ping.	Error

Table 13-8. Array Pair Events

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

Table 13-9. Datastore Events

Event	Description	Cause	Category
StorageDsDiscoveredEvent	Discovered replicated datastore.	Site Recovery Manager Server discovered replicated datastore.	Info
StorageDsLostEvent	Specified datastore is no longer replicated.	User turned off replication of storage devices backing the datastore.	Info
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.	Info
StorageRdmLostEvent	RDM attached to specified virtual machine is no longer replicated.	User turned off replication of the LUN backing the RDM.	Info

Table 13-10. Protection Events

Event	Description	Cause	Category	Event Target
SPDsProtEvent	Protected datastore in specified protection group.	User included datastore in new or existing protection group.	Info	Datastore
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.	Info	Datastore
SPVmDiscoveredEvent	Discovered replicated virtual machine.	User created virtual machine on a replicated datastore.	Info	Virtual machine
SPVmLostEvent	Specified virtual machine is no longer replicated.	User migrated virtual machine off the replicated datastore.	Info	Virtual machine
SPDsProtMissingEvent	Replicated datastore must be included in a specified protection group but is included in an alternate protection group.	This is raised if you have a datastore that must be merged and is still not protected. At the conflict event, the datastore is already protected.	Warning	Datastore
SPDsProtConflictEvent	Replicated datastore must be included in a specified protection group.	This is raised if you have a datastore that must be merged and is still not protected. At the conflict event, the datastore is already protected.	Error	Datastore
SPDsReplicationLostEvent	Datastore included in a specified protection group is no longer replicated.	User turned off replication for devices backing the datastore.	Error	Datastore
SPGroupProtRestoredEvent	Protection has been restored for specified protection group.	The previous (non-empty) issues of a protection group are cleared.	Info	Protection group
SPVmDsProtMissingEvent	Datastore used by virtual machine must 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 must add it.	Warning	Datastore

Table 13-10. Protection Events (continued)

Event	Description	Cause	Category	Event Target
SPVmDsProtConflictEvent	Datastore used by a specified virtual machine must be added to specified protection group, but is 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 must add it.	Error	Datastore
SPVmDsReplicationLostEvent	Datastore used by specified virtual machine and included in specified protection group is no longer replicated.	See description.	Error	Datastore
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.	Info	Virtual machine
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.	Error	Datastore
SPCgDsMissingProtEvent	Datastore from specified consistency group must be included in specified protection group.	See description.	Error	Datastore
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.	Error	Datastore

Table 13-10. Protection Events (continued)

Event	Description	Cause	Category	Event Target
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.	Error	Datastore
SPCgDsProtEvent	The user included a datastore belonging to a consistency group in new or existing protection group.	When a protected datastore part of a consistency group is added in new or existing protection group.	Info	Datastore
SPCgDsUnprotEvent	The user removed a datastore belonging to a consistency group from a protection group.	The datastore belonging to a consistency group is removed from a protection group.	Info	Datastore
SPCgProtEvent	The user included a consistency group in new or existing protection group.	The consistency group is added to new or existing protection group.	Info	Datastore
SPCgProtIssueEvent	The consistency group has errors or warnings.	The protected consistency group has errors or warnings.	Error	Datastore
SpCgProtRestoredEvent	The consistency group no longer has errors or warnings.	When the consistency group issues are resolved.	Info	Datastore
SPCgUnprotEvent	The user removed a consistency group from a protection group.	The consistency group was removed from a protection group.	Info	Datastore

Licensing Events

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

Table 13-11. Licensing Events

Event	Description	Cause
LicenseExpiringEvent	The Site Recovery Manager License at the specified site expires in the specified number of days.	Every 24 hours, non-evaluation, expiring licenses are checked for the number of days left. This event is posted with the results.
EvalLicenseExpiringEvent	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.
EvalLicenseExpiredEvent	The Site Recovery Manager Evaluation License at the specified site license has expired.	Every 30 minutes, evaluation licenses will post this event.
UnlicensedFeatureEvent	The Site Recovery Manager license at the specified site is overallocated by the specified number of licenses.	Every 24 hours and upon the protection or unprotection of a virtual machine, this event will be posted if the total number of licenses exceeds the capacity in the license.
LicenseUsageChangedEvent	The Site Recovery Manager license at the specified site is using the specified number out of the total number licenses.	Every 24 hours and upon the protection or unprotection of a virtual machine, this event will be posted if the total number of licenses does not exceed the capacity in the license.

Permissions Events

Permission events provide information about changes to Site Recovery Manager permissions.

Table 13-12. Permissions Events

Event	Description	Cause
PermissionsAddedEvent	Permission created for the entity on Site Recovery Manager.	A permission for the entity was created using the role specified. The IsPropagate flag indicates whether the permission is propagated down the entity hierarchy.
PermissionsDeletedEvent	Permission rule removed for the entity on Site Recovery Manager.	A permission for the entity was deleted.
PermissionsUpdatedEvent	Permission changed for the entity on Site Recovery Manager.	A permission for the indicated entity was modified.

SNMP Traps

Site Recovery Manager sends SNMP traps to community targets defined in vCenter Server. You can configure them using the vSphere Web Client. When you enter localhost or 127.0.0.1 as a

target host for SNMP traps, Site Recovery Manager uses the IP address or host name of the vSphere server as configured by the Site Recovery Manager installer.

Table 13-13. 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.
`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.

Table 13-13. SNMP Traps (continued)

Event	Description	Cause
`RecoveryPlanVmCommandBeginTrap`	This trap is sent when a recovery plan starts the execution of a command callout on a recovered virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name, virtual machine name, virtual machine UUID.
`RecoveryPlanVmCommandEndTrap`	This trap is sent when a recovery plan has finished the execution of a command callout on a recovered virtual machine.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, command name, virtual machine name, virtual machine UUID, result status.
`RecoveryPlanPromptDisplayTrap`	This trap is sent when a recovery plan requires user input before continuing.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, prompt string.
`RecoveryPlanPromptResponseTrap`	This trap is sent when a recovery plan no longer requires user input before continuing.	Site Recovery Manager site name, recovery plan name, recovery type, and execution state.

Collecting Site Recovery Manager Log Files

14

To help identify the cause of any problems you encounter during the day-to-day running of Site Recovery Manager, you might need to collect Site Recovery Manager log files to review or send to VMware Support.

Site Recovery Manager creates several log files that contain information that can help VMware Support diagnose problems. You can 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 Server log bundle also contains system information and history reports of the latest recovery plan executions.

The Site Recovery Manager client log files contain information about the client configuration and messages related to client plug-in operations. The Site Recovery Manager bundle also includes installer log files and the contents of the storage replication adapters (SRA) subdirectory of the log directory.

Log files from vCenter Server instances and ESXi Server instances that are part of your Site Recovery Manager system might also include information useful for diagnosing Site Recovery Manager problems.

The Site Recovery Manager log file collects or retrieves the files and compresses them in a zipped file that is placed in a location that you choose.

Errors that you encounter during Site Recovery Manager operations appear in error dialog boxes or appear in the **Recent Tasks** window. Most errors also generate an entry in a Site Recovery Manager log file. Check the recent tasks and log files for the recovery site and the protected site.

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

You can download logs for Site Recovery Manager to a user-specified location.

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

Procedure

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

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

3   On the **Site Pair** tab, click **Summary** and then click **Name** in the Site Recovery Manager box.

4   Select a server and click **Export Logs**.

5   Click **Download** to download the logs.

Collect Site Recovery Manager Log Files Manually

You can download Site Recovery Manager Server log files in a log bundle that you generate manually. Collecting the log files manually 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

◆   To collect the Site Recovery Manager log files, use one the following methods:

Task	Action
Generate a log bundle from the Site Recovery Manager Server Windows host machine by using the command prompt	a Log in to the Site Recovery Manager Server host and open a command prompt. b Change the working directory to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`. c Run the following command: `cscript srm-support.wsf` The individual log files are collected in a file named `srm-support-MM-DD-YYYY-HH-MM.zip`, where *MM-DD-YYYY-HH-MM* indicates the month, day, year, hour, and minute when the log files were created. The log bundle is saved on the desktop by default.
Generate a log bundle from the Site Recovery Manager Server Windows host machine by using the Start menu	a Log in to the Site Recovery Manager Server host. b Select **Start > Programs > VMware > VMware Site Recovery Manager > Generate VMware vCenter Site Recovery Manager log bundle**.
Generate a log bundle from the Site Recovery Manager Appliance	a Log in to the Site Recovery Manager Appliance host machine and open a command prompt. b Change the working directory to `/opt/vmware/srm/bin/`. c Run the following command: ■ If you are logged in as admin user: `sudo ./srm-support-linux.sh`. ■ If you are logged in as root user: `./srm-support-linux.sh`.

Change Size and Number of Site Recovery Manager Server Log Files

You can change the size, number, and location of Site Recovery Manager Server log files.

You can modify the Site Recovery Manager log settings in the `vmware-dr.xml` configuration file on the Site Recovery Manager Server.

Procedure

1 Log in to the Site Recovery Manager Server host.

2 Open the `vmware-dr.xml` file in a text editor.

   ▪ If you are using Site Recovery Manager for Windows, you find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder on the Site Recovery Manager Server host machine.

   ▪ If you are using the Site Recovery Manager Virtual Appliance, you find the `vmware-dr.xml` file in the `/opt/vmware/srm/conf/` directory on the appliance.

3 Find the `<log>` section in the `vmware-dr.xml` file.

4 Set the maximum size in bytes of the logs to retain.

   You set the maximum log size by adding a `<maxFileSize>` section to the `<log>` section. The default is 10485760 bytes.

   ```
   <log>
       <maxFileSize>10485760</maxFileSize>
   </log>
   ```

5 Set the maximum number of log files to retain.

   You set the maximum number of logs by adding a `<maxFileNum>` section to the `<log>` section. The default is 20 log files.

   ```
   <log>
       <maxFileNum>20</maxFileNum>
   </log>
   ```

6 (Optional) Change the location on the Site Recovery Manager Server in which to store the log files by modifying the `<directory>` section in the `<log>` section.

   Note If you change the location of the log files, you must verify that your Site Recovery Manager user account has the necessary permissions to write in the new directory.

   ▪ If you are using Site Recovery Manager for Windows, the default path to the logs is `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs`.

   ▪ If you are using the Site Recovery Manager Appliance, the default location of the log files is `/var/log/vmware/srm`.

7 Change the default prefix for log files.

You change the default prefix by modifying the `<name>` section in the `<log>` section.

```
<log>
    <name>vmware-dr</name>
</log>
```

8 Change the logging level.

You change the logging level by modifying the `<level>` section in the `<log>` section. The possible logging levels are error, warning, info, verbose, and trivia. If you set the level to trivia, you see a noticeable negative effect on performance.

```
<log>
    <level>info</level>
</log>
```

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

You can set specific logging levels for components by modifying the appropriate `<level>` sections. For example, you can set the logging level for the recovery component to trivia.

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

10 (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.

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

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

Configure Site Recovery Manager Core Dumps

You can configure Site Recovery Manager core dump settings to change the location of the core dump files and compress them.

You can modify the Site Recovery Manager core dump settings in the `vmware-dr.xml` configuration file on the Site Recovery Manager Server.

Procedure

1 Log in to the Site Recovery Manager Server host.

2 Open the `vmware-dr.xml` file in a text editor.

- If you are using Site Recovery Manager for Windows, you find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder on the Site Recovery Manager Server host machine.

- If you are using the Site Recovery Manager Virtual Appliance, you find the `vmware-dr.xml` file in the `/opt/vmware/srm/conf/` directory on the appliance.

3 Change the location on the Site Recovery Manager Server in which to store core dumps by modifying the `<coreDump>` section of the `vmware-dr.xml` file.

Note If you change the location of the core dump files, you must verify that your Site Recovery Manager user account has the necessary permissions to write in the new directory.

- If you are using Site Recovery Manager for Windows, the default path to the core dump is `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles`, unless this location does not exist or is not writable. In that case, Site Recovery Manager Server uses `C:\ProgramData\VMware`.

- If you are using the Site Recovery Manager Appliance, the default location of the core dump is `/var/log/vmware/srm/DumpFiles`.

4 Use the core dump system parameters to limit the number of created and compressed dump files.

```
<debug>
   <dumpCoreCompression>true,false</dumpCoreCompression>
   <dumpFullCore>true,false</dumpFullCore>
</debug>
```

Parameter	Description
`dumpCoreCompression`	If unspecified, the default value is false. Site Recovery Manager Server does not compress previous core dump files as it creates core dump files. If you specify *true*, then Site Recovery Manager Server compresses all older core dumps when it generates a new core dump.
`dumpFullCore`	If unspecified, the default value is *false*. Site Recovery Manager Server generates a core dump file of several MB and provides some assistance to support when a problem occurs. If you set this value to true, Site Recovery Manager Server generates a full core dump file that might be several GBs in size, depending on the workload at the time the core dump occurs. This larger file can provide greater assistance to support when a problem occurs. If disk space allows, set this value to *true*.

5 To modify the maximum number of core dump files, add a row to the `<debug>` section.

```
<maxCoreDumpFiles>max files</maxCoreDumpFiles>
```

If unspecified, the default value is 4. This value specifies the maximum number of core dump files that are retained in the core dump directory. When Site Recovery Manager Server creates core dumps, Site Recovery Manager Server deletes older files as necessary to avoid exceeding the maximum and consuming excessive disk space, especially when `dumpFullCore` is true.

Troubleshooting Site Recovery Manager

<div style="text-align: right">15</div>

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/.

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   Log in to the Site Recovery Manager Server host.

2 Open the `vmware-dr.xml` file in a text editor.

- If you are using Site Recovery Manager for Windows, you find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder on the Site Recovery Manager Server host machine.

- If you are using the Site Recovery Manager Virtual Appliance, you find the `vmware-dr.xml` file in the `/opt/vmware/srm/conf/` directory on the appliance.

3 Update the `defaultMaxBootAndShutdownOpsPerCluster` and `defaultMaxBootAndShutdownOpsPerHost` values to limit the number of power-on operations at the recovery site.

The following example shows how to limit the number of power-on operations to a maximum of 32 per cluster and 4 per standalone host.

```
<config>
   <defaultMaxBootAndShutdownOpsPerCluster>32</defaultMaxBootAndShutdownOpsPerCluster>
   <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
</config>
```

4 Restart the Site Recovery Manager Server service.

LVM.enableResignature=1 Remains Set After a Site Recovery Manager Test Recovery

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

Problem

During a test recovery or an actual recovery, Site Recovery Manager sets `LVM.enableResignature` to 1 if the flag is not already set. Site Recovery Manager sets this flag to resignature snapshot volumes and mounts them on ESXi hosts for recovery. After the operation finishes, the flag remains set to 1.

Cause

Site Recovery Manager does not check how snapshot volumes are presented to ESXi hosts. Site Recovery Manager does not support setting the `LVM.enableResignature` flag to 0. If you set the flag from 1 to 0, a virtual machine outage might occur each time you perform a test recovery or an actual recovery occurs.

Setting the `LVM.enableResignature` flag on ESXi hosts is a host-wide operation. When this flag is set to 1, during the host rescan or the next host reboot, all snapshot LUNs that are visible to the ESXi host, and that can be resignatured, are resignatured.

If snapshot volumes unrelated to Site Recovery Manager are forcefully mounted to ESXi hosts on the recovery site, these LUNs are resignatured as part of a host rescan during a test recovery or an actual recovery process. As a result, all the virtual machines in these volumes become inaccessible.

Solution

To prevent outages, make sure that no snapshot LUNs that are unrelated to Site Recovery Manager, and that are forcefully mounted, are visible to ESXi hosts on the recovery site.

Adding Virtual Machines to a Protection Group Fails with an Unresolved Devices Error

Adding virtual machines to a protection group fails with an error if you did not map the devices of the virtual machine.

Problem

When you add a virtual machine to a protection group, you see the error `Unable to protect VM '`*`virtual machine name`*`' due to unresolved devices`.

Cause

You did not map the devices of the virtual machine on the protected site to the corresponding devices on the recovery site.

Solution

Configure the protection settings of the virtual machine as described in Modifying the Settings of a Virtual Machine in an Array-Based, Virtual Volumes, or vSphere Replication Protection Group.

Configuring Protection fails with Placeholder Creation Error

When you configure protection on multiple virtual machines, the configuration fails with a placeholder creation error.

Problem

Configuring protection on a large number of virtual machines at the same time fails with either a placeholder creation timeout error or a placeholder creation naming error:

- `Placeholder VM creation error:Operation timed out:300 seconds`

- `Placeholder VM creation error:The name '`*`placeholder_name`*`' already exists`

This problem occurs when you configure protection in different ways:

- You create a protection group that contains a datastore or datastores that contain a large number of virtual machines.

- You use the **Protection Groups > Virtual Machines > Restore All** option in the Site Recovery Manager interface on a large number of virtual machines.

- You use the Site Recovery Manager API to protect a large number of virtual machines manually.

Cause

The infrastructure on the recovery site is unable to handle the volume of concurrent creations of placeholder virtual machines.

Solution

Increase the `replication.placeholderVmCreationTimeout` setting from the default of 300 seconds. See Change Replication Settings.

You do not need to restart Site Recovery Manager Server after changing this setting. Site Recovery Manager applies the setting the next time that you configure protection on a virtual machine.

Rapid Deletion and Recreation of Placeholders Fails

If you delete all of the placeholder virtual machines from a datastore, unmount the datastore, and remount the datastore, recreation of the placeholder virtual machines might fail.

Problem

Recreating the placeholders too rapidly after unmounting the datastore can fail with the error `NoCompatibleHostFound`.

Cause

The associations between ESXi hosts and datastores are updated at 10-minute intervals. If you recreate the placeholders after unmounting and remounting the datastore but before the next update, the host cannot be found.

Solution

Wait for more than 10 minutes after unmounting and remounting the datastore before you recreate the placeholder virtual machines.

Planned Migration Fails Because Host is in an Incorrect State

If you put the ESXi host on the recovery site into maintenance mode during a planned migration, the planned migration fails.

Problem

Planned migration fails with the error `Error - The operation is not allowed in the current state of the host`.

Cause

Site Recovery Manager cannot power on virtual machines on the recovery site when the ESXi host on the recovery site is in maintenance mode.

Solution

Exit maintenance mode on the ESXi host on the recovery site and rerun the planned migration.

Planned Migration Fails Due to Unsuccessful Synchronization of Storage Policy Protection Group

When you attempt to run a planned migration of a recovery plan that contains a storage policy protection group, the recovery plan fails because of an unfinished synchronization of changes to the protection group.

Problem

When you attempt to run a planned migration of a recovery plan that contains a storage policy protection group, you see the following error message: `The peer site has not finished synchronizing changes to protection group.`

Cause

When you run a planned migration of a recovery plan that contains a storage policy protection group, Site Recovery Manager checks whether the protection groups are synchronized on both of the protected and recovery sites before it runs the recovery plan.

If the protection group is synchronized on both sites, the planned migration begins. If the protection group is not synchronized on both sites, you see the error message.

Solution

1   Close the error message and click **Finish** again.

2   (Optional) If the error persists, cancel the planned migration, wait a short time, and attempt to run the planned migration again.

Recovery Fails with a Timeout Error During Network Customization for Some Virtual Machines

During a recovery some virtual machines do not recover and show a timeout error during network customization.

Problem

During recovery some virtual machines do not recover within the default timeout period of 120 seconds.

Cause

This problem can occur for one of the following reasons.

- The VMware Tools package is not installed on the virtual machine that you are recovering.

- The cluster on the recovery site is experiencing heavy resource use while trying to simultaneously recover multiple virtual machines. In this case you can increase certain timeout settings to allow more time for tasks to complete. See Change Recovery Settings.

Solution

1 Verify that VMware Tools is installed on the virtual machine that you are recovering.

2 Check the available capacity on the recovery site.

   If the recovery site is experiencing heavy resource use, increasing the timeout period for guest customization can resolve the issue.

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

   b   On the Site Recovery home tab, select a site pair and click **View Details**.

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

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

   e   Increase the `recovery.customizationTimeout` parameter from the default of 600 seconds.

   f   Increase the `recovery.powerOnTimeout` parameter from the default of 300 seconds.

3 Run the recovery again.

Recovery Fails with Unavailable Host and Datastore Error

Recovery or test recovery fails with an error about host hardware and datastores being unavailable if you run the recovery or test shortly after changes occur in the vCenter Server inventory.

Problem

Recovery or test recovery fails with the error `No host with hardware version '7' and datastore 'ds_id' which are powered on and not in maintenance mode are available....`

Cause

Site Recovery Manager Server keeps a cache of the host inventory state. Sometimes when recent changes occur to the inventory, for example if a host becomes inaccessible, is disconnected, or loses its connection to some of the datastores, Site Recovery Manager Server can require up to 15 minutes to update its cache. If Site Recovery Manager Server has the incorrect host inventory state in its cache, a recovery or test recovery might fail.

Solution

Wait for 15 minutes before running a recovery if you change the host inventory. If you receive the error again, wait for 15 minutes and rerun the recovery.

Reprotect Fails with a vSphere Replication Timeout Error

When you run reprotect on a recovery plan that contains vSphere Replication protection groups, the operation times out with an error.

Problem

Reprotect operations on recovery plans that contain vSphere Replication protection groups fail with the error `Operation timed out: 7200 seconds VR synchronization failed for VRM group <Unavailable>. Operation timed out: 7200 seconds.`

Cause

When you run reprotect, Site Recovery Manager performs an online sync for the vSphere Replication protection group, which might cause the operation to timeout. The default timeout value is 2 hours and corresponds to a working synchronization timeout of 4 hours.

Solution

Increase the `vrReplication.synchronizationTimeout` and `vrReplication.reverseReplicationTimeout` timeout values in Advanced Settings. See Change vSphere Replication Settings.

Recovery Plan Times Out While Waiting for VMware Tools

Running a recovery plan fails with a timeout error while waiting for VMware Tools to start.

Problem

Recovery operations fail at the Shutdown VMs step or Waiting for VMware Tools step of a recovery plan.

Cause

Site Recovery Manager uses VMware Tools heartbeat to discover when recovered virtual machines are running on the recovery site. Recovery operations require that you install VMware Tools on the protected virtual machines. Recovery fails if you did not install VMware Tools on the protected virtual machines, or if you did not configure Site Recovery Manager to start without waiting for VMware Tools to start.

Solution

Install VMware Tools on the protected virtual machines. If you do not or cannot install VMware Tools on the protected virtual machines, you must configure Site Recovery Manager not to wait for VMware Tools to start in the recovered virtual machines and to skip the guest operating system shutdown step. See Change Recovery Settings.

Synchronization Fails for vSphere Replication Protection Groups

During test recovery, planned migration, and reprotect of recovery plans that contain vSphere Replication protection groups, the virtual machine synchronization step fails with an error.

Problem

Synchronization of virtual machines in a vSphere Replication protection group fails with the error message `Error – VR synchronization failed for VRM group <Unavailable>. The object has already been deleted or has not been completely created`.

Cause

Excessive I/O traffic on one or more of the virtual machines in the protection group causes the synchronization to time out before it can finish. This might occur because of heavy traffic. For example, setting the logging level to trivia mode can generate heavy I/O traffic.

Solution

1   Log in to the Site Recovery Manager Server host.

2   Open the `vmware-dr.xml` file in a text editor.

    ▪   If you are using Site Recovery Manager for Windows, you find the `vmware-dr.xml` file in the `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` folder on the Site Recovery Manager Server host machine.

    ▪   If you are using the Site Recovery Manager Virtual Appliance, you find the `vmware-dr.xml` file in the `/opt/vmware/srm/conf/` directory on the appliance.

3   Add a `<topology><drTaskCleanupTime>` element to the `vmware-dr.xml` file.

    You can add the `<topology>` element anywhere at the top level in the `<Config>` tags. Set the value of `<drTaskCleanupTime>` to at least 300 seconds. If you set the logging level to trivia, set `<drTaskCleanupTime>` to 1000 seconds.

    ```
    <topology>
        <drTaskCleanupTime>1000</drTaskCleanupTime>
    </topology>
    ```

4   Save and close the `vmware-dr.xml` file.

5   Restart the Site Recovery Manager Server service to apply the new settings.

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.

Recovery Sticks at 36% During Planned Migration

If you stop the Site Recovery Manager service on the protected site during a planned migration, the operation sticks at 36%.

Problem

During a planned migration, if you stop the Site Recovery Manager service on the protected site, when the workflow proceeds to step 15 **Unmount protected site storage**, it might not fail gracefully, but instead remains at 36%.

Solution

Click **Cancel** to cancel the workflow, then re-run the workflow.

Operations Fail with Error About a Nonreplicated Configuration File

When running several recovery or reprotect operations simultaneously in both directions, the operation fails with an error about a nonreplicated virtual machine configuration file.

Problem

When you run several recovery plans simultaneously that contain array-based replication protection groups or storage policy protection groups, with some operations running from site A to site B, and some operations running from site B to site A, some or all of the plans fail with the error `Cannot protect virtual machine 'virtual_machine_name' because its config file 'virtual_machine_config_file.vmx' is located on a non-replicated or non-protected datastore.`

Cause

This problem can occur because datastore computation on a site is delayed by the recovery operations that are running in the opposite direction.

Solution

Wait until some of the operations have completed and rerun the operation on the recovery plans that failed. Alternatively, run all planned migrations in the same direction together. When the planned migrations have finished, run the planned migrations in the opposite direction.

Recovery Fails Due to Restricted User Permissions

You might receive an error during the recovery process if the Site Recovery Manager solution user does not have permissions to perform an IP customization or in-guest OS callout operations.

Problem

If the Site Recovery Manager solution user does not have appropriate permissions to the guest OS of the recovered VM, you might receive one of the following error messages during the recovery process.

```
GuestPermissionDenied
```

```
CannotAccessFile
```

Cause

The problem appears if the Site Recovery Manager solution user is mapped to a guest OS user that does not have access to a file in the guest OS or permissions to run commands.

Solution

1   If you use Site Recovery Manager to configure the guest user mappings, ensure that the guest OS user who runs the VMware Tools service has access to a file or has permissions to run commands.

For information about how to enable or disable the automatic configuration of the guest user mappings, see Change Recovery Settings.

2   (Optional) If you manually configure the guest user mappings, map the local Site Recovery Manager solution user on the recovery site to the guest OS user with appropriate permissions.

3   Rerun the recovery plan.

Recovery Fails Due to an Unsupported Combination of VMware Tools and ESXi

The recovery process might fail if the version of VMware Tools installed on your VM and the version of the ESXi host on the recovery site are incompatible with Site Recovery Manager.

Problem

You might receive the following error during the recovery process.

```
OperationNotSupportedByGuest
```

Cause

The problem might appear if you use incompatible versions of VMware Tools and ESXi. For information about the compatibility between Site Recovery Manager, VMware Tools, and ESXi, see *Compatibility Matrices for Site Recovery Manager 8.3*.

Solution

◆   Ensure that the versions of VMware Tools and ESXi are compatible with your Site Recovery Manager.