vmware by Broadcom

VMware Site Recovery Manager 8.8

Table of Contents

Release Notes

Product enhancements, updates, support notices, known and resolved issues for the VMware Site Recovery Manager 8.8 releases.

VMware Site Recovery Manager 8.8.0.3 Release Notes

This document contains the following sections

Introduction

Site Recovery Manager 8.8.0.3 | 08 FEB 2024 | Build 23263427 | Download
Check for additions and updates to these release notes.
VMware Site Recovery Manager 8.8.0.3 is a minor product patch release that provides bug fixes and improvements. The content of the VMware Site Recovery Manager 8.8 Release Notes and all following 8.8.0.x patch release notes applies to this version as well.

What's New in Site Recovery Manager 8.8.0.3

The VMware Site Recovery Manager 8.8.0.3 Express Patch provides security and bug fixes.

Updated Postgres to version 14.10.

Updated the Tomcat server.

Installation and Upgrade

For information about installing and upgrading Site Recovery Manager, see *Site Recovery Manager Installation and Configuration*.

For the supported upgrade paths for Site Recovery Manager, select **Upgrade Path** and **VMware Site Recovery Manager** in the VMware Product Interoperability Matrices.

If you are running Site Recovery Manager 8.8, upgrade to Site Recovery Manager 8.8.0.3. See *Upgrading Site Recovery Manager* in *Site Recovery Manager 8.8 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 8.8, upgrade the vSphere Replication appliance to version 8.8.0.3. See the vSphere Replication 8.8.0.3 Release Notes for information about vSphere Replication 8.8.0.3.

NOTES:

- If the vCenter Server instances on the protected and recovery sites are in Enhanced Linked Mode, they must be direct replication partners. Otherwise, upgrade might fail.

Resolved Issues

The Site Recovery Manager server service might fail to start

The Site Recovery Manager server service might fail to start with an error `"Job for srm-server.service failed because a fatal signal was delivered to the control process"`. The `drconfig.log` shows the following errors.

```
YYYY-MM-DDTHH:MM:SS.186-06:00 error drconfig[01440] [SRM@6876 sub=ServiceControl opID=a27c6787-e22e-4923-
b4d8-3c893a908e35-configure:5f0a] Command "/usr/bin/systemctl start srm-server" exit code: 1--> stderr:--> Job
 for srm-server.service failed because a fatal signal was delivered to the control process.--> See "systemctl
 status srm-server.service" and "journalctl -xe" for details.-->
```

This issue is fixed in Site Recovery Manager 8.8.0.3.

VMware Site Recovery Manager 8.8.0.2 Release Notes

This document contains the following sections

Introduction

Site Recovery Manager 8.8.0.2 | 21 NOV 2023 | Build 22795449
Check for additions and updates to these release notes.
VMware Site Recovery Manager 8.8.0.3 replaces the previously released VMware Site Recovery Manager 8.8.0.2. The content of the VMware Site Recovery Manager 8.8 Release Notes and all following 8.8.0.x patch release notes applies to this version as well.

What's New in Site Recovery Manager 8.8.0.2

The VMware Site Recovery Manager 8.8.0.2 Express Patch provides security and bug fixes.

FIPS compliance for Site Recovery user interface and vSphere Client plug-in. For more information, see How do I activate FIPS on the Site Recovery Manager appliance and How do I validate that FIPS mode is activated.

Installation and Upgrade

For information about installing and upgrading Site Recovery Manager, see *Site Recovery Manager Installation and Configuration*.

For the supported upgrade paths for Site Recovery Manager, select **Upgrade Path** and **VMware Site Recovery Manager** in the VMware Product Interoperability Matrices.

If you are running Site Recovery Manager 8.8, upgrade to Site Recovery Manager 8.8.0.2. See *Upgrading Site Recovery Manager* in *Site Recovery Manager 8.8 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 8.8, upgrade the vSphere Replication appliance to version 8.8.0.2. See the vSphere Replication 8.8.0.2 Release Notes for information about vSphere Replication 8.8.0.2.

NOTES:

- If the vCenter Server instances on the protected and recovery sites are in Enhanced Linked Mode, they must be direct replication partners. Otherwise, upgrade might fail.

Resolved Issues

Site Recovery Manager 8.8.0.x fails to register in vCenter Server 8.0 Update 2

Site Recovery Manager 8.8.0.x might fail to register in vCenter Server 8.0 Update 2 with an error `"Failed to register H5 UI"`. The `drconfig.log` shows the following error:

```
--> YYYY-MM-DD HH:MM:SS [srm-reactive-thread-7] ERROR
com.vmware.dr.client.shared.utils.ExtManagerHelper - Failed to mirror plugin registration
to VC ExtensionManager.
```

```
--> invalidProperty = Extension server certificate is invalid.
```

This issue is fixed in Site Recovery Manager 8.8.0.2.

VM tags are changed after performing a failover

When assigning tags to virtual machines, if there are more than ten categories on the same VM, the category of some tags changes after performing a failover.

This issue is fixed in Site Recovery Manager 8.8.0.2.

VMware Site Recovery Manager 8.8.0.1 Release Notes

This document contains the following sections

Introduction

Site Recovery Manager 8.8.0.1 | 17 OCT 2023 | Build 22602689 | Download Check for additions and updates to these release notes. VMware Site Recovery Manager 8.8.0.1 is a minor product patch release that provides bug fixes and improvements. The content of the VMware Site Recovery Manager 8.8 Release Notes applies to this version as well.

What's New in Site Recovery Manager 8.8.0.1

The VMware Site Recovery Manager 8.8.0.1 Express Patch provides bug fixes.

Installation and Upgrade

For information about installing and upgrading Site Recovery Manager, see *Site Recovery Manager Installation and Configuration*.

For the supported upgrade paths for Site Recovery Manager, select **Upgrade Path** and **VMware Site Recovery Manager** in the VMware Product Interoperability Matrices.

If you are running Site Recovery Manager 8.8, upgrade to Site Recovery Manager 8.8.0.1. See *Upgrading Site Recovery Manager* in *Site Recovery Manager 8.8 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 8.8, upgrade the vSphere Replication appliance to version 8.8.0.1. See the vSphere Replication 8.8.0.1 Release Notes for information about vSphere Replication 8.8.0.1.

NOTES:

- If the vCenter Server instances on the protected and recovery sites are in Enhanced Linked Mode, they must be direct replication partners. Otherwise, upgrade might fail.

Resolved Issues

Running a failover of Virtual Volumes protection groups might fail

When there are many virtual machines in a Virtual Volumes fault domain, the `moId` of some of the virtual machines has a common prefix, for example, `vm-12` and `vm-123` , causing Site Recovery Manager to fail to match the correct storage profile. As a result the failover operation fails.

This issue is fixed in Site Recovery Manager 8.8.0.1.

Site Recovery Manager request for query sync status shows incorrect tag in the XML for ongoing sync use case

There is an issue in the XML structure for querying the sync status. Instead of the `<ConsistencyGroups>` tag, the XML shows the `<TargetGroups>` tag.

```
<QuerySyncStatusParameters>
<ArrayId>xxxx</ArrayId>
<PeerArrayId>xxxx</PeerArrayId>
<TargetGroups>
<TargetGroup key="xxx.r12121" syncId="ongoing_syncing-xxx.r12121" />
</TargetGroups>
</QuerySyncStatusParameters>
```

This issue is fixed in Site Recovery Manager 8.8.0.1.

Reprotect is failing for Recovery Plans with NVMe/TCP and NVMe/FC devices

The issue is caused by the `CopyDeviceIdentity` function which does not copy the NVMe specific data to the `StorageDeviceBaseDBObject` .

This issue is fixed in Site Recovery Manager 8.8.0.1.

Upgrade to Site Recovery Manager 8.8 fails with an error

When you attempt to perform a chain upgrade from an earlier version of Site Recovery Manager, for example from version 8.3 to version 8.8, the upgrade might fail with an error.

```
Operation Failed: Failed to install update.
```

The logs located in `/opt/vmware/var/log/vami/updatecli.log` show the following:

```
Error: Failed to synchronize cache for repo 'VMware Photon Linux 3.0 (x86_64)' from
'https://packages.vmware.com/photon/3.0/photon_release_3.0_x86_64'1. package xml-security-
c-1.7.3-4.ph2.x86_64 requires libcrypto.so.1.0.0()(64bit), but none of the providers can
be installed.
```

Alternatively, the appliance might fail to boot displaying the following error.

```
Loading Linux 4.19.182-2.ph3 ...

error: file '/vmlinuz-4.19.182-2.ph3' not found.

Loading initial ramdisk ...

error: you need to load the kernel first.
```

This issue is fixed in Site Recovery Manager 8.8.0.1.

VMware Site Recovery Manager 8.8 Release Notes

This document contains the following sections

Introduction

Site Recovery Manager 8.8 | 21 SEP 2023 | Build 22434509 | Download
Site Recovery Manager Configuration Import/Export Tool 8.8 | 21 SEP 2023 | Build 22432313 | Download
Check for additions and updates to these release notes.

What's New in Site Recovery Manager 8.8

VMware Site Recovery Manager 8.8 adds compatibility with VMware vSphere 8.0 Update 2.

For more information on interoperability with earlier or later releases of VMware vSphere, see the VMware Product Interoperability Matrices. For information about the features of vSphere 8.0 Update 2, see the vSphere 8.0 Update 2 documentation.

Recovery plan queuing support for more than 10 recovery plans

Site Recovery Manager has an upper limit of executing a maximum of 10 concurrent recovery plans. With the queue option, as the recovery plans complete, additional ones in the queue are automatically executed in sequence to a maximum of 10 concurrent plans. This provides greater flexibility so that a DR test can be enabled by an application team, for example to conduct their DR test when needed and not be tied to a company wide test.

Remove multiple protection groups or recovery plans through the Site Recovery UI

You can use the Site Recovery user interface to delete multiple protection groups or recovery plans at the same time.

Expose the DR REST APIs through VMware Aria Automation Orchestrator plug-in

Introducing the end-to-end support of Site Recovery Manager REST APIs through the DR REST plug-in for VMware Aria Automation Orchestrator. Customers will benefit by automating manual workflows to monitor, protect, manage appliances and run recovery plans. For more information, see DR REST plug-in for VMware Aria Automation Orchestrator Release Notes.

VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8.

For information about the management pack, see VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8 Release Notes.

VMware Aria Automation Orchestrator Plug-in for VMware Site Recovery Manager 8.8.

For information about the new workflows, see VMware Aria Automation Orchestrator Plug-in for VMware Site Recovery Manager 8.8 Release Notes.

Localization

VMware Site Recovery Manager 8.8 is available in the following languages:

- English
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese
- Spanish

Compatibility

Site Recovery Manager Compatibility Matrix

Site Recovery Manager 8.8 is compatible with vSphere 7.0 Update 3 and later, and supports ESXi versions 7.0 Update 3 and later.

http://2610771Site Recovery Manager 8.8 requires a supported vCenter Server version on both the protected site and the recovery site.

For interoperability and product compatibility information, including support for guest operating system customization, see the Compatibility Matrices for VMware Site Recovery Manager 8.8.

Compatible Storage Arrays and Storage Replication Adapters

For the current list of supported compatible storage arrays and SRAs, see the Site Recovery Manager Storage Partner Compatibility Guide.

Compatible Virtual Volumes Partner VASA Providers

For the current list of compatible Virtual Volumes Partner VASA providers, see the VMware Compatibility Guide.

VMware vSAN Support

Site Recovery Manager 8.8 can protect virtual machines that reside on VMware vSAN and vSAN Express Storage by using vSphere Replication. vSAN does not require a Storage Replication Adapter (SRA) to work with Site Recovery Manager 8.8.

Installation and Upgrade

For information about installing and upgrading Site Recovery Manager, see *Site Recovery Manager Installation and Configuration*.

For the supported upgrade paths for Site Recovery Manager, select **Upgrade Path** and **VMware Site Recovery Manager** in the VMware Product Interoperability Matrices.

NOTES:

- If the vCenter Server instances on the protected and recovery sites are in Enhanced Linked Mode, they must be direct replication partners. Otherwise, upgrade might fail.

Network Security

Site Recovery Manager requires a management network connection between paired sites. The Site Recovery Manager Server instances on the protected site and on the recovery site must be able to connect to each other. In addition, each

Site Recovery Manager instance requires a network connection to the Platform Services Controller and the vCenter Server instances that Site Recovery Manager extends at the remote site. Use a restricted, private network that is not accessible from the Internet for all network traffic between Site Recovery Manager sites. By limiting network connectivity, you limit the potential for certain types of attacks.

For the list of network ports that Site Recovery Manager requires to be open on both sites, see *Network Ports for Site Recovery Manager*.

Operational Limits for Site Recovery Manager 8.8

For the operational limits of Site Recovery Manager 8.8, see *Operational Limits of Site Recovery Manager*.

Open Source Components

The copyright statements and licenses applicable to the open source software components distributed in Site Recovery Manager 8.8 are available at VMware Site Recovery Manager Downloads. You can also download the source files for any GPL, LGPL, or similar licenses that require the source code or modifications to the source code to be made available for the most recent generally available release of Site Recovery Manager.

Caveats and Limitations

- Site Recovery Manager does not support the protection of virtual machines that have persistent memory (PMem) devices, PMem disks, or are configured for replication on a PMem datastore.
- In a federated environment with linked vCenter Server instances, when you log in to the REST API gateway local site this will automatically log you in to the remote site. You do not have to make a POST /remote-session request. It is not possible to log in to the remote site with a different user name.
- The protection and recovery of encrypted virtual machines with vSphere Replication requires VMware vSphere 7.0 Update 2c or later.
- When a linked clone virtual machine is created, some of its disks continue to use the base virtual machine disks. If you use vVols replication, you must replicate the linked clone virtual machine on the same replication group as the base virtual machine, otherwise you get the following error message: "`Virtual machine '{vmName}' is replicated by multiple replication groups.`" If you have to replicate the base virtual machine in a different replication group than the linked clone virtual machines, or the base virtual machine cannot be replicated at all, the linked clone virtual machines must be converted to full clones.
- Site Recovery Manager does not support Virtual Volumes replication of unattached disks which are present only in a snapshot.
- Site Recovery Manager does not currently support NetApp Cloud Volumes Service for Google Cloud VMware Engine neither as source nor as target for a replication.
- VMware Site Recovery Manager does not currently support AVS ANF for NetApp ONTAP NFS storage neither as source nor as target for a replication.
- The VMware Site Recovery Manager 8.8 Configuration Import/Export Tool Importing attempts to import the recovery settings of protected virtual machines only once no matter whether the protected virtual machines are part of one or many recovery plans.
- vSphere Flash Read Cache is disabled on virtual machines after recovery and the reservation is set to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take a note of the virtual machine's cache reservation from the vSphere Web Client. You can reconfigure vSphere Flash Read Cache on the virtual machine after the recovery.
- Site Recovery Manager 8.8 supports the protection of virtual machines with uni-processor vSphere FT, but deactivates uni-processor vSphere FT on the virtual machines on the recovery site after a recovery.
  - If you use uni-processor vSphere FT on virtual machines, you must configure the virtual machines on the protected site so that Site Recovery Manager can deactivate vSphere FT after a recovery. For information about how

to configure virtual machines for uni-processor vSphere FT on the protected site, see https://kb.vmware.com/kb/2109813.

- Site Recovery Manager 8.8 supports vSphere Replication 8.8 with vSphere Virtual Volumes with the following limitations.
  - You cannot use vSphere Replications Point-in-Time Snapshots with virtual machines where the replication target is a Virtual Volumes datastore.
  - When using vSphere Virtual Volumes storage as a replication target all disks belonging to the virtual machine must be replicated to a single vSphere Virtual Volumes datastore.
  - When a replicated virtual machine is located on vSphere Virtual Volumes storage, all disks belonging to that virtual machine must be located on a single vSphere Virtual Volumes datastore.
- Site Recovery Manager 8.8 does not support NFSv4.1 datastores for array-based replication. You can use Site Recovery Manager 8.8 with NFSv4.1 datastores for vSphere Replication.
- To use Two-factor authentication with RSA SecureID or Smart Card (Common Access Card) authentication your environment must meet the following requirements:
  a. Use the administrator credentials of your vCenter Server to install Site Recovery Manager 8.8 and to pair your Site Recovery Manager 8.8 sites.
  b. The vCenter Server instances on both Site Recovery Manager 8.8 sites must work in Enhanced Linked Mode. To prevent failures during upgrade of Site Recovery Manager from 8.8 to a newer version of Site Recovery Manager, the vCenter Server instances on both sites must be direct replication partners.

Known Issues

DR REST API v.8.8. hits DR server session limit exceeded

A bug in the DR REST API v.8.8 Rate Limiter tier *Session* prevents the DR server session to auto-close after a preconfigured timeout interval. The DR REST API client maintains a high number of DR sessions which results in exhaustion of the maximum possible number of DR server live sessions.

Workaround: Switch off the DR REST API Rate Limiter tier *Session* by performing the following steps.

1. Navigate to `/opt/vmware/dr-rest/webapps/rest/WEB-INF/web.xml` and comment out the following section.

```
<!--
<filter>
   <filter-name>SessionRateLimitFilter</filter-name>
   <filter-class>com.vmware.dr.restapi.infrastructure.rateLimit.SessionRateLimitFilter</filter-class>
   <async-supported>true</async-supported>
</filter>
-->
...
<!--
<filter-mapping>
   <filter-name>SessionRateLimitFilter</filter-name>
   <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

2. To close all live sessions, restart the DR service.
3. Restart the DR REST API service to switch off the DR REST API Rate Limiter tier *Session*.
4. Apply the workaround on all DR REST API instances of the server ecosystem.

Upgrade to Site Recovery Manager 8.8 fails with an error

When you attempt to perform a chain upgrade from an earlier version of Site Recovery Manager, for example from version 8.3 to version 8.8, the upgrade might fail with an error: `Operation Failed: Failed to install update.`

The logs located in `/opt/vmware/var/log/vami/updatecli.log` show the following:

```
Error: Failed to synchronize cache for repo 'VMware Photon Linux 3.0 (x86_64)' from
'https://packages.vmware.com/photon/3.0/photon_release_3.0_x86_64'1. package xml-security-
c-1.7.3-4.ph2.x86_64 requires libcrypto.so.1.0.0()(64bit), but none of the providers can
be installed.
```

The previous upgrades from Photon 2.0 to Photon 3.0 did not clean the packages properly causing the error in the upgrade procedure.

Workaround: Before performing the upgrade check whether package `xml-security-c` exist. If the package exists, remove it.

1. Revert the appliance before the update begins.
2. Check if the `xml-security-c` package exist. Run the following command `rpm -qa | grep ph2`.
   The output will be similar to this:
   ```
   xml-security-c-1.7.3-4.ph2.x86_64
   xerces-c-3.2.1-1.ph2.x86_64
   openjre8-1.8.0.232-1.ph2.x86_64
   libarchive-3.3.1-5.ph2.x86_64
   apache-ant-1.10.1-7.ph2.noarch
   libdnet-1.11-5.ph2.x86_64
   ```
3. To remove the `xml-security-c` package, run the following command `rpm -e xml-security-c-1.7.3-4.ph2.x86_64`.
4. Continue with the upgrade of the appliance.

Array pair pairing is failing with an error

When you attempt to create an array pair, the operation fails with the following error: "`SRA command 'discover Arrays' failed. Internal error: library initialization failed - unable to allocate file descriptor table - out of memory/srm/sra/command: line 2: 343 Aborted (core dumped) java Duser.country=US -Duser.language=en -jar EmcUnityBlockSra.jar .`"

When the implementation of the SRA is java based, the loading of the jar files might fail with a library initialization error because of a low default parameter of the user limit for the number of opened files.

Workaround: Run the following command on the Site Recovery Manager virtual appliance with root privileges: `docker rm $(docker ps -a -q) -f`

When you try to refer to a non-existing VM as a request path parameter the Site Recovery Manager REST API returns response error

If you use the vSphere UI to remove a virtual machine from a protection group, the Site Recovery Manager REST API shows a warning for the protection group `'There are configuration issues.'` and the following Site Recovery Manager REST API requests fail with an error `Status 404, Not Found`:

- 'Get Group VM'
- 'Remove VM From Protection Group'
- 'Remove VM Protection'
- 'Get VM Protection Settings'
- 'Update VM Protection Settings'

Workaround: Call the Site Recovery Manager REST API request 'Reconfigure Group'.

Failover or Planned Migration fails with an error during the virtual machine Power ON operation

A large scale Failover or Planned Migration might fail with an error "`A general system error occurred: Sandboxd call timed out`" during the VM Power ON operation.

Workaround: Re-run the failed recovery plan.

Planned Migration or failover might fail with an error "Unable to write VMX .." during the VM power on step.

When you attempt to perform a planned migration or a failover at a 4000 VMs scale, the operation might fail during the VM power on step with the following error: "`Unable to write VMX file: /vmfs/volumes/...vmx`" .

Workaround: Re-run the recovery plan.

During recovery of a large-scale environment the Site Recovery UI might throw an error

When you attempt to run a recovery of a large-scale environment, during the operation the Site Recovery UI might throw the following error:

"`Unable to retrieve recovery steps data.Unable to connect to Site Recovery Manager Server at https://VCHostname/drserver/vcdr/vmomi/sdk. Reason: https://VCHostname/drserver/vcdr/vmomi/sdk invocation failed with "java.net.SocketTimeoutException: 30,000 milliseconds timeout on connection http-outgoing-238 [ACTIVE]`"

Workaround: Refresh the Site Recovery UI, switch between the tabs, or open it in a different browser tab.

Planned Migration fails with an error

If you trigger replication sync, due to connectivity issues the replication might fail with the following error "`VR synchronization failed for VRM group 'VM Name'. A general system error occurred: VM has no replication group`" . Even though this might be a sporadic issue, the replication might not get back to an `OK` status automatically.

Workaround: Reconfigure the replication of all the failed virtual machines.

After an upgrade to Site Recovery Manager and vSphere Replication 8.8 on a vCenter Server 8.0.x, the local Site Recovery Manager integration plug-in is not removed

There are both local and remote Site Recovery Manager integration plug-ins in version 8.7. After the upgrade to version 8.8, the local plug-in is no longer needed, but it is not automatically removed.

Workaround: To remove the local integration plug-in, restart the vCenter Server client service from the vCenter Server terminal by using the following command `vmon-cli -r vsphere-ui` .

Known Issues from Previous Releases

For additional information, see the *Troubleshooting Site Recovery Manager* chapter in the Site Recovery Manager Administration guide.

Site Recovery Manager alarms are not visible in the alarm definitions

Site Recovery Manager events might not be visible when adding an alarm definition in vCenter Server 8.0 and vCenter Server 8.0 Update 1.

Workaround: Upgrade your vCenter Server instance to vCenter Server 8.0 Update 2.

A CD/DVD device is not connected after the recovery of a Virtual Volumes protected VM, when the device points to an image file on a datastore

When a virtual machine with a CD/DVD device pointing to an image file on a datastore is recovered, you receive the following error "`Connection control operation failed for disk 'sata0:0'.`" and the device is not connected.

Workaround: Recreate the device pointing to the desired image file.

Site Recovery Manager status is Not Connected after upgrading Site Recovery Manager in a shared recovery vCenter Server topology

After performing an upgrade of Site Recovery Manager 8.5.x or 8.6.x to Site Recovery Manager 8.7, you might observe a `Not connected remote SRM` status in the Site Recovery UI Summary tab with the following error. `"SRM Server cannot connect to vCenter Server at '<vc-address>:443/sdk'. Permission to perform this operation was denied."` This might happen when the remote vCenter Server has multiple Site Recovery Manager instances installed on it and you use it as a shared recovery site.

Workaround: Use the Site Recovery user interface to reconnect the Site Recovery Manager pair.

Reprotect fails with an error "Unable to reverse replication for the virtual machine ...The operation is not allowed in the current state"

In large-scale environments with lots of datastore modification operations, reprotect might fail due to overloaded OSFS module of vSAN.

Workaround: Verify that there are no inaccessible virtual machines. See *Virtual Machine Appears as Noncompliant, Inaccessible or Orphaned in vSAN* in the *vSAN Monitoring and Troubleshooting* guide.

When a virtual machine is on a vSAN datastore and is replicated by vSphere Replication with NSX-T present, it takes additional 60 seconds to recover when migrating back to the protected site after being recovered on the recovery site

The NSX-T is storing port configuration inside the VM directory, which is not replicated by vSphere Replication. When the VM is migrated to the recovery site, the port configuration becomes invalid and is removed. Migrating the VM back to the protected site and resolving the removed port configuration causes a 60 second per VM delay when registering it in the vCenter Server inventory.

Workaround: Fixed in ESXi version 8.0.2. Update all target recovery ESXi hosts to avoid the issue.

Planned migration after reprotect fails during vSphere Replication synchronization with an error

During reprotect of large scale VMs, the VMware Crypto Manager module that takes care of the encryption keys on the hosts looses track of some of the encryption keys. As a result the planned migration cannot complete successfully and fails with the following error.

```
"An encryption key is required."
```

Workaround 1: Use the following PowerCLI cmdlet to unlock all locked virtual machines in the vCenter Server instance.

```
Get-VM|Where-Object {$_.ExtensionData.Runtime.CryptoState -eq 'locked'} | Unlock-VM
```

Workaround 2: In the vSphere UI, navigate to the Summary tab of the virtual machine and click **Issues and Alarms > Virtual Machine Locked Alarm > Actions > Unlock VM**.

Workaround 3: Fixed in vCenter Server version 8.0.2 version. Update the recovery site to vCenter Server 8.0.2 to avoid the issue.

Disaster recovery with stretched storage freezes during the 'Change recovery site storage to writable' step

When using Pure Storage storage arrays with unified configuration for stretched storage, if Site Recovery Manager on the protected site loses connection but the vCenter Server remains accessible, disaster recovery freezes during the 'Change recovery site storage to writable' step. This is related to the way Pure Storage SRA commands operate.

Workaround: Navigate to the protected site and power off the virtual machines you are trying to recover. This unblocks the disaster recovery operation and all virtual machnies are successfully recovered.

Changing the value of the recovery.powerOnTimeout settings does not change the actual timeout

When you attempt to change the value of the `recovery.powerOnTimeout` advanced setting, the changes do not take effect.

Workaround:

1. In the vSphere 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. Click **Edit** and set `replication.archiveRecoverySettingsLifetime` to 0.
5. Repeat the steps on the other site.
6. In the left pane, click **Configure > Advanced Settings > Recovery**.
7. Click **Edit** and set `recovery.powerOnTimeout` to the required value.
8. Repeat the step on the other site.

Two similar items for VMware Site Recovery integration plug-in are visible in the vCenter Server Client Plug-ins list

When you install vSphere Replication or Site Recovery Manager on vCenter Server 8.0, the vCenter Server Client Plug-ins list contains two similar items for the VMware Site Recovery integration plug-in. This does not affect the plug-in functionality as long as both plug-ins are activated or deactivated.

Workaround: No actions are required to continue to use the plug-in functionality. If you must deactivate the plug-in, deactivate both plug-ins. If you want to activate the plug-in, activate both plug-ins.

Disaster recovery fails with an error

Disaster recovery for virtual machines residing on stretched storage fails with the following error: `"A general system error occurred: Cannot allocate memory"`

Workaround: Re-run the disaster recovery operation.

Recovery plan in a Recovery incomplete state cannot be successfully completed

If a failover with vMotion is interrupted during the vMotion step and the plan goes into **Recovery interrupted** state, all the following plan re-runs might fail at the **Change recovery site storage to writable** step. The error at this step is incorrect and Failover is successfully completed. However, the plan stays in **Recovery incomplete** state and cannot be switched back to **Ready** state because of this.

Workaround: To successfully failback VMs to the primary site, recreate the Protection Groups and the Recovery Plan.

Reprotect fails with an error

When you are replicating virtual machines at a large scale, reprotect might fail with the following error: `"Unable to reverse replication for the virtual machine A generic error occurred in the vSphere Replication Management Server "java.net.SocketTimeoutException: Read timed out"`

Workaround:

1. Navigate to the `/opt/vmware/hms/conf/hms-configuration.xml` file.
2. Increase the value of `hms-default-vlsi-client-timeout` to 15 minutes on both sites.
3. Restart the HMS services.

Recovery plan with a vSphere Replication replicated virtual machine fails with an error

If the vSphere Replication replicated virtual machine with MPITs has several replicated disks on several different datastores and you stop the replication of one disk and detach it from the protection group, the failover will fail with the following error `"Invalid configuration for device '0'".`

Workaround: Do not stop the replication of one of the disks and do not detach the disk from the protection group.

Reprotect operation for a large scale of VMs fails with an error

When you try to perform a reprotect operation for a large scale of VMs, the process might fail with one of the following erros:

```
Unable to reverse replication for the virtual machine <VM_name>
```

or

```
A general system error occurred: Failed to open virtual disk
```

These problems might be observed due to temporary storage overload or network issues.

Workaround: Retry the reprotect operation for these VMs.

After performing disaster recovery and then powering on the same site some virtual machines go into orphaned state

When powering on the down site after performing a Disaster Recovery in a Stretched Storage environment, some virtual machines might appear in an orphan state. The problem is observed for virtual machine protection groups in a Stretched Storage environment.

Workaround: Remove the entries for all orphaned virtual machines from the vCenter Server inventory before running other Site Recovery Manager workflows.

When a replicated disk is on Virtual Volumes storage and is resized, the disk is recovered as Thin Provisioned regardless of original disk type

The internal working of the disk resize operation involves making a copy of the disk, which due to the specifics of Virtual Volumes storage defaults to Thin Provisioned disk type regardless of the base disk type. The disk resize is completed but the resulting resized disk now has the Thin Provisioned type when recovered by vSphere Replication.

Workaround: If required, you can change the disk type manually after recovery.

One or more replications go into Error (RPO violations) state after reprotect operation

After you perform a reprotect operation, one or more of the replications go into error state with the following error:

```
A problem occurred with the storage on datastore path '[<datastore-name>] <datastore-
path>/hbrdisk.RDID-<disk-UUID>.vmdk
```

Workaround:

1. Remove the replication
2. Configure the replication again, using seed disks.

The Configure Replication wizard starts lagging

If you are using a Mozilla Firefox browser on an Apple Mac OS, you might experience UI performance degradation and lagging in the Configure Replication wizard.

Workaround: Use a Chrome browser.

Reprotect fails with error: Protection Group '{protectionGroupName}' has protected VMs with placeholders which need to be repaired.

When Site Recovery Manager runs a reprotect on the protection group, Site Recovery Manager cannot repair the protected virtual machines nor restore the placeholder virtual machines. The error occurs when the first reprotect operation fails for a virtual machine because the corresponding placeholder operation failed. The protected virtual machine is marked with a configuration error and protection group is left in a partially reprotected state.

Workaround:

1. Rerun reprotect with the **force cleanup** option enabled. This option completes the reprotect operation and enables the **Recreate placeholder** option. Note that the reprotect execution will be marked with success status on completion.
2. Explicitly initiate **Recreate placeholder** operation to repair the affected protected virtual machines and to restore the placeholder virtual machines. Note that if this is not done and you run disaster recovery workflow, the recovery of

those virtual machines will fail with the following error `Placeholder VM for the protected VM '<vm-name>' is missing.`

Some of the recovered virtual machines throw the following alarm 'vSphere HA virtual machine failover failed'

During a Site Recovery Manager workflow, post Test Recovery or Failover operations, some of recovered virtual machines might throw the following alarm: `vSphere HA virtual machine failover failed.` From Site Recovery Manager perspective, there is no functional impact as all virtual machines are recovered successfully.

Workaround: None. You must acknowledge the alarm.

DNS servers are available in the network configuration of the Site Recovery Manager Appliance Management Interface, even if you selected static DNS without DNS servers

When the requirements of the network settings are for No DNS servers but with automatic DHCP adapter configuration, the setting static DNS and DHCP in the adapter configuration results in DNS servers acquired from DHCP.

Workaround: Use 127.0.0.1 or ::1 in the static DNS servers list, depending on the selected IP protocol.

Reprotect fails when using stretched storage on some storage arrays

The command to reverse the replication on some devices is skipped intentionally when the devices are already in the expected state. As a result the storage array are not getting required notifications and this causes the reprotect operation to fail.

Workaround:

1. Navigate to the vmware-dr.xml file and open it in a text editor.
2. Set the configuration flag `storage.forcePrepareAndReverseReplicationForNoopDevices` to true.

```
<storage>
<forcePrepareAndReverseReplicationForNoopDevices>true</forcePrepareAndReverseReplicationForNoopDevices>
</storage>
```

3. Save the file and restart the Site Recovery Manager server service.

Exporting grids is not working in the Microsoft Edge browser

When you open a view with a grid, select **Export**, and click **All rows/Selected rows** no file is downloaded. When you attempt to export and download the history of a recovery plan, you receive an error in the console and the download files are corrupted.

Workaround: Upgrade to the latest version of the Microsoft Edge browser based on the Chromium engine.

PowerCLI Connect-SrmServer command fails to connect to the Site Recovery Manager appliance using the default port

When you try to connect to the Site Recovery Manager appliance by using the PowerCLI `Connect-SrmServer` command, the connection fails with the following error: `Unable to connect to the remote server.`

Workaround: Specify port 443 to the Site Recovery Manager appliance by using the following command `Connect-SrmServer -Port 443`. For a complete list of all Site Recovery Manager network ports, see *Network Ports for Site Recovery Manager*.

Devices and Datastores information is missing during the failover of a recovery plan with array-based replication protection groups

When you run a recovery plan failover, depending on the SAN type and whether it detaches the datastore from the host during recovery, the information in the Devices and the Datastores tabs might disappear during the failover process.

Workaround: None. The information in both tabs appears again after a successful reprotect.

Customization through IP subnet mapping rules is not fully supported for Linux VMs using multiple NICs which are named ethX

Site Recovery Manager does not fully support IP rule-based customization for Linux virtual machines that have multiple NICs, if the NICs have mixed DHCP and static IP settings. Site Recovery Manager customizes only the NICs with static IP addresses for which it has matching IP subnet mapping rule and might clear some configuration settings for the other NICs configured with DHCP. Known issue related to this scenario was observed for Red Hat Enterprise Linux 6.x/7.x and CentOS 6.x/7.x, where Site Recovery Manager customization deletes `/etc/sysconfig/network-scripts/ifcfg-ethX` files for the NICs configured with DHCP and successfully customizes the rest with static IP settings according to the matched IP subnet mapping rule. This issue also happens when the VM's NICs are all configured with static IP addresses, but some of them have a matching IP subnet rule while others do not. Some configuration settings for those NICs without a matching IP subnet rule might be cleared after IP customization.

Workaround: For correct IP customization for Linux VMs using multiple NICs with some of them having a matching IP subnet mapping rule while the others do not, use the Manual IP Customization Site Recovery Manager option.

The Site Recovery UI becomes unusable showing a constant stream of 403 - OK error message

The Site Recovery UI shows no data and an error 403 - OK.

Workaround:

1. Log out from Site Recovery UI and log in again.
2. Disable the browser's 'Restore last session' checkbox. For Chrome disable the 'Continue where you left off' option.

Datastore cluster that consists of datastores that are not replicated or are from different consistency groups visible to Site Recovery Manager does not have an SRM warning.

You create a datastore cluster that consists of datastoreas that are not all in a same consistency group or are not replicated. A Site Recovery Manager warning should exist but does not.

Workaround: None

Export report from the Recovery Plan History or the Recovery Steps screens does not work when using Microsoft Edge browser

When you try to export the report from the Recovery Plan History or the Recovery Steps screens using MS Edge browser, you get the following error in the dev console.

```
ERROR XML5610: Quote character expected.
```

```
ERROR Error: Invalid argument.
```

This is a known Microsoft Edge browser issue with XSLTProcessor used to transform server's xml into html.

Workaround: Use Chrome, Microsoft Internet Explorer, or Firefox browser.

This issue is fixed in the Chromium-based version of the Microsoft Edge browser.

When you right-click on a replicated VM and select Reconfigure Replication in the vSphere UI, the pop-up window for the Site Recovey UI is blocked without notification in Mozilla Firefox browser

By default the Site Recovery UI opens in a new tab. When you right-click on a replicated VM and select Reconfigure Replication in the vSphere UI, the pop-up window for the Site Recovey UI is blocked without notification in Mozilla Firefox browser.

Workaround: From the Options menu in Mozilla Firefox, select the Content tab and add the URL of the vCenter Server to the Pop-ups exception list.

The Test and Recovery operations fail if a vSAN stretched cluster has one fault domain that is not available

If you test or recover a VM on a vSAN stretched cluster with one fault domain that is not available, the operation fails. The cause is that the vSAN Default Storage Policy cannot be satisfied and provisioning a VM with Site Recovery Manager on the storage fails.

Workaround: Register the recovered VM on the vSAN stretched cluster manually. The VM becomes compliant with the vSAN Default Storage Policy when the fault domain is available.

Your datastore might appear as inactive in the inventory of the original protected site after reprotect

If you use a stretched storage and run reprotect after a disaster recovery, you might receive the following warning.

```
The requested object was not found or has already been deleted.
```

After reprotect, the datastore in the inventory of the original protected site appears as inactive.

Workaround: Refresh or rescan the storage adapters.

1. Click the **Configure** tab and click **Storage Adapters**.
2. Click the **Refresh** or **Rescan** icon to refresh or rescan all storage adapters.

Recovery of an encrypted VM might fail during the Power On step if the encryption key is not available on the recovery site

If you recover an encrypted VM and the encryption key used on the protected site is not available on the recovery site during the recovery process, the recovery fails when Site Recovery Manager powers on the VM.

Workaround: Complete the following steps.

1. Remove the encrypted VM from the inventory of the recovery site.
2. Ensure that the Key Management Server on the recovery site is available and that the encryption key used on the protected site is available on the recovery site.
3. Register the encrypted VM to the inventory of the recovery site.
4. In the Site Recovery Manager user interface, open the recovery settings of the encrypted VM and disable power on of the VM during recovery.
5. Rerun recovery.

Planned Migration might fail with an error for VMs protected on vSphere Virtual Volumes datastore

If you have VMs protected on vSphere Virtual Volumes datastores, the planned migration of the VMs might fail with the following error on the Change recovery site storage to writable step.

```
Error - Storage policy change failure: The vSphere Virtual Volumes target encountered a
vendor specific error. Invalid virtual machine configuration. A specified parameter was
not correct: path.
```

Workaround: Rerun the recovery plan.

The IP customization or in-guest callout operations might fail with Error - `Failed to authenticate with the guest operating system using the supplied credentials`

Workaround:

When **recovery.autoDeployGuestAlias** option in Advanced Settings is TRUE (default).

- If the time of the ESX host where the VM is recovered and running is not synchronized with vCenter Single Sign-On servers on the recovery site.
- If the guest OS of the recovered VM is Linux and the time is ahead from the ESX host on which the recovered VM is running, update the configuration parameters of the VM by using the following procedure and rerun the failed recovery plan.
  a. Right-click the recovered VM.
  b. Click **Edit** Settings.
  c. In the **Options** tab, click **General**.
  d. Click **Configuration** to update the configuration parameters.
  e. Click **Add Row** and enter `time.synchronize.tools.startup.backward` in the **Name** text box and **TRUE** in the **Value** text box.
  f. Click **OK** to confirm.

When the **recovery.autoDeployGuestAlias** option in Advanced Settings is FALSE.

- Ensure proper time synchronization between your guest OS on the protected VM and vCenter Single Sign-On servers on the recovery site.
- Ensure that your protected VMs have correct guest aliases configured for the Solution User on the recovery site SRM server. For more information see, the description of **recovery.autoDeployGuestAlias** option in *Change Recovery Settings*.

For more information, see the related troubleshooting sections in the *Site Recovery Manager 8.8 Administration* guide.

Replacing the SSL certificate of vCenter Server causes certificate validation errors in Site Recovery Manager.

If you replace the SSL certificate on the vCenter Server system, a connection error might occur when Site Recovery Manager attempts to connect to vCenter Server.

Workaround: For information about how to update vCenter Server certificates and allow solutions such as Site Recovery Manager to continue to function, see http://kb.vmware.com/kb/2109074.

Test network mappings are not deleted when the corresponding network mapping is deleted.

If, when you create network mappings, you configure a specific network mapping for testing recovery plans, and if you subsequently delete the main network mapping, the test network mapping is not deleted, even if the recovery site network that you configured is not the target of another mapping. For example:

- You configure a network mapping from *Protected_Network_Main* on the protected site to *Recovery_Network_Main* on the recovery site.
- You configure a test network mapping from *Recovery_Network_Main* to *Recovery_Network_Test* to use as the network for testing recovery plans.
- *Recovery_Network_Main* on the recovery site is not used as the target for any other network mappings.
- You delete the network mapping from *Protected_Network_Main* to *Recovery_Network_Main* that is used for full recoveries.
- The test network mapping from *Recovery_Network_Main* to *Recovery_Network_Test* is not deleted.

Workaround: Delete the test network mapping manually.

Dependency between two virtual machines, one vMotion enabled and one vMotion disabled, on stretched storage fails during a migrating workflow.

Workarounds: Remove dependency between virtual machines and rerun planned migration with vMotion. Manually re-enable dependency for future recovery workflows.

If you want to preserve the dependency between virtual machines, then run planned migration without vMotion. Both virtual machines migrate as regular virtual machines according to the dependency order.

Site Recovery Manager fails to track removal of non-critical virtual machines from the vCenter Server inventory, resulting in MONF errors in recovery, test recovery and test cleanup workflows.

Site Recovery Manager loses connections to the vCenter Servers on the protected and recovery sites and cannot monitor removal of non-critical virtual machines.

Workaround: Restart the Site Recovery Manager server.

Cleanup fails if attempted within 10 minutes after restarting recovery site ESXi hosts from maintenance mode.

The cleanup operation attempts to swap placeholders and relies on the host resilience cache which has a 10 minute refresh period. If you attempt a swap operation on ESXi hosts that have been restarted within the 10 minute window, Site Recovery Manager does not update the information in the Site Recovery Manager host resiliency cache, and the swap operation fails. The cleanup operation also fails.

Workaround: Wait for 10 minutes and attempt cleanup again.

Recovery Fails to Progress After Connection to Protected Site Fails

If the protection site becomes unreachable during a deactivate operation or during RemoteOnlineSync or RemotePostReprotectCleanup, both of which occur during reprotect, then the recovery plan might fail to progress. In such a case, the system waits for the virtual machines or groups that were part of the protection site to complete those interrupted tasks. If this issue occurs during a reprotect operation, you must reconnect the original protection site and restart the recovery plan. If this issue occurs during a recovery, it is sufficient to cancel and restart the recovery plan.

Recovered VMFS volume fails to mount with error: Failed to recover datastore.

This error might occur due to a latency between vCenter, ESXi, and Site Recovery Manager Server.

Workaround: Rerun the recovery plan.

Temporary Loss of vCenter Server Connections Might Create Recovery Problems for Virtual Machines with Raw Disk Mappings

If the connection to the vCenter Server is lost during a recovery, one of the following events might occur:

- The vCenter Server remains unavailable, the recovery fails. To resolve this issue re-establish the connection with the vCenter Server and re-run the recovery.
- In rare cases, the vCenter Server becomes available again and the virtual machine is recovered. In such a case, if the virtual machine has raw disk mappings (RDMs), the RDMs might not be mapped properly. As a result of the failure to properly map RDMs, it might not be possible to power on the virtual machine or errors related to the guest operating system or applications running on the guest operating system might occur.
  - If this is a test recovery, complete a cleanup operation and run the test again.
  - If this is an actual recovery, you must manually attach the correct RDM to the recovered virtual machine.

Refer to the vSphere documentation about editing virtual machine settings for more information on adding raw disk mappings.

Error in recovery plan when shutting down protected virtual machines: `Error - Operation timed out: 900 seconds during Shutdown VMs at Protected Site step.`

If you use Site Recovery Manager to protect datastores on arrays that support dynamic swap, for example Clariion, running a disaster recovery when the protected site is partially down or running a force recovery can lead to errors when rerunning the recovery plan to complete protected site operations. One such error occurs when the protected site comes back online, but Site Recovery Manager is unable to shut down the protected virtual machines. This error usually occurs

when certain arrays make the protected LUNs read-only, making ESXi unable to complete I/O for powered on protected virtual machines.

Workaround: Reboot ESXi hosts on the protected site that are affected by read-only LUNs.

Planned migration fails with Error: Unable to copy the configuration file...

If there are two ESXi hosts in a cluster and one host loses connectivity to the storage, the other host can usually recover replicated virtual machines. In some cases the other host might not recover the virtual machines and recovery fails with the following error: `Error: Unable to copy the configuration file...`

Workaround: Rerun recovery.

Test cleanup fails with a datastore unmounting error.

Running cleanup after a test recovery can fail with the error `Error - Cannot unmount datastore 'datastore_name' from host 'hostname'. The operation is not allowed in the current state..` This problem occurs if the host has already unmounted the datastore before you run the cleanup operation.

Workaround: Rerun the cleanup operation.

VMware Aria Automation Orchestrator Plug-In for VMware Site Recovery Manager 8.8 Release Notes

This document contains the following sections

Introduction

Site Recovery Manager 8.8 | 21 SEP 2023 | Build 22434509 VMware Aria Automation Orchestrator Plug-In for Site Recovery Manager 8.8 | 21 SEP 2023 | Build 22432313 | Download Check for additions and updates to these release notes.

What's New in VMware Aria Automation Orchestrator Plug-In for VMware Site Recovery Manager 8.8

The VMware Aria Automation Orchestrator Plug-in for VMware Site Recovery Manager 8.8 release adds support for VMware vRealize Orchestrator 8.12.2.

About the VMware Aria Automation Orchestrator Plug-In for VMware Site Recovery Manager 8.8

With the VMware Aria Automation Orchestrator plug-in for VMware Site Recovery Manager, Site Recovery Manager administrators can simplify the management of their Site Recovery Manager infrastructure by extending the robust workflow automation platform of VMware Aria Automation Orchestrator. You build these workflows by using the drag-and-drop capability of the workflow editor in the VMware Aria Automation Orchestrator client. VMware Aria Automation Orchestrator uses the plug-in to access the functionality of Site Recovery Manager and the Site Recovery Manager API. The included prebuilt workflows simplify the process of creating custom workflows.

The VMware Aria Automation Orchestrator plug-in for VMware Site Recovery Manager 8.8 release runs with VMware Aria Automation Orchestrator 8.12.2. For more information on interoperability with earlier or later releases of VMware Aria Automation Orchestrator, see the VMware Product Interoperability Matrices.

Installation and Upgrade

The VMware Aria Automation Orchestrator plug-in for Site Recovery Manager software is distributed as an VMware Aria Automation Orchestrator application file.

You must install and configure VMware Aria Automation Orchestrator before you install the VMware Aria Automation Orchestrator plug-in for Site Recovery Manager, see the *Installing and Configuring VMware Aria Automation Orchestrator 8.12* documentation.

For information about how to install the Automation Orchestrator plug-in for Site Recovery Manager on VMware Aria Automation Orchestrator 8.12, see the *Install, update, or delete a plug-in* topic in the *VMware Aria Automation Orchestrator 8.12* documentation.

After you install the VMware Aria Automation Orchestrator plug-in for Site Recovery Manager, you must configure the connection between the VMware Aria Automation Orchestrator instance and the vCenter Server instance on your Site Recovery Manager site. For information about how to configure the connection with your vCenter Server, see the *VMware Aria Automation Orchestrator 8.12* documentation.

After you install the Orchestrator plug-in for Site Recovery Manager, you can find the Site Recovery Manager workflows in the VMware Aria Automation Orchestrator UI:

1. Go to **Library > Workflows**
2. Search for the workflow by name or switch to tree view from the top right icon. In tree view you can find the workflows under **Library >SRM** folder.

Before you can run the Site Recovery Manager workflows, you must configure the plug-in to work with your Site Recovery Manager by selecting **Library** > **SRM > Configuration** and running the following workflows:

1. Run the **Configure Local Sites** workflow.
2. Run the **Configure Remote Site** workflow.
3. Run the **Login Remote Site** workflow.

You must run the Login Remote Site workflow once per VMware Aria Automation Orchestrator Client session to log in to Site Recovery Manager on the remote site. VMware Aria Automation Orchestrator automatically logs out of Site Recovery Manager when you log out of the VMware Aria Automation Orchestrator client.

For information about how to uninstall your Site Recovery Manager plug-in, see the *Delete a Plug-In* topic in the *Installing and Configuring VMware vRealize Orchestrator* documentation.

Example Workflows

The VMware Aria Automation Orchestrator plug-in for Site Recovery Manager includes example workflows that demonstrate how you can automate Site Recovery Manager operations by using Orchestrator, such as:

- Create VM and Protect It:
  a. Creates a virtual machine
  b. Adds the virtual machine to an existing protection group
- Create Protection Group for Array Based Replication, Protect Virtual Machines, Add Protection Group to Recovery Plan:
  a. Creates an array-based protection group
  b. Protects the virtual machines in a given datastore by adding that datastore to the protection group
  c. Adds the new protection group to an existing recovery plan

Caveats and Limitations

- The VMware Aria Automation Orchestrator Plug-In for Site Recovery Manager 8.8 supports vRealize Orchestrator 8.10.x with certain limitations. For more information, see the *Known Issues from Previous Releases* section.
- If you change the Site Recovery Manage certificate, the Site Recovery Manager site is no longer visible in VMware Aria Automation Orchestrator inventory. You must run 'Configure Local Sites' workflow to add the site and accept the new certificate, and then run 'Login Remote Sites' to log in to the site.
- If the protection site is not available, you cannot perform the following actions by using vRealize Orchestrator workflows, but you can use the Site Recovery Manager user interface instead:
  - Create a recovery plan or change VM recovery settings;
  - Add or remove a test network mapping to a recovery plan;
  - Add or remove a protection group to an existing recovery plan.

Known Issues from Previous Releases

When you attempt to register a new vCenter Server instance you receive an error in the vCenter Server plug-in

When you attempt to register a new vCenter Server instance, the operation fails because of a vmodl mismatch error. `(unusable: (vmodl.fault.InvalidType) { faultCause = null, faultMessage = null, argument = ImageLibraryManager })` As a result you are blocked from using the VMware Aria Automation Orchestrator plug-in for Site Recovery Manager 8.7 as it depends on the vCenter Server registration from the vCenter plug-in. The issue is present with the out-of-the-box vCenter Server plug-in that comes with vRealize Orchestrator versions 8.10.1, 8.10.2, 8.11, 8.11.1, and 8.11.2.

Workaround: Download and install the latest vCenter Server plug-in from the marketplace.

The Configure Local Sites workflow fails when using the plug-in with vRealize Orchestrator 8.9.1 and higher

When you run the Configure Local Sites workflow, the workflow fails at the Validate step with the following exception: `"com.vmware.vim.vmomi.core.exception.CertificateValidationException: Server certificate chain is not trusted and thumbprint doesn't match"`

Workaround:

1. SSH into the vRealize Orchestrator appliance.
2. To synchronize the local keystore with vRealize Orchestrator, run the following command:

```
vracli cluster exec -- bash -c 'base64 -d <<< "a3ViZWN0bCAtbiBwcmVsdWRlIGV4ZWMgLXQgJChrdWJlY3RsIGdldCBw-
b2QgLW4gcHJlbHVkZSAtbCBhcHA9dmNvLWFwcCAtbyBqc29ucGF0aD0iey5pdGVtc1swXS5tZXRhZGF0YS5uYW1lfSIgLS1maWVsZC1zZ-
WxlY3RvciBzcGVjLm5vZGVOYW1lPSQoY3VycmVudF9ub2RlKSkgLWMgdmNvLXNlcnZlci1hcHAgLS0gYmFzaCAtYyAiYmFzZTY0IC1kID-
w8PCAnUzFOZlVFRlVTRDBpTDNWemNpOXNhV0l2ZG1OdkwyRndjQzF6WlhKMlpYSXZZMjl1Wmk5elpXTjFjbWwwZVM5cWMzT-
mxZMkZqWlhKMGN5SUtURTlIWDBaSlRFVTlKRXhQUTBGTVNFOVRWRjlNVDBkZlJrbE1SVjlFU1ZKRlExUlBVbGt2ZG5Kdlgye-
HZZMkZzWDJ0bGVYTjBiM0psWDNONWJtTXViRzluQ2dwR1NWQlRYMDFQUkVWZlJVNUJRa3hGUkQwaVpXNWhZbXhsWkNJS1JrbF-
FVMTlOVDBSRlgxTlVVa2xEVkQwaWMzUnlhV04wSWdwcFppQmJXeUFpSkVaSlVGTmZUVTlFUlNJZ1BYNGdYaWdrUmtsUVUxOU5UM-
FJGWDBWT1FVSk1SVVI4SkVaSlVGTmZUVTlFUlY5VFZGSkpRMVFwSkNCZFhRcDBhR1Z1Q2lBZ0lDQkxVMTlVV1ZCRlBTSkNRMF-
pMVXlJS1pXeHpaUW9nSUNBZ1MxTmZWRmxRUlQwaVNrdFRJZ3BtYVFvS0NteHZaMTl0WlhOellXZGxLQ2tnZXdvZ0lHVmphRzh-
nSWxza0tHUmhkR1VnTFMxMWRHTWdJaXNsUmxRbFZDNGxNMDVhSWlsZElDUXhJaUErUGlBa1RFOUhYMFpKVEVVS2ZRb0tablZ1WT-
NScGIyNGdhVzV6ZEdGc2JGOWpaWEowS0NrZ2V3b2dJQ0FnYkc5allXd2dZV3hwWVhNOUpERUtJQ0FnSUd4dlkyRnNJSEJsYlY5em-
RISnBibWM5SkRJS0lDQWdJR2xtSUZzZ0xYb2dJaVJoYkdsaGN5SWdYVHNnZEdobGJnb2dJQ0FnSUNBZ0lHVmphRzhnSWtObGNuUn-
BabWxqWVhSbElHRnNhV0Z6SUdseklHVnRjSFI1TGlCRGIzVnNaQ0J1YjNRZ2MzbHVZMmh5YjI1cGVtVWdkR2hsSUdObGNuUnBab-
WxqWVhSbExpSUtJQ0FnSUNBZ0lDQnNiMmRmYldWemMyRm5aU0FpUTJWeWRHbG1hV05oZEdVZ1lXeHBZWE1nYVhNZ1pXMXdkSGt1SU-
VOdmRXeGtJRzV2ZENCemVXNWphSEp2Ym1sNlpTQjBhR1VnWTJWeWRHbG1hV05oZEdVdUlnb2dJQ0FnSUNBZ0lISmxkSFZ5Yml-
BeENpQWdJQ0JtYVFvZ0lDQWdhV1lnV3lBdGVpQWlKSEJsYlY5emRISnBibWNpSUYwN0lIUm9aVzRLSUNBZ0lDQWdJQ0JsWTJod-
klDSkRaWEowYVdacFkyRjBaU0J3WlcwZ2FYTWdaVzF3ZEhrdUlFTnZkV3hrSUc1dmRDQnplVzVqYUhKdmJtbDZaU0JqWlhKMGFXWn-
```

```
BZMkYwWlRvZ0pHRnNhV0Z6SWk0S0lDQWdJQ0FnSUNCc2IyZGZiV1Z6YzJGblpTQWlRMlZ5ZEdsbWFXTmhkR1VnY0dWdElHbH-
pJR1Z0Y0hSNUxpQkRiM1ZzWkNCdWIzUWdjM2x1WTJoeWIyNXBlbVVnWTJWeWRHbG1hV05oZEdVNklDUmhiR2xoY3k0aUNpQWd-
JQ0FnSUNBZ2NtVjBkWEp1SURJS0lDQWdJR1pwQ2dvZ0lDQWdaV05vYnlBaVUzbHVZMmh5YjI1cGVtbHVaeUJqWlhKMGFXWnBZMkY-
wWlNBa1lXeHBZWE1nZEc4Z2JHOWpZV3dnYTJWNWMzUnZjbVVpQ2lBZ0lDQnNiMmRmYldWemMyRm5aU0FpVTNsdVkyaHliMjVwZW1s-
dVp5QmpaWEowYVdacFkyRjBaU0IzYVhSb0lHRnNhV0Z6T2lBa1lXeHBZWE1nZEc4Z2JHOWpZV3dnYTJWNWMzUnZjbVV1WEc0Z1EyVn-
lkR2xtYVdOaGRHVTZJRnh1SUNSd1pXMWZjM1J5YVc1bklnb0tJQ0FnSUhSbGMzUWdMV1FnTDNWemNpOXNhV0l2ZG1OdkxXTnNhUzl-
tYVhCekx5QjhmQ0J5Y0cwZ0xXa2dMUzF1YjJSbGNITWdMM1pqYnkxalptY3RZMnhwTG5Kd2JRb2dJQ0FnUWtOZlJrbFFVMTlLUVZKVF-
BTUW9abWx1WkNBdmRYTnlMMnhwWWk5MlkyOHRZMnhwTDJacGNITXZJQzF1WVcxbElDY3FabWx3Y3lvbklDMTBlWEJsSUdaOGVHRn-
laM01nZkhSeUlDY2dKeUFuT2ljcENpQWdJQ0JDUTE5UFVGUlRQU0l0Y0hKdmRtbGtaWEp3WVhSb0lDUjdRa05mUmtsUVUxOUtRVkpU-
ZlNBdGNISnZkbWxrWlhJZ2IzSm5MbUp2ZFc1amVXTmhjM1JzWlM1cVkyRnFZMlV1Y0hKdmRtbGtaWEl1UW05MWJtTjVRMkZ6ZEd4bFJtb-
HdjMUJ5YjNacFpHVnlJZ29LSUNBZ0lHTmxjblJmWm1sc1pUMGtLRzFyZEdWdGNDQXZkRzF3TDJObGNuUXVNUzVZV0ZndWNHVn-
RLUW9nSUNBZ1pXTm9ieUFpSkhCbGJWOXpkSEpwYm1jaUlENGdKR05sY25SZlptbHNaUW9nSUNBZ2JHOWpZV3dnY21WemRXeD-
BQU1FvYTJWNWRHOXZiQ0FrUWtOZlQxQlVVeUF0YTJWNWMzUnZjbVVnSkV0VFgxQkJWRWdnTFhOMGIzSmxkSGx3WlNBa1MxTmZWR-
mxRU1NBdGMzUnZjbVZ3WVhOeklDUkxVMTlRUVZOVFYwOVNSQ0F0YVcxd2IzSjBZM1Z5ZENBdGJtOXdjbTl0Y0hRZ0xXRnNhV0Z6SUN-
Ja1lXeHBZWE1pSUMxbWFXeGxJQ0lrWTJWeWRGOW1hV3hsSWlrS0lDQWdJR3h2WjE5dFpYTnpZV2RsSUNJa2NtVnpkV3gwSWdvS0lDQWd-
JSEp0SUMxbUlDUmpaWEowWDJacGJHVUtmUW9LWldOb2J5QWlRMkZzWTNWc1lYUnBibWNnZGxKUElFTmxjblJwWm1sallYUmxjeTR-
pQ2t0RldWTlVUMUpGWDB4SlUxUTlKQ2d2ZFhOeUwyeHBZaTkyWTI4dlkyWm5MV05zYVM5aWFXNHZkbkp2TFhSb2FXNHRZMlpuTG5Ob0l-
HdGxlWE4wYjNKbElHeHBjM1FwQ214dloxOXRaWE56WVdkbElDSkxaWGx6ZEc5eVpTQmpiMjUwWlc1ME9pQWtTMFZaVTFSUFVrVmZUR-
WxUVkNJS0NpTWdRMjkxYm5RZ2RHaGxJR05sY25ScFptbGpZWFJsY3dwalpYSjBYMk52ZFc1MFBTUW9aV05vYnlBaUpFdEZXVk5VVD-
FKRlgweEpVMVFpSUh3Z1ozSmxjQ0FpUVd4cFlYTTZJaUI4SUhkaklDMXNLUXBzYjJkZmJXVnpjMkZuWlNBaVJtOTFibVFnSkdObGNu-
UmZZMjkxYm5RZ1kyVnlkR2xtYVdOaGRHVnpMaUlLQ2lNZ1NYUmxjbUYwWlNCdmRtVnlJR05sY25ScFptbGpZWFJsY3dwbWIzSWd-
hVzVrWlhnZ2FXNGdKQ2h6WlhFZ01TQWtZMlZ5ZEY5amIzVnVkQ2s3SUdSdkNpQWdZM1Z5Y21WdWRGOWpaWEowUFNRb1pXTm9ieUF-
pSkV0RldWTlVUMUpGWDB4SlUxUWlJSHdnWVhkcklDSXZRV3hwWVhNNkwzdHBLeXQ5YVQwOUpHbHVaR1Y0SWlrS0lDQmpkWEp5Wl-
c1MFgyRnNhV0Z6UFNRb1pXTm9ieUFpSkdOMWNuSmxiblJmWTJWeWRDSWdmQ0JoZDJzZ0p5OUJiR2xoY3pvdklIdHdjbWx1ZEN-
Ba01uMG5LUW9nSUdOMWNuSmxiblJmY0dWdFBTUW9aV05vYnlBaUpHTjFjbkpsYm5SZlkyVnlkQ0lnZkNCaGQyc2dKeTlDUlVkSlR-
pQkRSVkpVU1VaSlEwRlVSUzhzTDBWT1JDQkRSVkpVU1VaSlEwRlVSUzhnZTNCeWFXNTBJQ1F3ZlNjcENpQWdhVzV6ZEdGc2JGOWpaWE-
owSUNJa1kzVnljbVZ1ZEY5aGJHbGhjeUlnSWlSamRYSnlaVzUwWDNCbGJTSUtaRzl1WlE9PScgfCBiYXNoIC0i" | bash -'
```

Note: You must run the command after the workflow fails, otherwise the certificate is not imported and is not synchronized.

3. Re-run the Configure Local Sites workflow.

No Site Recovery Manager sites are displayed in the VMware Aria Automation Orchestrator inventory if the user does not have privileges on all of the sites in an N:1 shared recovery site configuration

You can have more than one Site Recovery Manager instance installed against a certain vCenter Server instance. If you run the Configure Local Sites workflow with a user that does not have privileges on all Site Recovery Manager instances, no Site Recovery Manager sites are displayed in the VMware Aria Automation Orchestrator inventory. The Site Recovery Manager sites that the user has privileges on are also not displayed.

Workaround: Run the Configure Local Sites workflow with a user that has privileges on all Site Recovery Manager instances.

Running Configure Remote Site workflow fails for a Site Recovery Manager instance that is paired after it has been added to VMware Aria Automation Orchestrator

If you add an unpaired Site Recovery Manager to a VMware Aria Automation Orchestrator inventory and then pair it, running the execution of Configure Remote Site workflow fails.

Workaround: Restart the VMware Aria Automation Orchestrator server.

Running the Configure Local Sites, Remove Local Sites, or Configure Remote Site workflow makes the existing sessions to the remote sites invalid

Running the Configure Local Sites, Remove Local Sites, or Configure Remote Site workflow makes the established sessions between the local sites and their remote sites invalid.

Workaround: Log in to the remote sites again.

An error occurs if you call the Server.findAllForType(string type, string query) method

You cannot find an object by using only the type name. The following error occurs if you pass only the **type** argument to the `Server.findAllForType(string type, string query)` method : `Unable to execute 'fetchAll' for type : … : 'java.lang.NullPointerException'.`

Workaround:You must pass the optional `query` argument if you call the `Server.findAllForType(string type, string query)` method.

For example: `x = Server.findAllForType(type, "");.`

VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8 Release Notes

This document contains the following sections

Introduction

Site Recovery Manager 8.8 | 21 SEP 2023 | Build 22434509 VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8 | 21 SEP 2023 | Build 22432313 | Download Check for additions and updates to these release notes.

What's New VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8

The VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8 provides the following new features:

Support for VMware Aria Operations 8.12.1.

About the VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8

The VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8 allows VMware administrators to monitor the local Site Recovery Manager services in VMware Aria Operations Manager. The VMware Aria 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 in Site Recovery Manager. Alarms are generated when there are Site Recovery Manager Server connectivity issues encountered or protection groups and recovery plans are in error state. The user interface provides statistics for the number of SRM-related objects and how many of them have errors. For more information, see VMware Site Recovery Manager and VMware Aria Operations.

The VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8 release runs with VMware vRealize Operations 8.12.1. For more information on interoperability with earlier or later releases of VMware Aria Operations Manager, see the VMware Product Interoperability Matrices.

You can download the VMware Aria Operations Management Pack for Site Recovery Manager 8.8 from the download page.

Installation and Configuration

The VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8 software requires VMware vRealize Operations 8.12.1, and Site Recovery Manager 8.8. For information on installing VMware vRealize Operations 8.12.1, see Installing VMware Aria Operations in the VMware Aria Operactions documentation. For information on installing Site Recovery Manager 8.8, see *Deploying the Site Recovery Manager Appliance* in the VMware Site Recovery Manager documentation.

The VMware Aria Operations Management Pack for Site Recovery Manager 8.8 software is distributed as PAK file. You install and configure the management pack by using the Aria Operations interface.

1. Log in to Aria Operations Manager with administrator privileges.
2. From the left menu select **Data Sources** > **Integrations**, and then click **Repository** in the right pane.
3. Click **Add**.
4. Navigate to the `VMware-srm-vrops-mp-8.8-<build number>.pak` file and click **Upload**. When the PAK file is uploaded, click **Next**.
5. Read and agree to the end-user license agreement. Click **Next** to install the management pack.
6. Review the installation progress, and click **Finish** when the installation completes.

After the installation you must configure the VMware Aria Operations Management Pack for Site Recovery Manager 8.8 so that Aria Operation can collect data from the target system. The minimum role required to collect data is **Ready-only**. For more information on roles and permissions, see *Site Recovery Manager Privileges, Roles, and Permissions* and *Using vCenter Server Roles to Assign Privileges*.

1. In the left menu, click **Data Sources** > **Integrations>Accounts**.
2. In the accounts tab, click **Add account**.
3. Select **Site Recovery Manager Adapter**.
4. Enter the required information and click **Add**.
   Note: User name and password are case-sensitive.

Network Ports

VMware Aria Operations Management Pack for Site Recovery Manager requires port 443 (HTTPS protocol) to be open.

Caveats and Limitations

- http://1997837 Restarting the Site Recovery Manager services during the first collection cycle of VMware Aria Operations results in dashboard widgets not working. If this happens, you must re-install the Site Recovery Manager adapter or adapters.

Resolved Issues

Alarms for errors or powered off VMs are triggered for every execution of the Recovery, Reprotect, Test, and Cleanup workflows

The VMware Aria Operations Management Pack for VMware Site Recovery Manager shows alarms for errors and powered off VMs from all previous runs of the Recovery, Reprotect, Test, and Cleanup workflows.

This issue is fixed in VMware Aria Operations Management Pack for VMware Site Recovery Manager 8.8. The management pack shows only the alarms triggered for the last run of the Recovery, Reprotect, Test, and Cleanup workflows.

Known Issues from Previous Releases

Using the vRealize Operations administration page for upgrade of management packs is not supported

Installing updates from the Software Updates pane of the vRealize Operations administration page is not supported for management pack due to a known issue with not updating the visual elements. The issue is fixed in VMware Aria Operations 8.12.

Workaround: Use the standard vRealize Operations UI to upgrade the management pack.

1. From the left menu click **Data Sources>Integrations**, and then click the Repository tab.
2. On the Repository tab, click **Add/Upgrade**.

Protection Group and Recovery Plan subfolders are listed twice in folder tree

Folders that have subfolders might be duplicated when exploring the Object browser view.

Workaround: None.

The Edition key metric for the Site Recovery Manager Site object is not readable

The Edition key metric must represent the type of license Evaluation or Permanent for the related Site Recovery Manager site but the value is not translated properly.

Workaround: None.

The Topology Graph widget does not load

If you are using the vRealize Operations Management pack for Site Recovery Manager with vRealize Operations 8.2 or later, when you open the dashboard for the Site Recovery Manager Configuration Summary, the Topology Graph widget does not load.

Workaround: This is an issue with the widget in vRealize Operations Manager 8.2 and later. Edit the widget without making any changes. That refreshes the widget and it will start working.

Srm Configuration Summary does not show 'Srm Server Configuration' and 'Srm Server Details' widgets

Srm Configuration Summary does not always show 'Srm Server Configuration' and 'Srm Server Details' widgets and displays three errors `"Could not find any of the requested resources"`.

Workaround: Refresh the page (app refresh) and the widgets will load and show accurate information.

DR REST plug-in for VMware Aria Automation Orchestrator Release Notes

This document contains the following sections

Introduction

Site Recovery Manager 8.8 | 21 SEP 2023 | Build 22434509 vSphere Replication 8.8 | 21 SEP 2023 | Build 22436165 DR REST plug-in for VMware Aria Automation Orchestrator 8.8 | 21 SEP 2023 | Build 22463882 | Download Check for additions and updates to these release notes.

About the DR REST plug-in for VMware Aria Automation Orchestrator

With the DR REST plug-in for VMware Aria Automation Orchestrator, Site Recovery Manager and vSphere Replication administrators can simplify the management of their Site Recovery Manager infrastructure by extending the robust workflow automation platform of VMware Aria Automation Orchestrator. VMware Aria Automation Orchestrator uses the plug-in to create REST API calls to the Site Recovery Manager and vSphere Replication REST APIs. You can use the plug-in develop custom workflows which can be plugged directly into existing customers' workflows.

The DR REST plug-in for VMware Aria Automation Orchestrator runs with VMware Aria Automation Orchestrator 8.12.2. For more information on interoperability with earlier or later releases of VMware Aria Automation Orchestrator, see the VMware Product Interoperability Matrices.

What's New

Expose the DR REST APIs through VMware Aria Automation Orchestrator plug-in

Introducing the end-to-end support of Site Recovery Manager and vSphere Replication REST APIs through the DR REST plug-in for VMware Aria Automation Orchestrator. Customers will benefit by automating manual workflows to monitor, protect, manage appliances and run recovery plans.

Installation and Upgrade

The DR REST plug-in for VMware Aria Automation Orchestrator software is distributed as an VMware Aria Automation Orchestrator application file.

You must install and configure VMware Aria Automation Orchestrator before you install the DR REST plug-in for VMware Aria Automation Orchestrator, see the *Installing and Configuring VMware Aria Automation Orchestrator 8.12* documentation.

For information about how to install the DR REST plug-in for VMware Aria Automation Orchestrator on VMware Aria Automation Orchestrator 8.12, see the *Install, update, or delete a plug-in* topic in the *VMware Aria Automation Orchestrator 8.12* documentation.

Example Workflows

The DR REST plug-in for VMware Aria Automation Orchestrator includes example workflows that demonstrate how you can automate Site Recovery Manager and vSphere Replication operations by using Automation Orchestrator, such as:

- Local Login
- Local and Remote Login
- Create Protection Group
- Get All Groups

Compatibility Matrices for VMware Site Recovery Manager 8.8

This document contains the following sections

Introduction

Site Recovery Manager 8.8 | 21 SEP 2023 | Build 22434509
Check for additions and updates to these release notes.

About the Compatibility Matrices for VMware Site Recovery Manager

The *Compatibility Matrices for VMware Site Recovery Manager 8.8* describe the compatibility between Site Recovery Manager 8.8 and platforms, database software, guest operating systems, storage partners, and other VMware solutions. Where compatibility information for Site Recovery Manager exists in the *VMware Product Interoperability Matrices* and the *VMware Compatibility Guide*, the present matrices describe how to use these tools to find the relevant information. Where the *VMware Product Interoperability Matrices* and the *VMware Compatibility Guide* do not provide information relating to Site Recovery Manager, this information is listed here.

In the compatibility tables listed in these matrices, YES means the versions are compatible and No means the versions are not compatible.

General Information

vSphere Editions

Site Recovery Manager 8.8 supports the following editions of vSphere.

vSphere Edition	Site Recovery Manager 8.8
vSphere Standard	YES
vSphere Advanced	No
vSphere Enterprise	YES
vSphere Enterprise Plus	YES
Infrastructure Enterprise	No

Infrastructure Foundation	No
Infrastructure Standard	No
vSphere Essentials	No
vSphere Essentials Plus	YES

NOTE: The protection and recovery of encrypted virtual machines with vSphere Replication requires VMware vSphere 7.0 Update 2c or later for 7.0.x based versions.

Upgrade Paths

You can upgrade existing installations of the Site Recovery Manager 8.7.x virtual appliance and the Site Recovery Manager 8.6.x virtual appliance to the Site Recovery Manager 8.8 virtual appliance.

For the most up to date supported upgrade paths for Site Recovery Manager, check the VMware Product Interoperability Matrixes.

1. Go to https://interopmatrix.vmware.com/.
2. Click **Upgrade Path**.
3. For **Solution** select **VMware Site Recovery Manager**.

vCenter Server Requirements

Site Recovery Manager 8.8 is compatible with vCenter Server 7.0 Update 3 and later versions. Site Recovery Manager supports the vCenter Server appliance (vCSA) on either or both of the protected and recovery sites.

For the most up to date vCenter Server compatibility, check the VMware Product Interoperability Matrixes.

1. Go to https://interopmatrix.vmware.com/Interoperability.
2. For **Solution** select **VMware Site Recovery Manager**.
3. For **Version** select **All**, or **8.8**, or an update release.
4. For **Platform/Solution** select **VMware vCenter Server**.

ESXi Host Requirements

Site Recovery Manager 8.8 supports ESXi host version 7.0 Update 3 and later.

For the supported versions of vSAN, see KB 2150753.

For the most up to date ESXi host compatibility for Site Recovery Manager, check the VMware Product Interoperability Matrixes.

1. Go to https://interopmatrix.vmware.com/.
2. Click **Interoperability**.
3. For **Solution** select **VMware Site Recovery Manager**.
4. For **Version** select **All**, or **8.8**.
5. For **Platform/Solution** select **VMware vSphere Hypervisor (ESXi)**.

vSphere Replications Requirements

Site Recovery Manager 8.8 is compatible with vSphere Replication 8.8. If your vSphere infrastructure is running a different version of vSphere Replication, you must upgrade to vSphere Replication 8.8 to use it with Site Recovery Manager 8.8. For information about the order in which to install vSphere Replication and Site Recovery Manager, see the relevant topics in the VMware Site Recovery Manager documentation center:

- Prerequisites and Best Practices for Site Recovery Manager Server Deployment

Interoperability with VMware Solutions

For details of the interoperability of Site Recovery Manager with other VMware solutions, check the VMware Product Interoperability Matrixes.

1. Go to https://interopmatrix.vmware.com/Interoperability.
2. For **Solution** select **VMware Site Recovery Manager**.
3. For **Version** select **All**, or **8.8**.
4. For **Platform/Solution** select a VMware solution, product, or feature, for example **VMware vRealize Orchestrator**.
5. Click **Check Interoperability**.

Supported Database Software

The Site Recovery Manager 8.8 Virtual Appliance supports only the embedded vPostgres database that it installs on the host system.

Guest Operating System Support

Site Recovery Manager 8.8 supports the protection and recovery of virtual machines that run all of the guest operating systems that vSphere 7.0 Update 3 and later versions support.

NOTE: If support for a guest operating system has been added in an update release of ESXi Server and Site Recovery Manager, to protect virtual machines that run those operating systems you must update ESXi Server to the corresponding update release as well as updating Site Recovery Manager. You must update ESXi Server on both the protected and recovery sites.

For the full list of guest operating systems that vSphere 7.0 Update 3 and later versions support, check the online VMware Compatibility Guide.

1. Go to http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software.
2. Select **Guest OS** from the **What are you looking for?** drop-down menu.
3. For **Product Name** select **ESXi**.
4. For **Product Release Version** select **All** or **ESXi *n*,** where *n* is a release of ESXi/ESX that Site Recovery Manager 8.8 supports.
5. To see all the supported versions of guest operating systems from an operating system vendor:
   a. For **OS Family Name**, select **All**.
   b. For **OS Vendor** , select the operating system vendor. For example, select **Red Hat**.
6. To check which updates of a particular operating system is supported:
   a. For **OS Family Name**, select the operating system. For example, select **Red Hat Enterprise Linux 3.0**.
   b. For **OS Vendor** , select **All**.
7. Click **Update and View Results**.

Guest Operating System Customization Support

Site Recovery Manager 8.8 supports guest operating system customization for all of the same guest operating systems for which vSphere 7.0 Update 3 supports customization. See the VMware Guest OS Customization Support Matrix.

Customization of Linux guest operating systems requires that Perl is installed in the Linux guest operating system. For more information, see Guest Operating System Customization Requirements.

Site Recovery Manager 8.8 does not support IP customization of virtual machines with Red Hat Enterprise Linux 5.x Guest OS.

NOTE: Site Recovery Manager 8.8 requires VMware Tools 10.1.0 and later.

NOTE: If support for IP customization of a guest operating system has been added in an update release of an ESXi host, to protect virtual machines that run those operating systems you must update the ESXi host to the corresponding update release as well as updating Site Recovery Manager. You must update the ESXi host on both the protected and recovery sites.

Storage Replication Adapter Support

For the full list of storage replication adapters supported by Site Recovery Manager 8.8, see http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.

Disclaimer:

Site Recovery Manager Installation and Configuration

Information about how to install and configure VMware Site Recovery Manager.

About VMware Site Recovery Manager Installation and Configuration

Site Recovery Manager Installation and Configuration provides information about how to install, upgrade, and configure VMware Site Recovery Manager.

This information also provides a general overview of Site Recovery Manager.

For information about how to perform day-to-day administration of Site Recovery Manager, see *Site Recovery Manager Administration*.

Intended Audience

This information is intended for anyone who wants to install, upgrade, or configure Site Recovery Manager. The information is written for experienced Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Overview of VMware Site Recovery Manager

VMware Site Recovery Manager is a business continuity and disaster recovery solution.

VMware Site Recovery Manager helps you to plan, test, and run the recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site.

You can configure Site Recovery Manager to protect virtual machines in different ways.

Datastore groups
: Protect the virtual machines in datastore groups by using third-party disk replication mechanisms to configure array-based replication. Array-based replication surfaces replicated datastores to recover virtual machine workloads.

Individual virtual machines
: Protect the individual virtual machines on a host by using Site Recovery Manager in combination with VMware vSphere Replication.

Storage policies
: Protect virtual machines based on their association with specific storage policies. Protecting virtual machines by using storage policies requires array-based replication.

You can use Site Recovery Manager to implement different types of recovery from the protected site to the recovery site.

Planned migration
: The orderly evacuation of virtual machines from the protected site to the recovery site. Planned migration prevents data loss when migrating workloads in an orderly fashion. For planned migration to succeed, both sites must be running and fully functioning.

Disaster recovery
: Similar to planned migration except that disaster recovery does not require that both sites be up and running, for example if the protected site goes offline unexpectedly. During a disaster recovery operation, failure of operations on the protected site is reported but is otherwise ignored.

Site Recovery Manager orchestrates the recovery process with the replication mechanisms, to minimize data loss and system down time.

- At the protected site, Site Recovery Manager shuts down virtual machines cleanly and synchronizes storage, if the protected site is still running.
- Site Recovery Manager powers on the replicated virtual machines at the recovery site according to a recovery plan.

A recovery plan specifies the order in which virtual machines start up on the recovery site. A recovery plan specifies network parameters, such as IP addresses, and can contain user-specified scripts that Site Recovery Manager can run to perform custom recovery actions on virtual machines.

Site Recovery Manager lets you test recovery plans. You conduct tests by using a temporary copy of the replicated data in a way that does not disrupt ongoing operations at either site.

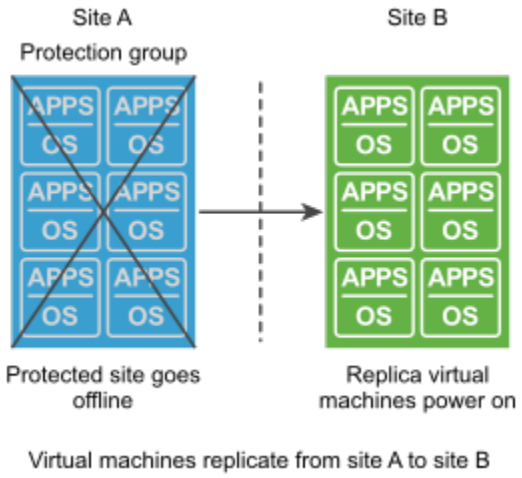
About Protected Sites and Recovery Sites

In a typical Site Recovery Manager installation, the protected site provides business-critical datacenter services.

The recovery site is an alternative infrastructure to which Site Recovery Manager can migrate these services.

The protected site can be any site where vCenter Server supports a critical business need. The recovery site can be located thousands of miles away from the protected site. Conversely, the recovery site can be in the same room as a way of establishing redundancy. The recovery site is usually located in a facility that is unlikely to be affected by environmental, infrastructure, or other disturbances that affect the protected site. You can establish bidirectional protection in which each site serves as the recovery site for the other. See Bidirectional Protection.

Figure 1: Site Recovery Manager Protected and Recovery Sites



The vSphere configurations at each site must meet requirements for Site Recovery Manager.

- The version of vCenter Server must be compatible with the version of Site Recovery Manager. For information about compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.8* at

https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html

- Each site must have at least one datacenter.
- If you are using array-based replication, the same replication technology must be available at both sites, and the arrays must be paired.
- If you are using vSphere Replication, you require a vSphere Replication appliance on both sites. The vSphere Replication appliances must be connected to each other.
- The vSphere Replication version must be compatible with the version ofSite Recovery Manager. For information about compatibility betweenvSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.8* at https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html

- The recovery site must have hardware, network, and storage resources that can support the same virtual machines and workloads as the protected site. You can oversubscribe the recovery site by running additional virtual machines there that are not protected. In this case, during a recovery you must suspend noncritical virtual machines on the recovery site.
- The sites must be connected by a reliable IP network. If you are using array-based replication, ensure that your network connectivity meets the arrays' network requirements.
- The recovery site should have access to comparable public and private networks as the protected site, although not necessarily the same range of network addresses.

Related Links

Bidirectional Protection on page 54
You can use a single set of paired Site Recovery Manager sites to protect virtual machines in both directions.

Heterogeneous Configurations on the Protected and Recovery Sites on page 54
Some components in the Site Recovery Manager and vCenter Server installations must be identical on each site.

Bidirectional Protection

You can use a single set of paired Site Recovery Manager sites to protect virtual machines in both directions.

Each site can simultaneously be a protected site and a recovery site, but for a different set of virtual machines.

You can implement bidirectional protection by protecting datastore groups or storage policies by using array-based replication or by protecting individual virtual machines by using vSphere Replication. If you are using array-based replication, each of the array’s LUNs replicates in only one direction. Two LUNs in paired arrays can replicate in different directions from each other.

Related Links

About Protected Sites and Recovery Sites on page 53
In a typical Site Recovery Manager installation, the protected site provides business-critical datacenter services.

Heterogeneous Configurations on the Protected and Recovery Sites on page 54
Some components in the Site Recovery Manager and vCenter Server installations must be identical on each site.

Heterogeneous Configurations on the Protected and Recovery Sites

Some components in the Site Recovery Manager and vCenter Server installations must be identical on each site.

Because the protected and recovery sites are often in different physical locations, some components on the protected site can be of a different type to their counterparts on the recovery site. Site Recovery Manager is compatible with N-1 version of Site Recovery Manager on the paired site. For example, if the current version of Site Recovery Manager is 8.8, the supported versions for the paired site is 8.7 and later.

Although components can be different on each site, you must use the types and versions of these components that Site Recovery Manager supports. See the

https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html

https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html.

Table 1: Heterogeneity of Site Recovery Manager Components Between Sites

Component	Heterogeneous or Identical Installations
Site Recovery Manager Server	Must be a compatible version on both sites. Site Recovery Manager is compatible with N-1 version of Site Recovery Manager on the paired site.
vCenter Server appliance	The Site Recovery Manager version must be compatible with the vCenter Server appliance version.
vSphere Replication	Must be a compatible version on both sites. The vSphere Replication version must be compatible with the Site Recovery Manager version and the vCenter Server version.
Storage arrays for array-based replication	Can be different versions on each site. You can use different versions of the same type of storage array on each site. The Site Recovery Manager Server instance on each site requires the appropriate storage replication adapter (SRA) for each version of storage array for that site. Check SRA compatibility with all versions of your storage arrays to ensure compatibility.
Site Recovery Manager database	Can be different on each site. You can use different versions of the same type of database on each site.

Heterogenous Configurations on the Protected and Recovery Sites

The Site Recovery Manager and vCenter Server installations might be in different countries, with different setups.

- Site A in Japan:
  - Site Recovery Manager Server runs in the Japanese locale
  - Site Recovery Manager extends a vCenter Server Appliance instance in the Japanese locale
- Site B in the United States:
  - Site Recovery Manager Server runs in the English locale
  - Site Recovery Manager extends a vCenter Server Appliance instance in the English locale

Related Links

About Protected Sites and Recovery Sites on page 53
In a typical Site Recovery Manager installation, the protected site provides business-critical datacenter services.

Bidirectional Protection on page 54
You can use a single set of paired Site Recovery Manager sites to protect virtual machines in both directions.

Site Recovery Manager System Requirements

The system on which you deploy Site Recovery Manager must meet specific hardware requirements.

Minimum System Requirements for the Site Recovery Manager Virtual Appliance

Site Recovery Manager is distributed as a 64-bit virtual appliance packaged in the `.ovf` format. You must deploy the virtual appliance in a vCenter Server environment by using the OVF deployment wizard on an ESXi host.

Deployment type	Requirement
Light	2 vCPU, 8 GB RAM, one 16 GB hard disk, and one 4 GB hard disk, 1 Gbit network card. You can use the light deployment type for deployments that protect less than 1000 virtual machines. **NOTE** To increase the number of vCPUs and RAM, edit the settings of the Site Recovery Manager appliance virtual machine.
Standard	4 vCPU, 12 GB RAM, one 16 GB hard disk, and one 4 GB hard disk, 1 Gbit network card. Use the standard deployment type for deployments that protect more than 1000 virtual machines.

Site Recovery Manager Licensing

After you install Site Recovery Manager, it remains in evaluation mode until you install a Site Recovery Manager license key.

After the evaluation license expires, existing protection groups remain protected and you can recover them, but you cannot create new protection groups or add virtual machines to an existing protection group until you obtain and assign a valid Site Recovery Manager license key. Obtain and assign Site Recovery Manager license keys as soon as possible after installing Site Recovery Manager.

Site Recovery Manager licenses allow you to protect a set number of virtual machines. To obtain Site Recovery Manager license keys, contact your VMware sales representative.

Site Recovery Manager License Keys and vCenter Server Instances in Linked Mode

If your vCenter Server instances are connected with vCenter Server instances in linked mode, you install the same Site Recovery Manager license on both vCenter Server instances.

Site Recovery Manager License Keys and Protected and Recovery Sites

Site Recovery Manager requires a license key on any site on which you protect virtual machines.

- Install a Site Recovery Manager license key at the protected site to enable protection in one direction from the protected site to the recovery site.
- Install the same Site Recovery Manager license keys at both sites to enable bidirectional protection, including reprotect.

Site Recovery Manager checks for a valid license whenever you add a virtual machine to or remove a virtual machine from a protection group. If licenses are not in compliance, vSphere triggers a licensing alarm and Site Recovery Manager prevents you from protecting further virtual machines. Configure alerts for triggered licensing events so that licensing administrators receive a notification by email.

Site Recovery Manager Licenses Required for Recovery and Reprotect

You have a site that contains 25 virtual machines for Site Recovery Manager to protect.

- For recovery, you require a license for at least 25 virtual machines, that you install on the protected site to allow one-way protection from the protected site to the recovery site.
- For reprotect, you require a license for at least 25 virtual machines for each site, that you install on both the protected and the recovery site to allow bidirectional protection between the sites.

You have two sites that contain 25 virtual machines each for Site Recovery Manager to protect.

- For reprotect, you require a license for at least 50 virtual machines for each site, that you install on both the protected and the recovery site to allow bidirectional protection between the sites.

Related Links

Operational Limits of Site Recovery Manager on page 57
Each Site Recovery Manager server can support a certain number of protected VMs, protection groups, recovery plans, and concurrent recoveries.

Network Ports for Site Recovery Manager on page 59
The operation of Site Recovery Manager requires certain ports to be open.

Operational Limits of Site Recovery Manager

Each Site Recovery Manager server can support a certain number of protected VMs, protection groups, recovery plans, and concurrent recoveries.

Protection Maximums for Site Recovery Manager 8.8

Table 2: Protection Maximums for Site Recovery Manager 8.8

Item	Maximum
Total number of virtual machines configured for protection (array-based replication, vSphere Replication, and Virtual Volumes Replication combined)	5000
Total number of virtual machines configured for protection using array-based replication	5000
Total number of virtual machines configured for protection using vSphere Replication	4000
Total number of virtual machines configured for protection using Virtual Volumes Replication	500 **NOTE** Contact your storage vendor for exact number of supported virtual machines, replicated with Virtual Volumes Replication.
Total number of virtual machines configured for protection using vSphere Replication on vSAN Express Storage datastores	1500
Total number of virtual machines configured for protection using array-based replication with stretched storage	1000
Total number of virtual machines per protection group	1500
Total number of array-based replication protection groups and vSphere Replication protection groups	500

Item	Maximum
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Total number of replicated datastores (using array-based replication) per Site Recovery Manager pair	255
Total number of replicated devices (using array-based replication) per Site Recovery Manager pair	255
Total number of replicated datastores and replicated devices (using array-based replication) per Site Recovery Manager pair	255

You can run array-based protection groups alongside vSphere Replication protection groups and storage policy protection groups in the same Site Recovery Manager server instance. The total number of protection groups cannot exceed 500 for all protection types combined. For example, you cannot create 250 array-based replication protection groups and then create 350 vSphere Replication protection groups, as this creates 600 protection groups in total.

If you have 250 array-based protection groups, you can create additional 250 vSphere Replication protection groups, to make a total of 500 protection groups. Similarly, in a setup that combines an array-based replication and vSphere Replication, you can protect a maximum of 5,000 virtual machines, even if you combine replication types. The protection limit for array-based replication is 5,000 virtual machines. The protection limit for vSphere Replication is 4,000 virtual machines. However, the maximum number of virtual machines that you can protect by using a combination of array-based and vSphere Replication is still 5,000 virtual machines, and not 9,000.

If you protect 3,000 virtual machines with vSphere Replication, you can protect a maximum of another 2,000 virtual machines with array-based replication.

If you protect 1,000 virtual machines with array-based replication, you can protect a maximum of another 4,000 virtual machines with vSphere Replication.

Bidirectional Protection

If you establish bidirectional protection, in which site B serves as the recovery site for site A and at the same time site A serves as the recovery site for site B, limits apply across both sites, and not per site. In a bidirectional implementation, you can protect a different number of virtual machines on each site, but the total number of protected virtual machines across both sites cannot exceed the limits.

If you protect 3,000 virtual machines using array-based replication from site A to site B, you can use array-based replication to protect a maximum of 2,000 virtual machines from site B to site A. If you are using array-based replication for bidirectional protection, you can protect a total of 5,000 virtual machines across both sites.

If you protect 155 replicated datastores using array-based replication from site A to site B, you can use array-based replication to protect a maximum of 100 replicated datastores from site B to site A. If you are using array-based replication for bidirectional protection, you can protect a total of 255 replicated datastores across both sites.

If you protect 2000 virtual machines using vSphere Replication from site A to site B, you can use vSphere Replication to protect a maximum of 2000 virtual machines from site B to site A. If you are using vSphere Replication for bidirectional protection, you can protect a maximum of 4000 virtual machines across both sites.

If you protect 3,000 virtual machines using array-based replication from site A to site B and 1,000 virtual machines using vSphere Replication from site A to site B, you can protect a maximum of 1,000 virtual machines from site B to site A. If you are using a combination of array-based replication and vSphere Replication for bidirectional protection, you can protect a maximum of 5,000 virtual machines across both sites, of which you can protect a maximum of 4,000 by using vSphere Replication.

Recovery Maximums for Site Recovery Manager 8.8

Item	Maximum
Total number of concurrently running recovery plans.	10

IP Customization Maximums for Site Recovery Manager 8.8

If you implement IP customization for recovered virtual machines, you can configure a maximum of one IP address for each NIC, using DHCP, static IPv4, or static IPv6. For static IPv4 or IPv6 addresses, you provide the following information per NIC:

- 1 IP address
- Subnet information
- 1 gateway server address
- 2 DNS servers (primary and secondary)

You also set 2 WINS addresses for DHCP or IPv4, on Windows virtual machines only.

Deployment Maximums for Site Recovery Manager 8.8 in a Shared Recovery Site Configuration

In a shared recovery site configuration, you can deploy a maximum of 10 Site Recovery Manager server instances for each vCenter Server instance. The limits apply to each Site Recovery Manager pair in a shared recovery site configuration.

Related Links

Site Recovery Manager Licensing on page 56
After you install Site Recovery Manager, it remains in evaluation mode until you install a Site Recovery Manager license key.

Network Ports for Site Recovery Manager on page 59
The operation of Site Recovery Manager requires certain ports to be open.

Network Ports for Site Recovery Manager

The operation of Site Recovery Manager requires certain ports to be open.

The components that make up a Site Recovery Manager deployment, namely vCenter Server, vSphere Client, Site Recovery Manager Server, the vSphere Replication appliance, and vSphere Replication servers, require different ports to be open. You must ensure that all the required network ports are open for Site Recovery Manager to function correctly.

vCenter Server and ESXi Server network port requirements for Site Recovery Manager 8.8

Site Recovery Manager requires certain ports to be open on vCenter Server, and on ESXi Server.

Default Port	Protocol or Description	Source	Target	Description
443	HTTPS	Site Recovery Manager	vCenter Server	Default SSL Web port.
443	HTTPS	Site Recovery Manager	vCenter Server	Traffic from Site Recovery Manager Server to local and remote vCenter Server.

Default Port	Protocol or Description	Source	Target	Description
443	HTTPS	Site Recovery Manager on the recovery site	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with configured IP customization, or callout commands on recovered virtual machines.
902	TCP and UDP	Site Recovery Manager Server on the recovery site.	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with IP customization, with configured callout commands on recovered virtual machines, or that use raw disk mapping (RDM). All NFC traffic for updating or patching the VMX files of virtual machines that are replicated using vSphere Replication use this port.

Site Recovery Manager 8.8 network ports

The Site Recovery Manager Server instances on the protected and recovery sites require certain ports to be open.

Default Port	Protocol or Description	Source	Target	Endpoints or Consumers
443	HTTPS	Site Recovery Manager HTML 5 user interface	Site Recovery Manager	Default port for the Site Recovery Manager HTML 5 user interface.
443	HTTPS	Site Recovery Manager HTML 5 user interface	Local and remote vCenter Server or all vCenter Server instances in Enhanced Linked Mode on which there is a registered Site Recovery Manager. For more information about Enhanced Linked Mode, see *vCenter Enhanced Linked Mode for vCenter Server Appliance* in the *vCenter Server Installation and Setup* documentation.	Default port for the Site Recovery Manager HTML 5 user interface. when you open it from the Site Recovery Manager appliance.
443	HTTPS	Site Recovery Manager HTML 5 user interface	Local and remote vCenter Server or all vCenter Server instances in Enhanced Linked Mode on which there is a registered Site Recovery Manager.	Default port for the Site Recovery Manager HTML 5 user interface. when you open it from the Site Recovery Manager appliance.
443	HTTPS	Site Recovery Manager	vCenter Server	Default SSL Web Port for incoming TCP traffic.
443	HTTPS	Site Recovery Manager	vCenter Server	Traffic from Site Recovery Manager Server to local and remote vCenter Server.
443	HTTPS	Site Recovery Manager on the recovery site	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with configured IP customization, or callout commands on recovered virtual machines.

Default Port	Protocol or Description	Source	Target	Endpoints or Consumers
443	HTTPS	vSphere Client	Site Recovery Manager Appliance	All management traffic to Site Recovery Manager Server goes to this port. This includes traffic by external API clients for task automation and HTTPS interface for downloading the UI plug-in and icons. This port must be accessible from the vCenter Server proxy system. Used by vSphere Client to download the Site Recovery Manager client plug-in.
443	TCP	Site Recovery Manager Appliance	https://vcsa.vmware.com	Customer Experience Improvement Program (CEIP) for Site Recovery Manager
902	TCP and UDP	Site Recovery Manager Server on the recovery site.	Recovery site ESXi host.	Traffic from the Site Recovery Manager Server on the recovery site to ESXi hosts when recovering or testing virtual machines with IP customization, with configured callout commands on recovered virtual machines, or that use raw disk mapping (RDM). All NFC traffic for updating or patching the VMX files of virtual machines that are replicated using vSphere Replication use this port.
5480	HTTPS	Web Browser	Site Recovery Manager Appliance	Site Recovery Manager Appliance Management Interface

Site Pairing Port Requirements

Port	Protocol	Source	Target	Description
443	HTTPS	vCenter Server	Site Recovery Manager Server	vCenter Server and target Site Recovery Manager Appliance communication.
443	HTTPS	Site Recovery Manager Server	Site Recovery Manager Server on target site	Bi-directional communication between Site Recovery Manager servers.
443	HTTPS	Site Recovery Manager	vCenter Server	Site Recovery Manager to vCenter Server communication - local and remote.

Network ports that must be open on Site Recovery Manager and vSphere Replication Protected and Recovery sites

Site Recovery Manager and vSphere Replication require that the protected and recovery sites can communicate.

Port	Protocol or Description	Source	Target	Endpoints or Consumers
31031	Initial replication traffic	ESXi host	vSphere Replication appliance on the recovery site	From the ESXi host at the protected site to the vSphere Replication appliance at the recovery site
32032	TCP	ESXi host on the source site	vSphere Replication server at the target site	Initial and outgoing replication traffic from the ESXi host at the source site to the vSphere Replication appliance or vSphere Replication server at the target site for replication traffic with network encryption.
8043	HTTPS	Site Recovery Manager	vSphere Replication appliance on the recovery and protected sites	Management traffic between Site Recovery Manager instances and vSphere Replication appliances.

Related Links

Site Recovery Manager Licensing on page 56

After you install Site Recovery Manager, it remains in evaluation mode until you install a Site Recovery Manager license key.

Operational Limits of Site Recovery Manager on page 57

Each Site Recovery Manager server can support a certain number of protected VMs, protection groups, recovery plans, and concurrent recoveries.

Creating the Site Recovery Manager Database

The Site Recovery Manager Server requires its own database, which it uses to store data such as recovery plans and inventory information.

Site Recovery Manager provides an embedded vPostgreSQL database that requires fewer steps to configure than an external database. The embedded vPostgreSQL database supports a full-scale Site Recovery Manager environment.

Each Site Recovery Manager site requires its own instance of the Site Recovery Manager database.

If you are updating Site Recovery Manager to a new version, you can use the existing database. Before you attempt an upgrade, make sure that both Site Recovery Manager Server databases are backed up. Doing so helps ensure that you can revert back to the previous version after the upgrade, if necessary.

For the list of database software that Site Recovery Manager supports, see the *Compatibility Matrices for Site Recovery Manager 8.8* at https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html.

Back Up and Restore the Embedded vPostgres Database

When you deploy the Site Recovery Manager appliance, Site Recovery Manager creates a vPostgres database during the installation process.

For information about the commands that you use to back up and restore the embedded vPostgres database, see the pg_dump and pg_restore commands in the PostgreSQL documentation at https://www.postgresql.org/docs/9.3/static/index.html.

You can back up and restore the embedded vPostgres database by using PostgreSQL commands. Always back up the Site Recovery Manager database before updating or upgrading Site Recovery Manager. You also might need to back up and restore the embedded vPostgres database if you need to unregister and then reinstall Site Recovery Manager and retain data from the previous installation, migrate Site Recovery Manager Server to another host machine, or revert the database to a clean state in the event that it becomes corrupted.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. In the Site Recovery Manager Appliance Management Interface, click **Services**, and stop the Site Recovery Manager service.
3. Log into the Site Recovery Manager host machine.
4. Create a backup of the embedded vPostgres database by using the `pg_dump` command.

   ```
   /opt/vmware/vpostgres/current/bin/pg_dump -Fc --username=db_username srmdb > srm_backup_name
   ```

   The default user name for the database is `srmdb` . The database name is `srmdb` and cannot be changed.
5. Perform the actions that necessitate the backup of the embedded vPostgres database.
   For example, update or upgrade Site Recovery Manager, uninstall and reinstall Site Recovery Manager, or migrate Site Recovery Manager Server.
6. Optional: Restore the database from the backup that you created in 4 by using the `pg_restore` command.

   ```
   /opt/vmware/vpostgres/current/bin/pg_restore -Fc --username=db_username --dbname=srmdb srm_backup_name
   ```

7. Optional: To restore the database on the same system from which you created the backup, you must use the `--clean` option with the `pg_restore` command.

   `/opt/vmware/vpostgres/current/bin/pg_restore --clean -Fc --username=`*`db_username`* `--dbname=srmdb` *`srm_backup_name`*

8. Start the Site Recovery Manager service.

Site Recovery Manager Authentication

The vCenter Server appliance handles the authentication between Site Recovery Manager and vCenter Server at the vCenter Single Sign-On level.

All communications between Site Recovery Manager and vCenter Server instances take place over transport layer security (TLS) connections.

Service Account Authentication

Site Recovery Manager uses service account authentication to establish a secure communication to remote services, such as the vCenter Server. A service account is a security principal that the Site Recovery Manager configuration service generates. The service account authenticates with a token or a user name and a password.

The service account is for internal use by Site Recovery Manager, vCenter Server, and vCenter Single Sign-On.

During operation, Site Recovery Manager establishes authenticated communication channels to remote services by using token-based authentication to acquire a holder-of-key SAML token from vCenter Single Sign-On. Site Recovery Manager sends this token in a cryptographically signed request to the remote service. The remote service validates the token and establishes the identity of the service account.

Service Accounts and Site Recovery Manager Site Pairing

When you pair Site Recovery Manager instances across vCenter Single Sign-On sites that do not use Enhanced Linked Mode, Site Recovery Manager creates an additional service account for the remote site at each site. This service account for the remote site allows the Site Recovery Manager Server at the remote site to authenticate to services on the local site.

When you pair Site Recovery Manager instances in a vCenter Single Sign-On environment with Enhanced Linked Mode, Site Recovery Manager at the remote site uses the same service account to authenticate to services on the local site.

Site Recovery Manager SSL/TLS Server Endpoint Certificates

Site Recovery Manager requires an SSL/TLS certificate for use as the endpoint certificate for all TLS connections established to Site Recovery Manager. The Site Recovery Manager server endpoint certificate is separate and distinct from the certificate that is used by Site Recovery Manager to obtain holder-of-key SAML token with the service account.

For information about the Site Recovery Manager SSL/TLS endpoint certificate, see Creating SSL/TLS Server Endpoint Certificates for Site Recovery Manager.

Creating SSL/TLS Server Endpoint Certificates for Site Recovery Manager

The Site Recovery Manager server endpoint certificate establishes the identity of Site Recovery Manager Server to clients.

The endpoint certificate secures the communication between the client and Site Recovery Manager Server.

The Site Recovery Manager 8.8 appliance generates a self-signed SSL certificate when the appliance first boots. The Site Recovery Manager 8.8 self-signed certificate expires after five years from the first boot of the appliance.

You can also provide a custom SSL/TLS certificate that is signed by a certificate authority. If you use a custom SSL/TLS certificate, the certificate must meet certain requirements to work with Site Recovery Manager.

NOTE
For information about how Site Recovery Manager authenticates with vCenter Server, see Site Recovery Manager Authentication.

Requirements When Using Custom SSL/TLS Certificates With Site Recovery Manager

If you use custom SSL/TLS certificates for the Site Recovery Manager server endpoint certificate, the certificates must meet specific criteria.

Site Recovery Manager 8.x uses standard PKCS#12 certificates. Site Recovery Manager places some requirements on the contents of those certificates.

- Site Recovery Manager does not accept certificates with MD5 signature algorithms. Use SHA256 or stronger signature algorithms.
- By default, Site Recovery Manager does not accept certificates with SHA-1 signature algorithms. Use SHA256 or stronger signature algorithms.
- The Site Recovery Manager certificate is not the root of a trust chain. You can use an intermediate CA certificate which is not the root of a trust chain, but that is still a CA certificate.
- If you use a custom certificate for vCenter Server you are not obliged to use a custom certificate for Site Recovery Manager. The reverse is also true.
- The private key in the PKCS #12 file must match the certificate. The minimum length of the private key is 2048 bits.
- The Site Recovery Manager certificate password must not exceed 31 characters.
- The current time must be within the period of validity of the certificate.
- The certificate must be a server certificate, for which the x509v3 Extended Key Usage must indicate TLS Web Server Authentication.
  - The certificate must include an `extendedKeyUsage` or `enhancedKeyUsage` attribute, the value of which is `serverAuth` .
  - There is no requirement for the certificate to also be a client certificate. The `clientAuth` value is not required.
- The Subject Name must not be empty and must contain fewer than 4096 characters. In this release, the Subject Name does not have be the same for both members of a Site Recovery Manager Server pair.
- The certificate must identify the Site Recovery Manager Server host.
  - The recommended way to identify the Site Recovery Manager Server host is with the host's fully-qualified domain name (FQDN). If the certificate identifies the Site Recovery Manager Server host with an IP address, this must be an IPv4 address. Using IPv6 addresses to identify the host is not supported.
  - Certificates generally identify the host in the Subject Alternative Name (SAN) attribute. Some CAs issue certificates that identify the host in the Common Name (CN) value of the Subject Name attribute. Site Recovery Manager accepts certificates that identify the host in the CN value, but this is not the best practice. For information about the SAN and CN best practices, see the Internet Engineering Task Force (IETF) RFC 6125 at https://tools.ietf.org/html/rfc6125.
  - The host identifier in the certificate must match the Site Recovery Manager Server local host address that you specify when you install Site Recovery Manager.

Enable the SHA-1 Hashing Function

You can install certificates, signed with the SHA-1 hashing function in the Site Recovery Manager Appliance in case your environment requires it.

By default, the Site Recovery Manager server rejects installation of new certificates, which are signed with the SHA-1 hashing function. To install a certificate, signed with the SHA-1 hashing function, you must enable it in the Site Recovery Manager Appliance.

1. Establish an SSH connection to the Site Recovery Manager Appliance.
2. Navigate to the `/opt/vmware/srm/conf/` folder and open the `vmware-dr.xml` and the `drconfig.xml` files in a text editor.
3. Find the `<connections>` section and add a `<allowSha1>` section.

```
<connections>
   <allowSha1>true</allowSha1>
</connections>
```

4. Save the files and restart the Site Recovery Manager Server service.
5. Use the following command to restart the *`dr-configurator`* service.
   `sudo systemctl restart dr-configurator`

How do I modify the minimum TLS version that Site Recovery Manager uses

You change the minimum version of TLS that Site Recovery Manager uses by modifying the envoy proxy settings.

Verify the version of TLS that Site Recovery Manager uses by running the following command `openssl s_client -connect <srm-fqdn>:443`.

By default Site Recovery Manager 8.8 uses only TLS 1.2.

1. SSH to `/opt/vmware/envoy/conf/`.
2. Open the `envoy-proxy.yaml` file in a text editor and edit the following line with the required minimum version of TLS.
   `tls_params: tls_minimum_protocol_version: TLSv1_2`
3. Save the changes and exit the editor.
4. Restart the envoy proxy service by running the following command.
   `systemctl restart envoy-proxy`

If you modify the minimum version of TLS, you must change all the occurrences where you want the change to take effect.

Deploying the Site Recovery Manager Appliance

The Site Recovery Manager Virtual Appliance is a preconfigured VM that is optimized for running Site Recovery Manager and its associated services.

You deploy the appliance on an ESXi host in your vSphere environment.

You can use the Site Recovery Manager Appliance Management Interface to configure the Site Recovery Manager Appliance and edit the appliance settings.

After you deploy and configure Site Recovery Manager instances on both sites, the Site Recovery Manager plug-in appears in the vSphere Client.

The Site Recovery Manager Appliance supports only the vPostgress embedded database.

For information about the compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.8* at

https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html

https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html.

Site Recovery Manager and vCenter Server Deployment Models

You can install Site Recovery Manager in any of the deployment models that vCenter Server supports.

For information about the deployment models that vCenter Server supports, see *Deploying the vCenter Server Appliance* in *vCenter Server Installation and Setup*.

You must take the deployment model of vCenter Server into consideration when you install Site Recovery Manager. During a disaster recovery, Site Recovery Manager and vCenter Server must be up and running on the recovery site.

Configuring the Platform Services Controller and Selecting the Correct vCenter Server Instance in an Enhanced Linked Mode Environment

When you install Site Recovery Manager Server, you provide the address of the Platform Services Controller that is associated with the vCenter Server instance to protect. You then select the vCenter Server instance with which to register Site Recovery Manager from the list of all of the vCenter Server instances that this Platform Services Controller serves. In an Enhanced Linked Mode environment, that list might include vCenter Server instances from other sites. If you select the wrong vCenter Server instance and complete the Site Recovery Manager installation, you cannot subsequently modify the Site Recovery Manager installation to select the correct vCenter Server instance. In this case, you must uninstall and reinstall Site Recovery Manager to select the correct vCenter Server instance.

- When you install Site Recovery Manager Server on the protected site, make sure that you select the vCenter Server instance that manages the virtual machines to protect.
- When you install Site Recovery Manager Server on the recovery site, make sure that you select the vCenter Server instance to which to recover virtual machines.
- Ensure that the vCenter Server and Site Recovery Manager Server are all located on the protected site, or all on the recovery site.

After you have installed Site Recovery Manager, if vCenter Server migrates to a different Platform Services Controller or if the address of the Platform Services Controller changes, you can reconfigure Site Recovery Manager with the new Platform Services Controller address. For example, you can change from an external Platform Services Controller to an embedded Platform Services Controller. For information about changing Platform Services Controller, see Converging vCenter Server with an External Platform Services Controller to a vCenter Server with an Embedded Platform Services Controller in *vCenter Server Installation and Setup*. If you plan on converging an external Platform Services Controller to an embedded Platform Services Controller, you must perform the steps in the correct order to ensure the proper operation of Site Recovery Manager.

1. Converge the external Platform Services Controller on the protected site to an embedded Platform Services Controller.
2. Reconfigure Site Recovery Manager and vSphere Replication at the protected site to use the new embedded Platform Services Controller. Verify through the Site Recovery user interface that Site Recovery Manager and vSphere Replication are connected to the new Platform Services Controller.
3. Converge the external Platform Services Controller on the recovery site to an embedded Platform Services Controller.
4. Reconfigure Site Recovery Manager and vSphere Replication at the recovery site to use the new embedded Platform Services Controller. Verify through the Site Recovery user interface that Site Recovery Manager and vSphere Replication are connected to the new Platform Services Controller.
5. If necessary, reconnect the protected and the recovery sites.

NOTE
If you are in an Enhanced Linked Mode environment, you must first converge the Platform Services Controller of all federated partners before reconfiguring Site Recovery Manager and vSphere Replication.

You change the Platform Services Controller address by reconfiguring the Site Recovery Manager appliance. If you are unable to connect Site Recovery Manager or vSphere Replication to the new Platform Services Controller, see KB 85970.

Concurrent Installations of Site Recovery Manager in an Enhanced Linked Mode Environment

In an Enhanced Linked Mode environment, do not install Site Recovery Manager under more than one vCenter Server at the same time. A conflict can arise in the creation of the service account that vCenter Server creates at the domain level for Site Recovery Manager authentication with vCenter Server if the following conditions exist:

- If the installation of one Site Recovery Manager Server instance overlaps with the installation of another Site Recovery Manager Server instance under two different vCenter Server instances.
- Those vCenter Server instances are in Enhanced Linked Mode.

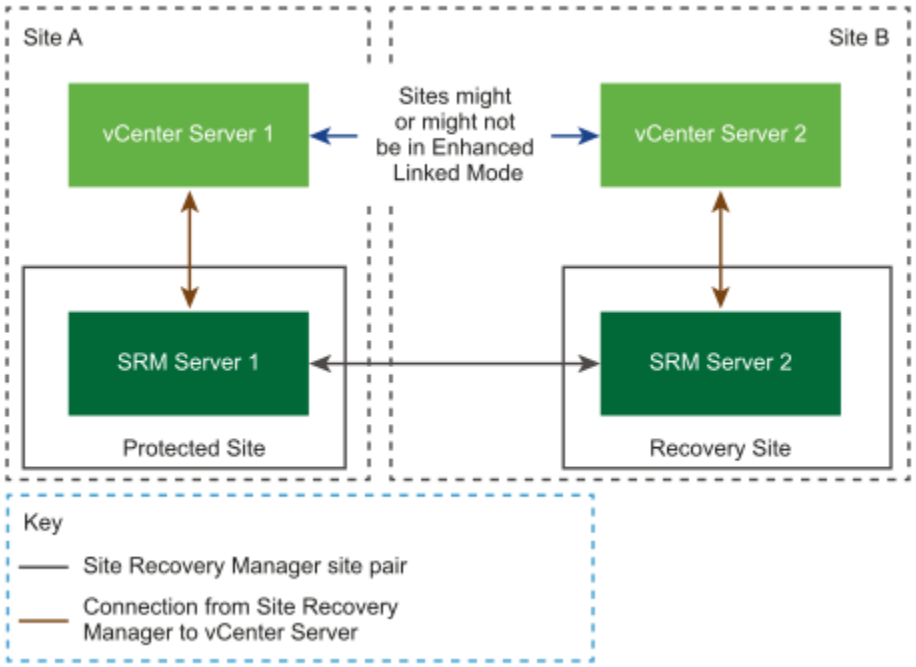
The conflict does not prevent installation, but it does cause one of the Site Recovery Manager Server instances to fail to start, with the error message `Failed to start service`. The message `Failed to start Authorization Manager` appears in the event log for that Site Recovery Manager Server instance.

Site Recovery Manager in a Two-Site Topology with One vCenter Server Instance per site

The most common deployment for Site Recovery Manager is to have two sites with one vCenter Server instance per site.

The vCenter Server instances can belong to vCenter Single Sign-On domains that are either in Enhanced Linked Mode or are not in Enhanced Linked Mode.

Figure 2: Site Recovery Manager in a Two-Site Topology with One vCenter Server Instance per site



Prerequisites and Best Practices for Site Recovery Manager Server Deployment

Before you deploy Site Recovery Manager Server, you must perform several tasks and verify that you have certain information.

- Install the appropriate version of the vCenter Server appliance on both sites. For information about compatibility between vCenter Server and Site Recovery Manager
  versions, see *vCenter Server Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.8* at https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/site-recovery-manager/8-8/release-notes/compatibility-matrices-for-vmware-site-recovery-manager-88.html
- When you install and configure vCenter Server and vSphere Replication, use fully qualified domain names (FQDN) whenever possible rather than IP addresses. Using FQDN rather than IP addresses allows you to change the vSphere infrastructure, for example by using DHCP, without having to redeploy or reconfigure Site Recovery Manager. You must also use FQDN if you use custom certificates, because most certificate authorities do not accept certificates that use IP addresses for the SAN or CN value.
- Obtain the address of the vCenter Server instance for both sites.
- Synchronize the clock settings of the systems on which the vCenter Server and Site Recovery Manager Server run. To avoid conflicts in the time management across these systems, use a persistent synchronization agent such as network time protocol daemon (NTPD), W32Time, or VMware Tools time synchronization. If you run vCenter Server and Site Recovery Manager Server in virtual machines, set up NTP time synchronization on the ESXi host on which the virtual machines run. For information about timekeeping best practices, see http://kb.vmware.com/kb/1318.
- Obtain the vCenter Single Sign-On administrator user name and password for both of the local and remote sites.
- If you use custom certificates, obtain an appropriate certificate file. See Requirements When Using Custom SSL/TLS Certificates With Site Recovery Manager.
- If you configure Site Recovery Manager in an IPv6 network, verify that the IPv6 address of the Site Recovery Manager Server, vCenter Server, the ESXi hosts, and the external database, if used, are mapped to fully qualified domain names on the DNS server. Deploy the Site Recovery Manager Server using FQDN and use only FQDNs, not static IPv6 addresses, for all connections.
- To use Site Recovery Manager with vSphere Replication, deploy the appropriate version of vSphere Replication on both of the protected and recovery sites before you deploy Site Recovery Manager Server. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Client to stop working. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.8* at https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html.
- If you cannot upgrade an existing incompatible version of vSphere Replication, you must unregister vSphere Replication from both vCenter Server instances before you deploy Site Recovery Manager. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Client to stop working. See Unregister an Incompatible Version of vSphere Replication.

Deploy the Site Recovery Manager Virtual Appliance

To run Site Recovery Manager and its associated services, you deploy the appliance both at the protected and at the recovery site.

If you are not deploying the appliance from an online URL, download the Site Recovery Manager ISO image and mount it on a system in your environment.

1. Log in to the vSphere Client on the protected site.
2. Right-click a host and select **Deploy OVF template**.
3. Provide the location of the OVF file from which to deploy the Site Recovery Manager Appliance, and click **Next**.

Option	Description
Online URL	Select **URL** and provide the URL to deploy the appliance from an online URL.
Downloadable ISO file	1. Select **Local file** > **Browse**, and navigate to the `\bin` directory in the ISO image. 2. Select the `srm-va_OVF10.ovf`, `srm-va-system.vmdk`, `srm-va-support.vmdk`, `srm-va_OVF10.cert`, and `srm-va_OVF10.mf` files.

4. Enter the name for the virtual appliance or accept the default, select, or search for a destination folder or data center for the appliance, and click **Next**.

   The name must be unique within each vCenter Server virtual machine folder.
5. Select a cluster, host, or resource pool where you want to run the deployed template, and click **Next**.
6. Review the virtual appliance details and click **Next**.
7. Accept the end-user license agreements (EULA) and click **Next**.
8. Select the number of vCPUs for the virtual appliance and click **Next**.
9. Select a destination datastore and disk format for the virtual appliance and click **Next**.
10. Select a network from the list of available networks, set the IP protocol and IP allocation, and click **Next**.

    Site Recovery Manager supports both DHCP and static IP addresses. You can also change the network settings by using the appliance management interface after installation.
11. On the **Customize template** page, select an option for the Site Recovery Manager Appliance hostname.

Option	Description
Leave the text box blank	The DNS server on your network performs reverse lookup of the host name, or the Site Recovery Manager Appliance is registered with its IP address as its host name.
Enter a host name	Depending on your network settings, select one of the following options: • If you have assigned a static IP address to the appliance, enter an FQDN for that IP. • If you do not use a DNS server, enter a host name that you have already mapped to an IP address in your network.

12. Optional: To enable the SSHD service of the appliance, select the **Enable SSHD** check box.
13. Set the admin and root user passwords, enter one or more NTP server host names or IP addresses, and click **Next**.

Setting	Action
Initial admin user password	Set the password for the `admin` user account, which you use for access to the Site Recovery Manager Appliance Management Interface and for an SSH access to the appliance OS.
Initial root password	Set the password for the `root` account, which you use to log in to the OS of the virtual appliance.
NTP Servers	Enter one or more NTP server host names or IP addresses.

NOTE
The admin and root user passwords must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters. The user name cannot be part of the password.

14. Optional: To check the integrity of the Site Recovery Manager Appliance binary files, select the **File Integrity Flag** check box.

    If the Site Recovery Manager Appliance detects changes to the binary files, it sends log traces to the syslog.
15. Optional: You can modify the default Network Properties.

Setting	Action
Host Network IP Address Family	Select the Network IP address family. The options are IPv4 or IPv6.
Host Network Mode	Select the host network mode. The options are static, DHCP, or autoconf. Autoconf is avalable only for IPv6.
Default Gateway	Enter the default gateway address for this VM.
Domain Name	Enter the domain name of this VM.
Domain Search Path	Enter the domain search path for this VM. Use comma or space separated domain names.
Domain Name Servers	The domain name server IP Addresses for this VM. Use commas to separate the IP addresses.
Network 1 IP Address	The IP address for the default Ethernet adapter.
Network 1 Netprefix	The prefix for the default Ethernet adapter.

16. Review the settings and click **Finish**.

    The Site Recovery Manager Appliance is deployed.
17. Power on the Site Recovery Manager Appliance.
18. Take a note of the IP address of the appliance and log out of the vSphere Client.
19. To deploy Site Recovery Manager on the recovery site, repeat the procedure.

Configure the Site Recovery Manager Appliance instances to connect to vCenter Server at both the protected and the recovery site.

Log In to the VMware Site Recovery Manager Appliance Management Interface

To access the Site Recovery Manager Appliance configuration settings, you must log in to the Appliance Management Interface using the admin account.

Deploy the Site Recovery Manager Appliance and power it on.

1. In a web browser, go to the Site Recovery Manager Appliance Management Interface at https://*appliance-IP-address-or-FQDN*.
2. Click **Launch Site Recovery Manager Appliance Management**.
3. Log in as admin.

   The default password is the admin user account password that you set during the deployment of the Site Recovery Manager Appliance.

Configure the Site Recovery Manager Appliance to Connect to a vCenter Server

You must configure the Site Recovery Manager Appliance to connect to a vCenter Server instance on both the protected and the recovery sites.

Deploy the Site Recovery Manager Appliance and power it on.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click the **Summary** tab, and click **Configure appliance**.
3. On the **Platform Services Controller** page, enter the information about the site where you deployed the Site Recovery Manager Appliance.

Menu Item	Description
PSC host name	Enter the host name (in lowercase letters) or IP address of the vCenter Server with which to register Site Recovery Manager.
PSC port	Accept the default value of `443`, or enter a new value if vCenter Server uses a different port. vCenter Server only supports connections over HTTPS.
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this vCenter Server instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the vCenter Server instance.
Password	The password for the specified vCenter Single Sign-On user name.

4. If prompted, click **Connect** to verify the vCenter Server certificate.
5. On the **vCenter Server** page, select the vCenter Server instance with which to register the Site Recovery Manager Appliance, and click **Next**.

CAUTION
The drop-down menu includes all the registered vCenter Server instances. In an environment that uses Enhanced Linked Mode, it might also include other vCenter Server instances. Make sure that you select the correct vCenter Server instance. After you configure the Site Recovery Manager Appliance, you cannot select a different vCenter Server instance.

6. On the **Name and Extension** page, enter the necessary information to register the Site Recovery Manager with vCenter Server, and select the default Site Recovery Manager extension identifier, or create a custom extension identifier.
   a) Enter the site name, administrator email address, and local host IP address or name.

Menu Item	Description
Site name	A name for this Site Recovery Manager site, which appears in the Site Recovery Manager interface. The vCenter Server address is used by default. Use a different name for each Site Recovery Manager instance in the pair.
Administrator email	The email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.
Local host	The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the Site Recovery Manager Appliance detects is not the interface that you want to use. **NOTE** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

   b) Select the default Site Recovery Manager extension identifier, or create a custom extension ID for this Site Recovery Manager pair, and click **Next**.

   Both Site Recovery Manager instances in a site pair must use the same extension ID.

Menu Item	Description
Default extension ID	Use this option when you deploy Site Recovery Manager in a standard configuration with one protected site and one recovery site.
Custom extension ID	Use this option when you deploy Site Recovery Manager in a shared recovery site configuration, with multiple protected sites and one recovery site. Enter the details for the custom extension ID. • Extension ID. A unique identifier. Assign the same identifier to the Site Recovery Manager instances on the protected site and the shared recovery site. • Organization. The name of the organization to which this Site Recovery Manager sites pair belongs. This name helps to identify Site Recovery Manager pairs in a shared recovery site configuration, especially when multiple organizations use the shared recovery site. • Description. An optional description of the Site Recovery Manager pair.

7. On the **Ready to Complete** page, review your settings and click **Finish**.
8. To configure the Site Recovery Manager Appliance on the other site, repeat the procedure.

Connect to the Site Recovery Manager Appliance Embedded vPostgres Database

If you need to access the content in the Site Recovery Manager embedded vPostgres database, you must connect to the database through the appliance OS.

1. Log in to the OS of the Site Recovery Manager Appliance as admin.
   You set the password for the `admin` user account during the deployment of the appliance.
2. Run `/opt/vmware/vpostgres/current/bin/psql –U` *`user`* `-d` *`dbdsn`*. Enter a user name and the database name.

User	Description
admin	The embedded vPostgres database super user account. **NOTE** The `admin` account uses the same password to access both the appliance OS and the embedded database.
srmdb	The embedded vPostgres database user account. Site Recovery Manager Server uses this account to access the embedded vPostgres database.

How do I set up a trusted environment for the Site Recovery Manager Virtual Appliance

To set up a trusted environment with your custom root CA certificates, you must manually import the certificates into the Site Recovery Manager Appliance.

The certificates must be in a `.pem` format.

1. To import the root certificate, log in to the Site Recovery Manager Appliance Management Interface as admin.
   a) Click the **Certificates** tab, and under **CA Certificates**, click **Root**.
   b) Click **Add**, insert the certificate in `.pem` format and click **Add**.
2. To import the Site Recovery Manager Server certificates, log in to the Site Recovery Manager Appliance Management Interface as admin.
   a) Click the **Certificates** tab, and click **Change**.
   b) Select a certificate type.

Menu item	Description
Generate a self-signed certificate.	Use an automatically generated certificate. 1. Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company. 2. Accept the default FQDN and IP values. **NOTE** Using a self-signed certificate is not recommended for production environments.
Use a PKCS #12 certificate file.	Use a custom certificate. 1. Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. 2. Enter the optional private key encryption password.
Use a CA-signed certificate generated from CSR.	Use a CA-signed certificate generated from a CSR. 1. In the **Certificate file** row, click **Browse**, navigate to the certificate file, and click **Open**. 2. In the **CA chain** row, click **Browse**, navigate to the CA chain, and click **Open**.

   c) Click **Change**.

Use the VMware OVF Tool to Deploy the Site Recovery Manager Virtual Appliance Virtual Machine from a Client OVF Template

You can use the VMware OVF Tool to deploy the Site Recovery Manager Virtual Appliance virtual machine from a client OVF template.

Verify that you have downloaded and installed VMware OVF Tool 4.2 or later.

VMware OVF Tool (`ovftool`) is a flexible command-line utility that you can use to import and export OVF packages to and from a wide variety of VMware products. For more information about the `ovftool`, see the VMware OVF Tool documentation.

To deploy the Site Recovery Manager Virtual Appliance with the VMware OVF Tool, use one the following command lines.

a) If you want to obtain network settings through DHCP:

```
ovftool
```

```
  --acceptAllEulas
  --ipAllocationPolicy=dhcpPolicy
  --ipProtocol=IPv4
  --deploymentOption=light | standard
  --name=SRM-VA-NAME
  --datastore=DATASTORE-NAME
  --network=NETWORK-NAME
  --net:"Network 1"=NETWORK-NAME
  --prop:varoot-password=ROOT-PASSWORD
  --prop:vaadmin-password=ADMIN-PASSWORD
  --prop:dbpassword=DB-PASSWORD
  --prop:ntpserver=NTP-SERVER
  --prop:network.netmode.VMware_Site_Recovery_Manager_Appliance='dhcp'
  --prop:network.addrfamily.VMware_Site_Recovery_Manager_Appliance='ipv4'
  http://HOST/PATH/srm-va_OVF10.ovf
  vi://VC_USERNAME:VC_PASSWORD@VC_ADDRESS/DATACENTER-NAME/host/CLUSTER-NAME/Resources/RESOURCE-POOL-NAME
```

b) If you want to obtain network settings through a static IP address:

```
ovftool
  --acceptAllEulas
  --ipAllocationPolicy=dhcpPolicy
  --ipProtocol=IPv4
  --deploymentOption=light | standard
  --name=SRM-VA-NAME
  --datastore=DATASTORE-NAME
  --network=NETWORK-NAME
  --net:"Network 1"=NETWORK-NAME
  --prop:varoot-password=ROOT-PASSWORD
  --prop:vaadmin-password=ADMIN-PASSWORD
  --prop:dbpassword=DB-PASSWORD
  --prop:ntpserver=NTP-SERVER
  --prop:"network.ip0.VMware_Site_Recovery_Manager_Appliance"="VA IP"
  --prop:"network.netprefix0.VMware_Site_Recovery_Manager_Appliance"="NETWORK PREFIX"
  --prop:"network.gateway.VMware_Site_Recovery_Manager_Appliance"="GATEWAY IP"
  --prop:"network.DNS.VMware_Site_Recovery_Manager_Appliance"="DNS SERVER 1, DNS SERVER 2"
  --prop:"network.searchpath.VMware_Site_Recovery_Manager_Appliance"="DNS SEARCH PATH - DOMAIN"
  --prop:"network.netmode.VMware_Site_Recovery_Manager_Appliance"='static'
  --ipAllocationPolicy="fixedPolicy"
  --prop:network.addrfamily.VMware_Site_Recovery_Manager_Appliance='ipv4'
  http://HOST/PATH/srm-va_OVF10.ovf
  vi://VC_USERNAME:VC_PASSWORD@VC_ADDRESS/DATACENTER-NAME/host/CLUSTER-NAME/Resources/RESOURCE-POOL-NAME
```

You must replace the variables in the example with values from your environment.

Variable	Description
light | standard	The deployment type for the Site Recovery Manager Appliance virtual machine. Use the light deployment type for deployments that protect less than 1000 virtual machines. Use the standard deployment type for deployments that protect more than 1000 virtual machines.
SRM-VA-NAME	The name of the Site Recovery Manager Appliance virtual machine.

Variable	Description
DATASTORE-NAME	The target datastore name.
NETWORK-NAME	The name of the target network.
ROOT-PASSWORD	The password for the `root` account, which you use to log in to the OS of the virtual appliance. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
ADMIN-PASSWORD	The password for the `admin` user account, which you use for access to the Site Recovery Manager Appliance Management Interface and for SSH access to the appliance OS. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
DB-PASSWORD	The password for the `srmdb` database account, which you use to connect to the embedded vPostgres database. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
NTP-SERVER	The NTP server host name.
HOST	The host address of the source virtual machine.
PATH	The path to the OVF package.
NETWORK PREFIX	The network prefix of the Site Recovery Manager Appliance.
DNS SEARCH PATH - DOMAIN	The domain search path for this virtual machine (use a comma or a space to separate the different names).
GATEWAY IP ADDRESS	The Gateway address of the Site Recovery Manager Appliance.
VA IP	The IP address of the Site Recovery Manager Appliance virtual machine.
DNS IP ADDRESS	The DNS address of the Site Recovery Manager Appliance .
VC_USERNAME	The user name for the target vCenter Server.
VC_PASSWORD	The password for the target vCenter Server.
VC_ADDRESS	The address of the target vCenter Server.
DATACENTER-NAME	The name of the target data center.
CLUSTER-NAME	The name of the target cluster.
RESOURCE-POOL-NAME	The name of the target resource pool.

Configure the Site Recovery Manager Appliance to Connect to a vCenter Server at both the protected and the recovery site.

Connect the Site Recovery Manager Server Instances on the Protected and Recovery Sites

Before you can use Site Recovery Manager, you must connect the Site Recovery Manager Server instances on the protected and recovery sites.

- Verify that you installed Site Recovery Manager Server instances at the protected and recovery sites.
- If you did not select the default plug-in ID when you installed Site Recovery Manager Server, you must have assigned the same custom plug-in ID to the Site Recovery Manager Server instances on each of the sites.

This is known as site pairing.

> **IMPORTANT**
> Site Recovery Manager does not support network address translation (NAT). If the network that you use to connect the Site Recovery Manager sites uses NAT, attempting to connect the sites results in an error. Use credential-based authentication and network routing without NAT when connecting the sites.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select a local vCenter Server from the list, select a pair type, and click **Next**.
   - Pair with a peer vCenter Server located in a different Single Sign-On domain
   - Pair with a peer vCenter Server located in the same Single Sign-On domain
4. Enter the address of the vCenter Server for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Find vCenter Server Instances**.

   The address that you provide for the vCenter Server must be an exact match of the of address that you provided when you installed Site Recovery Manager Server on the recovery site.

   > **IMPORTANT**
   > To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
5. Select the vCenter Server and the services you want to pair, and click **Next**.
6. On the Ready to complete page, review your settings selection, and click **Finish**.

The protected and the recovery sites are connected. The pair appears under **Site Pairs** on the Site Recovery Home tab.

Reconnect a Site Pair and Breaking a Site Pair

You can reconfigure or break an existing site pair.

If you have problems with an existing site pair, you can attempt to reconnect the site pair with the **Reconnect** action. When you provide the required credentials, the reconfiguration operation attempts to repair the existing site pair.

With the **Break Site Pair** action, you can break the pairing between the Site Recovery Manager Server and vSphere Replication instances on the protected and the recovery sites. You can select which pairing to break. For example, you can break the pairing between the two Site Recovery Manager Server instances, the two vSphere Replication appliances, or both.

> **NOTE**
> You cannot use the **Reconnect** action to add a missing pairing or a pairing that was manually broken with **Break Site Pair**. If your site pair is missing a pairing, you must use **New Site Pair** to configure it.

Establish a Client Connection to the Remote Site Recovery Manager Server Instance

You must establish a connection from the Site Recovery Manager interface in the vSphere Client to the remote Site Recovery Manager Server.

You connected the Site Recovery Manager Server instances on the protected and recovery sites.

You require a client connection to the remote Site Recovery Manager Server to perform operations that affect both sites, such as configuring inventory mappings and creating protection groups. If you do not establish the client connection, Site Recovery Manager prompts you to log in to the remote site when you attempt operations that affect both sites.

1. Connect to the vSphere Client on one of the sites, and select **Site Recovery** > **Open Site Recovery**.
2. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
3. Enter the vCenter Single Sign-On user name and password for the remote site, and click **Log in**.

Install the Site Recovery Manager License Key

Install a Site Recovery Manager license key as soon as possible after you install Site Recovery Manager.

Site Recovery Manager uses the vSphere licensing infrastructure for license management. Ensure that you have sufficient vSphere licenses for Site Recovery Manager to protect and recover virtual machines on both sites.

Site Recovery Manager Server requires a license key to operate.

1. Log in to the vSphere Client.
2. Click **Menu** > **Administration**.
3. Expand **Licensing** and click **Licenses**.
4. On the **Assests** tab, click the **Solutions** tab.
5. Select the vCenter Server instance on which Site Recovery Manager is installed.
6. Click **Assign License**.
7. In the **Assign License** dialog box, click **New License** tab.
8. In the **Assign License** dialog box, type or copy and paste a license key and click **OK**.
9. Enter a name for the new license and click **OK**.
   Details about the product, product features, capacity, and expiration period appear on the page.
10. Click **OK**.
11. In the **Assign License** dialog box, select the newly created license, and click **OK**.
12. Repeat the steps to assign Site Recovery Manager license keys to all appropriate vCenter Server instances.

Unregister an Incompatible Version of vSphere Replication

Site Recovery Manager requires the corresponding version of vSphere Replication.

If you install an incompatible version of vSphere Replication after you deployed this version of Site Recovery Manager, the verification of the vSphere Replication version is not performed and vSphere Web Client stops working.

vSphere Web Client stops working, if you install an incompatible version of vSphere Replication after you have installed Site Recovery Manager.

If you installed an incompatible version of vSphere Replication after you deployed this version of Site Recovery Manager, you must upgrade vSphere Replication to the correct version.

For information about the compatible versions of vSphere Replication, see https://interopmatrix.vmware.com/Interoperability.

If you cannot upgrade vSphere Replication to the correct version, unregister vSphere Replication from vCenter Server. For information about how to unregister vSphere Replication from vCenter Server, see Uninstall vSphere Replication and Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted in *vSphere Replication Administration*.

Reconfiguring the Site Recovery Manager Virtual Appliance

If necessary, you can reconfigure the Site Recovery Manager Appliance settings by using the Site Recovery Manager Appliance Management Interface.

How do I set up a trusted environment for the Site Recovery Manager Virtual Appliance

To set up a trusted environment with your custom root CA certificates, you must manually import the certificates into the Site Recovery Manager Appliance.

The certificates must be in a `.pem` format.

1. To import the root certificate, log in to the Site Recovery Manager Appliance Management Interface as admin.
   a) Click the **Certificates** tab, and under **CA Certificates**, click **Root**.
   b) Click **Add**, insert the certificate in `.pem` format and click **Add**.
2. To import the Site Recovery Manager Server certificates, log in to the Site Recovery Manager Appliance Management Interface as admin.
   a) Click the **Certificates** tab, and click **Change**.
   b) Select a certificate type.

Menu item	Description
Generate a self-signed certificate.	Use an automatically generated certificate. 1. Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company. 2. Accept the default FQDN and IP values. **NOTE** Using a self-signed certificate is not recommended for production environments.
Use a PKCS #12 certificate file.	Use a custom certificate. 1. Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. 2. Enter the optional private key encryption password.

Menu item	Description
Use a CA-signed certificate generated from CSR.	Use a CA-signed certificate generated from a CSR. 1. In the **Certificate file** row, click **Browse**, navigate to the certificate file, and click **Open**. 2. In the **CA chain** row, click **Browse**, navigate to the CA chain, and click **Open**.

c) Click **Change**.

Reconfigure the Site Recovery Manager Appliance

You reconfigure the Site Recovery Manager virtual appliance settings by using the Site Recovery Manager Virtual Appliance Management Interface.

Deploying the Site Recovery Manager Server binds the instance to a number of values that you supply, including the vCenter Server instance to extend, DSN and credentials, the certificate, and so on. You can change some of the values from the Site Recovery Manager Virtual Appliance Management Interface.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click **Summary**, and click **Reconfigure**.
3. On the **Platform Services Controller** page, enter the information about the site where you deployed the Site Recovery Manager Appliance.

Menu Item	Description
PSC host name	Enter the host name (in lowercase letters) or IP address of the vCenter Server with which to register Site Recovery Manager.
PSC port	Accept the default value of `443`, or enter a new value if vCenter Server uses a different port. vCenter Server only supports connections over HTTPS.
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this vCenter Server instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the vCenter Server instance.
Password	The password for the specified vCenter Single Sign-On user name.

4. If prompted, click **Connect** to verify the vCenter Server certificate.
5. On the **vCenter Server** page, click **Next**.

   After the initial configuration of the Site Recovery Manager Appliance, you cannot select a different vCenter Server instance.

6. On the **Name and Extension** page, enter the site name, administrator email address, and local host IP address or name, to register the Site Recovery Manager with vCenter Server.

Menu Item	Description
Site name	A name for this Site Recovery Manager site, which appears in the Site Recovery Manager interface. The vCenter Server address is used by default. Use a different name for each Site Recovery Manager instance in the pair.
Administrator email	The email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.
Local host	The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the Site Recovery Manager Appliance detects is not the interface that you want to use. **NOTE** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

7. On the **Ready to Complete** page, review your settings and click **Finish**.
8. To configure the Site Recovery Manager Appliance on the other site, repeat the procedure.

When the modification operation is finished and the Site Recovery Manager Server restarts, log in to the vSphere Client to check the connection between the sites. If the connection is broken, or if you changed the vCenter Server address, reconfigure the site pairing. For instructions about how to reconfigure the site pairing, see Reconfigure the Connection Between Sites.

Change the Site Recovery Manager Appliance Hostname

To change the Site Recovery Manager appliance hostname, you use the Site Recovery Manager Appliance Management Interface .

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click **Networking** and then click **Edit**.
3. Change the hostname and if necessary the IP address of the Site Recovery Manager virtual appliance.
4. Close the browser and open it again to clear the old session.
5. Log in to the Site Recovery Manager Appliance Management Interface with the new hostname as admin.
6. To change the certificate with the new hostname information, click **Certificate** and then click **Change**.
7. Close the browser and open it again to clear the old session.
8. Log in to the Site Recovery Manager Appliance Management Interface with the new hostname as admin.
9. To reconfigure the Site Recovery Manager Appliance with the new hostname, click **Summary**, then click **Reconfigure**, and complete the wizard.
10. Close the Site Recovery Manager Appliance Management Interface and open the Site Recovery User Interface.
11. On the **Site Recovery** home tab, select the site pair, click **View Details**, and verify the connection status.
12. Optional: If the sites are not connected, click **Reconnect** and provide the required credentials.

Verify the status of all protections groups and recovery plans.

Configure the Time Zone and Time Synchronization Settings for the Site Recovery Manager Appliance

You either use the time settings of the ESXi host on which theSite Recovery Manager Appliance is running, or you configure time synchronization with an NTP server.

If the time settings in your network change, you can edit the time zone and time synchronization settings of the appliance.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click the **Time** tab.
3. Configure Site Recovery Manager Appliance time zone settings.
   a) On the **Time zone** pane, click **Edit**.
   b) From the **Time zone** drop-down menu, select a location or a time zone and click **Save**.
4. On the **Time synchronization** pane, click **Edit**.
5. Configure the time synchronization settings and click **Save**.

Mode	Description
Disabled	No time synchronization. Uses the system time zone settings.
Host	Uses VMware Tools to synchronize the time of the appliance with the time of the ESXi host.
NTP	Enables NTP synchronization. You must enter the IP address or FQDN of one or more NTP servers.

Start, Stop, and Restart Site Recovery Manager Appliance Services

You use the Site Recovery Manager Appliance Management Interface to view the state of the services and to start, stop, and restart them.

You can start, stop, and restart the Site Recovery Manager Server service, the embedded database service, and the `dr-client` service.

1. Log in to the Site Recovery Manager Appliance Management as admin.
2. In the Site Recovery Manager Appliance Management Interface, click **Services**.
   The Services page displays a table of the installed services that can be sorted by name, startup type, and state.
3. Select a service and click **Start**, **Stop**, or **Restart**, then click **OK**.
   Restarting some services might lead to functionality becoming temporarily unavailable.
4. Restart the appliance for the changes to take effect.

Configure the Site Recovery Manager Appliance Network Settings

You use the Site Recovery Manager Appliance Management Interface to customize the network settings of the appliance.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click **Networking**.
3. To configure your network settings, click **Edit**.
4. Configure the DNS settings in the **Hostname and DNS** pane.

Menu Item	Description
Obtain DNS settings automatically	Obtains the DNS settings automatically from the network.
Enter DNS settings manually	Uses the DNS address settings that you set manually. If you select this option, you must provide the IP addresses for a primary and a secondary DNS server.

5. In the **eth0** pane, select the IPv4 or theIPv6 protocol type and configure the IP address settings.
   - Configure the IPv4 address settings.

Option	Description
Obtain IPv4 settings automatically	Obtains the IP address for the appliance from the network.
Enter IPv4 settings manually	Uses an IPv4 address that you set manually. 1. Enter the IPv4 address 2. Enter subnet prefix length. 3. Enter the default IPv4 gateway.

   - Configure the IPv6 address settings.

Option	Description
Obtain IPv6 settings automatically using DHCP	Assigns IPv6 addresses to the appliance from the network by using DHCP. **NOTE** To apply this setting, you must restart the Site Recovery Manager Appliance.
Obtain IPv6 settings automatically using router advertisement	Assigns IPv6 addresses to the appliance from the network by using router advertisement.

Option	Description
Use static IPv6 addresses	Uses static IPv6 addresses that you set up manually. 1. Enter the IPv6 address and the subnet prefix length in the address box. 2. To enter additional IPv6 addresses, click **Add**. 3. Enter the default IPv6 gateway.

6. Click **Save**.
7. Optional: If you change the IP address of the Site Recovery Manager Appliance, you must first reconfigure the Site Recovery Manager Appliance, then change the certificate, and then reconfigure the Site Recovery Manager Appliance again to register the new certificate into the vCenter Server.
   a) Log in to the Site Recovery Manager Appliance Management Interface as admin.
   b) Click the **Summary** tab, click **Configure appliance**, and complete the wizard.
   c) Click the **Access** tab, and then, in the **Certificate** pane, click **Change**.
   d) Select a certificate type, and click **Change**.
   e) Click the **Summary** tab, click **Configure appliance**, and complete the wizard.

Change the Site Recovery Manager Appliance Certificate

You use the Site Recovery Manager Appliance Management Interface to change the appliance certificate.

You can change the certificate for security reasons or if your certificate is expiring. The certificate must be in a `.pem` format.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click **Certificates** and then click **Change**.
3. Select a certificate type.

Menu item	Description
Generate a self-signed certificate	Use an automatically generated certificate. 1. Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company. 2. Accept the default FQDN and IP values. **NOTE** Using a self-signed certificate is only recommended for non-production environments.
Use a PKCS #12 certificate file	Use a custom certificate. 1. Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate. 2. Enter the optional private key encryption password.
Use a CA-signed certificate generated from CSR	Use a CA-signed certificate generated from a CSR. 1. In the **Certificate file** row, click **Browse**, navigate to the certificate file, and click **Open**. 2. In the **CA chain** row, click **Browse**, navigate to the CA chain, and click **Open**.

4. Click **Change**.

Generate and Download a Certificate Signing Request for the Site Recovery Manager Appliance

You generate a certificate signing request (CSR) and a matching private key. The private key remains on the Site Recovery Manager Appliance.

A certificate signing request (CSR) is an encrypted text file that contains specific information, such as organization name, common name, locality, and country. You send the CSR file to a certificate authority (CA) to apply for a digital identity certificate.

ATTENTION
Generating a new private key invalidates any existing CSR configuration.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click the **Access** tab.
3. In the **Certificate** pane, click **Generate CSR**.
4. Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company.
5. Accept the default FQDN and IP values and click **Generate and download**.

To submit a certificate request to the CA in accordance with the CA enrollment process, use the contents of the CSR file.

The CA creates a server certificate based on the information in the CSR file, signs it with its private key, and sends you the certificate, which you can then import to the Site Recovery Manager Appliance.

Add or Delete Additional Certificates

You use the Site Recovery Manager Appliance Management Interface to add or delete additional intermediate and root certificates.

The certificate must be in a `.pem` format.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click **Certificates**, and then click the **Intermediate** or the **Root** tab.
3. Click **Add**, insert the certificate, and then click **Add**.
4. Optional: To delete a certificate, select the certificate, and click **Delete**.

Change the Site Recovery Manager Appliance Password

You use the Site Recovery Manager Appliance Management Interface to change the appliance password.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click **Access**, and change the password from the **Password** pane.

Option	Description
SRM appliance password	Use this option to change the password for the `admin` account.

3. Click **Change**, provide the necessary information, and click **Change** again.

Activate or Deactivate SSH Access to the Site Recovery Manager Appliance

You can use the Site Recovery Manager Appliance Management Interface to edit the appliance SSH access settings.

You can activate or deactivate an SSH access to the appliance only for the `admin` account.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click **Access**.
3. In the **SSH** pane, click **Enable** or **Disable**.

Forward Site Recovery Manager Appliance Log Files to Remote Syslog Server

You can forward the Site Recovery Manager Appliance log files to a remote syslog server to conduct an analysis of your logs.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. In the Site Recovery Manager Appliance Management Interface, select **Syslog Forwarding**.
3. Click **New**, and enter the server address of the destination host in the **New Syslog Forwarding** pane.
4. From the **Protocol** drop-down menu, select the protocol to use.
5. In the **Port** text box, enter the port number to use with the destination host.
   The default port number is `514`.
6. Click **OK**.
7. Verify that the remote syslog server is receiving messages.
8. In the **Syslog Forwarding** section, click **Send Test Message**.
9. Verify that the test message is received on the remote syslog server.

Reconfigure the Connection Between Sites

You must reconfigure the connection between the sites if you made modifications to your Site Recovery Manager installation.

You cannot reconfigure the site pairing to connect Site Recovery Manager to a different vCenter Server instance. You reconfigure an existing pairing to update Site Recovery Manager on both sites if the infrastructure has changed on one or both of the sites.

- You upgraded Site Recovery Manager to a new version.
- You changed the Site Recovery Manager certificate.
- You changed the vCenter Server certificate.
- You changed the vCenter Server address.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
3. Select **Site Pair** > **Summary**, and click **Reconnect**.
   You can initiate the reconnect from either site, even if you only changed the installation on one of the sites.

4. Select the services you want to pair. Enter the address of the vCenter Server on the remote site, provide the vCenter Single Sign-On username and password, and click **Reconnect**.

   If the remote site is in a vCenter Enhanced Linked Mode, the other vCenter Server instances appear in the list but you cannot select a different instance. You can only select the vCenter Server instance that Site Recovery Manager already extends.

Break the Site Pairing and Connect to a New Remote Site

To connect a Site Recovery Manager site to a new remote site, you must remove the existing configurations and break the existing pairing.

- You have an existing Site Recovery Manager installation with two connected sites.
- Make a full backup of the Site Recovery Manager database on both sites by using the tools that the database software provides. For instructions about how to back up the embedded database, see Back Up and Restore the Embedded vPostgres Database.

Site pairing makes modifications on both Site Recovery Manager sites. You cannot reconfigure an existing pairing between Site Recovery Manager sites to connect Site Recovery Manager on one site to a new Site Recovery Manager site. You must remove all configuration from both sites in the existing pair, then break the connection between the sites before you can configure a new site pairing. You cannot break the site pairing until you have removed all existing configurations between the sites.

1. In the vSphere 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 on a recovery plan and select **Delete**.

   You cannot delete recovery plans that are running.
4. Select the **Protection Groups** tab, click on a protection group, and select the **Virtual Machines** tab.
5. Highlight all virtual machines, right-click, and select **Remove Protection**.

   Removing protection from a virtual machine deletes the placeholder virtual machine from the recovery site. Repeat this operation for all protection groups.
6. In the **Protection Groups** tab, right-click a protection group and select **Delete** .

   You cannot delete a protection group that is included in a recovery plan. You cannot delete vSphere Replication protection groups that contain virtual machines on which protection is still configured.
7. Select **Site Pair** > **Configure**, and remove all inventory mappings.
   a) Click each of the **Network Mappings**, **Folder Mappings**, and **Resource Mappings** tabs.
   b) In each tab, select a site, right-click a mapping, and select **Delete**.
8. For both sites, click **Placeholder Datastores**, right-click the placeholder datastore, and select **Remove**.
9. Optional: If you use array-based replication, select **Configure** > **Array Based Replication** > **Array Pairs**, and remove all array pairs.
   a) Select an array pair, click **Array Pair**, and click **Disable**.
   b) Click **Array Manager Pair** and click **Remove**.
10. Select **Site Pair** > **Summary**, and click **Break Site Pair**.

    Breaking the site pairing removes all information related to registering Site Recovery Manager with Site Recovery Managerand vCenter Server on the remote site.

The connection between the sites is broken. You can reconfigure Site Recovery Manager to connect to a new remote site.

- Install a new Site Recovery Manager instance on the new remote site. For instructions about installing Site Recovery Manager, see Deploy the Site Recovery Manager Virtual Appliance.

  IMPORTANT
  The new Site Recovery Manager instance must have the same Site Recovery Manager extension ID as the existing site.
- Optionally uregister Site Recovery Manager Server from the previous remote site. For instructions about unregistering Site Recovery Manager Server, see the steps of Unregister the Site Recovery Manager Appliance from the **Break Pairing** step onwards.
- Reconfigure the inventory mappings and placeholder datastore mappings to map objects on the existing site to objects on the new remote site. For instructions about configuring mappings, see *Site Recovery Manager Administration*.
- Reconfigure the replication of virtual machines from the existing site to the new remote site. For information about configuring array-based replication and vSphere Replication, see Replicating Virtual Machines in *Site Recovery Manager Administration*.
- Create new protection groups and recovery plans to recover virtual machines to the new remote site. For information about creating protection groups and recovery plans, see *Site Recovery Manager Administration*.

How do I activate FIPS on the Site Recovery Manager appliance

This topic outlines the necessary task that you must perform to activate Federal Information Processing Standards (FIPS) mode on the Site Recovery Manager appliance.

Make sure to use trusted certificates when deploying your environment.

NOTE
The certificate file format `PKCS#12` is not supposrted in the Certificates configuration in FIPS mode. The `PKCS#12` file format uses non-FIPS compliant algorithms as a standart specification.

1. Edit the configuration files for the Site Recovery Manager services.
   a) Navigate to `/opt/vmware/dr/conf/drconfig.xml`, open the file and change the following setting.

```
<Config>
    <vmacore>
        <ssl>
            <fips>true</fips>
        </ssl>
    </vmacore>
</Config>
```

   b) Navigate to `/opt/vmware/srm/conf/vmware-dr.template.xml`, open the file and change the following setting.

```
<Config>
    <vmacore>
        <ssl>
            <fips>true</fips>
        </ssl>
    </vmacore>
</Config>
```

   c) Optional: If the appliance is configured, edit the `/opt/vmware/srm/conf/vmware-dr.xml` file.

```
<Config>
    <vmacore>
        <ssl>
            <fips>true</fips>
        </ssl>
```

```
    </vmacore>
</Config>
```

2. Start the Site Recovery Manager services in strict mode.
   a) Edit `/usr/lib/systemd/system/dr-configurator.service`. Uncomment the lines under `# Uncomment to enable FIPS`.
   The file fragment must look like this.
   ```
   # Uncomment to enable FIPS
   Environment=OPENSSL_MODULES=/opt/vmware/dr/lib/ossl-modules
   Environment=OPENSSL_CONF=/opt/vmware/etc/dr/ssl/openssl.cnf
   ```
   b) Edit `/usr/lib/systemd/system/srm-server.service`. Uncomment the lines under `# Uncomment to enable FIPS`.
   The file fragment must look like this.
   ```
   # Uncomment to enable FIPS
   Environment=OPENSSL_MODULES=/opt/vmware/dr/lib/ossl-modules
   Environment=OPENSSL_CONF=/opt/vmware/etc/dr/ssl/openssl.cnf
   ```
   c) Restart the **dr-configurator** and the **srm-server**. Run the following commands.
   ```
   systemctl daemon-reload
   systemctl restart dr-configurator
   systemctl restart srm-server
   ```
3. Log in the appliance as **root** user and edit the kernel cmdline.
   a) Open `/boot/grub/grub.cfg`.
   b) Locate the **menuentry** entry.
   c) Append the following at the end of the line in each **menuentry** that starts with **linux**.
   ```
   fips=1
   ```
   d) Save the file.
4. Start the Config UI in strict mode.
   a) Edit `/usr/lib/systemd/system/drconfigui.service`. Comment out the existing `Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'` and uncomment the lines under `# Uncomment to enable FIPS`.
   The file fragment must look like this.
   ```
   Environment=JRE_HOME=/usr/java/jre-vmware
   # Comment when enable FIPS
   # Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'
   # Uncomment to enable FIPS
   Environment='SERVICE_CLASSPATH=$CATALINA_BASE/lib/ext/*'
   Environment='CATALINA_OPTS=-Xms768m -Xmx1024m -Djava.security.properties==/opt/vmware/dr-client/
   conf/vmware-override-java.security -Dorg.bouncycastle.jca.enable_jks=true -Dorg.bouncycastle.fips.ap-
   proved_only=true'
   ```
   b) Uncomment the `<Manager>` tag in the `/opt/vmware/drconfigui/conf/context.xml` file.
   The file fragment with the tag must look like this.
   ```
   <!-- Uncomment to enable FIPS mode.          -->
   <Manager pathname="" secureRandomAlgorithm=""/>
   ```
   c) Optional: Restart the drconfigui service if FIPS is already enabled for the appliance.
   ```
   systemctl daemon-reload; systemctl restart drconfigui
   ```

5. Start the UI in strict mode.
   a) Edit `/usr/lib/systemd/system/dr-client.service`. Comment out the existing `Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'` and uncomment the lines under `# Uncomment to enable FIPS`.

      The file fragment must look like this.

      ```
      Environment=JRE_HOME=/usr/java/jre-vmware
      # Comment when enable FIPS
      # Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'
      # Uncomment to enable FIPS
      Environment='SERVICE_CLASSPATH=$CATALINA_BASE/lib/ext/*'
      Environment='CATALINA_OPTS=-Xms768m -Xmx1024m -Djava.security.properties==/opt/vmware/dr-client/
      conf/vmware-override-java.security -Dorg.bouncycastle.jca.enable_jks=true -Dorg.bouncycastle.fips.ap-
      proved_only=true'
      ```

   b) Uncomment the `<Manager>` tag in the `/opt/vmware/dr-client/conf/context.xml` file.

      The file fragment with the tag must look like this.

      ```
      <!-- Uncomment to enable FIPS mode.              -->
      <Manager pathname="" secureRandomAlgorithm=""/>
      ```

   c) Edit the `/opt/vmware/dr-client/lib/h5dr.properties` file and modify parameters to point to BCFKS format keystore and truststore with root CA certificates.

      The property must look like this.

      ```
      drTrustStorePass=<same as keyStorePass>
      drTrustStoreName=h5dr.truststore.bks
      keyStoreName=h5dr.keystore.bks
      ```

      If you choose to use a truststore other than the default one, you must add a link to the truststore in `/opt/vmware/dr-client/lib/` or `/opt/vmware/dr-client/webapps/dr/WEB-INF/classes/`. The keystore format must be BCFKS. To import it from JKS format use the following command.

      ```
      $JAVA_HOME/bin/keytool -importkeystore -srckeystore <path-to-jks-keystore> -srcstoretype JKS -src-
      storepass <keystorepass> -destkeystore <path-to-target-bks-keystore> -deststoretype BCFKS -dest-
      storepass <keystorepass> -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -provider-
      path /opt/vmware/dr-client/lib/ext/bc-fips-1.0.2.3.jar
      ```

      NOTE
      The keystore and truststore files you use must have **Others: Read** permission. After reconfiguring the appliance you must reedit the file `/opt/vmware/dr-client/lib/h5dr.properties` according the rules above.

   d) Optional: Restart the dr-client service if FIPS is already enabled for the appliance.

      ```
      systemctl daemon-reload; systemctl restart dr-client
      ```

6. Start the UI plugin (dr-client-plugin) in strict mode.
   a) Edit `/usr/lib/systemd/system/dr-client-plugin.service`. Comment out the existing `Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'` and uncomment the lines under `# Uncomment to enable FIPS`.

      The file fragment must look like this.

      ```
      Environment=JRE_HOME=/usr/java/jre-vmware
      # Comment when enable FIPS
      # Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'
      # Uncomment to enable FIPS
      Environment='SERVICE_CLASSPATH=$CATALINA_BASE/lib/ext/*'
      ```

```
Environment='CATALINA_OPTS=-Xms768m -Xmx1024m -Djava.security.properties==/opt/vmware/dr-client/
conf/vmware-override-java.security -Dorg.bouncycastle.jca.enable_jks=true -Dorg.bouncycastle.fips.ap-
proved_only=true'
```

b) Uncomment the `<Manager>` tag in the `/opt/vmware/dr-client-plugin/conf/context.xml` file.

The file fragment with the tag must look like this.

```
<!-- Uncomment to enable FIPS mode.          -->
<Manager pathname="" secureRandomAlgorithm=""/>
```

c) Optional: Restart the dr-client-plugin service if FIPS is already enabled for the appliance.

```
systemctl daemon-reload; systemctl restart dr-client-plugin
```

7. Start the REST API service (dr-rest) in strict mode.

a) Edit `/usr/lib/systemd/system/dr-rest.service`. Comment out the existing `Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'` and uncomment the lines under `# Uncomment to enable FIPS`.

The file fragment must look like this.

```
Environment=JRE_HOME=/usr/java/jre-vmware
# Comment when enable FIPS
# Environment='CATALINA_OPTS=-Xms768m -Xmx1024m'
# Uncomment to enable FIPS
Environment='SERVICE_CLASSPATH=$CATALINA_BASE/lib/ext/*'
Environment='CATALINA_OPTS=-Xms768m -Xmx1024m -Djava.security.properties==/opt/vmware/dr-client/
conf/vmware-override-java.security -Dorg.bouncycastle.jca.enable_jks=true -Dorg.bouncycastle.fips.ap-
proved_only=true'
```

b) Uncomment the `<Manager>` tag in the `/opt/vmware/dr-rest/conf/context.xml` file.

The file fragment with the tag must look like this.

```
<!-- Uncomment to enable FIPS mode.          -->
<Manager pathname="" secureRandomAlgorithm=""/>
```

c) Optional: Restart the dr-rest service if FIPS is already enabled for the appliance.

```
systemctl daemon-reload; systemctl restart dr-rest
```

8. Reboot the appliance.

Make sure that the `systemctl daemon-reload` command is executed at least once after making the modifications and before rebooting the appliance.

> **NOTE**
> SSHD will read that the kernel has enabled FIPS mode and will activate it too. There is no need to edit anything in the sshd configuration.

Validate that FIPS mode is activated.

How do I validate that FIPS mode is activated

This topic outlines the necessary task that you must perform to validate that Federal Information Processing Standards (FIPS) mode is activated on the Site Recovery Manager appliance.

1. Validate the kernel command line. Run the following command.

```
cat /proc/cmdline
```

2. Validate that the kernel has activated FIPS mode. Run the following command.

```
cat /proc/sys/crypto/fips_enabled
```

3. Validate that the dr-configurator has activated FIPS mode. Run the following command.

```
grep "FIPS" /var/log/vmware/dr/drconfig*
```

4. Validate that vmware-dr has activated FIPS mode. Run the following command.

   ```
   grep "FIPS" /var/log/vmware/srm/vmware-dr*
   ```

5. Validate UI strict mode.

   All UI features must be available and work as expected.

Rename a Site Recovery Manager Site

After you have installed Site Recovery Manager, you can rename a site directly in the Site Recovery Manager interface in the vSphere Client.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
3. Click **Site Pair** > **Summary**, and in the Site Recovery Manager box click **Rename** next to the name of the site you want to rename.
4. Enter a new name for the site and click **Save**.

Unregister the Site Recovery Manager Appliance

If you no longer require Site Recovery Manager, you must follow the correct procedure to cleanly unregister Site Recovery Manager.

Deploying Site Recovery Manager, creating inventory mappings, protecting virtual machines by creating protection groups, and creating and running recovery plans makes significant changes on both Site Recovery Manager sites. Before you unregister Site Recovery Manager, you must remove all Site Recovery Manager configurations from both sites in the correct order. If you do not remove all configurations before unregistering Site Recovery Manager, some Site Recovery Manager components, such as placeholder virtual machines, might remain in your infrastructure.

If you use Site Recovery Manager with vSphere Replication, you can continue to use vSphere Replication after you unregister Site Recovery Manager.

1. In the vSphere 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 on a recovery plan and select **Delete**.

   You cannot delete recovery plans that are running.
4. Select the **Protection Groups** tab, click a protection group, and select the **Virtual Machines** tab.
5. Highlight all virtual machines, right-click, and select **Remove Protection**.

   Removing protection from a virtual machine deletes the placeholder virtual machine from the recovery site. Repeat this operation for all protection groups.
6. In the **Protection Groups** tab, right-click a protection group and select **Delete** .

   You cannot delete a protection group that is included in a recovery plan. You cannot delete vSphere Replication protection groups that contain virtual machines on which protection is still configured.

7. Select **Site Pair** > **Configure**, and remove all inventory mappings.
   a) Click each of the **Network Mappings**, **Folder Mappings**, and **Resource Mappings** tabs.
   b) In each tab, select a site, right-click a mapping, and select **Delete**.
8. For both sites, click **Placeholder Datastores**, right-click the placeholder datastore, and select **Remove**.
9. Optional: If you use array-based replication, select **Configure** > **Array Based Replication** > **Array Pairs**, and remove all array pairs.
   a) Select an array pair, click **Array Pair**, and click **Disable**.
   b) Click **Array Manager Pair** and click **Remove**.
10. Select **Site Pair** > **Summary**, and click **Break Site Pair**.

    Breaking the site pairing removes all information related to registering Site Recovery Manager with Site Recovery Managerand vCenter Server on the remote site.
11. Log in to the Site Recovery Manager Appliance Management Interface as admin.
12. Click **Summary**, and click **Unregister**.
13. Provide the required credentials, review the information, and click **Unregister**.

    IMPORTANT
    Unregistering the Site Recovery Manager Appliance deletes the embedded database. This process cannot be reversed.
14. Repeat the procedure on the other site.

Clean up the vCenter Lookup Service

Use the Managed Object Browser (MOB) to clean up the old Site Recovery Manager registration in Lookup Service after deleting the appliance.

Verify that you have the credentials of a vSphere administrator.

If you delete the Site Recovery Manager Appliance before you unregister it from the environment, you cannot use the Site Recovery Manager virtual appliance management interface (VAMI) to unregister Site Recovery Manager from vCenter Server.

1. Log in with vCenter Server credentials to `https://<vCenter_Server_address>/lookupservice/mob/?moid=ServiceRegistration&method=List&vmodl=1`.
2. To search for the Site Recovery Manager registrations, replace the value in the **Value** field with the following text and click **Invoke Method**.

```
<filterCriteria>
   <serviceType>
      <product>com.vmware.dr</product>
      <type>vcDr</type>
   </serviceType>
</filterCriteria>
```

3. Look for the old Site Recovery Manager registration and copy its **serviceId** value.
4. Navigate to `https://<vCenter_Server_address>/lookupservice/mob/?moid=ServiceRegistration&method=Delete`.
5. To delete the service registration, enter the **serviceId** value and click **Invoke Method**.

Using the Site Recovery Manager Configuration REST APIs Gateway

VMware Site Recovery Manager Configuration REST APIs Gateway provides an API access to the Site Recovery Manager Virtual Appliance.

The Configuration REST APIs Gateway allows you to programmatically perform various configuration tasks without the use of the Site Recovery Virtual Appliance Management Interface.

SRM Configuration REST API Gateway

To access the Site Recovery Manager Configuration REST API Gateway documentation and guidelines, see https://developer.broadcom.com/xapis/srm-appliance-config-api/latest/.

Appliance REST APIs

Table 3: Site Recovery Manager REST APIs Realated to Appliance Operations

Category	Operation Type	REST API Name	Description
Appliance	GET	Get Appliance Disks	Get information about the virtual appliance's disks
Appliance	GET	Get Appliance Info	Get information about the virtual appliance
Appliance	POST	Restart Appliance	Restart the virtual appliance.
Appliance	POST	Shutdown Appliance	Shut down the virtual appliance.

Site Recovery Manager REST APIs for Appliance Settings

Table 4: REST APIs for Appliance Settings

Category	Operation Type	REST API Name	Description
Appliance Settings	GET	Get Syslog Servers	List of all configured syslog servers
Appliance Settings	GET	Get Time Settings	Information about current time settings
Appliance Settings	GET	Get Time Zones	Information about supported time zones.
Appliance Settings	POST	Send Syslog Test Message	Send test message to all syslog servers.
Appliance Settings	POST	Update Appliance Password	Update appliance password.
Appliance Settings	POST	Update Database Password	Update database password.

Category	Operation Type	REST API Name	Description
Appliance Settings	PUT	Update Syslog Servers	Update configured syslog servers.
Appliance Settings	PUT	Update Time Settings	Update current time settings.

Site Recovery Manager REST APIs for Authentication

Table 5: REST APIs for Authentication

Category	Operation Type	REST API Name	Description
Authentication	GET	Get Current Session	Return information about the current session if any.
Authentication	POST	Login	Logs in and returns the session id. Include ‘x-dr-session’ header with value the returned session id in subsequent requests.
Authentication	DELETE	Logout	Logs out if the session is authenticated.

Site Recovery Manager REST APIs for Certificates

Table 6: REST APIs for Certificates

Category	Operation Type	REST API Name	Description
Certificates	POST	Add CA Certificates	Add certificate authorities (CA) certificates.
Certificates	POST	Delete CA Certificates	Delete certificate authorities (CA) certificates.
Certificates	POST	Generate CSR	Generate new key and certificate signing request (CSR) and return it for signing.
Certificates	GET	Get Appliance CA Certificates	Get installed certificate authorities (CA) certificates used to validate other server’s certificates.
Certificates	GET	Get Appliance Certificate	Get appliance certificate information.
Certificates	POST	Probe SSL	Check if the appliance can establish successful SSL connection to the specified endpoint.
Certificates	POST	Update Appliance Certificate	Update appliance certificate.

Site Recovery Manager REST APIs for Configuration

Table 7: REST APIs for Configuration

Category	Operation Type	REST API Name	Description
Configuration	POST	Check Extension Key	Check whether given extension key is already registered in SSO, lookup service and as vCenter Server extension.
Configuration	POST	Delete Configuration	Remove current configuration.
Configuration	GET	Get Configuration	Get appliance configuration information.
Configuration	GET	Get Reconfigure Required	Check if reconfigure operation is required after upgrade.
Configuration	POST	List VC Services	List all vCenter Server instances in the Platform Services Controller.
Configuration	PUT	Update Configuration	Update appliance configuration
Configuration	POST	Validate Connection	Validate connections to the vSphere infrastructure.

Site Recovery Manager REST APIs for Network Settings

Table 8: REST APIs for Network Settings

Category	Operation Type	REST API Name	Description
Network Settings	GET	Get All Network Interfaces Settings	Get all network interface settings.
Network Settings	GET	Get All Network Settings	Current appliance network settings.
Network Settings	GET	Get Network DNS Settings	Get DNS settings.
Network Settings	GET	Get Network Interface Settings	Get network interface settings.
Network Settings	PUT	Update Network DNS Settings	Update DNS settings.
Network Settings	POST	Update Network Interface Settings	Update network interface settings.

Site Recovery Manager REST APIs for Services

Table 9: REST APIs for Services

Category	Operation Type	REST API Name	Description
Services	GET	Get All Services	Get information about all services.
Services	GET	Get Service	Get information about a specific service.
Services	POST	Restart Service	Restart the service.
Services	POST	Start Service	Start the service.
Services	POST	Stop Service	Stop the service.

Site Recovery Manager REST APIs for Tasks

Table 10: REST APIs for Tasks

Category	Operation Type	REST API Name	Description
Tasks	GET	Get All Tasks Info	Retrieve all configuration-related tasks.
Tasks	GET	Get Tasks Info	Retrieve task information.

Site Recovery Manager REST APIs for Updates

Table 11: REST APIs for Updates

Category	Operation Type	REST API Name	Description
Updates	PUT	Change Updates Repository	Change current updates repository.
Updates	POST	Get Updates	Get all available updates in the repository.
Updates	GET	Get Updates Repository	Get information about the current updates repository.
Updates	POST	Install Update	Install the update.

Site Recovery Manager REST APIs for Storage Replication Adapters

Table 12:

Category	Operation Type	REST API Name	Description
Storage Replication Adapters	GET	Get All Storage Replication Adapters	Get all storage replication adapters available on the server.
Storage Replication Adapters	GET	Download SRA Configuration	Download configuration archive for a given storage replication adapter from the server.
Storage Replication Adapters	POST	Upload SRA Configuration	Upload configuration archive for a given storage replication adapter to the server.
Storage Replication Adapters	POST	Copy SRA Configuration	Configuration from the given storage replication adapter is copied over to a specified storage replication adapter.
Storage Replication Adapters	POST	Reset SRA Configuration	Reset configuration of a given storage replication adapter.
Storage Replication Adapters	POST	Reload Storage Replication Adapter	Reload a given storage replication adapter.
Storage Replication Adapters	POST	Create SRA	Create a new storage replication adapter by uploading an installation archive to the server.
Storage Replication Adapters	DELETE	Delete Storage Replication Adapter	Delete a given storage replication adapter.

Site Recovery Manager REST APIs for Support Bundles

Table 13:

Category	Operation Type	REST API Name	Description
Support Bundles	GET	Get Support Bundles	Get all support bundles available on the server.
Support Bundles	GET	Download Support Bundle	Download support bundle information from the server.
Support Bundles	POST	Generate Support Bundle	Generate support bundle.
Support Bundles	DELETE	Delete Support Bundle	Delete the existing support bundle on the server.

Configuring the Customer Experience Improvement Program

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information.

VMware use the information to improve the quality, reliability, and functionality of VMware products and services. To join or leave the CEIP for this product, see *Join or Leave Customer Experience Improvement Program in vSphere Client* in the *VMware vSphere Product Documentation*.

Categories of Information that VMware Receives

This product participates in the VMware Customer Experience Improvement Program (CEIP).

Details regarding the data collected by CEIP and the purposes for which it is used by VMware are available at the Trust & Assurance Center at https://www.vmware.com/trustvmware/ceip.html.

Join or Leave Customer Experience Improvement Program

- CEIP participation requires connection from the Site Recovery Manager virtual appliance to `https://vcsa.vmware.com:443`.
- If the system uses a firewall or a proxy to connect to the Internet, you must specify a firewall or a proxy rule allowing outbound traffic through for `https://vcsa.vmware.com:443/ph/api/*`.
- Verify that you are a member of the Administrators@vsphere.local group.

You can activate or deactivate data collection at any time.

1. Log in to the vCenter Server instance as a member of Administrators@vsphere.local by using the vSphere Client.
2. On the vSphere Client Home page, click **Administration**.
3. Under Deployment, click **Customer Experience Improvement Program**.
4. To join the CEIP, click **Join Program**. To leave the Program, click **Leave Program**.

Provide Feedback with the Site Recovery User Interface

You can use the feedback tool in the Site Recovery user interface to provide timely feedback to our developers.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. From the Site Recovery home screen, click the feedback icon in the top right corner.
3. Rate your overall satisfaction with Site Recovery Manager.
4. Rate the ease of use of Site Recovery Manager.
5. Optional: Enter any feedback about Site Recovery Manager.
6. Click **Send**.

Exporting and Importing Site Recovery Manager Configuration Data

You can use the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool to export and import configuration data.

If you plan to migrate Site Recovery Manager to a different host, you can use the tool to export inventory mappings, recovery plans, protection groups, and the related objects into an XML file. You can then import the configuration data from the previously exported file.

The VMware Site Recovery Manager 8.8 Configuration Import/Export Tool is available through the Site Recovery User Interface and as a standalone `.jar` file. When you deploy the Site Recovery Manager appliance, the tool is also deployed with the appliance. The tool is located in the `/opt/vmware/impex` directory.

Requirements for Using the Standalone Configuration Import/Export Tool

- You must have Java 11.0.x or later installed on the Site Recovery Manager host machine.
- If you want to use the standalone VMware Site Recovery Manager 8.8 Configuration Import/Export Tool from a different virtual machine, you must properly configure the `JAVA_HOME` environment variable. For example, `JAVA_HOME=/usr/lib/java-11-openjdk-11.0.18`.

Requirements for Exporting and Importing Site Recovery Manager Configuration Data

- Before you can export a configuration, you must have a site pair with Site Recovery Manager 8.8.x up and running on both the protected and the recovery site.
- Import is supported in a clean Site Recovery Manager 8.8.x installation, registered to the same vCenter Server instance or to a vCenter Server instance which contains the same inventory.

Input Parameters Required for Import with the Standalone Configuration Tool

- Lookup Service host name. The host name of the vCenter Server.
- vCenter Single Sign-On administrator user name and password for both sites or service account.

Exported Information

The VMware Site Recovery Manager 8.8 Configuration Import/Export Tool exports the Site Recovery Manager version, build number, local and remote site names, inventory mappings, and placeholder datastores. Other exported information includes advanced settings, array managers with SRA information, protection groups, recovery plans, power on and power off settings, shutdown actions, and so on. The information is stored in an XML file. You can validate the XML file by using the following XSD schema.

Export Site Recovery Manager Configuration Data Through the User Interface

You use the Site Recovery User Interface to export Site Recovery Manager configuration data in an XML file.

Verify that you have a site pair with Site Recovery Manager running on both the protected and the recovery sites.

1. In the vSphere 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 **Summary** pane, click **Export/Import SRM Configuration** > **Export**, and click **Download**.

Export Site Recovery Manager Configuration Data by Using a Script Without Credentials

The Site Recovery Manager virtual appliance is bundled with a script generated during pairing that you can use to export configuration data.

Ensure that you have a working Site Recovery Manager pair.

When you use the script to export Site Recovery Manager configuration data, you are not required to enter any credentials.

1. Log in to the Site Recovery Manager virtual appliance host machine as root by using `su`.
2. To export the configuration data, run `sh /opt/vmware/impex/bin/export.sh`.

   The VMware Site Recovery Manager 8.8 Configuration Import/Export Tool exports the configuration data to `/opt/vmware/impex/exports/`.

Modify the Export Script of the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool

The Site Recovery Manager virtual appliance is bundled with a script that you can use to export Site Recovery Manager configuration data.

You can modify the script to change the default export location, the number of exports, and so on.

1. Log in to the Site Recovery Manager virtual appliance host machine.
2. Log in as root by using `su`.
3. SSH to the following location `/opt/vmware/impex/bin/`.
4. Use a text editor to open the `export.sh` file and add the following text to the last line of the script.

Option	Description
To change the location of the export files.	Add "`-e|--exportPath /path/to/export`". The default location is `/opt/vmware/impex/exports/`.
To change the maximum number of export files.	Add "`-m|--maxExports NumberOfMaxExports`". The default number of export files is 24.

5. Save the changes and close the editor.

Schedule an Export of Site Recovery Manager Configuration Data by Using a Cron Job

The Site Recovery Manager virtual appliance is bundled with a script that you can use to schedule a cron job for the export of configuration data.

Ensure that you have a working Site Recovery Manager pair.

1. Log in to the Site Recovery Manager virtual appliance host virtual machine.
2. Run `su`.
3. Run the following command `crontab -e`.
4. Enter the configuration data.
   For example, to export the configuration data at every hour enter the following information.`0 * * * * /usr/bin/sudo /bin/bash /opt/vmware/impex/bin/export.sh`

Export Site Recovery Manager Appliance Configuration Data by Using a Callout

You can use a top-level recovery step in the recovery plan to export configuration data from the Site Recovery Manager appliance.

- Verify that you are using the Site Recovery Manager virtual appliance.
- Ensure that you have a working Site Recovery Manager pair.

1. In the vSphere 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 and select **Recovery Steps**.
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**.
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. Enter the following command in the **Content** text box. `/usr/bin/sudo /bin/bash /opt/vmware/impex/bin/export.sh`
9. Optional: Modify the **Timeout** setting for the command to run on Site Recovery Manager Server.
10. Click **Add** to add the step to the recovery plan.

When you run the recovery plan, the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool exports the configuration data on the recovery site. The default location for the exported configuration data is `/opt/vmware/impex/exports`. You can change the location by modifying the export script, see Modify the Export Script of the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool.

Export Site Recovery Manager Configuration Data with the Standalone Import/Export Tool

You can use the standalone VMware Site Recovery Manager 8.8 Configuration Import/Export Tool to export configuration data in an XML file.

- Verify that you have Java 11.0.x or later installed on the Site Recovery Manager host virtual machine.
- Verify that you have a site pair with Site Recovery Manager running on both the protected and the recovery sites.

1. Log in to the Site Recovery Manager virtual appliance host virtual machine.
2. Navigate to `/opt/vmware/impex`, and run the following command.
   `java -jar import-export.jar --exportInteractive`
   To make the XML file more human-readable, add the `format` option. Adding the `format` option significantly increases the XML file size.

   ```
   java -jar import-export.jar --exportInteractive --format
   ```
3. Enter the host name or the IP address of the Lookup Service.
4. Enter the port number or press Enter, if you use the default port.
5. Accept the SHA-1 Thumbprint.
6. Optional: Select whether to use service account instead of the local vCenter Server credentials.
   a) If you select yes, follow the prompts and provide the necessary information.

Service account path	Path to the service account. For example, *`path:/opt/vmware/impex/sa/file`*.

7. If you selected no, enter the user name and password for the local vCenter Server instance.
8. Select a local Site Recovery Manager instance.
9. Optional: Select whether to use service account instead of the remote vCenter Server credentials.
   a) If you select yes, follow the prompts and provide the necessary information.

Service account path	Path to the service account. For example, *`path:/opt/vmware/impex/sa/file`*.

10. If you selected no, enter user name and password for the remote vCenter Server instance.

Use a Properties File to Export Site Recovery Manager Configuration Data

You can use a properties file to simplify or automate the export of Site Recovery Manager configuration data in an XML file.

- Verify that you have Java 11.0.x or later installed on the Site Recovery Manager host virtual machine.
- Verify that you have a site pair with Site Recovery Manager running on both the protected and the recovery site.
- Verify that you have prepared an *srm_configuration*.properties file.

If you are using the Site Recovery Manager appliance, you can schedule a cron job to automate the export of configuration data.

1. Log in to the Site Recovery Manager virtual appliance host virtual machine.
2. Navigate to `/opt/vmware/impex`, and run the following command.
   `java -jar import-export.jar --exportProperties=`*`Path_to_properties_file`*
   To make the XML file more readable, add the `format` option.
   `java -jar import-export.jar --exportProperties=`*`Path_to_properties_file`* `--format`

Import the Site Recovery Manager Configuration Data through the User Interface

You can use the Site Recovery User Interface to import Site Recovery Manager configuration data from a previously exported XML file.

Provide a clean Site Recovery Manager installation, registered with the same vCenter Server instance or with a vCenter Server instance with the same inventory as the exported.

1. In the vSphere 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 **Summary** tab, click **Export/Import SRM Configuration** > **Import**.
4. On the **Confirmation** page, select the check boxes, and click **Next**.
5. Click **Browse**, navigate to the previously exported XML file, and click **Import**.
6. If the selected export file contains array managers, select which array manager pairs to import and provide credentials, and click **Import**.
   If there are problems with an import stage, you can download a CSV report file.

7. When the import is complete, click **Close**.

Import Site Recovery Manager Configuration Data with the Standalone Import/Export Tool

You use the Standalone Import/Export Tool to import Site Recovery Manager configuration data from a previously exported XML file.

- Provide a clean Site Recovery Manager installation, registered with the same vCenter Server instance or with a vCenter Server instance with the same inventory as the exported.
- Verify that you have Java 11.0.x or later installed on the Site Recovery Manager host virtual machine.

1. Log in to the Site Recovery Manager virtual appliance host virtual machine.
2. Navigate to `/opt/vmware/impex`, and run the following command.
   `java -jar import-export.jar --importInteractive --path` *`Path_to_exported_XML_file`*
   By default the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool is set to retry the import of virtual machines recovery settings after a delay of 10 000 milliseconds up to five times. You can manually change the default values for retry counts and delay between retries by adding the `retries` and `delay` options to the import command. For example, to make 10 retries with a 20 seconds delay, run the following command.
   `java -jar import-export.jar --importInteractive --path` *`Path_to_exported_XML_file`* `--delay 20000 --retries 10`
3. Enter the host name or the IP address of the Lookup Service.
4. Enter the port number or press Enter to use the default.
5. Accept the SHA-1 Thumbprint.
6. Optional: Select whether to use service account instead of the local vCenter Server credentials or not.
   a) If you select yes, follow the prompts and provide the necessary information.

Service account path	Path to the service account. For example, *`path:/opt/vmware/impex/sa/file`*.

7. If you selected no, enter user name and password for the local vCenter Server instance.
8. Select a local Site Recovery Manager.
9. Optional: Select whether to use service account instead of the remote vCenter Server credentials or not.
   a) If you select yes, follow the prompts and provide the necessary information.

Service account path	Path to the service account. For example, *`path:/opt/vmware/impex/sa/file`*.

10. If you selected no, enter user name and password for the remote vCenter Server instance.
11. Provide credentials for the array managers.

The VMware Site Recovery Manager 8.8 Configuration Import/Export Tool imports the Site Recovery Manager configuration data to the new Site Recovery Manager instance.

Use a Properties File to Import Site Recovery Manager Configuration Data

You can use a properties file to simplify or automate the import of Site Recovery Manager configuration data from an XML file.

- Provide a clean Site Recovery Manager installation, registered with the same vCenter Server instance or with a vCenter Server instance with the same inventory as the exported.
- Verify that you have Java 11.0.x or later installed and environment variables configured on the Site Recovery Manager host virtual machine.
- Verify that you have prepared an *srm_configuration*.properties file.

1. Log in to the Site Recovery Manager virtual appliance host virtual machine.
2. Navigate to `/opt/vmware/impex`, and run the following command.
   `java -jar import-export.jar --importProperties=`*`Path_to_properties_file`* `--path` *`Path_to_exported_XML_file`*

Syntax of the Import/Export Tool

The VMware Site Recovery Manager 8.8 Configuration Import/Export Tool includes options that you can use to import or export configuration data.

You can also use the options to change the delay between retries when importing virtual machine recovery settings, to customize the number of retries, to override the network mappings with the mappings from the XML file, and so on.

NOTE
You can use Service Account authentication to import or export data from Site Recovery Manager 8.8. You cannot use solution user authentication to import or export configuration data from Site Recovery Manager 8.8. Solution user authentication is supported for Site Recovery Manager 8.6.x and earlier.

Table 14: VMware Site Recovery Manager 8.8 Configuration Import/Export Tool Options

Option	Description
`--export`	Required when doing an export. Cannot be used together with `--import`.
`--exportProperties`	Used for exporting data by using a properties file.
`--exportInteractive`	Used to start an interactive export with prompts for the required information.
`--importProperties`	Required when importing configuration data with a properties file. Cannot be used together with `--export`.
`--importInteractive`	Used to start an interactive import with prompts for the required information.
`--lspp`	The vCenter Server address. It can be an IP address or FQDN.
`--port <[1, 2147483647]>`	The port number for the Lookup Service. The default value is 443.
`--localSrmName`	The name of the local Site Recovery Manager Server. Required unless you use `--localSrmGuid`.
`--localSrmGuid`	The guid of the local Site Recovery Manager Server. Required unless you use `--localSrmName`.
`--localAuthUseSA`	Used to specify whether to use a Service Account file to log in to the local site.
`--localAuthCredsUsername`	The user name for the local vCenter Server.

Option	Description
`--localAuthCredsPass`	The password for the local vCenter Server.
`--localAuthSAPath`	Used to specify the path to the Service Account file.
`--remoteAuthUseSA`	Used to specify whether to use a Service Account file to log in to the remote site.
`--remoteAuthCredsUsername`	The password for the remote vCenter Server.
`--remoteAuthCredsPass`	The password for the remote vCenter Server.
`--remoteAuthSAPath`	Used to specify the path to the Service Account file.
`--path`	Used for importing data. Path to the previously exported file.
`--delay <[1, 2147483647]>`	An integer value for the desired delay between retries in milliseconds when importing recovery settings. The default value is 10000.
`--retries <[1, 2147483647]>`	An integer value for the count of the retries when importing recovery settings. The default value is 5.
`--overrideProtectionSettings`	Used to override the network mappings. • If there is a protection group, the tool attempts to update the network mappings for each protected virtual machine (override the site-level mappings) with the mappings from the XML file. • If there is a recovery plan, the tool attempts to update the test network mappings for the recovery plan with the mappings from the XML file.
`--format`	Used to make the exported XML file better formatted and human-readable. The `--format` option significantly increases the file size.
`--exportPath`	Path to a directory in which to create the exported file.

Properties for Automated Export and Import of Site Recovery Manager Configuration Data

You use the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool properties file to automate the export and import of configuration data.

The use of *`srm_configuration`*`.properties` file with the standalone VMware Site Recovery Manager 8.8 Configuration Import/Export Tool is optional.

NOTE
You can use Service Account authentication to import or export data from Site Recovery Manager 8.8. You cannot use solution user authentication or keystore authentication to import or export configuration data from Site Recovery Manager 8.8. Solution user authentication and keystore authentication are supported for Site Recovery Manager 8.6.x and earlier.

Table 15: Required Parameters for the Properties File

Parameter	Description
`lookup.service.address`	The vCenter Server address. Can be an IP address or FQDN.
`local.srm.name`	The name of the local Site Recovery Manager Server.

Parameter	Description
local.srm.guid	The GUID of the local Site Recovery Manager Server. Required when two or more local sites share the same name.
local.auth.use.service.account	Set this parameter to true to use service account to log in to the local site. The default value is false.
local.auth.credentials.vc.username	The user name for the local vCenter Server. Required when local.auth.use.service.account is set to false.
local.auth.credentials.vc.password	The password for the local vCenter Server. Required when local.auth.use.service.account is set to false.
local.auth.sa.path	Path to the service account. Required when local.auth.use.service.account is set to true.
remote.auth.use.service.account	Set this parameter to true to use service account to log in to the remote site. The default value is false.
remote.auth.credentials.vc.username	The user name for the remote vCenter Server. Required when remote.auth.use.service.account is set to false. Required if your environment is not federated.
remote.auth.credentials.vc.password	The password of the user for the remote vCenter Server. Required when remote.auth.use.service.account is set to false. Required if your environment is not federated.
remote.auth.sa.path	Path to the service account. Required when remote.auth.use.service.account is set to true.
array.manager.n.name	The name of the array manager, where n is a number. All array managers must be defined at least by a name and a skip flag. Required field for import, if your environment contains any array managers.
array.manager.n.skip	Sets whether the array manager must be imported or skipped. The default value is false. Required if array.manager.n.name is present.
array.manager.n.username	The user name for the array manager. Required if array.manager.n.name is present and array.manager.n.skip value is set to false.
array.manager.n.password	The password for the array manager. Required if array.manager.n.name is present and array.manager.n.skip value is set to false.

Table 16: Optional Parameters for the Properties File

Parameter	Description
port	The port number for the Lookup Service. The default value is 443.
continue.after.array.manager.errors	If you set the value to true, the tool does not fail when an array manager is missing or there is an array-based error. The default value is false.

Sample Properties File

```
lookup.service.address=my.psc.address.com
```

```
port=443
local.srm.name=My local SRM
local.auth.credentials.vc.username=localAdmin
local.auth.credentials.vc.password=localAdminSecretPass
remote.auth.credentials.vc.username=remoteAdmin
remote.auth.credentials.vc.password=remoteAdminSecretPass
continue.after.array.manager.errors=false
array.manager.1.name=am_1
array.manager.1.skip=false
array.manager.1.username=am1AdminUserName
array.manager.1.password=am1AdminSecretPass
array.manager.2.name=am_2
array.manager.2.skip=true
array.manager.3.name=am_3
array.manager.3.skip=true
array.manager.4.name=am_4
array.manager.4.skip=true
```

Troubleshooting the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool

If you encounter problems with exporting or importing Site Recovery Manager configuration data, you can troubleshoot the problem.

When searching for the cause of a problem, also check the VMware knowledge base at http://kb.vmware.com/.

Export Fails with an Error About a Duplicate Key

When you try to export Site Recovery Manager configuration data, the export fails with an error about duplicate INSTANCE_UUID values.

When you try to export Site Recovery Manager configuration data, the export fails due to the following error "`Export ended with errors, check log for more information. Error: Duplicate key l_vm_vm-123456`".

The problem can occur when a virtual machine and a virtual machine template in one of the vCenter Server inventories have the same INSTANCE_UUIDs. The virtual machine and the virtual machine template must have different INSTANCE_UUID values.

The `l_` prefix in the error message means that the objects with the same INSTANCE_UUIDs are in the inventory of the local site. An `r_` prefix in the error message means that the objects with the same INSTANCE_UUIDs are in the inventory of the remote site. The local site is the site from which the export operation is initiated, the remote site is the other site in the Site Recovery Manager pair. The end part of the error message `vm-123456` represents the ManagedObjectReference value of one of the vCenter Server objects.

Delete the virtual machine or the virtual machine template from the vCenter Server inventory. Deleting one of the objects removes the duplicate key.

Upgrading Site Recovery Manager

You can upgrade existing Site Recovery Manager installations.

The Site Recovery Manager upgrade process preserves existing information about Site Recovery Manager configurations.

For information about supported upgrade paths, see **Upgrade Path** > **VMware Site Recovery Manager** in the VMware Product Interoperability Matrixes at https://interopmatrix.vmware.com/Upgrade before you upgrade.

Information That Site Recovery Manager Upgrade Preserves

The Site Recovery Manager upgrade procedure preserves information from existing installations.

Site Recovery Manager preserves settings and configurations that you created for the previous release.

- Datastore groups
- Protection groups
- Inventory mappings
- Recovery plans
- IP customizations for individual virtual machines
- Custom roles and their memberships
- Site Recovery Manager object permissions in vSphere
- Custom alarms and alarm actions
- Test plan histories
- Security certificates
- Mass IP customization files (CSVs)

> **IMPORTANT**
> During an upgrade, Site Recovery Manager preserves only protection groups and recovery plans that are in a valid state.

Site Recovery Manager License

Site Recovery Manager preserves the license only during an upgrade within the same version, for example, from version 8.3.0.x to version 8.3.1, or from version 8.4.0.1 to version 8.4.0.2. During an upgrade to a different version, for example, from 8.4 to 8.5 or later, Site Recovery Manager reverts to an evaluation license. After the upgrade, you must reinstall your Site Recovery Manager license key.

Related Links

Prerequisites and Best Practices for Site Recovery Manager Upgrade on page 111
Before you upgrade Site Recovery Manager, you must perform preparatory tasks on both sites and verify that you have certain information.

Order of Upgrading vSphere and Site Recovery Manager Components on page 113
There are alternative strategies for the upgrade of Site Recovery Manager sites.

Update the Site Recovery Manager Virtual Appliance on page 114
You use the Site Recovery Manager Appliance Management Interface to apply patches and updates to the virtual appliance.

Prerequisites and Best Practices for Site Recovery Manager Upgrade

Before you upgrade Site Recovery Manager, you must perform preparatory tasks on both sites and verify that you have certain information.

- Make a full backup of the Site Recovery Manager database by using the tools that the database software provides. For information about how to back up the embedded database, see Back Up and Restore the Embedded vPostgres Database. Migration of data from an external database to the embedded database is not supported. Failure to back up the database results in the loss of all Site Recovery Manager data if the upgrade fails.
- Perform a configuration export by using the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool. See, Exporting and Importing Site Recovery Manager Configuration Data.
- If you configured advanced settings in the existing installation, take a note of the settings that you configured in **Site Pair** > **Configure** > **Advanced Settings** in the

Site Recovery
user interface.

- Before you upgrade, check the supported upgrade paths.
  For information about supported upgrade paths, see **Upgrade Path** > **VMware Site Recovery Manager** in the VMware Product Interoperability Matrixes at https://interopmatrix.vmware.com/Upgrade before you upgrade.
- The local and remote vCenter Server instances must be running when you upgrade Site Recovery Manager.
- Upgrade the vCenter Server on the site on which you are upgrading Site Recovery Manager to a supported version.
  - When you upgrade or migrate a vCenter Server deployment using an external
    Platform Services Controller, you must first converge the externalPlatform Services Controller to an embedded Platform Services Controller
    and then perform the upgrade or migration. For more information, see *Upgrade or Migration for vCenter Server Instances with an External Platform Services Controller* in the *vCenter Server Upgrade* documentation.
  - For information about how to upgrade vCenter Server and its components, see *vCenter Server Upgrade* in the *ESXi and vCenter Server Documentation*.
  - For information about compatibility between vCenter Server and Site Recovery Manager versions, see *vCenter Server Requirements* in the
    Compatibility Matrices for Site Recovery Manager 8.8 at
    https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html
  - For information about the order in which to upgrade the components on each site, see Order of Upgrading vSphere and Site Recovery Manager Components.
- Obtain the address of the vCenter Server appliance instance for both sites.
- Obtain the vCenter Single Sign-On administrator user name and password for both of the local and remote sites.
- To use Site Recovery Manager with vSphere Replication, upgrade vSphere Replication before you upgrade Site Recovery Manager Server. After upgrading vSphere Replication, you must restart the Site Recovery Manager Server. See Order of Upgrading vSphere and Site Recovery Manager Components.
  - For information about how to upgrade
    vSphere Replication , see *Upgrading vSphere Replication* in *vSphere Replication Administration*.
  - For information about compatibility between vSphere Replication and
    Site Recovery Manager versions, see *vSphere Replication Requirements* in the
    Compatibility Matrices for Site Recovery Manager 8.8 at
    https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html
- If you cannot upgrade an existing incompatible version of vSphere Replication, you must unregister vSphere Replication from both vCenter Server instances before you upgrade Site Recovery Manager. Incompatible versions of Site Recovery Manager and vSphere Replication cause the vSphere Client to stop working.
- If you use custom certificates, obtain an appropriate certificate file. Custom certificates must use at least the SHA1, or preferably SHA256, thumbprint algorithm. This release of Site Recovery Manager does not support certificates that use the MD5 thumbprint algorithm. See Requirements When Using Custom SSL/TLS Certificates With Site Recovery Manager.
- **IMPORTANT**
  Verify that there are no pending cleanup operations on recovery plans and that there are no configuration issues for the virtual machines that Site Recovery Manager protects.
  - All recovery plans are in the Ready state.
  - The protection status of all the protection groups is OK.
  - The protection status of all the individual virtual machines in the protection groups is OK.
  - The recovery status of all the protection groups is Ready.

Related Links

Information That Site Recovery Manager Upgrade Preserves on page 111
The Site Recovery Manager upgrade procedure preserves information from existing installations.

Order of Upgrading vSphere and Site Recovery Manager Components on page 113
There are alternative strategies for the upgrade of Site Recovery Manager sites.

Update the Site Recovery Manager Virtual Appliance on page 114
You use the Site Recovery Manager Appliance Management Interface to apply patches and updates to the virtual appliance.

Order of Upgrading vSphere and Site Recovery Manager Components

There are alternative strategies for the upgrade of Site Recovery Manager sites.

You can upgrade all components of one of your sites before upgrading all the components on the other site or you can upgrade the Site Recovery Manager components on both sites. When you upgrade all components of one of your sites, it is a best practice to upgrade the Site Recovery Manager components before the vCenter Server components.

An alternative strategy is to upgrade the Site Recovery Manager components on both sites before upgrading the vCenter Server components.

You can upgrade the ESXi hosts at any time.

IMPORTANT

- If you configured bidirectional protection, in which each site acts as the recovery site for the virtual machines on the other site, upgrade the most critical of the sites first.
- In an Enhanced Linked Mode environment, do not upgrade Site Recovery Manager and vSphere Replication under more than one vCenter Server instance at the same time.

Upgrading Site Recovery Manager by Sites

Upgrade the protected site first, so you can perform a disaster recovery on the recovery site if you encounter problems during the upgrade that render the protected site unusable.

1. If you use vSphere Replication, upgrade any additional vSphere Replication servers on the protected site.
2. Upgrade the vSphere Replication appliance on the protected site.
3. Upgrade Site Recovery Manager Server on the protected site.
4. If you use array-based replication, upgrade the storage replication adapters (SRA) on the protected site.
5. Upgrade all components of vCenter Server on the protected site.
6. Upgrade the ESXi host on the protected site.
7. If you use vSphere Replication, upgrade any additional vSphere Replication servers on the recovery site.
8. Upgrade the vSphere Replication appliance on the recovery site.
9. Upgrade Site Recovery Manager Server on the recovery site.
10. If you use array-based replication, upgrade the storage replication adapters (SRA) on the recovery site.
11. Upgrade all components of vCenter Server on the recovery site.
12. Upgrade the ESXi hosts on the recovery site.
13. Verify the connection between the Site Recovery Manager sites.
14. Verify that your protection groups and recovery plans are still valid.
15. Upgrade the virtual hardware and VMware Tools on the virtual machines on the ESXi hosts.

Upgrading Site Recovery Manager by Components

With this strategy, you can decide when to upgrade certain components. For example, you can delay the upgrade of the vCenter Server components or the ESXi hosts. Verify which new functionalities are available with earlier versions of vCenter Server.

1. If you use vSphere Replication, upgrade any additional vSphere Replication servers on the protected site.
2. Upgrade the vSphere Replication appliance on the protected site.
3. Upgrade Site Recovery Manager Server on the protected site.
4. If you use array-based replication, upgrade the storage replication adapters (SRA) on the protected site.
5. If you use vSphere Replication, upgrade any additional vSphere Replication servers on the recovery site.
6. Upgrade the vSphere Replication appliance on the recovery site.
7. Upgrade Site Recovery Manager Server on the recovery site.
8. If you use array-based replication, upgrade the storage replication adapters (SRA) on the recovery site.
9. Upgrade all components of vCenter Server on the protected site.
10. Upgrade all components of vCenter Server on the recovery site.
11. Verify the connection between the Site Recovery Manager sites.
12. Verify that your protection groups and recovery plans are still valid.
13. Upgrade the ESXi host on the recovery site.
14. Upgrade the ESXi host on the protected site.
15. Upgrade the virtual hardware and VMware Tools on the virtual machines on the ESXi hosts.

Related Links

Information That Site Recovery Manager Upgrade Preserves on page 111
The Site Recovery Manager upgrade procedure preserves information from existing installations.

Prerequisites and Best Practices for Site Recovery Manager Upgrade on page 111
Before you upgrade Site Recovery Manager, you must perform preparatory tasks on both sites and verify that you have certain information.

Update the Site Recovery Manager Virtual Appliance on page 114
You use the Site Recovery Manager Appliance Management Interface to apply patches and updates to the virtual appliance.

Update the Site Recovery Manager Virtual Appliance

You use the Site Recovery Manager Appliance Management Interface to apply patches and updates to the virtual appliance.

- If you are not updating the appliance from an online URL, download the Site Recovery Manager ISO image and mount it on a system in your environment.
- Perform a configuration export by using the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool. See, Exporting and Importing Site Recovery Manager Configuration Data.

1. In a web browser, go to the Site Recovery Manager Appliance Management Interface at https://*appliance-IP-address-or-FQDN*.
2. Click **Launch Site Recovery Manager Appliance Management**.
3. Log in to the Site Recovery Manager Appliance Management Interface as admin.

   The default password is the admin user account password that you set during the deployment of the Site Recovery Manager Appliance.

4. Click **Update**.
5. To configure your update settings, click **Edit**.

Option	Description
Online repository	To use the repository, you must copy the `update` folder from the ISO image to a web server and provide the URL of that folder. 1. Select **Use repository**. 2. Enter the repository URL, user name (optional), and password (optional).
Downloadable ISO file	Select **Use CD-ROM**.

6. Click **OK**.
7. In the **Available updates** pane, click **Install**.
8. Accept the end-user license agreement, and click **Install**.
   After the update is complete, the appliance restarts.
9. Refresh the browser window to reload the Site Recovery Manager Appliance Management Interface.
10. Log in to the Site Recovery Manager Appliance Management Interface as admin.
11. Click **Reconfigure**.
12. Follow the prompts, provide the required information, and click **Finish**.

Related Links

Information That Site Recovery Manager Upgrade Preserves on page 111
The Site Recovery Manager upgrade procedure preserves information from existing installations.

Prerequisites and Best Practices for Site Recovery Manager Upgrade on page 111
Before you upgrade Site Recovery Manager, you must perform preparatory tasks on both sites and verify that you have certain information.

Order of Upgrading vSphere and Site Recovery Manager Components on page 113
There are alternative strategies for the upgrade of Site Recovery Manager sites.

Installing Site Recovery Manager to Use with a Shared Recovery Site

With Site Recovery Manager, you can connect multiple protected sites to a single recovery site.

The virtual machines on the protected sites all recover to the same recovery site. This configuration is known as a shared recovery site, a many-to-one, fan-in, or an N:1 configuration.

In a shared recovery site configuration, you install one Site Recovery Manager Server instance on each protected site, each of which connects to a different vCenter Server instance.

On the recovery site, you install multiple Site Recovery Manager Server instances to pair with each Site Recovery Manager Server instance on the protected sites. All the Site Recovery Manager Server instances on the shared recovery site connect to a single vCenter Server instance.

Each Site Recovery Manager Server instance in a pair must have the same Site Recovery Manager extension ID, which you can set when you install Site Recovery Manager Server.

You can use either array-based replication or vSphere Replication or a combination of both when you configure Site Recovery Manager Server to use a shared recovery site.

Site Recovery Manager also supports shared protected site (one-to-many, fan-out, or 1:N) and many-to-many (N:N) configurations.

Converting One-to-One Site Recovery Manager Configuration into a Shared Recovery Site Configuration

To convert a one-to-one configuration to a shared recovery site configuration, you deploy additional Site Recovery Manager Server and vCenter Server instances as protected sites, and pair them with additional Site Recovery Manager Server instances that all connect to the existing vCenter Server instance on the recovery site.

Each pair of Site Recovery Manager Server instances in the shared recovery site configuration must use a different Site Recovery Manager extension ID.

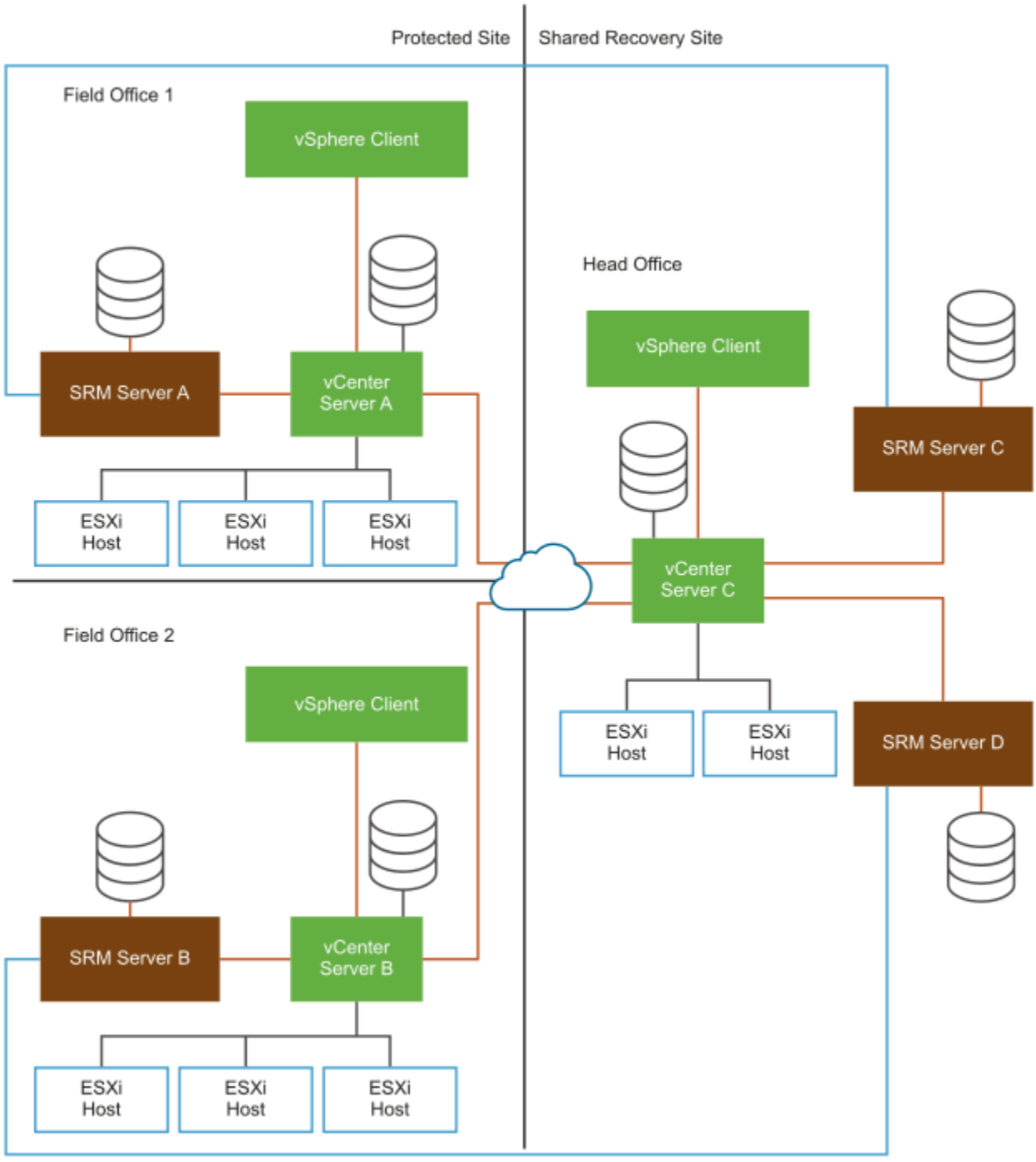
For example, if you installed a one-to-one configuration that uses the default Site Recovery Manager extension ID, you must deploy all subsequent Site Recovery Manager Server pairs with different custom extension IDs.

Using Site Recovery Manager with Multiple Protected Sites and a Shared Recovery Site

An organization has two field offices and a head office. Each of the field offices is a protected site. The head office acts as the recovery site for both of the field offices. Each field office has a Site Recovery Manager Server instance and a vCenter Server instance. The head office has two Site Recovery Manager Server instances, each of which is paired with a Site Recovery Manager Server instance in one of the field offices. Both of the Site Recovery Manager Server instances at the head office extend a single vCenter Server instance.

- Field office 1
  - Site Recovery Manager Server A
  - vCenter Server A
- Field office 2
  - Site Recovery Manager Server B
  - vCenter Server B
- Head office
  - Site Recovery Manager Server C, that is paired with Site Recovery Manager Server A
  - Site Recovery Manager Server D, that is paired with Site Recovery Manager Server B
  - vCenter Server C, that is extended by Site Recovery Manager Server C and Site Recovery Manager Server D

Figure 3: Using Site Recovery Manager in a Shared Recovery Site Configuration



Shared Recovery Sites and vCenter Server Deployment Models

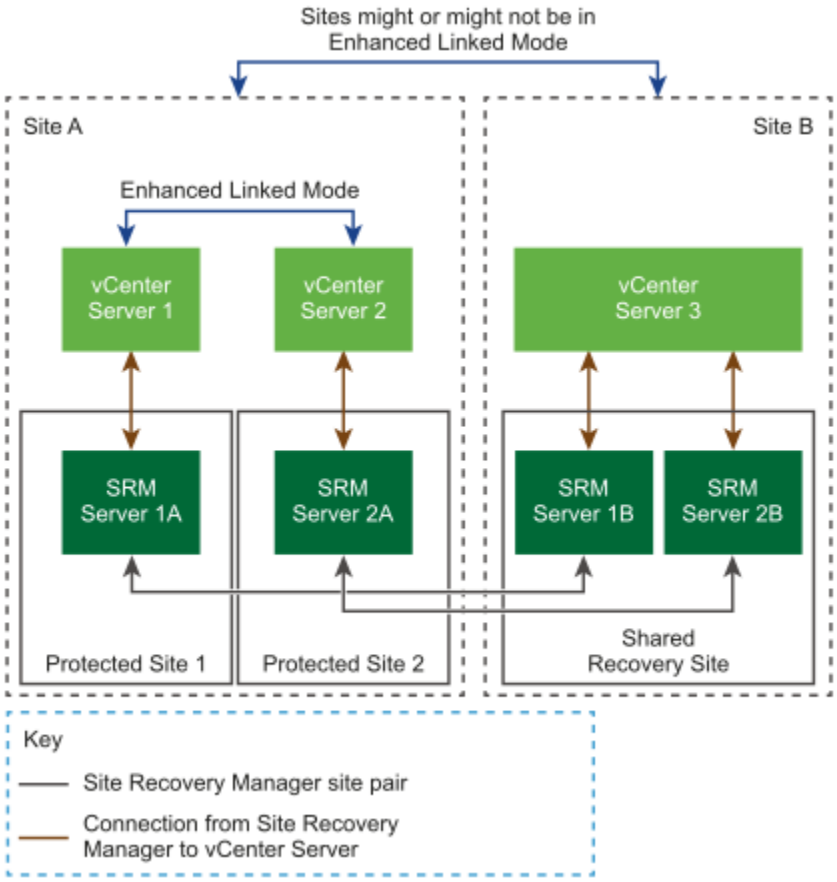
You can use Site Recovery Manager in a shared recovery site configuration in any of the deployment models that vCenter Server supports.

For information about how the vCenter Server deployment model affects Site Recovery Manager, see Site Recovery Manager and vCenter Server Deployment Models.

Site Recovery Manager in a Shared Recovery Site Configuration

In a shared recovery site configuration, the Site Recovery Manager Server instances on the recovery site connect to the same vCenter Server instance.

Figure 4: Site Recovery Manager in a Shared Recovery Site Configuration

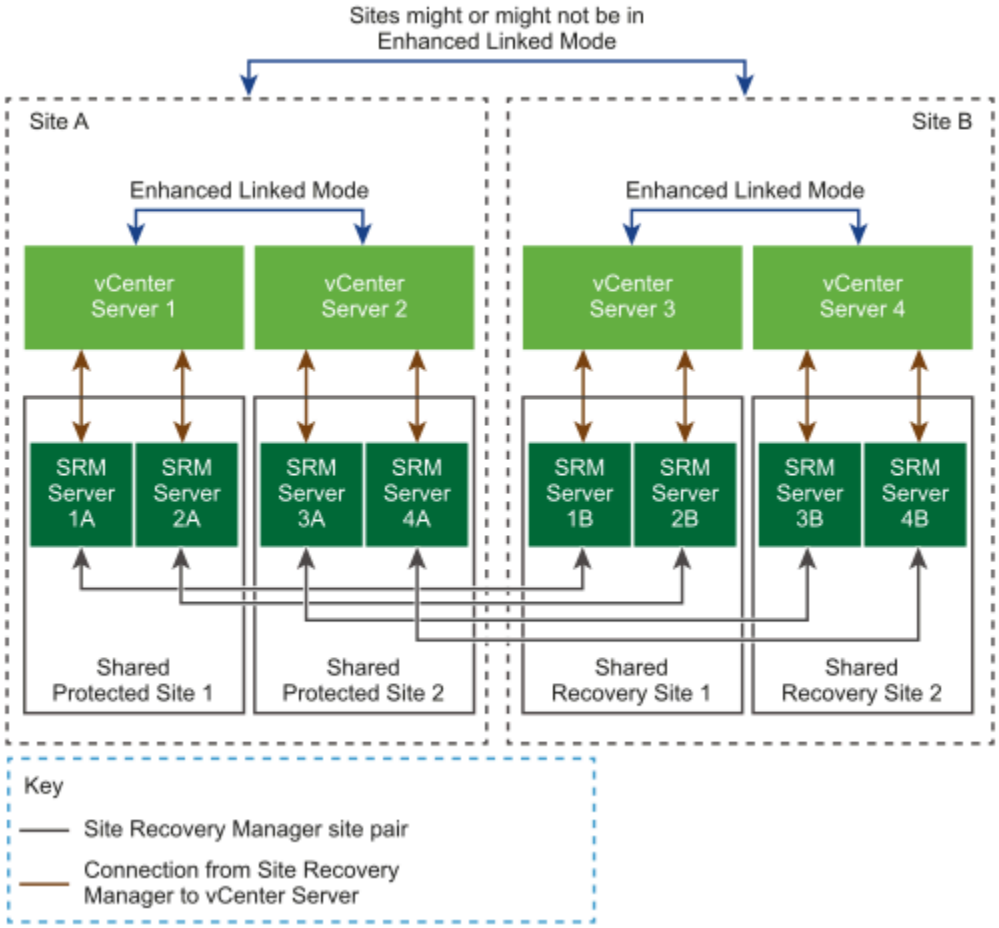


Site Recovery Manager in a Shared Protected Site Configuration

In a shared protected site configuration, the Site Recovery Manager Server instances on the protected site connect to the same vCenter Server.

In this example, two Site Recovery Manager Server instances share a vCenter Server instance on each of two shared protected sites. On the recovery sites, two Site Recovery Manager Server instances share a vCenter Server instance on each shared recovery site.

Figure 5: Site Recovery Manager in a Shared Protected Site and Shared Recovery Site Configuration



Limitations of Using Site Recovery Manager in Shared Recovery Site Configuration

Using Site Recovery Manager with a shared recovery site is subject to some limitations.

When you configure Site Recovery Manager to use a shared recovery site, Site Recovery Manager supports the same operations as it does in a standard one-to-one configuration.

- Site Recovery Manager supports point-to-point replication. Site Recovery Manager does not support replication to multiple targets, even in a multi-site configuration.
- For each shared recovery site customer, you must install Site Recovery Manager Server once at the customer site and again at the recovery site.
- You must specify the same Site Recovery Manager extension ID when you install the Site Recovery Manager Server instances on the protected site and on the shared recovery site. For example, you can install the first pair of sites with the default Site Recovery Manager extension ID, then install subsequent pairs of sites with custom extension IDs.
- Each Site Recovery Manager Server instance on the protected site and on the shared recovery site requires its own database.
- A single shared recovery site can support a maximum of ten protected sites. You can run concurrent recoveries from multiple sites. See Operational Limits of Site Recovery Manager for the number of concurrent recoveries that you can run with array-based replication and with vSphere Replication.

- In a large Site Recovery Manager environment, you might experience timeout errors when powering on virtual machines on a shared recovery site. See Timeout Errors When Powering on Virtual Machines on a Shared Recovery Site.
- When connecting to Site Recovery Manager on the shared recovery site, every customer can see all of the Site Recovery Manager extensions that are registered with the shared recovery site, including company names and descriptions. All customers of a shared recovery site can have access to other customers' folders and potentially to other information at the shared recovery site.

Timeout Errors When Powering on Virtual Machines on a Shared Recovery Site

In a large Site Recovery Manager environment, you might encounter timeout errors when powering on virtual machines on a shared recovery site.

When you power on virtual machines on a shared recovery site, you see the error message `Error:Operation timed out:900 seconds`.

This problem can occur if a single vCenter Server instance manages a large number of virtual machines on the shared recovery site, for example 1000 or more.

1. Increase the `remoteManager.defaultTimeout` timeout value on the Site Recovery Manager Server on the recovery site.
   For example, increase the timeout from the default of 300 seconds to 1200 seconds. For information about how to increase the `remoteManager.defaultTimeout` setting, see Change Remote Manager Settings in the *Site Recovery Manager Administration*.

   Do not increase the timeout period excessively. Setting the timeout to an unrealistically long period can hide other problems, for example problems related to communication between Site Recovery Manager Server and vCenter Server or other services that Site Recovery Manager requires.
2. Open the `vmware-dr.xml` file in a text editor.
   The `vmware-dr.xml` file is located in the `/opt/vmware/srm/conf/` directory.
3. Set the timeout for reading from the vSphere Client.
   Set the timeout to 900 seconds (15 minutes) by adding a line to the `<vmacore><http>` element.

```
<vmacore>
  <http>
    <defaultClientReadTimeoutSeconds>900</defaultClientReadTimeoutSeconds>
  </http>
</vmacore>
```

4. Restart the Site Recovery Manager Server service.

Models for Assigning Site Recovery Manager Licenses in a Shared Recovery Site Configuration

If you configure Site Recovery Manager to use with a shared recovery site, you can assign licenses individually on the shared recovery site.

You can also share a license between all Site Recovery Manager Server instances on the shared recovery site.

In a shared recovery site configuration, you install Site Recovery Manager license keys on each of the protected sites to enable recovery.

- You can install the same license key on the shared recovery site and assign it to the partner Site Recovery Manager Server instance to enable bidirectional operation, including reprotect.
- You can use the same license key for both Site Recovery Manager Server instances in the Site Recovery Manager pair, in the same way as for a one-to-one configuration.
- Alternatively, you can install one Site Recovery Manager license key on the shared recovery site. All Site Recovery Manager Server instances on the shared recovery site share this license. In this configuration, you must ensure that you have sufficient licenses for the total number of virtual machines that you protect on the shared recovery site, for all protected sites.

  Sharing Site Recovery Manager Licenses on a Shared Recovery Site

  You connect two protected sites to a shared recovery site. You install a single Site Recovery Manager license on the shared recovery site.

  - If you protect 20 virtual machines on protected site A, you require a license for 20 virtual machines on protected site A to recover these virtual machines to the shared recovery site.
  - If you protect 10 virtual machines on protected site B, you require a license for 10 virtual machines on protected site B to recover these virtual machines to the shared recovery site.
  - You share a Site Recovery Manager license for 25 virtual machines between two Site Recovery Manager Server instances, C and D, on the shared recovery site. The Site Recovery Manager Server instances on sites A and B connect to Site Recovery Manager Server instances C and D respectively.

  Because you have a license for 25 virtual machines on the shared recovery site, the total number of virtual machines for which you can perform reprotect after a recovery is 25. If you recover all of the virtual machines from sites A and B to the shared recovery site and attempt to perform reprotect, you have sufficient licenses to reprotect only 25 of the 30 virtual machines that you recovered. You can reprotect all 20 of the virtual machines from site A to reverse protection from Site Recovery Manager Server C to site A. You can reprotect only 5 of the virtual machines to reverse protection from Site Recovery Manager Server D to site B. In this situation, you can purchase licenses for more virtual machines for the shared recovery site. Alternatively, you can add the license keys from sites A and B to vCenter Server on the shared recovery site, and assign the license from site A to Site Recovery Manager Server C and the license from site B to Site Recovery Manager Server D.

Install Site Recovery Manager In a Shared Recovery Site Configuration

You can only pair protected and recovery sites that have the same Site Recovery Manager extension ID.

To install Site Recovery Manager in a shared recovery site configuration, you deploy Site Recovery Manager Server on one or more protected sites, and deploy a corresponding number of Site Recovery Manager Server instances on the shared recovery site.

Use vSphere Replication in a Shared Recovery Site Configuration

You use vSphere Replication with Site Recovery Manager in a shared recovery site configuration in the same way that you do in a standard configuration.

- To use
  Site Recovery Manager
  with
  vSphere Replication
  , deploy the appropriate version of
  vSphere Replication

on both of the protected and recovery sites before you install Site Recovery Manager Server. For information about compatibility between vSphere Replication and Site Recovery Manager versions, see *vSphere Replication Requirements* in the *Compatibility Matrices for Site Recovery Manager 8.8* at https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html.

- If you have existing vSphere Replication appliances on the sites, you must either upgrade them to the correct version or unregister them from both vCenter Server instances before you install Site Recovery Manager.

You deploy one vSphere Replication appliance on each protected site. You deploy only one vSphere Replication appliance on the shared recovery site. All of the vSphere Replication appliances on the protected sites connect to this single vSphere Replication appliance on the recovery site. You deploy the vSphere Replication appliances in the same way as for a standard one-to-one configuration.

IMPORTANT
Deploy only one vSphere Replication appliance on the shared recovery site. If you deploy multiple vSphere Replication appliances on the shared recovery site, each new vSphere Replication appliance overwrites the registration of the previous vSphere Replication appliance with vCenter Server. This overwrites all existing replications and configurations.

You can deploy multiple additional vSphere Replication servers on the shared recovery site to distribute the replication load. For example, you can deploy on the shared recovery site a vSphere Replication server for each of the protected sites that connects to the shared recovery site. For information about protection and recovery limits when using vSphere Replication with Site Recovery Manager in a shared recovery site configuration, see Operational Limits of Site Recovery Manager.

1. Deploy a vSphere Replication appliance on each of the protected sites.
2. Deploy one vSphere Replication appliance on the shared recovery site.
3. Optional: Deploy additional vSphere Replication servers on the shared recovery site.
4. Optional: Register the additional vSphere Replication servers with the vSphere Replication appliance on the shared recovery site.

   The vSphere Replication servers become available to all Site Recovery Manager instances on the shared recovery site.

Configure the Site Recovery Manager Appliance on Multiple Protected Sites to Use with a Shared Recovery Site

You must deploy and configure a Site Recovery Manager Appliance on each protected site to use with a shared recovery site.

Deploy the Site Recovery Manager Virtual Appliance and power it on. See *Deploy the Site Recovery Manager Virtual Appliance*.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click the **Summary** tab, and click **Configure appliance**.
3. On the **Platform Services Controller** page, enter the information about the site where you deployed the Site Recovery Manager Appliance.

Menu Item	Description
Address	Enter the host name (in lowercase letters) or IP address of the vCenter Server with which to register Site Recovery Manager.
PSC port	Accept the default value of `443`, or enter a new value if vCenter Server uses a different port. vCenter Server only supports connections over HTTPS.
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this vCenter Server instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the vCenter Server instance.
Password	The password for the specified vCenter Single Sign-On user name.

4. If prompted, click **Connect** to verify the vCenter Server certificate.
5. On the **vCenter Server** page, select the vCenter Server instance with which to register the Site Recovery Manager Appliance, and click **Next**.

   CAUTION
   The drop-down menu includes all the registered vCenter Server instances. In an environment that uses Enhanced Linked Mode, it might also include other vCenter Server instances. Make sure that you select the correct vCenter Server instance. After you configure the Site Recovery Manager Appliance, you cannot select a different vCenter Server instance.
6. On the **Name and Extension** page, enter the necessary information to register the Site Recovery Manager with vCenter Server, and select the default Site Recovery Manager extension identifier, or create a custom extension identifier.
   a) Enter the site name, administrator email address, and local host IP address or name.

Menu Item	Description
Local site name	A name for this Site Recovery Manager site, which appears in the Site Recovery Manager interface. The vCenter Server address is used by default. Use a different name for each Site Recovery Manager instance in the pair.
Administrator email	The email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.

Menu Item	Description
Local host	The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the Site Recovery Manager Appliance detects is not the interface that you want to use. **NOTE** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

b) Select the default Site Recovery Manager extension identifier, or create a custom extension ID for this Site Recovery Manager pair, and click **Next**.

Both Site Recovery Manager instances in a site pair must use the same extension ID.

Menu Item	Description
Default extension ID	Use this option when you deploy Site Recovery Manager in a standard configuration with one protected site and one recovery site.
Custom extension ID	Use this option when you deploy Site Recovery Manager in a shared recovery site configuration, with multiple protected sites and one recovery site. Enter the details for the custom extension ID. • Extension ID. A unique identifier. Assign the same identifier to the Site Recovery Manager instances on the protected site and the shared recovery site. • Organization. The name of the organization to which this Site Recovery Manager sites pair belongs. This name helps to identify Site Recovery Manager pairs in a shared recovery site configuration, especially when multiple organizations use the shared recovery site. • Description. An optional description of the Site Recovery Manager pair.

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

Configure Multiple Site Recovery Manager Server Instances on a Shared Recovery Site

You deploy multiple Site Recovery Manager Server instances that all extend the same vCenter Server instance on the shared recovery site.

- You created one or more protected sites, each with a Site Recovery Manager Server instance for which you configured a unique Site Recovery Manager Extension ID.
- This information presumes knowledge of the standard procedure for deploying Site Recovery Manager. See Deploy the Site Recovery Manager Virtual Appliance for information about a standard Site Recovery Manager deployment.

The Site Recovery Manager Server instances that you deploy on a shared recovery site each correspond to a Site Recovery Manager Server on a protected site.

1. Log in to the Site Recovery Manager Appliance Management Interface as admin.
2. Click the **Summary** tab, and click **Configure appliance**.
3. On the **Platform Services Controller** page, enter the information about the site where you deployed the Site Recovery Manager Appliance.

Menu Item	Description
Address	Enter the host name (in lowercase letters) or IP address of the vCenter Server with which to register Site Recovery Manager.
PSC port	Accept the default value of `443` , or enter a new value if vCenter Server uses a different port. vCenter Server only supports connections over HTTPS.
User name	Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this vCenter Server instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the vCenter Server instance.
Password	The password for the specified vCenter Single Sign-On user name.

4. If prompted, click **Connect** to verify the vCenter Server certificate.
5. On the **vCenter Server** page, select the vCenter Server instance with which to register the Site Recovery Manager Appliance, and click **Next**.

CAUTION
The drop-down menu includes all the registered vCenter Server instances. In an environment that uses Enhanced Linked Mode, it might also include other vCenter Server instances. Make sure that you select the correct vCenter Server instance. After you configure the Site Recovery Manager Appliance, you cannot select a different vCenter Server instance.

6. On the **Name and Extension** page, enter the necessary information to register the Site Recovery Manager with vCenter Server, and select the default Site Recovery Manager extension identifier, or create a custom extension identifier.
   a) Enter the site name, administrator email address, and local host IP address or name.

Menu Item	Description
Local site name	A name for this Site Recovery Manager site, which appears in the Site Recovery Manager interface. The vCenter Server address is used by default. Use a different name for each Site Recovery Manager instance in the pair.
Administrator email	The email address of the Site Recovery Manager administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for Site Recovery Manager events.
Local host	The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the Site Recovery Manager Appliance detects is not the interface that you want to use. **NOTE** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

   b) Create a custom extension ID for this Site Recovery Manager pair as the partner of a Site Recovery Manager Server instance on a protected site, and click **Next**.

      Both Site Recovery Manager instances in a site pair must use the same extension ID.

Menu Item	Description
Default extension ID	Use this option when you deploy Site Recovery Manager in a standard configuration with one protected site and one recovery site.
Custom extension ID	Enter the same Site Recovery Manager ID as you provided for the corresponding Site Recovery Manager Server instance on the protected site. Enter the details for the custom extension ID. • Extension ID. A unique identifier. Assign the same identifier to the Site Recovery Manager instances on the protected site and the shared recovery site. • Organization. The name of the organization to which this Site Recovery Manager sites pair belongs. This name helps to identify Site Recovery Manager pairs in a shared recovery site configuration, especially when multiple organizations use the shared recovery site. • Description. An optional description of the Site Recovery Manager pair.

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

Repeat the procedure to configure further Site Recovery Manager Server instances on the shared recovery site, each with a Site Recovery Manager Extension ID that matches a Site Recovery Manager Server instance on another protected site. Each additional Site Recovery Manager Server instance that you deploy and configure on the recovery site connects

to the vCenter Server instance. You can connect a maximum of 10 Site Recovery Manager Server instances to a single vCenter Server instance.

Connect the Site Recovery Manager Sites in a Shared Recovery Site Configuration

In a shared recovery site configuration, you connect the Site Recovery Manager sites in the same way as for a standard one-to-one configuration.

- You installed Site Recovery Manager Server on one or more protected sites.
- You installed one or more Site Recovery Manager Server instances on a shared recovery site.
- You assigned the same Site Recovery Manager extension ID to a Site Recovery Manager Server instance on a protected site and to a Site Recovery Manager Server instance on the shared recovery site.

If you start the site connection from one of the protected sites, Site Recovery Manager uses the Site Recovery Manager ID that you set during installation to connect to the corresponding Site Recovery Manager Server instance on the recovery site.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select the first site from the list. Enter the address of the vCenter Server for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.

   The address that you provide for the vCenter Server must be an exact match of the of address that you provided when you installed Site Recovery Manager Server on the recovery site.

   IMPORTANT
   To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
4. Select the vCenter Server and the services you want to pair, and click **Next**.

   If several Site Recovery Manager Server instances are registered with this vCenter Server instance, Site Recovery Manager connects to the Site Recovery Manager Server instance that has the corresponding Site Recovery Manager ID.
5. On the Ready to complete page, review the pairing settings, and click **Finish**.
6. Repeat Step 1 to 4 to configure the site pairing for all of the sites that use the shared recovery site.

Use Array-Based Replication in a Shared Recovery Site Configuration

You use array-based replication with Site Recovery Manager in a shared recovery site configuration in the same way as you do in a standard configuration.

- You installed Site Recovery Manager in a shared recovery site configuration.
- You connected the protected sites with the shared recovery site.

To use array-based replication with Site Recovery Manager in a shared recovery site configuration, you must install storage arrays and storage replication adapters (SRA) on each of the protected sites. Each protected site can use a different type of storage array.

Each protected site can either share the same storage on the shared recovery site, or you can allocate storage individually for each protected site. You can use storage from multiple vendors on the shared recovery site, as long as they correspond to storage that you use on the respective protected sites. You must install the appropriate SRA for each type of storage that you use on the shared recovery site.

For information about protection and recovery limits when you use array-based replication with Site Recovery Manager in a shared recovery site configuration, see Operational Limits of Site Recovery Manager.

1. Set up storage arrays on the protected sites following the instructions that your storage array provides.
2. Install the appropriate SRAs on Site Recovery Manager Server systems on the protected sites.
3. Install the appropriate SRAs on Site Recovery Manager Server systems on the shared recovery site.
4. Configure the array managers on the protected sites and on the shared recovery sites.
5. Configure the mappings from the resources on the protected sites to resources on the shared recovery site and configure the placeholder datastores.

Configure Placeholders and Mappings in a Shared Recovery Site Configuration

The customers of the shared recovery site can share the resources on the recovery site. Alternatively, you can assign isolated resources to each customer.

- You installed Site Recovery Manager in a shared recovery site configuration.
- You connected the protected sites with the shared recovery site.
- Familiarize yourself with the procedure for configuring placeholders and mappings. For information about configuring placeholders and mappings in a standard configuration, see *Site Recovery Manager Administration*.

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.

For information about how to assign permissions to allow users to access the resources on a shared recovery site, see *Managing Permissions in a Shared Recovery Site Configuration* in *Site Recovery Manager Administration*.

1. In the vSphere 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, **Network Mappings**, **Folder Mappings**, **Resource Mappings**, **Storage Policy Mappings**, and **Placeholder Datastores**.

Option	Action
Share customer resources	Map the resources, networks, and datastores on the protected sites to a common datacenter, network, and placeholder datastore on the shared recovery site. You can create individual folders for each customer on the recovery site and map the folders on the protected sites to the individual folders.
Isolate customer resources	Map the resources, networks, folders, and datastores on the protected sites to separate datacenters, networks, folders, and placeholder datastores on the shared recovery site.

4. Optional: If you use vSphere Replication, select the appropriate target datastores for the replica virtual machines when you configure replication.

   Avoid using the same datastore as the target for vSphere Replication as you use as the placeholder datastore for Site Recovery Manager.

Option	Action
Share customer resources	Select a common target datastore on the shared recovery site. You can create individual folders in the target datastore for each customer on the recovery site.
Isolate customer resources	Select a different datastore for each customer on the shared recovery site.

Upgrade Site Recovery Manager in a Shared Recovery Site Configuration

You can upgrade existing Site Recovery Manager installations that use a shared recovery site.

- Verify that you know the standard procedure for upgrading Site Recovery Manager. For information about a standard Site Recovery Manager upgrade, see Upgrading Site Recovery Manager.
- Evaluate the importance of each protected site, and prioritize the upgrade of the sites accordingly.

When you upgrade a Site Recovery Manager installation that uses a shared recovery site, apply the same recommendations for upgrading a standard one-to-one installation of Site Recovery Manager. See Upgrading Site Recovery Manager.

Upgrade all of the protected sites before you upgrade the shared recovery site. When you upgrade all of the protected sites before you upgrade the shared recovery site, you can run recoveries on the shared recovery site if failures occur on a protected site during the upgrade process. If you upgrade vCenter Server on the shared recovery site before you upgrade all of the protected sites, you must complete all the upgrades to perform recovery.

Upgrade the protected sites in order of importance, upgrading the most important sites first and the least important sites last. For example, upgrade protected sites that run business-critical applications before you upgrade sites that are less vital to your operations.

1. Optional: Upgrade vCenter Server on the most critical of the protected sites.
2. Optional: If you use vSphere Replication, upgrade the vSphere Replication appliance that connects to the vCenter Server instance that you upgraded in 1.
3. Upgrade the Site Recovery Manager Server instance that connects to the vCenter Server instance that you upgraded in 1.
4. Optional: If you use array-based replication, upgrade the storage replication adapters (SRA) on the Site Recovery Manager Server host machine that you upgraded in 3.
5. Repeat 1 to 4 for each of the protected sites that connect to the shared recovery site.
6. Optional: Upgrade vCenter Server on the shared recovery site.
7. Optional: If you use vSphere Replication, upgrade the vSphere Replication appliance on the shared recovery site.
8. Upgrade the Site Recovery Manager Server instance on the shared recovery site that is paired with the first protected site that you upgraded.
9. Optional: If you use array-based replication, upgrade the SRAs for this Site Recovery Manager Server instance on the shared recovery site.
10. Repeat 8 and 9 for each of the remaining Site Recovery Manager Server instances on the shared recovery site.
11. Optional: Upgrade the ESXi Server instances on the shared recovery sites and each of the protected sites.
12. Upgrade the virtual hardware and VMware Tools on the virtual machines on the ESXi Server instances.

Site Recovery Manager Administration

Detailed instructions on how to use VMware Site Recovery Manager to protect your environment.

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.

Site Recovery Manager Privileges, Roles, and Permissions

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 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*.

Related Links

Site Recovery Manager and the vCenter Server Administrator Role on page 131
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 on page 132
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 on page 133
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 on page 135
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 on page 136
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.

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.

Related Links

How Site Recovery Manager Handles Permissions on page 130

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 vSphere Replication Roles on page 132

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 on page 133

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 on page 135

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 on page 136

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.

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.

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.

Related Links

How Site Recovery Manager Handles Permissions on page 130
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 on page 131
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.

Managing Permissions in a Shared Recovery Site Configuration on page 133
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 on page 135
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 on page 136
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.

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.

Related Links

How Site Recovery Manager Handles Permissions on page 130
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 on page 131
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 on page 132
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.

Assign Site Recovery Manager Roles and Permissions on page 135

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 on page 136

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.

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 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.

1. In the vSphere 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 3 through 5 to assign roles and privileges to the users or user groups on the other Site Recovery Manager site.

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

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.

Related Links

How Site Recovery Manager Handles Permissions on page 130
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 on page 131
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 on page 132
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 on page 133
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.

Site Recovery Manager Roles Reference on page 136
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.

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 17: 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 grant access to a user, the Site Recovery Manager Administrator must add a new role.	**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
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.	**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

Related Links

How Site Recovery Manager Handles Permissions on page 130
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 on page 131
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 on page 132
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 on page 133
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 on page 135
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.

Replicating Virtual Machines

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.

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.

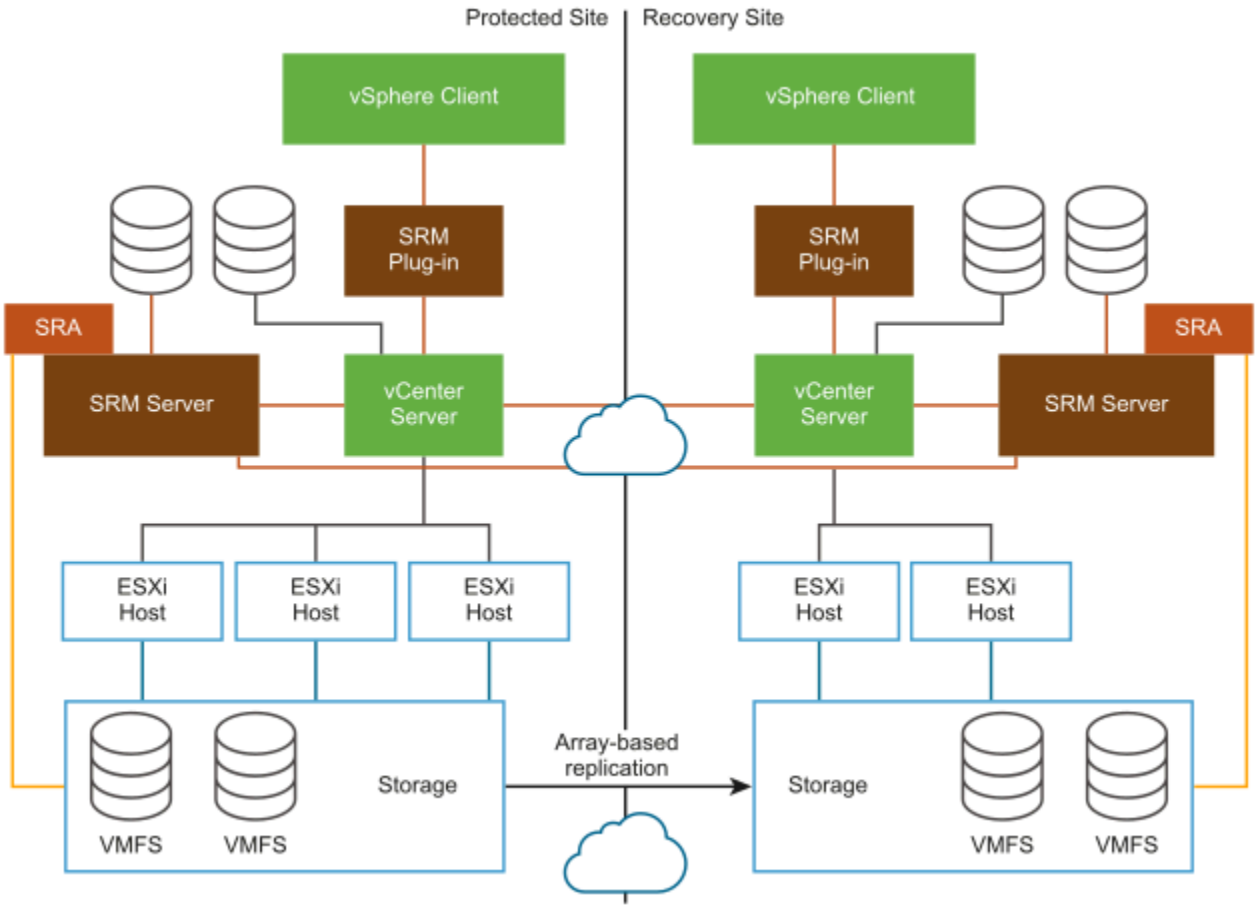
If your storage array supports consistency groups, Site Recovery Manager is compatible with vSphere Storage DRS and vSphere Storage vMotion. You can use Storage DRS and Storage vMotion to move virtual machine files within a consistency group that Site Recovery Manager protects. If your storage array 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 deactivates 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 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.

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 6: Site Recovery Manager Architecture with Array-Based Replication



Configure Array-Based Replication

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

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.

- 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.

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.

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.
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.

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

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. 1. Navigate to the directory where you saved the SRA configuration archive file and select it. The configuration files are distributed as `.tar.gz` archives. 2. 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.

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.

1. In the vSphere 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.

- 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 Add Storage Replication Adapters to the Site Recovery Manager Appliance.

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.

1. In the vSphere 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.

1. In the vSphere 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.

How do I activate NVMe support in Pure Storage SRAs

To use NVMe datastores with Pure Storage SRAs, you must reconfigure the storage replication adapter.

1. Log in to the Site Recovery Manager Appliance Management Interface on the protected site as admin.
2. Click the **Storage Replication Adapters** tab.
3. Select the appropriate Storage Replication Adapter card, click the drop-down menu (⋮), and click **Download Configuration Archive**.
   The configuration files are distributed as `.tar.gz` archives.
4. Navigate to the directory where you saved the SRA configuration archive file and open it.
5. Change the NVMe support option to `true` and save the file.
   `<NvmeSupport>true</NvmeSupport>`
6. Log in to the Site Recovery Manager Appliance Management Interface on the protected site as admin.
7. Click the **Storage Replication Adapters** tab.
8. Select the appropriate Storage Replication Adapter card, click the drop-down menu (⋮), and click **Upload Configuration Archive**.
9. Navigate to the directory where you saved the SRA configuration archive file, select it and click **Open**.
10. Repeat Step 1 through Step 9 on the recovery site.
11. In the vSphere Client on the protected site, click **Site Recovery** > **Open Site Recovery**.
12. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
13. On the Site Pair tab, click **Configure** > **Array Based Replication** > **Array Pairs**.
14. Select the array pair and click **Array Manager Pair** > **Discover Array Pairs** to rescan the arrays.
15. Repeat Step 11 through Step 14 on the recovery site.

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.

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

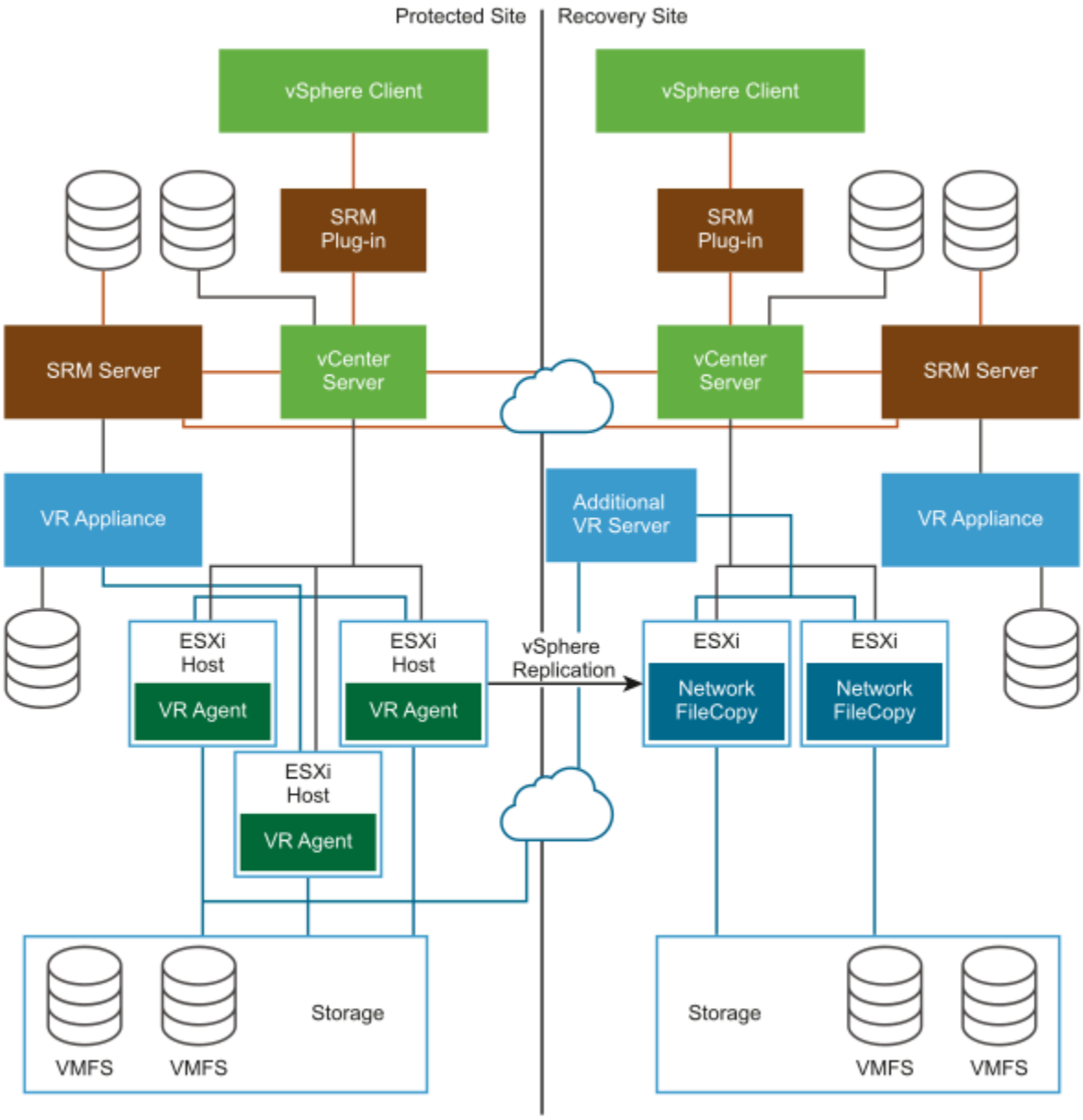
Site Recovery Manager can use vSphere Replication to replicate data to servers at the recovery site.

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://docs.vmware.com/en/vSphere-Replication/index.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 7: 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.

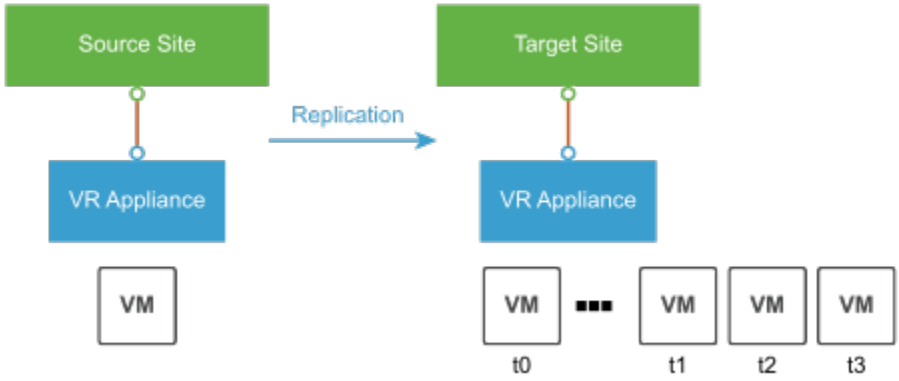
When you configure a replication, you can enable multiple point in time (MPIT) instances in the recovery settings. vSphere Replication keeps several snapshot instances of the virtual machine on the target site, based on the retention policy that you specify. vSphere Replication supports a maximum of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

During the replication process, vSphere Replication replicates all aspects of the virtual machine to the target site, including any potential viruses and corrupted applications. If a virtual machine has a virus or a corruption and you have configured vSphere Replication to keep PIT snapshots, you can recover the virtual machine and then revert it to a snapshot 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 8: Recovering a Virtual Machine at Points in Time



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.

NOTE
Site Recovery Manager supports protection and orchestrated recovery of NVMe over Fabrics (NVMe-oF) datastores for Virtual Volumes replication protection groups with vSphere 8.0 and later.

Configure Virtual Volumes

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

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

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.

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

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.

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**.

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.

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**.

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.

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. Deactivate or activate 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.

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

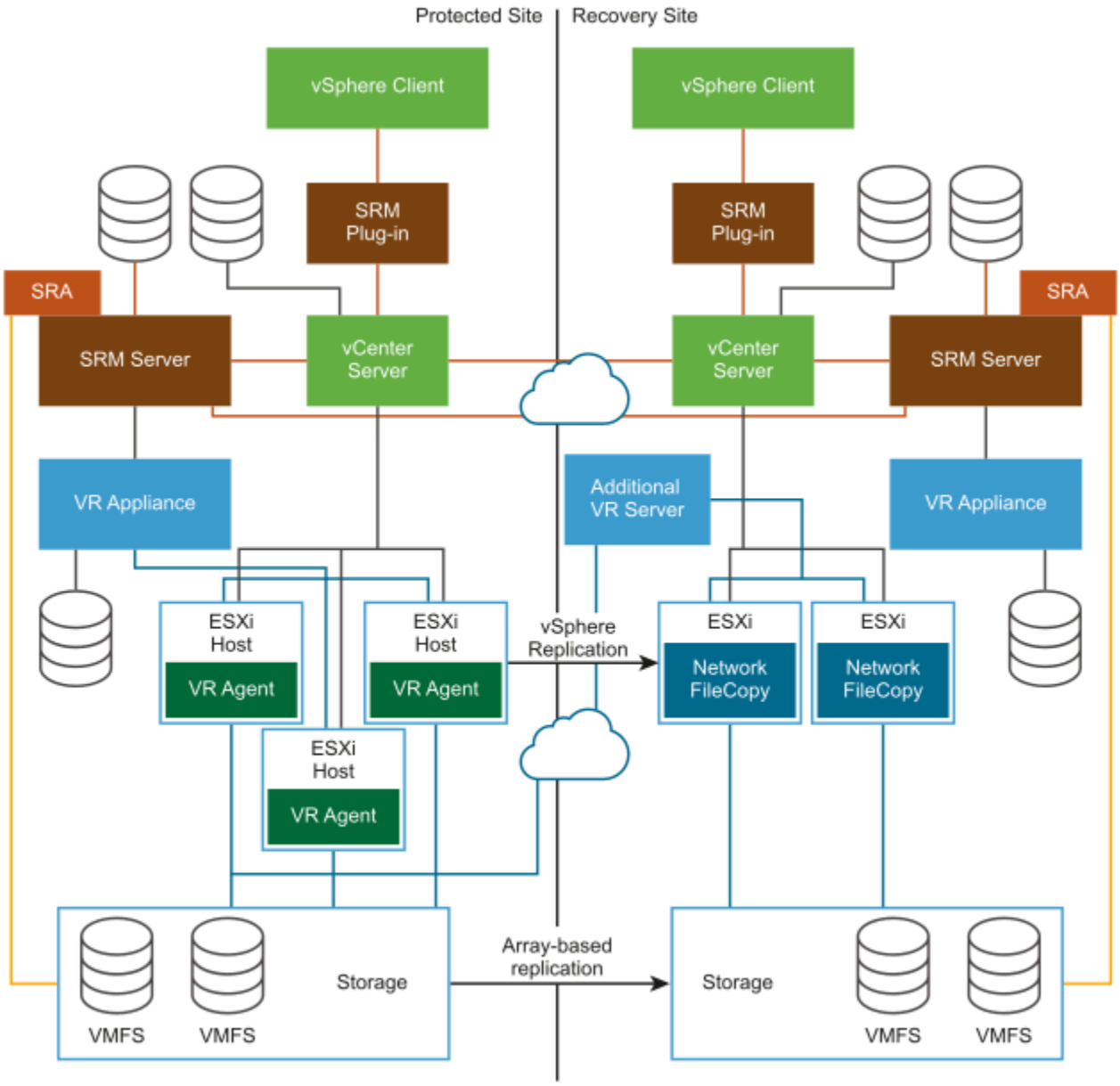
To create a mixed Site Recovery Manager deployment that uses array-based replication and vSphere Replication, you must configure the protected and recovery sites for both types of replication.

- 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 9: Site Recovery Manager Architecture with Array-Based Replication and vSphere Replication



Configuring Mappings

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.

Inventory Mappings for Array-Based Replication Protection Groups, Virtual Volumes Protection Groups, and vSphere Replication Protection Groups

For array-based protection, Virtual Volumes 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, Virtual Volumes, 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, by default the changes affect virtual machines that Site Recovery Manager already protects in an existing protection group. Site Recovery Manager updates recovery target (folder, resource pool, or network) for all protected virtual machines to reflect the concrete mapping change. You can control this feature through the **replication.updateVmProtectionOnInvMappingChange** advance setting. The advanced setting is activated by default.

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, Virtual Volumes protection groups, and vSphere Replication protection groups. If you create an array-based replication protection group, a Virtual Volumes protection group, or a vSphere Replication protection group without having defined site-wide inventory mappings, you can configure each virtual machine in the group individually. You can override site-wide inventory mappings by configuring the protection of the virtual machines in a protection group. You can also create site-wide inventory mappings after you create a protection group, and then apply those site-wide mappings to that protection group.

- For information about configuring site-wide inventory mappings, see Configure Inventory Mappings.
- For information about configuring mappings on virtual machines individually, see Configure Inventory Mappings for an Individual Virtual Machine in 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.

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, Virtual Volumes 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, Virtual Volumes protection group, or a vSphere Replication protection group at the moment that you create the protection group. When you create a new side-wide mapping Site

Recovery Manager updates accordingly the protection of all already protected virtual machines related to the new side-wide mapping.

1. In the vSphere 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.
7. Click **Add mappings**.

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

10. Optional: If you are configuring network mappings, in the **Test networks** page, click **Change** and in the **Edit Test Network** page 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 as specific network on the recovery site to use for tests.

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

12. Repeat 3 through 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 array-based replication 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.

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

1. In the vSphere 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

When you create an array-based replication protection group that contains datastore groups, Virtual Volumes protection group, 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. To avoid name collisions with the folders vSphere Replication creates, the name of a folder of the placeholder virtual machine on the datastore is suffixed with `-phVm` . The suffix is removed on recovery.

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

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

About Placeholder 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, Virtual Volumes replication, 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.

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.

What Happens to Placeholder Virtual Machines During Recovery

When you create array-based protection groups, Virtual Volumes 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.

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.

If vSphere vMotion is activated for array-based replication protection groups, the virtual machines are live migrated and the placeholder VMs are not replaced.

Related Links

About Placeholder Virtual Machines on page 155
When you create an array-based replication protection group that contains datastore groups, Virtual Volumes protection group, 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.

Select a Placeholder Datastore on page 157
If you use array-based protection groups, Virtual Volumes 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.

Select a Placeholder Datastore

If you use array-based protection groups, Virtual Volumes 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.

- 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.

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

If you remove an existing placeholder datastore and want the placeholder VMs to go to another placeholder datastore, you must delete manually all placeholder VMs on the old datastore and recreate them for the affected protection groups. Alternatively, you can remove the protection from the virtual machines and recreate it.

1. In the vSphere 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.
6. Select the other site in the pair.
7. Repeat 3 to 5 to configure a placeholder datastore on the other site.

Related Links

What Happens to Placeholder Virtual Machines During Recovery on page 156
When you create array-based protection groups, Virtual Volumes 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.

About Placeholder Virtual Machines on page 155

When you create an array-based replication protection group that contains datastore groups, Virtual Volumes protection group, 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.

Reprotect fails with an error

Reprotect fails with an error "`Protection group pg_name has protected VMs with placeholders which need to be repaired.`".

When performing a reprotect, the operation fails with an error "`Protection group pg_name has protected VMs with placeholders which need to be repaired.`".

If the placeholder datastore is not visible from a given host, that might cause the reprotect operation to fail.

Fix the placeholder datastores to meet the requirements outlined in Select a Placeholder Datastore and re-run the reprotect operation.

Automatic Placeholder Datastore Selection

Site Recovery Manager supports automatic placeholder datastore selection.

A datastore is suitable for placeholder virtual machines when it meets certain criteria.

- The datastore is not replicated.
- The datastore is mounted with read/write permissions.
- The datastore has enough free space. For more information about the minimum required free space , see Change Replication Settings.
- The datastore is accessible from all hosts in the compute resource.
- The automatic protection user has read/write permissions on the datastore. For more information about the user account, see Change the Automatic Protection Settings.

Site Recovery Manager triggers automatic placeholder datastore selection when you pair your Site Recovery Manager instance with a remote Site Recovery Manager site or when you change **`replication.automaticPlaceholderDatastoreSelection`** from deactivated to activated. When you change the **`replication.automaticPlaceholderDatastoreSelection`** advanced setting from activated to deactivated, all automatically selected placeholder datastores are removed from the list without affecting the existing virtual machines protection.

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, or Virtual Volumes replication. You cannot create protection groups that combine virtual machines for which you configured array-based replication with virtual machines for which you configured vSphere Replication, or Virtual Volumes replication. 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.

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.

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.

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.

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.

Protect an Encrypted VM

You can protect and recover encrypted VMs by using, an array-based replication protection group or a vSphere Replication protection group.

- 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 8.0* documentation.

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

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 or a vSphere Replication 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.

Automatic Protection of Virtual Machines

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

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 service account as automatic protection user. The local service account is *SRM-<srm-server-uuid>*. 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.

Automatic Protection Removal

Site Recovery Manager can automatically remove the protection of an already protected virtual machine if it meets certain preconditions.

The automatic protection removal functionality is available for array-based replication protection groups and Virtual Volumes replication protection groups. The automatic protection removal is not supported for vSphere Replication protection groups. To use the automatic protection removal functionality, you must activate both the advanced settings for Automatic Protection and the advanced settings for Automatic Protection Removal. For more information see, Change the Automatic Protection Settings.

To become eligible for automatic protection removal, the virtual machines must fall into one of the following categories.

- For array-based replication and Virtual Volumes replication protection groups, protected VMs for which the production VM is no longer registered in the vCenter Server inventory.
- For array-based replication protection groups, protected VMs for which all disks, configuration files, snapshot descriptors, and other critical for failover file backed devices are provisioned or moved on datastores that are not part of the replicated datastore groups from which the protected VM is part of.
- For Virtual Volumes replication groups, protected VMs for which all disks, configuration files, snapshot descriptors, and other critical for failover file backed devices are no longer part of Virtual Volumes replication groups that in turn are part of corresponding protection groups.

CAUTION
When the automatic protection removal is activated and the virtual machine is unprotected you cannot recover the VM. When the automatic protection removal is deactivated and the virtual machine is unregistered from the vCenter Server inventory, if the protected virtual machine is still available, you can run the recovery and get the virtual machine up and running on the recovery site. Activate the automatic protection removal functionality only when reconfiguring protection groups is intended.

Once the protection is automatically removed, the virtual machine can become eligible for protection immediately in another protection group or after some time in the same protection group or a different protection group. If the the virtual machine is automatically protected within a configurable amount of time, the VM is associated with the last used recovery settings. If the virtual machine is automatically protected after that period of time, the VM uses the default recovery settings. The lifetime for the archived records for the recovery settings is configured through the **replication.archiveRecoverySettingsLifetime** advanced setting. You can use the **replication.archiveRecoverySettingsCleanupInterval** advanced setting to configure the time interval in minutes between separate executions of the task to cleanup old archived VM recovery settings. For more information, see Change Replication Settings.

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 18: 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.
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.

State	Description
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 19: 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.
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.

State	Description
`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.

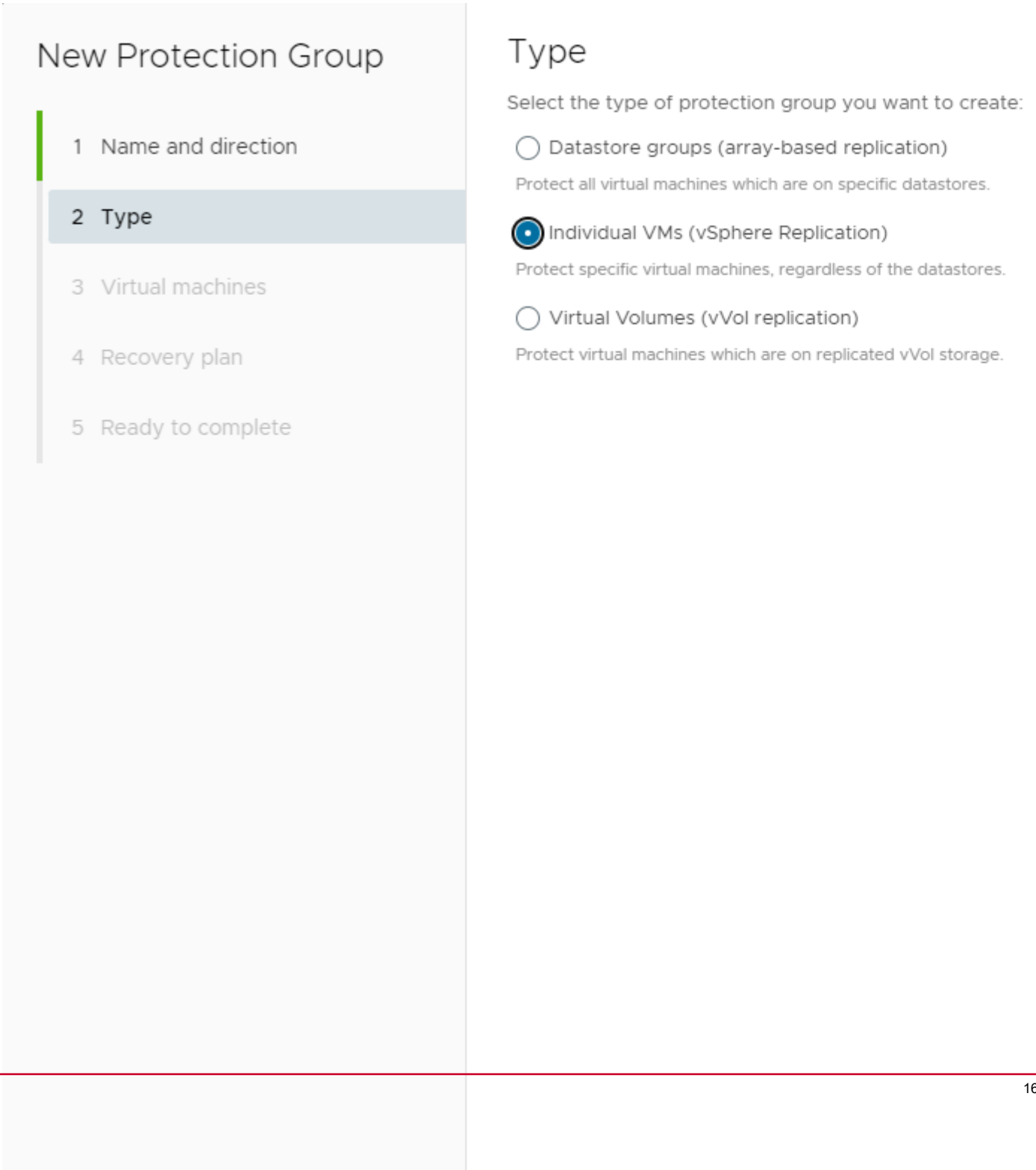
NOTE
The name of the protection group must be different than the name of the selected folder.

Create vSphere Replication Protection Groups

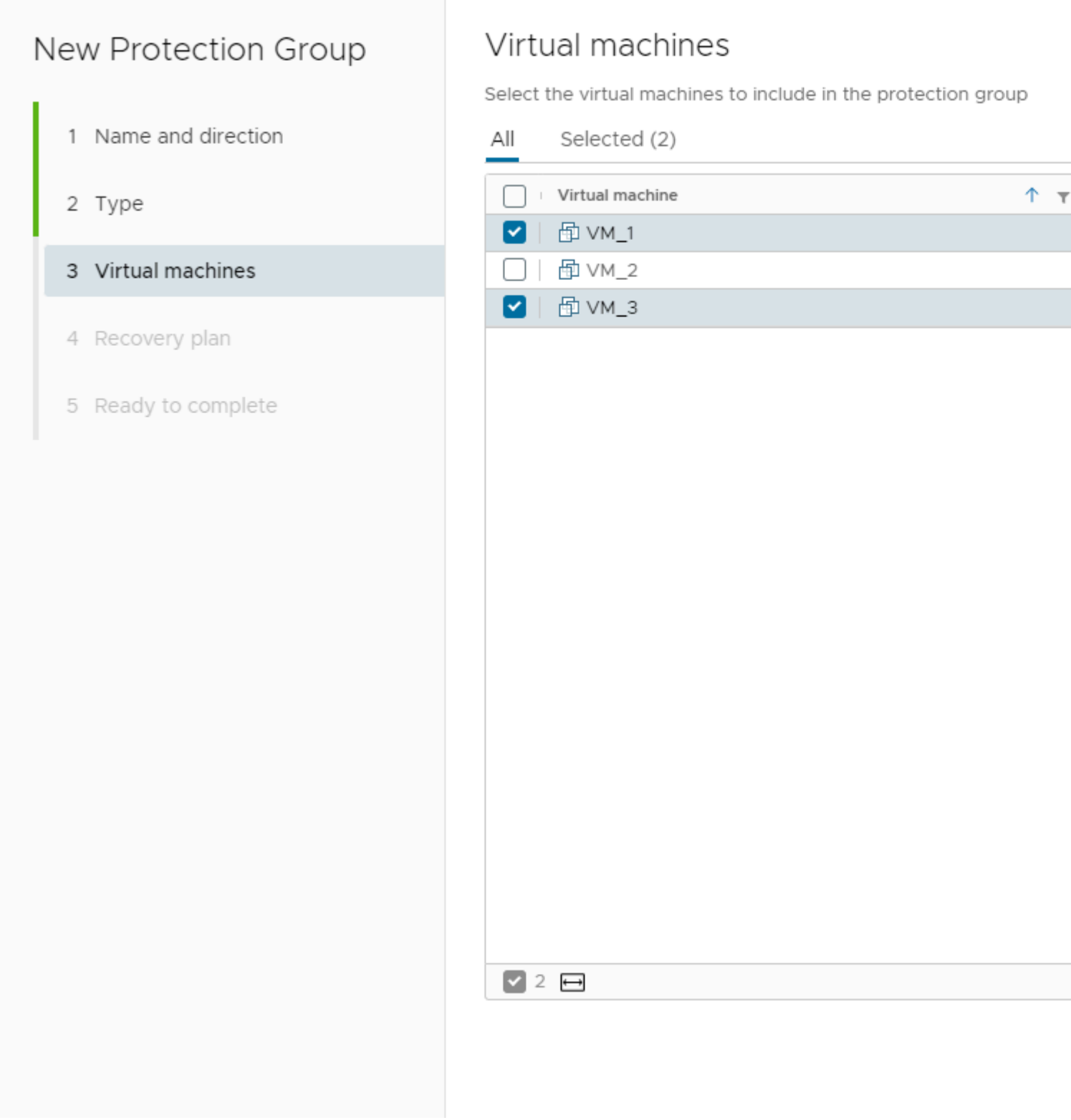
Create vSphere Replication protection groups to protect virtual machines for which you configured vSphere Replication.

Verify that you configured vSphere Replication on virtual machines.

1. In the vSphere 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 Protection Group** 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 **Type** page, 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**.

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`.

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

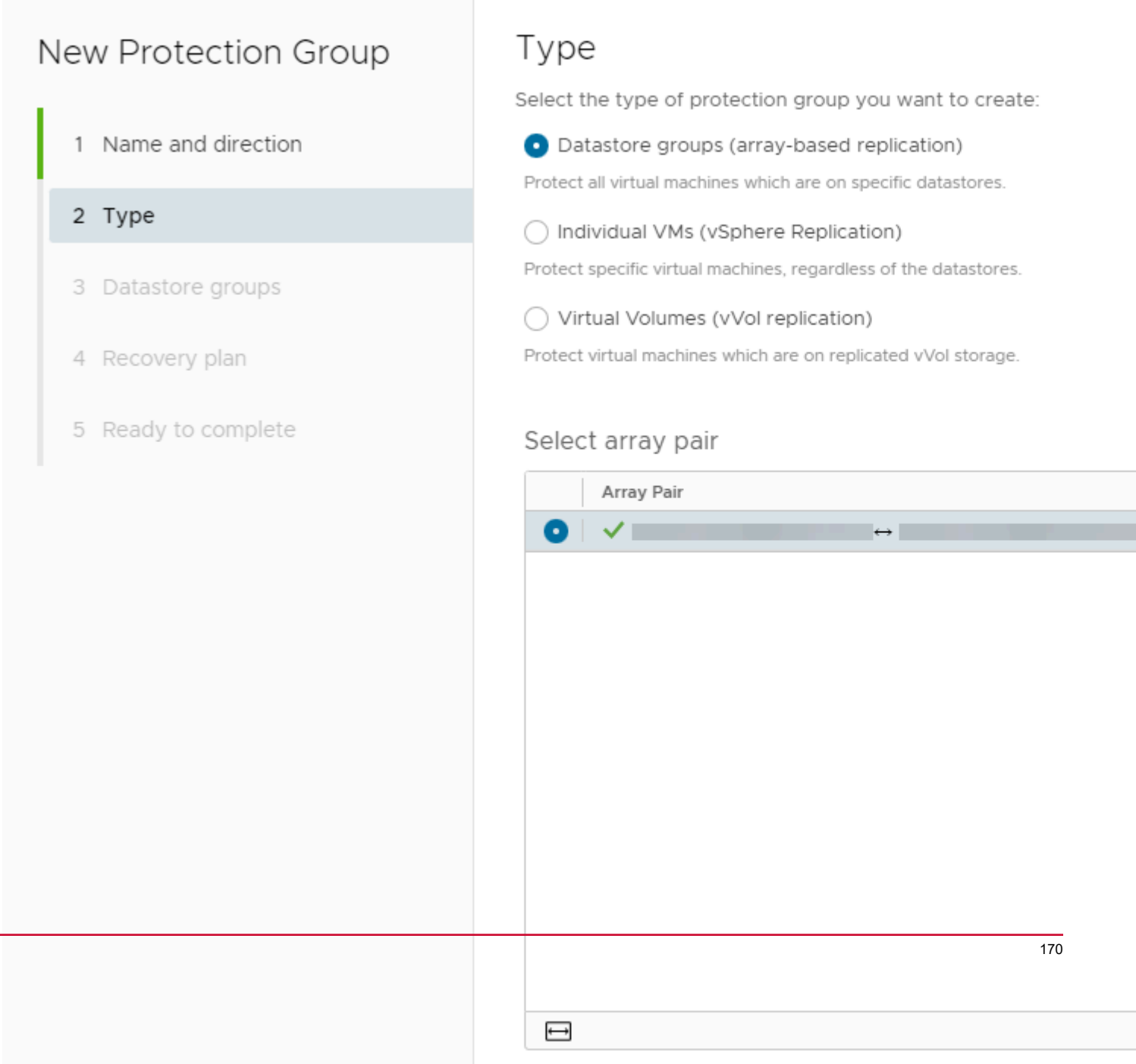
- To apply site-wide inventory mappings, or to check whether inventory mappings that you have already set are valid, see Configure Inventory Mappings. To apply these mappings to all the virtual machines, see Apply Inventory Mappings to All Members of an Array-Based, Virtual Volumes, or vSphere Replication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

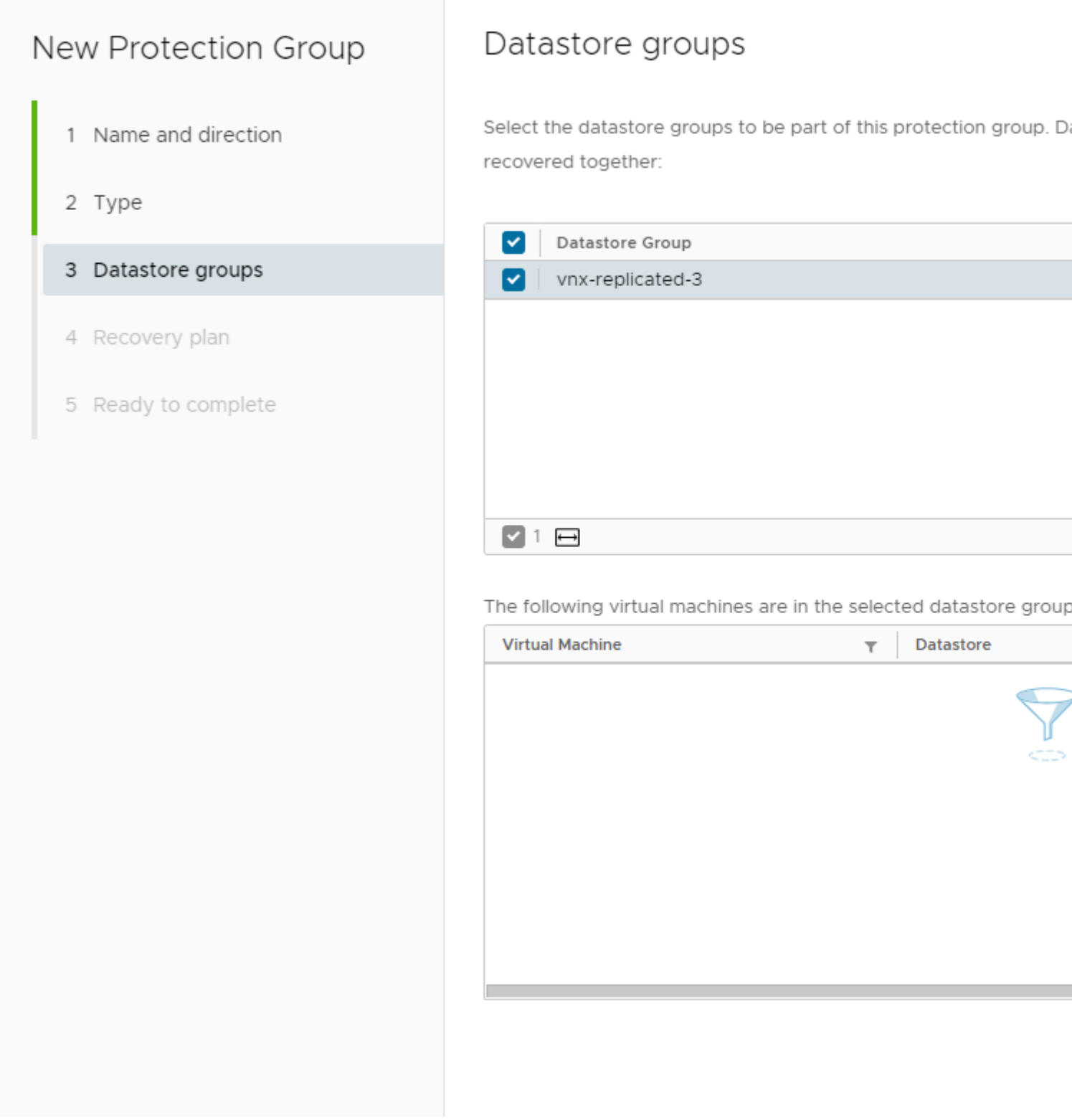
Create array-based replication protection groups to protect virtual machines for which you configured array-based replication.

- Verify that you have included virtual machines in datastores for which you configured array-based replication.
- Verify that if you are using resource pools in the array pair resource mappings section, there is also a mapping from the parent cluster.

1. In the vSphere 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 Protection Group** 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 **Type** page, 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`.

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.

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

1. In the vSphere 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 Protection Group** 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`.

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.

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.

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

1. In the vSphere 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**.

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`.

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.

- 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.

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.

1. In the vSphere 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 created an array-based, Virtual Volumes, or vSphere Replication protection group.

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.

1. In the vSphere 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.

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.

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 deactivate 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.

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

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.

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.

Related Links

Performing a Planned Migration or Disaster Recovery by Running a Recovery Plan on page 180
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 experiences 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 on page 182
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 on page 183
You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

Create, Test, and Run a Recovery Plan on page 184
You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

Export Recovery Plan Steps on page 190
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 on page 191
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 on page 193
If you do not need a recovery plan, you can delete it.

Overview of Recovery Plan States on page 193
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.

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 experiences 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.

Related Links

Testing a Recovery Plan on page 178

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

Differences Between Testing and Running a Recovery Plan on page 182
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 on page 183
You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

Create, Test, and Run a Recovery Plan on page 184
You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

Export Recovery Plan Steps on page 190
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 on page 191
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 on page 193
If you do not need a recovery plan, you can delete it.

Overview of Recovery Plan States on page 193
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.

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 20: 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.
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.

Area of Difference	Test a Recovery Plan	Run a Recovery Plan
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.

Related Links

Testing a Recovery Plan on page 178
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 on page 180
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 experiences an unforeseen event that might result in data loss, you can also run a recovery plan under unplanned circumstances.

Performing Test Recovery of Virtual Machines Across Multiple Hosts on the Recovery Site on page 183
You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

Create, Test, and Run a Recovery Plan on page 184
You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

Export Recovery Plan Steps on page 190
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 on page 191
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 on page 193
If you do not need a recovery plan, you can delete it.

Overview of Recovery Plan States on page 193
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.

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.

Related Links

Testing a Recovery Plan on page 178
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 on page 180
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 experiences 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 on page 182
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.

Create, Test, and Run a Recovery Plan on page 184
You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

Export Recovery Plan Steps on page 190
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 on page 191
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 on page 193
If you do not need a recovery plan, you can delete it.

Overview of Recovery Plan States on page 193
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.

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.

Related Links

Testing a Recovery Plan on page 178
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 on page 180

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 experiences 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 on page 182
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 on page 183
You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

Export Recovery Plan Steps on page 190
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 on page 191
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 on page 193
If you do not need a recovery plan, you can delete it.

Overview of Recovery Plan States on page 193
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.

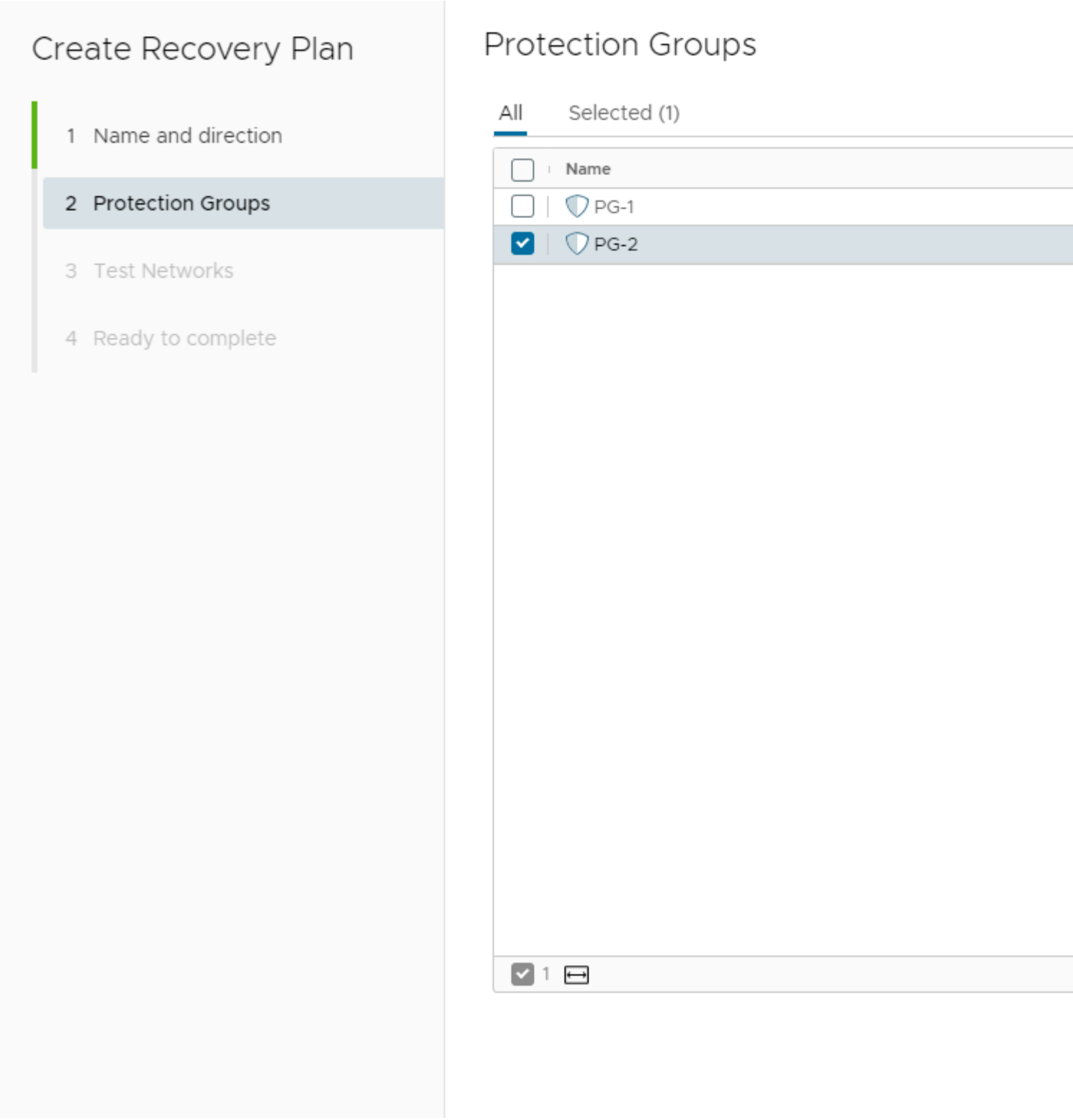
Create a Recovery Plan

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

1. In the vSphere 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 Recovery Plan** 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 one or more protection groups for the plan to recover, and click **Next**.



6. On the **Test Network** page, click **Change**, 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.

7. 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.

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.

1. In the vSphere 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.

1. In the vSphere 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.

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.

Verify that you tested a recovery plan.

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.

1. In the vSphere 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.

- 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.
- 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.

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.

1. In the vSphere 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.

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.

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.

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.

1. In the vSphere 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.

Run a cleanup after canceling a test.

Export Recovery Plan Steps

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

Verify that no test recovery or real recovery is in progress.

1. In the vSphere 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.

Related Links

Testing a Recovery Plan on page 178
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 on page 180
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 experiences 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 on page 182
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 on page 183
You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

Create, Test, and Run a Recovery Plan on page 184
You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

View and Export a Recovery Plan History Report on page 191
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 on page 193
If you do not need a recovery plan, you can delete it.

Overview of Recovery Plan States on page 193
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.

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.

You ran or tested a recovery plan, or performed a cleanup after a test.

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.

> **NOTE**
> When exporting the history report in HTML format, the custom per virtual machine commands are missing from the report. To see the custom per virtual machine commands, export the report in XML format.

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

1. In the vSphere 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.

Related Links

Testing a Recovery Plan on page 178
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 on page 180
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 experiences 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 on page 182
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 on page 183
You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

Create, Test, and Run a Recovery Plan on page 184
You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

Export Recovery Plan Steps on page 190
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.

Delete a Recovery Plan on page 193
If you do not need a recovery plan, you can delete it.

Overview of Recovery Plan States on page 193
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.

Delete a Recovery Plan

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

Verify that the recovery plan is in a consistent state.

1. In the vSphere 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**.

Related Links

Testing a Recovery Plan on page 178
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 on page 180
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 experiences 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 on page 182
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 on page 183
You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

Create, Test, and Run a Recovery Plan on page 184
You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

Export Recovery Plan Steps on page 190
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 on page 191
You can view and export reports about each run of a recovery plan, test of a recovery plan, or test cleanup.

Overview of Recovery Plan States on page 193
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.

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 21: Recovery States

State	Description
`Ready`	Recovery steps are cleared. You can verify protected virtual machines in a recovery plan in the **Virtual Machines** tab.
`Test in progress`	Canceling a test moves plan to `Cancel in progress` state.

State	Description
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.
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. 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. 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.
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.

State	Description
Cancel in progress	Canceling a test results in Test complete with last result canceled. Canceling a recovery results in Incomplete recovery with last result canceled. If the operation is canceled early enough, 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.
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.

State	Description
`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.

Related Links

Testing a Recovery Plan on page 178
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 on page 180
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 experiences 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 on page 182
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 on page 183
You can create recovery plans that recover virtual machines across multiple recovery site hosts in a quarantined test network.

Create, Test, and Run a Recovery Plan on page 184
You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

Export Recovery Plan Steps on page 190
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 on page 191
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 on page 193
If you do not need a recovery plan, you can delete it.

Configuring a Recovery Plan

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.

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. You cannot run top-level commands on Site Recovery Manager Server on Azure VMware Solution.

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. You cannot run commands on Site Recovery Manager Server on Azure VMware Solution. 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 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 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 22: 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 23: 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_Guest*Name	Name of the guest OS as defined by the VIM API.	otherGuest
*VMware_VM_Guest*Ip	IP address of the virtual machine, if known.	192.168.0.103
Vmware_VM_Path	Path to the VMX file of this virtual machine.	`[datastore-123] jquser-vm2/jquser-vm2.vmx`

Table 24: 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`

Commands That Can Run on Site Recovery Manager

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
```

You cannot run commands on Site Recovery Manager Server on Azure VMware Solution.

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_Re-
coveryMode% 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.

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

1. In the vSphere 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.

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.

- 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.

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.

1. In the vSphere 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.

1. In the vSphere 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**.

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.

1. In the vSphere 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.

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.

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.

1. In the vSphere 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 activate or deactivate vSphere vMotion from the **Recovery Properties** dialog box.

- Before performing a vSphere vMotion migration, confirm that the virtual machine belongs to an array-based replication 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.
- For your array-based replication protection groups, ensure that you have configured reverse mappings.

1. In the vSphere 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**.

There is no power cycle during the planned migration. Configured shutdown or startup actions or steps configured before and after power on are ignored.

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 created a recovery plan.

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.

1. In the vSphere 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 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 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

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 8.8* at https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.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 (OSPs) on the virtual machine. See https://www.vmware.com/support/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.

1. In the vSphere 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 25: 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 7 through 10 to configure recovery site or protected site settings, if necessary.

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

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.

Related Links

Customizing IP Properties for Multiple Virtual Machines on page 211

You can customize the IP properties for multiple virtual machines on the protected and recovery sites by using the DR IP Customizer tool, by defining subnet-level IP mapping rules, or by using the Site Recovery Manager Public APIs.

Apply IP Customization Rules to a Virtual Machine

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

For the list of guest operating systems for which Site Recovery Manager supports an IP customization, see the *Compatibility Matrices for Site Recovery Manager 8.8* at https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html.

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.

1. In the vSphere 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, by defining subnet-level IP mapping rules, or by using the Site Recovery Manager Public APIs.

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 Client.

Virtual machines that you configure by using DR IP Customizer are not subject to subnet-level IP customization rules.

You can use the Site Recovery Manager Public APIs to customize the IP properties for multiple virtual machines on the protected and recovery sites. For more information about the Site Recovery Manager Public APIs, see the Site Recovery Manager API Developer's Guide.

Related Links

Manually Customize IP Properties for an Individual Virtual Machine on page 209

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 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 8.8* at https://docs.vmware.com/en/Site-Recovery-Manager/8.8/rn/compatibility-matrices-for-vmware-site-recovery-manager-88/index.html.

Report IP Address Mappings for Recovery Plans

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

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

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 `/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:

     ```
     /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.

     ```
     /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:

```
/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
```

Related Links

Syntax of the DR IP Customizer Tool on page 213
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 on page 215
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 on page 218
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 on page 223
You can use the DR IP Customizer tool to customize the IP properties for multiple virtual machines that Site Recovery Manager protects.

Syntax of the DR IP Customizer Tool

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

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.

The `dr-ip-customizer` is located in the `/opt/vmware/srm/bin/` directory on the appliance.

When you run `dr-ip-customizer`, you specify different options depending on whether you are generating or applying a comma-separated value (CSV) file.

```
dr-ip-customizer
--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 26: 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.
`--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.

Option	Description	Mandatory
`-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:

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml" -i --cmd generate -
o "/home/admin/output.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`

Related Links

Report IP Address Mappings for Recovery Plans on page 212
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.

Structure of the DR IP Customizer CSV File on page 215
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 on page 218
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 on page 223
You can use the DR IP Customizer tool to customize the IP properties for multiple virtual machines that Site Recovery Manager protects.

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 27: 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.
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`.

Column	Description	Customization Rules
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.
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.

Related Links

Report IP Address Mappings for Recovery Plans on page 212
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 on page 213
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.

Modifying the DR IP Customizer CSV File on page 218
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 on page 223
You can use the DR IP Customizer tool to customize the IP properties for multiple virtual machines that Site Recovery Manager protects.

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.

Related Links

Report IP Address Mappings for Recovery Plans on page 212
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 on page 213
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 on page 215
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.

Run DR IP Customizer to Customize IP Properties for Multiple Virtual Machines on page 223
You can use the DR IP Customizer tool to customize the IP properties for multiple virtual machines that Site Recovery Manager protects.

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` 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.

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.

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 28: 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)
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	vcenter-server-site-B	0							example.com
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	vcenter-server-site-B	0							eng.example.com
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	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	
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	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	
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	vcenter-server-site-A	1			192.168.0.21	255.255.255.0	192.168.0.1		
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	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.

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 29: 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)
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	vcenter-server-site-B	0							example.com
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	vcenter-server-site-B	0							eng.example.com
103b9e8b-1f90-faca-8028-13820b8[illegible]		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	
103b9e8b-1f90-faca-8028-13820b8[illegible]		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	
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
103b9e8b-1f90-faca-8028-13820b8[illegible]	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
103b9e8b-1f90-faca-8028-13820b8[illegible]		vcenter-server-site-A	1			dhcp				
103b9e8b-1f90-faca-8028-13820b8[illegible]		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.

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 30: Setting Static and DHCP IPv4 and IPv6 Addresses in a Modified CSV File

VM ID	VM Name	vCente Server	Adapte ID	Primar WINS	Secon WINS	IP Address	Subnet Mask	Gatewa	IPv6 Address	IPv6 Subnet Prefix length	IPv6 Gatewa	DNS Server(s	DNS Suffix(es)
103b9e8b-1f90-faca-8028-138[illegible]	vm-3-win	vcenter-server-site-B	0										example.com
103b9e8b-1f90-faca-8028-138[illegible]	vm-3-win	vcenter-server-site-B	0										eng.example.com
103b9e8b-1f90-faca-8028-138[illegible]	vm-3-win	vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.2[illegible]	255.255.[illegible]	192.168.1.1	dhcp			1.1.1.1	
103b9e8b-1f90-faca-8028-138[illegible]	vm-3-win	vcenter-server-site-B	2	2.2.3.4	2.2.3.5	dhcp			::ffff:192.168.1.22	128	::ffff:192.168.1.1	1.1.1.1	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0										example.com
103b9e8b-1f90-faca-8028-138[illegible]	vm-3-win	vcenter-server-site-A	0										eng.example.com
103b9e8b-1f90-faca-8028-138[illegible]	vm-3-win	vcenter-server-site-A	1			dhcp			::ffff:192.168.0.22	128	::ffff:192.168.0.1	1.1.1.1	192.168.0.250
103b9e8b-1f90-faca-8028-138[illegible]	vm-3-win	vcenter-server-site-A	1									::ffff:192.168.0.251	
103b9e8b-1f90-faca-8028-138[illegible]	vm-3-win	vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.2[illegible]	255.255.[illegible]	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.

- Use the DR IP Customizer tool on a computer with access to vCenter Server instances in your environment.
- When using the Site Recovery Manager Virtual Appliance, you must SSH with the admin user.

  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.

1. Log in to the Site Recovery Manager Server host and open a command shell.
2. Change the working directory to `/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 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. 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, 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. 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`*.

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.

Related Links

Report IP Address Mappings for Recovery Plans on page 212
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 on page 213
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 on page 215
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 on page 218
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.

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.

1. In the vSphere 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

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 and vSphere Replication protection groups.

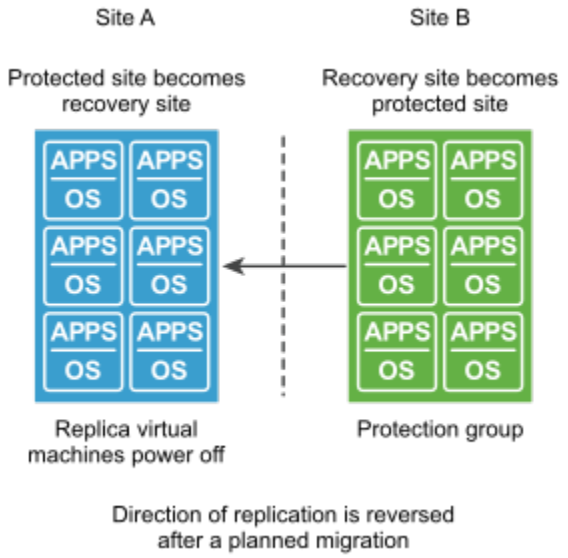
> **NOTE**
> If you change the disk size of a virtual machine replicated with vSphere Replication after it was recovered, and then run reprotect, the reprotect operation will fail.

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 10: 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.

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.

Related Links

How Site Recovery Manager Reprotects Virtual Machines with vSphere Replication on page 228
In the reprotect process using vSphere Replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

Preconditions for Performing Reprotect on page 228
You can perform reprotect only if you meet certain preconditions.

Reprotect Virtual Machines on page 229

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 on page 230
The reprotect process can pass through several states that you can observe in the recovery plan in the Site Recovery user interface.

Using vSphere Replication Optimized Reprotect on page 231
Optimized reprotect reduces the time needed for a reprotect operation.

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.

Related Links

How Site Recovery Manager Reprotects Virtual Machines with Array-Based Replication on page 227
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.

Preconditions for Performing Reprotect on page 228
You can perform reprotect only if you meet certain preconditions.

Reprotect Virtual Machines on page 229
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 on page 230
The reprotect process can pass through several states that you can observe in the recovery plan in the Site Recovery user interface.

Using vSphere Replication Optimized Reprotect on page 231
Optimized reprotect reduces the time needed for a reprotect operation.

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 and vSphere Replication protection groups.

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

1. Run a planned migration and make sure that all steps of the recovery plan finish successfully. If errors occur during the recovery, resolve the problems that caused the errors and rerun the recovery. When you rerun a recovery, operations that succeeded previously are skipped. For example, successfully recovered virtual machines are not recovered again and continue running without interruption.
2. The original protected site must be available. The vCenter Server instances, ESXi Servers, Site Recovery Manager Server instances, 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.

- If the 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.

Related Links

How Site Recovery Manager Reprotects Virtual Machines with Array-Based Replication on page 227
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 on page 228
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.

Reprotect Virtual Machines on page 229
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 on page 230
The reprotect process can pass through several states that you can observe in the recovery plan in the Site Recovery user interface.

Using vSphere Replication Optimized Reprotect on page 231
Optimized reprotect reduces the time needed for a reprotect operation.

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.

See Preconditions for Performing Reprotect.

1. In the vSphere 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.

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.

Related Links

How Site Recovery Manager Reprotects Virtual Machines with Array-Based Replication on page 227
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 on page 228
In the reprotect process using vSphere Replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

Preconditions for Performing Reprotect on page 228
You can perform reprotect only if you meet certain preconditions.

Overview of Reprotect States on page 230
The reprotect process can pass through several states that you can observe in the recovery plan in the Site Recovery user interface.

Using vSphere Replication Optimized Reprotect on page 231
Optimized reprotect reduces the time needed for a reprotect operation.

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 31: Reprotect States

State	Description	Remedial Action
`Reprotect In Progress`	Site Recovery Manager is running reprotect.	None
`Partial Reprotect`	Occurs if multiple recovery plans share the same protection groups and some of the protection groups were successfully reprotected in another plan.	Run reprotect again on the partially reprotected plans.
`Incomplete Reprotect`	Occurs because of failures during reprotect. For example, this state might occur because of a failure to perform 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.

Related Links

How Site Recovery Manager Reprotects Virtual Machines with Array-Based Replication on page 227
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 on page 228
In the reprotect process using vSphere Replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

Preconditions for Performing Reprotect on page 228
You can perform reprotect only if you meet certain preconditions.

Reprotect Virtual Machines on page 229
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.

Using vSphere Replication Optimized Reprotect on page 231
Optimized reprotect reduces the time needed for a reprotect operation.

Using vSphere Replication Optimized Reprotect

Optimized reprotect reduces the time needed for a reprotect operation.

After you perform the recovery and before you power on the new recovered VM, vSphere Replication prepares to track the changes, which occur on the recovered VM. During recovery, vSphere Replication creates a Persistent State File (PSF) for each disk of the recovered VM. The PSF files are used to track the changes on the disks, which helps to omit

the initial sync during reprotect. If you delete the PSF files, the optimization process is interrupted and the reprotect operation switches to full sync operation.

If you are using Thin Provisioning and do not perform reprotect within the configured period (See the *Configuring the Optimized Reprotect* section), vSphere Replication removes the PSF files and any further reprotect operation triggers a full sync operation.

When using a VMware vSAN datastore, once the VM is selected for Site Recovery Manager protection, the PSF files are created per vmdk by vSphere Replication. For VMware vSAN datastores, the PSF file provisioned type depends on the configured VM namespace storage policy. If the namespace storage policy is set to Thick Provisioning, the PSF files are required and cannot be removed.

You cannot use optimized reprotect to initial sync with seed disks.

> **NOTE**
> You can only reprotect to the original protected site. You cannot use optimized reprotect with Disaster Recovery workflow. You can use optimized reprotect only after a planned migration Site Recovery Manager workflow.

Calculating the PSF file size

Below is calculation how the PSF file size is determined based on how much disk is allocated to any VM.

For Thin Provisioning the determing factor is the changed block size and the PSF file size is calculated as 512 bytes file header + 2 x RoundupTo2KB(vmdkSize/extentSize/8) + 512 bytes demandlog header + 512 x [changed block size] / [extent size] + [changed block size].

For Thick Provisioning the determing factor is the vmdk size. The PSF file size is calculated as 512 bytes file header + 2 x RoundupTo2KB(vmdkSize/extentSize/8) + 512 bytes demandlog header + 512 x [vmdk size] / [extent size] + [vmdk size]. By default, for vmdks less than 2TB, the extent size is 8192.

Optimized Reprotect Support

Optimized Reprotect depends on the type of the target datastore and the quiescing option.

Target Datastore	Quiescing	ESXi Version
VMFS	OFF	For all host versions, the reprotect operation is optimized.
VMFS	ON	For ESXi 7.0 and ESXi 7.0 Update 1, if optimized reprotect is enabled, the reprotect operation fails. You must deactivate the optimized reprotect feature to restore the reprotect operation. Set the `reprotect-optimization-enabled` property to false. See Configuring the Optimized Reprotect section below. For all other host versions, the reprotect operation is optimized.
vSAN or Virtual Volumes	OFF or ON	For ESXi 7.02 or later versions, the reprotect operation is optimized. For earlier ESXi versions, you must deactivate the optimized reprotect feature. Set the `reprotect-optimization-enabled` property to false. See Configuring the Optimized Reprotect section below.

Configuring the Optimized Reprotect

Use the VRMS configuration properties in `/opt/vmware/hms/conf/hms-configuration.xml` to modify the behavior of your environment during reprotect.

Table 32: VRMS Configuration Properties for the Optimized Reprotect

Property	Description	Default Value
`reprotect-optimization-enabled`	Activate or deactivate the optimized reprotect option.	`true`
`reprotect-optimization-time-window-mins`	The period for which the replication stays in optimized mode (measured in minutes). When this period is passed, reprotect triggers a full sync.	`10080`
`reprotect-optimization-monitor-period-mins`	The period for which VRMS cleans expired data related to optimized reprotect, when the reprotect optimization time window is expired (measured in minutes).	`60`

Related Links

How Site Recovery Manager Reprotects Virtual Machines with Array-Based Replication on page 227
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 on page 228
In the reprotect process using vSphere Replication, Site Recovery Manager reverses the direction of protection, then forces synchronization of the storage from the new protected site to the new recovery site.

Preconditions for Performing Reprotect on page 228
You can perform reprotect only if you meet certain preconditions.

Reprotect Virtual Machines on page 229
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 on page 230
The reprotect process can pass through several states that you can observe in the recovery plan in the Site Recovery user interface.

Restoring the Pre-Recovery Site Configuration by Performing Failback

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 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.

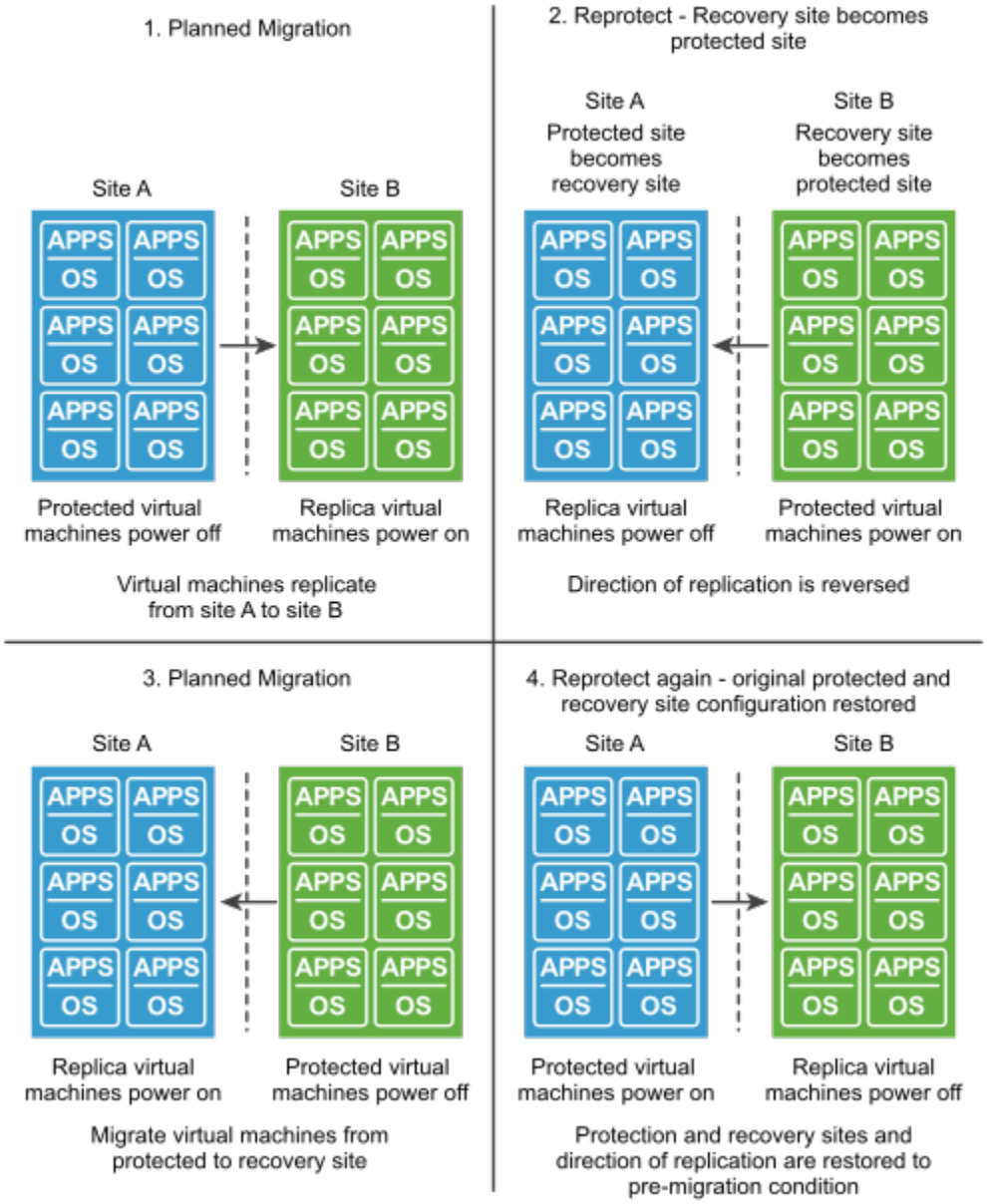
You can configure and run a failback when you are ready to restore services to the original protected site, after you have brought it back online after an incident.

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 11: Site Recovery Manager Failback Process



Perform a Failback

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

- 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.

After a recovery from site A to site B, the recovered virtual machines are running on site B without protection.

1. In the vSphere 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.

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.

Using the Site Recovery Manager REST API Gateway

VMware Site Recovery Manager REST API Gateway provides an API access to the Site Recovery Manager functionality and allows you to programmatically perform various Site Recovery Manager tasks without the use of the Site Recovery user interface.

System Requirements to use the Site Recovery Manager REST API Gateway

To use the public REST APIs you must have an installation of Site Recovery Manager 8.8 or later.

Before you run any REST APIs to or from a target site, verify that you have created a session to the desired vCenter Server instance.

> **NOTE**
> In a federated environment with linked vCenter Server instances, when you log in to the REST API gateway local site this will automatically log you in to the remote site. You do not have to make a `POST /remote-session` request. It is not possible to log in to the remote site with a different user name.

Site Recovery Manager REST API Gateway Documentation

The Site Recovery Manager REST APIs introduce end-to-end automation for Site Recovery Manager.

- Ability to create, remove, and reconfigure site pairs.
- Ability to create, edit, delete Protection Groups and Recovery Plans.
- Get protection and recovery settings for VMs. Protect and remove protection VM operations.
- Create, modify, remove Inventory mappings and IP customization.
- Reconfigure Recovery settings for VMs - Add, Edit, Delete Callouts and Prompts, Set, Get priority and dependencies.
- Full set of APIs to retrieve information about different vCenter Server and Site Recovery Manager objects.
- Operations for working with array managers and array pairs - create, delete, discover devices and so on.
- Recovery plans execution - Test, Planned Migration, Failover, Re-protect, and Failback.
- Full set of APIs to configure and manage VMware Site Recovery Manager appliance. See Using the Site Recovery Manager Configuration REST APIs Gateway.

To access the Site Recovery Manager REST API Gateway documentation and guidelines, see https://developer.broadcom.com/xapis/vmware-site-recovery-manager-rest-api-gateway/latest/.

Download the Open API Specification

You can explore the Site Recovery Manager REST APIs and download the Open API specifications from the REST API Explorer.

1. Navigate to the Site Recovery Manager Appliance home page.
2. Click **Explore REST API**.
3. From the **Select product** drop-down menu, select an API, and click **DOWNLOAD OPEN API SPEC**.

Option	Description
configure	Downloads the Site Recovery Manager Appliance configuration REST APIs.
srm	Downloads the Site Recovery Manager Server REST APIs.

4. Optional: To discover the available REST API versions, make a `GET` request.

```
GET <SRM-APPLIANCE-FQDN>/api/rest/supported-versions
```

5. Optional: To retrieve the Open API specifications, use the following endpoints.

```
GET <SRM-APPLIANCE-FQDN>/api/rest/configure/<VERSION>/open-api.yaml

GET <SRM-APPLIANCE-FQDN>/api/rest/configure/<VERSION>/open-api.json

GET <SRM-APPLIANCE-FQDN>/api/rest/srm/<VERSION>/open-api.yaml

GET <SRM-APPLIANCE-FQDN>/api/rest/srm/<VERSION>/open-api.json
```

List of Site Recovery Manager REST APIs

The following REST APIs are available with Site Recovery Manager 8.8.

Site Recovery Manager Authentication APIs

Table 33: Authentication-related APIs

Category	Operation Type	REST API Name	Description
Authentication	GET	Get Current Session	Returns information about the current session, if any.
Authentication	POST	Login	Logs in and returns the session ID. In the subsequent requests, include the 'x-dr-session' header with the returned session ID value.
Authentication	DELETE	Logout	Logs out if the session is authenticated.

Site Recovery Manager Inventory Mappings REST APIs

Table 34: REST APIs Related to Inventory Mappings Functionality

Category	Operation Type	REST API Name	Description
Inventory Mappings	POST	Create Folder Mapping	Add folder mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	POST	Create Network Mapping	Add network mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	POST	Create Placeholder Datastores	Add placeholder datastores for a Site Recovery Manager in a given pairing.
Inventory Mappings	POST	Create Resource Mapping	Add resource mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	POST	Create Storage Policy Mapping	Add storage policy mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	POST	Create Test Network Mappings	Add test network mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	DELETE	Delete Folder Mapping	Delete a configured folder mapping for a Site Recovery Manager in a given pairing.
Inventory Mappings	DELETE	Delete Network Mapping	Delete a configured network mapping for a Site Recovery Manager in a given pairing.
Inventory Mappings	DELETE	Delete Placeholder Datastores	Delete a configured placeholder datastore for a Site Recovery Manager in a given pairing.

Category	Operation Type	REST API Name	Description
Inventory Mappings	DELETE	Delete Resource Mapping	Delete a configured resource mapping for a Site Recovery Manager in a given pairing
Inventory Mappings	DELETE	Delete Storage Policy Mapping	Delete a configured storage policy mapping for a Site Recovery Manager in a given pairing.
Inventory Mappings	DELETE	Delete Test Network Mappings	Delete a configured test network mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Folder Mapping	Get details about a configured folder mapping for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Folder Mappings	Get currently configured folder mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Network IP Subnet Mapping	Get details about a configured IP subnet mapping for a network mapping.
Inventory Mappings	GET	Get Network Mapping	Get details about a configured network mapping for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Network Mappings	Get currently configured network mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Placeholder Datastore	Get details about a configured placeholder datastore for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Placeholder Datastores	Get currently configured placeholder datastores for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Resource Mapping	Get details about a configured resource mapping for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Resource Mappings	Get currently configured resource mappings for a Site Recovery Manager in a given pairing.

Category	Operation Type	REST API Name	Description
Inventory Mappings	GET	Get Storage Policy Mapping	Get details about a configured storage policy mapping for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Storage Policy Mappings	Get currently configured storage policy mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Test Network Mapping	Get details about a configured test network mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	GET	Get Test Network Mappings	Get currently configured test network mappings for a Site Recovery Manager in a given pairing.
Inventory Mappings	POST	Query Suitable Datastores	Query for suitable datastores to be used as placeholder datastores.
Inventory Mappings	DELETE	Remove Network IP Subnet Mapping	Delete configured IP subnet mapping for a network mapping.
Inventory Mappings	PUT	Update Network IP Subnet Mapping	Create or update IP subnet mapping for a network mapping.

Site Recovery Manager Site Pairing REST APIs

Table 35: Site Pairing REST APIs

Category	Operation Type	REST API Name	Description
Pairing	POST	Create Pairing	Pair to remote Site Recovery Manager server.
Pairing	DELETE	Delete Pairing	Delete existing pairing with remote Site Recovery Manager server.
Pairing	POST	Reconnect Pairing	Reconnect existing pairing to remote Site Recovery Manager server.
Pairing	POST	Create Remote Session	Create session to remote Site Recovery Manager server.
Pairing	GET	Get Pairing	Get information about the pairing.
Pairing	GET	Get Pairing Issues	Get all issues for the pairing.
Pairing	GET	Get Pairings	Get a list of all existing pairings.

Category	Operation Type	REST API Name	Description
Pairing	GET	Get Remote Session	Return information about the current session to the remote Site Recovery Manager server, if any.
Pairing	GET	Get SRM	Get information about a Site Recovery Manager server, which is part of a given pairing.
Pairing	GET	Get SRM Issues	Get a list of all Site Recovery Manager server issues for a given Site Recovery Manager server.
Pairing	GET	Get SRMs	Get a list of all Site Recovery Manager servers in the pairing.

Site Recovery Manager Protection REST APIs

Table 36: REST APIs Related to Protection Management

Category	Operation Type	REST API Name	Description
Protection	GET	Get SRM Protection Inventory	Get information about Site Recovery Manager server protection inventory.
Protection	POST	Create Protection Group Folder	Create Site Recovery Manager protection group folder.
Protection	GET	Get Protection Group Folder Information	Get information about Site Recovery Manager protection group folder.
Protection	DELETE	Delete Protection Group Folder	Remove Site Recovery Manager protection group folder.
Protection	POST	Move Protection Group Folder	Move Site Recovery Manager protection group folder.
Protection	POST	Rename Protection Group Folder	Rename Site Recovery Manager protection group folder.
Protection	GET	Get SRM Protection Group Folder Children	Get information about Site Recovery Manager protection group folder children.
Protection	POST	Add Datastore Group	Add a replicated datastore group to a protection group in a given pairing.
Protection	POST	Configure All	Configure protection for all virtual machines, which are part of the protection group in a given pairing.

Category	Operation Type	REST API Name	Description
Protection	POST	Create Group	Create a new protection group in a given pairing.
Protection	DELETE	Delete Group	Delete a protection group in a given pairing.
Protection	GET	Get All Groups	Get information about all protection groups in a given pairing.
Protection	GET	Get Datastore Group	Get details about a replicated datastore group for a protection group in a given pairing.
Protection	GET	Get Datastore Groups	Get a list of replicated datastore groups for a protection group in a given pairing.
Protection	GET	Get Group	Get information about a protection group in a given pairing.
Protection	GET	Get Group Issues	Get issues about a protection group in a given pairing.
Protection	GET	Get Group Related Recovery Plans	Get recovery plans of which the protection group is part of.
Protection	GET	Get Group VM	Get details about a protected virtual machine that is part of a protection group in a given pairing.
Protection	GET	Get Group VMS	Get a list of virtual machines that are part of a protection group in a given pairing.
Protection	GET	Get VM Protection Settings	Get details about the current protection settings of a virtual machine.
Protection	GET	Get vVol Replication Group	Get information about the source Virtual Volumes replication group for a protection group in a given pairing.
Protection	GET	Get vVol Replication Groups	Get the source Virtual Volumes replication groups for a protection group in a given pairing.
Protection	POST	Reconfigure Group	Reconfigure settings for a protection group in a given pairing.
Protection	DELETE	Remove Datastore Group	Remove a replicated datastore group from a protection group in a given pairing.

Category	Operation Type	REST API Name	Description
Protection	POST	Remove VM From Protection Group	Remove a virtual machine from a vSphere Replication protection group in a given pairing.
Protection	POST	Remove VM Protection	Remove the protection of a virtual machine within a protection group in a given pairing.
Protection	POST	Restore All Placeholders	Repair all placeholder virtual machines that are part of the protection group in a given pairing.
Protection	PUT	Update VM Protection Settings	Update the protection settings of a virtual machine.

Site Recovery Manager Recovery REST APIs

Table 37: REST APIs Related to Recovery Management

Category	Operation Type	REST API Name	Description
Recovery	POST	Cancel Recovery Plan	Cancel a running recovery task.
Recovery	POST	Create Plan	Create a new recovery plan in a given pairing.
Recovery	DELETE	Delete recovery Plan	Delete a recovery plan from a given pairing.
Recovery	GET	Get All Plan History Records	Get a list of all history reports for recovery runs in a given timeframe in a given pairing.
Recovery	GET	Get All Recovery Plans	Get a list of all recovery plans in a given pairing.
Recovery	GET	Get Plan History Record	Get information about the history report for a recovery run of a recovery plan in a given pairing.
Recovery	GET	Get Plan History Records	Get a list of all history reports for recovery runs in a given timeframe of a recovery plan in a given pairing.
Recovery	GET	Get Plan Related Protection Groups	Get protection groups that are part of a recovery plan in a given pairing.
Recovery	GET	Get Plan Related Test Networks	Get the test networks configured for a recovery plan in a given pairing.

Category	Operation Type	REST API Name	Description
Recovery	GET	Get Plan Virtual Machine	Get the protected virtual machine included in a recovery plan in a given pairing.
Recovery	GET	Get Plan Virtual Machine Dependent VMS	Get the dependent VMs for a protected virtual machine.
Recovery	GET	Get Plan Virtual Machine IP Customization	Get the IP customization for a protected virtual machine.
Recovery	GET	Get Plan Virtual Machine Recovery Priority	Get the protected virtual machine priority during a recovery.
Recovery	GET	Get Plan Virtual Machine Recovery Settings	Get recovery settings for a protected virtual machine.
Recovery	GET	Get Plan Virtual Machine Summarized Recovery Settings	Get a summary of the recovery settings for a protected virtual machine.
Recovery	GET	Get Plan Virtual Machines	Get virtual machines that are part of a recovery plan in a given pairing.
Recovery	GET	Get Recovery Plan	Get information about a recovery plan in a given pairing.
Recovery	GET	Get Recovery Plan Issues	Get issues about a recovery plan in a given pairing.
Recovery	POST	Plan Virtual Machine Check Dependent VMS	Check if a given list of dependent VMs is valid against the current VM.
Recovery	POST	Reconfigure Recovery Plan	Reconfigure settings for a recovery in a given pairing.
Recovery	POST	Run Cleanup Test Recovery	Run a cleanup after a test recovery for a recovery plan in a given pairing.
Recovery	POST	Run Recovey	Run the recovery for a recovery plan in a given pairing.
Recovery	POST	Run Reprotect	Run the reprotect operation after a successful recovery for a recovery plan in a given pairing.
Recovery	POST	Run Test Recovery	Run a test recovery for a recovery plan in a given pairing.
Recovery	POST	Update Plan Virtual Machine Dependent VMS	Update the dependent VMs of a protected virtual machine.
Recovery	POST	Update Plan Virtual Machine IP Customization	Update the IP customization for a protected virtual machine.
Recovery	PUT	Update Plan Virtual Machine Recovery Priority	Update the recovery priority of a protected virtual machine.

Category	Operation Type	REST API Name	Description
Recovery	POST	Update Plan Virtual Machine Recovery Settings	Update recovery settings for a protected virtual machine.
Recovery	GET	Get SRM Recovery Inventory	Get information about Site Recovery Manager server recovery inventory.
Recovery	GET	Get SRM Recovery Plan Folder Information	Get information about Site Recovery Manager recovery plan folder.
Recovery	DELETE	Delete Recovery Plan Folder	Delete Site Recovery Manager recovery plan folder.
Recovery	POST	Move Recovery Plan Folder	Move Site Recovery Manager recovery plan folder.
Recovery	POST	Rename Recovery Plan Folder	Rename Site Recovery Manager recovery plan folder.
Recovery	POST	Create Recovery Plan Folder	Create Site Recovery Manager recovery plan folder.
Recovery	GET	Get SRM Recovery Folder Children	Get information about Site Recovery Manager recovery plan folder children.
Recovery	GET	Get All User Prompts	Get a list of all user prompts currently waiting for an acknowledgment.
Recovery	GET	Get User Prompt Details	Get information about a given user prompt currently waiting for an acknowledgment.
Recovery	POST	Dismiss Prompt	Dismiss a given user prompt waiting for a client acknowledgment during a recovery operation.
Recovery	GET	Get All Recovery Steps	Get information about recovery steps in a given recovery view mode.
Recovery	POST	Create Recovery Step Callout/ Prompt	Add a callout/prompt to the list of recovery steps in a given recovery view mode.
Recovery	GET	Get Recovery Step Details	Get information about a recovery step in a given recovery view mode.
Recovery	DELETE	Delete Recovery Step Callout/ Prompt	Delete a recovery step callout/ prompt in a given recovery view mode.
Recovery	GET	Get Recovery Step Callout Details	Get data about a callout/prompt related to a given recovery step in a given recovery view mode.

Category	Operation Type	REST API Name	Description
Recovery	POST	Edit Recovery Step Callout/ Prompt	Modify a callout/prompt to the list of recovery steps in a given recovery view mode.

Site Recovery Manager Replication REST APIs

Table 38: REST APIs Related to Replication Management

Category	Operation Type	REST API Name	Description
Replication	GET	Get All vVol Fault Domain Replication Groups	Get information about all replication groups that are part of a VMware vSphere Virtual Volumes fault domain.
Replication	GET	Get All vVol Fault Domains	Get information about all VMware vSphere Virtual Volumes fault domains that are part of a given pairing.
Replication	GET	Get Replicated Array Pair	Get information about a replicated array pair that is part of a given pairing.
Replication	GET	Get Replicated Array Pairs	Get information about replicated array pairs that are part of a given pairing.
Replication	GET	Get vVol Fault Domain	Get details about a VMware vSphere Virtual Volumes fault domain that is part of a given pairing.
Replication	GET	Get vVol Fault Domain Replication Group	Get information about a replication group that is part of a VMware vSphere Virtual Volumes fault domain.
Replication	POST	Retrieve Unassigned Datastore Groups	Retrieve the unassigned datastore groups that are part of a replicated array pair. These datastore groups could be included in the Array-Based Replication protection groups.
Replication	GET	Get Array Managers	Get information about all Site Recovery Manager array managers.
Replication	POST	Create Array Managers	Create a Site Recovery Manager array manager.
Replication	GET	Get Array Manager	Get information about a Site Recovery Manager array manager.

Category	Operation Type	REST API Name	Description
Replication	DELETE	Delete Array Manager	Delete a Site Recovery Manager array manager.
Replication	POST	Discover Replicated Array Pairs	Discover storage arrays configured for replication by executing SRA command `discoverArrays`.
Replication	POST	Create Replicated Array Pair	Create a Site Recovery Manager replicated array pair.
Replication	DELETE	Delete Replicated Array Pair	Delete a Site Recovery Manager replicated array pair.
Replication	POST	Discover Replicated Array Pair Storage Devices	Discover storage devices and consistency groups of a Site Recovery Manager replicated array pair.
Replication	GET	Get Replicated Array Pair Storage Devices	Get information about all storage devices of a Site Recovery Manager replicated array pair.
Replication	GET	Get Storage Adapters	Get information about all storage replication adapters of a Site Recovery Manager.
Replication	GET	Get Storage Adapter	Get information about a storage replication adapter of a Site Recovery Manager.
Replication	GET	Get Storage Adapters Connection Params	Get connection parameters for a storage replication adapter of a Site Recovery Manager.

Site Recovery Manager Server REST APIs

Table 39: REST APIs Related to Local Server Functionality

Category	Operation Type	REST API Name	Description
Server	GET	Get Info	Information about the current Site Recovery Manager server.

Site Recovery Manager Tasks REST APIs

Table 40: Rest APIs Related to Task Management

Tasks	GET	Get Recent Tasks Info	Retrieve all the recent tasks.
Tasks	GET	Get Task Info	Retrieve the task information.

Site Recovery Manager vCenter Related REST APIs

Table 41: REST APIs Related to vCenter Server Functionality

Category	Operation Type	REST API Name	Description
vCenter	GET	Get Replicated VMS	Get a list of VMs replicated by vSphere Replication in a given vCenter Server.
vCenter	GET	Get VC Storage Policies	Retrieve the storage policies of the vCenter Server.
vCenter	GET	Get VC Storage Policy	Get information about the storage policy objects of the vCenter Server.
vCenter	GET	Get vCenter	Get information about a vCenter Server that is part of a given pairing.
vCenter	GET	Get vCenters	Get a list of all vCenter Server instances in the pairing.
vCenter	GET	Get vCenter Compute Inventory	Get information about the compute inventory of the vCenter Server.
vCenter	GET	Get vCenter Compute Item	Get information about the compute object of the vCenter Server.
vCenter	GET	Get vCenter Datastore Item	Get information about the datastore object of the vCenter Server.
vCenter	GET	Get vCenter Datastores	Get information about the datastores of the vCenter Server.
vCenter	GET	Get vCenter Network Inventory	Get information about the network inventory of the vCenter Server.
vCenter	GET	Get vCenter Network Item	Get information about the network object of the vCenter Server.
vCenter	GET	Get vCenter VM Folder	Get information about the VM folder object of the vCenter Server.

Category	Operation Type	REST API Name	Description
vCenter	GET	Get vCenter VM Folder Inventory	Get information about the VM folder inventory of the vCenter Server.
vCenter	GET	Browse vCenter Compute Resource	Browse files and folders accessible to vCenter Server's compute object.

How to use the REST APIs to run a recovery plan

You can use the Site Recovery Manager REST APIs to run a recovery plan.

1. Make a `POST` request to login to the primary site.

   ```
   POST BASE_URL/api/rest/srm/API_VERSION/session
   ```

2. Make a `GET` request to get the pairing ID and the local vCenter ServerID.

   ```
   GET BASE_URL/api/rest/srm/v1/pairings/
   ```

   Example response:

   ```
   [
      {
         "pairing_id": "7ae3c72d-9fd6-3157-bec5-07c2982bd1e8",
         "local_vc_server": { "id": "0a98c22d-a553-47e4-bd56-2844f45d8ef6",
         "url": "https://s2-srm2-219-12.eng.vmware.com:443/sdk",
         "name": "s2-srm2-219-12.eng.vmware.com",
         "server_status": "OK",
      },
      ...
   ]
   ```

   Save the pairing ID and the local vCenter Server ID.

3. Make a `GET` request to get a list of all existing recovery plans.

   ```
   GET BASE_URL/api/rest/srm/v1/pairings/PAIRING_ID/recovery-management/plans
   ```

   Replace *PAIRING_ID* with the value recorded in Step 1.

   Example response:

   ```
   [
       {
           "id": "DrRecoveryRecoveryPlan:08ba3a70-5770-4089-a395-f11226e6fe21:93eb1820-f2fd-4238-b8f-
   b-418cd96c1146",
           "status": "TEST_COMPLETE",
           "protected_site_name": "primary-vc",
           "recovery_site_name": "secondary-vc",
           "protected_vc_guid": "0a98c22d-a553-47e4-bd56-2844f45d8ef6",
           "recovery_vc_guid": "71541212-0cb3-409f-9974-1733cd53d993",
           "name": "rp2",
           "description": null,
           "location": "DrFolder:DrRecoveryRootFolder:93eb1820-f2fd-4238-b8fb-418cd96c1146",
           "location_name": "Recovery Plans",
           "progress": 0,
           "is_running": false
   ```

```
        },
        {...},
        {...},
        {...},
    ]
```

Save the Recovery Plan ID.

4. Log in to the remote site by making a `POST` request.

   ```
   POST BASE_URL/api/rest/srm/v1/pairings/PAIRING_ID/remote-session
   ```

   Replace *`PAIRING_ID`* with the value recorded in Step 1.

   Enter the user name and password for the remote Platform Services Controller in the Authentication header.

5. Make a `POST` request to run the recovery plan.

   ```
   POST BASE_URL/api/rest/srm/v1/pairings/PAIRING_ID/recovery-management/plans/RECOVERY_PLAN_ID/actions/re-
   covery
   ```

   Replace *`PAIRING_ID`* with the value recorded in Step 1, and *`RECOVERY_PLAN_ID`* with the value recoded in Step 2.

   Example response:

   ```
   {
       "skip_protection_site_operations": "false",
       "migrate_eligible_vms": "false",
       "sync_data": "true",
       "planned_failover": "true"
   }
   ```

DR REST API Rate Limiter

The DR REST API Rate Limiter is a mechanism to manage the risks of API resource exhaustion and brute force attacks.

The rate limiter is available in the DR REST API of Site Recovery Manager 8.8 and later and vSphere Replication 8.8 and later. The DR REST API Rate Limiter is a trade off between security and performance.

Table 42: DR REST API Request Rate Limit Tiers

Tier	Description	Configuration	Default Value
`IP address`	Considers requests per IP address.	*`ipRateLimitQuota`*	100
		`ipRateLimitWindow`	60 000 in ms (1 min)
`Service`	Considers requests per DR REST API service name. In DR REST API there are three service names: *`srm`*, *`vr`*, and *`configure`*. The 'srm v1' and 'srm v2' have the same service name of 'srm'.	*`serviceRateLimitQuota`*	1000
		`serviceRateLimitWindow`	60 000 in ms (1 min)
`Session`	Considers requests per session.	*`sessionRateLimitQuota`*	50
		`sessionRateLimitWindow`	60000 in ms (1 min)

Tier	Description	Configuration	Default Value
n/a	Periodic clean of obsolete request rate limiter data structures to reduce the runtime memory fingerprint. Value of 0 (zero) means no cleanup is performed at all.	*rateLimitLogPurgeInterval*	7 200 000 in ms (2h)

DR REST API Rate Limiter consists of three tiers which work in a chain to rate limit the incoming requests against the tier's criteria. In case the tier's criteria is met a request response is returned immediately thus skipping the rest of the tier chain. DR REST API Rate Limiter tier chain is IP address, Service, Session in that particular order.

You change the DR REST API Rate Limiter configuration by adding or updating the values of the specified properties in the `dr-rest-api.properties` file. The file is located in the `/opt/vmware/dr-rest/lib/` folder. If a Rate Limiter property is not explicitly defined in the DR REST API `dr-rest-api.properties` configuration file, the Rate Limiter uses the default value. To predefine a configuration value, add the corresponding configuration if missing, and set the required value. The updated values become effective when a new rate limit window begins.

Example of `dr-rest-api.properties` file

```
...
ipRateLimitQuota=100
ipRateLimitWindow=60000
serviceRateLimitQuota=1000
serviceRateLimitWindow=60000
sessionRateLimitQuota=50
sessionRateLimitWindow=60000
rateLimitLogPurgeInterval=0
...
```

HTTP Response

Every DR REST API request response has the following headers.

- *RateLimit-Limit* - the server's quota for requests by the client in the time window.
- *RateLimit-Remaining* - the remaining quota in the current window.
- *RateLimit-Reset* - the time remaining in the current window, specified in milliseconds.

> **ATTENTION**
> When an HTTP request is rate limited, the response error code is `429 Too Many Requests` and header RateLimit-Remaining is 0 (zero). DR REST API responses contain Rate Limit headers from the last rate limit tier which processed the client request.

Best practices for setting the optimal Rate Limit configuration

Setting up the optimal Rate Limit configuration requires taking into consideration various factors.

- Begin with the default values of the Rate Limiter configurations.
  - *ipRateLimitQuota*, *ipRateLimitWindow*, *serviceRateLimitQuota*, *serviceRateLimitWindow*, *sessionRateLimitQuota*, *sessionRateLimitWindow*
  - *rateLimitLogPurgeInterval*
- Listen for request responses with error code `429 Too Many Requests` and take actions accordingly.
  - Wait for the next rate limit window and repeat the requests which were rate limited.
  - Decrease the request intensity at the client side.
  - Update the Rate Limit configurations - increase the related configuration *RateLimitQuota* and or decrease the related configuration *RateLimitWindow*.
- Analyze the response headers *RateLimit-Limit*, *RateLimit-Remaining*, and *RateLimit-Reset* and takes actions accordingly.
  - Change the request intensity at the client side in the required direction.
  - Update the Rate Limit configurations in the required direction.

Interoperability of Site Recovery Manager with Other Software

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*.

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.

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 and vSAN Express Storage. You cannot use vSAN storage with array-based replication.

For information about the compatible versions of vSphere Replication and vSAN, see *VMware Product Interoperability Matrix* at https://interopmatrix.vmware.com/Interoperability.

For information about using vSphere Replication with vSAN, see *Using vSphere Replication with VMware vSAN Storage* in *vSphere Replication Administration*.

Site Recovery Manager and VMware Cloud Disaster Recovery High-Frequency Snapshots

You can use Site Recovery Manager protection and VMware Cloud Disaster Recovery high-frequency snapshots on the same virtual machine, with certain limitations.

Interoperability of the same VM is enabled in VMware Live Recovery. For more information, see *Protect the Same VM with Both VMware Live Site Recovery and VMware Live Cyber Recovery* and *VMware Live Site Recovery and VMware Live Cyber Recovery*.

You can replicate a VMware Cloud Disaster Recovery high-frequency snapshot protected virtual machine with vSphere Replication but you cannot protect the virtual machine in a vSphere Replication protection group in Site Recovery Manager. For example, if you want to migrate a VMware Cloud Disaster Recovery protected virtual machine to a new vCenter Server by using vSphere Replication.

If you have a virtual machine that is already replicated by vSphere Replication and added in a Site Recovery Manager protection group, you cannot protect this VM with VMware Cloud Disaster Recovery.

You cannot perform a parallel failover of the same VM with VMware Cloud Disaster Recovery and Site Recovery Manager.

You cannot include a VMware Cloud Disaster Recovery high-frequency snapshot protected virtual machine in an array-based replication protection group or a Virtual Volumes protection group.

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 deactivates 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 deactivates 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.

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 array-based replication protection groups.

- 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. For array-based replication protection groups, restore the placeholder virtual machines for the VMs for which vMotion failed and then 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 deactivated for the cluster
- If the virtual machine has snapshots
- If the virtual machine is a linked clone
- If the virtual machine is attached to RDM devices

Cross vCenter Server vMotion requirements in vSphere are discussed in the *ESXi and vCenter Server 8.0* 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.

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

- 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://developer.vmware.com/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 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 vSphere Replication and encrypted virtual machines, see *Replicating Encrypted Virtual Machines* in the *vSphere Replication Administration* documentation.

vSphere Native Key Provider

VMware vSphere® Native Key Provider™ enables encryption-related functionality without requiring an external key server (KMS). Initially, vCenter Server is not configured with a vSphere Native Key Provider. You must manually configure a vSphere Native Key Provider. See *Configuring and Managing vSphere Native Key Provider* in the *VMware vSphere Product Documentation*.

Requirements for using vSphere Native Key Provider for encrypting virtual machines and virtual disks:

- You need vSphere 7.0 Update 3 or later.
- You must purchase the vSphere Enterprise+ edition.

You must configure a vSphere Native Key Provider on both the local and remote sites. The vSphere Native Key Provider ID of the encrypted VM on the local site must match the vSphere Native Key Provider ID on the remote site.

To use encryption with a vSphere Native Key Provider for replicated virtual machines, the replica disks must be located on datastores, which are accessible through at least one host, which is a part of a vCenter cluster.

For more information, see *Configuring and Managing vSphere Native Key Provider* in the VMware vSphere 7.0 Product 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.

Site Recovery Manager and VMware Aria Automation Orchestrator

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

The VMware Aria Automation Orchestrator plug-in for VMware Site Recovery Manager includes actions and workflows that run Site Recovery Manager operations. If you are a VMware Aria Automation 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 VMware Aria Automation Orchestrator workflows, you can combine Site Recovery Manager operations with the automated operations that other VMware Aria Automation Orchestrator plug-ins provide.

For example, you can create a workflow that uses the actions and workflows of the VMware Aria Automation 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 VMware Aria Automation Orchestrator workflow thus allows you to automate the process of creating and protecting virtual machines.

You can use the VMware Aria Automation Orchestrator plug-in for VMware 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 VMware Aria Automation Orchestrator plug-in for VMware 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 VMware Aria Automation Orchestrator, see the VMware Aria Automation Orchestrator documentation.

VMware Site Recovery Manager and VMware Aria Operations

The VMware Aria Operations Management Pack for Site Recovery Manager allows VMware administrators to monitor the local Site Recovery Manager services in VMware Aria Operations.

The VMware Aria 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 VMware Aria 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).

Site Recovery Manager alerts tracked with the VMware Aria Operations Management Pack

You can track the following alerts with the VMware Aria Operations management pack for Site Recovery Manager.

- Site Recovery Manager server is not paired.
- Site Recovery Manager server is not connected to the paired site.
- Recovery plan is currently running.
- Recovery plan is in canceling state.
- Recovery plan is prompting the user.
- Recovery plan needs cleanup.
- Recovery plan needs failover.
- Recovery plan needs reprotect.
- Recovery plan has errors.
- Recovery plan run finished with VMs with errors.
- Recovery plan run finished with VMs that are powered off.
- Protection group is not configured.
- Protection group is partially recovered.
- Protection group is recovering.
- Protection group is testing.
- These VM(s) are part of one or more protection group(s), but they are not included in any recovery plan(s).
- There are VM(s) that are part of one or more protection group(s), but they are not included in any recovery plan(s).
- Protected VM has errorsLicense expires in less than three days.
- Placeholder VM Needs Repair.
- Protected VM Placeholder Error.
- Replicated Array Pairs Have Errors.
- Array Manager Ping Failed.

Site Recovery Manager Metrics Tracked with the VMware Aria Operations Management Pack

Site Recovery Manager Site Metrics

1. Paired
2. Pair Name
3. Pair VC Address
4. Is Pair Site Connected
5. Name
6. Number of Protection Groups
7. Number of Recovery Plans
8. Number of Recovery Virtual Machines
9. Number of Array Managers
10. Number of Recovery Virtual Machines
11. These VM(s) are part of one or more protection group(s), but they are not included in any recovery plan(s).
12. Product Name
13. Edition Key
14. Total capacity of the license
15. Units currently used in this asset
16. Cost Unit
17. Days to expire
18. Product Version
19. Version
20. Build number

Protection Groups Metrics

1. Protection Group Name
2. Protection Group Status
3. Protection Group Type
4. Protection Group Folder
5. Number of Protected Virtual Machines
6. Part of Recovery Plan

Recovery Plans Metrics

1. Recovery Plan Name
2. Recovery Plan Status
3. Recovery Plan Folder

Recovery History Metrics

1. Description
2. Error Count
3. Execution Time
4. Result State
5. Mode
6. Total Paused Time
7. Warning Count

8. Powered On VMs
9. Powered Off VMs
10. Successfully IP customized VMs
11. Successfully recovered VMs
12. VMs recovered with error
13. Latest from this type run

Protection Group Folders Metrics

1. Folder Name

Recovery Plan Folders Metrics

1. Folder Name

Recovery Virtual Machines Metrics

1. Name
2. Recovery Status

Protected Virtual Machines Metrics

1. Name
2. Recovery Status
3. Errors
4. Placeholder VM Error
5. Placeholder VM Needs Repair

Array Manager Metrics

1. Name
2. Replicated Array Pairs Errors
3. Array Manager Ping Message

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 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 deactivate 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 deactivate 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 deactivate 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 deactivates 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 deactivate 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 deactivate Admission Control during recovery, you must manually reactivate Admission Control after you perform cleanup following a test recovery. Deactivating Admission Control might affect the ability of High Availability to restart virtual machines on the recovery site. Do not deactivate 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.

- 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.
- Cross vCenter Server vMotion is not supported for virtual machines attached to RDM devices.

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

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.

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.

Change Connections Settings

Site Recovery Manager communicates with other services.

1. In the vSphere 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.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 **connections.drPingFailedDelay** text box.
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.

Option	Action
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**.
6. You must restart the Site Recovery Manager server for the settings to take effect.

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.

- 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.

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.

1. In the vSphere 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.

1. In the vSphere 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.
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.

1. In the vSphere 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**.
Set logging level for recovery configuration operations. The default is verbose.	Select a logging level from the **logManager.RecoveryConfig** drop-down menu.

Option	Description
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.

1. In the vSphere 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
Activate or deactivate 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 8.8*.**	Select the value of **recovery.autoDeployGuestAlias** to activate or deactivate 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 service account on the recovery site to a guest user account on the protected VM. The local service account is *SRM-<srm-server-uuid>*. 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 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.

Option	Action
Change the default base directory in which Site Recovery Manager creates a temporary subdirectory when customizing Linux VMs	Enter a new value in the **recovery.defaultLinuxCustomizationBaseDir** text box. An empty value indicates to use the default temporary directory per target guest OS VMware Tools configuration. If the value is not empty, ensure that the guest OS user on whose behalf Site Recovery Manager runs in-guest operations has read, write, and execute permission on the preexisting target base directory.
Change the default priority for recovering a virtual machine. The default value is 3.	Enter a new value in the **recovery.defaultPriority** text box.
Activate or deactivate 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.
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.
Activate or deactivate 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.

Option	Action
	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.
Activate or deactivate 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**.

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.

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**.

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.

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.

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.

1. In the vSphere 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.
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	Enter a new value in the **remoteManager.taskProgressDefaultTimeout** text box.

Option	Action
update is received within that time, the task is allowed more time to complete. The default value is 180 seconds.	
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 Replication Settings

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

1. In the vSphere 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
Set the time interval in minutes between two executions of the cleanup task for archived recovery settings. The default value is 1440 minutes.	Enter a new value in the **replication.archiveRecoverySettingsCleanupInterval** text box.
Set the time duration in days to keep the archived recovery settings. The default value is 30 days.	Enter a new value in the **replication.archiveRecoverySettingsLifetime** text box.
Exclude CD/DVD and floppy media devices from protection. The default value is true.	To deactivate the setting, move the slider to change the value of **replication.autoExcludeMediaDevices** to false.
Automatically try to select placeholder datastores. The default value is true.	To deactivate the setting, move the slider to change the value of **replication.automaticPlaceholderDatastoreSelection** to false.
Set the minimum amount of free disk space available in megabytes for an automatic placeholder datastore selection. The default value is 50 MB.	To change the amount of free disk space, enter a new value in the **replication.automaticPlaceholderDatastoreSelectionMinFreeSpace** text box.
Use minimum CPUs and memory resources when creating a placeholder virtual machine. The default value is false.	Move the slider to change the value **replication.createPlaceholderVmWithMinResources** to true.
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** to true.
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.
Keep individual VM inventory mappings in case of a site-wide inventory mappings change. If the value is set to false, in case of a site-wide inventory mappings change	Move the slider to change the value of **replication.keepOverridesOnInvMappingChange** to true.

Option	Action
Site Recovery Manager overrides the original individual VM inventory mappings. If the value is set to true, Site Recovery Manager keeps the original individual VM inventory mappings until explicit change or VM protection recreation. The default value is false.	
Keep individual VM inventory mappings in case of production VM relocation. You can configure individual inventory mappings on virtual machines through Configure Protection. If the value is set to false, in case of a production VM relocation Site Recovery Manager always updates the VM protection uppon inventory mappings for the new production VM location. If the value is set to true, Site Recovery Manager keeps the original individual VM inventory mappings until explicit change or VM protection recreation. The default value is false.	Move the slider to change the value of **replication.keepOverridesOnVmPlacementChange** to true.
Activate or deactivate 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 of **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.
Update VM protection in case of inventory mappings change. The default value is true.	Move the slider to change the value of **replication.updateVmProtectionOnInvMappingChange** to false.
Update VM protection in case of production VM relocation by applying the inventory mappings on the new production VM location. The default value is true.	Move the slider to change the value of **replication.updateVmProtectionOnPlacementChange** to false.

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.

1. In the vSphere 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).

1. In the vSphere 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.
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.

Option	Action
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 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.

1. In the vSphere 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 deactivate, `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.

Option	Action
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.
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.
Set 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.
Set 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.

1. In the vSphere 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

Option	Description
	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.

1. In the vSphere 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
Activate or deactivate the automatic protection for array-based replication protection groups. The setting must be configured independently for the protection site and the recovery site. The default value is true.	Move the slider to change the value of **autoprotect.abrEnabled**.
Activate or deactivate the automatic protection removal for array-based replication protection groups. The setting must be configured independently for the protection site and the recovery site. The default value is false.	Move the slider to change the value of **autoprotect.abrUnprotectEnabled**.
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.
Activate or deactivate the automatic protection for Virtual Volumes protection groups. The setting must be configured	Move the slider to change the value of **autoprotect.vvolEnabled**.

Option	Action
independently for the protection site and the recovery site. The default value is true.	
Activate or deactivate the automatic protection removal for Virtual Volumes protection groups. The setting must be configured independently for the protection site and the recovery site. The default value is false.	Move the slider to change the value of **autoprotect.vvolUnprotectEnabled**.

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.

1. In the vSphere 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.

1. In the vSphere 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.

Change the Lifetime of Remote Site Authentication Requests

You can modify the lifetime of the OAuth 2.0 remote site authentication requests setting for Site Recovery Manager.

1. In the vSphere 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** > **OAuth 2.0**.
4. To change the **oauth2.authRequestLifetime** setting, select a site, click **Edit**, and specify the number of seconds. The default value is 60 seconds.

Modify Settings to Run Large Site Recovery Manager Environments

If you use Site Recovery Manager to test or recover a large number of virtual machines, you might need to modify the default Site Recovery Manager settings to achieve the best possible recovery times in your environment or to avoid timeouts.

In large environments, Site Recovery Manager might simultaneously power on or power off large numbers of virtual machines. Simultaneously powering on or powering off large numbers of virtual machines can create a heavy load on the virtual infrastructure, which might lead to timeouts. You can modify certain Site Recovery Manager settings to avoid timeouts, either by limiting the number of power on or power off operations that Site Recovery Manager performs concurrently, or by increasing the timeout periods.

The limits that you set on power on or power off operations depend on how many concurrent power on or power off operations your infrastructure can handle.

You modify certain options in the **Advanced Settings** menus in the vSphere Client or in the Site Recovery Manager client plug-in. To modify other settings, you edit the `vmware-dr.xml` configuration file on the Site Recovery Manager Server 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.

1. In the vSphere Client, select a cluster.
2. On the **Configure** 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.
   The `vmware-dr.xml` file is located in the `/opt/vmware/srm/conf/` directory.
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, 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 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 43: Settings that Modify the Number of Simultaneous Power On or Power Off Operations

Option	Description
srmMaxBootShutdownOps	Specifies the maximum number of concurrent power-on operations for any given cluster. Guest shutdowns, but not forced power offs, are throttled according to this value. Guest shutdowns occur during primary site shutdowns (planned failover) and IP customization workflows. Modify this option per cluster in the vSphere Client by right-clicking a cluster and selecting **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 Client. By default, throttling is turned off.
defaultMaxBootAndShutdownOpsPerCluster	Specifies the maximum number of concurrent power-on operations for all clusters that Site Recovery Manager protects. Guest shutdowns, but not forced power offs, are throttled according to this value. Guest shutdowns occur during primary site shutdowns (planned failover) and IP customization workflows. You modify this setting in the `vmware-dr.xml` file. The **srmMaxBootShutdownOps** value that you can set in the vSphere Client overrides the **defaultMaxBootAndShutdownOpsPerCluster** value. You can set a global value **defaultMaxBootAndShutdownOpsPerCluster** in the `vmware-dr.xml` file, and then set different **srmMaxBootShutdownOps** values for individual clusters in the vSphere Client. By default, throttling is turned off.
defaultMaxBootAndShutdownOpsPerHost	Specifies the maximum number of concurrent power-on operations on any standalone host. You can only set the option in the `vmware-dr.xml` file. By default, throttling is turned off.

Table 44: 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.

Option	Description
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

Site Recovery Manager supports event logging. Each event includes a corresponding alarm that Site Recovery Manager can trigger if the event occurs. This provides a way to track the health of your system and to resolve potential issues before they affect the protection that Site Recovery Manager provides.

How Site Recovery Manager Monitors Connections Between Sites

Site Recovery Manager monitors the connection between the protected and recovery sites and logs events if the remote site stops responding.

When Site Recovery Manager establishes the connection between two paired Site Recovery Manager Server instances, the Site Recovery Manager Server that initiated the connection sends a `RemoteSiteUpEvent` 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.

For alarms to send email notifications, configure the **Mail** settings in the **vCenter Server Settings** menu. See *ESXi and vCenter Server Documentation*.

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.

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 45: 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

Event Name	Event Type	Event Description	Category
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
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 46: 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

Event	Description	Cause	Category
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
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 47: 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
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

Event Name	Event Type	Event Description	Category
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 48:

Event	Description	Cause	Category
AutomaticProtectionOffEvent	Event to indicate that Automatic Protection is deactivated.	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
AutoprotectDisabledRpEvent	Event to indicate that Automatic Protection is deactivated for a particular replication provider.	Automatic Protection is deactivated for a particular replication provider.	Info
AutoprotectEnabledRpEvent	Event to indicate that Automatic Protection is activated for a particular replication provider.	Automatic Protection is activated for a particular replication provider.	Info

Event	Description	Cause	Category
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
VmEligibleForProtectionEvent	Event to indicate that Automatic Protection detects a new virtual machine that is eligible for protection.	Automatic Protection detects a new virtual machine eligible for protection.	Info
VmEligibleForUnprotectionEvent	Event to indicate that Automatic Protection detects a new virtual machine or a virtual machine template that is eligible for automatic protection removal.	There is a virtual machine or a virtual machine template that can be unprotected in an existing virtual machine protection group and the automatic protection is deactivated for the replication provider.	Info
VmAutoUnprotectEvent	Event to indicate that the Automatic Protection removal operation completed successfully.	A virtual machine or a virtual machine template is automatically unprotected successfully.	Info
VmAutoUnprotectErrorEvent	Event to indicate that the Automatic Unprotection operation failed.	Automatic Unprotection operation failed.	Error

Virtual Volumes Events

Virtual Volumes events provide information about actions and status related to Virtual Volumes.

Virtual Volumes Events

Table 49:

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

Event	Description	Cause	Category
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 50: 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 51: 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
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 52: 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	Activated replicated array pair with Array Manager.	User activated an Array Pair.	Info

Event	Description	Cause	Category
SAPairDisabledEvent	Deactivated replicated array pair with Array Manager.	User deactivated 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 53: 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 54: 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

Event	Description	Cause	Category	Event Target
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
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

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 55: 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 56: 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 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 57: 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.
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.

Event	Description	Cause
RecoveryPlanPromptDisplayTrap	This trap is sent when a recovery plan requires user input before continuing.	Site Recovery Manager site name, recovery plan name, recovery type, execution state, prompt string.
RecoveryPlanPromptResponseTrap	This trap is sent when a recovery plan no longer requires user input before continuing.	Site Recovery Manager site name, recovery plan name, recovery type, and execution state.

Collecting Site Recovery Manager Log Files

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.

1. In the vSphere 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 **Actions** 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 the procedure generates is identical to the logs that you generate by using the vSphere Client.

1. Log in to the Site Recovery Manager Appliance host machine and open a command prompt.
2. Change the working directory to `/opt/vmware/dr/bin/`.
3. Run the following command:
   - If you are logged in as an admin user: `sudo ./dr-support-linux.sh`.
   - If you are logged in as a root user: `./dr-support-linux.sh`.

You can access the generated log bundles from the `/opt/vmware/support/logs/Support` directory.

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.

1. Log in to the Site Recovery Manager Server host.
2. Open the `vmware-dr.xml` file in a text editor.
   The `vmware-dr.xml` file is located in the `/opt/vmware/srm/conf/` directory.
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.

   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.

1. Log in to the Site Recovery Manager Server host.
2. Open the `vmware-dr.xml` file in a text editor.

   The `vmware-dr.xml` file is located in the `/opt/vmware/srm/conf/` directory.

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.

   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

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 by Broadcom knowledge base at https://support.broadcom.com/.

VPXD service crashes during Site Recovery Manager workflows in a stretched storage environment

Test Recovery and Planned Migration with VMware vMotion might fail in a stretched storage environment.

When you attempt to perform a Test Recovery or Planned Migration with VMware vMotion in a stretched storage environment, the workflows fail.

The failure is a result of the `vpxd` service crashing in vCenter Server 8.0 and later.

Power off the vCenter Server instances on the protected and the recovery site and increase the memory to at least 32 GB.

Test recovery and planned migration fail for some virtual machines with multiple errors

Test recovery and planned migration might fail for some virtual machines with multiple errors.

During test recovery and planned migration the vSphere Replication server might restart causing some replications to fail with the following errors:

```
Cannot commit group '<group-id>' to an image on vSphere Replication Server '<VR-server>' (address '<VR-serv-
er-address>'). A generic error occurred in the vSphere Replication Management Server. Exception details:
 'https://<VR-server-address>:8123/ invocation failed with "org.apache.http.conn.HttpHostConnectException:
 Connect to <VR-server-address>:8123 [/<VR-server-address>] failed: Connection refused (Connection refused)"'.
Error : Cannot commit group '<group-id>' to an image on vSphere Replication Server '<VR-server>' (address
 '<VR-server-address>'). A generic error occurred in the vSphere Replication Management Server. Exception de-
tails: 'https://<VR-server-address>:8123/ invocation failed with "java.net.SocketException: Connection re-
set"'.
Error : A runtime error occurred in the vSphere Replication Management Server. Exception details: ''. A run-
time error occurred in the vSphere Replication Management Server. Exception details: ''
```

While performing test recovery and planned migration the vSphere Replication server might restart causing some of the replications to fail.

Re-run the Test recovery plan. After the vSphere Replication server restarts, the operations that failed complete successfully.

Reconfigure replication fails after re-protect when changing the target datastore for a vmdk

After performing re-protect operation, reconfigure replication that involves disk moves might fail.

After performing reprotect operation, reconfigure replication that involves disk moves, for example moving the disk to another datastore or path, fails with the following error:

```
Unable to complete the reconfiguration task at remote site for replication group 'hbr-vm' (managed object ID:
 'GID-xxxx'): task 'HTID-xxxx'.
Details: 'A runtime error occurred in the vSphere Replication Management Server.
Exception details: 'VR Server error: 'Virtual Machine exists at the target datastore path'.
```

The problem can occur when there is disk with the same name at the target location.

You must rename or move the vmx of the original virtual machine at the target location.

Reprotect fails with an error during the synchronize storage step

The reprotect operation might fail during the synchronize storage step.

Reprotect fails with the following error: "`Operation timed out: 1080 seconds`".

If the discover devices storage operation is still in progress, it prevents synchronize storage which is the last sub-step of the reprotect workflow to finish in time. Even though the re-protect workflow fails, the synchronize storage sub-step will start and complete successfully after the discover devices operation is complete.

Wait for the discover devices operation to complete and allow some more time for synchronize storage to finish. When discover devices and synchronize storage operations finish, you must run test failover to check that everything is OK with the recovery plan.

1. On the Site Recovery home tab, select a site pair, and click **View Details**.
2. n the left pane, click **Configure** > **Advanced Settings** > **Remote Manager**.
3. Select a site and click **Edit** to modify the remote manager settings.
4. Increase the value in the **remoteManager.taskDefaultTimeout** text box.

Reprotect operation fails with an error for one VM

When you attempt to perform reprotect the operation fails with an error for a single VM.

Reprotect operation fails with one of the following errors: `Unable to reverse replication for the virtual machine '<vm-name>'. A general system error occurred: Fault cause: vim.fault.GenericVmConfigFault` or `Unable to reverse replication for the virtual machine '<vm-name>'. A general system error occurred:.`

On the target vCenter Server site, the task for the virtual machine fails with the following details:

`Task Name: Remove all snapshots`

`Status: A general system error occurred: Fault cause: vim.fault.GenericVmConfigFault` Or
`Status: A general system error occurred: Snapshot configuration missing for snapshot <>`

`Initiator: <initiator>`

`Target: <vm-name>`

`Server: <VC-name>`

1. Remove the replication.
2. Configure the replication again, using seed disks.

Exporting Site Recovery Manager configuration by using a remote Site Recovery Manager solution user fails with an error

When you attempt to export the Site Recovery Manager configuration by using a script without credentials, the export fails with an error.

In a Site Recovery Manager environment with only array-based replications, when you attempt to export the Site Recovery Manager configuration by using a script without credentials, the export fails. The Impex log contains the following error:

```
YYYY-MM-DD 04:35:57,061 [srm-reactive-thread-13] ERROR com.vmware.srm.client.impex.Main - Export SRM configu-
ration ended.(vim.fault.NoPermission) {
faultCause = null,
faultMessage = null,
object = ManagedObjectReference: type = Folder, value = group-d1, serverGuid = ,privilegeId = StoragePro-
file.View }
```

Add **policy-driven storage view** to the remote Site Recovery Manager solution user role or export the Site Recovery Manager configuration by either using a properties file, or in interactive mode with credentials. See, Use a Properties File to Export Site Recovery Manager Configuration Data and Export Site Recovery Manager Configuration Data with the Standalone Import/Export Tool.

The name of the downloaded file with exported recovery steps is not displayed properly

When you export the recovery plan steps, the name of the downloaded file is not displayed properly.

If you have a recovery plan with non-ascii characters in the name, when you export the recovery plan steps, the name of the downloaded file is not displayed properly.

Site Recovery Manager replaces all non-ascii characters with an underscore sign.

Do not use non-ascii characters for the name of the Recovery Plan.

The Site Recovery user interface freezes and becomes unresponsive

If you use Chromium-based browser and you try to resize a column of a grid, the Site Recovery user interface freezes and becomes unresponsive.

When you attempt to resize a column of a grd the user interface freezes and becomes unresponsive.

`LayoutNG` in Chromium is having a bug that causes performance issues. For more information, see https://bugs.chromium.org/p/chromium/issues/detail?id=1008523 and https://bugs.chromium.org/p/chromium/issues/detail?id=1098231. Updating your Chrome browser to version 85.0.4183.83 or later fixes the issue.

1. Close all Chrome windows.
2. Edit the Chrome shortcut link and update it to: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-blink-features=LayoutNG`.
3. Open Chrome again.

After a successful login in the vCenter Single Sign-On, you are unable to log in to the Site Recovery user interface

You are unable to log in to the Site Recovery user interface.

The Site Recovery user interface log contains the following error message `"Certificate for <host> doesn't match any of the subject alternative names: <subjectaltlist>"` . When you attempt to do a remote login within the Site Recovery user interface by using the remote login dialog box, you receive similar error message in the user interface.

The Site Recovery user interface might not be able to connect to the Platform Services Controller hosts because of the way the host certificate is generated:

- If the Platform Services Controller certificate does not have a host's address (IP or FQDN) as a subject alternative name;
- If the Platform Services Controller certificate lacks subject alternative names and the host name is not matched in the certificate's CN fields.

1. Reconfigure the Platform Services Controller with a certificate with a SAN (Subject Alternative Name Field) that contains an entry for the Platform Services Controller address (the '<host>' string from the error message).
2. If the certificate is properly generated, but the address used by user interface is not, you must reconfigure the user interface and the corresponding Site Recovery Manager and vSphere Replication Appliances to use the correct Platform Services Controller address.
3. Reconfigure the existing pairings for the appliances.

Recovery plan execution might fail to power on a virtual machine with 'InvalidArgument:path'

Recovery plan execution might fail to power on a VM.

When you run a recovery plan, Site Recovery Manager might fail to power on a VM with `(vmodl.fault.InvalidArgument:path)` error. The following error message appears in the Site Recovery Manager recovery site server logs:

```
YYYY-MM-DDT20:24:35.996-08:00 error vmware-dr[02448] [SRM@6876 sub=Recovery ...] Plan execution (test work-
flow) failed;
plan id: 34f86036-3bc7-4c2d-a841-e15c5d781532, plan name: HBRRP_LIMITS, error: (vmodl.fault.InvalidArgument) {
-->    faultCause = (vmodl.MethodFault) null,
-->    faultMessage = <unset>,
-->    invalidProperty = "path"
-->    msg = "A specified parameter was not correct: path"
--> }
-->
```

This error is a result of a failing 'Relocating VM before powered on' operation on the target destination ESXi host. The related error message in the ESXi vpxa service logs is:

```
YYYY-MM-DDT03:56:48.255Z error vpxa[2099931] [Originator@6876 sub=vpxaVmprov opID=failedOpId]
Failed to canonicalize vm register path;
/vmfs/volumes/.../recoveredVm.vmx, err: 16(Device or resource busy)
...
YYYY-MM-DDT03:56:48.256Z info vpxa[2099931] [Originator@6876 sub=Default opID=failedOpId]
[VpxLRO] -- ERROR task-1824 -- vpxa -- vpxapi.VpxaService.registerVm: vmodl.fault.InvalidArgument:
--> Result:
--> (vmodl.fault.InvalidArgument) {
-->    faultCause = (vmodl.MethodFault) null,
-->    faultMessage = <unset>,
-->    invalidProperty = "path"
```

Re-run the failed recovery plan.

Reprotect fails with an internal error

When you run reprotect, the operation might fail with an error.

When you run reprotect, the operation fails with the following error. `Internal error: Received unexpected exception during prepare phase. The session is not authenticated.`

Re-run the reprotect operation.

VMware Site Recovery Manager 8.8 Configuration Import/Export Tool might error out when you import a configuration

VMware Site Recovery Manager 8.8 Configuration Import/Export Tool might error out when you import a configuration with protected VMs that are not part of any recovery plan.

The VMware Site Recovery Manager 8.8 Configuration Import/Export Tool might error out when you import a configuration with protected VMs that are not part of any recovery plan. The rest of your exported configuration is properly imported.

If you put protected virtual machines in recovery plans, then delete all recovery plans containing these VMs, and export your configuration with the VMware Site Recovery Manager 8.8 Configuration Import/Export Tool, the VM recovery settings for those VMs are exported but you are unable to import them later. If you try to import your settings, you see errors similar to: `Error while importing VM settings for server with guid '6f81a31e-32e0-4d35-b329-783933b50868'.`

Recreate your recovery plan, reconfigure the desired recovery settings, and export your configuration again. Do not delete recovery plans if you want to export and import VM recovery settings.

IP customization fails when you use special characters in the Recovery Plan name

Special characters in the recovery plan name cause IP customization to fail.

When you run a Test Recovery for a Recovery Plan with special characters in the name and configured IP customization, the IP customization fails.

Remove any OS-specific special symbols from the Recovery Plan name.

If the protected vCenter Server is down, you might experience performance degradation in the HTML 5 user interface on the recovery site

You might experience performance degradation in the Site Recovery user interface on the recovery site.

You might experience performance degradation in the HTML 5 user interface on the recovery site, especially in the Configure Recovery Settings dialog box, if the protected vCenter Server instance is down.

The user interface assumes that the remote site is still online and makes network calls causing the delays.

Refresh the HTML 5 user interface on the recovery site and re-try your operation.

After the recovery plan workflow completes, the last recovery steps continue to show a Running status

Some of the recovery steps continue to show a running status after the completion of the recovery plan workflow.

The last recovery steps continue to show a "Running" status after the recovery plan workflows completes.

The incorrect status is a transient UI problem. Site Recovery Manager executes all the steps to completion.

Click the global refresh icon to refresh the interface. All steps display the correct completed status.

Prompts and commands disappear from the list of steps in recovery view

If you try to edit a prompt or command in test view, the prompt or command specific to the recovery view might disappear from the list of steps

After you add a prompt or command in **Recovery Steps** > **Recovery View**, you can see the same prompt or command in test view. However if you try to edit a prompt or command in test view, the prompt or command specific to the recovery view might disappear from the list of steps.

Disappearing prompts or commands is a transient UI problem that affects only the detailed list of recovery steps. Site Recovery Manager executes all prompts and commands when you run a test or recovery even if they do not appear in the detailed list of steps.

Click the global refresh icon to refresh the interface. All callouts reappear in the list of steps.

The placeholder virtual machine on the recovery site still exists after you delete the protection group and recovery plan

When you delete the recovery plan and protection group from the Site Recovery Manager inventory, the placeholder VM might still be visible on the recovery site.

When you delete the recovery plan and protection group from the Site Recovery Manager inventory, the placeholder VM is still visible on the recovery site. An error occurs when you try to create a new protection group with the same datastore and virtual machine. When you try to manually delete the placeholder virtual machine from the vCenter Server inventory, an error occurs. Site Recovery Manager marks the virtual machine as orphaned.

Delete the placeholder virtual machine and remove the orphaned virtual machine, then create the protection group with the same virtual machine.

Cancellation of Recovery Plan is not complete

When you attempt to cancel a Recovery Plan the status might remain as Not Completed.

When you attempt to cancel a recovery plan, the status is Not Completed.

When you run a recovery plan, an attempt is made to synchronize virtual machines. It is possible to cancel the recovery plan, but attempts to cancel the recovery plan run do not complete until the synchronization either completes or expires. The default expiration is 60 minutes.

You can use the following options to complete cancellation of the recovery plan.

- Pause vSphere Replication, causing synchronization to fail. After recovery enters an error state, use the vSphere Client to restart vSphere Replication in the vSphere Replication tab. After replication is restarted, you can run the the recovery plan again, if desired.
- Wait for synchronization to complete or time out. This might take considerable time, but does eventually finish. After synchronization finishes or expires, cancellation of the recovery plan continues.

When you remove permission for a user on a protected site while logged in as that user, you receive an error

If you remove permission for a user on a protected site while logged in as that user, you receive an incorrect error message.

When you remove permission for a user on a protected site while logged in as that user, the following error message appears: `Unable to retrieve Permissions data. The session is already logged in.`

A similar error appears on the Advanced Settings tab.

This error appears when you remove your own permissions at the site level. Instead, the message should inform you that you do not have permissions to view the page.

None.

Reconfiguring Site Recovery Manager fails after an upgrade from an external Platform Services Controller to an embedded node

Reconfiguring Site Recovery Manager fails after you upgrade a vCenter Server 6.5.x or 6.7.x instance with an external Platform Services Controller to an embedded vCenter Server 7.x node.

When you attempt to reconfigure Site Recovery Manager after an upgrade of a vCenter Server 6.5.x or 6.7.x instance with an external Platform Services Controller to a vCenter Server with an embedded 7.x node, the operation fails with an error.

```
ERROR
Operation Failed
A general system error occurred: 22ConfigurationException Failed to configure DR server with the Infrastruc-
ture Node services. Reason: Fault cause: lookup.fault.EntryExistsFault

Exit code: 61
```

When you upgrade a vCenter Server 6.5.x or 6.7.x instance with an external Platform Services Controller to a vCenter Server 7.x instance with an embedded node the vCenter Single Sign-On site name id changes.

1. Record the `serviceId` from the `Error 61` message.
2. Log in with vCenter Server credentials to `https://<vCenter_Server_address>/lookupservice/mob/` on the protected site.
3. Navigate to **RetrieveServiceContent** > **Invoke Method** > **ServiceRegistration** > **Delete method** to delete `serviceId: <serviceId>`.
4. Log in to the Site Recovery Manager Appliance Management on the protected site as admin.
5. Click **Summary**, click **Reconfigure**, and follow the prompts.
6. Record the `serviceId` from the `Error 61` message.
7. Log in with vCenter Server credentials to `https://<vCenter_Server_address>/lookupservice/mob/` on the recovery site.
8. Navigate to **RetrieveServiceContent** > **Invoke Method** > **ServiceRegistration** > **Delete method** to delete `serviceId: <serviceId>`.
9. Log in to the Site Recovery Manager Appliance Management as admin.
10. In the Site Recovery Manager Appliance Management Interface, click **Services**.
11. Select the **srm-server** service, click Stop, then click **OK**.
12. SSH to the upgraded embedded vCenter Server, run the following command and take note of the vCenter Single Sign-On site name.

    ```
    /usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name localhost
    ```

13. SSH to Site Recovery Manager, run the following comment and take node of the `db_id`.

    ```
    echo "select * from pds_solutionuser;" | PGPASSWORD='<password>' /opt/vmware/vpostgres/
    current/bin/psql -U srmdb -d srmdb -p 5432
    ```

    NOTE
    Password is the `password` for the embedded vPostgres database that you set during the installation of Site Recovery Manager.

14. Run the following command.

    ```
    echo "update pds_solutionuser set siteid = 'default-first-site' where db_id =<db_id> ;"
    | PGPASSWORD='<password>' /opt/vmware/vpostgres/current/bin/psql -U srmdb -d srmdb -p
    5432
    ```

15. Log in to the Site Recovery Manager Appliance Management on the recovery site as admin and reconfigure Site Recovery Manager.
16. Log in to Site Recovery Manager on the protected site.
17. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
18. Select **Site Pair** > **Summary**, and click **Reconnect**.
    a) If you encounter an error, restart both Site Recovery Manager instances and vCenter Server instances and repeat the reconnect operation.

```
Unable to connect to Site Recovery Manager Server at https://<SRM FQDN/IP>:443/drserver/vcdr/vmo-
mi/sdk.
Reason: java.net.SocketTimeoutException: 30,000 milliseconds timeout on connection http-outgoing-431
 [ACTIVE]
```

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.

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.`

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.

1. Log in to the Site Recovery Manager Server host.
2. Open the `vmware-dr.xml` file in a text editor.
   The `vmware-dr.xml` file is located in the `/opt/vmware/srm/conf/` directory.
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.

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.

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.`

You did not map the devices of the virtual machine on the protected site to the corresponding devices on the recovery site.

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.

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.

The infrastructure on the recovery site is unable to handle the volume of concurrent creations of placeholder virtual machines.

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.

Recreating the placeholders too rapidly after unmounting the datastore can fail with the error `NoCompatibleHostFound`.

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.

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.

Planned migration fails with the error `Error - The operation is not allowed in the current state of the host.`

Site Recovery Manager cannot power on virtual machines on the recovery site when the ESXi host on the recovery site is in maintenance mode.

Exit maintenance mode on the ESXi host on the recovery site and rerun the planned migration.

Recovery Fails with a Timeout Error During Network Customization for Some Virtual Machines

During a recovery some virtual machines do not recover and show a timeout error during network customization.

During recovery some virtual machines do not recover within the default timeout period of 120 seconds.

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.

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, 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.

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....`

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.

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.

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.`

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.

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.

Recovery operations fail at the Shutdown VMs step or Waiting for VMware Tools step of a recovery plan.

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.

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.

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.`

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.

1. Log in to the Site Recovery Manager Server host.
2. Open the `vmware-dr.xml` file in a text editor.

   The `vmware-dr.xml` file is located in the `/opt/vmware/srm/conf/` directory.
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.

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.

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

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.

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%.

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%.

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.

When you run several recovery plans simultaneously that contain array-based replication 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.`

This problem can occur because datastore computation on a site is delayed by the recovery operations that are running in the opposite direction.

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.

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
```

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.

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 activate or deactivate 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.

You might receive the following error during the recovery process.

```
OperationNotSupportedByGuest
```

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 8.8*.

Ensure that the versions of VMware Tools and ESXi are compatible with your Site Recovery Manager.

Site Recovery Manager Security

Provides a concise reference to the security features of VMware Site Recovery Manager.

About VMware Site Recovery Manager Security

Site Recovery Manager Security provides a concise reference to the security features of Site Recovery Manager.

To help you protect your Site Recovery Manager installation, this guide describes security features built into Site Recovery Manager and the measures that you can take to safeguard it from attack.

- External interfaces, ports, and services that are necessary for the proper operation of Site Recovery Manager
- Configuration options and settings that have security implications
- Location of log files and their purpose
- Required system accounts
- Information on obtaining the latest security patches

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of Site Recovery Manager.

Site Recovery Manager Security Reference

Use the Security Reference to learn about the security features of your Site Recovery Manager installation and the measures that you can take to safeguard your environment from attack.

Site Recovery Manager Services

The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Table 58: Services that Site Recovery Manager Requires

Service Name	Startup Time	Description
srm-server	Automatic	Provides the core Site Recovery Manager functions.
srm-postgress	Automatic	The vPostgres server for the Site Recovery Manager embedded database.
rsyslog	Automatic	The rocket-fast system for log processing.
dr-client	Automatic	Provides Site Recovery Manager Client (Tomcat, HTML5 user interface) functionality.
telegraf	Manual	Plugin-driven server agent for collecting and sending metrics and events. The service is stopped by default.
dr-iperf3	Manual	Tool for active measurements of the maximum achievable bandwidth on IP networks. The service is stopped by default.
auditd	Manual	Component responsible for writing audit records to the disk. The service is stopped by default.

Service Name	Startup Time	Description
dr-rest	Automatic	Provides Site Recovery Manager REST API functionality.
dr-client-plugin	Automatic	Provides Site Recovery Manager plug-in functionality.

Related Links

Site Recovery Manager Network Ports on page 316
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Configuration Files on page 317
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Certificates and Keys on page 319
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Stored Credentials on page 319
Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager License and EULA Files on page 320
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Site Recovery Manager Log Files on page 321
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Accounts on page 323
Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

Site Recovery Manager Security Updates and Patches on page 324
You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Best Practices for Securing Site Recovery Manager Server on page 325
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Site Recovery Manager Network Ports

Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

All Site Recovery Manager Virtual Appliance services run behind a reverse HTTP proxy on port 443. The Site Recovery Manager Appliance Management Interface requires port 5480.

Site Recovery Manager Server communicates with vCenter Server, ESXi hosts, and Arrays at the local site. You must verify that the network firewall policies enable the traffic to network ports of all components at the local site. For the list of the default ports that all VMware products use, see http://kb.vmware.com/kb/1012382.

The connection between the local and the remote site of a Site Recovery Manager pair must be private such as VPN. The local Site Recovery Manager Server communicates with Site Recovery Manager Server and vCenter Server on the remote site, and your network provider must ensure the appropriate network policies to enable the traffic.

For a list of all the ports that must be open for Site Recovery Manager, see the *Network Ports for Site Recovery Manager* topic in the *Site Recovery Manager Installation and Configuration* documentation.

Related Links

Site Recovery Manager Services on page 315
The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Site Recovery Manager Configuration Files on page 317
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Certificates and Keys on page 319
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Stored Credentials on page 319
Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager License and EULA Files on page 320
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Site Recovery Manager Log Files on page 321
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Accounts on page 323
Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

Site Recovery Manager Security Updates and Patches on page 324
You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Best Practices for Securing Site Recovery Manager Server on page 325
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Site Recovery Manager Configuration Files

Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Virtual Appliance Configuration Files

NOTE
Do not move, or delete the configuration files.

File or Directory Location	Description
`/opt/vmware/srm/conf/vmware-dr.xml`	Defines system configuration of Site Recovery Manager Server. You can safely change the system settings of a Site Recovery Manager instance by using the **Advanced Settings** on the Site Pair tab in the Site Recovery Manager user interface.
`/opt/vmware/dr/conf/drconfig.xml`	Defines configuration of the `dr-configurator` service.

File or Directory Location	Description
`/opt/vmware/dr-client/lib/h5dr.properties`	Defines configuration of the Site Recovery Manager HTML 5 user interface. You can safely change the telemetry settings of the Site Recovery Manager HTML 5 user interface by changing the *phonehomeEnabled* value from true to false and the reverse. You can change the session timeout setting of the Site Recovery Manager HTML 5 user interface by changing the *sessionTimeout* value in seconds. By default, the session timeout is set to 7200 seconds. Changing the values in the `h5dr.properties` file requires restart of the `dr-client` service.
`/opt/vmware/srm/conf/extension.xml`	Defines configuration of Site Recovery Manager Server Extension. The `extension.xml` file contains definitions of default user roles and their privileges. **NOTE** Do not modify the `extension.xml` file.
`/var/lib/srmdb/`	Contains the embedded database configuration files. **NOTE** Do not modify the configuration files.

Related Links

Site Recovery Manager Services on page 315
The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Site Recovery Manager Network Ports on page 316
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Certificates and Keys on page 319
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Stored Credentials on page 319
Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager License and EULA Files on page 320
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Site Recovery Manager Log Files on page 321
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Accounts on page 323
Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

Site Recovery Manager Security Updates and Patches on page 324
You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Best Practices for Securing Site Recovery Manager Server on page 325
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Site Recovery Manager Certificates and Keys

Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Virtual Appliance Certificates and Keys

All Site Recovery Manager Virtual Appliance services run behind a reverse HTTP proxy and do not use SSL for the communication path to the proxy. There is only one certificate for the proxy service. The certificate files are stored in `/opt/vmware/dr/conf/keys/vmware-dr/`.

CA certificate or private key or both	Location
TLS certificate and key for the HTML5 user interface created during the Site Recovery Manager Appliance deployment	In the `/opt/vmware/dr-client/lib/h5dr.keystore` file.

For more information about the Site Recovery Manager authentication mechanisms, see the *Site Recovery Manager Authentication* topic in the *Site Recovery Manager Installation and Configuration Guide*.

Related Links

Site Recovery Manager Services on page 315
The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Site Recovery Manager Network Ports on page 316
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Configuration Files on page 317
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Stored Credentials on page 319
Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager License and EULA Files on page 320
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Site Recovery Manager Log Files on page 321
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Accounts on page 323
Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

Site Recovery Manager Security Updates and Patches on page 324
You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Best Practices for Securing Site Recovery Manager Server on page 325
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Site Recovery Manager Stored Credentials

Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager Virtual Appliance Credentials

File Path	Description
`/opt/vmware/srm/conf/db:datastore name`	Credentials to access Site Recovery Manager Virtual Appliance database using *datastore name* System Datastore.
`/opt/vmware/srm/conf/prefix-keyname-username`	User name that must be used by the SRA when connecting to the array manager identified by manager id.
`/opt/vmware/srm/conf/prefix-keyname-password`	Password that must be used by the SRA when connecting to the array manager identified by *manager id*.
`opt/vmware/srm/conf/SRM-<local-srm-uuid>`	Credentials for the local service account.
`opt/vmware/srm/conf/SRM-remote-<local-srm-uuid>`	Credentials for the remote service account.

The credentials for the java keystore `h5dr.keystore` are stored in the `h5dr.properties` file located in the `/opt/vmware/dr-client/lib/` folder.

Related Links

Site Recovery Manager Services on page 315
The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Site Recovery Manager Network Ports on page 316
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Configuration Files on page 317
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Certificates and Keys on page 319
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager License and EULA Files on page 320
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Site Recovery Manager Log Files on page 321
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Accounts on page 323
Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

Site Recovery Manager Security Updates and Patches on page 324
You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Best Practices for Securing Site Recovery Manager Server on page 325
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Site Recovery Manager License and EULA Files

The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Table 59: Site Recovery Manager Virtual Appliance License and EULA Files

File or Directory	Description
`/opt/vmware/etc/isv/EULA`	Directory containing the Site Recovery Manager End-user license agreement files.
`/opt/vmware/srm/open_source_licenses.zip`	Site Recovery Manager Open Source Licenses file.

Related Links

Site Recovery Manager Services on page 315
The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Site Recovery Manager Network Ports on page 316
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Configuration Files on page 317
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Certificates and Keys on page 319
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Stored Credentials on page 319
Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager Log Files on page 321
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Accounts on page 323
Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

Site Recovery Manager Security Updates and Patches on page 324
You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Best Practices for Securing Site Recovery Manager Server on page 325
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Site Recovery Manager Log Files

Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Virtual Appliance Server Logs

The Site Recovery Manager Virtual Appliance stores the system log files in the `/var/log/vmware/srm/` directory. The latest messages from Site Recovery Manager Server are placed in the `vmware-dr-`*`number`*`.log` file.

The support bundle is located in the `/var/log/vmware/Support/` folder.

Log Levels for Server Logs

Level	Description
error	Displays only error log entries.
info	Displays information, error, and warning log entries.
trivia	Displays information, error, warning, verbose, and trivia log entries.
verbose	Displays information, error, warning, and verbose log entries.
warning	Displays warning and error log entries.

Site Recovery Manager supports components such as:

- Default
- Replication
- Recovery
- Storage
- StorageProvider
- Vdb
- Persistence

The `vmware-dr-number.log` file does not contain security messages concerning the authentication process and connections with the remote side.

Site Recovery Manager Virtual Appliance User Interface Logs

The Site Recovery Manager Virtual Appliance stores the Site Recovery user interface log files in the `/var/log/vmware/dr-client/` folder. The latest messages are placed in the `dr.log` file.

You can modify the log level of each component by updating the level value element in the `log4j2.xml` file in the `/opt/vmware/dr-client/webapps/dr/WEB-INF/classes/` directory. The default level of all components is info.

The Site Recovery Manager Virtual Appliance Management Interface logs are located in the `/var/log/vmware/drconfigui/` folder. The latest messages are placed in the `drconfigui.log` file.

You can modify the log level of each component by updating the level value element in the `log4j2.xml` file in the `/opt/vmware/drconfigui/webapps/configure/WEB-INF/classes/` folder. The default level of all components is info.

Log Levels for User Interface Logs

Level	Description
error	Displays only error log entries.
warn	Displays warning and error log entries.
info	Displays information, error, and warning log entries.
debug	Displays debug, information, error, and warning log entries.
trace	Displays the most detailed information.

The tomcat server used by the Site Recovery user interface supports components such as:

- Http Async I/O
- Per handler call time
- VC L10N catalogs
- SRM
- VR
- Common

Related Links

Site Recovery Manager Services on page 315
The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Site Recovery Manager Network Ports on page 316
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Configuration Files on page 317
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Certificates and Keys on page 319
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Stored Credentials on page 319
Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager License and EULA Files on page 320
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Site Recovery Manager Accounts on page 323
Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

Site Recovery Manager Security Updates and Patches on page 324
You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Best Practices for Securing Site Recovery Manager Server on page 325
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Site Recovery Manager Accounts

Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

User Accounts

The vCenter Server administrators have administration access to Site Recovery Manager in the default configuration. You must use administrator credentials when you try to log in to Site Recovery Manager for the first time after the installation.

If you have administrator credentials, you can grant access to Site Recovery Manager to other users by using the vSphere Client.

For more information about Site Recovery Manager roles, privileges, and permissions, see the *Site Recovery Manager Privileges, Roles, and Permissions* in the *Site Recovery Manager Administration* documentation.

Service Account

Site Recovery Manager creates a service account during the installation and uses it during the authentication with vCenter Server . The service account is unique for each Site Recovery Manager instance and is for internal use by Site Recovery Manager and vCenter Server.

Site Recovery Manager creates an additional service account on each remote site during the pairing process of sites that do not use Enhanced Linked Mode. Site Recovery Manager uses the service account to perform necessary operations on the remote site.

Site Recovery Manager creates a service account for the HTML5 user interface during the installation. The service account is unique for each Site Recovery Manager instance and is for internal use by Site Recovery Manager HTML5 UI client and vCenter Server.

NOTE
You must not delete and modify the roles and privileges associated with the service accounts.

For more information about the service accounts and authentication between the local and remote site, see the *Site Recovery Manager Authentication* topic in the *Site Recovery Manager Installation and Configuration* documentation.

Related Links

Site Recovery Manager Services on page 315
The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Site Recovery Manager Network Ports on page 316
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Configuration Files on page 317
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Certificates and Keys on page 319
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Stored Credentials on page 319
Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager License and EULA Files on page 320
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Site Recovery Manager Log Files on page 321
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Security Updates and Patches on page 324
You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Best Practices for Securing Site Recovery Manager Server on page 325
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Site Recovery Manager Security Updates and Patches

You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

The Site Recovery Manager virtual appliance uses VMware Photon OS 4.0 as the guest operating system.

Applying Site Recovery Manager Patches and Security Updates to the Site Recovery Manager Virtual Appliance

You apply Site Recovery Manager security patches and updates by performing an update of your existing Site Recovery Manager Virtual Appliance installation. For information about updating the Site Recovery Manager Virtual Appliance, see the *Update the Site Recovery Manager Virtual Appliance* topic in *Site Recovery Manager Installation and Configuration*.

Related Links

Site Recovery Manager Services on page 315
The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Site Recovery Manager Network Ports on page 316
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Configuration Files on page 317
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Certificates and Keys on page 319
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Stored Credentials on page 319
Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager License and EULA Files on page 320
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Site Recovery Manager Log Files on page 321
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Accounts on page 323
Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

Best Practices for Securing Site Recovery Manager Server on page 325
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

Best Practices for Securing Site Recovery Manager Server

Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

The secure operation of Site Recovery Manager depends on the proper configuration and maintenance of the Site Recovery Manager Server.

- Apply the latest Site Recovery Manager updates and patches to address any known issues with Site Recovery Manager.
- Ensure the integrity of your Site Recovery Manager deployment when you run Site Recovery Manager as a VM. See the *Virtual Machine Security Best Practices* topic in the *vSphere Security* documentation.
- Allow only administrators to access the server. To limit the number of accounts that an attacker can use, limit the number of accounts that can access the server.
- Check the network ports that Site Recovery Manager uses and configure a firewall to protect your server.

Related Links

Site Recovery Manager Services on page 315

The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

Site Recovery Manager Network Ports on page 316
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Configuration Files on page 317
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

Site Recovery Manager Certificates and Keys on page 319
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

Site Recovery Manager Stored Credentials on page 319
Site Recovery Manager stores the credentials of the storage replication adapter (SRA) and database in `/opt/vmware/srm/conf/`.

Site Recovery Manager License and EULA Files on page 320
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

Site Recovery Manager Log Files on page 321
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager Accounts on page 323
Site Recovery Manager uses Single Sign-On (SSO) to access vCenter Server and Platform Services Controller.

Site Recovery Manager Security Updates and Patches on page 324
You can apply Site Recovery Manager security updates and patches as they are made available by VMware.

Using Site Recovery Manager with Hyperscalers

How to install and configure Site Recovery Manager in a supported cloud environment.

Using Site Recovery Manager with Hyperscalers

The *Using Site Recovery Manager with Hyperscalers* guide provides information about how to install and configure VMware Site Recovery Manager in a supported cloud environment.

This guide is for customers planning to use Site Recovery Manager in supported cloud environments such as Azure VMware Solution, Google Cloud VMware Engine, and Oracle Cloud VMware Solution.

Intended Audience

This information is intended for anyone who wants to install and configure Site Recovery Manager. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Deploying Site Recovery Manager on Azure VMware Solution

You can use Site Recovery Manager 8.8.x and vSphere Replication 8.8.x with Azure VMware Solution.

Azure VMware Solution is an infrastructure-as-a-service private cloud offering built on VMware Cloud Foundation stack. It is a service sold and supported by Microsoft, verified by VMware, that runs on Azure infrastructure.

You can use Site Recovery Manager 8.8.x and vSphere Replication 8.8.x to plan, test, and run the recovery of virtual machines between a protected vCenter Server on-premises site and a recovery vCenter Server site on Azure VMware Solution and the reverse, or between two Azure VMware Solution cloud sites.

Operational Limits of Site Recovery Manager onAzure VMware Solution

Each Site Recovery Manager instance onAzure VMware Solution can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries.

Protection and Recovery Maximums for Site Recovery Manager

Table 60: Protection and Recovery Maximums for Site Recovery Manager

Item	Maximum
Total number of protected virtual machines per SDDC onAzure VMware Solution	4000 **NOTE** To achieve the 4000 virtual machines scale, you must manually balance the replications between the different vSphere Replication nodes. Contact Microsoft for the scale up/down of vSphere Replication appliances within Azure VMware Solution. You must manually add additional vSphere Replication servers to your on-premises environment, see *Deploying Additional vSphere Replication Servers* in the *vSphere Replication Administration* guide.
Maximum number of protected virtual machines pervSphere Replication appliance (through embeddedvSphere Replication server).	400
Maximum number of protected virtual machines pervSphere Replication server.	400
Total number of virtual machines per protection group	500
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Total number of virtual machines per recovery plan	2000
Total number of virtual machine recoveries that you can start simultaneously across multiple recovery plans	2000

Bidirectional Protection

If you establish a bidirectional protection, in which site B serves as the recovery site for site A and at the same time site A serves as the recovery site for site B, limits apply across both sites, and not per site. In a bidirectional implementation, you can protect a different number of virtual machines on each site, but the total number of protected virtual machines across both sites cannot exceed the limits.

For example, if you protect 2600 virtual machines usingvSphere Replication from site A to site B, you can use vSphere Replication to protect a maximum of 1400 virtual machines from site B to site A. If you are usingvSphere Replication for a bidirectional protection, you can protect a maximum of 4000 virtual machines across both sites.

IP Customization Maximums for Site Recovery Manager

If you implement IP customization for recovered virtual machines, you can configure a maximum of one IP address for each NIC, using DHCP, static IPv4, or static IPv6. For static IPv4 or IPv6 addresses, you provide the following information per NIC:

- 1 IP address
- Subnet information
- 1 gateway server address
- 2 DNS servers (primary and secondary)

You also set 2 WINS addresses for DHCP or IPv4, on Windows virtual machines only.

Recovery Point Objective lower than 15 minutes

For information about Recovery Point Objective (RPO) lower than 15 minutes, see *Recovery Point Objective* in the *vSphere Replication Administration* guide.

Custom Command Recovery Steps

You cannot run commands onSite Recovery Manager Server onAzure VMware Solution. See Types of Custom Recovery Steps

Deploy Site Recovery Manager on Azure VMware Solution

This topic explains how to deploy Site Recovery Manager and vSphere Replication on Azure VMware Solution.

For a cloud to cloud recovery, make sure that the following ports are open: 80, 443, 902, 1433, 1521, 1526, 5480, 8123, 9086, 31031, 32032, 8043, 10000-10010.

1. Log in to the Azure portal.
2. Navigate to your subscription `AVS-2.XXX` and search for **Azure VMware Solution**.
3. Click a private cloud, go to **Manage** and click **Add-ons**.
4. On the right-side pane, click **Start** under **Disaster Recovery**.
5. From the drop-down menu, select **VMware Site Recovery Manager (SRM) - vSphere replication** as a disaster recovery solution.
6. Provide a license key or select to use an evaluation version.
7. Accept the terms and conditions and click **Install**.
8. Once the Site Recovery Manager installation completes, go back to **Manage** and click **Add-ons**.
9. On the right-side pane, click **Start** under **Disaster Recovery**.
10. Go to **Setup replication**. From the drop-down menu, select **vSphere Replication** and click **Install**.

You must connect the Site Recovery Manager Server instances on the protected and recovery sites.

Connect the Site Recovery Manager Instances on the Protected and Recovery Sites

Before you can use Site Recovery Manager, you must connect the Site Recovery Manager Server instances on the protected and recovery sites. This is known as site pairing.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.

   The address that you provide for the Platform Services Controller must be an exact match of the of address that you provided when you installed Site Recovery Manager Server on the recovery site.

   IMPORTANT
   To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.

4. Select the vCenter Server and the services you want to pair, and click **Next**.
5. On the **Ready to complete** page, review the pairing settings, and click **Finish**.

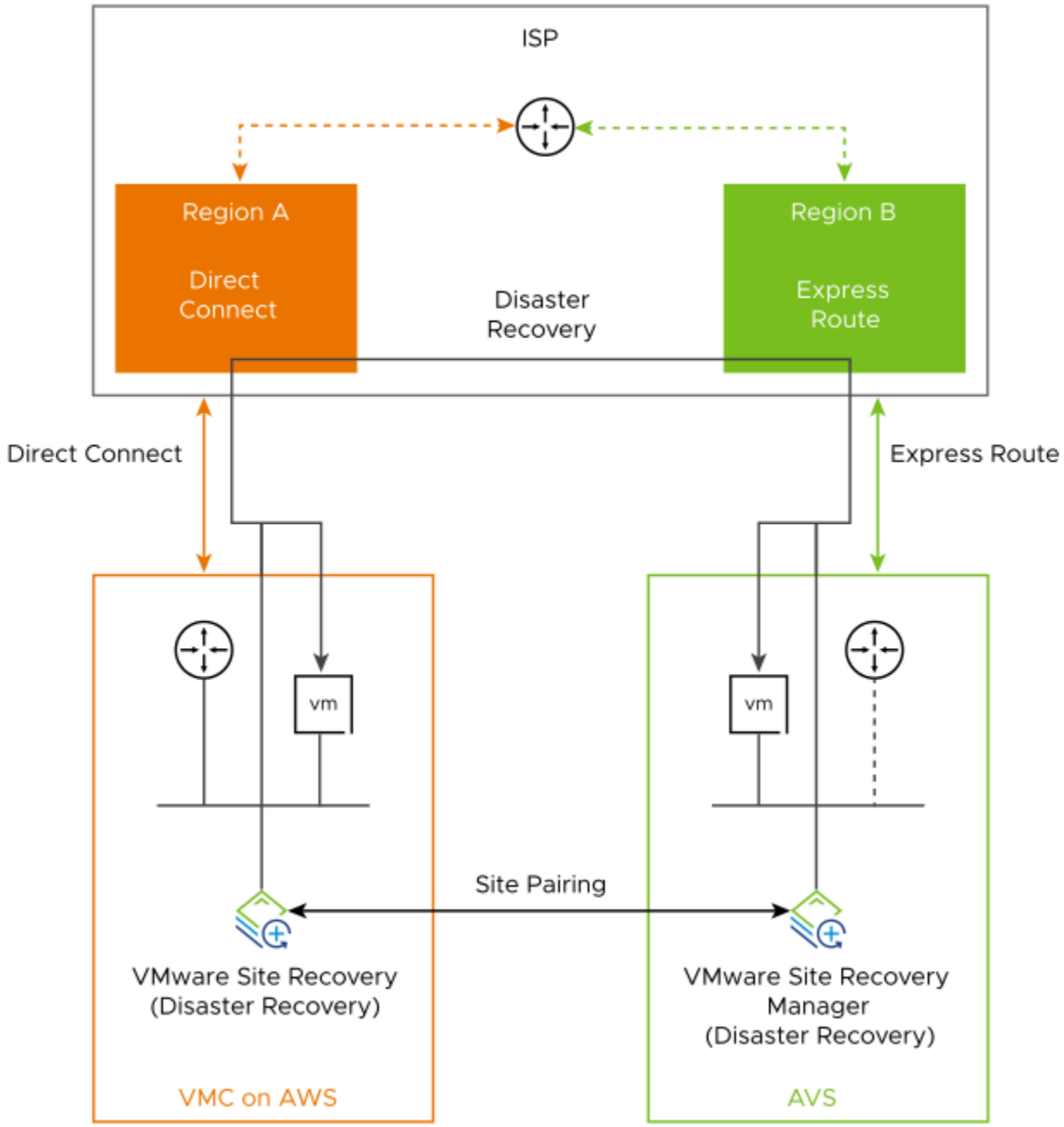
The protected and the recovery sites are connected. The pair appears under **Site Pairs** on the Site Recovery Home tab.

How do I connect a Site Recovery Manager instance on an Azure VMware Solution SDDC to a VMware Site Recovery instance on a VMware Cloud on AWS SDDC

This use case provides instructions for connecting a Site Recovery Manager instance on an Azure VMware Solution SDDC site to a VMware Site Recovery instance on a VMware Cloud on AWS SDDC. You must use a VPN connection to access VMware Site Recovery on VMware Cloud on AWS and the Site Recovery Manager instance on Azure VMware Solution.

Verify that you have deployed Site Recovery Manager and vSphere Replication on Azure VMware Solution. See Deploy Site Recovery Manager on Azure VMware Solution.

Figure 12: Network connectivity between VMware Site Recovery on VMware Cloud on AWS and VMware Site Recovery Manager on Azure VMware Solution



Activate VMware Site Recovery

To use your Site Recovery Manager instance on an Azure VMware Solution SDDC with a VMware Site Recovery service, you must activate the VMware Site Recovery service on a VMware Cloud™ on AWS SDDC.

- Verify that you have deployed a Software-Defined Data Center (SDDC) on VMware Cloud™ on AWS.

1. Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.
2. Click your SDDC, and then click **Integrated Services**.
3. Select Site Recovery and click **Activate**.
4. Read the information on the Activate Site Recovery page and click **Activate**.

Set the NSX-T Edge Management Gateway Firewall Rules for VMware Site Recovery

To enable VMware Site Recovery on your SDDC environment that uses VMware NSX-T®, you must create firewall rules between your VMware Cloud on AWS SDDC and the Management Gateway. After the initial firewall rules configuration, you can add, edit or delete any rules as needed.

1. Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.
2. Select **Networking & Security** > **Gateway Firewall** > **Management Gateway**.
3. Click **Add New Rule**.
4. Enter the management gateway rule parameters.

   Management gateway controls management traffic that flows in and out of the SDDC.

Option	Description
Name	Enter a descriptive name for the rule.
Source	Click **Set Source** and enter or select one of the following options: • Select **Any** to allow traffic from any source address or address range. **IMPORTANT** Although you can select **Any** as the source address in a firewall rule, using **Any** as the source address in this firewall rule can enable attacks on your SDDC and might lead to compromise of your SDDC. As a best practice, configure this firewall rule to allow access only from trusted source addresses. See VMware Knowledge Base article 84154. • Select **System Defined Groups** and select one of the following source options. – **vCenter** to allow traffic from your SDDC's vCenter Server – **Site Recovery Manager** to allow traffic from your SDDC's Site Recovery Manager. – **vSphere Replication** to allow traffic from your SDDC's vSphere Replication. • Select **User Defined Groups** to enter the name and CIDR IP range of a remote network.

Option	Description
Destination	Click **Set Destination** and enter or select one of the following options: • Select **Any** to allow traffic to any destination address or address range. • Select **System Defined Groups** and select one of the following destination options. – **vCenter** to allow traffic to your SDDC's vCenter Server. – **Site Recovery Manager** to allow traffic to your SDDC's Site Recovery Manager. – **vSphere Replication** to allow traffic to your SDDC's vSphere Replication. • Select **User Defined Groups** to enter the name and CIDR IP range of a remote network.
Service	Select one of the services to apply the rule to. • HTTPS (TCP 443) applies to vCenter Server and vSphere Replication as destinations. • VMware Site Recovery SRM applies only to Site Recovery Manager as a destination. • VMware Site Recovery vSphere Replication applies only to vSphere Replication as a destination.
Action	The only action available for management gateway firewall rules is **Allow**.

5. Repeat the previous step to apply the following firewall rules for VMware Site Recovery.

Name	Source	Destination	Service	Action
Remote SRM to vCenter Server	User-Defined Group that includes the remote Site Recovery Manager IP address.	vCenter	**HTTPS (TCP 443)**	Allow
Remote VR to vCenter Server	User-Defined Group that includes the remote vSphere Replication IP address.	vCenter	**HTTPS (TCP 443)**	Allow
Remote network to SRM (SRM Server Management)	User-Defined Group that includes the remote Site Recovery Manager and vSphere Replication IP addresses.	Site Recovery Manager	**VMware Site Recovery SRM**	Allow
Remote network to VR (VM Replication)	User-Defined Group that includes the remote ESXi hosts IP addresses.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
Remote network to VR (VR Server Management)	or User-Defined Group that includes the remote Site Recovery Manager and vSphere Replication IP addresses.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow

Name	Source	Destination	Service	Action
Remote network to VR (UI and API)	User-Defined Group that includes the remote browser IP address.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
SRM (HTTPS) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote Platform Services Controller and vCenter Server IP addresses.	**Any**	Allow
VR (HTTPS) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote Platform Services Controller and vCenter Server IP addresses.	**Any**	Allow
SRM (SRM Server Management) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote Site Recovery Manager IP address.	**Any**	Allow
VR (SRM Server Management) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote Site Recovery Manager IP address.	**Any**	Allow
ESXi (VM Replication) to remote network	ESXi	Any or User-Defined Group that includes the remote vSphere Replication IP addresses (combined vSphere Replication appliance and any add-on vSphere Replication appliances).	**Any**	Allow
SRM (VR Server Management) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote vSphere Replication IP address.	**Any**	Allow
VR (VR Server Management) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote vSphere Replication IP address.	**Any**	Allow

6. Click **Publish**.

After the firewall rules are created, they are shown in the Management Gateway Edge Firewall list.

Connect the Site Recovery Manager Server Instances on the Azure VMware Solution SDDC and the VMware Cloud on AWS SDDC

Before you can protect your virtual machines between an Azure VMware Solution SDDC and a VMware Cloud on AWS SDDC and the reverse, you must connect the Site Recovery Manager Server and vSphere Replication instances on the protected and the recovery sites. This procedure is known as site pairing.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the VMware Cloud on AWS site, provide the user name and password, and click **Next**.
4. Select the vCenter Server and the services you want to pair, and click **Next**.
5. On the **Ready to complete** page, review the pairing settings, and click **Finish**.

The protected and the recovery sites are connected. The pair appears under **Site Pairs** on the Site Recovery Home tab.

Deploying Site Recovery Manager on Google Cloud VMware Engine

You can use Site Recovery Manager 8.8.x and vSphere Replication 8.8.x with Google Cloud VMware Engine.

Google Cloud VMware Engine is an infrastructure-as-a-service offering built on Google Cloud's highly performant scalable infrastructure and VMware Cloud Foundation stack. It enables a fast path to the cloud, seamlessly migrating or extending existing VMware workloads from on-premises environments to Google Cloud Platform.

You can use Site Recovery Manager 8.8.x and vSphere Replication 8.8.x to plan, test, and run the recovery of virtual machines between a protected vCenter Server on-premises site and a recovery vCenter Server site on Google Cloud VMware Engine and the reverse, or between two Google Cloud VMware Engine cloud sites.

Operational Limits of Site Recovery Manager onGoogle Cloud VMware Engine

Each Site Recovery Manager instance onGoogle Cloud VMware Engine can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries.

Protection and Recovery Maximums for Site Recovery Manager

Table 61: Protection and Recovery Maximums for Site Recovery Manager

Item	Maximum
Total number of protected virtual machines per SDDC onGoogle Cloud VMware Engine	4000 **NOTE** To achieve the 4000 virtual machines scale, you must manually balance the replications between the different vSphere Replication nodes. You must manually add additional vSphere Replication servers to your environments, see *Deploying Additional vSphere Replication Servers* in the *vSphere Replication Administration* guide.
Maximum number of protected virtual machines pervSphere Replication appliance (through embeddedvSphere Replication server).	400
Maximum number of protected virtual machines pervSphere Replication server.	400

Item	Maximum
Total number of virtual machines per protection group	500
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Total number of virtual machines per recovery plan	2000
Total number of virtual machine recoveries that you can start simultaneously across multiple recovery plans	2000

Bidirectional Protection

If you establish a bidirectional protection, in which site B serves as the recovery site for site A and at the same time site A serves as the recovery site for site B, limits apply across both sites, and not per site. In a bidirectional implementation, you can protect a different number of virtual machines on each site, but the total number of protected virtual machines across both sites cannot exceed the limits.

For example, if you protect 2600 virtual machines usingvSphere Replication from site A to site B, you can use vSphere Replication to protect a maximum of 1400 virtual machines from site B to site A. If you are usingvSphere Replication for a bidirectional protection, you can protect a maximum of 4000 virtual machines across both sites.

IP Customization Maximums for Site Recovery Manager

If you implement IP customization for recovered virtual machines, you can configure a maximum of one IP address for each NIC, using DHCP, static IPv4, or static IPv6. For static IPv4 or IPv6 addresses, you provide the following information per NIC:

- 1 IP address
- Subnet information
- 1 gateway server address
- 2 DNS servers (primary and secondary)

You also set 2 WINS addresses for DHCP or IPv4, on Windows virtual machines only.

Recovery Point Objective lower than 15 minutes

For information about Recovery Point Objective (RPO) lower than 15 minutes, see *Recovery Point Objective* in the *vSphere Replication Administration* guide.

Setting Up Site Recovery Manager on Google Cloud VMware Engine

To ensure a successful vSphere Replication and Site Recovery Manager deployments, follow the sequence of tasks required.

Setting up your private cloud environment

You can use your Google Cloud VMware Engine private cloud as a disaster recovery site for your on-premises site.

1. Create a private cloud in the VMware Engine portal. See Creating a private cloud in the *Google Cloud VMware Engine documentation*.
2. Set up private cloud networking for Site Recovery Manager. See Creating a subnet in the *Google Cloud VMware Engine documentation*.
3. Set up the on-premises to cloud connectivity. You must use a site-to-site VPN or Cloud Interconnect. For more information, see the Google Cloud Cloud VPN documentation and the Google Cloud Cloud Interconnect documentation.

4. Set up the infracstructure services in your private cloud. For more information, see Configuring disaster recovery using SRM in the *Google Cloud VMware Egine documentation*.

Setting up vSphere Replication and Site Recovery Manager on your Google Cloud VMware Engine private cloud

1. Prepare a solution user account for installation. See Using solution user accounts in the *Google Cloud VMware Egine documentation*.
2. Deploy the
   vSphere Replication
   appliance on your private cloud. The procedure is the same as installing
   vSphere Replication
   on your on-premises site. See *Installing and Setting Up vSphere Replication* in the *vSphere Replication Administration* guide.
3. Configure firewall rules for the vSphere Replication appliance. See Firewall tables in the *Google Cloud VMware Egine documentation*.
4. Install
   Site Recovery Manager
   on your private cloud. The procedure is the same as the procedure for the on-premises installation. See *Deploy the Site Recovery Manager Appliance* in *Site Recovery Manager Installation and Configuration*.
5. Configure firewall rules for the Site Recovery Manager appliance. See Firewall tables in the *Google Cloud VMware Egine documentation*.
6. Connect the Site Recovery Manager Instances on the Protected and Recovery Sites.
7. Install the
   Site Recovery Manager
   License Key. See *Install the Site Recovery Manager License Key* in *Site Recovery Manager Installation and Configuration*.

Connect the Site Recovery Manager Instances on the Protected and Recovery Sites

Before you can use Site Recovery Manager on Google Cloud VMware Engine, you must connect the Site Recovery Manager Server instances on the protected and recovery sites. This is known as site pairing.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.

   The address that you provide for the Platform Services Controller must be an exact match of the of address that you provided when you installed Site Recovery Manager Server on the recovery site.

   IMPORTANT
   To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
4. Select the vCenter Server and the services you want to pair, and click **Next**.
5. On the **Ready to complete** page, review the pairing settings, and click **Finish**.

The protected and the recovery sites are connected. The pair appears under **Site Pairs** on the Site Recovery Home tab.

How do I connect a Site Recovery Manager instance on a Google Cloud VMware Engine SDDC to a VMware Site Recovery instance on a VMware Cloud on AWS SDDC

This use case provides instructions for connecting a Site Recovery Manager instance on a Google Cloud VMware Engine SDDC site to a VMware Site Recovery instance on a VMware Cloud on AWS SDDC. You must use a VPN connection to access VMware Site Recovery on VMware Cloud on AWS and the Site Recovery Manager instance on Google Cloud VMware Engine.

Verify that you have deployed Site Recovery Manager and vSphere Replication on Google Cloud VMware Engine. See Setting Up Site Recovery Manager on Google Cloud VMware Engine.

Activate VMware Site Recovery

To use your Site Recovery Manager instance on an Google Cloud VMware Engine SDDC with a VMware Site Recovery service, you must activate the VMware Site Recovery service on a VMware Cloud™ on AWS SDDC.

- Verify that you have deployed a Software-Defined Data Center (SDDC) on VMware Cloud on AWS.

1. Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.
2. Click your SDDC, and then click **Integrated Services**.
3. Select Site Recovery and click **Activate**.
4. Read the information on the Activate Site Recovery page and click **Activate**.

Set the NSX-T Edge Management Gateway Firewall Rules for VMware Site Recovery

To enable VMware Site Recovery on your SDDC environment that uses VMware NSX-T®, you must create firewall rules between your VMware Cloud on AWS SDDC and the Management Gateway. After the initial firewall rules configuration, you can add, edit or delete any rules as needed.

1. Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.
2. Select **Networking & Security** > **Gateway Firewall** > **Management Gateway**.
3. Click **Add New Rule**.
4. Enter the management gateway rule parameters.

   Management gateway controls management traffic that flows in and out of the SDDC.

Option	Description
Name	Enter a descriptive name for the rule.
Source	Click **Set Source** and enter or select one of the following options: • Select **Any** to allow traffic from any source address or address range. **IMPORTANT** Although you can select **Any** as the source address in a firewall rule, using **Any** as the source address in this firewall rule can enable attacks on your SDDC and might lead to compromise of your SDDC. As a best practice, configure this firewall rule to allow access only

Option	Description
	from trusted source addresses. See VMware Knowledge Base article 84154. • Select **System Defined Groups** and select one of the following source options. – **vCenter** to allow traffic from your SDDC's vCenter Server – **Site Recovery Manager** to allow traffic from your SDDC's Site Recovery Manager. – **vSphere Replication** to allow traffic from your SDDC's vSphere Replication. • Select **User Defined Groups** to enter the name and CIDR IP range of a remote network.
Destination	Click **Set Destination** and enter or select one of the following options: • Select **Any** to allow traffic to any destination address or address range. • Select **System Defined Groups** and select one of the following destination options. – **vCenter** to allow traffic to your SDDC's vCenter Server. – **Site Recovery Manager** to allow traffic to your SDDC's Site Recovery Manager. – **vSphere Replication** to allow traffic to your SDDC's vSphere Replication. • Select **User Defined Groups** to enter the name and CIDR IP range of a remote network.
Service	Select one of the services to apply the rule to. • HTTPS (TCP 443) applies to vCenter Server and vSphere Replication as destinations. • VMware Site Recovery SRM applies only to Site Recovery Manager as a destination. • VMware Site Recovery vSphere Replication applies only to vSphere Replication as a destination.
Action	The only action available for management gateway firewall rules is **Allow**.

5. Repeat the previous step to apply the following firewall rules for VMware Site Recovery.

Name	Source	Destination	Service	Action
Remote SRM to vCenter Server	User-Defined Group that includes the remote Site Recovery Manager IP address.	vCenter	**HTTPS (TCP 443)**	Allow
Remote VR to vCenter Server	User-Defined Group that includes the remote vSphere Replication IP address.	vCenter	**HTTPS (TCP 443)**	Allow

Name	Source	Destination	Service	Action
Remote network to SRM (SRM Server Management)	User-Defined Group that includes the remote Site Recovery Manager and vSphere Replication IP addresses.	Site Recovery Manager	**VMware Site Recovery SRM**	Allow
Remote network to VR (VM Replication)	User-Defined Group that includes the remote ESXi hosts IP addresses.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
Remote network to VR (VR Server Management)	or User-Defined Group that includes the remote Site Recovery Manager and vSphere Replication IP addresses.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
Remote network to VR (UI and API)	User-Defined Group that includes the remote browser IP address.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
SRM (HTTPS) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote Platform Services Controller and vCenter Server IP addresses.	**Any**	Allow
VR (HTTPS) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote Platform Services Controller and vCenter Server IP addresses.	**Any**	Allow
SRM (SRM Server Management) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote Site Recovery Manager IP address.	**Any**	Allow
VR (SRM Server Management) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote Site Recovery Manager IP address.	**Any**	Allow
ESXi (VM Replication) to remote network	ESXi	Any or User-Defined Group that includes the remote vSphere Replication IP addresses (combined vSphere Replication appliance and any add-on vSphere Replication appliances).	**Any**	Allow
SRM (VR Server Management) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote vSphere Replication IP address.	**Any**	Allow

Name	Source	Destination	Service	Action
VR (VR Server Management) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote vSphere Replication IP address.	**Any**	Allow

6. Click **Publish**.

After the firewall rules are created, they are shown in the Management Gateway Edge Firewall list.

Connect the Site Recovery Manager Server instances on the Google Cloud VMware Engine SDDC and the VMware Cloud on AWS SDDC

Before you can protect your virtual machines between an Google Cloud VMware Engine SDDC and a VMware Cloud on AWS SDDC and the reverse, you must connect the Site Recovery Manager Server and vSphere Replication instances on the protected and the recovery sites. This procedure is known as site pairing.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the VMware Cloud on AWS site, provide the user name and password, and click **Next**.
4. Select the vCenter Server and the services you want to pair, and click **Next**.
5. On the **Ready to complete** page, review the pairing settings, and click **Finish**.

The protected and the recovery sites are connected. The pair appears under **Site Pairs** on the Site Recovery Home tab.

Deploying Site Recovery Manager on Oracle Cloud VMware Solution

You can use Site Recovery Manager 8.8.x and vSphere Replication 8.8.x with Oracle Cloud VMware Solution.

Oracle Cloud VMware Solution integrates VMware on-premises tools, skillsets, and processes with public Oracle Cloud services. The solution is a fully customer-managed, customer-operated native VMware cloud environment based on VMware Validated Solutions for use with the public Oracle Cloud Infrastructure.

You can use Site Recovery Manager 8.8.x and vSphere Replication 8.8.x to plan, test, and run the recovery of virtual machines between a protected vCenter Server on-premises site and a recovery vCenter Server site on Oracle Cloud VMware Solution and the reverse, or between two Oracle Cloud VMware Solution cloud sites.

Operational Limits of Site Recovery Manager onOracle Cloud VMware Solution

Each Site Recovery Manager instance onOracle Cloud VMware Solution can support a certain number of protected virtual machines, protection groups, recovery plans, and concurrent recoveries.

Protection and Recovery Maximums for Site Recovery Manager

Table 62: Protection and Recovery Maximums for Site Recovery Manager

Item	Maximum
Total number of protected virtual machines per SDDC onOracle Cloud VMware Solution	4000 **NOTE** To achieve the 4000 virtual machines scale, you must manually balance the replications between the different vSphere Replication nodes. You must manually add additional vSphere Replication servers to your environments, see *Deploying Additional vSphere Replication Servers* in the *vSphere Replication Administration* guide.
Maximum number of protected virtual machines pervSphere Replication appliance (through embeddedvSphere Replication server).	400
Maximum number of protected virtual machines pervSphere Replication server.	400
Total number of virtual machines per protection group	500
Total number of recovery plans	250
Total number of protection groups per recovery plan	250
Total number of virtual machines per recovery plan	2000
Total number of virtual machine recoveries that you can start simultaneously across multiple recovery plans	2000

Bidirectional Protection

If you establish a bidirectional protection, in which site B serves as the recovery site for site A and at the same time site A serves as the recovery site for site B, limits apply across both sites, and not per site. In a bidirectional implementation, you can protect a different number of virtual machines on each site, but the total number of protected virtual machines across both sites cannot exceed the limits.

For example, if you protect 2600 virtual machines usingvSphere Replication from site A to site B, you can use vSphere Replication to protect a maximum of 1400 virtual machines from site B to site A. If you are usingvSphere Replication for a bidirectional protection, you can protect a maximum of 4000 virtual machines across both sites.

IP Customization Maximums for Site Recovery Manager

If you implement IP customization for recovered virtual machines, you can configure a maximum of one IP address for each NIC, using DHCP, static IPv4, or static IPv6. For static IPv4 or IPv6 addresses, you provide the following information per NIC:

- 1 IP address
- Subnet information
- 1 gateway server address
- 2 DNS servers (primary and secondary)

You also set 2 WINS addresses for DHCP or IPv4, on Windows virtual machines only.

Recovery Point Objective lower than 15 minutes

For information about Recovery Point Objective (RPO) lower than 15 minutes, see*Recovery Point Objective* in the *vSphere Replication Administration* guide.

Setting Up Site Recovery Manager on Oracle Cloud VMware Solution

To ensure a successful vSphere Replication and Site Recovery Manager deployments, follow the sequence of required tasks.

Setting up your private cloud environment

You can use your Oracle Cloud VMware Solution private cloud as a disaster recovery site for your on-premises site.

1. Deploy an Oracle Cloud VMware Solution SDDC on Oracle Cloud Infrastructure. See the Deploy a highly available VMware-based SDDC to the cloud Playbook in the *Oracle Help Center*.
2. Configure the DNS settings for your SDDC. See Configure DNS for an Oracle Cloud VMware Solution SDDC in the *Protect your VMware SDDC in the cloud against disasters* Playbook.
3. Configure the network and connectivity of your primary on-premiese site. See Configure the Primary Site in the *Protect your VMware SDDC in the cloud against disasters* Playbook.
4. Configure the Oracle Cloud VMware Solution site. For more information, see Configure the Recovery Site in the *Protect your VMware SDDC in the cloud against disasters* Playbook.
5. Pair the sites over FastConnect or IPSec VPN. For more information about FastConnect, see FastConnect in the *Oracle Cloud Infrastructure Documentation*. For more information about IPSec VPN, see Site-to-Site VPN in the *Oracle Cloud Infrastructure Documentation*.

Setting up vSphere Replication and Site Recovery Manager on your Oracle Cloud VMware Solution private cloud

1. Deploy the
   vSphere Replication
   appliance on your private cloud. The procedure is the same as installing
   vSphere Replication
   on your on-premises site. See *Installing and Setting Up vSphere Replication* in the *vSphere Replication Administration* guide.
2. Install
   Site Recovery Manager
   on your private cloud. The procedure is the same as the procedure for the on-premises installation. See *Deploy the Site Recovery Manager Appliance* in the *Site Recovery Manager Installation and Configuration*.
3. Connect the Site Recovery Manager Instances on the Protected and Recovery Sites.
4. See *Install the Site Recovery Manager License Key* in the *Site Recovery Manager Installation and Configuration*.

For more information about the architecture and the different use cases, see Learn About Protecting your VMware SDDC in the Cloud Against Disasters in the *Protect your VMware SDDC in the cloud against disasters* Playbook.

Connect the Site Recovery Manager Instances on the Protected and Recovery Sites

Before you can use Site Recovery Manager on Oracle Cloud VMware Solution, you must connect the Site Recovery Manager Server instances on the protected and recovery sites. This is known as site pairing.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the second site, provide the user name and password, and click **Next**.

   The address that you provide for the Platform Services Controller must be an exact match of the of address that you provided when you installed Site Recovery Manager Server on the recovery site.

   IMPORTANT
   To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
4. Select the vCenter Server and the services you want to pair, and click **Next**.
5. On the **Ready to complete** page, review the pairing settings, and click **Finish**.

The protected and the recovery sites are connected. The pair appears under **Site Pairs** on the Site Recovery Home tab.

How do I connect a Site Recovery Manager instance on an Oracle Cloud VMware Solution SDDC to a VMware Site Recovery instance on a VMware Cloud on AWS SDDC

This use case provides instructions for connecting a Site Recovery Manager instance on an Oracle Cloud VMware Solution SDDC site to a VMware Site Recovery instance on a VMware Cloud on AWS SDDC. You must use a VPN connection to access VMware Site Recovery on VMware Cloud on AWS and the Site Recovery Manager instance on Oracle Cloud VMware Solution.

Verify that you have deployed Site Recovery Manager and vSphere Replication on Oracle Cloud VMware Solution. See Setting Up Site Recovery Manager on Oracle Cloud VMware Solution.

Activate VMware Site Recovery

To use your Site Recovery Manager instance on an Oracle Cloud VMware Solution SDDC with a VMware Site Recovery service, you must activate the VMware Site Recovery service on a VMware Cloud™ on AWS SDDC.

- Verify that you have deployed a Software-Defined Data Center (SDDC) on VMware Cloud™ on AWS.

1. Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.
2. Click your SDDC, and then click **Integrated Services**.
3. Select Site Recovery and click **Activate**.
4. Read the information on the Activate Site Recovery page and click **Activate**.

Set the NSX-T Edge Management Gateway Firewall Rules for VMware Site Recovery

To enable VMware Site Recovery on your SDDC environment that uses VMware NSX-T®, you must create firewall rules between your VMware Cloud on AWS SDDC and the Management Gateway. After the initial firewall rules configuration, you can add, edit or delete any rules as needed.

1. Log in to the VMware Cloud on AWS Console at https://vmc.vmware.com.
2. Select **Networking & Security** > **Gateway Firewall** > **Management Gateway**.
3. Click **Add New Rule**.
4. Enter the management gateway rule parameters.

   Management gateway controls management traffic that flows in and out of the SDDC.

Option	Description
Name	Enter a descriptive name for the rule.
Source	Click **Set Source** and enter or select one of the following options: • Select **Any** to allow traffic from any source address or address range. **IMPORTANT** Although you can select **Any** as the source address in a firewall rule, using **Any** as the source address in this firewall rule can enable attacks on your SDDC and might lead to compromise of your SDDC. As a best practice, configure this firewall rule to allow access only from trusted source addresses. See VMware Knowledge Base article 84154. • Select **System Defined Groups** and select one of the following source options. – **vCenter** to allow traffic from your SDDC's vCenter Server – **Site Recovery Manager** to allow traffic from your SDDC's Site Recovery Manager. – **vSphere Replication** to allow traffic from your SDDC's vSphere Replication. • Select **User Defined Groups** to enter the name and CIDR IP range of a remote network.

Option	Description
Destination	Click **Set Destination** and enter or select one of the following options: • Select **Any** to allow traffic to any destination address or address range. • Select **System Defined Groups** and select one of the following destination options. – **vCenter** to allow traffic to your SDDC's vCenter Server. – **Site Recovery Manager** to allow traffic to your SDDC's Site Recovery Manager. – **vSphere Replication** to allow traffic to your SDDC's vSphere Replication. • Select **User Defined Groups** to enter the name and CIDR IP range of a remote network.
Service	Select one of the services to apply the rule to. • HTTPS (TCP 443) applies to vCenter Server and vSphere Replication as destinations. • VMware Site Recovery SRM applies only to Site Recovery Manager as a destination. • VMware Site Recovery vSphere Replication applies only to vSphere Replication as a destination.
Action	The only action available for management gateway firewall rules is **Allow**.

5. Repeat the previous step to apply the following firewall rules for VMware Site Recovery.

Name	Source	Destination	Service	Action
Remote SRM to vCenter Server	User-Defined Group that includes the remote Site Recovery Manager IP address.	vCenter	**HTTPS (TCP 443)**	Allow
Remote VR to vCenter Server	User-Defined Group that includes the remote vSphere Replication IP address.	vCenter	**HTTPS (TCP 443)**	Allow
Remote network to SRM (SRM Server Management)	User-Defined Group that includes the remote Site Recovery Manager and vSphere Replication IP addresses.	Site Recovery Manager	**VMware Site Recovery SRM**	Allow
Remote network to VR (VM Replication)	User-Defined Group that includes the remote ESXi hosts IP addresses.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
Remote network to VR (VR Server Management)	or User-Defined Group that includes the remote Site Recovery Manager and vSphere Replication IP addresses.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow

Name	Source	Destination	Service	Action
Remote network to VR (UI and API)	User-Defined Group that includes the remote browser IP address.	vSphere Replication	**VMware Site Recovery vSphere Replication**	Allow
SRM (HTTPS) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote Platform Services Controller and vCenter Server IP addresses.	**Any**	Allow
VR (HTTPS) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote Platform Services Controller and vCenter Server IP addresses.	**Any**	Allow
SRM (SRM Server Management) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote Site Recovery Manager IP address.	**Any**	Allow
VR (SRM Server Management) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote Site Recovery Manager IP address.	**Any**	Allow
ESXi (VM Replication) to remote network	ESXi	Any or User-Defined Group that includes the remote vSphere Replication IP addresses (combined vSphere Replication appliance and any add-on vSphere Replication appliances).	**Any**	Allow
SRM (VR Server Management) to remote network	Site Recovery Manager	Any or User-Defined Group that includes the remote vSphere Replication IP address.	**Any**	Allow
VR (VR Server Management) to remote network	vSphere Replication	Any or User-Defined Group that includes the remote vSphere Replication IP address.	**Any**	Allow

6. Click **Publish**.

After the firewall rules are created, they are shown in the Management Gateway Edge Firewall list.

Connect the Site Recovery Manager Server instances on the Oracle Cloud VMware Solution SDDC and the VMware Cloud on AWS SDDC

Before you can protect your virtual machines between an Oracle Cloud VMware Solution SDDC and a VMware Cloud on AWS SDDC and the reverse, you must connect the Site Recovery Manager Server and vSphere Replication instances on the protected and the recovery sites. This procedure is known as site pairing.

1. In the vSphere Client, click **Site Recovery** > **Open Site Recovery**.
2. Click the **New Site Pair** button.
3. Select the first site from the list. Enter the address of the Platform Services Controller for the Site Recovery Manager Server on the VMware Cloud on AWS site, provide the user name and password, and click **Next**.
4. Select the vCenter Server and the services you want to pair, and click **Next**.
5. On the **Ready to complete** page, review the pairing settings, and click **Finish**.

The protected and the recovery sites are connected. The pair appears under **Site Pairs** on the Site Recovery Home tab.

Using the VMware Aria Automation Orchestrator Plug-In for VMware Site Recovery Manager 8.8

Information and instructions about configuring and using the Automation Orchestrator plug-in for Site Recovery Manager.

Using the Site Recovery Manager Plug-In

Using the VMware Aria Automation Orchestrator Plug-In for VMware Site Recovery Manager 8.8 guide provides information and instructions about configuring and using the VMware®VMware Aria Automation Orchestrator plug-in for VMware Site Recovery Manager.

Intended Audience

The information in *Using the VMware Aria Automation Orchestrator Plug-In for VMware Site Recovery Manager* 8.8 guide is intended for experienced administrators who want to automate protection and recovery configuration tasks on a vSphere environment using the Site Recovery Manager plug-in. The information is written for experienced users who are familiar with virtual machine technology, with VMware Aria Automation Orchestrator workflow development, and with VMware Site Recovery Manager.

For more information about VMware Aria Automation Orchestrator, see the *VMware Aria Automation Orchestrator Documentation*.

For more information about Site Recovery Manager, see the *VMware Site Recovery Manager Documentation*.

Automated Operations That the VMware Aria Automation Orchestrator Plug-In for Site Recovery Manager Provides

With VMware Aria Automation Orchestrator plug-in for VMware Site Recovery Manager, you can use VMware Aria Automation Orchestrator to automate the creation of your Site Recovery Manager infrastructure to manage resource mappings between sites, configure protection groups and recovery plans, add virtual machines to protection groups, configure recovery settings of virtual machines, and run recoveries.

You can use the VMware Aria Automation Orchestrator plug-in for VMware Site Recovery Manager to protect virtual machines by adding them to array-based replication, vSphere Replication or to Virtual Volumes protection groups. The plug-in does not automate the configuration of vSphere Replication on virtual machines. You can use the VMware Aria Automation Orchestrator Plug-In for vSphere Replication to configure vSphere Replication on virtual machines, or configure vSphere Replication manually. For information about the VMware Aria Automation Orchestrator Plug-In for vSphere Replication, see the release notes of the VMware Aria Automation Orchestrator Plug-In for vSphere Replication.

The VMware Aria Automation Orchestrator plug-in for VMware Site Recovery Manager includes VMware Aria Automation Orchestrator actions, workflows, policy templates to trigger actions when certain events occur, and scripting objects to expose selected elements of the Site Recovery Manager API to workflows.

The plug-in provides workflows to configure local and remote sites, to remove local sites, and to log in to remote site.

> **NOTE**
> The workflows to configure local and remote sites assume that the VMware Aria Automation Orchestrator trust store already contains the local site infrastructure node SSL certificate and the local site vCenter Server SSL certificate. In an embedded configuration, the VMware Aria Automation Orchestrator trust store contains only one certificate. You must rerun the appropriate workflows if an administrator updates any of the SSL certificates.

The plug-in provides actions and workflows to manage inventory mappings in Site Recovery Manager infrastructure:

- Add, get, or remove Folder Mapping.
- Add, get, or remove Network Mapping.
- Add, get, or remove Resource Mapping.
- Add, get, or remove Test Network Mapping.
- Add or remove IP customization rules.

The plug-in provides actions and workflows that manage and configure protection groups:

- Create, list, move, or remove protection groups for array-based replication, vSphere Replication or Virtual Volumes.
- Create or move protection group folder.
- Add or remove replicated virtual machines from vSphere Replication protection groups.
- Protect or unprotect virtual machines.
- Protect all virtual machines associated with a protection group.
- Protect virtual machines with custom inventory mappings.
- List protected datastores.
- Update group datastores.
- Get unassigned replicated datastores.
- Find array-based replication protection group by datastore.
- Add and remove datastores in an array-based replication protection group.

The plug-in provides actions and workflows that manage and configure recovery plans:

- Create, move, or delete recovery plan.
- Create or move recovery plan folder.
- Delete callouts.
- Add to or remove protection group from recovery plan.
- Add to or remove test network mapping from recovery plan.
- Configure virtual machine recovery settings.
- List recovery plans and get recovery plan state.
- Set VM recovery settings,
- Set IP settings.
- Delete pre and post power-on custom recovery settings for a virtual machine.
- Initiate:
  - Test recovery plan
  - Cleanup recovery plan
  - Failover recovery plan
  - Reprotect recovery plan
  - Cancel recovery plan
  - Planned migration recovery plan

    NOTE
    When the plug-in starts a test, cleanup, failover, reprotect, planned migration, or cancel recovery plan, it performs an initial check on the recovery plan state. The workflow then succeeds or fails but does not provide information on the progress of the operation. You can monitor the plan progress in vSphere Web Client.

The plug-in provides actions and workflows for storage operations:

- Add, get, and remove placeholder datastores.
- Discover replicated devices.

The plug-in provides sample automated actions and workflows:

- Convert single or multiple virtual machines to UnassignedReplicatedVM.
- Create an array-based protection group, protect existing virtual machines, and add to a recovery plan.
- Create and protect a virtual machine.

Installing the Site Recovery Manager Plug-In

To create and run workflows on the protected and recovery Site Recovery Manager sites, you must install and configure the Site Recovery Manager plug-in in VMware Aria Automation Orchestrator.

Site Recovery Manager Plug-In Functional Prerequisites

To install and use the Site Recovery Manager plug-in, your system must meet certain functional prerequisites.

Site Recovery Manager

Your Site Recovery Manager plug-in version works only with the corresponding Site Recovery Manager version.

For information about the compatibility between the Site Recovery Manager plug-in and Site Recovery Manager, see *VMware Aria Automation Orchestrator plug-in for VMware Site Recovery Manager 8.8 Release Notes*.

For information about setting up Site Recovery Manager, see the *Site Recovery Manager Installation and Configuration* documentation.

VMware Aria Automation Orchestrator

Verify that you have a running instance of VMware Aria Automation Orchestrator and its version is compatible with the versions of your Site Recovery Manager, and Site Recovery Manager plug-in.

For information about the compatibility between Site Recovery Manager and VMware Aria Automation Orchestrator, see the *VMware Aria Automation Orchestrator plug-in for VMware Site Recovery Manager 8.8 Release Notes* and *Compatibility Matrices for Site Recovery Manager 8.8* documentation.

For information about setting up VMware Aria Automation Orchestrator, logging in the VMware Aria Automation Orchestrator client, and available authentication methods, see the *Installing and Configuring VMware VMware Aria Automation Orchestrator* documentation.

Other Prerequisites

Verify the compatibility between the vCenter Server plug-in for VMware Aria Automation Orchestrator and the vCenter Server. See the *VMware Aria Automation Orchestrator 8.9.x Release Notes* .

Installing, Upgrading, and Uninstalling the Site Recovery Manager Plug-In

You can use the Site Recovery Manager plug-in after you install it on an VMware Aria Automation Orchestrator instance. The version of the Site Recovery Manager plug-in must be compatible with your Site Recovery Manager and VMware Aria Automation Orchestrator.

Installing the Site Recovery Manager Plug-In

You can install the Site Recovery Manager plug-in if your Site Recovery Manager sites are paired and your VMware Aria Automation Orchestrator instance is configured to work with your vSphere environment.

You must configure VMware Aria Automation Orchestrator to use the vSphere environment. For information about how to configure your VMware Aria Automation Orchestrator to work with a vSphere environment, see the *Configuring*

VMware Aria Automation Orchestrator section in the *Installing and Configuring VMware Aria Automation Orchestrator* documentation.

You can download the Site Recovery Manager plug-in installation `.vmoapp` file from the download page of Site Recovery Manager.

You can install the Site Recovery Manager plug-in by using the `http://your_orchestrator_host/vco-controlcenter/config/#/` configuration interface. For information about how to install the `.vmoapp` file on your VMware Aria Automation Orchestrator instance, see the *Manage the Orchestrator Plug-Ins* topic in the *Installing and Configuring VMware Aria Automation Orchestrator* documentation.

Upgrading and Uninstalling the Site Recovery Manager Plug-In

You can upgrade your Site Recovery Manager plug-in by uninstalling your plug-in and installing the new version.

You can uninstall your Site Recovery Manager plug-in by using the `http://your_orchestrator_host/vco-controlcenter/config/#/` configuration interface. For more information about how to uninstall your Site Recovery Manager plug-in, see the *Uninstall a Plug-in* topic in the *Installing and Configuring VMware Aria Automation Orchestrator* documentation.

Using the Site Recovery Manager Plug-In Workflows

The Site Recovery Manager plug-in workflow library contains workflows that you can use to automate Site Recovery Manager tasks. With the predefined workflows you can run tests and cleanup, run recoveries and reprotect, and cancel recovery plans. You can use the predefined workflows to create custom workflows.

You can use the **Inventory** view in the VMware Aria Automation Orchestrator client to manage the available Site Recovery Manager resources. You can use the scripting API of the plug-in to create custom workflows.

Available Workflows in Site Recovery Manager Plug-In

Site Recovery Manager plug-in provides Configuration, Inventory Mappings, Protection Groups, and Storage workflows.

Table 63: Configuration workflows

Workflow	Description of Operation
Configure Local Sites	Gets a Site Recovery Manager URL, validates connection, imports certificate, and registers the local sites associated with the local or provided Platform Services Controller.
Configure Remote Site	Gets a remote lookup service URL, imports a certificate, gets a remote vCenter Server URL, and imports a certificate.
Configure SRM plugin Connection Settings	Configures the Site Recovery Manager plug-in connection settings.
Login Remote Site	Logs in to a remote site.
Remove Local Sites	Removes a local site.

Table 64: Inventory Mapping workflows

Workflow	Description of Operation
Add Folder Mapping	Adds a folder mapping between paired sites.
Add Network Mapping	Adds a network mapping between paired sites.
Add Resource Mapping	Adds a resource pool mapping between paired sites.

Workflow	Description of Operation
Add Test Network Mapping	Adds a test network mapping to a remote site.
Get Folder Mapping Pairs	Lists the data centers or virtual machine folders on the local site that have existing mapping between the corresponding objects (pairs).
Get Folder Mappings	Lists the folder mappings for a local site.
Get Network Mapping Pairs	Lists the networks on the local site that have existing mapping between the corresponding objects (pairs).
Get Network Mappings	Lists the network mappings for a local site.
Get Resource Mapping Pairs	Lists the resources on the local site that have existing mapping between the corresponding objects (pairs).
Get Resource Mappings	Lists the resource mappings for a local site.
Get Test Network Mapping Pairs	Lists the networks that have existing mappings between the corresponding objects (pairs) to test networks on the remote site.
Get Test Network Mappings	Lists the test network mappings for a remote site.
Remove Folder Mapping	Removes a folder mapping from a local site.
Remove Network Mapping	Removes a network mapping from a local site.
Remove Resource Mapping	Removes a resource mapping from a local site.
Remove Test Network Mapping	Removes a remote test network mapping.

Table 65: IP Customization workflows

Workflow	Description of Operation
Add IP Customization Rules	Customizes a previously created network mapping.
Remove IP Customization Rules	Removes a customization for previously created network mapping.

Table 66: Protection Group workflows

Workflow	Description of Operation
Add Replicated VM to vSphere Replication Protection Group	Adds a selected replicated virtual machine to an existing vSphere Replication protection group.
Create Protection Group Folder	Creates a protection group folder.
Create Protection Group for Array Based Replication	Creates an array-based replication protection group based on unassigned replicated datastore.
Create Protection Group for vSphere Replication	Creates a vSphere Replication protection group and adds virtual machines to the protection group.
Create a vVol Protection Group	Creates a vVol protection group and adds vVol replication groups to a protection group.
Find ABR Protection Group by Datastore	Lists the array-based replication protection group that protects the selected datastore.
Get Unassigned Replicated Datastores	Lists the unassigned replicated datastores on a local site.
List Protected Datastores	Lists the replicated datastores in a protection group.
List Protection Groups	Lists the protection groups on a local site.
List Replication Groups in vVol Protection Group	Lists the replication groups which are part of a vVol protection group.

Workflow	Description of Operation
List Virtual Machines in a vVol Replication Group	Lists the virtual machines, which are part of a vVol replication group.
Move Protection Group	Moves a protection group to a destination folder.
Move Protection Group Folder	Moves a particular protection group folder to a different destination folder.
Protect All Unprotected Virtual Machines Associated with Protection Group	Enables a protection for all unprotected virtual machines members of a protection group.
Protect Virtual Machine	Enables a protection for unprotected virtual machine member of a protection group.
Protect Virtual Machine with Custom Inventory Mappings	Sets the custom inventory mappings for an individual virtual machine in a protection group.
Remove Protection Group	Removes a protection group.
Remove Protection Group Folder	Remove an empty protection group folder.
Remove Replicated VM from vSphere Replication Protection Group	Removes a selected virtual machine from vSphere Replication protection group.
Unprotect Virtual Machines	Disables the protection for the selected virtual machines.
Update Group Datastore	Adds or removes datastores in an array-based replication protection group.

Table 67: Recovery Plan workflows

Workflow	Description of Operation
Add Protection Group to Recovery Plan	Adds a protection group to a recovery plan.
Add Test Network Mapping to Recovery Plan	Adds a test network mapping to a recovery plan.
Create Recovery Plan	Creates a recovery plan.
Create Recovery Plan Folder	Creates a recovery plan folder.
Delete Callouts	Deletes a pre and post power-on custom recovery settings for a virtual machine.
Delete Recovery Plan	Deletes a recovery plan.
Get Recovery Plan State	Lists a recovery plan state.
Initiate Cancel Recovery Plan	Cancels a running recovery plan.
Initiate Cleanup Recovery Plan	Clean ups a recovery plan after a test.
Initiate Failover Recovery Plan	Starts a fail over to recovery site process.
Initiate Planned Migration Recovery Plan	Starts a planned migration to recovery site.
Initiate Reprotect Recovery Plan	Starts a reprotect of site and reverses the protection.
Initiate Test Recovery Plan	Starts a test of recovery plan.
List Recovery Plans	Lists recovery plans.
Move Recovery Plan	Moves a recovery plan to a destination folder.
Move Recovery Plan Folder	Moves a particular recovery plan folder to a different destination folder.
Remove Protection Group from Recovery Plan	Removes a protection group from a recovery plan.
Remove Recovery Plan Folder	Removes a recovery plan folder.
Remove Test Network Mapping from Recovery Plan	Removes a test network mapping from a recovery plan.

Workflow	Description of Operation
Set IP Settings	A nested workflow that cannot be run independently. It is called as part of the **Set VM Recovery Settings** workflow.
Set VM Recovery Settings	Sets a priority group, power state, pre power on commands and prompts, and post power on commands and prompts for a virtual machine in a recovery plan.

Table 68: Storage workflows

Workflow	Description of Operation
Add Placeholder Datastores	Adds placeholder datastores for Site Recovery Manager to use to store placeholder virtual machines on the recovery site.
Discover Replicated Devices	Initiates discover replicated devices operation for all available array pairs.
Get Placeholder Datastores	Lists all the placeholder datastores in the selected site.
Remove Placeholder Datastores	Removes placeholder datastores.

Prerequisites for Using the Site Recovery Manager Plug-In

To use the Site Recovery Manager plug-in, your environment must meet certain requirements.

- Verify that you have server instances installed on both sites and that they are paired.
- Verify that your VMware Aria Automation Orchestrator instance is configured to work with the vSphere infrastructure. For information about how to configure your VMware Aria Automation Orchestrator to work with a vSphere environment, see the *Configuring VMware Aria Automation Orchestrator* section in the *Installing and Configuring VMware Aria Automation Orchestrator* documentation.

Configuration Workflows

Configuration workflows register information about vCenter Server and Site Recovery Manager topology including lookup services, authentication providers, and platform services controllers.

Configuration workflows are a functional prerequisite - before running workflows from the inventory tree you must run Configure Local Sites, Configure Remote Site, and Login Remote Site workflows.

Configure Local Sites

The workflow registers Site Recovery Manager sites with the plug-in to provide access to the Site Recovery Manager and vCenter Server inventory.

Verify that your vCenter Server is registered with your VMware Aria Automation Orchestrator client. If vCenter Server is not registered with VMware Aria Automation Orchestrator, the plug-in is unable to get the Site Recovery Manager URL and cannot import the Site Recovery Manager certificate.

> **NOTE**
> For information about how to configure your Site Recovery Manager to work with a vSphere environment, see the *Configuring VMware Aria Automation Orchestrator* section in the *Installing and Configuring VMware Aria Automation Orchestrator* documentation.

Registering a Site Recovery Manager site as a local site in the plug-in defines the functional direction of workflows for that site. For example, running inventory mapping workflows on a local site maps inventory objects from the local sites to inventory objects on the remote site.

You can register as local sites both Site Recovery Manager protected and recovery sites in a single VMware Aria Automation Orchestrator instance. To do that, you must register both vCenter Server instances with the VMware Aria Automation Orchestrator client. You can then run the rest of the available workflows from the chosen direction for both sites from a single VMware Aria Automation Orchestrator client.

You can run the workflow again on the same vCenter Server instance to change the user name or password you want to use. After that the other workflows in the plug-in will use the updated credentials.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Configure Local Sites` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 69: Configure Local Sites Workflow

Input		Description
Set local site properties	IP or host name of the local Platform Services Controller	IP or host name of the local vCenter Server.
	Port of the Local site	Port of the Local site (default value is set to 443).
	Path to Lookup Service	Path to Lookup Service.
	Ignore certificate warnings	When you select it, the certificate is accepted silently and added to the trusted store.
Set the connection properties	User name for the Local Site	User name for the Local Site.
	Password for the Local Site	Password for the Local Site.

Configure Remote Site

The Configure Remote Site workflow registers the paired remote Site Recovery Manager site with the VMware Aria Automation Orchestrator instance.

Verify that the local and remote Site Recovery Manager sites are paired before running this workflow.

If you have registered both the protected and the recovery sites as local sites, you must run the workflow for both sites to run workflows in both directions.

The workflow imports certificates of the remote vCenter Server or Platform Services Controller so that you can log in to the remote site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Configure Remote Site` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 70: Configure Remote Site Workflow Input

Input	Description
Local Site	Local Site Recovery Manager site.
Ignore certificate warnings	When you select it, the certificate is accepted silently and added to the trusted store.

Configure Site Recovery Manager Plug-in Connection Settings

The workflow configures the Site Recovery Manager plug-in connection settings.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Configure SRM plugin Connection Settings` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the maximum number of connections and the connection timeout, and click **Run**.
   You can view the workflow status in the **Value** column of the **Variables** tab of the workflow. You can use the value as a parameter in another workflow.

Login Remote Site

The workflow logs you to the remote site, so that you can run other Site Recovery Manager workflows.

Verify that the protected and the recovery Site Recovery Manager sites are paired.

You must run this workflow once per each VMware Aria Automation Orchestrator client session.

VMware Aria Automation Orchestrator logs out of the remote Site Recovery Manager site when you log out of the VMware Aria Automation Orchestrator client.

If you have registered the recovery and the protected sites as local sites, you must run the workflow for both sites. In case the protected and the recovery site are configured in Enhanced Linked Mode, it is not necessary to run the Login Remote Site workflow.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Login Remote Site` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 71: Mandatory Inputs for Login Remote Site Workflow

Input	Description
Local Site	Local Site Recovery Manager Site.
User name	User name for the local site.
Password	Password for the local site.

Remove Local Sites

The workflow unregisters the local Site Recovery Manager site and refreshes the internal plug-in cache. Removing a local site does not remove previously set configurations such as mappings, protection groups, and so on.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Local Sites` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 72: Remove Local Sites Workflow Inputs

Input	Description
Local Platform Services Controller	Local Platform Services Controller for which Site Recovery Manager site is added.

Inventory Mapping Workflows in Site Recovery Manager Plug-In

With inventory mappings you can configure how Site Recovery Manager maps virtual machine resources on the protected site to resources on the recovery site. Inventory mappings provide default objects in the inventory on the recovery site for the recovered virtual machines to use when you run recovery.

Site wide configured inventory mappings are used by default when creating protection groups for protected virtual machines. Array-based replication, vSphere Replication and Virtual Volumes protection groups are supported. 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 when you create the protection group. You can set site-wide inventory mappings between corresponding objects on the protected and recovery sites:

- Networks, including test networks
- Data centers or virtual machine folders
- Resource pools, standalone hosts, vApps, or clusters

NOTE
Recovery site resource pool, folder, or network must be in the same remote data center.

Add Folder Mapping

The workflow adds site-wide mappings of data centers or virtual machine folders on the local site to data centers or virtual machine folders on the remote site.

Verify that the Site Recovery Manager sites are paired. If the pairing is broken, all existing mappings are deleted and no additional mappings can be added.

You can map multiple parent (data center) and child (virtual machine folder) objects to a single object. A single object can have only one mapping. You can run the workflow multiple times for a single object, the latest workflow run sets the site-wide mapping. You can map a data center to a virtual machine folder and a virtual machine folder to a data center.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Add Folder Mapping` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 73: Add Folder Mapping Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.
Local Folder	Local data center or virtual machine folder.
Remote Folder	Remote datastore or virtual machine folder.

Add Network Mapping

The workflow adds site-wide mappings of networks on the local site to networks on the remote site.

Verify that the Site Recovery Manager sites are paired. If the pairing is broken, all existing mappings are deleted and no additional mappings can be added.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Add Network Mapping` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 74: Add Network Mapping Workflow Inputs

Input	Description
Site	Local Site Recovery Manager.
Local Network	Local network mapped to a remote network.
Remote Network	Remote network to which virtual machines connect when recovered.

Add Resource Mapping

The workflow adds site-wide mappings of computer resources, including pools, standalone hosts, vApps, or clusters from the local site to computer resources, including pools, standalone hosts, vApps, or clusters on the remote site.

Verify that the Site Recovery Manager sites are paired. If the pairing is broken, all existing mappings are deleted and no additional mapping can be added.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Add Resource Mapping` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 75: Add Resource Mapping Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.
Local Resource	Local resource - resource pool, standalone host, vApp.
Remote Resource	Remote resource - resource pool, standalone host, vApp, or cluster.

Add Test Network Mapping

The workflow adds site-wide mappings of networks on the remote site to test networks on the remote site.

Verify that the Site Recovery Manager sites are paired. If the pairing is broken, all existing mappings are deleted and no additional mappings can be added.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Add Test Network Mapping` and click **Enter**.
4. Enter the input parameters that the workflow requires, and click **Run**.

Table 76: Add Test Network Mapping Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.
Remote Network	Remote site network.
Test Network	Remote site test network.

Get Folder Mappings

The workflow lists data centers or virtual machine folders on the local site that have existing mappings.

If the protected and the recovery sites are registered as local sites, you can check all data centers or virtual machine folders which have existing mappings on both sites. The workflow does not show the exact mapping between corresponding objects.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Folder Mappings` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 77: Get Folder Mappings Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

Get Folder Mapping Pairs

The workflow lists data centers or virtual machine folders on the local site that have existing mapping between the corresponding objects (pairs).

Verify that you are logged in the remote Site Recovery Manager site to see the remote part of the mapping pair.

If the protected and the recovery sites are registered as local sites, you can check all data centers or virtual machine folders which have existing mappings on both sites.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Folder Mapping Pairs` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 78: Get Folder Mapping Pairs Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

Get Network Mappings

The workflow lists networks on the local site that have existing mappings.

If the protected and the recovery sites are registered as local sites, you can check all networks which have existing mappings on both sites. The workflow does not show the exact mapping between corresponding objects.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Network Mappings` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 79: Get Network Mappings Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

Get Network Mapping Pairs

The workflow lists networks on the local site that have existing mapping between the corresponding objects (pairs).

Verify that you are logged in the remote Site Recovery Manager site to see the remote part of the mapping pair.

If the protected and the recovery sites are registered as local sites, you can check all networks which have existing mappings on both sites.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the search box, enter `Get Network Mapping Pairs` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 80: Get Network Mapping Pairs Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

Get Resource Mappings

The workflow lists resources on the local site that have existing mappings.

If the protected and the recovery site are registered as local sites, you can check all resources which have existing mappings on both sites. The workflow does not show the exact mapping between corresponding objects.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Resource Mappings` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 81: Get Resource Mappings Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

Get Resource Mapping Pairs

The workflow lists resources on the local site that have existing mapping between the corresponding objects (pairs).

Verify that you are logged in the remote Site Recovery Manager site to see the remote part of the mapping pair.

If the protected and the recovery site are registered as local sites, you can check all resources which have existing mappings on both sites.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Resource Mapping Pairs` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 82: Get Resource Mapping Pairs Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

Get Test Network Mappings

The workflow lists networks that have existing mappings to test networks on the remote site.

If the protected and the recovery site are registered as local sites, you can check all remote networks which have existing mappings to remote test networks on both sites. The workflow does not show the exact mapping between corresponding objects.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Test Network Mappings` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 83: Get Test Network Mappings Workflow Inputs

Input	Description
Site	Local site.

Get Test Network Mapping Pairs

The workflow lists networks that have existing mappings between the corresponding objects (pairs) to test networks on the remote site.

Verify that you are logged in the remote Site Recovery Manager site to see the remote part of the mapping pair.

If the protected and the recovery site are registered as local sites, you can check all remote networks which have existing mappings to remote test networks on both sites.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Test Network Mapping Pairs` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 84: Get Test Network Mapping Pairs Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

Remove Folder Mapping

The workflow removes an existing site-wide mapping between a local folder or data center and remote folder or data center.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Folder Mapping` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 85: Remove Folder Mapping Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.
Folder Mapping	Folder mapping to be removed.

Remove Network Mapping

The workflow removes an existing site-wide mapping between a network on the local site and a network on the remote site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Network Mapping` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 86: Remove Network Mapping Workflow Inputs

Input	Description
Site	Local Site Recovery Managersite.
Network mapping	Network mapping to be removed.

Remove Resource Mapping

The workflow removes an existing site-wide mapping between resources on the local site and resources on the remote site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Resource Mapping` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 87: Remove Resource Mapping Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.
Resource Mapping	Resource mapping to be removed.

Remove Test Network Mapping

The workflow removes an existing site-wide mapping between a network on the remote site and a test network on the remote site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Test Network Mapping` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 88: Remove Test Network Mapping Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.
Test Networking Mapping	Test network mapping to be removed.

IP Customization Workflows

You can customize the IP mapping rules for a selected configured virtual network mapping on the protected and recovery sites.

Add IP Customization Rules

This workflow allows you to customize a previously created network mapping.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box enter `Add IP Customization Rules` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 89: Add IP Customization Rules Workflow Inputs

Input		Description
Network Information	Site	Local Site Recovery Manager site.
	Local Network	Local network which is part of the existing network mapping.
Subnet Details	Local Network Subnet	Valid IPv4 address to be identified as the local network.
	Remote Network Subnet	Valid IPv4 address to be identified as the remote network.
	Local and Remote Network Prefix	Number between 8 and 31 which serves as an indicator of the subnet mask.
Recovery Network Settings	Gateway	Valid IPv4 address for the gateway.

Input		Description
	DNS Addresses (set of IP addresses separated by semicolon)	List of IPv4 addresses, separated by semicolon.
	DNS Suffixes (domain names separated by semicolon)	Domain names, separated by semicolon.
	Primary WINS Server	Valid IPv4 address only for Windows virtual machines (this address is ignored by the Linux virtual machines.)
	Secondary WINS Server	Valid IPv4 address only for Windows virtual machines (this address is ignored by the Linux virtual machines.)

Remove IP Customization Rules

This workflow allows you to remove the customization of a previously created network mapping.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box enter `Remove IP Customization Rules` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 90: Remove IP Customization Rules Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.
Network Mapping	Local network which is part of the existing network mapping.

Protection Group Workflows in Site Recovery Manager Plug-In

Protection groups are collections of virtual machines or replicated datastores that Site Recovery Manager protects together. The Site Recovery Manager plug-in enables you to organize virtual machines into protection groups based on array-based replication or vSphere Replication.

Add Replicated Virtual Machine to vSphere Replication Protection Group

The workflow adds a virtual machine configured for vSphere Replication to a vSphere Replication protection group.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Add Replicated VM to vSphere Replication Protection Group` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 91: Add Replicated Virtual Machine to vSphere Replication Protection Group Workflow Inputs

Input	Description
vSphere Replication Protection Group	Local vSphere Replication protection group.
VM	Virtual Machine for which vSphere Replication is enabled.

Create Protection Group Folder

The workflow creates a folder for the protection groups.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Create Protection Group Folder` and click **Enter**.
4. Click the workflow and click **Run**.
5. Select where to place the protection group folder.
6. Enter a name for the folder and click **Run**.

Create Protection Group for Array-Based Replication

The workflow creates an array-based replication protection group.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Create Protection Group for Array Based Replication` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 92: Create Protection Group for Array-Based Replication Workflow Inputs

Input	Description
Protection Folder	Folder under local Site Recovery Manager site in which the protection group is placed.
Name	Protection group name.
Description	Short description.

Input	Description
Datastores	Datastore for which array-based replication is enabled.

Create Protection Group for vSphere Replication

The workflow creates a vSphere Replication protection group.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Create Protection Group for vSphere Replication` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 93: Create Protection Group for vSphere Replication Workflow Inputs

Input	Description
Protection Folder	Folder under a local Site Recovery Manager site in which the protection group is placed.
Name	Name of protection group.
Description	Short Description.
VMs	Virtual Machines added to the protection group.

Create a Virtual Volumes Protection Group

With this workflow you can create a Virtual Volumes protection group.

You can run the `List VMs in a vVol Replication Group` workflow before you run the `Create vVol Protection Group`, to locate your virtual machines among the Virtual Volumes replication groups.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box enter `Create vVol Protection Group` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 94: Create Virtual Volumes Protection Group Workflow Inputs

Input	Description
Protection Folder	Folder under local Site Recovery Manager site in which the protection group is placed.
Name	Virtual Volumes protection group name.
Description	Short description.
Fault Domain	Selecting a fault domain prevents you from selecting Virtual Volumes replication groups from different domains.

Input	Description
Replication Groups	List of Virtual Volumes replication groups that you want to include in the Virtual Volumes protection group (only unprotected Virtual Volumes replication groups can be selected.)

Find Array-Based Replication Protection Group by Datastore

The workflow lists the array-based replication protection group for a local datastore.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Find ABR Protection Group By Datastore` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 95: Find Array-Based Replication Protection Group by Datastore Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.
Datastore	Datastore attached to the local vCenter Server.

Get Unassigned Replicated Datastores

The workflow lists all replicated datastores on the local site that are not associated with an array-based replication protection group.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Unassigned Replicated Datastores` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 96: Get Unassigned Replicated Datastores Workflow Inputs

Inputs	Description
Site	Local Site Recovery Manager site.

List Protected Datastores

The workflow lists all replicated datastores that are associated with an array-based replication protection group.

The workflow accepts as input array-based replication protection groups only, returns a list of datastores that have array-based replication enabled and are associated with the selected protection group.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `List Protected Datastores` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 97: List Protected Datastores Workflow Inputs

Input	Description
Protection Group	Array-based replication protection group only.

List Protection Groups

The workflow lists existing array-based replication and vSphere Replication protection groups.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `List Protection Groups` and click **Enter**.
4. Click the workflow and click **Run**.
5.

Table 98: List Protection Groups Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

List Replication Groups in Virtual Volumes Protection Group

This workflow allows you to get a list of the replication groups, which are part of a Virtual Volumes protection group.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box enter `List Replication Groups in vVol Protection Group` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 99: List Replication Groups in Virtual Volumes Protection Group Workflow Inputs

Input	Description
Virtual Volumes Protection Group	The Virtual Volumes protection group, whose replication groups you want to list.

List Virtual Machines in a Virtual Volumes Replication Group

This workflow allows you to get a list of the virtual machines, which are part of an unassigned Virtual Volumes protection group.

You can run this workflow before you run the `Create vVol Protection Group` workflow, to locate your virtual machines among the Virtual Volumes replication groups.

> **NOTE**
> A Virtual Volumes protection group can contain multiple Virtual Volumes replication groups from the same fault domain, but it cannot contain Virtual Volumes replication groups from different fault domains.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the search box enter `List VMs in a vVol Replication Group` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 100: List VMs in a Virtual Volumes Replication Group Workflow Inputs

Input	Description
Protection Folder	Folder under local Site Recovery Manager site in which the protection group is placed.
Fault Domain	Selecting a fault domain prevents you from selecting Virtual Volumes replication groups from different domains.
Unprotected Replication Group	The Virtual Volumes replication group, whose virtual machines you want to list.

Move Protection Group

This workflow moves a protection group from one folder to another.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Move Protection Group` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 101: Move Protection Group Workflow Inputs

Input	Description
Protection group to be moved	The protection group that you want to move.
Destination folder	The destination folder, to which you want to move the protection group.

Move Protection Group Folder

The workflow allows you to move a particular protection group folder to a different destination folder.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Move Protection Group Folder` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 102: Move Protection Group Folder Workflow Inputs

Input	Description
Protection group folder to be moved	The protection group folder that you want to move.
Destination folder	The destination folder, to which you want to move the protection group folder.

Protect All Unprotected Virtual Machines Associated with Protection Group

The workflow enables protection for all unprotected virtual machines that are members of a protection group and creates placeholder virtual machines on the recovery site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Protect All Unprotected Virtual Machines Associated with Protection Group` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 103: Protect All Unprotected Virtual Machines Associated with Protection Group Workflow Inputs

Input	Description
Protection Group	Protection group on the local Site Recovery Manager site.

Protect Virtual Machine

The workflow enables protection for a virtual machine and creates a placeholder virtual machine on the recovery site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Protect Virtual Machine` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 104: Protect Virtual Machine Workflow Inputs

Input	Description
Protection Group	Protection group on the local Site Recovery Manager site.
VM	Virtual machine with enabled replication.

Protect Virtual Machine with Custom Inventory Mappings

This workflow allows you to set custom inventory mappings for an individual virtual machine in a protection group.

Verify that the virtual machine you want to protect with custom inventory mappings is part of a protection group.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Protect Virtual Machine with custom Inventory Mappings` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 105: Protect Virtual Machine with Custom Inventory Mappings

Input	Description
Protection group	The protection group, where the virtual machine is included.
Virtual Machine	The individual virtual machine, that you want to protect with custom inventory mappings.
Remote Folder	The virtual machine folder on the recovery site, to which you want to map the virtual machine folder on the protected site.
Choose remote networks per device	When you select it, *Network Devices* and *Remote Networks* array-based steps appear. They are a mapping between the virtual machine network devices and the remote networks. When you select a group and a virtual machine, the *Network Devices* step is automatically populated.
Remote Network	Network on the recovery site, to which you want to map the network on the protected site.
Remote Resource Pool	The resource pool on the recovery site, to which you want to map the resource pool on the protected site.

Remove Protection Group

The workflow removes a protection group.

When removing a protection group, Site Recovery Manager removes all virtual machines from the group, stops protection, and removes all placeholder virtual machines on the recovery site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Protection Group` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 106: Remove Protection Group Workflow Inputs

Input	Description
Protection Group	Local protection group to be removed.

Remove Protection Group Folder

This workflow allows you to remove an empty protection group folder.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Protection Group Folder` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 107: Remove Protection Group Folder Workflow Inputs

Input	Description
Protection group folder to be removed	The empty protection group folder that you want to remove.

Remove Replicated Virtual Machine from vSphere Replication Protection Group

The workflow removes a virtual machine from a vSphere Replication protection group.

When running the workflow, you must select a virtual machine from the vCenter Server inventory that is a member of the protection group.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Replicated VM from vSphere Replication Protection Group` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 108: Remove Replicated VM from vSphere Replication Protection Group Workflow Inputs

Input	Description
Protection Group	Local Site Recovery Manager site protection group.
Virtual Machine	Virtual machine member of the selected vSphere Replication protection group.

Unprotect Virtual Machines

The workflow unprotects virtual machines from the selected protection group and removes placeholder virtual machines from the recovery site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Unprotect Virtual Machines` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 109: Unprotect Virtual Machines Workflow Inputs

Input	Description
Protection Group	Local Site Recovery Manager site protection group.
Protected Virtual Machines	Protected virtual machine member of the selected protection group.

Update Group Datastore

The workflow adds or removes datastores in an array-based replication protection group.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Update Group Datastore` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 110: Update Group Datastore Workflow Inputs

Input	Description
Protection Group	The array-based replication protection group that you want to modify.
Datastores to Remove	Datastores to remove from the protection group.
Datastores to Add	Datastores to add to the protection group.

Recovery Plan Workflows in Site Recovery Manager Plug-In

Recovery plans hold instructions on how Site Recovery Manager recovers virtual machines from the protected to the recovery site.

A recovery plan can include one or more protection groups. You can add or remove protection groups to a recovery plan using the **Add Protection Group to Recovery Plan** and **Remove Protection Group from Recovery Plan** workflows. A recovery plan can contain both array-based replication protection groups and vSphere Replication protection groups.

Add Protection Group to Recovery Plan

The workflow adds a protection group to the selected Site Recovery Manager site.

The protection group added to the recovery plan must be local to the selected Site Recovery Manager site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box enter `Add Protection Group to Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 111: Add Protection Group to Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Recovery Plan to which you want to add the protection group.
Protection Group	Protection Group that was created on the local Site Recovery Manager site.

Add Test Network Mapping to Recovery Plan

The workflow adds a mapping between an existing network and an existing test network on the remote site for the selected recovery plan.

The test network must be created manually or through the **Create Recovery Plan** workflow. You must configure a test network for every network that a recovery plan uses during recovery.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Add Test Network Mapping to Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 112: Add Test Network Mapping to Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Recovery plan under local Site Recovery Manager site.
Remote Network	Remote network that maps to the test network.
Test Network	Remote network that assumes the role of test network.

Create Recovery Plan

The workflow creates a recovery plan and adds existing protection groups.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Create Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 113: Create Recovery Plan Workflow Inputs

Input	Description
Recovery Folder	Folder under local Site Recovery Manager site in which to place the recovery plan.
Name	Name of recovery plan.
Description	Short description.
Protection Groups	Existing array-based or vSphere Replication protection groups to add to the recovery plan.

Create Recovery Plan Folder

The workflow creates a folder for the recovery plans.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Create Recovery Plan Folder` and click **Enter**.
4. Click the workflow and click **Run**.
5. Select where to place the recovery plan folder.
6. Enter a name for the folder and click **Run**.

Delete Callouts

The workflow deletes pre and post power-on steps, such as commands and prompts that you specified earlier and that are run at the VM level during recovery.

When recovering a virtual machine, Site Recovery Manager runs predefined steps in a specific order. You can use the Delete Callouts workflow to remove the pre and post power-on steps that you have specified for a virtual machine.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Delete Callouts` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 114: Delete Callouts Workflow Inputs

Input	Description
Recovery Plan	Local Site Recovery Manager site recovery plan.
VM	Virtual machine to be configured.
Commands	Command names.
Prompts	Prompt names.

Delete Recovery Plan

The workflow deletes a recovery plan.

The workflow performs a check for the recovery plan state when running. If the recovery plan is in an incorrect state, the workflow fails with the following error message: `This operation is not allowed in the current state`.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Delete Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 115: Delete Recovery PlanWorkflow Inputs

Input	Description
Recovery Plan	Recovery plan under the local Site Recovery Manager site.

Get Recovery Plan State

The workflow lists the selected recovery plan state.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Recovery Plan State` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 116: Get Recovery Plan State Workflow Inputs

Input	Description
Recovery Plan	The recovery plan whose state you want to check.

Site Recovery Manager external API assigns different recovery plan states compared to the default internal ones. The following table shows the mapping between external API recovery plan states and internal Site Recovery Manager recovery plan statuses.

Table 117: Mapping of External Recovery Plan States

State	Local state	Peer state
running	testInitiated testInProgress cleanupInProgress failoverInitiated failoverInProgress reprotectInitiated reprotectInProgress rollbackInitiated rollbackInProgress	testInitiated testInProgress cleanupInProgress failoverInitiated failoverInProgress reprotectInitiated reprotectInProgress rollbackInitiated rollbackInProgress
failedOver	failedOver partialRollback	failedOver partialRollback
needsReprotect	partialReprotect reprotectIncomplete reprotectInterrupted	partialReprotect reprotectIncomplete reprotectInterrupted
needsCleanup	testComplete cleanupIncomplete cleanupInterrupted	testComplete cleanupIncomplete cleanupInterrupted
needsFailover	partialFailover failedOverSplit failoverIncomplete failoverInterrupted	failedOverSplit failoverIncomplete failoverInterrupted
needsRollback	rollbackIncomplete rollbackInterrupted	rollbackIncomplete rollbackInterrupted

State	Local state	Peer state
error	readyMixed noProtectionGroups deleting groupsInUse unknownState syncConflict	readyMixed noProtectionGroups deleting groupsInUse unknownState syncConflict
ready	readyReceiving testInterrupted	

Initiate Cancel Recovery Plan

The workflow initiates a cancel of failover or test of a recovery plan.

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. Canceling a test requires you to run a cleanup.

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

The workflow performs a check for the recovery plan state when running. If the recovery plan is in state **running**, you can cancel a recovery or a test.

Recovery plans are created with a specified direction of protection between the paired sites. You can run an **Initiate Cancel Recovery Plan** workflow to cancel recovery or test on the recovery (receiving) site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Initiate Cancel Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 118: Initiate Cancel Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Recovery plan on the remote Site Recovery Manager site in state running.

Initiate Cleanup Recovery Plan

The workflow initiates a cleanup of recovery plan.

The workflow performs a check for the recovery plan state when running. If the recovery plan is in state **needsCleanup**, you can clean up a test.

Recovery plans are created with a specified direction of protection between the paired sites. You can run the **Initiate Cleanup Recovery Plan** workflow to clean up a test of a recovery plan on the recovery site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Initiate Cleanup Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 119: Initiate Cleanup Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Recovery plan on the recovery Site Recovery Manager site.

Initiate Failover Recovery Plan

The workflow starts a disaster recovery failover from the protected to the recovery site through the selected recovery plan.

When completing a disaster recovery failover, Site Recovery Manager recovers virtual machines to the recovery site. If an error occurs on the protected site during operations, the disaster recovery failover continues and does not fail.

You can run the **Initiate Failover Recovery Plan** workflow on the recovery site.

The workflow performs a check for the recovery plan state when running. If the recovery plan is in state **ready**, you can run a failover.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter **Initiate Failover Recovery Plan** and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 120: Initiate Failover Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Recovery plan that fails over from the protected to the recovery site.

Initiate Planned Migration Recovery Plan

The workflow starts a planned migration failover from the protected to the recovery site through the selected recovery plan.

When completing a planned migration failover, Site Recovery Manager migrates virtual machines to the recovery site and attempts to shut down corresponding virtual machines on the protected site.

If errors occur on the protected site, the planned migration operation stops so that you can resolve the errors and rerun the plan.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Initiate Planned Migration Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 121: Initiate Planned Migration Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Recovery plan on the recovery Site Recovery Manager site.

Initiate Reprotect Recovery Plan

The workflow starts a reprotect process to protect the virtual machines on the recovery site after a failover has been completed.

You can initiate a reprotect process only if the recovery finishes without errors and the originally protected site is operational. Reverse folder, network, and resource mappings must exist from the original recovery to the original protected sites. During a reprotect process, Site Recovery Manager reverses the direction of protection, then forces a synchronization of the storage from the new protected site to the new recovery site.

You can run the **Initiate Reprotect Recovery Plan** workflow on the recovery site.

The workflow performs a check for the recovery plan state when running. If the recovery plan is in state **failedOver**, you can run a reprotect workflow.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Initiate Reprotect Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 122: Initiate Reprotect Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Recovery plan that is failed over from the protected to the recovery site.

Initiate Test Recovery Plan

The workflow starts a test of the selected recovery plan.

The workflow performs a check for the recovery plan state when running. If the recovery plan is in state **ready**, you can run a test.

Recovery plans are created with a specified direction of protection between the paired sites. You can run the **Initiate Test Recovery Plan** workflow on the recovery site. After a test of a recovery plan, you must run a cleanup of the recovery plan to return it to its original state.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Initiate Test Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 123: Initiate Test Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Recovery plan to run a test on the recovery site.

List Recovery Plans

The workflow lists all recovery plans.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `List Recovery Plans` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 124: List Recovery Plans Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

Move Recovery Plan

This workflow moves a recovery plan from one folder to another.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Move Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 125: Move Recovery Plan Workflow Inputs

Input	Description
Recovery plan to be moved	The recovery plan that you want to move.
Destination folder	The destination folder, to which you want to move the recovery plan.

Move Recovery Plan Folder

The workflow allows you to move a particular recovery plan folder to a different destination folder.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Move Recovery Plan Folder` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 126: Move Recovery Plan Folder Workflow Inputs

Input	Description
Recovery plan folder to be moved	The recovery plan folder that you want to move.
Destination folder	The destination folder, to which you want to move the recovery plan folder.

Remove Protection Group from Recovery Plan

The workflow removes a protection group from a recovery plan.

The workflow performs a check for the recovery plan state when running. If a recovery plan is in state **ready**, you can remove a protection group from it.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Protection Group from Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 127: Remove Protection Group from Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Local Site Recovery Manager site recovery plan.
Protection Group	Protection group member of the selected recovery plan.

Remove Recovery Plan Folder

This workflow allows you to remove a recovery plan folder.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Recovery Plan Folder` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 128: Remove Recovery Plan Folder Workflow Inputs

Input	Description
Recovery plan folder to be removed	The recovery plan folder that you want to remove.

Remove Test Network Mapping from Recovery Plan

The workflow removes a test network mapping from a recovery plan.

The workflow performs a check for the recovery plan state when running. If the recovery plan is in state **ready**, you can remove a protection group from it.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Test Network Mapping from Recovery Plan` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 129: Remove Test Network Mapping from Recovery Plan Workflow Inputs

Input	Description
Recovery Plan	Local Site Recovery Manager site recovery plan.
Test Network	Remote test network mapping to be removed.

Set IP Settings

The workflow customizes IP settings for individual virtual machines. It is a nested workflow that cannot be run on its own. The Set IP Settings workflow is called only as part of the Set Virtual Machine Recovery Settings workflow.

For more information on how to automate IP settings customization for individual virtual machines, see Set Virtual Machine Recovery Settings.

Set Virtual Machine Recovery Settings

When recovering a virtual machine,Site Recovery Manager runs predefined steps in a specific order.

You can use the Set VM Recovery Settings workflow to configure and customize how the virtual machine is recovered. You can add custom steps by using the Command or Prompt inputs available in the workflow.

You can also customize the IP settings of individual virtual machines. Customizing the IP properties of a virtual machine overrides the default IP settings when the recovered virtual machine starts at the recovery site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the search box, enter `Set VM Recovery Settings` and press **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 130: Set VM Recovery Settings Workflow Inputs

Input		Description
Choose objects	Recovery Plan	Local site recovery plan.

Input		Description
	VM	Virtual machine to be configured.
VM final power state	Power	The power state in which the virtual machine is recovered, for example powered-on, suspended, or powered-off.
VM recovery priority group	Priority Group	Specifies the shut-down and power-on order of virtual machines from the highest priority, which is 1, to the lowest priority, which is 5.
Pre Power On Command	Command Name	Specifies the command name.
	Command Text	Specifies the command or script to run.
	Command Timeout	Sets timeout after execution.
Pre Power On Prompt	Prompt Name	Specifies the prompt name.
	Prompt Text	Prompts user to perform a task or provides information that the user must acknowledge.
Post Power On Command	Command Name	Specifies the command name.
	Command Text	Specifies the command or script to run.
	Command Timeout	Sets timeout after execution.
	Command Run in Recovered VM	Specifies the command name, which was run in the recovered virtual machine.
Post Power On Prompt	Prompt Name	Specifies the prompt name.
	Prompt Text	Prompts user to perform a task or provides information that the user must acknowledge.

Input		Description	
Mode	Select an IP customization mode	Auto	Allows Site Recovery Manager to control the IP customization through the advanced recovery setting `recovery.useIpMapperAutomatically`. If its value is set to `True` and if you defined IP mapping rules earlier, Site Recovery Manager applies the rules during recovery. If the value is set to `False`, Site Recovery Manager does not apply any IP mapping rules to the virtual machine during recovery, even if such rules exist.
		Use IP customization rules if applicable	Uses IP customization rules that you defined earlier.
		No IP customization	Does not apply the IP customization to the virtual machine.

Input		Description	
		Manual IP customization	Customize manually the IP settings thatSite Recovery Manager pushes to the VM during recovery. 1. Select the NIC whose IP settings you want to modify. 2. Configure IPv4, IPv6, DNS settings, and primary and secondary WINS addresses.

Storage Workflows in Site Recovery Manager plug-in

Discover Replicated Devices

The workflow initiates discover replicated devices operation on all enabled array pairs.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Discover Replicated Devices` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 131: Discover Replicated Devices Workflow Inputs

Input	Description
Site	Local Site Recovery Manager site.

Placeholder Datastore Workflows in Site Recovery Manager Plug-In

With **Placeholder Datastore** workflows you can create and remove placeholder datastores for your Site Recovery Manager. You can use the *Get Placeholder Datastores* workflow to obtain a list with all the placeholder datastores for a selected site.

Add Placeholder Datastores

This workflow allows you to add placeholder datastores for Site Recovery Manager to use to store placeholder virtual machines on the recovery site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Add Placeholder Datastores` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 132: Add Placeholder Datastores Workflow Inputs

Input	Description
Site	Site Recovery Manager site where you want to add placeholder datastores.
Unreplicated datastores	The datastore, which contains the unprotected virtual machines.

Get Placeholder Datastores

This workflow provides you with a list of all the placeholder datastores in the selected site.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Get Placeholder Datastores` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 133: Get Placeholder Datastores Workflow Inputs

Input	Description
Site	Site Recovery Manager site for which you want to get a list of all the placeholder datastores.

Remove Placeholder Datastores

This workflow allows you to remove any placeholder datastores.

1. Log in to the VMware Aria Automation Orchestrator Client as an administrator.
2. Navigate to **Library** > **Workflows**.
3. In the **Filter** box, enter `Remove Placeholder Datastores` and click **Enter**.
4. Click the workflow and click **Run**.
5. Enter the input parameters that the workflow requires, and click **Run**.

Table 134: Remove Placeholder Datastores Workflow Inputs

Input	Description
Site	Site Recovery Manager site from which you want to remove placeholder datastores.
Placeholder datastores	An array of placeholder datastores, that you want to remove.

Site Recovery Manager API Developer's Guide

Information about programming applications with the Web services interfaces to Site Recovery Manager.

About Site Recovery Manager API Developer's Guide

The Site Recovery Manager API Developer’s Guide provides information about programming applications with the Web services interfaces to VMware Site Recovery Manager.

This manual provides information about interfaces in the Site Recovery Manager for developers who are interested in automating configuration of Site Recovery Manager Virtual Appliance or Site Recovery Manager tasks.

Intended Audience

This book is intended for developers who want to set up their environment to program applications with the Site Recovery Manager API. These developers are typically programmers using the Java or C# language and libraries to perform configuration of Site Recovery Manager Virtual Appliance or perform replication, recovery, and reprotection of virtual machines in VMware vSphere.

Site Recovery Manager developers should have some familiarity with the Web Services Description Language (WSDL) and the Simple Object Access Protocol (SOAP) for transmitting XML across the network. However, the important interfaces are completely visible in Java or C# code.

> **NOTE**
> The SOAP-based Site Recovery Manager APIs are deprecated. For the latest features and functionality, use the Site Recovery Manager Configuration REST API Gateway and the Site Recovery Manager REST API Gateway.

VMware Developer Publications

To view the current version of this book and other VMware API and SDK public documentation, go to http://www.vmware.com/support/developer.

Visit https://www.vmware.com/support/pubs/srm_pubs.html for information about this version of Site Recovery Manager.

VMware Technical Publications Glossary

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

APIs for VMware Site Recovery Manager

This manual describes Web services programming interfaces to programmatically configure the Site Recovery Manager Virtual Appliance, and create protection groups and recovery plans in VMware Site Recovery Manager.

The Site Recovery Manager Virtual Appliance Management API and the Site Recovery Manager API provides an interface similar to vSphere API, an object-oriented Web service that provides access to vSphere and virtual machine management on vCenter Server and ESXi hosts.

You can program the vSphere API in Java, C#, or any language that supports the Web services definition language (WSDL).

The Site Recovery Manager Virtual Appliance Management API provides a way for configuring Site Recovery Manager Server or OS-specific settings. The Site Recovery Manager API allows the third-party systems to create protection groups and initiate test, recovery, and reprotect operations and collect the results.

API Releases

NOTE
The SOAP-based Site Recovery Manager APIs are deprecated. For the latest features and functionality, use the Site Recovery Manager Configuration REST API Gateway and the Site Recovery Manager REST API Gateway.

The Site Recovery Manager 5.0 release extended the API with new methods to list and modify protection groups, and revised methods to list, modify, and run recovery plans.

The Site Recovery Manager 5.8 release introduced 30 methods and 4 new managed objects, adding several requested features to the API :

- Ability to add folder, network, and resource pool mappings
- Support for planned migrations
- Navigation capabilities for protection group folders and recovery plan folders
- Ability to create protection groups, and to modify selected fields in a virtual machine's recovery settings

The Site Recovery Manager 6.0 release introduced new methods to support authentication by tokens:

- New concept of the Site Recovery Manager solution user for authentication
- Functions to get the Site Recovery Manager solution user name for the local and remote sites
- Functions to log in to local or remote sites using security assertion markup language (SAML) token
- Ability to use lookup service URL and vCenter Server instance ID
- Although `DisasterRecoveryApi` is deprecated, it gains forward compatibility with `LoginByToken`

In release 6.1, introduced Storage Profile Protection Groups (SPPG). However, the Site Recovery Manager API does not support SPPG related objects.

Site Recovery Manager API 6.5 introduced methods that expand the operations on the inventory mappings, recovery plans, and protection groups.

The Site Recovery Manager 8.1 release introduces new methods that provide ability to:

- Add replicated datastores (that are newly provisioned) to an existing protection group.
- Remove datastores from the protection group.
- Configure the IP address and corresponding DNS, WINS of the virtual machine, after the migration is complete.

The Site Recovery Manager 8.2 release introduces new methods that provide ability to:

- Read information specific to an ArrayManager instance and list all the array pairs in the array manager.
- Get information about all the replicated RDMs in a replicated array pair.
- Get a list all the available array managers.

The Site Recovery Manager 8.3 release introduces the following:

- Site Recovery Manager Virtual Appliance Management APIs for configuring Site Recovery Manager Virtual Appliance or OS-specific settings.
- APIs for vVOL management.
- APIs for automatic protection.
- APIs for managing IP Subnet Mapping between protection and recovery site networks, defining the rules used for translating VM's IP settings between protection and recovery sites, and customizing the IP information for a specific network adapter.

The Site Recovery Manager 8.4 release introduces the following:

- Site Recovery Manager APIs for pairing, manual per VM protection, array manager management, and folders operations.
- Site Recovery Manager Virtual Appliance Management APIs can be used for configuring VRMS vSphere replication management server (VRMS-HMS) and VRS vSphere replication server (VRS-HBR).

The Site Recovery Manager 8.5 release introduces the following:

- APIs to start and monitor a recovery plan execution, additional options to ignore errors during Test cleanup or Reprotect.
- APIs to get specific details for an ABR Protection Group.
- The Appliance Management API is extended with new APIs, which allow more custom configuration of the appliance.

Terminology

This document uses the following terms.

SOAP
: Client applications invoke operations by sending SOAP formatted messages. When passing data objects between client and server, programs build or parse XML messages representing data structures described by the WSDL. Standardized by W3C as Simple Object Access Protocol (SOAP) 1.1.

Web service operations
: Client interfaces that perform server-side management and monitoring tasks. Standardized as Web Services Interoperability Organization (WS-I) Basic Profile 1.0.

WSDL
: The Web services API is defined in a WSDL file, which is used by client-side Web services to create proxy code (stubs) that client applications use to interact with the server. Standardized as Web Services Description Language (WSDL) 1.1.

XML
: A text representation scheme similar to HTML but with more stringent, regularized syntax. Standardized by W3C as Extensible Markup Language (XML) 1.0.

The Site Recovery Manager Appliance Management API and the Site Recovery Manager API are similar to and derived from the vSphere API. For information about the vSphere API, see the *vSphere Web Services SDK Programming Guide* and the *vSphere API Reference* at the VMware website.

Site Recovery Manager Appliance Management API

The Site Recovery Manager Appliance Management API provides language-neutral interfaces to the Site Recovery Manager Virtual Appliance management framework for configuring Site Recovery Manager Server or OS specific settings.

The API is implemented as industry-standard Web service, running on Site Recovery Manager Virtual Appliance. The Site Recovery Manager Appliance Management API complies with the Web Services Interoperability Organization (WS-I) Basic Profile 1.0, which includes XML Schema 1.0, SOAP 1.1, WSDL 1.1. For more information about the WS-I Basic Profile 1.0, see:

http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html

List of API Operations

The following tables provide a list of Site Recovery Manager Appliance Management API methods arranged in alphabetical order:

Table 135: Appliance Manager

Method	Description of Operation
GetAllTimeZones	Gets all available time zones. It returns list representing all available time zones.
GetCurrentDateTime	Gets current date and time of the appliance. It returns a vmodl.DateTime object with the appliance date and time.
GetCurrentTimeZone	Gets current time zone of the appliance. It returns a string representing the current time zone.
GetDiskInfo	Retrieves appliance disks information. It returns an array of DiskInfo objects, which contain disk information about the appliance.
GetInfo	Retrieves appliance information. It returns an ApplianceInfo object which contains information about the appliance.
GetNetworkInfo	Retrieves appliance network information. It returns a NetworkInfo object which contains network information about the appliance.
GetTimeSyncConfig	Gets appliance time sync mode. It returns a TimeSyncInfo object representing the timeSyncMode.
Restart	Restarts the appliance.
SetCurrentTimeZone	Sets appliance time zone.
SetNetworkInfo	Sets appliance network information.
SetTimeSync	Sets appliance time sync information.
Stop	Stops the appliance.

Table 136: Configuration Manager

Method	Description of Operation
CheckRegistration	Checks whether the given extension key is already registered in SSO, lookup service, and as vCenter extension. Applicable to SRM and VRMS.
ClearSrmConfiguration	Clears the SRM server configuration with the vSphere infrastructure. Applicable to SRM and VRMS.
ConfigureSrm	Configures the SRM server and connects it to the vSphere infrastructure. Applicable to SRM and VRMS.
ConfigureSyslogForwarding	Sets syslog log forwarding. Applicable to SRM, VRMS, and VRS.
ConfigureSyslogServers	Sets the syslog log forwarding. Applicable to SRM, VRMS, and VRS.
EnableSyslogLogging	Enables or disables logging to syslog. Applicable to SRM.
GetHbrSrvNic	Gets the HBR filter and management IP addresses. Applicable to VRMS, and VRS.
GetRunningTask	Gets the currently active configuration task or null. Applicable to SRM, VRMS, and VRS.

Method	Description of Operation
GetServicesSyslogLogLevel	Gets syslog log level information of the services. Applicable to SRM, VRMS, and VRS.
GetSyslogServers	Gets the syslog log forwarding information. Applicable to SRM, VRMS, and VRS.
IsReconfigureRequired	Checks if the reconfigure operation is required after an upgrade. Applicable to SRM and VRMS.
ListVcServices	Lists all the vCenters in the Platform Service Controller (PSC). Applicable to SRM and VRMS.
ReadCurrentConfig	Reads the specification for the currently configured SRM server. Applicable to SRM and VRMS.
SendSyslogTestMessage	Sends test message to all configured syslog servers. Applicable to SRM, VRMS, and VRS.
SetHbrSrvNic	Sets the HBR filter and management addresses. Applicable to VRMS and VRS.
ValidateConnection	Validates connections to the vSphere infrastructure. Applicable to SRM and VRMS.

Table 137: Configuration Task

Method	Description of Operation
CancelSrmConfiguration	Cancels a running configuration task. Multiple cancel requests are treated as a single cancelation request.
GetTaskInfo	Gets the current configuration task status.

Table 138: Database Manager

Method	Description of Operation
ChangePassword	Changes the embedded database password.
ReadStatus	Checks the database status and return the version information.

Table 139: Diagnostic Manager

Method	Description of Operation
GetRunningTask	Gets the currently active retrieve update task or null.
GenerateSystemLogBundle	Instructs the server to generate a system log bundle.
RetrieveSystemLogBundle	Retrieves the log bundle using the Binary datatype.
DeleteSystemLogBundle	Instructs the server that this log bundle is no longer needed by the client that generated it.

Table 140: Service Instance

Method	Description of Operation
`ChangeUserPassword`	Assigns password to the user, who is running the drconfig service.
`LoginDrConfig`	Logs on to the server by verifying user and password with the local OS.
`LogoutDrConfig`	Log out and terminate the current session.
`RetrieveContent`	Retrieves the properties of the service instance.

Table 141: Service Manager

Method	Description of Operation
`DrConfigStartService`	Starts the service.
`DrConfigStopService`	Stops the service.
`DrConfigServiceStatus`	Returns a ServiceStatus object which contains the service status information about the service.
`DrConfigRestartService`	Stops the service and then restarts it.
`DrConfigAllServicesStatus`	Returns a ServiceStatus object for all the services.
`IsSrmServerRunning`	Returns the current service state of the Site Recovery Manager

Table 142: SRA Manager

Method	Description of Operation
`CopySraConfiguration`	Copies the SRA configuration from a source image to a destination image.
`DeleteImage`	Stops and then deletes the containers instantiated from the given image, and deletes the image itself.
`DeleteImageContainers`	Stops and then deletes the containers which were instantiated from the given image.
`GetRunningTask`	Gets the currently active retrieve update task or null.
`GetSraImages`	Returns a collection of SRA images loaded into the docker daemon of the Site Recovery Manager Virtual Appliance.
`GetImageInfo`	Returns the image information as taken from the queryInfo SRA command.
`ResetToFactorySettings`	Reverts the SRA image's configuration to its factory settings.

Table 143: SSL Certificate Manager

Method	Description of Operation
AddCaCertificates	Adds certificate authority certificates to the list of validating certificates.
ClearCaCertificates	Completely clears Site Recovery Manager specific list of certificate authority certificates, used by the Site Recovery Manager to validate other server's certificates.
DrConfigGenerateCSR	Generates a new key and CSR, and returns them for signing.
DrConfigSetCertificate	Sets a new certificate. Reconfigures the Site Recovery Manager if already configured. Restarts the proxy service.
DrConfigSetKeyCertificate	Sets a new key and certificate, reconfigures Site Recovery Manager if already configured, and then restarts the proxy service.
GetCertificateInfo	Lists the certificate info.
InstallSelfSignedCertificate	Installs self-signed certificate, reconfigures the Site Recovery Manager if already configured, and restarts the proxy service.
InstallCertificate	Installs the PKCS#12 certificate, reconfigures Site Recovery Manager if already configured, and restarts the proxy service.
RemoveCaCertificates	Removes certificate authority certificates from the list of validating certificates.
RetrieveCaCertificates	Gets the current SRM specific list of certificate authority certificates used by SRM to validate other server's certificates.
ProbeSsl	Checks if the Site Recover Manager can establish successful SSL connection to the specified endpoint.

Table 144: Update Manager

Method	Description of Operation
DrConfigCheckForUpdates	Checks for updates. It checks the repository for available updates.
GetRepositories	Gets update repos.
GetRunningTask	Tests the currently active retrieve update task or returns null.
InstallUpdate	Installs the update.
UpdateRepository	Changes the update repository location.

Managed Object Hierarchy

The following table shows the managed object hierarchy of the Site Recovery Manager Appliance Management API with the methods of each managed object in an alphabetical order.

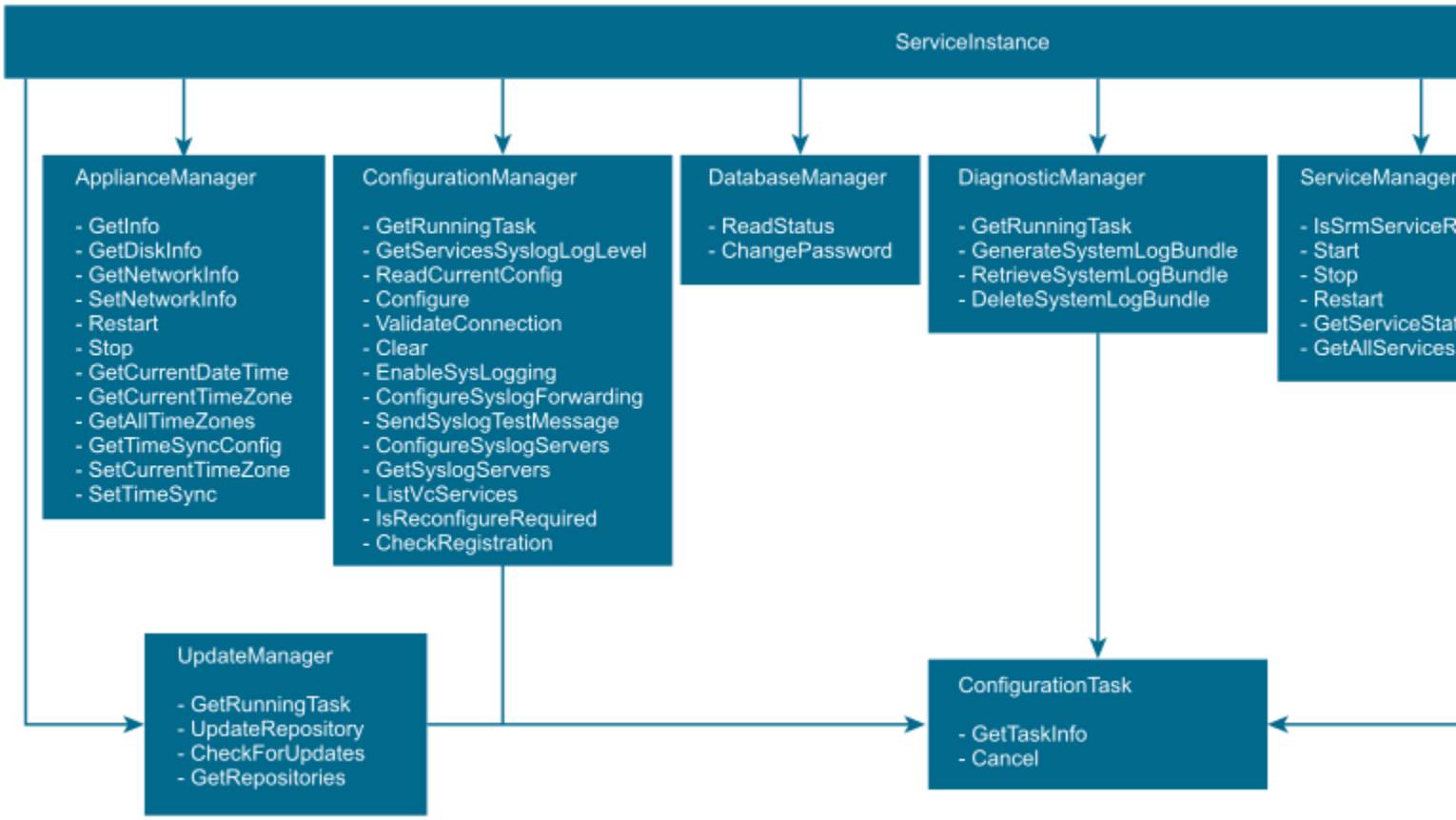
Table 145: Managed Object Hierarchy

Managed Object	Remarks	Local Methods
ApplianceManager	Tools to manipulate the appliance of SRM server.	GetAllTimeZones GetCurrentDateTime GetCurrentTimeZone GetDiskInfo GetInfo GetNetworkInfo GetTimeSyncConfig Restart SetCurrentTimeZone SetNetworkInfo SetTimeSync Stop
Configuration Manager	Tools to configure SRM server	CheckRegistration ClearSrmConfiguration ConfigureSrm ConfigureSyslogForwarding ConfigureSyslogServers EnableSyslogLogging GetHbrSrvNic GetRunningTask GetServicesSyslogLogLevel GetSyslogServers IsReconfigureRequired ListVcServices ReadCurrentConfig SendSyslogTestMessage SetHbrSrvNic ValidateConnection
ConfigurationTask	Operations to configure SRM server	GetTaskInfo CancelSrmConfiguration
DatabaseManager	Operations to configure SRM database.	ChangePassword ReadStatus
DiagnosticManager	Describes the interface to get the Site Recovery Manager system log bundles that contains log files, cores and configuration files that are useful for diagnosis of issues.	DeleteSystemLogBundle GetRunningTask GenerateSystemLogBundle RetrieveSystemLogBundle
ServiceInstance	Singleton object which provides access to the functionality of the DrConfig server.	ChangeUserPassword LoginDrConfig LogoutDrConfig RetrieveContent
ConfigServiceManager	Describes the operations to control appliance services.	DrConfigAllServicesStatus DrConfigRestartService DrConfigServiceStatus DrConfigStartService DrConfigStopService IsSrmServerRunning

Managed Object	Remarks	Local Methods
SraManager	Describes the interface for managing SRA images and containers in the SRM Configuration Service.	CopySraConfiguration DeleteImage DeleteImageContainers GetImageInfo GetRunningTask GetSraImages ResetToFactorySettings
SslCertificateManager	Describes operations to configure certificates for the configuration service and SRM.	AddCaCertificates ClearCaCertificates DrConfigGenerateCSR DrConfigSetCertificate DrConfigSetKeyCertificate InstallCertificate InstallSelfSignedCertificate ProbeSsl RemoveCaCertificates RetrieveCaCertificates
UpdateManager	Describes operations to update the Site Recover Manager appliance.	DrConfigCheckForUpdates GetRepositories GetRunningTask InstallUpdate UpdateRepository

The Site Recovery Manager Appliance Management Object Classes graphic shows the managed object class hierarchy with the methods of each managed object.

Figure 13: Site Recovery Manager Appliance Management API Object Classes



Site Recovery Manager API

The Site Recovery Manager API provides language-neutral interfaces to the Site Recovery Manager server management framework.

The API is implemented as industry-standard Web service, running on Site Recovery Manager server. The Site Recovery Manager API complies with the Web Services Interoperability Organization (WS-I) Basic Profile 1.0, which includes XML Schema 1.0, SOAP 1.1, WSDL 1.1. For more information about the WS-I Basic Profile 1.0, see:

http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html

List of API Operations

The following tables provide a list of Site Recovery Manager API methods arranged in alphabetical order.

Table 146: Service Instance

Method	Description of Operation
`BreakPairing`	Remove the connection with the remote SRM server. This operation automatically logs out from the remote site.
`GetSiteName`	Get the name of the current local site. (deprecated in 6.5)

Method	Description of Operation
GetPairedSite	Retrieve information about the remote site that is paired with this local site.
GetLocalSiteInfo	Get information about the local site
GetSolutionUserInfo	Obtain the Site Recovery Manager solution user name for the local site.
GetPairedSiteSolutionUserInfo	Obtain the Site Recovery Manager solution user name for the remote site.
GetLicenseInfo	Get assigned license information.
PairSrm	Establish persistent network connection with a remote SRM server. Remote SRM server must have the same VC extension key.
ProbeSsl	Returns (host and thumbprint) tuples for all PSC/MGMT/DR hosts to which SRM should connect under specified root PSC node.
ReconfigureConnection	Reconfigure RemoteSite object with connection information for remote PSC node.
RetrieveContent	Retrieve the properties of a service instance. Additionally the AboutInfo data object provides information about this service.
SrmLoginByTokenLocale	Begin a session with Site Recovery Manager Server.
SrmLoginSitesByToken	Log in to both the local and remote vCenter Server.
SrmLoginRemoteSiteByToken	Log in to remote site when escalated privileges are required and the current session has already been authenticated using SrmLoginSitesByToken.
SrmLoginLocale	Begin a session with Site Recovery Manager Server.
SrmLoginSites	Log in to both the local and remote vCenter Server.
SrmLogoutLocale	Log out sites and terminate the current session.
SrmLoginRemoteSite	Log in to remote site when escalated privileges are required on the remote site and the current session has already been authenticated using SrmLoginSites.

Table 147: SRM ExtApi Task

Method	Description of Operation
GetSrmExtApiTaskInfo	Gets the results of this task
IsSrmExtApiTaskComplete	Returns True if this task has been completed

Table 148: Inventory Mapping

Method	Description of Operation
AddFolderMapping	Add a folder mapping between the primary and secondary vCenter Server.
AddNetworkMapping	Add a network mapping between the primary and secondary vCenter Server.

Method	Description of Operation
AddResourcePoolMapping	Add resource pool mapping between primary and secondary vCenter Server.
AddTestNetworkMapping	Add a test network mapping.
GetFolderMappings	Returns an array of the folder mappings for a specific inventory mapper.
GetnetworkMappings	Returns an array of the network mappings for a specific inventory mapper.
GettestNetworkMappings	Returns an array of the test network mappings for a specific inventory mapper.
GetresourcePoolMappings	Returns an array of the resource pool mappings for a specific inventory mapper.
RemoveFolderMapping	Remove a folder mapping.
RemoveNetworkMapping	Remove a network mapping.
RemoveResourcePoolMapping	Remove a resource pool mapping.
RemoveTestNetworkMapping	Remove a test network mapping.

Table 149: Storage

Method	Description of Operation
CreateArrayManager	Creates ArrayManager object.
DiscoverDevices	Loops through all array managers, local and remote, discovering devices.
QueryArrayManagers	Returns a list of all the available array managers.
QueryStorageAdapters	List of Storage Replication Adapters (SRAs) info successfully loaded into SRM.
ReloadAdapters	Scans SRA installation directory and re-loads SRAs.
RemoveArrayManager	Deletes ArrayManager object.

Table 150: Storage Adapter

Method	Description of Operation
FetchInfo	Fetches basic information about the SRA.
GetAdapterConnectionSpec	Gets the connection parameters for the SRA provided by the user.

Table 151: Autoprotect Manager

Method	Description of Operation
GetAutoprotectUser	Gets the user for the automatic protection.
IsActive	Checks if the automatic protection is globally activated (true) or deactivated (false).

Method	Description of Operation
SetAutoprotectUser	Configures the user to be used by automatic protection on this site. If not called, the default autoprotect user is used.
SetDefaultAutoprotectUser	Reverts the current user to the default user.

Table 152: Folder

Method	Description of Operation
GetName	Get the name of ProtectionGroupFolder or RecoveryPlanFolder.
GetParentFolder	Get parent folder for a ProtectionGroupFolder or RecoveryPlanFolder.
GetChildType	Specifies the object types a folder may contain.
CreateFolder	Creates a new sub-folder with the specified name.
MoveFolder	Moves the specified folder into another folder.
DestroyFolder	Destroys the specified folder.
RenameFolder	Renames the specified Folder.

Table 153: Protection

Method	Description of Operation
CreateAbrProtectionGroup	Create an array-based replication (ABR) protection group. The method returns a CreateProtectionGroupTask.
CreateHbrProtectionGroup	This method is deprecated. It creates a host-based replication (HBR) protection group. Returns a CreateProtectionGroupTask.
CreateHbrProtectionGroup2	Create a new host based (that is vSphere replication) ProtectionGroup using the provided virtual machines.
CreateVvolProtectionGroup	Creates a new vVol protection group.
GetProtectionGroupRootFolder	Get the root folder for all protection groups, so as to navigate folder hierarchy. The methods below give users the ability to locate replicated resources and construct protection groups, key features of the 5.8 API.
ListProtectionGroups	Get a list of the protection groups that are currently configured.
ListInventoryMappings	Get a list of the configured inventory mappings on the protection site.
ListReplicatedDatastores	Get a list of the replicated datastores. (deprecated in 6.0)
ListUnassignedReplicatedDatastores	Get list of replicated datastores that can be used to create new protection groups.
ListUnassignedReplicatedVms	Get list of replicated VMs not currently assigned to a Site Recovery Manager protection group.
ProtectionListProtectedDatastores	Get list of replicated datastores that are protected by Site Recovery Manager.

Method	Description of Operation
ProtectionListProtectedVms	Get list of virtual machines that are protected by Site Recovery Manager.
RemoveProtectionGroup	Delete a protection group.

Table 154: Protection Group Folder

Method	Description of Operation
GetProtectionGroup	Retrieves the protection group with the specified name, if any.
ListChildProtectionGroupFolders	Return the child ProtectionGroupFolders located in this folder.
ListChildProtectionGroups	Return the SrmProtectionGroup objects located in this folder.

Table 155: Create Protection Group Task

Method	Description of Operation
GetCreateProtectionGroupResult	Once task is complete, check the result to ensure that it succeeded.
GetNewProtectionGroup	After checking task result, obtain the newly created SrmProtectionGroup.
IsCreateProtectionGroupComplete	Check completeness of the task to create a new protection group.

Table 156: Protection Group

Method	Description of Operation
AssociateVms	Associate the specified VMs with a group. This is a prerequisite for protection. Only for vSphere Replication.
AddDatastores	Adds datastores to the protection group. Additionally, the virtual machines on these datastores can be protected by the protection group. This can be done by calling protectVms method from this interface.
CheckConfigured	Check the protection group for VMs that are not configured, have configuration issues, and protected VMs that must be configured.
GetAbrGroupDetails	Get ABR-specific details for this protection group.
GetInfo	Retrieve basic information about this protection group.
GetPeer	Retrieve the peer protection group.
GetPlaceholderVmInfo	This method returns information for the placeholder VM for the specified protected VM.
GetRecoveryLocationSettings	This method returns the recovery location settings for the specified protected VM.
GetProtectionState	Get the current state of the protection group.
GetVvolGroupDetails	Gets vVol specific details for this protection group.

Method	Description of Operation
ListProtectedVms	List VMs protected in this group with information about their protection state.
ListProtectedDatastores	Retrieve a list of the Datastores protected by this protection group.
ListAssociatedVms	Retrieve a list of VMs associated with this group. Only for vSphere Replication and vVol.
MoveGroup	This method moves specified ProtectionGroup to a different folder.
ProtectionGroupGetParentFolder	Retrieve the folder that contains this protection group.
ProtectionGroupListRecoveryPlans	Retrieve a list of all Recovery Plans this protection group is a member of.
ProtectionGroupQueryVmProtection	Determine whether the specified VMs can be or currently are protected, which must be mapped to the recovery site as per ListInventoryMappings.
ProtectVms	Protect the specified VMs. The folder, resource pool, and network of each virtual machine must be mapped to the recovery site. Returns a ProtectionTask.
ProtectionGroupGetOperationalLocation	Get the effective location of the protection group.
RemoveDatastores	Removes datastores from the protection group. Virtual machines on the removed datastores are no longer protected by the protection group.
ReconfigureRecoveryLocationSettings	Reconfigures the recovery location settings for the specified protected VM.
ReconfigureVvolProtectionGroup	Reconfigure settings for this group. For a vVvol ProtectionGroup this method can reconfigure the name, description, fault domain, and associated virtual machines. If the clearAssociatedVms flag is set to true, then the associated virtual machines with this protection group will be cleared. If the flag is not set and the associated Vm's list is not empty, then the associated virtual machines will be added to this protection group replacing the old virtual machines.
RecreatePlaceholder	Recreates a placeholder VM.
UnprotectVms	Unprotect the specified VMs.
UnassociateVms	Unassociate the specified VMs with this group. Only for vSphere Replication and vVol.

Table 157: Protection Task

Method	Description of Operation
GetProtectionStatus	Get the results of ProtectVms or UnprotectVms
GetTasks	Get Task information from the vCenter Server for each virtual machine that was requested to be protected or unprotected.
GetResult	Get the results of this Task.
IsComplete	Check if this Task has finished.

Table 158: Recovery

Method	Description of Operation
CreateRecoveryPlan	Create a recovery plan.
DeleteRecoveryPlan	Delete a recovery plan.
GetHistory	Retrieve the history for a given Recovery Plan.
GetRecoveryPlanRootFolder	Retrieve the root folder for all Recovery Plans.
ListPlans	Retrieve all the Recovery Plans for Site Recovery Manager Server.
MovePlan	Moves the RecoveryPlan to a different folder.

Table 159: Recovery Plan Folder

Method	Description of Operation
GetRecoveryPlan	Get MoRef to recovery plan with the specified name in the RecoveryPlanFolder.
ListChildRecoveryPlanFolders	Return the child RecoveryPlanFolders located in the folder.
ListChildRecoveryPlans	Return an array of SrmRecoveryPlan objects located in the folder.

Table 160: Recovery Plan

Method	Description of Operation
AddProtectionGroup	Add a protection group to this Recovery Plan.
AddTestNetworkMappingToRecoveryPlan	Add a test network mapping to a recovery plan.
AnswerPrompt	Answer the current prompt displayed by a Recovery Plan. Requires the Run privilege for test, or the Failover privilege for the other modes.
Cancel	Cancel the specified Recovery Plan.
GetRecoverySettings	Retrieve the per-VM recovery settings for VMs in the Recovery Plan.
ListPrompts	List the current prompts that are waiting for input. When a prompt step is reached, the plan goes into the waiting state until AnswerPrompt is received. Prompts are given in the same order in which VMs are scheduled to start up.
RecoveryPlanGetPeer	Get the peer plan for this Recovery Plan. The returned object refers to a plan at the paired site, not the local site.
RecoveryPlanGetInfo	Retrieve basic information about the specified Recovery Plan.
RecoveryPlanGetParentFolder	Retrieve the root folder for all Recovery Plans.
RemoveProtectionGroupFromRecoveryPlan	Remove a protection group from a recovery plan.
RemoveTestNetworkMappingFromRecoveryPlan	Remove a test network mapping from a recovery plan.
RecoveryPlanGetLocation	Check whether the recovery plan is hosted locally or on the paired site.

Method	Description of Operation
RecoveryPlanHasRunningTask	Check whether there is a task that is associated with the recovery plan.
Start	Start the Recovery Plan in the selected mode: test, cleanupTest, recovery, or reprotect. Requires Run privilege for tests, and the Failover privilege for the others. This method is deprecated in 8.5.
StartEx	Start the Recovery Plan in the selected mode: test, cleanupTest, reprotect, revert, or migrate. Requires Run privileges for tests, and the Failover privileges for the others.
SetRecoverySettings	Modify the per-VM recovery settings for VMs in the Recovery Plan. Configure the IP address and corresponding DNS, WINS of the virtual machine, after the migration is complete, using the VmIpCustomization API.

Table 161: Recovery History

Method	Description of Operation
GetRecoveryResult	Retrieve the recovery result for a given run of a Recovery Plan.
GetResultCount	Retrieve total number of stored results, including Recovery and peer plans.
GetResultLength	Get length of XML result document for the requested recovery result.
RetrieveStatus	Retrieve XML document for a historical run of the specified Recovery Plan.

Table 162: IP Subnet Mapper

Method	Description of Operation
AddIpMapping	Associates an IPMapping object with an inventory-mapped protected site network.
GetIpSubnetMappings	Returns an array of the IP subnet mappings for this IP Subnet Mapper.
RemoveIpMappings	Removes IPMappings from mapped protected site networks. This must be called on secondary (recovery) site.

Table 163: Array Manager

Method	Description of Operation
AddArrayPair	Creates ReplicatedArrayPair object for a given pair of storage arrays.
DiscoverArrays	Discovers storage arrays configured for replication by executing SRA command discoverArrays.
GetAdapter	Returns the corresponding storage adapter to the ArrayManager.

Method	Description of Operation
GetArrayDiscoveryStatus	Returns the status and timestamp information of latest array discovery.
GetArrayInfo	This method gets the list of discovered storage arrays.
QueryReplicatedArrayPairs	Returns list of all the replicated array pairs in the ArrayManager.
ReadInfo	Returns information specific to the ArrayManager instance.
Reconfigure	Updates array manager name and connection parameters for the SRA.
RemoveArrayPair	Deletes specified ReplicatedArrayPair object.

Table 164: Replicated Array Pair

Method	Description of Operation
GetDevices	Returns list of storage devices configured for replication.
GetDeviceGroups	Returns list of consistency groups of storage devices configured for replication.
GetReplicatedDatastores	Returns list of datastores residing on replicated storage devices.
GetOwner	Returns the ArrayManager for the local array in this pair.
GetDeviceDiscoveryStatus	Gets the storage device discovery status.
QueryReplicatedRdms	Returns info for all replicated RDMs in the ReplicatedArrayPair.

Table 165: Vvol Replication

Method	Description of Operation
GetDomains	Returns a list of local vVol fault domains with their replication groups which target fault domains matching SRM peer site.
GetUnprotectedVms	Returns a list of unprotected vVol replicated virtual machines part of vVol replication groups that target the SRM peer site.
Rescan	Initiates a rescan of the server's local vVol configuration. The server keeps updating its view of the local vVol configuration periodically. This results in the newly provisioned vVol virtual machines being available for protection only after the passage of update interval. This function is called to force an update.

Table 166: Placeholder Datastore Manager

Method	Description of Operation
AddDatastore	Adds datastore to the list of placeholder datastores.
GetPlaceholderDatastores	Gets the list of all configured placeholder datastores.
RemoveDatastore	Removes datastore(s) from the list of placeholder datastores.

Table 167: Deprecated DisasterRecoveryApi

Method	Description of Operation
`GetApiVersion`	Obtain the API version.
`GetFinalStatus`	Get the final status of a Recovery Plan.
`Login`, `Logout`, `LoginByToken`	Log in to and out of Site Recovery Manager Server.
`ListRecoveryPlans`	Get a list of Recovery Plans at the SRM site.
`RecoveryPlanSettings`	Get the settings of a specific Recovery Plan at the SRM site.
`RecoveryPlanStart`	Start a specific Recovery Plan in recovery or test mode.
`RecoveryPlanPause`	Pause a running Recovery Plan.
`RecoveryPlanResume`	Restart a paused Recovery Plan.
`RecoveryPlanAnswerPrompt`	Answer a prompt.
`RecoveryPlanCancel`	Cancel a Recovery Plan.

New vCenter Single Sign-On APIs

A set of login-by-token functions was added to the ServiceInstance managed object. For an example of use, see the Functions for Logging Into Sites table.

Deprecated APIs

The version 1.0 DisasterRecoveryApi was discontinued in Site Recovery Manager 5.8 and marked deprecated in Site Recovery Manager 6.0, although a new login-by-token function was implemented for backward compatibility.

> **NOTE**
> The InvalidLogin fault and others use a different namespace in DisasterRecoveryApi (drextapi.fault.InvalidLogin) than in ServiceInstance (vim.fault.InvalidLogin).

In the RemoteSite managed object, the vcHost and vcPort fields are deprecated. They are replaced by the lkpUrl (Lookup Service URL) and vcInstanceUUID (vCenter Server unique ID).

The `GetSiteName` method is deprecated in Site Recovery Manager 6.5. You must use `LocalSiteInfo.siteInfo` to get the local site name.

The `SrmProtection.listReplicatedDatastores` method is replaced with `SrmProtection.listUnassignedReplicatedDatastores`.

In the Protection managed object, the `createHbrProtectionGroup` method is deprecated. It is replaced by the `createHbrProtectionGroup2` method.

Managed Object Hierarchy

The following table shows the managed object hierarchy of the Site Recovery Manager API with the methods of each managed object in an alphabetical order.

Table 168: Managed Object Hierarchy

Managed Object	Remarks	Local Methods

ArrayManager	Query information about array managers	`AddArrayPair`
		`DiscoverArrays`
		`GetAdapter`
		`GetArrayDiscoveryStatus`
		`GetArrayInfo`
		`ReadInfo`
		`Reconfigure`
		`RemoveArrayPair`
		`QueryReplicatedArrayPairs`

SrmAutomaticProtection	External API for automatic protection	`GetAutoprotectUser`
		`IsActive`
		`SetAutoprotectUser`
		`SetDefaultAutoprotectUser`

CreateRecoveryPlanTask	Contains the status of the operation	`GetCreateRecovryPlanFailure`
		`GetNewRecoveryPlan`
		`IsCreateRecoveryPlanComplete`

CreateProtectionGroupTask	Handle an ABR or HBR protection group	`GetCreateProtectionGroupResult`
		`GetNewProtectionGroup`
		`IsCreateProtectionGroupComplete`

DeleteRecoveryPlanTask	Contains the status of the operation	`GetDeleteRecovryPlanFailure` `IsDeleteRecoveryPlanComplete`

SrmRecoveryApi1	Old version 1.0 API, deprecated but still provided for backward compatibility	`GetApiVersion`
		`GetFinalStatus`
		`ListRecoveryPlans`
		`RecoveryPlanAnswerPrompt`
		`RecoveryPlanCancel`
		`RecoveryPlanPause`
		`RecoveryPlanResume`
		`RecoveryPlanSettings`
		`RecoveryPlanStart`
		`SrmLogin`
		`SrmLoginByToken`
		`SrmLogout`

DiscoverDevicesTask	Contains the status of the operation	`GetDiscoverDevicesTaskFailures` `IsDiscoverDevicesTaskComplete`

Folder	Site Recovery Manager folder class	`CreateFolder`
		`DestroyFolder`
		`GetChildType`
		`GetName`
		`GetParentFolder`
		`MoveFolder`
		`RenameFolder`

Managed Object	Remarks	Local Methods
SrmInventoryMapping	Map items from the local to the remote site	AddFolderMapping AddNetworkMapping AddResourcePoolMapping AddTestNetworkMapping GetFolderMappings GetNetworkMappings GetResourcePoolMappings GetTestNetworkMappings RemoveFolderMapping RemoveNetworkMapping RemoveResourcePoolMapping RemoveTestNetworkMapping
SrmIpSubnetMapper	Component that resides on the Recovery site. It manages the IP Subnet Mapping between Protection and Recovery site networks.	AddIpMapping GetIpSubnetMappings IpSubnetMappings RemoveIpMappings
ProtectionGroupFolder	Site Recovery Manager folder for protection groups	GetProtectionGroup ListChildProtectionGroupFolders ListChildProtectionGroups
ProtectionTask	Handle VM protection	GetProtectionStatus GetResult GetTasks IsComplete
RecoveryPlanFolder	Site Recovery Manager folder for recovery plans	GetRecoveryPlan ListChildRecoveryPlanFolders ListChildRecoveryPlans
RemoveProtectionGroupTask	Handle protection group removal	GetRemoveProtectionGroupResult IsRemoveProtectionGroupComplete
ReplicatedArrayPair	Query info about RDM devices	GetDevices GetDeviceGroups GetDeviceDiscoveryStatus GetReplicatedDatastores GetOwner QueryReplicatedRdms
SrmExtApiTask	Base external API task	IsSrmExtApiTaskComplete GetSrmExtApiTaskInfo
SrmRecovery	Query recovery plans	CreateRecoveryPlan DeleteRecoveryPlan GetHistory GetRecoveryPlanRootFolder ListPlans MovePlan

Managed Object	Remarks	Local Methods

SrmRecoveryPlan	Run a recovery plan	`AddProtectionGroup`
		`AddTestNetworkMappingToRecoveryPlan`
		`AnswerPrompt`
		`Cancel`
		`GetRecoverySettings`
		`ListPrompts`
		`RecoveryPlanGetInfo`
		`RecoveryPlanGetPeer`
		`RecoveryPlanGetParentFolder`
		`RecoveryPlanGetLocation`
		`RemoveProtectionGroupFromRecoveryPlan`
		`RecoveryPlanHasRunningTask`
		`RemoveTestNetworkMappingFromRecoveryPlan`
		`SetRecoverySettings`
		`Start` (deprecated in 8.5)
		`StartEx`

SrmStorageAdapter	Gets information about a storage adapter	`FetchInfo` `GetAdapterConnectionSpec`

SrmStorage	Access the storage	`CreateArrayManager`
		`DiscoverDevices`
		`QueryArrayManagers`
		`QueryStorageAdapters`
		`ReloadAdapters`
		`RemoveArrayManager`

SrmRecoveryHistory	Recovery plan status	`GetRecoveryResult`
		`GetResultCount`
		`GetResultLength`
		`RetrieveStatus`

SrmServiceInstance	Open or close session, get information about local and remote sites	`BreakPairing`
		`GetLicenseInfo`
		`GetPairedSite`
		`GetSiteName` (deprecated in 6.5)
		`PairSrm`
		`ProbeSsl`
		`ReconfigureConnection`
		`RetrieveContent`
		`SrmLoginLocale`
		`SrmLoginRemoteSite`
		`SrmLoginSites`
		`SrmLogoutLocale`
		`GetLocalSiteInfo`
		`GetSolutionUserInfo`
		`GetPairedSiteSolutionUserInfo`
		`SrmLoginByTokenLocale`
		`SrmLoginRemoteSiteByToken`
		`SrmLoginSitesByToken`

Managed Object	Remarks	Local Methods

SrmProtection	Create an ABR or HBR protection group, list inventory mappings, query datastores and VMs, and list protection groups	`CreateAbrProtectionGroup`
		`CreateHbrProtectionGroup` (deprecated in 8.4)
		`CreateHbrProtectionGroup2`
		`CreateVvolProtectionGroup`
		`GetProtectionGroupRootFolder`
		`ListInventoryMappings`
		`ListProtectionGroups`
		`ListReplicatedDatastores` (deprecated in 6.0)
		`ListUnassignedReplicatedDatastores`
		`ListUnassignedReplicatedVms`
		`ProtectionListProtectedDatastores`
		`ProtectionListProtectedVms`
		`RemoveProtectionGroup`

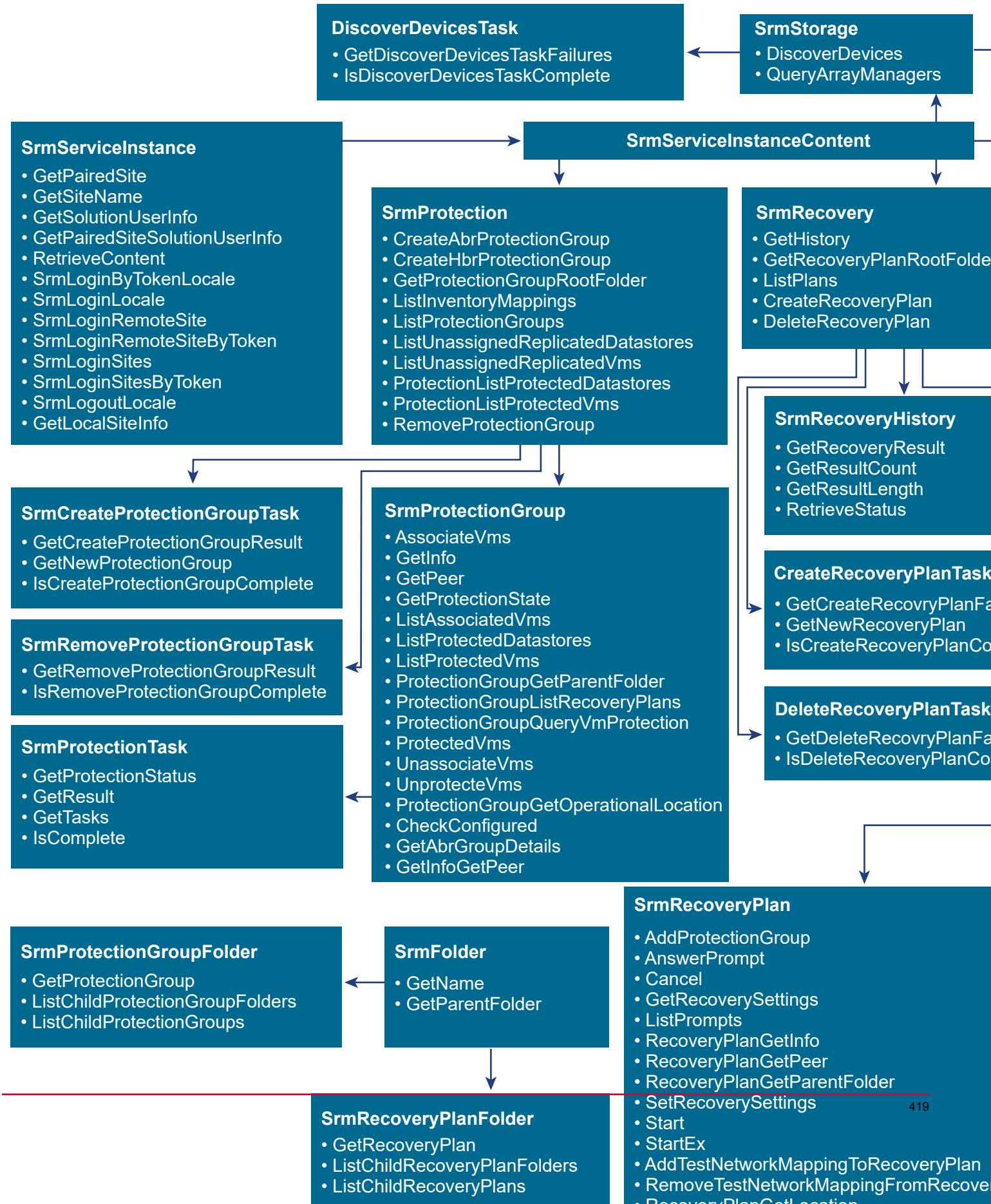
SrmProtectionGroup	Add virtual machines to a protection group, get peer, query protected datastores, add datastore, and remove datastore	`AddDatastores`
		`AssociateVms`
		`CheckConfigured`
		`GetAbrGroupDetails`
		`GetInfoGetPeer`
		`GetPeer`
		`GetPlaceholderVmInfo`
		`GetProtectionState`
		`GetRecoveryLocationSettings`
		`GetVvolGroupDetails`
		`ListAssociatedVms`
		`ListProtectedDatastores`
		`ListProtectedVms`
		`MoveGroup`
		`ProtectionGroupGetOperationalLocation`
		`ProtectionGroupGetParentFolder`
		`ProtectionGroupListRecoveryPlans`
		`ProtectionGroupQueryVmProtection`
		`ProtectVms`
		`ReconfigureRecoveryLocationSettings`
		`ReconfigureVvolProtectionGroup`
		`RecreatePlaceholder`
		`RemoveDatastores`
		`UnassociateVms`
		`UnprotectVms`

SrmVvolReplication	Provide information about the local vVol topology replicated to the SRM peer site	`GetDomains`
		`GetUnprotectedVms`
		`Rescan`

SrmPlaceholderDatastoreManager	Manages placeholder datastores	`AddDatastore`
		`RemoveDatastore`
		`GetPlaceholderDatastores`

The SRM Object Classes graphic shows the Site Recovery Manager managed object class hierarchy with the methods of each managed object.

Figure 14: Site Recovery Manager API Object Classes



Logging into Sites with SAML Tokens

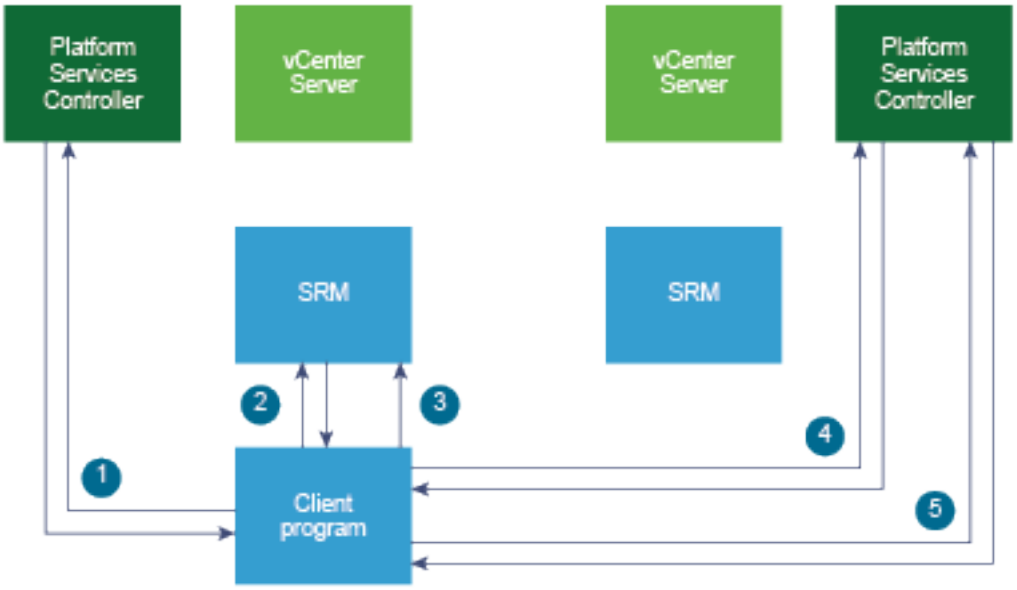
Site Recovery Manager release 6.0 improves security by obtaining a security assertion markup language (SAML) token from the vCenter Single Sign-On service for both the local and remote sites.

Table 169: Functions for Logging Into Sites

Function	Description of Operation
`GetSolutionUserInfo`	Obtain the UUID of Site Recovery Manager Server and the Site Recovery Manager solution user name.
`SrmLoginByTokenLocale`	After obtaining a token from vCenter Single Sign-On, begin session with the local Site Recovery Manager Server
`GetPairedSiteSolutionUserInfo`	Obtain the remote the UUID of Site Recovery Manager Server and the solution user name
`SrmLoginRemoteSiteByToken`	After obtaining remote token, begin session with the paired Site Recovery Manager Server
`SrmLoginSitesByToken`	Log in to both local and remote Site Recovery Manager Server, passing both SAML tokens

The following figure shows the sequence of calling for LoginSitesByToken

Figure 15: Calling Sequence for LoginSitesByToken



Order of operations

1. Obtain local token from the vCenter Single Sign-On service located on the local Platform Services Controller.
2. Get remote site information from Site Recovery Manager, and extract the URL of remote LookupService.
3. Use remote LookupService to find the remote vCenter Single Sign-On service.
4. Obtain remote access SAML token from vCenter Single Sign-On service located on the remote Platform Services Controller.
5. Make the SrmLoginSitesByToken call locally to Site Recovery Manager.

WSDL Programming Environments

You can program Web services and read WSDL files using the C# language with Visual Studio .NET, or using the Java language with the Axis framework or the JAX-WS framework. You can program Web services using many other languages and frameworks, but they are beyond the scope of this manual.

Java JAX-WS Framework

The SDK provides sample code that uses the Java Development Kit (JDK) 1.6 with the JAX-WS framework bundled with the JDK 1.6. The build scripts generate Java stubs from the Site Recovery Manager specific WSDL.

> **NOTE**
> For Site Recovery Manager Appliance Management APIs, use JDK 1.8.0_202.

C# and Visual Studio

The Site Recovery Manager SDK provides sample C# .NET code prepared for use with Visual Studio 2008, which you can convert for use with Visual Studio 2010 and perhaps later versions as well.

> **NOTE**
> For Site Recovery Manager Appliance Management APIs, use Microsoft Visual Studio 2017.

Java Axis Framework

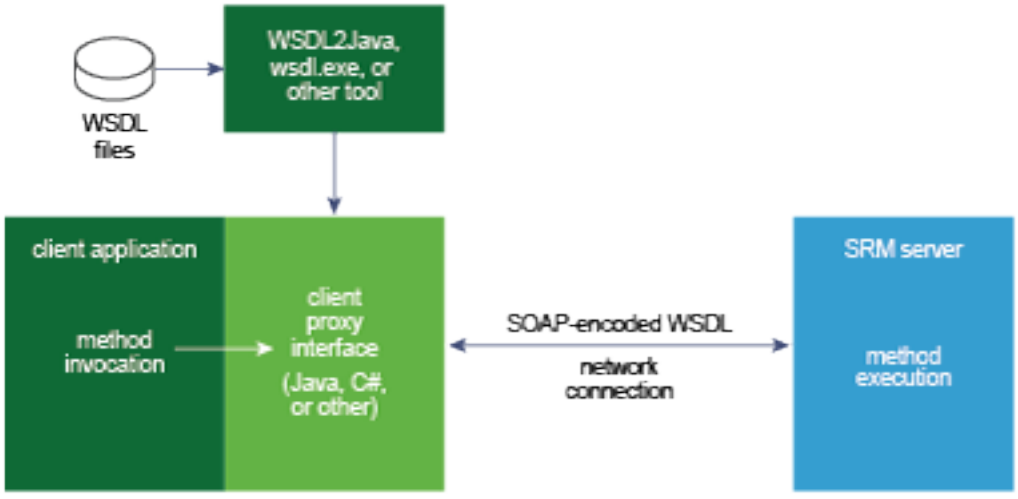
The Site Recovery Manager SDK provides legacy sample code that requires Java SE 1.5 or later and Apache Axis 1.4. Samples are set up for stub generation on Windows or on Linux.

> **NOTE**
> For Site Recovery Manager Appliance Management APIs, use Apache Axis2.

Managed Objects as WSDL

The WSDL Programming Components graphic shows the WSDL programming components used by various language frameworks.

Figure 16: WSDL Programming Components



Site Recovery Manager managed objects and methods are derived from classes and methods in the vSphere API, also known as the virtual machine object description language (VMODL). In the SDK, the Site Recovery Manager interfaces

are mixed in with vSphere interfaces. For specific information about vSphere interfaces, see the *vSphere API Reference* manual, which is in the *vSphere Web Services SDK* under the *VMware vSphere Management SDK*.

Accessing Site Recovery Manager APIs

The Site Recovery Manager Appliance Management API and Site Recovery Manager API provides language-neutral interfaces for configuring Site Recovery Manager Server or OS-specific settings, managing protection groups, and recovery plans. Array-based replication, vSphere Replication, and vVols are supported.

Location of the API

The Site Recovery Manager 8.3 API is located at the following endpoints:

- Site Recovery Manager Appliance Management API
  `https//<FQDN_Server_or_IP_Address>:5480/configureserver/sdk`
- Site Recover Manager APIs for Windows
  `https://<FQDN_Server_or_IP_Address>:9086/vcdr/extapi/sdk`
- Site Recover Manager APIs for Photon Virtual Appliance (VA)
  `https://<FQDN_Server_or_IP_Address>:443/drserver/vcdr/extapi/sdk`

All services use this single network port, and all communications are TLS encrypted. SSLv3 is disabled for security reasons. The API is implemented as an industry-standard Web service running on Site Recovery Manager Server.

The API complies with the Web Services Interoperability Organization (WS-I) Basic Profile 1.0, which includes XML Schema 1.0, SOAP version 1.1, and WSDL version 1.1. For details about WS-I Basic Profile 1.0, see the http://www.ws-i.org website.

Obtaining WSDL for APIs

- WSDL for Site Recovery Manager Appliance Management API: Request the file `drconfig-service.wsdl` from the server root path.
  `https://<FQDN_Server_or_IP_Address>:5480/drconfig-service.wsdl`
- WSDL for Site Recovery Manager API: Request the file `srm-Service.wsdl` from the server root path.
  - On a Windows server, the root path can be `https://<FQDN_Server_or_IP_Address>:9086/srm-Service.wsdl`
  - On a Virtual Appliance, the root path can be `https://<FQDN_Server_or_IP_Address>:443/drserver/srm-Service.wsdl`

Associated vCenter Servers for Site Recovery Manager API

As of SRM 6.0, Platform Services Controller and vCenter Server are associated with the Site Recovery Manager Server at both the local (protected) and the remote (recovery) sites.

Platform Services Controller can be embedded in vCenter Server, or it can be hosted on a separate machine. Platform Services Controller performs three services: Lookup, vCenter Single Sign-On, and Licensing.

The vCenter Server performs tagging and authorization for Site Recovery Manager. A system administrator installs the Site Recovery Manager plug-in at both local and remote sites to control the site's Site Recovery Manager Server through vCenter Server.

Managed object SrmServiceInstance provides functions for local and remote site discovery. You obtain the local site information with `getLocalSiteInfo`, and obtain the local solution user with `GetSolutionUserInfo`.

The local Platform Services Controller LookupService does not know anything about services on the remote site. You obtain the remote site name with `GetPairedSite` and obtain the remote solution user with `GetPairedSiteSolutionUserInfo`. The RemoteSiteobject contains the URL of the remote LookupService, and the UUID of the remote vCenter Server.

SDK Installation and Setup

The SDK Installation and Setup chapter describes how to unpack and use the software development kit (SDK).

Contents of the SDK Package

The Site Recovery Manager SDK is delivered as a ZIP archive (`VMware-srm-sdk-<version>-<build>.zip` file.

You can obtain the SDK package by navigating to http://www.vmware.com/support/developer/srm-api and clicking the **Download SDK** link. You must provide an email address or customer number, with a valid password, for the authentication on the Site Recovery Manager download site.

The package contains:

- Sample code demonstrating common use cases for programmatically managing the Site Recovery Manager server. The sample code includes Java and C# source code files. See the following Readme files for information about building and using the samples:
  - `doc/srm/readme_dotnet.htm`
  - `doc/srm/readme_java.htm`
  - `doc/srm/readme_jaxws.htm`
- Sample code demonstrating common use cases for programmatically configuring the Site Recovery Manager Virtual Appliance. The sample code includes Java and C# source code files. See the following Readme files for information about building and using the samples:
  - `doc/drconfig/readme_jaxws.htm`
  - `doc/drconfig/readme_java.htm`
  - `doc/drconfig/readme_dotnet.htm`
- The WSDL and XML schema files that define the Site Recovery Manager API and Site Recovery Manager Appliance Management API.
- Batch files and shell scripts to automate the process of generating client-side stubs, and for rebuilding the sample applications. For C# developers, the Microsoft Visual Studio project files (.sln) are included.
- Documentation, including VMware Site Recovery Manager API Reference Guide and VMware Site Recovery Manager Appliance Management API Reference Guide, that provides a language-neutral descriptive information about object type definitions, properties, and method signatures for the VMware Site Recovery Manager API 8.3.

SDK Directory Structure

After you unzip the Site Recovery Manager SDK, the following directories and sub-directories appear. Many of the sub-directories contain helpful readme files.

Table 170: SDK Directory Structure

Directory or File	Description
/doc	Contains SDK README files and reference documentation for the SDK.
/doc/srm/ReferenceGuide	API Reference for the Site Recovery Manager API. To view the API Reference, open index.html with a Web browser.
/doc/drconfig/ReferenceGuide	API Reference for the Site Recovery Manager Appliance Management API. To view the API Reference, open index.html with a Web browser.
/doc/SDK_Terms_and_Conditions.*	End-user license agreement for the Site Recovery Manager SDK.

Directory or File	Description
/samples	Top-level directory for language-specific versions of sample client applications.
samples/srm/DotNet	Directory containing command scripts to generate the .NET proxy classes and Web service stubs for the VMware Site Recovery Manager API. The `GeneratingStubs.txt` file gives helpful notes about how to generate stubs with your own namespace for Visual Studio 2008.
samples/srm/DotNet/cs	Directory containing Visual Studio 2008 solution (.sln) file and sub-directories with C# `AppUtil` support code and `RecoveryPlan.cs` sample application with project (.csproj) file VMware Site Recovery Manager API.
/samples/srm/JAXWS	Directory containing Java source code for the JAX-WS framework for the VMware Site Recovery Manager API. Sample program RecoveryPlanList.java is in the `com/vmware/samples/recovery` subdirectory. Shell scripts and batch files are provided to build and run the sample program.
/samples/srm/Axis	Directory containing Java source code for the Axis framework for the VMware Site Recovery Manager API. Sample program RecoveryPlanList.java is in the `java\com\vmware\samples\recovery` subdirectory. Shell scripts and batch files are provided to build and run the sample program.
/wsdl/srm/srm.wsdl	The Web Services Description Language (WSDL) file containing definition of the VMware Site Recovery Manager API.
/wsdl/srm/srm-Service.wsdl	A WSDL file defining the Web services endpoint at which the VMware Site Recovery Manager API is available. This file references the srm.wsdl with an import statement, so you will use the appropriate generation tool with srm-Service.wsdl (rather than srm.wsdl directly).
/wsdl/srm/*.xsd	XML schema definition files (six).
/samples/drconfig/Axis	Directory containing batch files and Axis source code for the VMware Site Recovery Manager Appliance Management API.
/samples/drconfig/DotNet/cs	Directory containing batch files, plus several other subdirectories containing Windows C# sample applications (in the appropriate namespace structure), the Microsoft Visual Studio project files (.sln files) for the VMware Site Recovery Manager Appliance Management API.
/samples/drconfig/JAXWS	Directory containing batch files and JAXWS source code for the VMware Site Recovery Manager Appliance Management API.
/wsdl/drconfig/drconfig.wsdl	The Web Services Description Language (WSDL) file containing definition of the VMware Site Recovery Manager Appliance Management API.

Directory or File	Description
/wsdl/drconfig/drconfig-service.wsdl	A WSDL file defining the Web services endpoint at which the VMware Site Recovery Manager Appliance Management API is available. The drconfig-service.wsdl file references the drconfig.wsdl with an import statement, so you will use the appropriate generation tool with drconfig-service.wsdl (rather than drconfig.wsdl directly).

Download and Setup

Setting up your environment to develop client applications with the SDK involves several steps, but if you are already developing vSphere applications, some of the steps are unnecessary.

1. Select a programming language (C# or Java) for the Web services client application development. You can use Linux or Windows for the Java development. C# development is done on Windows.
2. Identify the target VMware Site Recovery Manager server (or servers) to use for development. A “target server” is a Site Recovery Manager server that your client application manages.
3. Install, or verify the presence of, the development environment appropriate for your programming language.
   - For C#, you need one of the Microsoft development environments, such as Visual Studio 2008 or Microsoft Visual C#. Use Microsoft Visual Studio 2008 or later, which includes the required .NET Framework. For more information, visit the MSDN website.

     NOTE
     For Site Recovery Manager Appliance Management APIs, use Microsoft Visual Studio 2017.
   - You can use Java Standard Edition (SE) 6.0 or 7.0. VMware recommends Java Development Kit (JDK) 1.7.0_45 or later. For more information, visit the Oracle Java website. Open JDK works also.

     NOTE
     For Site Recovery Manager Appliance Management APIs, use JDK 1.8 Update 202.
4. Obtain the appropriate Web services client tools (XML parser, WSDL-to-proxy-code generation tools, and runtime) for your programming language.
   - For C#, you need Microsoft .NET Framework 2.0 or 1.1. If you already use Microsoft development tools, it is likely you already have this. You can obtain the .NET Framework 2.0 from MSDN. You also need the .NET 2.0 Software Development Kit, which includes the WSDL-to-stub generation tool (`wsdl.exe`) and the command-line C# compiler (`csc.exe`), both of which get called from the `gensrmstubs.cmd` script. You can get the .NET 2.0 Software Development Kit from Microsoft: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=19988.
   - For Java with JAX-WS, you can use the JAX-WS framework that includes the JDK.

     NOTE
     For Site Recovery Manager APIs, use Java 1.4. For Site Recovery Manager Appliance Management APIs, use Java 1.8.
   - For Java with Axis, you need the Apache Axis 1.4 client-side Web service libraries. For documentation and downloads, visit the Axis Apache website.

     NOTE
     For Site Recovery Manager Appliance Management APIs, use Apache Axis2.

SDK Samples for Site Recovery Manager Appliance Management API

The Site Recovery Manager SDK package includes sample code demonstrating common use cases for programmatically configuring Site Recovery Manager Virtual Appliance. The sample code includes Java and C# source code files for

building a simple command-line tool. This command-line tool can configure srm-va, retrieve the srm-va configuration, and clear the srm-va configuration.

About C# .NET Samples

This section describes how to build and run the sample code that uses C# .NET for the Site Recovery Manager Appliance Management API. The samples have been developed to work with the Microsoft Visual Studio 2017. They are located in subdirectories contained in the following SDK directory:

`/samples/srm/DotNet`

Build Sample Code with Visual Studio 2017

You can build C# .NET samples using Microsoft Visual Studio 2017.

Procedure

1. Open a Developer Command Prompt for Visual Studio 2017 from the Windows Start Menu.
2. Navigate to the `SDK\samples\drconfig\DotNet` subdirectory.
3. At the command prompt, type BuildSamples.cmd to run the build commands.

Run Sample Code from Visual Studio 2017

Procedure

1. Start Visual Studio.
2. Open the `DrConfigSamples.sln` file.
3. Change the Project Properties to specify the command-line arguments:
   a. From the Project menu, select **Properties** to display the Property Pages dialog box.
   b. In the Project_Name Property Pages dialog box, select **Configuration Properties—Debugging** in the left pane.
   c. In the right pane (under Start Options), select **Command Line Arguments**.
   d. To save the changes, click **OK**.
4. Run the sample at the command prompt.

About Java JAX-WS Samples

This section describes how to build and run the sample code that uses the JAX-WS bindings for the Site Recovery Manager Appliance Management API. The samples have been developed to work with the JAX-WS bundled with the JDK 1.8.0_202. They are located in subdirectories contained in the following SDK directory:

`SDK/samples/drconfig/JAXWS/com/vmware`

Build JAX-WS Sample Code

The build scripts (`build.bat` or `build.sh`) generate Site Recovery Manager Appliance Management API Java stubs from the Site Recovery Manager Appliance Management API WSDL, compile the generated stubs, and compile the sample programs.

Procedure

1. Set the JAVAHOME environment variable to the base directory of your installed JDK 1.8.

For example,

- On Linux, this can be `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.232.b09-0.el7_7.x86_64`, or `/` , depending on your java location
- On Windows, this can be `C:\Program Files\Java\jdk1.8.0_202`

2. Change directory to `sdk/samples/drconfig/JAXWS` and run the build.sh script (or on Windows, the build.bat file) to generate the Site Recovery Manager Appliance Management API Java stubs from the drconfig-Service.wsdl definitions, generate the Java stubs, and compile the sample Java code into class files, from which jars will be created (drconfig.jar, samples.jar and vim25.jar).
   Note the WSDL file dependency: JAX-WS requires a WSDL file for the stub generation and compilation. To manage this dependency, the build script performs the following operations:
   1. Calls the wsimport JDK tool to generate the Site Recovery Manager Appliance Management Java stubs from the Site Recovery Manager Appliance Management API WSDL file (`drconfig-service.wsdl`).
   2. Specifies the wsimport -wsdlLocation command-line option to identify the WSDL file location.
   3. Copies the WSDL file and related schema files into the drconfig.jar file.

The script compiles the Sample Java code, and imports the generated stubs. It uses the drconfig.jar built by the build.sh script. The WSDL file must be in the same location that was specified by the -wsdlLocation command-line option. To establish this location, the build script modifies the DrConfigService class to reference the WSDL location inside the JAR file. The Sample.jar will be modified to have the class path reference to the dependant JAR files.

Run JAX-WS Sample Code

After building, you can run the sample program that uses JAX-WS bindings for the Site Recovery Manager Appliance Management API. The program was developed to work with the JAX-WS framework that is bundled with the JDK 1.8.0_202

Procedure

1. Change directory to `sdk\samples\drconfig\JAXWS`, where the JAR files are located, if you are not already there.
2. Define VMKEYSTORE as the path to the Java key store. This can be the default Java keystore, or custom defined. This is needed to securely access Site Recovery Manager Server.
   ```
   export VMKEYSTORE=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.232.b09-0.el7_7.x86_64/jre/lib/security/cacerts" or your custom java keystore location
   set VMKEYSTORE=C:\Program Files\Java\jdk1.8.0_202\jre\lib\security\cacerts
   ```
   For more information about VMKEYSTORE, see SSL Certificates.
3. Call the run script or batch file to execute the sample program. This sample program prints a usage summary if you do not specify any options or if you specify --help on the command line.

Clean up JAX-WS Sample Code

To explicitly delete the JAX-WS Sample Code, use either a script or a batch file.

Procedure

1. Change directory to `sdk\samples\drconfig\JAXWS`, if you are not already there.
2. Run the `clean.sh` script or the `clean.bat` batch file.

About Java Axis Samples

This section describes how to build and run the VMware sample code that uses the AXIS2 web services for the Site Recovery Manager Appliance Management API. The samples have been developed to work with the AXIS2 version axis2-1.7.9, as for the JAVA use JDK 1.8.0_202. The samples are located in the subdirectories contained in the `SDK/samples/drconfig/Axis/java/com/vmware/samples` directory.

Build JAVA AXIS Sample Code

The build scripts (build.bat or build.sh) generate Site Recovery Manager Appliance Management API Java stubs from the Site Recovery Manager Appliance Management API WSDL, compile the generated stubs, and compile the sample programs.

Procedure

1. Make sure that the Java development kit and Apache Axis2 are installed and functioning.
2. Start the Linux terminal (shell) or Windows command prompt.
3. Set the environment variables as shown in the Java and Axis environment variables table.

Table 171: Java and Axis Environment Variables

Environment Variable	Description and Usage Notes	Example Setting
`AXIS2_HOME`	Complete path to the Apache Axis2 installation top-level directory. Must be set prior to using the build.bat script.	`C:\apache\axis2-1.7.9`
`JAVAHOME`	Path to the binary directory for the Java JDK.	`C:\Program Files\Java\jdk1.8.0_202`

4. Change directory to `sdk/samples/drconfig/Axis/java` and run the `build.sh` script (or on Windows, the `build.bat` file) to compile the sample Java code into a class files.

Run Java Axis Sample Code

Source code build files are located in the `samples\drconfig\Axis\java\com\vmware\samples` directory, as extracted from the ZIP archive.

Procedure

1. Change directory to `sdk/samples/drconfig/JAXWS`, where the JAR files are located.
2. When running the samples, if you are going to use your own certificates, then you must set the `VMKEYSTORE` environment variable to your Java keystore location. `export VMKEYSTORE=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.232.b09-0.el7_7.x86_64/jre/lib/security/cacerts" or custom java keystore location` and `set VMKEYSTORE=C:\Program Files\Java\jdk1.8.0_202\jre\lib\security\cacert`
3. After building the sample program, you can call it with the run script. For example, if you are building the `ConfigureSrm` sample, you can call it using the following command:

   ```
   run.bat com.vmware.samples.drconfig.ConfigureAppliance configure --drconfigaddr
   https://FQDN_or_IP_Address:5480/configureserver/sdk --drconfiguser admin --pscuri
   pscfqdn:443 --pscuser Administrator@vsphere.local
   ```

Clean up JAVA AXIS Sample Code

To explicitly delete the JAVA AXIS Sample Code, use either a script or a batch file.

Procedure

1. Change directory to `SDK/samples/drconfig/Axis/java`, if you are not already there.
2. Run the clean.sh script or the clean.bat batch file.

SDK Samples for Site Recovery Manager API

The Site Recovery Manager SDK package includes sample code demonstrating common use cases for programmatically creating protection groups and initiating test, recovery, and reprotection operations.

About the C# .NET Samples

Currently the SDK includes recovery plan sample code that you can build on .NET. You can build C# .NET samples using Microsoft Visual C# 2008 Express or Microsoft Visual Studio 2008.

If you have a later version of Visual Studio, it might ask to convert the solution and project files before proceeding. An earlier version of this SDK supported Visual Studio 2005. Visual Studio 2003 was never supported because of performance issues (.NET took a long time to instantiate the `VimService` class).

Build Sample Code with Visual Studio 2008

You can build C# .NET samples using Microsoft Visual C# 2008 Express or Microsoft Visual Studio 2008.

1. Open a Visual Studio 2008 command prompt from the Windows Start Menu as follows: **Start** > **Programs** > **Visual Studio 2008** > **Visual Studio Tools** > **Command Prompt**.
2. Start the Windows command prompt.

   On 64-bit Windows systems, run `C:\Windows\SysWOW64\cmd.exe` so the sample programs execute under Windows 32-bit on Windows 64-bit (WOW64).
3. Navigate to the `SDK\samples\DotNet` sub-directory.
4. At the command prompt, type `Build2008.cmd` to execute the build commands.

Build Sample Code with Visual C# 2008 Express

You can build C# .NET samples using Microsoft Visual C# 2008 Express or Microsoft Visual Studio 2008. If you have a later version of Visual Studio, it might ask to convert the solution and project files before proceeding.

1. Select the default (Full) Microsoft Visual C# 2008 Express installation.
2. If you installed Visual C# 2008 Express in the default location, skip this step. Otherwise:
   a) Create the System environment variable `VSINSTALLDIR`.
   b) Set the `VSINSTALLDIR` environment variable to the location of the Microsoft Visual Studio tools, in the `Common7` sub-directory of the Microsoft Visual C# 2008 Express installation. Default locations are shown below. Use quotation marks around directory names that contain spaces, as these do.

      “`C:\Program Files\Microsoft Visual Studio 9.0\Common7`"

      “`C:\apps\Microsoft Visual Studio 9.0\Common7`”

      If Visual C# Express is installed in its default folder `C:\Program Files\Microsoft Visual Studio 9.0`, you do not need to create or set the VSINSTALLDIR environment variable.

3. Open a Visual Studio 2008 command prompt from the Windows Start Menu as follows: **Start** > **Programs** > **Visual Studio 2008** > **Visual Studio Tools** > **Command Prompt**
4. Navigate to the `SDK\samples\DotNet` sub-directory.
5. At the command prompt, type `Build2008.cmd` to execute the build commands.

   The build process generates the RecoveryPlan sample program, which lists all recovery plans and optionally gets state for the specified recovery plan. A sample build can be executed from the `\bin` or `\debug` directory of a project. You can also run samples from within Visual Studio, at the .NET command prompt. To display help text for any application, you can run the application without any parameters.

Run Sample Code from Visual Studio

You can build C# .NET samples using Microsoft Visual C# 2008 Express or Microsoft Visual Studio 2008.

1. Start Visual Studio.
2. Open the `Sample2008.sln` solution file.
3. Change the Project Properties to specify the command line arguments:
   a) From the **Project** menu, select **Properties** to display the **Property Pages** dialog.
   b) In the Project_Name Property Pages dialog, select **Configuration Properties—Debugging** on the left.
   c) In the right-hand pane (under Start Options), select **Command Line Arguments**.
   d) Click **OK** to save your changes.
4. Run the sample code at the command prompt.

Run C# Sample Code

You can build C# .NET samples using Microsoft Visual C# 2008 Express or Microsoft Visual Studio 2008.

1. After you generate the sample program, you can run it as follows: `RecoveryPlan --url <webserviceurl> --username <user> --password <passwd> --planname <plan>`

   The `RecoveryPlan` program lists all recovery plans and optionally gets the state for the plan specified after the `--planname` option.
2. You can remove build files by running the `clean.bat` batch script.

About Java JAX-WS Samples

This section describes how to build and run the sample program that uses JAX-WS bindings for the Site Recovery Manager API.

The program was developed to work with the JAX-WS framework that is bundled with the JDK 1.6 and later Java source code is located in the `samples/JAXWS/com/vmware/samples/recovery` directory, as extracted from the ZIP archive.

Build JAX-WS Sample Code

The sample program that uses JAX-WS bindings for the Site Recovery Manager API was developed to work with the JAX-WS framework that is bundled with the JDK 1.6 and later.

1. Set the `JAVAHOME` environment variable to the base directory of your installed JDK.

   On Linux this could be `/usr/lib/jvm/java-7-openjdk-i386` for example.

   On Windows this could be `C:\Program Files\Java\jdk1.7.0_65` for example.

2. Change directory to `sdk/samples/JAXWS` and run the `build.sh` script (or on Windows, the `build.bat` file) to generate the Site Recovery Manager API Java stubs from the `srm-Service.wsdl` definitions, generate the Java stubs, and compile the sample Java code into a class file.

   Note the WSDL file dependency: JAX-WS requires a WSDL file for stub generation and compilation. To manage this dependency, the build script performs the following operations:

   - It calls the wsimport JDK tool to generate Java stubs from the `srm-Service.wsdl` SRM WSDL file.
   - It specifies the wsimport -wsdlLocation command line option to identify the WSDL file location.
   - It copies the WSDL file and related schema files into the `srm.jar` file.

   To compile Java code that imports the generated stubs and uses the `srm.jar` built by the `build.sh` script, the WSDL file must be in the same location that was specified by the `-wsdlLocation` command line option. To establish this location, the build script modifies the `SrmService` class to reference the WSDL location inside the JAR file. Then you just need to add the `srm.jar` file to your class path.

Run JAX-WS Sample Code

After building, you can run the sample program that uses JAX-WS bindings for the Site Recovery Manager API. The program was developed to work with the JAX-WS framework that is bundled with the JDK 1.6 and later.

1. Change directory to `sdk\samples\JAXWS`, where the JAR files are located, if you are not already there, and set `CLASSPATH`. Sometimes `%CLASSPATH%` has already been set system wide. Example settings for Linux and Windows are `export CLASSPATH=/usr/lib/jvm/java-7-openjdk-i386/lib` and `set CLASSPATH=%JAVAHOME%\lib`.
2. Define `VMKEYSTORE` as the path to the Java key store. This is needed to securely access Site Recovery Manager Server.

   ```
   export VMKEYSTORE=/usr/share/mime/application/x-java-keystore.xml
   ```

   ```
   set VMKEYSTORE=C:\cygwin\usr\share\mime\application\x-java-keystore.xml
   ```

   For more information about `VMKEYSTORE`, see SSL Certificates.
3. Call the run script or batch file. This sample program prints its usage summary, as if you specified --help on the command line, `run.sh com.vmware.samples.recovery.RecoveryPlanList` or `run.bat com.vmware.samples.recovery.RecoveryPlanList`.
4. As you can see from the usage message, the RecoveryPlanList sample code requires a user name and password for log in to the Site Recovery Manager administrator account. You need to pass in additional options: `--username srmadmin --password secret --planname myRecoveryPlan`

Clean Up JAX-WS Sample Code

You can clean up the JAX-WS Sample Code by using either a script or a batch file.

1. Change directory to `sdk\samples\JAXWS`, if you are not already there.
2. Run the `clean.sh` script or the `clean.bat` batch file.

About Java Axis Samples

This section describes how to build and run the sample program that uses Axis Web services for the Site Recovery Manager API.

Axis can be downloaded from the Apache Web site, or as the libaxis-java package in some Linux distributions. Axis works with JDK 1.6 and later. Source code build files are located in the `samples/Axis/java` directory, as extracted from the ZIP archive.

Build Java Axis Sample Code

You can build the sample program that uses Axis Web services for the Site Recovery Manager API. Axis can be downloaded from the Apache Web site, or as the `libaxis-java` package in some Linux distributions. Axis works with JDK 1.6 and later. Source code build files are located in the `samples/Axis/java` directory, as extracted from the ZIP archive.

1. Make sure the Java development kit and Apache Axis are installed and functioning.
2. Start the Linux terminal (shell) or Windows command prompt.
3. Set the environment variables as shown in the Java and Axis environment variables table.

Table 172: Java and Axis environment variables

Environment Variable	Description and Usage Notes	Example Setting
`AXISHOME`	Complete path to the top-level Axis installation directory. Must be set before using the build scripts.	`C:\Apache\axis1.4 /usr/share/java`
`JAVAHOME`	Path to the binary directory for the Java JDK.	`C:\Java\jdk1.7.0_65 /usr/lib/jvm/java-7-openjdk-i386`

4. Change directory to `sdk/samples/Axis/java` and run the `build.sh` script (or on Windows, the `build.bat` file) to compile the sample Java code into a class file.
5. If the build script produces error messages about missing classes (could not find or load a class), edit the script and change the `LOCALCLASSPATH` line so path names refer to the proper jar file versions. Some Java archives contain symbolic links where a generic file points to a specific version of the jar file.

   The script takes time to build the `RecoveryPlanList` sample program, which lists all recovery plans, or optionally gets state for a specified recovery plan.

   NOTE
   The sample program was written for Axis version 1. It may require modifications for version 2.

Run Java Axis Sample Code

Source code build files are located in the `samples/Axis/java` directory, as extracted from the ZIP archive.

1. Change directory to `sdk/samples/JAXWS`, where the JAR files are located, if you are not already there, and set `CLASSPATH`. Example settings for Linux and Windows are `export CLASSPATH=/usr/lib/jvm/java-7-openjdk-i386/lib` and `set CLASSPATH=%JAVAHOME%\lib`

   Sometimes `CLASSPATH` has already been set system wide.
2. Define `VMKEYSTORE` as the path to the Java key store. This is needed to securely access a Site Recovery Manager Server, `export VMKEYSTORE=/usr/share/mime/application/x-java-keystore.xml` and `set VMKEYSTORE=C:\cygwin\usr\share\mime\application\x-java-keystore.xml`
3. After you build the sample program, you can call it with the run script as follows, `run.sh com.vmware.samples.recovery.RecoveryPlanList --url <srm-URL> --username <user> --password <passwd>`

   If you include the `--ignorecert` option, the sample code runs the following to get around an untrusted server certificate: `System.setProperty("org.apache.axis.components.net.SecureSocketFactory", "org.apache.axis.components.net.SunFakeTrustSocketFactory");`

Clean Up Java Axis Sample Code

You can clean up the JAVA Axis sample code by either running a script or a batch file.

1. Change directory to `sdk/samples/Axis/java`, if you are not already there.
2. Run the `clean.sh` script or the `clean.bat` batch file.

Logical Usage Order - Site Recovery Manager Appliance Management API

This chapter contains descriptions for Site Recovery Manager Appliance Management APIs.

The API descriptions in this chapter follow the logical usage order of List of API Operations. In examples below, `MoRef` indicates a String that references a managed object.

Appliance Manager

This section describes the tools to manipulate the appliance of Site Recover Manager server. These operations are applicable on SRM, VRMS, and VRS deployments.

GetAllTimeZones

This method gets all available time zones. It returns a list representing all the available time zones.

Synopsis

```
String[] getAllTimeZones();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetCurrentDateTime

This method gets the current date and time of the appliance. It returns a vmodl.DateTime object with the appliance date and time.

Synopsis

```
DateTime getCurrentDateTime();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetCurrentTimeZone

This method gets the current time zone of the appliance. It returns a string representing the current time zone.

Synopsis

```
String getCurrentTimeZone();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetDiskInfo

This method retrieves appliance disks information. It returns an array of `DiskInfo` objects, which contain disk information about the appliance.

Synopsys

```
DiskInfo[] getDiskInfo();
```

> **NOTE**
> If the returned DiskInfo object has zero as totalSize value, it is an indication that some error occurred while getting the partition size.

DiskInfo contains appliance disk info. It has the following fields:

Field	Description
`name`	Appliance hostname.
`partitionName`	Partition name. For example, root, swap, core, log, etc.
`description`	ALocalized description.
`usedSize`	Disk used size in bytes
`totalSize`	Total disk size in bytes

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetInfo

This method retrieves appliance information. It returns an ApplianceInfo object which contains information about the appliance.

Synopsis

```
ApplianceInfo getInfo();
```

`ApplianceInfo` contains information about the appliance. It has the following fields:

Field	Description
`hostname`	Appliance hostname
`srmBuild`	Appliance product (SRM) build number

Field	Description
srmProduct	Appliance product name
srmVersion	Appliance product (SRM) version
vaFullVersion	Virtual appliance full version - version + build number
vaBuildNumber	Virtual appliance build number
systemInfo	System information

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetNetworkInfo

This method retrieves appliance network information. It returns a NetworkInfo object which contains network information about the appliance.

Synopsis

```
NetworkInfo getNetworkInfo();
```

`NetworkInfo` contains network information of the appliance. It has the following fields:

Field	Description
DnsInfo dns	DNS information about the appliance.protectedNetwork
InterfaceInfo[] interfaces	Class that contains network interface information about the appliance.

`DnsInfo` contains information about the DNS configuration of the appliance. It has the following fields:

Field	Description
DnsMode	Enum that describes the source of DNS servers. It enumerates the following values: • `DHCP`: DNS servers addresses that are obtained from a DHCP server. • `STATIC`: The DNS servers addresses are specified explicitly.
dnsMode	DNS mode. The value should be one of DnsMode enum.
hostname	Hostname
servers	Servers. This value is ignored while in DHCP mode.

`InterfaceInfo` contains network interface information about the appliance. It has the following fields:

Field	Description
`name`	Interface name. For example, "nic0", "nic1".
`interfaceStatus`	Interface status. The value should be one of the `InterfaceStatus` Enums.
`mac`	MAC address. For example, 00:0C:29:94:BB:5A.
`IPv4Info ipv4`	IPv4 Address information.
`IPv6Info ipv6`	IPv6 Address information.

`IPv4Info` defines the IPv4 configuration state of a network interface. It has the following fields:

Field	Description
`interfaceName`	Interface name. For example, "nic0", "nic1".
`mode`	Address assignment mode. Value should be one of the IPv4Mode enums.
`address`	IPv4 address, for example, "10.20.80.191". Value not needed when DHCP mode.
`prefix`	IPv4 CIDR prefix, for example , 24. This value is not required while in DHCP mode. For more information, see http://www.oav.net/mirrors/cidr.html for netmask-to-prefix conversion.
`defaultGateway`	IPv4 address of the default gateway. This Value is not required while in DHCP mode.

`IPv4Mode` defines different IPv4 modes. It has the following fields:

Field	Description
`DHCP`	IPv4 address is automatically assigned by a DHCP server.
`STATICMODE`	IPv4 address is static.
`UNCONFIGURED`	The IPv4 protocol is not configured.

`IPv6Info` contains IPv6 info on a particular interface. It has the following fields:

Field	Description
`interfaceName`	Network interface. For example, "nic0" to configure.
`dhcp`	Address assigned by a DHCP server. This option can be set to true in parallel with autoconf and static IPv6 addresses.
`autoconf`	Address is assigned by Stateless Address Autoconfiguration (SLAAC). This option can be set to true in parallel with dhcp and static IPv6 addresses.
`IPv6Address[] addresses`	A list of addresses to be statically assigned. Values can be available in parallel with set dhcp and autoconf.

Field	Description
defaultGateway	Default gateway for static IP address assignment. This configures the global IPv6 default gateway on the appliance with the specified gateway address and interface. This gateway replaces the existing default gateway configured on the appliance. However, if the gateway address is link-local, then it is added for that interface. This does not support configuration of multiple global default gateways through different interfaces.

IPv6Address is used for naming an IPv6 address. It has the following fields:

Field	Description
address	IPv6 address, for example, fc00:10:20:83:20c:29ff:fe94:bb5a.
prefix	IPv6 CIDR prefix, for example, 64.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetTimeSyncConfig

This method gets the appliance time sync mode. It returns a TimeSyncInfo object representing the timeSyncMode.

Synopsis

```
TimeSyncInfo getTimeSyncConfig();
```

TimeSyncInfo has the following fields:

Field	Description
TimeSyncMode	The TimeSyncMode defines time synchronization modes. It enumerates the following: • DISABLED: Time synchronization is disabled. • NTP: NTP-based time synchronization. • HOST: VMware Tool-based time synchronization.
timeSyncMode	The Time Synchronization Mode. Must be one of the enum values.
ntpServers	NTP servers. Used only when timeSyncMode is NTP.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

Restart

This method restarts the appliance.

Synopsis

```
void restart();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

SetCurrentTimeZone

This method sets the appliance time zone.

Synopsis

```
void setCurrentTimeZone(String timeZone)
```

`timeZone` parameter represents the time zone.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

SetNetworkInfo

This method sets the appliance network information.

Synopsis

```
void setNetworkInfo(NetworkInfo networkInfo)
```

`networkInfo` parameter is a NetworkInfo object that contains network information of the appliance.

`NetworkInfo` contains network information of the appliance. For more information see GetNetworkInfo

Faults

- InvalidArgument
- InvalidNetworkConfiguration
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

SetTimeSync

This method sets appliance time sync information.

Synopsis

```
void setTimeSync(TimeSyncInfo timeSyncInfo)
```

`timeSyncInfo` is a TimeSyncInfo that contains the time sync information of the appliance. For more information, see GetTimeSyncConfig.

Faults

- HostUnreachableFault
- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

Stop

This method stops the appliance.

Synopsis

```
void stop();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

Configuration Manager

This section describes the tools to configure the SRM server.

GetRunningTask

This method gets the currently active configuration task or null.

Synopsis

```
ConfigurationTask getRunningTask();
```

`ConfigurationTask` is a managed object that provides operations to configure the SRM server. For more information, see Configuration Task.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

CheckRegistration

This method checks whether the given extension key is already registered in SSO, lookup service, and as a vCenter extension. Returns a list of existing registrations for the requested extension key.

Synopsis

```
Registration[] checkRegistration(String adminUser, @secret String adminPassword, ConnectionSpec connection,
 String extensionKey)
```

`CheckRegistration` has the following parameters:

Field	Description
`adminUser`	Name of a user with sufficient privileges to perform checks.
`adminPassword`	Password for the administration user.
`connection`	The connection specification. For more information about connection `ConnectionSpeck` see ClearSrmConfiguration.
`extensionKey`	`extensionKey` for which checks should be performed. This value is returned in the result: `Registration.extensionKey`

`Registration` contains information about existing LS++, SSO, or vCenter registration. It has the extensionKey field which is the requested extension key.

Faults

- InvalidLogin
- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ClearSrmConfiguration

This method clears the SRM server configuration with the vSphere infrastructure. Returns a task object that can be used to monitor the operation.

Synopsis

```
ConfigurationTask clear(ConfigurationSpec config)
```

`config` parameter is a `ConfigurationSpec` data object that contains SRM configuration specification.

`ConfigurationSpec` has the following fields:

Field	Description
`siteName`	The SRM site name. If not set the site name is read from the current SRM configuration if it exists.
`hostName`	The SRM server FQDN. Used when registering with infrastructure and management nodes. If not set, the DNS name will be used.
`extensionKey`	The SRM extension key. If not set the default extension key value of "com.vmware.vcDr" will be used.

Field	Description
clockToleranceSeconds	The allowed server clock tolerance in seconds. If not set the default value of 3 seconds will be used. This parameter is used only when validating the VC server where SRM will be registered. Clock difference between SRM virtual appliance and vCenter Server should not exceed this value, otherwise the validation (or configuration) fails.
ConnectionSpec connection	The connection specification. If not set the connection parameters will be read from the current SRM configuration if it exists.
adminUser	The name of a user with sufficient privileges to perform configuration tasks on the infrastructure and management nodes as well as SSO service configuration tasks on the infrastructure node.
adminPassword	Password for the administrator user.
deleteSrmData	Delete SRM data. Used only when clearing SRM configuration. If set to true, existing SRM database will be deleted.
extraConfig	Additional configuration settings in XML format. These settings are used to upgrade database.
localSrmUuid	UUID of the local SRM Server. This is out parameter returned by `ConfigurationManager.readCurrentConfig()`
organization	Organization name.
description	Plugin description.
adminEmail	Admin email.
moId	Managed Object ID of this VM.
UICapabilities uiCapabilities	A data object that represents what UI capabilities should be enabled.

`ConnectionSpec` is a structure that contains connection information for a service. It has the following fields:

Field	Description
uri	The PSC node URI. FQDN + optional port. If port not specified 443 will be used.
thumbprint	Thumbprint of the PSC node's certificate. When the correct value is provided all security checks of the certificate are off.
vcInstanceId	Identifier of the MGMT node to register with. If not specified the configuration service will assume embedded environment is used and will look for MGMT node services at the PSC node address.
vcThumbprint	Thumbprint of the MGMT node's certificate.

`UICapabilities` is a structure that contains information about the DR-UI functionality.

Field	Description
showApplianceConfigLink	Boolean to indicate whether VC plugin should display the link to the management address.

`ConfigurationTask` is a managed object that provides operations to configure the SRM server. For more information, see Configuration Task.

Faults

- InvalidArgument
- RuntimeFault
- ServiceBusy
- SrmAlreadyRunning

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ConfigureSrm

This method configures the SRM server and connects it to the vSphere infrastructure.

Synopsis

```
ConfigurationTask configure(ConfigurationSpec config)
```

`config` parameter is a ConfigurationSpec data object that contains SRM configuration specification. For more information, see ClearSrmConfiguration.

`ConfigurationTask` is a managed object that provides operations to configure the SRM server. For more information, see Configuration Task.

Faults

- InvalidArgument
- RuntimeFault
- ServiceBusy
- SrmAlreadyRunning

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ConfigureSyslogForwarding

This method sets syslog log forwarding. When `enable` is set to true, this method adds a rule to syslog configuration for given apps and restarts rsyslog service. With this rule, all the logs written by these apps to syslog are forwarded to the specified server. Note that the rule will be either appended or updated in the syslog configuration file and this does not remove any existing rules for other apps. When `enable` is set to false, the existing rules for given apps added with this method are deleted.

Synopsis

```
void configureSyslogForwarding(boolean enable, @optional String[] appNames, SyslogForwardInfo info, @optional
 LogLevelInfo[] logLevels)
```

`ConfigureSyslogForwarding` has the following parameters:

Field	Description
`enable`	True to enable log forwarding, false to disable.
`appNames`	An array containing application names for which log forwarding should be configured. Values must be one of the enums `AppName`. This value is not used since @version3.
`info`	Structure that holds log forwarding information.
`logLevels`	An array containing information about the services syslog log levels. The last value of a duplicate service is taken. If a service is not specified, a default log level of info is set. Services need to be explicitly restarted in order for the changes to take effect.

`SyslogForwardInfo` contains information for syslog log forwarding. It has the following fields:

Field	Description
`Protocol`	Enumerates the list of available protocols to use. The available constants are tcp, udp, and relp.
`host`	IP address or FQDN of the syslog server to which the logs will be forwarded.
`port`	Port of the syslog server to which the logs will be forwarded.
`protocol`	Protocol to use for log forwarding. The value must be one of the `Protocol` enums.

`LogLevelInfo` has the following fields:

Field	Description
`AppNames`	Enumerates the application names available for syslog configuration. The values are srm, drconfigurator, hms, hbrsrv, drclient, and drconfigui.
`VmacoreLogLevel`	Enumerates the list of Vmacore log levels, which are none, quiet, panic, error, warning, info, verbose, and trivia.
`JavaLogLevel`	Enumerates the list of Java log levels, which are OFF, FATAL, ERROR, WARN, INFO, DEBUG, TRACE, and ALL.
`service`	The service should correspond to one of the AppNames enum values.
`logLevel`	Specified log level. This should coresspond to one of the values in the `VmacoreLogLevel` or `JavaLogLevel` enum values. Srm, drconfigurator, and hbrsrv expect value from the `VmacoreLogLevel`. Hms, drclient, and drconfigui expect value from the `JavaLogLevel` enum.
`restart`	It is a boolean value. Specifies whether the service should be restarted for the log level configuration to take effect.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ConfigureSyslogServers

This method sets the syslog log forwarding. It configures all the SRM applications to forward to the specified servers. Receiving null deletes all the configurations. The new spec completely replaces the old configured servers.

Synopsis

```
void configureSyslogServers(@optional SyslogForwardInfo[] info, LogLevelInfo[] logLevels)
```

- `info` parameter is a list of `SyslogForwardInfo` objects.
- `SyslogForwardInfo` object contains information for syslog log forwarding. For more information, see ConfigureSyslogForwarding.
- `Loglevels` parameter is a list containing information about the services syslog log levels. If a service is not specified, a default log level information is set. Services need to be explicitly restarted for the changes to take effect. For more information, see ConfigureSyslogForwarding.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

EnableSyslogLogging

This method enables or disables logging to syslog. When enabling syslog logging for SRM, this method call must be preceded by `configure` call which will generate the SRM configuration file.

Synopsis

```
void enableSyslogLogging(boolean enable, @optional String[] appNames)
```

`EnableSyslogLogging` has the following parameters:

Field	Description
`enable`	True to enable logging to syslog and false to disable.
`appNames`	List of application names for which logging to syslog should be set. Values must be one of the enums`AppName`. App must be stopped before calling this method. This value not used since @version3.

Faults

- InvalidArgument
- RuntimeFault
- SrmAlreadyRunning
- SrmNotConfigured

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetSyslogServers

This method gets the syslog log forwarding information. Returns fwdInfo which is a list of `SyslogForwardInfo` objects that contain information about all the syslog servers.

Synopsis

```
SyslogForwardInfo[] getSyslogServers()
```

`SyslogForwardInfo` contains information for syslog log forwarding. For more information, see ConfigureSyslogForwarding.

Faults

- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

IsReconfigureRequired

This method checks if the reconfigure operation is required after an upgrade. Returns the boolean True if the reconfiguration is required. Reconfiguration is required after an upgrade when the Site Recovery Manager has been configured prior to the upgrade operation. This flag is not set after the upgrade if the Site Recovery Manager was never configured.

Synopsis

```
boolean isReconfigureRequired();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ListVcServices

This method lists all the vCenters in the Platform Service Controller (PSC).

Synopsis

```
VcInfo[] listVcServices(String pscUri, @optional String pscThumbprint, @optional String serviceId)
```

`listVcServices` has the following parameters:

Parameter	Description
`pscUri`	Platform Service Controller URI.
`pscThumbprint`	Thumbprint of the PSC node's certificate. When the correct value is provided all security checks of the certificate are off.
`serviceId`	Optionally narrow VC search to a specific service ID.

`VcInfo` contains vCenter information. It has the following fields:

Field	Description
`url`	vCenter URL
`serviceId`	Service ID
`nodeId`	Node ID
`productVersion`	Product version.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ReadCurrentConfig

This method reads the specification for the currently configured SRM server. Returns null if the SRM is not yet configured. If a configuration task is currently in progress this method returns its config parameter.

Synopsis

```
ConfigurationSpec readCurrentConfig();
```

`ConfigurationSpec` is a data object that contains SRM configuration specification . For more information, see ClearSrmConfiguration.

Faults

- DatabaseConnectionFault
- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

SendSyslogTestMessage

This method sends a test message to all the configured syslog servers. It sends a specified message to the syslog servers. The operation to send a message cannot get the result for the connection, so the client must manually verify that the syslog server logs contain the specified string. The test message is hardcoded.

Synopsis

```
void sendSyslogTestMessage(String message)
```

`message` parameter is the content of the test message.

Faults

- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ValidateConnection

This method validates connections to the vSphere infrastructure. If there is no explicit and valid `vcInstanceId` in the connection spec, no vCenter validation is done. Only the infranode is validated.

Synopsis

```
void validateConnection(String adminUser, @secret String adminPassword, ConnectionSpec connection)
```

`ValidateConnection` has the following parameters:

Parameter	Description
`adminUser`	The name of a user with sufficient privileges to perform configuration tasks on the infrastructure and management nodes and SSO service configuration tasks on the infrastructure node.
`adminPassword`	Password for the administration user.
`connection`	The connection specification. For more inforamtion about `ConnectionSpec`, see ClearSrmConfiguration.

Faults

- InvalidArgument
- InvalidLogin
- RuntimeFault
- SsoTokenNotAcquired
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

SetHbrSrvNic

Sets the HBR filter and management addresses.

Synopsis

```
void setHbrSrvNic(HbrFilterInfo filterInfo)
```

`setHbrSrvNic` has the following parameters:

Field	Description
`filterInfo`	A `HbrFilterInfo` data object representing the filter and management addresses.

`HbrFilterInfo` data object type describes the HBR filter and management traffic. It has the following fields:

Field	Description
`filterIp`	Filter IP address. Can be empty.
`managementIp`	Management IP address. Can be empty.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetHbrSrvNic

Gets the HBR filter and management IP addresses.

Synopsis

```
HbrFilterInfo getHbrSrvNic()
```

`getHbrSrvNic` returns `HbrFilterInfo` data object representing the filter and management addresses. For more information, see SetHbrSrvNic.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetServicesSyslogLogLevel

It returns the configured log level that is forwarded via syslog, for each supported service.

Synopsis

```
LogLevelInfo[] getServicesSyslogLogLevel()
```

NOTE
This method returns all configured services. For more information, see the LogLevelInfo table. If a service is not restarted, the changes might not correspond with the actual value.

Faults

- SystemError
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Configuration Task

This section describes the operations to configure the SRM server. These operations are applicable according to the API that return this data object, generally SRM and VRMS.

GetTaskInfo

This method gets the current configuration task status.

Synopsis

```
ConfigurationTaskInfo getTaskInfo();
```

`ConfigurationTaskInfo` provides status information for a configuration task. It has the following fields:

Field	Description
`TaskType`	Enumerates the list of following task types: • clear • configuration • installUpdate • retrieveUpdate • generateBundle • getSraImages
`complete`	Flag to indicate whether the task has completed.
`progress`	Overall configuration progress.
`currentOp`	Current operation name.
`currentOpProgress`	Current operation progress.
`startTime`	Time stamp when the task started running.
`completeTime`	Time stamp when the task was completed.
`cancelled`	Flag to indicate whether the client requested cancellation of the task.
`error`	If the configuration state is 'failed', then this property contains the fault code.
`result`	The result of the task.
`type`	Type of the task. Can be one of the `TaskType` enum values.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

CancelSrmConfiguration

This method cancels a running configuration task. Multiple cancel requests are treated as a single cancellation request. Cancelling a completed or an already cancelled task throws `ServiceIdle` exception. If successfully canceled, the `StateInfo.error` property is set to `RequestCanceled`. A cancel operation is asynchronous. The operation may return before the task is cancelled. After invoking it, the configuration task continues to remain working, and it can still succeed. In such a situation, the `StateInfo.cancelled` property is set.

Synopsis

```
void cancel()
```

Faults

- RuntimeFault
- ServiceIdle

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

Database Manager

This section describes the operations to configure SRM database. These operations are applicable only on SRM deployments.

ReadStatus

This method checks the database status and returns the version information.

Synopsis

```
DatabaseStatus readStatus()
```

`DatabaseStatus` provides the database status information. It contains currently installed database version and the database version of the currently running service. It also contains the currently used ODBC driver version and name. It has the following fields:

Field	Description
`drVersion`	Database version. This can be unset if the database is empty.
`runtimeVersion`	DB manager runtime version.
`upgradeRequired`	Flag set if the versions do not match and upgrade is required.
`driverName`	ODBC driver name.
`driverVersion`	ODBC driver version.
`licenseAssetId`	License asset identifier. Unset if the SRM was not started.

Faults

- ReadDbStatusFault
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

ChangePassword

This method changes the embedded database password.

Synopsis

```
void changePassword(@secret String oldPassword, @secret String newPassword)
```

`ChangePassword` has the following parameters:

Parameter	Description
`oldPassword`	Old password for the database.
`newPassword`	New password for the database.

Faults

- ChangePasswordFault
- RuntimeFault
- SrmAlreadyRunning

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Diagnostic Manager

This section describes the interface to get the Site Recovery Manager system log bundles that contains log files, cores, and configuration files that are useful for the diagnosis of issues. These operations are applicable on SRM, VRMS, and VRS deployments.

GetRunningTask

This method gets the currently active diagnostic task or null.

Synopsis

```
ConfigurationTask getRunningTask();
```

`ConfigurationTask` is a managed object that provides operations to configure the SRM server. For more information, see Configuration Task.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GenerateSystemLogBundle

This method instructs the server to generate a system log bundle. A log bundle includes log files and other configuration information that can be used to investigate failures. The bundle can be retrieved with calls to `retrieveSystemLogBundle(String, long, long)` method.

The Site Recovery Manager maintains five outstanding bundles. This method returns Configuration Task object that can be used to monitor the operation. `ConfigurationTask.getTaskInfo` method returns the current task status.

Synopsis

```
ConfigurationTask generateSystemLogBundle()
```

`ConfigurationTask.getTaskInfo` returns `SystemLogBundleInfo`. It has the following fields:

Parameter	Description
`key`	The unique key for this bundle.
`type`	The type of the file generated by the Diagnostics Manager. The value can be either "zip", "gz", or "txt". This value is used by the client to construct a file with the proper extension.
`timeCreated`	The date and time when the bundle was generated. This is the local server time in UTC.
`size`	The size in bytes of the diagnostic bundle file.
`md5`	The MD5 checksum for the bundle file. Can be used to verify its contents after page assembly using `retrieveSystemLogBundle(String, long, long)`.
`url`	The URL to download the bundle.

Faults

- RuntimeFault
- ServiceBusy

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

RetrieveSystemLogBundle

This method retrieves the log bundle using the `Binary` data type. The bundle is downloaded in chunks which the client is supposed to assemble into a single file. The MD5 checksum in `SystemLogBundleInfo` object can be used to verify that the retrieved file is correctly assembled. It returns a binary object containing the requested chunk of the bundle file. Its size may be less than the `maxPageSize`.

Synopsis

```
Binary retrieveSystemLogBundle(String key, long offset, long maxPageSize)
```

`RetrieveSystemLogBundle` has the following parameters:

Parameter	Description
`key`	The `SystemLogBundleInfo.key` returned by a call to `generateSystemLogBundle()` method.
`offset`	Byte offset into the bundle file to the start of the chunk that is to be returned.
`maxPageSize`	Maximum size in bytes of the chunk to be returned. This parameter can be used to control the size and number of chunks while retrieving a bundle. The maximum page size can also be limited internally by the server so the size of the returned chunk may be smaller than `maxPageSize` even if the bundle file contains more bytes.

Faults

- OutOfBounds
- RuntimeFault
- SystemLogBundleNotFound

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DeleteSystemLogBundle

This method instructs the server that a specific log bundle is no longer needed by the client that generated it. The server can then safely delete the file.

Calling this method after each call to GenerateSystemLogBundle method helps the server work more efficiently.

Synopsis

```
void deleteSystemLogBundle(String key)
```

`DeleteSystemLogBundle` has the following parameters:

Parameter	Description
`key`	`SystemLogBundleInfo.key` returned by a call to `generateSystemLogBundle()` method. For more information, see GenerateSystemLogBundle.

Faults

- RuntimeFault
- SystemLogBundleNotFound

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

Service Instance

The ServiceInstance managed object is the singleton object which provides access to the functionality of the Site Recovery Manager Appliance Management Server. Authorization and authentication support are limited to local OS users and method only privileges.

Do not specify the parameter privileges as they do not work. The authorization code currently recognizes only the following privileges:

- **System.Anonymous**: No authorization required. It can be called with an unauthenticated session.
- **System.View or System.Read**: Authorization is required. Call `Login` before invoking a method that requires this privilege.
- **VcDr.Internal.com.vmware.vcDr.InternalAccess**: Administrator access is required to invoke a method annotated with this privilege.

  NOTE
  If a method requires a privilege not listed in the list above, then it is treated as if the administrator access privilege is required.

RetrieveContent

This method retrieves the properties of the service instance. It returns the properties belonging to the service instance, including various object managers.

Synopsis

```
ServiceInstanceContent retrieveContent();
```

`ServiceInstanceContent` is the properties of the `ServiceInstance` class. It has the following fields:

Field	Description
`about`	Information about this service.
`applianceManager`	`ApplianceManager` instance. For more inforamtion, see Appliance Manager.
`cfgManager`	`ConfigurationManager` instance. For more information, see Configuration Manager.
`dbManager`	`DatabaseManager` instance. For more information, see Database Manager.
`diagnosticManager`	`DiagnosticManager` instance. For more information, see Diagnostic Manager.
`serviceManager`	`ServiceManager` instance. For more information, see Service Manager.
`sslCertificateManager`	`SslCertificateManager` API. For more information, see SSL Certificate Manager.
`updateManager`	`UpdateManager` API. For more information, see Update Manager.
`sraManager`	`sraManager` instance. For more information, see SRA Manager.
`propertyCollector`	Property Collector for external API

`AboutInfo` is a data object type that describes system information including the name, type, version, and build number. It has the following fields:

Field	Description
`name`	Short form of the product name.
`fullName`	Complete product name, including the version information.
`vendor`	Name of the vendor of this product.
`version`	Dot-separated version string. For example, "1.2".
`build`	Build string for the server on which this call is made. For example, x.y.z-num. This string does not apply to the API.
`osType`	Operating System type and architecture.
`productLineId`	Product ID. Unique identifier of the product line.
`apiType`	Indicates whether or not the service instance represents a standalone host.

Field	Description
`apiVersion`	The version of the API as a dot-separated string. For example, "1.0.0".
`instanceUuid`	A globally unique identifier associated with this service instance.
`deployment`	Deployment type of the appliance. It enumerates the following : • `SRM` • `VRMS` • `VRS` • `Combined`

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

LoginDrConfig

This method logs you on to the server by verifying user and password with the local Operating System.

Synopsis

```
void login(String userName, @secret String password, @version3 @optional String locale)
```

`login` has the following parameters:

Parameter	Description
`userName`	ID of the user who is logging on to the server.
`password`	Password of the user logging on to the server.
`locale`	Locale for this session.

Faults

- InvalidArgument
- InvalidLocale
- InvalidLogin
- NoPermission
- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

LogoutDrConfig

This method logs out and terminates the current session.

Synopsis

```
void logout();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ChangeUserPassword

This method assigns password to the user who is running the configuration service.

Synopsis

```
void ChangePassword(String userName, @secret String currentPassword, @secret String newPassword)
```

`ChangePassword` has the following parameters:

Parameter	Description
`userName`	User for whom the password should be changed. Currently, this parameter is not taken into account and the password is changed only for the SRM user.
`currentPassword`	Current user password.
`newPassword`	New user password.

Faults

- ChangePasswordFault
- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

Service Manager

This section describes the operations to control appliance services. These operations are applicable on SRM, VRMS, and VRS deployments.

> **NOTE**
> IsSrmServerRunning can be executed on VRMS deployment but it will return false.

IsSrmServerRunning

This method returns the current service state of the Site Recovery Manager.

Synopsis

```
boolean isSrmServerRunning();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DrConfigStartService

This method starts the service. It does nothing if the service is already running.

Synopsis

```
void Start(String service)
```

`service` is the parameter for the service to start. The value must be one of the following `Service` enums:

- `srm`
- `db`
- `rsyslog`
- `sshd`
- `drclient`
- `envoy_proxy`
- `hbrsrv`
- `hmsdb`
- `hms`

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DrConfigStopService

This method stops the service. It does nothing if the service is not running.

Synopsis

```
void Stop(String service)
```

`service` is the parameter for the service to be stopped. Value must be one of the `service` enums. For more inforamtion, see DrConfigStartService.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DrConfigServiceStatus

This method returns status information of the service.

Synopsis

```
ServiceStatusInfo getServiceStatus(String service)
```

`ServiceStatusInfo` is the information for service. It has the following fields:

Parameter	Description
`StartUpType`	List of startup types. Enumerates the following: • Automatic • Manual
`serviceId`	The service id. This should correspond to the `ServiceManager::Service` enum.
`name`	Name of the service.
`description`	Description of the service.
`startupType`	Startup type. Value must be one of the enums.
`isRunning`	Boolean if the service is running.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DrConfigRestartService

This method stops the service and then starts it. If the service is not running, it will be started.

Synopsis

```
void Restart(String service)
```

`service` is the parameter for service that must be restarted. Value must be one of the `service` enums. For more information, see DrConfigStartService.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DrConfigAllServicesStatus

This method returns `ServiceStatusInfo` object for all the services.

Synopsis

```
ServiceStatusInfo[] getAllServicesStatus()
```

`ServiceStatusInfo` is the information about the service. For more information about `ServiceStatusInfo`, see DrConfigServiceStatus.

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

SRA Manager

This section describes the interface for managing SRA images and containers in the SRM Configuration Service. These operations are applicable only on SRM deployments.

GetRunningTask

This method gets the currently active SRA task or null.

Synopsis

```
ConfigurationTask getRunningTask();
```

`ConfigurationTask` is a managed object that provides operations to configure the SRM server. For more information, see Configuration Task.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetSraImages

This method returns a collection of SRA images loaded into the docker daemon of the Site Recovery Manager Virtual Appliance. It returns the `ConfigurationTask` object that can be used to monitor the operation. `ConfigurationTask.getTaskInfo()` method returns status information for the current task. `ConfigurationTaskInfo.result` returns a collection of `SraImage` objects.

Synopsis

```
ConfigurationTask getSraImages()
```

`ConfigurationTask` is a managed object that provides operations to configure the SRM server. For more information see, Configuration Task.

`SraImage` describes an SRA image loaded into docker. It has the following fields:

Field	Description
`Info`	Information about the SRA as taken from 'queryInfo' command. It has the following values: • `uuid`: Universally unique identifier of the SRA which is preserved on SRA upgrades. • `name`: Name of the adapter. • `version`: Version of the adapter. • `vendor`: Storage Vendor who owns the adapter. • `helpUrl`: URL for on-line documentation for the adapter.
`imageId`	Sha256 id of the image.
`SraContainer[] containers`	List of containers instantiated from the image.
`repoTags`	Docker repository tags the image is known by in the [REPOSITORY[:TAG]] format.
`info`	SRA image info as taken from the 'queryInfo' SRA command. This can be null if there was an error retrieving the info from the SRA. In this case `error` will be populated with the error that occurred.
`error`	Populated when there is an error executing the 'queryInfo' SRA command. The `info` field will be null in this scenario.

`SraContainer` describes an SRA container instantiated from an SRA docker image. It has the following fields:

Field	Description
`containerId`	The container id.
`imageId`	The sha256 image id of the image from which the container was instantiated.
`MountPoint[] mountPoints`	An array of mount points the container has, if any.

`MountPoint` describes a bind mount of the SRA container. For more information see https://docs.docker.com/storage/bind-mounts/. `MountPoint` has the following fields:

Field	Description
`source`	The source of the mount point, i.e this is the path outside of the container.
`destination`	The destination path where the the source is mounted at. This is the path inside the container.

Faults

- RuntimeFault
- ServiceBusy
- SraOperationsDisabled

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DeleteImage

This method stops and then deletes the containers instantiated from the given image, and deletes the image itself. It returns True if the image is deleted, and False if the image does not exist.

Synopsis

```
boolean deleteImage(String imageId)
```

The `imageId` of the image that should be deleted. This can be either the sha256 id of the image, or the image repository tag in the [REPOSITORY[:TAG]] format.

Faults

- CannotExecuteDockerCommand
- DockerCommandFailed
- RuntimeFault
- SraOperationsDisabled

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DeleteImageContainers

This method stops and then deletes the containers which were instantiated from the given image. It returns True if the image's containers are deleted, and False if the image does not exist or if the image does not have containers.

Synopsis

```
boolean deleteImageContainers(String imageId)
```

`imageId` is the id of the image whose containers must be stopped. This can be either the sha256 id of the image or the image repository tag in the [REPOSITORY[:TAG]] format.

Faults

- CannotExecuteDockerCommand
- DockerCommandFailed
- RuntimeFault
- SraOperationsDisabled

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetImageInfo

This method returns the image information as taken from the `queryInfo` SRA command. Because the docker images are immutable, the `queryInfo` SRA command is executed only once, the first time the information is requested. Subsequent calls return a cached value which lives for the duration of the Site Recovery Manager Configuration Service lifetime.

Synopsis

```
Info getImageInfo(String imageId)
```

`imageId` is the id of the image for which the information is being requested. This can be either the sha256 id of the image, or the image repository tag in the [REPOSITORY[:TAG]] format.

`SraImage.Info` is the information about the SRA as taken from the 'queryInfo' command. It has the following fields:

Field	Description
`uuid`	Universally unique identifier of the SRA which is preserved on SRA upgrades.
`name`	Name of the adapter.
`version`	Version of the adapter.
`vendor`	Storage Vendor who owns the adapter.
`helpUrl`	URL for on-line documentation for the adapter.

Faults

- CannotCreateSraLogDirectory
- CannotExecuteDockerCommand
- DockerCommandFailed
- DockerImageDoesNotExist
- RuntimeFault
- SraOperationsDisabled

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

CopySraConfiguration

This method copies the SRA configuration from a source image to a destination image.

Synopsis

```
void copySraConfiguration(String fromImage, String toImage)
```

`copySraConfiguration` has the following parameters:

Parameter	Description
`fromImage`	Docker image id of the source image. It can be either in the [REPOSITORY:[TAG]] format or in the canonical sha256 format.
`toImage`	Docker image id of the destination image. It can be either in the [REPOSITORY:[TAG]] format or in the canonical sha256 format.

Faults

- CannotCreateSraLogDirectory
- CannotExecuteDockerCommand
- DockerCommandFailed
- DockerImageDoesNotExist
- RuntimeFault
- SraOperationsDisabled

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ResetToFactorySettings

This method reverts the SRA image's configuration to its factory settings. Any changes to the configuration made since the image was loaded into docker will be lost.

Synopsis

```
void resetToFactorySettings(String imageId)
```

`imageId` is the docker image id of the source image. It can be either in the [REPOSITORY:[TAG]] format or in the canonical sha256 format.

Faults

- CannotExecuteDockerCommand
- DockerCommandFailed
- DockerImageDoesNotExist
- RuntimeFault
- SraOperationsDisabled

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

SSL Certificate Manager

This section describes operations to configure certificates for the configuration service and SRM. These operations are applicable on SRM, VRMS, and VRS deployments.

The following methods that are used for setting or installing a new SRM certificate restarts the envoy service.When you are using the follwoing APIs, if you encounter a `ConnectonLost` error, ignore it.

- `SetCertificate`
- `SetKeyCertificate`
- `InstallSelfSignedCertificate`
- `InstallCertificate`

Wait for the restart process to complete and reconnect to the SRM Configuration Service to make new calls.

ProbeSsl

This method checks if the Site Recovery Manager can establish successful SSL connection to the specified endpoint. It returns `CertificateInfo` that describes if this SRM server can validate the certificate coming from the specified endpoint.

Synopsis

```
CertificateInfo probeSsl(String uri)
```

`uri` is the URI of the endpoint to probe.

`CertificateInfo` provides information about X509 certificate. It has the following fields:

Parameter	Description
`certificate`	PEM encoded X509 certificate.
`thumbprint`	SHA-2 hash of the certificate. The format is two capital hexadecimal digits separated by ':'. For example: CF:2B:8A:63:9F:71:63:7C:5D:61:3C:83:A7:D0:17:E0:CA:7C:89:5B:F3:D9:2B:BB:75:12:AA:C2:7C:C5:F3:9A
`dnsName`	DNS name of the server extracted from the certificate. The client is expected to use this DNS name to establish a secure connection to the server.
`isTrusted`	True if the SRM server can successfully validate the certificate without using thumbprints and false otherwise.
`issuedTo`	IP or FQDN of the receiver of the certificate.
`issuedBy`	IP or FQDN of the issuer. The one who signed the certificate.
`expiresOn`	Date on which the certificate expires.

Faults

- ConnectionRefusedFault
- DnsLookupFault
- HostUnreachableFault
- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DrConfigGenerateCSR

This method generates a new key and CSR, and returns the CSR for signing. It returns the certificate signing request in PEM format.

Synopsis

```
String generateCSR(@optional CsrData requestData);
```

`requestData` parameter is the `CsrInfo` with desired CSR parameters.

`CsrData` is a data object. It provides information about about X509 certificate. It has the following fields:

Field	Description
`commonName`	Common name to be set in the certificate. Usually the fully qualified domain name for server. If not set, data provided in FQDN (OS hostname) will be used.
`organization`	Exact legal name of the organization. Do not use an abbreviation. If not set, VMware default will be used.
`organizationUnit`	Section within the organization. If not set, VMware default will be used.
`locality`	City where organization is legally located. If not set, VMware default will be used.

Field	Description
state	State or province where organization is legally located. Do not use an abbreviation. If not set, VMware default will be used.
country	Two letter ISO abbreviation for organization country. If not set, VMware default will be used.
emailAddress	Email address to contact the organization. If not set, this will be empty.
fqdn	List of comma-separated FQDN strings to be used for SAN extensions. If not set, the OS hostname will be used.
ip	List of comma-separated IP strings to be used for SAN extensions. If not set, this will be empty.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DrConfigSetCertificate

This method sets a new certificate. It reconfigures the Site Recovery Manager if already configured and restarts the proxy service. If you encounter an error while using this method, ignore the error and then reconnect to the management service.

Synopsis

```
void setCertificate(String certificate, @optional String[] caChain)
```

`setCertificate` has the following parameters:

Parameter	Description
certificate	New server certificate that must be used. It should be in PEM format.
caChain	List of intermediate CA certificates used to sign the server certificate. It should be in PEM format.

Faults

- CertificateBadKeyPair
- CertificateCaNotAllowed
- CertificateDnsMismatch
- CertificateHasExpired
- CertificateInvalidKeyLength
- CertificateMd5NotAllowed
- CertificateNotYetValid
- InvalidArgument
- PrivateKeyNotFound
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DrConfigSetKeyCertificate

This method sets a new key and certificate, reconfigures Site Recovery Manager if already configured and then restarts the proxy service. If you encounter an error while using this method, ignore the error and then reconnect to the management service.

NOTE
This method does not allow you to password protect the private key. Consider using the following methods to set the key and certificate:

- `generateCSR()` method with the `setCertificate()` method.
- `installCertificate()` method

Synopsis

```
void setKeyCertificate(String key, String certificate, @optional String[] caChain)
```

`setKeyCertificate` has the following parameters:

Parameter	Description
`key`	New server private key to use in PEM format.
`certificate`	New server certificate to use in PEM format.
`caChain`	List of intermediate CA certificates, used to sign the server certificate in PEM format. During connect in 'Certificate' message, the server sends this chain and server certificate. The chain may or may not include the root CA.

Faults

- CertificateBadKeyPair
- CertificateCaNotAllowed
- CertificateDnsMismatch
- CertificateHasExpired
- CertificateInvalidKeyLength
- CertificateMd5NotAllowed
- CertificateNotYetValid
- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

AddCaCertificates

This method adds certificate authority certificates to the list of validating certificates. This list is used to validate server certificates when the Site Recovery Manager acts as a client.

Synopsis

```
void addCaCertificates(@optional String[] certs);
```

`certs` is an array of CA certificates. Each item contains a single certificate in PEM format.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

RemoveCaCertificates

This method removes certificate authority certificates from the list of validating certificates. If a certificate requested for removal is not found, this will be noop.

Synopsis

```
void removeCaCertificates(@optional String[] certs)
```

`certs` parameter is an array of CA certificates. Each item contains a single certificate in the PEM format.

Faults

- InvalidArgument
- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

RetrieveCaCertificates

This method gets the current list of certificate authority certificates used by SRM to validate other server's certificates. It returns the collection of PEM encoded CA certificates. The list includes all system level certificates.

Synopsis

```
String[] retrieveCaCertificates();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

ClearCaCertificates

This method completely clears the certificate authority certificates installed on Site Recovery Manager Virtual Appliance.

Synopsis

```
void clearCaCertificates();
```

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

InstallSelfSignedCertificate

This method installs self-signed certificate, reconfigures the Site Recovery Manager if already configured, and restarts the proxy service. If you encounter an error while using this method, ignore the error and then reconnect to the management service.

Synopsis

```
void installSelfSignedCertificate(CsrData csrData)
```

`csrData` is the `CsrData` object that should be used to sign the certificate.

`CsrData` is a data object. It provides information about about X509 certificate. For more information, see DrConfigGenerateCSR.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

InstallCertificate

This method installs the PKCS#12 certificate, reconfigures the Site Recovery Manager if already configured, and restarts the proxy service. If you encounter an error while using this method, ignore the error and then reconnect to the management service.

Synopsis

```
void installCertificate(String pkcs, @optional @secret String pkcsPassword)
```

`InstallCertificate` has the following parameters:

Parameter	Description
`pkcs`	Certificate as string. Base64 encoded.
`pkcsPassword`	Password for the certificate.

Faults

- CertificateBadKeyPair
- CertificateCaNotAllowed
- CertificateDnsMismatch
- CertificateHasExpired
- CertificateInvalidKeyLength
- CertificateMd5NotAllowed
- CertificateNotYetValid
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetCertificateInfo

This method lists the certificate info. Returns a `CertificateInfo` object that contains information about the certificate.

Synopsis

```
CertificateInfo getCertificateInfo();
```

`CertificateInfo` provides information about X509 certificate. For more information, see ProbeSsl.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

Update Manager

This section describes operations to update the Site Recovery Manager appliance. These operations are applicable on SRM, VRMS, and VRS deployments.

GetRunningTask

This method gets the currently active update task or null.

Synopsis

```
ConfigurationTask getRunningTask();
```

`ConfigurationTask` is a managed object that provides operations to configure the SRM server. For more information, see Configuration Task.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

UpdateRepository

This method changes the update repository location.

Synopsis

```
void updateRepository(UpdateRepoInfo info)
```

`info` parameter is a `UpdateRepoInfo` object that contains information about the update repository location.

`UpdateRepoInfo` contains appliance update repository information. It has the following fields:

Field	Description
`url`	Repository url.
`mountedIso`	True if the mounted iso is used. If this value is set, everything else is ignored.

Field	Description
username	User name
password	Password

Faults

- InvalidArgument
- RuntimeFault
- SystemError

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

DrConfigCheckForUpdates

This method checks the repository for available updates. It returns a task object used for monitoring the operation. It returns a null if no updates are available.

Synopsis

```
ConfigurationTask checkForUpdates()
```

`ConfigurationTask` is a managed object that provides operations to configure the SRM server. For more information, see Configuration Task.

`ConfigurationTask.getTaskInfo()` method returns status information for the current task. `ConfigurationTaskInfo.result` returns an `UpdateInfo` data object which to be used in installUpdate method.

`UpdateInfo` contains the appliance update repository information. It has the following fields:

Field	Description
UpdateType	Enumerates the following update types: • `FEATURE` - Update contains a new feature. • `SECURITY` - Update contains security fixes. • `FIX` - Update contains other fixes. • `MULTIPLE` - Update contains multiple types of modifications.
UpdateSeverity	Enumerates the following levels of importance: • `MODERATE` - Update is moderate. • `IMPORTANT`- update is important. • `CRITICAL` - Update is critical.
version	Update version string.
type	Update type. Value must be one of `UpdateType` enums.
releaseDate	Release date.
rebootRequired	Reboot required.
severity	Severity. Value must be one of `UpdateSeverity` enums.
summary	Update summary.
eula	End-user license agreement.

Faults

- RuntimeFault
- ServiceBusy

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

InstallUpdate

This method installs the update. It returns a task object used for monitoring the operation. `CheckForUpdates` must be called before this operation. This stops all the services to update them.

Synopsis

```
ConfigurationTask installUpdate(@optional UpdateInfo info)
```

`info` parameter is a `UpdateInfo` object that contains information for the update that should be installed. If null, installs the latest update.

`UpdateInfo` contains the appliance update repository information. For more information on `UpdateInfo`, see DrConfigCheckForUpdates.

`ConfigurationTask` is a managed object that provides operations to configure SRM server. For more information, see Configuration Task.

Faults

- InvalidArgument
- RuntimeFault
- UpdateNotAvailableFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

GetRepositories

This method gets update repos. It returns a `UpdateRepoInfo` object representing the current repository and the default repository. It returns only one object if no custom repository is set.

Synopsis

```
UpdateRepoInfo[] getRepositories();
```

`UpdateRepoInfo[]` contains the appliance update repository information. For more information on `UpdateRepoInfo`, see UpdateRepository.

Faults

- RuntimeFault

For more information about the faults, see Faults in Site Recovery Manager Appliance Management API.

Logical Usage Order - Site Recovery Manager API

This chapter contains descriptions for Site Recovery Manager APIs.

The API descriptions in this chapter follow the logical usage order of List of API Operations. In examples below, `MoRef` indicates a String that references a managed object.

> **NOTE**
> In the various examples provided in this chapter, the `srmPortType` is a class instance which should be setup from the SDK examples. For more information, see About Java JAX-WS Samples.

Service Instance

Site Recovery Manager methods take a managed object reference `_this`, which references the `SessionManager` used for making method calls. Programs obtain `_this` by retrieving content of the `ServiceInstance`, which is accomplished by creating a new managed object reference of type `SrmServiceInstance`.

C# code to create `SrmServiceInstance`

```
public SvcConnection(string svcRefVal)
{
...
_svcRef = new ManagedObjectReference();
_svcRef.type = "SrmServiceInstance";
_svcRef.Value = svcRefVal;
}
```

The Java code is similar to the C# code.

Java code to create `SrmServiceInstance`

```
final ManagedObjectReference _svcRef = new ManagedObjectReference();
                _svcRef.setType("SrmServiceInstance");
                _svcRef.setValue("SrmServiceInstance");
```

GetSiteName

Gets the name of the current site.

> **NOTE**
> The method is deprecated. You should not rely on it in production code, as it is not guaranteed to provide valid information in future releases. Instead, you should use GetLocalSiteInfo method.

Synopsis

```
String getSiteName( )
```

String representing the local Site Recovery Manager site name.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetPairedSite

This function gets the remote site paired with this site. A remote site may be acting as the secondary site for this site, or may be acting as the primary site with this site as its secondary. Most of the initial Site Recovery Manager calls work for everyone (`System.Anonymous` privilege) but `GetPairedSite` requires the `System.View` role, so it must be called after login to the local site. Also `GetPairedSiteSolutionUserInfo` is useless without the remote paired site, so the two must be called together.

Synopsis

```
RemoteSite getPairedSite( )
```

The `RemoteSite` class contains the following fields:

Field	Description
`name`	a String with the name of the site.
`uuid`	a String with the UUID of the site.
`vcHost`	a String with the DNS name or IP address of the remote vCenter Server. **NOTE** This property has been deprecated. You should not rely on this property in production code, as it is not guaranteed to contain valid information in future releases. Instead, you should use `lkpUrl` and `vcInstanceUuid` to locate services on the remote site.
`vcInstanceUuid`	a String with instance UUID of the vCenter Server associated with the remote Site Recovery Manager.
`vcPort`	an integer with the port used for VMOMI access to the remote vCenter Server. **NOTE** This property has been deprecated. You should not rely on this property in production code, as it is not guaranteed to contain valid information in future releases. Instead, you should use `lkpUrl` and `vcInstanceUuid` to locate services on the remote site.
`vcUrl`	a String with the URL of the remote vCenter Server
connected	a boolean that is true when the sites are connected and false when the sites are disconnected.
lkpUrl	a String with the URL of the remote LookupService server.

Faults

- RemoteSiteNotEnabled if the remote site is not enabled.
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example

```
com.vmware.srm.SrmRemoteSite remoteSite = srmPortType.getPairedSite(ManagedObjectReference _this);

Where ManagedObjectReference _this = _svcRef;
```

RetrieveContent

Retrieves properties of the service instance.

Synopsis

```
ServiceInstanceContent retrieveContent()
```

The `ServiceInstanceContent` class contains the following fields.

Field	Description
`about`	shows information about this service.
`apiVersion`	represents the version of this API.
`inventoryMapping`	an external API to InventoryMappings. For more information, see Inventory Mappings.
`protection`	an external API to Protection. For more information, see Protection.
`recovery`	an external API to Recovery. For more information, see Recovery.
`storage`	an external API to Storage. For more information, see Storage.
`autoprotectManager`	an external API to Automatic Protection. For more information, see Autoprotect Manager.
`ipSubnetMapper`	an external API to IP Subnet Mapper. For more information, see IP Subnet Mapper.
`vvolReplication`	an external API to Vvol Protection. For more information, see Vvol Replication.
`propertyCollector`	Property Collector for external API
`placeholderDatastoreManager`	External API to `PlaceholderDatastoreManager`

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetLocalSiteInfo

The `getLocalSiteInfo` method gets information about the local site.

Synopsis

```
LocalSiteInfo getLocalSiteInfo()
```

Returns information about the local site such as site name, UUID, and URLs of the local LookupService server and vCenter Server.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Solution User Information

At install time Site Recovery Manager creates a solution user at the local and remote sites. This improves security by avoiding use of adminstrator@vsphere.local or the Windows administrator. Programs can obtain both solution users before Site Recovery Manager login because the privilege required for these functions is `System.Anonymous` .

GetSolutionUserInfo

Obtain the Site Recovery Manager solution user name and site UUID for the local site. You must call the `getSolutionUserInfo` method before logging in (with `SrmLoginByTokenLocale` for example) if you wish to delegate a token to the Site Recovery Manager solution user.

Synopsis

```
SolutionUserInfo getSolutionUserInfo()
```

`SolutionUserInfo.siteUuid` is a string with the immutable unique identifier of the Site Recovery Manager server.

`SolutionUserInfo.username` is the name of the Site Recovery Manager solution user.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetPairedSiteSolutionUserInfo

Obtain the Site Recovery Manager solution user name and site UUID for the paired remote site.

Synopsis

```
SolutionUserInfo getPairedSiteSolutionUserInfo()
```

`SolutionUserInfo.siteUuid` is a string with the immutable unique identifier of the remote Site Recovery Manager Server.

`SolutionUserInfo.username` is the name of the remote Site Recovery Manager solution user.

Faults

- RuntimeFault
- RemoteSiteNotEnabled, if the remote site is not enabled.

See Faults in Site Recovery Manager API for more details.

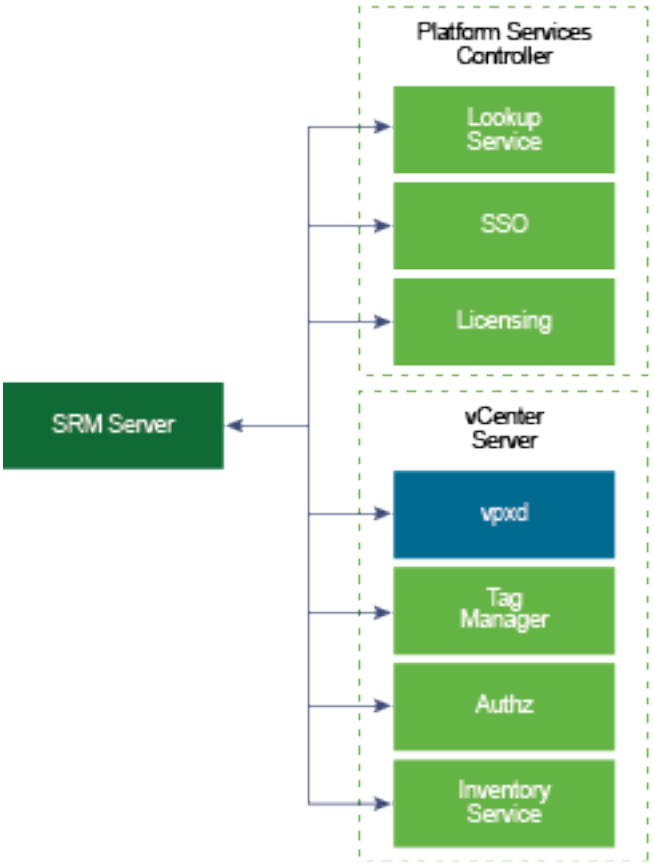
SAML Token Authentication

In the 6.0 release, Site Recovery Manager interacts with both vCenter Server (as before) and Platform Services Controller (PSC).

The PSC contains a Lookup Service to locate other services, a Licensing Service to replace the VIM license manager, and Single Sign On (SSO) service for authentication and token acquisition.

The vCenter Server management node contains a new Tag Manager to create categories and tags for Storage DRS or SPBM, and a new Authz service to replace the VIM authorization manager.

Figure 17: Management (M) and PSC (N) nodes



When programs connect to the local or remote SRM server, they must obtain a SAML token from the SSO service on the local or remote PSC. (The older login functions implicitly obtain a SAML token.)

SrmLoginByTokenLocale

This function begins a session with Site Recovery Manager Server.

Synopsis

```
void
loginByToken(String samlToken, @optional String locale)
```

`samlToken` is an XML encoded security assertion markup language (SAML) token for authenticating login to the SRM server. The token should either be a bearer token or a holder of key token delegated to the Site Recovery Manager solution user.

`locale` is the optional locale for this session.

Faults

- AlreadyLoggedInFault if there is already an established session.
- ConnectionLimitReached if the configured connection limit has been reached.
- InvalidLogin if the given token is not valid.
- InvalidLocale if the requested locale is invalid or unavailable.

- InvalidTokenLifetime if the SSO token is either expired or not yet valid.
- NoPermission if the user does not have permissions.
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

SrmLoginSitesByToken

Log in to both the local and remote vCenter Servers using the provided tokens. This function is needed when escalated privileges are required to perform operations on the remote site, such as protecting virtual machines.

Synopsis

```
void loginSitesByToken(String samlToken,
         String remoteSamlToken, @optional String locale)
```

`samlToken` is an XML encoded SAML token for authenticating login to the Site Recovery Manager server. The token should either be a bearer token or a holder of key token delegated to the Site Recovery Manager solution user.

`remoteSamlToken` is an XML encoded SAML token for authenticating login to the remote Site Recovery Manager server. The token should either be a bearer token or a holder of key token delegated to the remote Site Recovery Manager solution user.

`locale` is the optional locale for this session.

Faults

- AlreadyLoggedInFault if there is already an established session.
- ConnectionLimitReached if the configured connection limit has been reached.
- InvalidLogin if the given token is not valid.
- InvalidLocale if the requested locale is invalid or unavailable.
- NoPermission
- RemoteSiteNotEnabled if the remote site is not enabled.
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

SrmLoginRemoteSiteByToken

Log in to the remote Site Recovery Manager server using the provided credentials. This function may be called when escalated privileges are required on the remote site and the current session has already been authenticated by login.

Synopsis

```
void loginRemoteSiteByToken(String remoteSamlToken,
         @optional String locale)
```

`remoteSamlToken` is an XML encoded SAML token for authenticating login to the Site Recovery Manager server. The token should either be a bearer token or a holder of key token delegated to the remote Site Recovery Manager solution user.

`locale` is the optional locale for this session.

Faults

- AlreadyLoggedInFault if there is already an established session.
- ConnectionDownFault
- ConnectionLimitReached if the configured connection limit has been reached.
- InvalidLogin if the given token is not valid.
- InvalidLocale if the requested locale is invalid or unavailable.
- NotAuthenticated if there is no session
- RemoteSiteNotEnabled if the remote site is not enabled.
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Credential Based Authentication

In the 6.0 release, login functions in earlier Site Recovery Manager releases have been implemented on top of the SAML token authentication functions. The password-based login functions are now offered for convenience.

Programs can connect to the local Site Recovery Manager Server using the `SrmLoginLocale` function, or to Site Recovery Manager Server instances at both the (local) protected site and the (remote) recovery site using the `SrmLoginSites` API.

SrmLoginLocale

This method logs in to the Site Recovery Manager server. The `Connect` public method requires the URL of a Site Recovery Manager server and authentication credentials. The `SrmLoginLocale` method takes the `_srcRef` managed object reference from `SrmServiceInstance`, and fails if the user name and password combination is invalid, or if the user is already logged in. In these examples, a locale string could be provided instead of the null parameter.

Synopsis

```
void SrmLoginLocale(String username, String password, @optional String locale)
```

`username` is the user name authorized for access to the local vCenter Server.

`password` is the password for that user on the local vCenter Server.

`locale` is the name of the locale for this session.

Faults

- AlreadyLoggedInFault
- ConnectionLimitReached
- InvalidLocale
- InvalidLogin
- NoPermission
- RuntimeFault

See Faults in Site Recovery Manager for more details.

C# code for Site Recovery Manager login

```
protected SrmService _service;
protected SrmServiceInstanceContent _sic;
protected ManagedObjectReference _svcRef;
```

```
...
public void Connect(string url, string username, string password)
{
_service = new SrmService();
_service.Url = url;
_service.Timeout = 600000;
_service.CookieContainer = new System.Net.CookieContainer();
_sic = _service.RetrieveContent(_svcRef);
_service.SrmLoginLocale(_svcRef, username, password, null);
...
}
```

The Java code is similar to the C# code but uses a service locator.

Java code for Site Recovery Manager login

```
private static SrmPortType srmPort;
private static SrmServiceInstanceContent serviceContent;
private static boolean isConnected = false;
...
srmPort = srmService.getSrmPort();
Map<String, Object> ctxt =
((BindingProvider) srmPort).getRequestContext();
ctxt.put(BindingProvider.ENDPOINT_ADDRESS_PROPERTY, url);
ctxt.put(BindingProvider.SESSION_MAINTAIN_PROPERTY, true);
serviceContent = srmPort.retrieveContent(_svcRef);
srmPort.srmLoginLocale(_svcRef, userName, password, null);
isConnected = true;
```

Subsequent methods in the Site Recovery Manager are called as a subclass of `_service`, for example `_service.ListPlans()` in C# or `srmport.listPlans()` in Java.

SrmLoginSites

The `SrmLoginSites` API is very similar to `SrmLoginLocale`, except it takes an additional user name and password combination for the remote (usually recovery) site. The `SrmServiceInstance _this` is obtained from the local (usually protected) site.

Synopsis

```
void SrmLoginSites(String username, String password, String remoteUser, String remotepass,@optional String lo-
cale)
```

`username` is the user name authorized for access to the local vCenter Server

`password` is the password for that user on the local vCenter Server

`remoteUser` is the user name authorized for access to the remote vCenter Server

`remotePass` is the password for that user on the remote vCenter Server

`locale` is the name of the locale for this session

Faults

- AlreadyLoggedInFault
- ConnectionLimitReached
- InvalidLocale

- InvalidLogin
- NoPermission
- RemoteSiteNotEnabled
- RuntimeFault

See Faults in Site Recovery Manager for more details.

C# and Java for double SRM login

```
/// C#
_service.SrmLoginSites(_svcRef, username, password, remoteuser, remotepass, locale);
// srmPort.srmLoginSites(__svcRef, username, password, remoteuser, remotepass, locale);
```

SrmLogoutLocale

This method logs out of the Site Recovery Manager server and terminates the current session. It takes the same managed object reference as for `SrmLoginLocale`, and should be called with other methods to clean up a connection.

Synopsis

```
void SrmLogoutLocale( )
```

Faults

- NotAuthenticated
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

C# code to log out

```
public void Disconnect() {
  if (_service != null) {
    _service.SrmLogoutLocale(_svcRef);
    _service.Dispose();
    _service = null;
    _sic = null;
  }
}
```

The Java code is simpler than the C# code.

Java code to log out

```
private static void disconnect() throws Exception {
  if (isConnected) {
    srmPort.srmLogoutLocale(_svcRef);
  }
  isConnected = false;
}
```

SrmLoginRemoteSite

Log in to the remote Site Recovery Manager server using the provided credentials. This function may be invoked when escalated privileges are required on the remote site and the current session has already been authenticated using login.

Synopsis

```
void SrmLoginRemoteSite(String remoteUser, String remotePassword, @optional String locale)
```

`remoteUser` is the username to be used to login to the remote VirtualCenter server.

`remotePassword` is the password to be used to login to the remote VirtualCenter server.

`locale` is the locale for this session.

Faults

- AlreadyLoggedInFault
- ConnectionLimitReached
- InvalidLocale
- InvalidLogin
- RemoteSiteNotEnabled
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetLicenseInfo

This method gets the assigned license information.

Synopsis

```
LicenseInfo getLicenseInfo();
```

`LicenseInfo` is a data object. It encapsulates information about a license. It has the following fields:

Field	Description
`editionKey`	The license edition
`costUnit`	The cost unit for this license. costUnit enumerates the following: • `cpuPackage`: One license is required per CPU package • `vm`: One license is required per VM • `unknown`: Unknown cost unit
`total`	Total capacity of the license
`used`	Number of units currently used from this asset
`productName`	The product name for this license
`productVersion`	The product version for this license
`expiryDays`	Number of days left until the license expires.
`expiryDate`	Expiration date of the license.
`inUseFeatures`	The features in this license.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

ProbeSsl

This method returns (host and thumbprint) tuples for all PSC/MGMT/DR hosts to which SRM should connect under specified root PSC node.

Synopsis

```
@optional HostThumbprintInfo[] probeSsl(String host, @optional int port, @optional String vcHost)
```

The `probeSsl` method returns an array of `HostThumbprintInfo` structures. Each entry contains host address and required thumbprint to establish connection to the services on that host. The `probeSsl` method has the following parameters:

Field	Description
`host`	Host name or IP address of the root PSC node.
`port`	Port of the root PSC node. When not provided the default value of 443 is used.
`vcHost`	Host where the VC is running. In case of embedded environment this field should not be specified. In this case the host on which the VC is running is the PSC host.

`HostThumbprintInfo` is a data object that contains host name/address and required thumbprint to establish connection to the services on that host. It has the following fields:

Field	Description
`host`	FQDN or IP address of the host.

thumbprint	SHA-2 hash of the SSL certificate of the server at the specified host. Format is two capital hexadecimal digits separated by ':'. For example:
	`CF:2B:8A:63:9F:71:63:7C:5D:61:3C:83:A7:D0:17:E0:CA:7C:89:5B:F3:D9:2B:BB:75:12:AA:C2:7C:C5:F3:9A`
	Example of SSL command to extract SHA-2 fingerprint from host is:
	`openssl s_client -connect <host>:<port> < /dev/null 2>/dev/null |`
	`openssl x509 -fingerprint -sha256 -noout -in /dev/stdin`

Faults

- RuntimeFault
- SitePairingFault

See Faults in Site Recovery Manager API for more details.

PairSrm

This method establishes the persistent network connection with a remote SRM server. Remote SRM server must have the same VC extension key.

Synopsis

```
@task RemoteSite pairSrm(ConnectionSpec spec);
```

This method returns the `drextapi.Task` that contains the paired `drextapi.RemoteSite` . For more information, see GetPairedSite.

`ConnectionSpec` contains the connection information used to connect to PSC node and locate peer services. It has the following fields:

Field	Description
`host`	Host name or IP address of the PSC node.
`port`	Port of the PSC node. When not provided the default value of 443 is used.
`vcHost`	Host where the VC is running. In case of embedded environment this field should not be specified. In this case the host on which the VC is running is the PSC host.
`HostThumbprintInfo[] thumbprints`	Thumbprints for PSC/MGMT/DR hosts to which SRM should connect when certificate validation fails. For more information, see ProbeSsl.
`creds`	Credentials to be used to authenticate to the remote PSC node. Credentials has the following fields: • `String user` - The name of a user with sufficient privileges to perform configuration tasks on the infrastructure and management nodes as well as SSO service configuration tasks on the infrastructure node. • `@secret String` - Password for the user.

NOTE

If the returned task fails, its error field may contain one of the following:

- `drextapi.site.fault.SelfPairFault` - If this SRM is already registered with the specified PSC/MGMT node.
- `drextapi.site.fault.SitePairingFault` - Contains the original error when a network connection cannot be established, there are invalid arguments, local site name is the same as remote SRM's name, another pair operation is in progress or there was other error while pairing sites.
- `drextapi.site.fault.AlreadyPairedFault` - If any of the SRM servers involved with the pairing is already paired.
- `drextapi.fault.RemoteSiteNotInitialized` - If the remote site is not correctly initialized.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

BreakPairing

This method removes the connection with the remote SRM server. This operation will automatically logs out from the remote site.

Synopsis

```
@task void breakPairing(RemoteSite site)
```

The `breakParing` method returns the `drextapi.Task` to track the operation. For more information, see SrmExtApiTask. `breakParing` has the following fields:

Field	Description
`site`	The remote SRM server to remove. For more information, see GetPairedSite.

NOTE

If the returned task fails, its error field may contain:

- `drextapi.fault.SitePairingFault` - If another pairing operation is in progress, site still has protected objects or a paired remote site cannot be found.

Faults

- InvalidArgument
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

ReconfigureConnection

This method reconfigures the RemoteSite object with connection information for remote PSC node and propagates the changed values to the paired site.

Synopsis

```
@task void reconfigureConnection(RemoteSite site, ConnectionSpec spec)
```

This method returns the `drextapi.Task` to track the operation. For more information, see SrmExtApiTask. `ReconfigureConnection` has the following parameters:

Field	Description
`site`	RemoteSite object to reconfigure. For more information, see GetPairedSite.
`spec`	The `ConnectionSpec` to use for the remote PSC node connection.

NOTE

Task result contains the paired `drextapi.RemoteSite` . For more information, see GetPairedSite.

If the returned task fails, its error field may contain one of the following:

- `drextapi.site.fault.SelfPairFault` - If this SRM is already registered with the specified PSC/MGMT node.
- `drextapi.site.fault.SitePairingFault` - Contains the original error when a network connection cannot be established, there are invalid arguments, the remote site name or network connections policy is

violated, either this SRM or the SRM registered with the given PSC/MGMT node is not paired with the other, another pair operation is in progress or there was other error while repairing sites.

Faults

- InvalidArgument
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

SrmExtApiTask

A base external API task.

IsSrmExtApiTaskComplete

This method checks whether the task has been completed.

Synopsis

```
boolean isComplete()
```

Returns True if this task has been completed.

GetSrmExtApiTaskInfo

This method gets detailed results of the completed task.

Synopsis

```
TaskInfo getTaskInfo()
```

`TaskInfo` is a data object that contains all information about a task. For more information see `TaskInfo` in the *Site Recovery Manager API Reference Guide*.

SRM Folder

This section covers the Site Recovery Manager API methods for Folders. This is the base class for all folder types in SRM APIs.

GetName

Retrieves the name of this folder object, given existence of a `ProtectionGroupFolder` or `RecoveryPlanFolder`.

Synopsis

```
String getName( )
```

Faults

- RuntimeFault

See for Faults in Site Recovery Manager API more details.

Example for GetName

```
java.lang.String name = srmPortType.getName(ManagedObjectReference _this);

where ManagedObjectReference _this = _folderRef;
where _folderRef can be taken from:
 SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
ManagedObjectReference _folderRef = srmPortType.getProtectionGroupRootFolder(
 ManagedObjectReference _this);
where ManagedObjectReference _this = _protectionRef;
```

GetParentFolder

Gets a reference to the parent folder. `Folder` extends and is inherited by Site Recovery Manager from the vSphere API, where it is a managed object acting as a container to store and organize inventory objects, such as protection groups and recovery plans.

Synopsis

```
Folder getParentFolder( )
```

Returns the parent `Folder` as a managed object. This value is null for the root object.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetChildType

Specifies the object types a folder may contain. When you create a folder, it inherits its `childType` from the parent folder in which it is created.

Synopsis

```
@optional TypeName[] getChildType();
```

`childType` is an array of strings.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

CreateFolder

Creates a new sub-folder with the specified name.

Because of the dual-server nature of SRM, the sites must be connected when creating folders. Any % (percent) character used in this name parameter must be escaped, unless it is used to start an escape sequence. Clients may also escape any other characters in this name parameter. This method requires

`VcDr.ProtectionProfile.com.vmware.vcDr.Create` privilege on the containing folder to create a protection group folder and `VcDr.RecoveryProfile.com.vmware.vcDr.Create` to create a recovery plan folder.

Synopsis

```
@task Folder createFolder(String folderName)
```

`createFolder` returns a task instance to monitor the asynchronous operation of this method. `Folder` object is returned as task result. `createFolder` contains the following parameters:

Field	Description
`name`	The name to be given the new folder. An entity name must be a non-empty string of less than 80 characters. The slash (/), backslash (\) and percent (%) will be escaped using the URL syntax. For example, %2F.

If a task fails, its error field may contain one of the following:

- `vim.fault.DuplicateName` - if another object in the same folder has the target name.
- `vim.fault.InvalidName` - if the name is not a valid entity name.
- `drextapi.fault.ConnectionDownFault` - if the sites are not connected.

Faults

- vim.fault.InvalidArgument
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

MoveFolder

Moves this folder into another folder.

The objects that can be moved into a folder depends on the parent folder's type (as defined by the parent folder's `childType()` property). For a folder constructed for recovery plans, only recovery plans and recovery folders can be moved into the folder. For a folder constructed to hold `ProtectionGroups` , only `ProtectionGroups` and protection folders can be moved into the folder.

For protection group folders this method requires `VcDr.ProtectionProfile.com.vmware.vcDr.Edit` on the moved folder, on the current parent folder, and on the destination folder.

For recovery plan folders this method requires `VcDr.RecoveryProfile.com.vmware.vcDr.Edit` on the moved folder, on the current parent folder, and on the destination folder.

Synopsis

```
@task void moveFolder(Folder destination);
```

`moveFolder` returns a task instance to monitor the asynchronous operation of this method. `moveFolder` has the following parameters:

Field	Description
`destination`	Folder that should become the new parent of this folder.

If a task fails, its error field may contain one of the following:

- `drextapi.fault.DuplicateName` - a folder with the same name already exists within the destination folder.
- `drextapi.fault.IllegalMove` if a cycle would be created by this move. For example, moving this folder into one of its children folders would create a cycle.
- `drextapi.fault.ImmutableFolder` - if move is initiated on the root folder.
- `vim.fault.NotSupported` - if the folder is being moved into a folder whose `childType()` property is not set to the appropriate value. For example, a folder cannot be moved into a folder whose `ChildType` property value does not contain `Dr::Folder` .

Faults

- InvalidType
- ManagedObjectNotFound
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

DestroyFolder

Destroys the specified `Folder`.

This method requires `VcDr.ProtectionProfile.com.vmware.vcDr.Delete` privilege for protection group folders and `VcDr.RecoveryProfile.com.vmware.vcDr.Delete` for recovery plan folders.

Synopsis

```
@task void destroyFolder();
```

`destroyFolder` returns a task instance to monitor the asynchronous operation of this method.

If a task fails, its error field may contain one of the following:

- `drextapi.fault.NotEmpty` - if this folder still contains child items.
- `drextapi.fault.ConnectionDownFault` - if the sites are not connected.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

RenameFolder

Renames the specified Folder. This method requires `VcDr.ProtectionProfile.com.vmware.vcDr.Edit` privilege for protection group folders and `VcDr.RecoveryProfile.com.vmware.vcDr.Edit` for recovery plan folders.

Synopsis

```
@task void renameFolder(String newName)
```

`renameFolder` returns a task instance to monitor the asynchronous operation of this method. `renameFolder` has the following parameters:

Field	Description
`newName`	The new folder name.

If a task fails, its error field may contain the following:

- `drextapi.fault.ConnectionDownFault` - if the sites are not connected.

Faults

- vim.fault.InvalidArgument
- RuntimeFault
- StringArgumentTooLong

See Faults in Site Recovery Manager API for more details.

Inventory Mappings

This section covers the Site Recovery Manager API methods for inventory (resource) mapping.

Resource mappings are the pairings of resources between the protected and recovery sites. In other words, mapping the networks, resource pools, datacenters and so forth on the protected site to their counterparts on the recovery site. This is done so that virtual machines will recover in the correct places on the recovery site. Previously this was done only in the UI, but APIs have been added to automate these mappings.

AddFolderMapping

Adds a folder mapping between a folder on the primary vCenter Server and another folder on the secondary vCenter Server.

Synopsis

```
void addFolderMapping(vim.Folder primaryFolder, vim.Folder secondaryFolder)
```

`primaryFolder` is a read-only `MoRef` to the folder on the protection site (must be local).

`secondaryFolder` is a read-only `MoRef` to the folder on the recovery site (must be remote).

Faults

- ConnectionDownFault
- InvalidPrimaryFolder
- InvalidSecondaryFolder
- NotAuthenticated
- RuntimeFault
- UnknownPrimaryFolder
- UnknownSecondaryFolder

See Faults in Site Recovery Manager API for more details.

RemoveFolderMapping

The `removeFolderMapping` method removes a folder mapping. The method does not check whether the folders in the mapping exist on the protected and recovery sites. You can use the method to remove broken mappings.

Synopsis

```
void removeFolderMapping(Folder primaryFolder)
```

The `primaryFolder` parameter specifies the folder on the primary site whose mapping must be deleted.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

AddNetworkMapping

Adds a network mapping between a network on the primary vCenter Server and another network on the secondary vCenter Server.

Synopsis

```
void addNetworkMapping(vim.Network primaryNetwork, vim.Network secondaryNetwork)
```

`primaryNetwork` is a read-only `MoRef` to the network on the protection site (must be local).

`secondaryNetwork` is a read-only `MoRef` to the network on the recovery site (must be remote).

Faults

- ConnectionDownFault
- InvalidPrimaryNetwork
- InvalidSecondaryNetowrk
- NotAuthenticated
- RuntimeFault
- UnknownPrimaryNetwork
- UnknownSecondaryNetwork

See Faults in Site Recovery Manager API for more details.

RemoveNetworkMapping

The `removeNetworkMapping` method removes a network mapping. The method does not check whether the networks in the mapping exist on the protected and recovery sites. You can use the method to remove broken mappings.

Synopsis

```
void removeNetworkMapping(Network primaryNetwork)
```

The `primaryNetwork` parameter specifies the primary site network whose mapping must be deleted.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

AddResourcePoolMapping

Adds a resource pool mapping between a resource pool on the primary vCenter Server and another on the secondary vCenter Server.

Synopsis

```
void addResourcePoolMapping(vim.ResourcePool primaryResourcePool,vim.ResourcePool secondaryResourcePool)
```

`addResourcePoolMapping` contains the following fields:

Field	Description
`primaryPool`	resource pool on the protection site (must be local)
`secondaryPool`	resource pool on the recovery site (must be remote)

Faults

- ConnectionDownFault
- NotAuthenticated
- RuntimeFault
- UnknownPrimaryResourcePool
- UnknownSecondaryResourcePool

See Faults in Site Recovery Manager API for more details.

RemoveResourcePoolMapping

The `removeResourcePoolMapping` method removes a resource pool mapping. The method does not check whether the pools in the mapping exists on the protected and recovery sites.

Synopsis

```
void removeResourcePoolMapping(ResourcePool primaryPool)
```

The `primaryPool` parameter specifies the resource pool on the primary site whose mapping must be deleted.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

AddTestNetworkMapping

The `addTestNetworkMapping` method adds a test network mapping between a network on the secondary site and a network on the secondary site that is used for testing.

Synopsis

```
void addTestNetworkMapping(@readonly Network secondaryNetwork,
  @readonly Network destinationTestNetwork)
```

`addTestNetworkMapping` has the following fields:

Field	Description
`secondaryNetwork`	Specifies a network on the remote recovery site
`destinationTestNetwork`	Specifies a test network on the remote recovery site

Faults

- ConnectionDownFault
- InvalidSecondaryNetwork
- RemoteSiteNotAuthenticated
- RuntimeFault
- UnknownSecondaryNetwork

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

RemoveTestNetworkMapping

The `removeTestNetworkMapping` method removes the test network mapping. The method does not check whether the networks in the mapping exist on the secondary site. You can use the method to remove broken mappings.

Synopsis

```
void removeTestNetworkMapping(vim.Network secondaryNetwork)
```

The `secondaryNetwork` parameter specifies the network on the secondary site whose mapping must be removed.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetFolderMappings

This method returns an array of the folder mappings for this inventory mapper. If one of the mappings does not have a secondary object, it means that the user does not have enough permissions to see that object on the secondary VC.

Synopsis

```
FolderMapping[] getFolderMappings();
```

`FolderMapping[]` is an array of mappings from a folder on the primary site to a folder on the secondary site with the following fields:

Field	Description
`primaryObject`	Folder on the primary site
`secondaryObject`	Folder on the secondary site

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetNetworkMappings

This method returns an array of the network mappings for this inventory mapper. If one of the mappings does not have a secondary object, it indicates that the user does not have enough permissions to see that object on the secondary VC.

Synopsis

```
NetworkMapping[] getNetworkMappings();
```

`NetworkMapping[]` is an array of mappings from a network on the primary site to a network on the secondary site with the following fields:

Field	Description
`primaryObject`	Network on the primary site
`secondaryObject`	Network on the secondary site

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetResourcePoolMappings

This method returns an array of the resource pool mappings for this inventory mapper. If one of the mappings does not have a secondary object, it means that the user does not have enough permissions to see that object on the secondary VC.

Synopsis

```
ResourcePoolMapping[] getResourcePoolMappings();
```

`ResourcePoolMapping[]` is an array of mappings from a resource pool on the primary site to a resource pool on the secondary site with the following fields:

Field	Description
`primaryObject`	Resource pool on the primary site
`secondaryObject`	Resource pool on the secondary site

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetTestNetworkMappings

This method returns an array of the test network mappings for this inventory mapper.

Synopsis

```
TestNetworkMapping[] getTestNetworkMappings();
```

`TestNetworkMapping[]` is an array of mappings from a network on the recovery site to a network that should be used for testing. It has the following fields:

Field	Description
`key`	Network on the recovery site
`testNetwork`	Network to be used while in the testing mode

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Autoprotect Manager

This section presents methods to enable automatic protection and related configuration settings.

SetAutoprotectUser

This method configures the user to be used by the automatic protection on this site. If not called, the default autoprotect user is used.

Synopsis

```
void setAutoprotectUser(String user)
```

The `user` parameter specifies the name of the user that will be used by automatic protection.

Faults

- RuntimeFault
- vmomi.fault.InvalidArgument
- vim.fault.NoPermission

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetAutoprotectUser

This method gets the user for automatic protection. Returns the current user account to be used by automatic protection on this site.

Synopsis

```
String getAutoprotectUser()
```

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

SetDefaultAutoprotectUser

This method reverts the current user to the default user.

Synopsis

```
void setDefaultAutoprotectUser()
```

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

IsActive

Checks if the automatic protection is globally activated (true) or deactivated (false). Automatic protection is active when both SRM servers in a pair support AutoprotectManager and the connection to the remote site is healthy. Automatic protection is not active when a peer SRM server does not support AutoprotectManager or the connection to the remote site is broken.

Synopsis

```
boolean IsActive()
```

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Protection

This section covers the Site Recovery Manager API methods for protection groups and virtual machine replication.

In SRM 5.8, new APIs appeared to create protection groups, assign them to recovery plans, and protect virtual machines using array-based or host-based replication. The new APIs provide three types of functionality for vSphere disaster recovery operations:

1. Infrastructure
   - workflows to create protection groups
   - workflows to create inventory mappings between matching objects
   - workflows to add protection groups to recovery plans
2. Virtual machine (VM) protection
   - workflows to protect VMs using a pre-configured array-based protection group
   - workflows to protect VMs using a pre-configured host-replicated protection group
3. Virtual machine (VM) recovery settings
   - recovery priority
   - per-VM callouts
   - final power state

ListProtectionGroups

This method lists the configured protection groups.

Synopsis

```
SrmProtectionGroup[] listProtectionGroups()
```

`SrmProtectionGroup[]` is an array of managed object references to all the `SrmProtectionGroup` managed objects that are currently configured. For more information, see Protection Group.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Method to list protection groups

```
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(ManagedObjectReference
 _this);

Where ManagedObjectReference _this = _protectionRef;
where _protectionRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
```

ListInventoryMappings

This method returns the configured inventory mappings. You establish placeholder datastores as described in the VMware Site Recovery Manager Documentation. You establish inventory mappings using the `AddFolderMapping`, `AddNetworkMapping`, and `AddResourcePoolMapping` methods documented in this manual, or using procedures described in the VMware Site Recovery Manager Documentation.

The destinations of each of the resources (network, resource pool, and folder) are not available in the data structure that is returned. If necessary, use the following:

- GetNetworkMappings
- GetResourcePoolMappings
- GetFolderMappings

Synopsis

```
Protection.InventoryMappingInfo listInventoryMappings( )
```

`inventoryMappingInfo` is a list of inventory mappings from the protected site to the recovery site:

- `folders` is a list of mapped VirtualMachine Folders.
- `networks` is a list of mapped virtual machine Networks and dvPortgroups.
- `pools` is a list of mapped Resource Pools.
- `testNetworks` is a list of mapped networks to test networks.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Method to list inventory mappings

```
SrmProtectionInventoryMappingInfo info = srmPortType.listInventoryMappings(ManagedObjectReference
 _this);
```

```
Where ManagedObjectReference _this = _protectionRef;
where _protectionRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
```

ListReplicatedDatastores

This method queries and lists replicated but unprotected datastores. A datastore is replicated if it contains any virtual machines in a protection group.

> **NOTE**
> This method is deprecated. As an alternative, use ListUnassignedReplicatedDatastores.

Synopsis

```
vim.Datastore[] listReplicatedDatastores()
```

`Datastore[]` is a list of replicated datastores on this site that can be used to create new protection groups.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Method to list replicated datastores

```
List < ManagedObjectReference > datastores = srmPortType.listReplicatedDatastores(ManagedObjectRef-
erence _this);

Where ManagedObjectReference _this = _protectionRef;
where _protectionRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
```

GetProtectionGroupRootFolder

Returns a reference to the top-level container for protection groups.

Synopsis

```
ProtectionGroupFolder getProtectionGroupRootFolder( )
```

`ProtectionGroupFolder` is the top-level folder for protection groups. For more information, see Protection Group Folder.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

ListUnassignedReplicatedDatastores

Gets a list of replicated datastores that can be used to create new protection groups.

Synopsis

```
vim.Datastore[] listUnassignedReplicatedDatastores( )
```

`Datastore[]` is a list of all datastores on this site that are replicated but not currently protected by Site Recovery Manager.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

ProtectionListProtectedDatastores

Get a list of the replicated datastores that are protected by Site Recovery Manager.

Synopsis

```
vim.Datastore[] ProtectionListProtectedDatastores( )
```

`Datastore[]` isa list of all datastores on this site that are replicated and protected by Site Recovery Manager.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

ListUnassignedReplicatedVms

Gets a list of replicated VMs that are currently not assigned to a Site Recovery Manager protection group.

Synopsis

```
vim.VirtualMachine[] listUnassignedReplicatedVms(String replicationType)
```

`listUnassignedReplicatedVms` has the following fields:

Field	Description
`replicationType`	an enumeration defined in `SrmProtectionGroup`. Valid values are `san` for ABR replicated virtual machines, `vr` for HBR replicated virtual machines and `vvol` for Vvol replicated virtual machines.
`VirtualMachine[]`	an enumeration defined in `SrmProtectionGroup`. Valid values are `san` for ABR replicated virtual machines, `vr` for HBR replicated virtual machines and `vvol` for Vvol replicated virtual machines.

Faults

- InvalidArgument
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

ProtectionListProtectedVms

Get a list of virtual machines that are protected by the Site Recovery Manager.

Synopsis

```
vim.VirtualMachine[] ProtectionListProtectedVms( )
```

`VirtualMachine[]` is a list of protected virtual machines.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

CreateAbrProtectionGroup

Create a new storage array-based ProtectionGroup using the provided datastores. This method does not automatically protect VMs on the storage array. Programs must call `ProtectVms()` separately for VMs on the storage array to be protected. If you have a replicated datastore with an existing VM on it and then create an ABR group, the VM will not be auto protected. Workaround is to add another VM to the datastore after the ABR protection group is created. This causes both the VMs to be protected with autoprotect.

NOTE
The protection group name cannot be the same as the folder in which it will be created.

Synopsis

```
CreateProtectionGroupTask createAbrProtectionGroup(Folder location, String name,@optional String description,
 vim.Datastore[] datastores)
```

Parameter	Description
`location`	folder in which to create the protection group
`name`	the name of the protection group
`description`	an optional description of the protection group
`datastores`	array of datastores to add to the new protection group

Returns `CreateProtectionGroupTask` to monitor the asynchronous operation of this method. For more information, see Create Protection Group Task.

Faults

- InvalidArgument
- InvalidType
- ReplicationProviderFault
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for CreateAbrProtectionGroup

```
ManagedObjectReference abrGroupRef = srmPortType.createAbrProtectionGroup(ManagedObjectReference
 _this,
```

```
    ManagedObjectReference location,
    String name,
    String description,
    List < ManagedObjectReference > datastores);

Where ManagedObjectReference _this = _protectionRef;
where _protectionRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
```

The following exceptions are presented by the `CreateProtectionGroupTask` instance that is returned by the `CreateAbrProtectionGroup` and `CreateHbrProtectionGroup` methods:

- `ConnectionDownFault` if the other site involved in the operation could not be contacted.
- `DuplicateName` if a group with this name already exists.
- `StringArgumentTooLong` if the size of either name or description in the settings parameter is too long.

CreateHbrProtectionGroup

Create a host based replication (vSphere replication) protection group using the provided VMs. This method does not automatically protect VMs on the storage array. Programs must call `ProtectVms()` separately for VMs on the storage array to be protected.

> **NOTE**
> The protection group name cannot be the same as the folder in which it will be created.

Synopsis

```
CreateProtectionGroupTask createHbrProtectionGroup(Folder location, String name,@optional String description,
 vim.VirtualMachine[] vms)
```

Parameter	Description
`location`	folder in which to create the protection group
`name`	the name of the protection group
`description`	an optional description of the protection group
`vms`	virtual machines to associate with the new protection group. The virtual machine list cannot be empty.

Returns `CreateProtectionGroupTask` to monitor the asynchronous operation of this method. For more information, see Create Protection Group Task.

Faults

- InternalError
- InvalidArgument
- InvalidType
- ReplicationProviderFault
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

CreateHbrProtectionGroup

```
ManagedObjectReference hbrGroupRef = srmPortType.createHbrProtectionGroup(ManagedObjectReference
 _this,
  ManagedObjectReference location,
  String name,
  String description,
  List < ManagedObjectReference > vms);

Where ManagedObjectReference _this = _protectionRef;
where _protectionRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
```

The following exceptions are presented by the `CreateProtectionGroupTask` instance that is returned by the `CreateAbrProtectionGroup` and `CreateHbrProtectionGroup` methods:

- `ConnectionDownFault` if the other site involved in the operation could not be contacted.
- `DuplicateName` if a group with this name already exists.
- `StringArgumentTooLong` if the size of either name or description in the settings parameter is too long.

CreateHbrProtectionGroup2

This method creates a new host based (that is vSphere replication) `Protection Group` using the provided virtual machines. The list of virtual machines can be empty.

> **NOTE**
> The protection group name cannot be the same as the folder in which it will be created.

Synopsis

```
CreateProtectionGroupTask createHbrProtectionGroup2(
       drextapi.Folder location,
       String name,
       @optional String description,
       @optional vim.VirtualMachine[] vms)
```

`createHbrProtectionGroup2` returns `CreateProtectionGroupTask` to monitor the asynchronous operation of this method. For more information, see Create Protection Group Task.

`createHbrProtectionGroup2` method has the following parameters:

Field	Description
`location`	Folder in which to create the protection group.
`name`	The name of the protection group.
`description`	An optional description of the protection group.
`vms`	VirtualMachines to associate with the new protection group. `ProtectVms` must be called for these VMs to be protected.

Faults

- InvalidArgument
- InternalError
- InvalidType

- ReplicationProviderFault
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

CreateVvolProtectionGroup

Creates a new VVol ProtectionGroup. Returns a task instance to monitor the asynchronous operation of this method.

Synopsis

```
CreateProtectionGroupTask createVvolProtectionGroup(
                drextapi.Folder location,
                String name,
                @optional String description,
                @optional ReplicationGroupId[] replicationGroups)
```

`createVvolProtectionGroup` has the following parameters:

Parameter	Description
`location`	Folder in which the protection group should be created
`name`	Name of the protection group
`description`	Description of the protection group
`replicationGroups`	List of the replication groups to be configured for the protection group. Only the virtual machines replicated by these replication groups can be protected in this protection group.

Faults

- InternalError
- InvalidArgument
- ReplicationProviderFault
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

RemoveProtectionGroup

The `removeProtectionGroup` method unprotects the VMs in the protection group and deletes the group.

Synopsis

```
RemoveProtectionGroupTask removeProtectionGroup(ProtectionGroup group)
```

The `group` parameter specifies the protection group that must be deleted.

RemoveProtectionGroupTask is a task object that contains information about the status of the operation. Site Recovery Manager Server retains the object for 30 minutes after the task finishes.

Faults

- ConnectionDownFault
- ProtectionGroupNotEmpty
- ReplicationProviderFault

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Protection Group Folder

This section presents methods to navigate folder hierarchy and retrieve specific protection groups.

ListChildProtectionGroupFolders

Returns the child Protection Group Folders located within this folder.

Synopsis

```
ProtectionGroupFolder[] listChildProtectionGroupFolders( )
```

`ProtectionGroupFolder[]` is the array of Protection Group Folders within this folder. Protection Group Folders for which the current session does not have the `System.View` privilege are removed from the result set. For more inforamtion, see Protection Group.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

ListChildProtectionGroups

Returns the child Protection Groups located within this folder.

Synopsis

```
ProtectionGroup[] listChildProtectionGroups( )
```

`ProtectionGroup[]` is the array of Protection Groups within this folder. Protection Groups for which the current session does not have the `System.View` privilege are removed from the result set. For more inforamtion, see Protection Group.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetProtectionGroup

Retrieves the protection group with the specified name, if any.

Synopsis

```
ProtectionGroup getProtectionGroup(String name)
```

`name` is the name of the protection group.

Returns a specific `ProtectionGroup` with the given name. For more information, see Protection Group.

Faults

- ProtectionGroupNotFound
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Create Protection Group Task

This chapter presents methods to track progress and completion of create protection group calls.

IsCreateProtectionGroupComplete

This function checks completeness of the operation. To get the result, see `GetCreateProtectionGroupResult`.

Synopsis

```
boolean IsCreateProtectionGroupComplete( )
```

True if this task has been completed.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetCreateProtectionGroupResult

This function gets the `TaskInfo` object containing the detailed results. To check completeness, see `IsCreateProtectionGroupComplete`.

Synopsis

```
TaskInfo GetCreateProtectionGroupResult( )
```

Returns the details results of this task.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetNewProtectionGroup

After calling `CreateAbrProtectionGroup` or `CreateHbrProtectionGroup` or `createVvolProtectionGroup` to create a protection group, this call makes a new one and fills in the protection group with the final result of the operation. To get the task results, see `GetCreateProtectionGroupResult`. To check status, see `IsCreateProtectionGroupComplete`.

Synopsis

```
ProtectionGroup GetNewProtectionGroup( )
```

Returns the newly created `ProtectionGroup`.

Faults

- InvalidState
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Protection Group

For array based replication, Site Recovery Manager organizes datastore groups to collect files associated with protected virtual machines. You configure array based replication by associating datastore groups with protection groups. All virtual machines in a datastore group replicate files together, and all virtual machines recover together.

Configure the host based replication (vSphere replication) for one virtual machine by associating it with a protection group, or you can configure multiple virtual machines by associating their folder or datacenter with a protection group.

You should configure vvol replication by associating replication groups with the protection groups.

Use the methods AssociateVms and UnassociateVms with the host based replication, but not with array based and vvol replications.

GetInfo

This method retrieves basic information about the specified protection group.

To get an `SrmProtectionGroup` managed object reference, see ListProtectionGroups.

Synopsis

```
ProtectionGroup.Info getInfo( )
```

`ProtectionGroup.Info` is information about the protection group. It has the following fields:

Field	Description
`description`	protection group description
`name`	protection group name
`type`	either `san` for array based replication, `vr` for vSphere replication or `vvol` for vVol replication

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for GetInfo

```
SrmProtectionGroupInfo info = srmPortType.getInfo(ManagedObjectReference _this);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
```

```
_protectionGroupRef = groups.get(0);
```

ProtectionGroupGetParentFolder

Given a protection group, gets the parent folder.

Synopsis

```
ProtectionGroupFolder ProtectionGroupGetParentFolder( )
```

`ProtectionGroupFolder` – extends `Folder`; can hold Protection Group and Protection Group Folder.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetPeer

Given an `SrmProtectionGroup` on the local site, this method retrieves the `SrmProtectionGroup` at the peer site.

Synopsis

```
ProtectionGroup.Peer getPeer( )
```

`ProtectionGroup.Peer` is the peer protection group from the remote site.

`Peer` is the peer protection group object at the paired site. It has the following fields:

Field	Description
`group`	`ProtectionGroup` at that site.
`state`	Last known state of this protection group. If the connection between sites is down, this value might be out-of-date.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for GetPeer

```
SrmProtectionGroupPeer peerGroup = srmPortType.getPeer(ManagedObjectReference _this);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

ListProtectedVms

Retrieves the list of virtual machines currently protected in the specified protection group, with information about their placeholder VM and protection state.

Synopsis

```
ProtectionGroup.ProtectedVm[] listProtectedVms( )
```

`ProtectedVm[]` is an array of ProtectedVm data objects with the following fields:

Field	Description
`faults`	any faults associated with this protected virtual machine
`needsConfiguration`	the protected virtual machine needs to be configured or repaired
`peerProtectedVm`	the protected virtual machine identifier on the remote site
`peerState`	the protection state on the remote site
`protectedVm`	the protected virtual machine identifier on the local site
`state`	the protection state of this particular virtual machine
`vm`	the locally protected virtual machine (this reference is valid after reprotect or revert operations)
`vmName`	the name of the locally protected virtual machine.
`drVmIdentity`	A DR-service (SRM) specific globally unique identifier for the virtual machine associated with this ProtectedVm object and similarly for the virtual machine associated with this ProtectedVm object's peer (e.g. the recovered virtual machine). This identifier is generated by an SRM server; it does not necessarily correspond to any identifier in vCenter or any other service. The value of this property is the same in the peer ProtectedVm managed object. The value is immutable and is maintained on both sites after failover and reprotect+failback. After this virtual machine is unprotected (ProtectedVm object is removed) the value of this identity may be reused but only by a ProtectedVm instance that is subsequently protecting the same virtual machine. **NOTE** There is no guarantee that a virtual machine's drVmIdentity value remains the same even if it is unprotected and then reprotected. Maintaining this value is currently only a best-effort operation.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for ListProtectedVms

```
List < SrmProtectionGroupProtectedVm > protectedVms = srmPortType.listProtectedVms(ManagedObjectRe-
ference _this);

Where ManagedObjectReference _this = _protectionGroupRef;
```

```
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

ListProtectedDatastores

This method retrieves the list of datastores that are protected by the specified protection group. A datastore can be a VMFS volume, a NAS directory, or a local file system path.

Synopsis

```
vim.Datastore[] listProtectedDatastores( )
```

`Returns Datastore[]` is an array of all Datastore objects protected by this protection group.

Faults

- RuntimeFault
- vmodl.fault.NotSupported if this protection group is not a SAN group.

See Faults in Site Recovery Manager API for more details.

Example for ListProtectedDatastores

```
List < ManagedObjectReference > datastores = srmPortType.listProtectedDatastores(ManagedObjectRef-
erence _this);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

ListAssociatedVms

This method retrieves the virtual machines currently associated with a specified vSphere Replication protection group.

For the method to get a list of protection groups, see ListProtectionGroups.

Synopsis

```
vim.VirtualMachine[] listAssociatedVms( )
```

`VirtualMachine[]` is an array listing the associated virtual machines.

Faults

- RuntimeFault
- vmodl.fault.NotSupported, if this protection group is not a VR group.

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for ListAssociatedVms

```
List < ManagedObjectReference > vms = srmPortType.listAssociatedVms(ManagedObjectReference _this);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

GetProtectionState

Gets current state of the specified protection group. Not to be confused with `GetProtectionStatus` which returns a virtual machine's (un)protect status, not the state of an entire protection group.

Synopsis

```
ProtectionGroup.ProtectionState getProtectionState( )
```

`ProtectionState` is an enumeration for the protection group state:

Fields	Description
`failedOver`	the protection group has been failed over to the remote site
`partiallyRecovered`	the protection group is partially recovered
`ready`	the protection group is in a ready state
`recovered`	the protection group has been recovered
`recovering`	the protection group is in the process of being recovered
`shadowing`	this protection group is shadowing the remote site group that is in a ready state
`testing`	the protection group is currently being tested

NOTE
While these states share a common type, they are specific to whether this Group is the Protection Group itself or the mirror of the group on the remote site. The Protection Group States are `ready` and `failedOver`. The Mirror States `partiallyRecovered`, `recovering`, `testing`, `shadowing`, and `recovered`.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for GetProtectionState

```
SrmProtectionGroupProtectionState state = srmPortType.getProtectionState(ManagedObjectReference
 _this);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
```

```
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

ProtectionGroupListRecoveryPlans

This method retrieves a list of all the recovery plans that this protection group is a member of.

Synopsis

```
RecoveryPlan[] ProtectionGroupListRecoveryPlans( )
```

`RecoveryPlan[]` is an array of all the Recovery Plans that this protection group belongs to. For more information, see Recovery Plan.

Fault

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for ProtectionGroupListRecoveryPlans

```
List < ManagedObjectReference > plans = srmPortType.protectionGroupListRecoveryPlans(ManagedObjec-
tReference _this);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

ProtectionGroupQueryVmProtection

Determine whether the specified virtual machines are currently protected, or can be protected. To protect a Virtual Machine, its folder, resource pool, and network must be mapped from the protected site to the recovery site.

To get a list of currently configured mappings, see ListInventoryMappings. You can also query replicated datastores with ListReplicatedDatastores.

Synopsis

```
ProtectionGroup.VmProtectionInfo[]
ProtectionGroupQueryVmProtection(vim.VirtualMachine[] vms)
```

`vms[]` is an array of managed object references to VirtualMachine objects.

`VmProtectionInfo[]` is an array of VmProtectionInfo data objects with the following fields:

Fields	Description
`faults`	any faults encountered while processing queryVmProtection for this virtual machine
`peerProtectedVm`	the protected virtual machine identifier on the remote site
`protectedVm`	the protected virtual machine identifier on the local site

Fields	Description
protectionGroup	the group this virtual machine is a member of, if it is protected
protectionGroupName	the name of this virtual machine's protection group, if it is protected
recoveryPlanNames	the name(s) of any recovery plans the virtual machine will be recovered in
recoveryPlans	any recovery plans the virtual machine will be recovered in
status	the current protection status of the virtual machine
vm	the virtual machine for which protection status is being returned

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for ProtectionGroupQueryVmProtection

```
List < SrmProtectionGroupVmProtectionInfo > protection = srmPortType.protectionGroupQueryVmProtec-
tion(
  ManagedObjectReference _this,
  List < ManagedObjectReference > vms);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

ProtectVms

This method adds virtual machines to a protection group.

With array-based replication, the protection group is determined by datastore location of the virtual machines. With host-based replication (vSphere replication), you can use the AssociateVms method to place virtual machines into a protection group. With vVol replication, the protection group is determined by replication groups of the virtual machines. To protect a Virtual Machine, its folder, resource pool, and network must be mapped from the protected site to the recovery site. To get a list of currently configured mappings, see ListInventoryMappings. If a few or all the VMs in the list are already protected, then the operation succeeds.

Synopsis

```
ProtectionTask protectVms(ProtectionGroup.VmProtectionSpec[] vms)
```

`vms[]` is a list of virtual machines to protect. If some of the virtual machines from the list or all of them are already protected, the operation succeeds.

`VmProtectionSpec` is a spec describing how a virtual machine to be protected. It has the following properties:

Field	Description
`@optional VirtualMachine vm`	The virtual machine to be protected
`VmRecoverySpec recoverySpec`	Information relevant at the recovery site to which the VM will be protected. Allows configuration of protection per VM instead of using global inventory mappings.

`VmRecoverySpec` is a spec describing virtual machine recovery locations. It has the following properties:

Field	Description
`@optional PlaceholderVmLocation placeholderVmLocation`	Location in which to create the placeholder VM.
`@optional RecoveryLocationSettings recoveryLocationSettings`	Recovery location settings.

`PlaceholderVmLocation` is a data object. It contains information about where a placeholder VM should be created. It has the following fields:

Field	Description
`folder`	Folder in which the placeholder VM should be created. If unset, the inventory mapper will be queried for a suitable location.
`hostSystem`	Host in which the placeholder VM should be created. If unset, SRM will attempt to pick one based on the resource pool mapping (this works only if the resource pool unambiguously designates a single host, or if it designates a DRS cluster).
`resourcePool`	Resource pool in which the placeholder VM should be created. If unset, the inventory mapper will be queried for a suitable location.
`placeholderDatastore`	Datastore in which the placeholder VM should be created. If unset, the placeholder datastore manager will be queried for a suitable location.

`RecoveryLocationSettings` is a spec that provides user-editable settings regarding where to find virtual machine components at recovery time. It has the following properties:

Field	Description
`@optional DeviceInfo[] protectedDevices`	Information about devices for which the user has supplied recovery-time information.
`@optional DeviceInfo[] excludedDevices`	Information about devices for which the user does not want to be present in the recovered VM. If autoExcludeMediaDevices advance settings is enabled, the list includes the media devices that are auto-excluded by SRM.

Field	Description
`@optional String changeVersion`	Change version control. When reconfiguring an existing settings this value must be set and must match the most recent value. This means that first `#getRecoveryLocationSettings` should be called. Then its result should be updated and passed to `#reconfigureRecoveryLocationSettings` . For newly protected VMs, leave it unset.

`DeviceInfo` is a data object with the following properties:

Field	Description
`key`	Device key

`NetworkDeviceInfo` extends DeviceInfo and has the following properties:

Field	Description
`vim.Network network`	Reference to a recovery network managed object to which to attach the NIC device.

`FileDeviceInfo` extends DeviceInfo and has the following properties:

Field	Description
`@optional vim.Datastore datastore`	Reference to the datastore the directory is located on. If the directory is not located on a datastore, this is omitted.
`path`	Directory path.
`fileName`	Name of the file under the directory.

`NetworkDeviceInfo` and `FileDeviceInfo` should be used to construct `RecoveryLocationSettings`.

`ProtectionTask` is the task object to monitor the status of requested virtual machines. For more information, see Protection Task.

If a task fails, its error field may contain one of the following:

- `drextapi.fault.ConnectionDownFault` - if the remote SRM could not be reached.
- `drextapi.fault.CannotProtectFTSecondaryVm` - if the VM is a fault tolerance secondary VM.
- `drextapi.fault.DeviceBackingConflict` - if the caller specified a device locator, or explicitly excluded, a device which the provider would like to protect.
- `drextapi.fault.DevicesNotResolved` - if any of the VM's devices were neither protected by the provider, nor was a backing locator provided by the caller, nor was the device explicitly excluded.
- `drextapi.fault.InsufficientLicensesFault` - If there were not enough licenses available to protect the VMs.
- `drextapi.InvalidState` - if the group we are trying to protect into is not in the 'ProtectedVm.State#active active' state.
- `drextapi.fault.ProductionVmDeleted` - if the VM to be protected did not exist on VC.
- `drextapi.fault.ReplicationProviderFault` - if the replication provider rejected the operation.
- `drextapi.fault.VmAlreadyProtectedEx` - if the VM was already protected in another group.
- `vim.fault.ConcurrentAccess` - if the group was modified during the operation.

Faults

- InvalidArgument - If the list of virtual machines is empty or null.
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for ProtectVms

```
ManagedObjectReference taskRef = srmPortType.protectVms(
  ManagedObjectReference _this,
  List < SrmProtectionGroupVmProtectionSpec > vms);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

UnprotectVms

This method removes virtual machines from their protection group. With an array-based replication, the protection group is determined by datastore location of the virtual machines. With vSphere Replication, you must also `UnassociateVms` from the protection group. With the vVol replication, the protection group is determined by replication groups of the virtual machines.

Synopsis

```
ProtectionTask unprotectVms(vim.VirtualMachine[] vms)
```

`vms[]` is an array Virtual Machine objects not to protect.

Protection Task is the task object to monitor for status of the requested virtual machines.

Faults

- InvalidArgument - If the list of virtual machines is empty or null.
- InvalidState, if a specified VM was not being protected.
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for UnprotectVms

```
ManagedObjectReference taskRef = srmPortType.unprotectVms(
  ManagedObjectReference _this,
  List < ManagedObjectReference > vms);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

AssociateVms

This method associates one or more virtual machines with a vSphere Replication (VR) protection group. Before you can protect a virtual machine, it must first be associated with a protection group.

Synopsis

```
void associateVms(vim.VirtualMachine[] vms)
```

`vms[]` is an array of Virtual Machine objects to associate with.

Faults

- InvalidArgument - If the list of virtual machines is empty or null.
- InvalidState, if a specified VM was already associated with another group.
- RuntimeFault
- vim.fault.ConcurrentAccess, if another operation has modified the object and the change version no longer matches.
- vmodl.fault.NotSupported, if this protection group is not a VR group.

See Faults in Site Recovery Manager API for more details.

Example for AssociateVms

```
srmPortType.associateVms(
  ManagedObjectReference _this,
  List < ManagedObjectReference > vms);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

UnassociateVms

This method removes the association of one or more virtual machines from a specified vSphere Replication (VR) protection group. Once a virtual machine is unassociated, it can no longer be protected.

Synopsis

```
void unassociateVms(vim.VirtualMachine[] vms)
```

`vms[]` is an array of Virtual Machine objects to disassociate from.

Faults

- InvalidArgument - If the list of virtual machines is empty or null.
- InvalidState, if a specified VM was already associated with another group.
- RuntimeFault
- vim.fault.ConcurrentAccess, if another operation has modified the object and the change version no longer matches.
- vmodl.fault.NotSupported, if this protection group is not a VR group.

See Faults in Site Recovery Manager API for more details.

Example for UnassociateVms

```
srmPortType.unassociateVms(
  ManagedObjectReference _this,
  List < ManagedObjectReference > vms);

Where ManagedObjectReference _this = _protectionGroupRef;
where _protectionGroupRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
```

CheckConfigured

The `checkConfigured` method checks the protection group for not configured VMs, configuration issues detected since the group was created or modified and protected virtual machines that needs configuration (if Placeholder VM needs repair or there are unresolved devices).

Synopsis

```
boolean checkConfigured()
```

The method returns true if the protection group is configured and you can use the group.

Faults

- InvalidState is thrown if the group is not on the protected site and cannot get information about the remote object.
- RuntimeFault
- vmodl.fault.NotSupported is thrown if the group is not a VR, SAN or vVol group.

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

ProtectionGroupGetOperationalLocation

The `ProtectionGroupGetOperationalLocation` method returns the effective location of the protection group for the purposes of determining when various operations should be run.

Synopsis

```
String ProtectionGroupGetOperationalLocation()
```

Faults

RuntimeFault

See Faults in Site Recovery Manager API for more details.

AddDatastores

Adds datastores to the protection group. Additionally, the virtual machines on these datastores can be protected by the protection group. This can be done by calling protectVms method from this interface.

Synopsis

```
void addDatastores(@optional Datastore[] datastores)
```

`datastores` is the list of datastores that will be added to the protection group.

Faults

- InvalidArgument
- InvalidState
- NotSupported
- ReplicationProviderFault
- RuntimeFault
- vim.fault.ConcurrentAccess

See Faults in Site Recovery Manager API for more details.

RemoveDatastores

Removes datastores from the protection group. Virtual machines on the removed datastores are no longer protected by the protection group.

Synopsis

```
void removeDatastores(@optional Datastore[] datastores)
```

`datastores` is the list of datastores that will be removed from the protection group.

Faults

- InvalidArgument
- InvalidState
- NotSupported
- ReplicationProviderFault
- RuntimeFault
- vim.fault.ConcurrentAccess

See Faults in Site Recovery Manager API for more details.

ReconfigureVvolProtectionGroup

Reconfigures settings for this group. For a vVol ProtectionGroup, this method can reconfigure the name, description, and replication groups.

Synopsis

```
void reconfigureVvolProtectionGroup(
        @optional String name,
        @optional String description,
```

```
        @optional ReplicationGroupId[] replicationGroups)
```

Parameter	Description
`name`	New name for this protection group.
`description`	Sets a new description for this protection group.
`replicationGroups`	Replication groups that will be configured for this group.

Faults

- ConcurrentAccess
- DuplicateName
- InvalidArgument
- InvalidState
- NotSupported
- ReplicationProviderFault
- RuntimeFault
- StringArgumentTooLong

See Faults in Site Recovery Manager API for more details.

GetVvolGroupDetails

Gets vVol specific details for this protection group.

Synopsis

```
drextapi.vvol.GroupDetails getVvolGroupDetails()
```

`GroupDetails` is the VvolProvider specific details for a protection group. It has the following fields:

Field	Description
`domain`	Identifier of the fault domain operated by this protection group. The VVOL protection group is limited to protecting VMs that belong to the same fault domain. The fault domain is determined by the replication groups configured for this protection group.
`ReplicationGroupInfo[] replicationGroups`	Source VVOL replication groups for this protection group. Both protection and recovery site report the same replication groups.
`VmInfo[] protectedVms`	Info about the protected VMs in this protection group including VMs replication groups association.
`VmInfo[] unprotectedVms`	The list of VMs that are not protected and are replicated by a replication group that is part of this protection group Available only from protection site, i.e. @primary == true
`primary`	Flag that is set if the protection group is primary.

`VmInfo` is the information about a local vVol replicated vim.VirtualMachine. It has the following fields:

Field	Description
`key`	The vim.VirtualMachine object at the local site.
`name`	Name of the virtual machine.
`ReplicationGroupInfo[] replicationGroups`	Replication groups for this VM. Virtual machines sharing the same replication groups belong to the same consistency group. They will be added or removed from a protection group together.

`ReplicationGroupInfo[]` is the information about a vVol replication group. It has the following fields:

Field	Description
`replicationGroup`	Replication group ID.
`name`	Name of the replication group. May be unset if not available.

`FaultInfo` is the warning and error information object. Both `VmInfo` and `ReplicationGroupInfo` inherits `FaultInfo`. It has the following fields:

Field	Description
`warnings`	Warnings associated with this object.
`name`	Errors associated with this object.

Fault

- NotSupported
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

MoveGroup

This method moves specified ProtectionGroup to a different folder.

Synopsis

```
@task void moveGroup(drextapi.Folderdestination);
```

`moveGroup` returns a task instance to monitor the asynchronous operation of this method. It has the following parameters:

Field	Description
`destination`	Folder which will become the new parent folder of this group. For more information, see SRM Folder.

If a task fails, its error field may contain one of the following:

- `drextapi.fault.DuplicateName` - A ProtectionGroup with the same name already exists within the destination folder.
- `vim.fault.NotSupported` - if the ProtectionGroup is being moved into a folder whose childType() property is not set to the appropriate value. For example, a ProtectionGroup cannot be moved into a folder whose ChildType property value does not contain "ProtectionGroup".
- `drextapi.fault.ConnectionDownFault` - if the sites are not connected.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetPlaceholderVmInfo

This method returns information for the placeholder VM for the specified protected VM.

Synopsis

```
PlaceholderVmInfo getPlaceholderVmInfo(ProtectedVm protectedVm)
```

`ProtectedVm` is an array of ProtectedVm data objects. For more information, see ListProtectedVms.

`PlaceholderVmInfo` is a data object. It provides information about the inventory location of the placeholder `vim.VirtualMachine` . It has the following fields:

Field	Description
`vm`	Placeholder VM. This can be unset if the placeholderVm has been deleted or has not been created succesfully.
`folder`	Placeholder VM folder
`computeResource`	Placeholder VM ComputeResource. Not set if the VM is a template.
`resourcePool`	Placeholder VM ResourcePool. Not set if the VM is a template.
`host`	Placeholder VM host.
`datacenter`	Placeholder VM datacenter
`placeholderCreationFault`	Fault from the most recent placeholder creation operation at the local site, if that operation failed. Otherwise unset.
`repairNeeded`	Set to true if the placeholder VM needs to be repaired. false otherwise.

Faults

- InvalidArgument
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

RecreatePlaceholder

Recreates a placeholder VM.

This method is called when the placeholder needs to be recreated due to one of these reasons:

- Placeholder creation failed.
- Placeholder was deleted.
- Placeholder inventory was lost or needs to be reentered - one use case for this is when production vm was a template but then gets converted to a VM.

This method can be called only on the recovery site. It does not need primary site to be up for succesful completion. This method requires `Resource.com.vmware.vcDr.RecoveryUse` on the host, resorce pool, datastore, and folder.

Synopsis

```
@task void recreatePlaceholder(ProtectedVm protectedVm, PlaceholderVmLocation placeholderVmLocation)
```

recreatePlaceholder has the following parameters:

Field	Description
`protectedVm`	ProtectedVm for which the placeholder VM will be recreated. For more information, see ListProtectedVms.
`placeholderVmLocation`	New location for the placeholder VM. For more information, see ProtectVms.

If a task fails, its error field may contain the following:

- `drextapi.fault.InvalidState` - if repair is called from the wrong site.

Faults

- InvalidArgument
- RuntimeFault

GetRecoveryLocationSettings

This method returns the recovery location settings for the specified protected VM.

Synopsis

```
RecoveryLocationSettings getRecoveryLocationSettings(ProtectedVm protectedVm)
```

`RecoveryLocationSettings` is a data object. It has user-editable settings regarding where to find the VM components during recovery time. For more information, see ProtectVms.

`ProtectedVm` is an array of protected VM data objects. For more information, see ListProtectedVms.

Faults

- InvalidArgument
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

ReconfigureRecoveryLocationSettings

Reconfigures the recovery location settings for the specified protected VM. This method should be invoked on the protection site only.

Synopsis

```
@task void reconfigureRecoveryLocationSettings(ProtectedVm protectedVm, RecoveryLocationSettings recoveryLocationSettings)
```

`reconfigureRecoveryLocationSettings` has he following parameters:

Field	Description
`protectedVm`	The protected VM which settings will be updated. For more information, see ProtectVms.
`recoveryLocationSettings`	The new settings to apply. For more information, see ProtectVms.

`ReconfigureRecoveryLocationSettings` returns the `drextapi.Task`. For more information, see SrmExtApiTask.

If a task fails, its error field may contain one of the following:

- `vim.fault.ConcurrentAccess` if another operation has modified the object and the change version no longer matches.
- `drextapi.fault.InvalidState` if the state of the protected VM is not 'active'.
- `drextapi.fault.DeviceBackingConflict` if the caller specified a device locator, or explicitly excluded, a device which the provider would like to protect.

Faults

- InvalidArgument
- InvalidState
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetAbrGroupDetails

Gets ABR-specific details for the specified protection group.

Synopsis

```
StorageProviderGroupDetails getAbrGroupDetails()
```

The `StorageProviderGroupDetails` has one parameter, `arrayPair`, which represents the replicated array pair holding the underlying storage devices. The `arrayPair` is of type ReplicatedArrayPair.

Faults

- NotSupported
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Protection Task

A task returned by `ProtectVms` or `UnprotectVms` acquires the final status of an operation upon completion. While the task is running, partial results may be returned. Once the task has been completed, the object will be removed from the server after 30 minutes.

GetProtectionStatus

This method gets the virtual machine protection status after completion of `ProtectVms` or `UnprotectVms`.

Synopsis

```
ProtectionGroup.VmProtectionInfo[] getProtectionStatus()
```

`VmProtectionInfo[]` – the completed protection status of VMs that were requested to be protected or unprotected. For more information about VmProtectionInfo, see ProtectionGroupQueryVmProtection.

The `VmProtectionInfo.ProtectionStatus` has the following fields:

Fields	Description
`canBeProtected`	the VM is able to be protected, but is not currently
`canNotBeProtected`	the VM is not able to be protected
`isProtected`	the VM is already protected
`needsConfiguration`	the VM must be configured or repaired before it may be protected. Please check the faults property for information about any additional prerequisites.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for GetProtectionStatus

```
List < SrmProtectionGroupVmProtectionInfo > protectionStatus = srmPortType.getProtectionStatus(Man-
agedObjectReference _this);

Where ManagedObjectReference _this = _protectionTaskRef;
where _protectionTaskRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
ManagedObjectReference _protectionTaskRef = srmPortType.protectVms(
  _protectionGroupRef,
  _vms);
```

GetTasks

This method retrieves task information from the vCenter Server after a `ProtectVms` or `UnprotectVms` request, which both take some time to complete.

Synopsis

```
ProtectionTask.VmTask[] getTasks()
```

`VmTask[]` is an array of monitorable task information keyed by Virtual Machine, containing:

- `task` – managed object reference to a task on the Site Recovery Manager server.
- `vm` – managed object reference to a VirtualMachine.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for GetTasks

```
List < SrmProtectionTaskVmTask > tasks = srmPortType.getTasks(ManagedObjectReference _this);

Where ManagedObjectReference _this = _protectionTaskRef;
where _protectionTaskRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
ManagedObjectReference _protectionTaskRef = srmPortType.protectVms(
  _protectionGroupRef,
  _vms);
```

IsComplete

This method checks whether the protection task has completed.

Synopsis

```
boolean isComplete( )
```

Returns true if the task has completed, false if not.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for IsComplete

```
boolean isComplete = srmPortType.isComplete(ManagedObjectReference _this);

Where ManagedObjectReference _this = _protectionTaskRef;
where _protectionTaskRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
ManagedObjectReference _protectionTaskRef = srmPortType.protectVms(
  _protectionGroupRef,
  _vms);
```

GetResult

This method gets detailed results of the completed protection task.

Synopsis

```
vim.TaskInfo[] getResult( )
```

`TaskInfo` is a data object that contains all information about a task. For more information, see `TaskInfo` in the *Site Recovery Manager API Reference Guide*.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for GetResult

```
List < TaskInfo > taskInfo = srmPortType.getResult(ManagedObjectReference _this);

Where ManagedObjectReference _this = _protectionTaskRef;
where _protectionTaskRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _protectionRef = content.getProtection();
List < ManagedObjectReference > groups = srmPortType.listProtectionGroups(_protectionRef);
_protectionGroupRef = groups.get(0);
ManagedObjectReference _protectionTaskRef = srmPortType.protectVms(
  _protectionGroupRef,
  _vms);
```

Recovery

This section covers the external Interface to Site Recovery Manager - Recovery. This interface works only on the locally connected site except where specified.

ListPlans

This method retrieves all the recovery plans for this Site Recovery Manager server. Once you have a list of recovery plans, you can retrieve information about each plan.

Synopsis

```
RecoveryPlan[] listPlans()
```

`RecoveryPlan[]` is a list of Recovery Plans, including plan information, peer recovery plan, recovery mode, recovery plan location, recovery prompt, and recovery state. For more information, see Recovery Plan.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetHistory

This method retrieves the history of a given recovery plan.

Synopsis

```
RecoveryPlanHistory getHistory(RecoveryPlan plan)
```

`plan` is the Recovery Plan of interest.

`RecoveryPlanHistory` is the history of the given Recovery Plan.

Faults

- RecoveryPlanNotFound
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for GetHistory

```
ManagedObjectReference history = srmPortType.getHistory(
  ManagedObjectReference _this,
  ManagedObjectReference plan);

Where ManagedObjectReference _this = _recoveryRef;
where _recoveryRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
```

GetRecoveryPlanRootFolder

Gets a reference to the top level container (the root folder) for recovery plans.

Synopsis

```
RecoveryPlanFolder getRecoveryPlanRootFolder()
```

`RecoveryPlanFolder` – a Site Recovery Manager folder that holds Recovery Plans and Recovery Plan Folders. For more information, see Recovery Plan Folder.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

CreateRecoveryPlan

The `createRecoveryPlan` method creates a recovery plan. You call the method by passing the name and folder of the plan, and the protection group(s) that must be included in the plan.

Synopsis

```
CreateRecoveryPlanTask createRecoveryPlan(
  String name,
  drextapi.Folder folder,
```

```
ProtectionGroup[] groups,
@optional String description,
@optional TestNetworkMapping[] mapping)
```

Parameter	Description
name	Specifies the name of the plan. Must be unique in the parent folder, and contain between 1 and 80 characters.
folder	Specifies the folder where the plan is created.
groups	Specifies the protection groups that are added to the recovery plan.
description	Optional parameter. Specifies the recovery plan description. Should not contain more than 4096 characters.
mapping	Optional parameter. Specifies the test network mappings. For more information, see GetTestNetworkMappings.

CreateRecoveryPlanTask is a task object that contains information about the status of the operation. Site Recovery Manager Server retains the object for 30 minutes after the task finishes.

`IsCreateRecoveryPlanComplete` returns true if the task for creating a recovery plan is complete.

`GetCreateRecoveryPlanFailure` returns the failure during the operation for creating a recovery plan. If you pass a name of a plan that exists, the failure is DuplicateNames.

If the operation is successful, the `GetNewRecoveryPlan` returns the created recovery plan.

> **NOTE**
> The recovery plan name can not be the same as the folder in which it will be created.

If a task fails, its error field may contain one of the following:

- `DuplicateNames` if a plan with this name already exists.
- `InvalidArgument` if the name parameter is empty string
- `InvalidType` if folder parameter isn't meant to hold a recovery plans.
- `InvalidPrimaryNetwork` if mapping parameter contains `TestNetworkMapping` with an invalid network on primary site. For example, uplink DVPortgroup.
- `InvalidSecondaryNetwork` if mapping parameter contains TestNetworkMapping with an invalid network on secondary site. For example uplink DVPortgroup.
- `NoPermission` if user doesn't have `VcDr.RecoveryProfile.com.vmware.vcDr.Create` privilege on the specified folder or `VcDr.ProtectionProfile.com.vmware.vcDr.AssignToRecoveryPlan` privilege on all protection groups in the plan.
- `StringArgumentTooLong` if the size of either name or description of the plan is too long.
- `UnknownPrimaryNetwork` if mapping parameter contains TestNetworkMapping with a network that does not exist on primary site.
- `UnknownSecondaryNetwork` if mapping contains `TestNetworkMapping` with a network that does not exist on secondary site.

Faults

- DirectionError
- InvalidArgument
- ProtectionGroupNotFound
- RemoteSiteNotEnabled

- RuntimeFault
- StringArgumentTooLong

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

DeleteRecoveryPlan

The `deleteRecoveryPlan` method deletes the recovery plan that is passed as parameter.

Synopsis

```
DeleteRecoveryPlanTask deleteRecoveryPlan(RecoveryPlan plan)
```

The `plan` parameter specifies the recovery plan that must be deleted

`DeleteRecoveryPlanTask` is a Task object that contains information about the status of the operation. Site Recovery Manager Server retains the object for 30 minutes after the task finishes.

The `IsDeleteRecoveryPlanComplete` returns true if the task is complete.

The `GetDeleteRecovryPlanFailure` returns the failure that occurs during the delete operation. If the plan or its peer is not in a valid state, the task fails with InvalidState.

Faults

RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

MovePlan

This method moves the RecoveryPlan to a different folder.

Synopsis

```
@task void movePlan(RecoveryPlan recoveryPlan, drextapi.Folder destination)
```

`movePlan` returns a task instance to monitor the asynchronous operation of this method. This method has the following parameters:

Field	Description
`recoveryPlan`	Recovery plan to move. For more information, see Recovery Plan.
`destination`	Folder which will become the new parent folder of this plan. For more information, see SRM Folder.

If a task fails, its error field may contain one of the following:

- `drextapi.fault.DuplicateName` - A RecoveryPlan with the same name already exists within the destination folder.
- `vim.fault.NotSupported` - if the RecoveryPlan is being moved into a folder whose childType() property is not set to the appropriate value. For example, a RecoveryPlan cannot be moved into a folder whose `ChildType` property value does not contain "RecoveryPlan".
- `drextapi.fault.ConnectionDownFault` - if the sites are not connected.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Recovery Plan Folder

This section presents methods to traverse the folder hierarchy for Recovery Plans.

ListChildRecoveryPlanFolders

Returns the child Recovery Plan Folders located in this folder.

Synopsis

```
RecoveryPlanFolder[] listChildRecoveryPlanFolders( )
```

`RecoveryPlanFolder[]` is the array of sub-folders within this folder. If the current session does not have the `System.View` privilege for a `RecoveryPlanFolder`, it is removed from the result set.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for ListChildRecoveryPlanFolders

```
List < ManagedObjectReference > childFolders = srmPortType.listChildRecoveryPlanFolders(ManagedOb-
jectReference _this);

Where ManagedObjectReference _this = _recoveryPlanRootFolderRef;
where _recoveryPlanRootFolderRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
ManagedObjectReference _recoveryPlanRootFolderRef = srmPortType.getRecoveryPlanRootFolder(_recov-
eryRef);
```

ListChildRecoveryPlans

Returns an array of `RecoveryPlan` objects located within this folder.

Synopsis

```
RecoveryPlan[] listChildRecoveryPlans( )
```

`RecoveryPlan[]` is the array of Recovery Plans within this folder. If the current session does not have the `System.View` privilege for a `RecoveryPlan`, it is removed from the result set. For more information, see Recovery Plan.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for ListChildRecoveryPlans

```
List < ManagedObjectReference > childPlans = srmPortType.listChildRecoveryPlans(ManagedObjectRefer-
ence _this);

Where ManagedObjectReference _this = _recoveryPlanRootFolderRef;
where _recoveryPlanRootFolderRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
ManagedObjectReference _recoveryPlanRootFolderRef = srmPortType.getRecoveryPlanRootFolder(_recov-
eryRef);
```

GetRecoveryPlan

Retrieves a specific recovery plan.

Synopsis

```
RecoveryPlan getRecoveryPlan(String name)
```

`name` is the name of a Recovery Plan.

`RecoveryPlan` is a Recovery Plan, which includes plan information, peer recovery plan, recovery mode, recovery plan location, recovery prompt, and recovery state. For more information, see Recovery Plan.

Faults

- RecoveryPlanNotFound
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for GetRecoveryPlan

```
ManagedObjectReference plan = srmPortType.getRecoveryPlan(
  ManagedObjectReference _this,
  String name);

Where ManagedObjectReference _this = _recoveryPlanRootFolderRef;
where _recoveryPlanRootFolderRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
ManagedObjectReference _recoveryPlanRootFolderRef = srmPortType.getRecoveryPlanRootFolder(_recov-
eryRef);
```

Recovery Plan

This section covers the interfaces to recovery plans.

RecoveryPlanGetInfo

This method retrieves status information about a given recovery plan, including the name of the recovery plan and its current state.

Synopsis

```
RecoveryPlan.Info RecoveryPlanGetInfo( )
```

`RecoveryPlan.Info` is a data object that describes details of this recovery plan, including:

- `name` is the name of this recovery plan.
- `description` is a description of this recovery plan.
- `protectionGroups[]` is an array of protection groups that will be recovered as part of this plan.
- `state` – the state of this recovery plan, enumerated as:
  - `cancelling` – recovery plan is in the process of cancelling
  - `error` – recovery plan has errors
  - `failedOver` – recovery plan has failed over
  - `needsCleanup` – need to cleanup a test run
  - `needsFailover` – need to re-run recovery (failover)
  - `needsReprotect` – need to re-run reprotect
  - `needsRollback` – need to re-run rollback
  - `prompting` – recovery plan is running, but requires user-interaction before it may continue
  - `protecting` – recovery plan is protecting to remote site, run peer recovery plan on remote site
  - `ready` – recovery plan is not in a running state and may be run
  - `running` – recovery plan is currently running

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Examples for RecoveryPlanGetInfo

```
SrmRecoveryPlanInfo planInfo = srmPortType.recoveryPlanGetInfo(ManagedObjectReference _this);

Where ManagedObjectReference _this = _recoveryPlan;
where _recoveryPlan can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List < ManagedObjectReference > plans = srmPortType.listPlans(
  _recoveryRef);
ManagedObjectReference _recoveryPlan = plans.get(0);
```

The sample C# and Java code below combines `ListPlans` with `RecoveryPlanGetInfo` to retrieve a specified plan. C# sample code for recovery plan

```
ManagedObjectReference[] plans = _service.ListPlans(_sic.recovery);
if (plans != null && plans.Length > 0)
{
for (int i = 0; i < plans.Length; ++i)
{ SrmRecoveryPlanInfo info = _service.RecoveryPlanGetInfo(plans[i]); Console.WriteLine("Recovery-
Plan : " + info.name);
if (info.name.Equals(planName))
{
Console.Write(" RecoveryPlan state : ");
Console.WriteLine(info.state);
}
}
}
```

Java sample code for recovery plan

```
private static void listPlans() throws Exception { List<ManagedObjectReference> plans = srm-
Port.listPlans(serviceContent.getRecovery());
if (plans != null && plans.size() > 0)
{
for (int i = 0; i < plans.size(); ++i)
{ SrmRecoveryPlanInfo info = srmPort.recoveryPlanGetInfo(plans.get(i)); System.out.println("Recov-
eryPlan : " + info.getName()); if (info.getName().equals(planName))
 {
 System.out.print(" RecoveryPlan state : "); System.out.println(info.getState());
 }
}
}
}
```

RecoveryPlanGetPeer

This method retrieves a recovery plan peer, which is the plan at the paired site rather than at the local site.

Synopsis

```
RecoveryPlan.Peer RecoveryPlanGetPeer()
```

`RecoveryPlan.Peer` is the peer recovery plan at the paired site.

- `plan` references to the `SrmRecoveryPlan` managed object.
- `state` is the same enumeration as for `RecoveryPlanGetInfo`. For more information, see RecoveryPlanGetInfo.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for RecoveryPlanGetPeer

```
SrmRecoveryPlanPeer peerPlan = srmPortType.recoveryPlanGetPeer(ManagedObjectReference _this);

 Where ManagedObjectReference _this = _recoveryPlan;
 where _recoveryPlan can be taken from:
SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List<ManagedObjectReference> plans = srmPortType.listPlans(
        _recoveryRef);
ManagedObjectReference _recoveryPlan = plans.get(0);
```

Start

This method starts or reconfigures the given recovery plan, or tests and cleans it up, depending on the mode specified. This operation requires one of these privileges depending on recovery mode, `VcDr.RecoveryProfile.com.vmware.vcDr.Failover` for a real recovery and `VcDr.RecoveryProfile.com.vmware.vcDr.Run` for a test recovery. You must use the UI, not the API, to initiate forced failover. It requires complicated set-up and validation steps.

NOTE
This method is deprecated. You should not rely on it in production code, as it is not guaranteed to provide valid information in future releases. Instead, you should use StartEx.

Synopsis

```
void start(RecoveryPlan.RecoveryMode mode, @version5 @optional RecoveryOptions options)
```

- `mode` – one of the following recovery modes:
  - `test` – run a test failover to the peer (recovery) site, without halting the local (protected) site.
  - `cleanupTest` – after testing a recovery plan, cleans up all effects of the test operation.
  - `failover` – move to the peer (recovery) site. When all groups are moved the recovery plan is complete.
  - `reprotect` – the peer site becomes the protected site, and the local site becomes the recovery site.
  - `revert` - revert a recovery, abandoning all the VMs on the peer site and powering on the original VMs on the local site. This operation is not allowed unless all the replication groups are in the shadowing, recovered, or partially recovered state. If the sites are not connected, the peer VMs may be left running. In order to correct this situation, you might have to re-run `revert` after the sites are connected.
  - `migrate` - Migrate the recovery plan to the peer site. Once completed successfully, the plan should be deleted or reprotected. For a successful migration to occur, all the groups in the plan must be in the shadowing or recovered states.
- `RecoveryOptions` data object has the following properties:
  - `syncData`: It is a boolean parameter that indicates whether to replicate the recent changes to the recovery site. This option is valid only for the `test` operation. If not specified, the default value of true is used.
  - `ignoreErrors`: It is a boolean parameter that indicates whether or not to ignore errors during recovery operations such as `cleanupTest` and `reprotect` . If not specified, the default value of true is used.

Faults

- IvalidArgument, if the recovery mode is not valid.
- InvalidState, if the recovery plan is not in the ready state.
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for Start

```
srmPortType.start(
        ManagedObjectReference _this,
        SrmRecoveryPlanRecoveryMode mode,
        SrmRecoveryOptions options);

 Where ManagedObjectReference _this = _recoveryPlan;
 where _recoveryPlan can be taken from:
SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List<ManagedObjectReference> plans = srmPortType.listPlans(
        _recoveryRef);
ManagedObjectReference _recoveryPlan = plans.get(0);
```

StartEx

This method starts or reconfigures the given recovery plan, or tests and cleans it up, depending on the mode specified.

This operation requires one of these privileges depending on your recovery mode:

- `VcDr.RecoveryProfile.com.vmware.vcDr.Failover` for a real recovery
- `VcDr.RecoveryProfile.com.vmware.vcDr.Run` for a test recovery

> **NOTE**
> You must use the UI, not the API, to initiate a forced failover. It requires complicated set-up and validation steps.

Synopsis

```
@task void startEx(RecoveryMode mode, @optional RecoveryOptions options)
```

- `mode` – one of the following recovery modes:
  - `test` – run a test failover to the peer (recovery) site, without halting the local (protected) site.
  - `cleanupTest` – after testing a recovery plan, cleans up all effects of the test operation.
  - `failover` – move to the peer (recovery) site. When all groups are moved the recovery plan is complete.
  - `reprotect` – the peer site becomes the protected site, and the local site becomes the recovery site.
  - `revert` - revert a recovery, abandoning all the VMs on the peer site and powering on the original VMs on the local site. This operation is not allowed unless all the replication groups are in the shadowing, recovered, or partially recovered state. If the sites are not connected, the peer VMs may be left running. In order to correct this situation, you might have to re-run `revert` after the sites are connected.
  - `migrate` - Migrate the recovery plan to the peer site. Once completed successfully, the plan should be deleted or reprotected. For a successful migration to occur, all the groups in the plan must be in the shadowing or recovered states.
- `RecoveryOptions` data object has the following properties:
  - `syncData`: It is a boolean parameter that indicates whether to replicate the recent changes to the recovery site. This option is valid only for the `test` operation. If not specified, the default value of true is used.
  - `ignoreErrors`: It is a boolean parameter that indicates whether or not to ignore errors during recovery operations such as `cleanupTest` and `reprotect` . If not specified, the default value of true is used.

Faults

- IvalidArgument, if the recovery mode is not valid.
- InvalidState, if the recovery plan is not in the ready state.
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Cancel

This method cancels this recovery plan. It can take some time to cancel a recovery plan depending on its state. This operation requires one of these privileges depending on recovery mode, `VcDr.RecoveryProfile.com.vmware.vcDr.Failover` for a real recovery and `VcDr.RecoveryProfile.com.vmware.vcDr.Run` for a test recovery.

Synopsis

```
void cancel()
```

Faults

- InvalidState, if the recovery plan cannot be canceled.
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for Cancel

```
srmPortType.cancel(ManagedObjectReference _this);

Where ManagedObjectReference _this = _recoveryPlan;
where _recoveryPlan can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List < ManagedObjectReference > plans = srmPortType.listPlans(
  _recoveryRef);
ManagedObjectReference _recoveryPlan = plans.get(0);
```

ListPrompts

This method lists the current prompts that are waiting on user input. Prompts appear in the order in which virtual machines are scheduled to power on.

When a prompt step is reached, the recovery plan remains in a waiting state until the user answers the prompt or a program calls AnswerPrompt.

Synopsis

```
RecoveryPlan.RecoveryPrompt[] listPrompts()
```

`RecoveryPrompt[]` is an array of data objects containing the prompt and the key for responding to it. It has the following fields:

- `key` - Key for responding to the prompt
- `data` - Data about the prompt

Faults

- InvalidState, if the recovery plan is not running.
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for ListPrompts

```
List < SrmRecoveryPlanRecoveryPrompt > listPrompts = srmPortType.listPrompts(ManagedObjectReference
 _this);

Where ManagedObjectReference _this = _recoveryPlan;
where _recoveryPlan can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List < ManagedObjectReference > plans = srmPortType.listPlans(
  _recoveryRef);
ManagedObjectReference _recoveryPlan = plans.get(0);
```

AnswerPrompt

This method answers the current prompt being displayed in a recovery plan. The operation requires one of these privileges depending on recovery mode, `VcDr.RecoveryProfile.com.vmware.vcDr.Failover` for a real recovery and `VcDr.RecoveryProfile.com.vmware.vcDr.Run` for a test recovery.

Synopsis

```
void answerPrompt(String key, boolean cancelVmRecovery, @optional String response)
```

`key` is a string with the key value from the recovery prompt.

`cancelVmRecovery` is true if you want to halt further processing on this virtual machine, false otherwise.

`response` is a response to the prompt that will be recorded.

Faults

- InvalidState, if the recovery plan is not running.
- PromptNotFound, if no prompt with that key exists.
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for AnswerPrompt

```
srmPortType.answerPrompt(
  ManagedObjectReference _this,
  String key,
  boolean cancelVmRecovery,
  String response);

Where ManagedObjectReference _this = _recoveryPlan;
where _recoveryPlan can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List < ManagedObjectReference > plans = srmPortType.listPlans(
  _recoveryRef);
ManagedObjectReference _recoveryPlan = plans.get(0);
```

RecoveryPlanGetParentFolder

Gets the parent folder (or root) for a recovery plan.

Synopsis

```
RecoveryPlanFolder RecoveryPlanGetParentFolder()
```

`RecoveryPlanFolder` is a Site Recovery Manager folder that can hold Recovery Plans and Recovery Plan Folders. For more information, see Recovery Plan Folder.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetRecoverySettings

Gets the recovery settings for the specified virtual machine.

Synopsis

```
RecoverySettings GetRecoverySettings (VirtualMachine vm)
```

`vm` is the Virtual Machine whose Recovery Settings are to be retrieved.

`RecoverySettings` – the VM recovery settings for presentation in the user interface, including:

- `changeVersion` – change version control. When reconfiguring an existing Protected workload this value must be set and must match the most recent value. For settings on newly added VMs, leave this unset.
- `status` – recovery status. This enumerates the following values:
  - `ok` - There are no recovery setting conditions to alert to the user.
  - `syncConflict` - Synchronization error. The settings are in a sync conflict with the remote site. Use the SRM user interface to clear the conflict.
- `recoveryPriority` – the recovery priority for this VM. This enumerates the following values:
  - highest
  - higher
  - normal
  - lower
  - lowest
- `skipGuestShutdown` – configure the shutdown behavior for this workload during real failover not to attempt a guest shutdown, even if VMware Tools are enabled.
- `powerOffTimeoutSeconds` – configure the timeout for guest shutdown operations for this VM.
- `finalPowerState` – final power state for this VM after recovery.
- `localFaultToleranceState` – configure FT override setting for this VM when it will be failed back.
- `remoteFaultToleranceState` – configure an FT override setting for this VM after recovery.
- `powerOnTimeoutSeconds` – configure the timeout for VMware Tools to respond with a heartbeat.
- `powerOnDelaySeconds` – configure the fixed time delay after power-on operations for this workload.
- `Callout[] prePowerOnCallouts` – before power-on Callouts (commands or prompts).
- `Callout[] postPowerOnCallouts` – after power-on Callouts.
- `Callout` - Base class for all Callouts (Commands or Prompts). It has the following fields:
  - `description` - Name/description of the Callout, for display purposes in UI. A short description or name of the Callout for display purposes in the UI.
  - `uuid` - UUID of the Callout, used by the UI for editing. This string should follow the definition of the string representation of a UUID as per RFC 4122. An example of a UUID is "08e3c162-9213-ff31-681b-ff6e35f2ac1b".
- `Prompt` - Specifies a Callout which pauses the execution of the recovery script and display a message until the user presses continue. It contains the `promptText` field. `promptText` is the text to display while running a recovery. This text will be displayed in the SRM UI and be placed in the SNMP Trap. `promptText` is a non-empty string. The maximum valid length is 4096 characters.
- `Command` - This class specifies a Command which runs during a Recovery, either on the server or on the recovered VM. If the command returns a non-zero value, then recovery indicates that an error has occurred. This Command can

be inserted before or after a particular VM is powered on. If inserted after a particular VM is powered on, the Command may be run either on the SRM server machine or inside the recovered VM that was just powered on.
This class has the following fields:

- `command` - Command to run while running a recovery. Non-empty string. The maximum valid length is 4096 characters.
- `long timeout` - Time in seconds to wait until the command is completed. If the command has not completed when the timeout occurs, the child process will be killed.
- `boolean runInRecoveredVm` - Should command be run on SRM server machine or in recovered VM? This only applies to Per-VM Callout Commands set to run post-power-on of a recovered VM. Those Commands may be run either on the SRM machine, or inside the recovered VM.

- `VmIpCustomization` - Contains all data, needed to perform IP customization for a virtual machine, when recovering it to a given SRM site.
- `dependentVmIds` - Dependent VMs. This is a list of VM identities that must be powered on before this VM can be powered on. Dependencies are only valid within VMs of the same recovery priority. If there are dependent VMs that are not in the current plan and same recovery priority, they will be ignored. VM identity is available through `ProtectionGroup#ProtectedVm#drVmIdentity`.

`VmIpCustomization` contains the following data required for performing IP customization for a virtual machine, when recovering it to a given SRM site:

- `IpAddressInfo` - IP address definitions.
- `IpV4AddressInfo` - IPv4 address definitions.
- `IpV6AddressInfo` - Ipv6 address definitions.
- `IpV4AddressSpec` - IPv4 address specification. Contains either static or DHCP configuration.
- `@optional IpV4AddressInfo staticAddressInfo` - If this optional field is set, then this spec denotes a static IPv4 address configuration. Otherwise, an unset field denotes a DHCPv4 configuration.
- `IpV6AddressSpec` - IPv6 address specification. Contains either static or DHCP configuration.
- `@optional IpV6AddressInfo staticAddressInfo` - If this optional field is set, then this spec denotes a static IPv6 address configuration. Otherwise, an unset field denotes a DHCPv6 configuration.
- `enum NetBiosMode` - Used to configure NetBIOS on Windows systems. The values correspond directly to Microsoft constants for NetBIOS mode.
- `NicCustomizationSpec` - Contains IP customization info for a specific network adapter.
- `WindowsNicCustomizationSpec` - Contains Windows specific IP customization info for a specific network adapter for a virtual machine.
- `@optional String dependentVmIds` - This is a list of VM identities that must be powered-on before this VM can be powered on. Dependencies are only valid within VMs of the same recovery priority. If there are dependent VMs that are not in the current plan and same recovery priority, they will be ignored. VM identity is available through `ProtectionGroup#ProtectedVm#drVmIdentity`.

Faults

- RecoveryPlanNotFound
- RuntimeFault
- VmNotFoundInRecoveryPlan

See Faults in Site Recovery Manager API for more details.

SetRecoverySettings

Updates the virtual machines' Recovery Settings. This method updates the specified virtual machine's Recovery Settings with values contained in the supplied `RecoverySettings` object. This class modifies the recovery

settings available through the external API. The `VmIpCustomization` data object allows user to configure the IP address and corresponding DNS, WINS of the virtual machine, after the migration is complete. You can disable IP customization by setting `VmIpCustomization` to `nullptr` or by not setting `IpCustomizationSpecMapping` within `VmIpCustomization`.

Synopsis

```
void setRecoverySettings(vim.VirtualMachine vm, RecoverySettings settings)
```

`vm` is the Virtual Machine which Recovery Settings are to be updated.

`settings` is the Recovery Settings to update the VM.

`RecoverySettings` is the VM recovery settings for presentation in the user interface. For more information, see GetRecoverySettings.

Faults

- DependencyConflict
- InvalidArgument
- RecoveryPlanLocked
- RecoveryPlanNotFound
- RuntimeFault
- VersionConflict
- VmNotFoundInRecoveryPlan

See Faults in Site Recovery Manager API for more details.

AddProtectionGroup

Adds a protection group to the recovery plan.

Synopsis

```
void addProtectionGroup(ProtectionGroup group)
```

`group` is the `ProtectionGroup` to be added. For information, see Protection Group.

Faults

- InvalidArgument
- NoPermission
- ProtectionGroupNotFound
- RecoveryPlanLocked
- RuntimeFault
- VersionConflict

See Faults in Site Recovery Manager API for more details.

AddTestNetworkMappingToRecoveryPlan

The `AddTestNetworkMappingToRecoveryPlan` method adds or updates a test network mapping to a recovery plan.

Synopsis

```
void AddTestNetworkMappingToRecoveryPlan(
  vim.Network secondaryNetwork,
  vim.Network testNetwork)
```

`secondaryNetwork` specifies the network on the remote recovery site.

`testNetwork` specifies the test network on the remote recovery site.

Faults

- CannotMapDvsUplinkPortgroup
- ConnectionDownFault
- ManagedObjectNotFound
- NoPermission
- RemoteSiteNotAuthenticated
- RemoteSiteNotEnabled
- RecoveryPlanLocked
- RuntimeFault
- VersionConflict

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

RemoveTestNetworkMappingFromRecoveryPlan

The `RemoveTestNetworkMappingFromRecoveryPlan` method removes a test network mapping from a recovery plan.

Synopsis

```
void RemoveTestNetworkMappingFromRecoveryPlan(vim.Network secondaryNetwork)
```

The `secondaryNetwork` parameter specifies the secondary site network whose mapping must be removed.

Faults

- ConnectionDownFault
- NetworkNotFound
- NoPermission
- RecoveryPlanLocked
- RemoteSiteNotAuthenticated
- RuntimeFault
- VersionConflict

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

RemoveProtectionGroupFromRecoveryPlan

The `RemoveProtectionGroupFromRecoveryPlan` method removes a protection group from a recovery plan.

Synopsis

```
void RemoveProtectionGroupFromRecoveryPlan(ProtectionGroup group)
```

The `group` parameter specifies the protection group that must be removed.

Faults

- NoPermission
- ProtectionGroupNotFound
- RecoveryPlanLocked
- RuntimeFault
- VersionConflict

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

RecoveryPlanGetLocation

The `RecoveryPlanGetLocation` method checks whether the recovery plan is hosted locally or on the paired site.

Synopsis

```
String RecoveryPlanGetLocation()
```

The method returns the localToRecoverySite, notLocalToRecoverySite, unknownLocationNoPgs, and unknownLocation Strings.

Returned Value	Description
localToRecoverySite	The recovery plan instance exists locally on the recovery site.
notLocalToRecoverySite	The recovery plan instance is a peer of the recovery site instance.
unknownLocationNoPgs	The recovery plan instance has no protection groups. A plan with no protection groups is not local to either site.
unknownLocation	The location of the recovery plan instance is not known.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

RecoveryPlanHasRunningTask

The `RecoveryPlanHasRunningTask` method checks whether there is a task that is associated with the recovery plan.

Synopsis

```
boolean RecoveryPlanHasRunningTask()
```

The method returns true if there is a task that is associated with the recovery plan.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Recovery History

This section covers the interfaces to recovery history.

GetRecoveryResult

Retrieves recovery results for a given run of this recovery plan. Use this method to get the key so subsequent methods can get recovery results history.

Synopsis

```
RecoveryResult[] getRecoveryResult(int length)
```

`length` is the maximum number of results to retrieve.

`RecoveryResult[]` is an array of recovery results for this recovery plan or its peer plan, including:

- `description` – summary of the plan at the time of this run
- `errorCount` – count of error-level faults that were generated by the operation
- `executionTimeInSeconds`– total execution time in seconds
- `key` – unique key for this recovery result, useful for subsequent methods

  NOTE
  Staring with Site Recovery Manager 8.8, `key` is deprecated and is replaced by `runKey`.
- `runKey` – unique key for this recovery result, useful for subsequent methods
- `name` – the recovery plan's name at the time of this run
- `plan` – recovery plan that this result covers
- `resultState` – the result state, which is only the final state indicating completion or failure. This enumerates the following values:
  - `success` - The operation completed with no warnings.
  - `warnings` - The operation completed with one or more warnings.
  - `errors` - The operation failed to complete due to one or more errors.
  - `cancelled` - The operation was cancelled.
- `runMode` – mode of recovery when plan was initiated. This enumerates the following:
  - `failover` - Failover the recovery plan to the peer site. You can failover multiple times in case problems occured on previous runs. Once completed successfully, the plan should be deleted or reprotected. For a plan to be successfully failed over, all of the groups in the plan must be in the shadowing, recovered, or partiallyRecovered states.
  - `test` - Run a test-failover at this site, leaving the primary state unaffected. For a plan to be successfully tested, all of the protection groups must be in the shadowing state.
  - `cleanupTest` - Cleanup after a test run.
  - `reprotect` - Complete an already finished recovery, and start protecting the groups so they may be recovered on the peer site. This will unregister the VMs on the peer site, configuring the storage, and the shadow VMs. This operation may only be performed when the sites are connected, and at least one protection group is in the recovered or partially Recovered state.
  - `revert` - Revert a recovery, abandoning all the VMs on the peer site and powering on the original VMs on the local site. This operation is not allowed unless all the replication groups are in the shadowing, recovered, or partially recovered state. If the sites are not connected, the peer VMs may be left running. In order to correct this situation, re-run `revert` after the sites are connected.

    NOTE
    `revert` is not supported currently.
  - `migrate` - Migrate the recovery plan to the peer site. Once completed successfully, the plan should be deleted or reprotected. For a successful migration to occur all of the groups in the plan must be in the shadowing or recovered states.
- `startTime`, `stopTime` – time when the recovery was started and when it completed or stopped
- `totalPausedTimeInSeconds` – total time the recovery plan was paused
- `warningCount` – count of warning-level faults that were generated by the operation

- `poweredOnVms` - The count of the VM's that are powered on
- `errorStateVms` - The count of the VM's that are in Error state
- `successfullyRecoveredVms` - The count of the VM's that are successfully recovered
- `ipCustomizedVms` - The count of the VM's that are successfully ip customized
- `errorCustomizedVms` - The count of the VM's that encountered an error during IP customization.
- `poweredOffVms` - The count of the VM's that are powered off
- `warnings` - The warnings encountered for this Recovery Plan
- `errors` - The errors encountered for this Recovery Plan

Faults

- InvalidArgument
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Example for GetRecoveryResult

```
List < SrmRecoveryResult > recoveryResult = srmPortType.getRecoveryResult(
  ManagedObjectReference _this,
  int length);

Where ManagedObjectReference _this = _historyRef;
where _historyRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List < ManagedObjectReference > plans = srmPortType.listPlans(
  _recoveryRef);
ManagedObjectReference _historyRef = srmPortType.getHistory(
  _recoveryRef,
  plans.get(0));
```

GetResultCount

Retrieves the total number of stored results. This include historical results from both the plan and its peer plan if the sites are connected.

Synopsis

```
int getResultCount()
```

Returns an integer count with the total number of history entries for this plan, and potentially its peer.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for GetResultCount

```
int resultCount = srmPortType.getResultCount(
  ManagedObjectReference _this);

Where ManagedObjectReference _this = _historyRef;
```

```
where _historyRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List < ManagedObjectReference > plans = srmPortType.listPlans(
  _recoveryRef);
ManagedObjectReference _historyRef = srmPortType.getHistory(
  _recoveryRef,
  plans.get(0));
```

GetResultLength

Retrieves the length of the XML result document for the requested Recovery Result.

Synopsis

```
int getResultLength(long key)
```

`key` is the unique key for the plan history, from return value of the `GetRecoveryResult` method.

Returns an integer specifying the number of lines in the XML result file.

Faults

- RecoveryResultNotFound, if no result with that key exists.
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for GetResultLength

```
int length = srmPortType.getResultLength(
  ManagedObjectReference _this,
  long key);

Where ManagedObjectReference _this = _historyRef;
where _historyRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List < ManagedObjectReference > plans = srmPortType.listPlans(
  _recoveryRef);
ManagedObjectReference _historyRef = srmPortType.getHistory(
  _recoveryRef,
  plans.get(0));
```

RetrieveStatus

Retrieves an XML representation of the specified historical run of the referenced recovery plan. This XML document is transmitted in chunks limited by the maximum length of a string in the transport layer. You specify what line to start at and how many lines to return.

Synopsis

```
String[] retrieveStatus(long key, int offset, int maxLines)
```

`key` is the unique key for the plan history, returned in RecoveryResult.runKey from getGetRecoveryResult.

`offset` is an integer specifying the starting line number in the XML file, beginning at 0,

`maxLines` is an integer specifying the maximum number of lines to retrieve.

Returns a string containing an XML representation of all recovery steps and their results.

Only after you have retrieved all the lines and assembled them do you have a valid XML document.

Faults

- RecoveryResultNotFound, if no result with that key exists.
- RuntimeFault
- vmomi.fault.InvalidArgument

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Example for RetrieveStatus

```
List < String > status = srmPortType.retrieveStatus(
  ManagedObjectReference _this,
  long key,
  int offset,
  int maxLines);

Where ManagedObjectReference _this = _historyRef;
where _historyRef can be taken from:
  SrmServiceInstanceContent content = _srmPortType.retrieveContent(_svcRef);
ManagedObjectReference _recoveryRef = content.getRecovery();
List < ManagedObjectReference > plans = srmPortType.listPlans(
  _recoveryRef);
ManagedObjectReference _historyRef = srmPortType.getHistory(
  _recoveryRef,
  plans.get(0));
```

IP Subnet Mapper

The IpSubnetMapper component resides on the recovery site and manages the IP subnet mapping between Protection and Recovery site networks.

GetIpSubnetMappings

This method returns an array of the IP subnet mappings for this IP Subnet Mapper.

Synopsis

```
IPSubnetMapping[] getIpSubnetMappings();
```

`IPSubnetMapping` represents an association between a mapped network on the primary site with an IPMapping describing IP parameter translation during IP Subnet based customization. It has the following fields:

Field	Description
`primaryObject`	Network on the primary (protected) site
`secondaryObject`	Network on the secondary (recovery) site

Field	Description
`IPMapping ipMapping`	IPMapping to apply to the destination network during IP customization

IPMapping defines the rule(s) used to translate VM's IP settings between protection and recovery sites. IPMapping can be associated with a protected site's `vim.Network` mapped to a recovery site's `vim.Network` with `InventoryMapping.addNetworkMapping` method. This allows IP settings for the recovered VMs be deduced based on the IP subnet parameters without a need to configure IP settings for each protected VM individually. It has the following fields:

Field	Description
`name`	Name of the IP mapping.
`@optional SubnetRule[] rules`	A set of network rules to evaluate/apply during recovery. The rules are evaluated in the order they are specified. SRM applies the first matched rule.

`SubnetRule` describes the mapping between protection site IP parameters to recovery site ones for a single IP subnet. It has the following fields:

Field	Description
`name`	Name of the Rule.
`recoverySiteSubnet`	CIDR specifying the recovery site subnet.
`protectedSiteSubnet`	CIDR specifying the protected site subnet.
`@optional IPSettings recoverySiteIPSettings`	IP settings to be applied for all matched network adapters on the recovery site when executing Test and Failover workflows.
`dnsSuffixes[]`	DNS Suffixes to be applied to all matched network adapters.

IPSettings is the IP customization info for a specific network adapter. It has the following fields:

Field	Description
`ipV4Gateways`	List of IPv4 gateways in the order of preference.
`ipV6Gateways`	List of IPv6 gateways in the order of preference.
`dnsServerList`	List of server IP addresses to use for DNS lookup.

In Windows, these settings are adapter-specific. In Linux they are used to build a global list of DNS servers for all adapters. Specify these servers in order of preference. If set in case of DHCP, the explicit DNS server list overrides the default DNS configuration acquired through DHCP protocol.

WindowsIPSettings is an extension for IPSettings. It is used for setting Windows specific IP customization information for a specific network adapter.

Field	Description
`domainName`	A connection-specific DNS domain name.
`wins`	The IP addresses of the primary and secondary WINS servers. The first element in this array is always the address of the primary WINS server and if a second element exists, it is the address of the secondary WINS server.
`netBios`	NetBIOS setting. Possible values are the constants defined by NetBiosMode enum.

`NetBiosMode` is used for configuring NetBIOS on Windows systems. The values correspond directly to Microsoft constants for NetBIOS mode. It enumerates the following:

Value	Description
`enableNetBiosViaDhcp`	Enables the DHCP server to decide whether or not to use NetBIOS.
`enableNetBios`	Explicitly enables NetBIOS.
`disableNetBios`	Explicitly disables NetBIOS.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

AddIpMapping

This method associates an `IPMapping` object with an inventory-mapped protected site network. This must be called on secondary (recovery) site. The protectedNetwork should be mapped to recoveryNetwork by #InventoryMapper.addNetworkMappings() for the IPMapping to be applied to VMs connected to recoveryNetwork during IP customization. If an IPMapping had been already associated with the protectedNetwork, then it gets replaced by the new IPMapping. Up to 1 IPMapping containing multiple SubnetRule rules can be associated with any given protected site network at any time. If the destination (recovery) network is associated with a Test Network on the recovery site, then the ipMapping will be applied to the test network as well. This method requires Resource.com.vmware.vcDr.RecoveryUse privilege on destinationNetwork.

Synopsis

```
void addIpMapping(vim.Network protectedNetwork, vim.Network recoveryNetwork, IPMapping ipMapping)
```

`addIpMapping` has the following parameters:

Parameter	Description
`protectedNetwork`	Primary site network
`recoveryNetwork`	Secondary site network
`ipMapping`	IPMapping to associate with the existing Network Mapping. For more information, see GetIpSubnetMappings.

Faults

- ConnectionDownFault
- IpMappingFault
- InvalidArgument
- MissingNetworkMapping
- RemoteSiteNotAuthenticated
- RemoteSiteNotEnabled
- RuntimeFault
- StringArgumentTooLong
- UnknownPrimaryNetwork
- UnknownSecondaryNetwork

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

RemoveIpMappings

This method removes IPMappings from mapped primary (protected) site networks. Must be called on secondary (recovery) site.

Synopsis

```
void removeIpMappings(@optional vim.Network[] protectedNetworks);
```

`protectedNetworks` primary (protected) site networks whose IPMapping is to be removed .

Faults

- RemoteSiteNotEnabled
- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Storage Adapter

This section describes the methods for getting information about a storage adapter.

FetchInfo

This method fetches basic information about the SRA.

Synopsis

```
@optional Info fetchInfo();
```

`Info` class has the following fields:

Field	Description
`uuid`	Universally unique identifier of the SRA which is preserved on SRA upgrades.
`installPath`	Path to the folder containing SRA installation.
`name`	Name of the adapter.

Field	Description
version	Version of the adapter.
vendor	Storage Vendor who owns the adapter.
helpUrl	URL for online documentation for the adapter.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetAdapterConnectionSpec

A partially complete connection spec that will have its address and opaque keys, for the key value pairs, pre-entered. Refer your SRA vendor specific documentation about what each key represents.

Synopsis

```
AdapterConnectionSpec[] getAdapterConnectionSpec();
```

This method returns array of AdapterConnectionSpec objects for the available SRAs. Part of the data is pre-entered, as shown in the example below:

Example of returned partially-complete spec

```
connectionSpec.name.key = "primary"
connectionSpec.name.name = "Primary SAN"
connectionSpec.name.hint = "Primary SAN connection parameters"
connectionSpec.adress[0].key = "spA"
connectionSpec.adress[0].name = "IP Address of SP-A"
connectionSpec.adress[0].hint = "Enter IP address of the Storage Processor A"
connectionSpec.adress[0].value = empty (expected user input)
connectionSpec.opaque[0].key = "volumeNameFilter"
connectionSpec.opaque[0].name = "Volume name prefix limiting discovery"
connectionSpec.opaque[0].hint = "Leave empty for full discovery"
connectionSpec.opaque[0].optional = "true"
connectionSpec.adress[0].value = empty (expected user input)
```

AdapterConnectionSpec has the following fields:

Field	Description
DataPrompt key	Identifier of a SRA-defined group of connection parameters. Refer your SRA vendor specific documentation for more information about this value. This will be automatically entered by the StorageAdapter#getAdapterConnectionSpec.
@optional DataPrompt[] address	List of address-type parameters. Refer your SRA vendor specific documentation about the keys and their corresponding values. Keys will be automatically entered by the StorageAdapter#getAdapterConnectionSpec.
username	Username.
password	Password if required.

Field	Description
`@optional OpaquePrompt[] opaque`	Opaque parameters if required. Refer your SRA vendor specific documentation about the keys and their corresponding values. Keys will be automatically entered by the `StorageAdapter#getAdapterConnectionSpec`.

`DataPrompt` contains key-value pairs with additional information about the key and what value it expects. It has the following fields:

Field	Description
`key`	SRA Specific key, this can be either for the address or the opaque.
`@optional LocalizableString name`	Prompt string.
`LocalizableString hint`	Sample or more verbose description of the requested data for
`value`	Value corresponding to the key.

`LocalizableString` describes localizable string returned from the SRA. Localization support is optional for SRA. If supported, then each string is returned with a key which could be used to lookup a translation in non-default locale.

Example of localizable string returned from SRA: `<Xxx stringId="Foo">Foo</Xxx>`

Example of non-localizable string returned from `SRA: <Xxx>Foo</Xxx>`

`LocalizableString` has the following fields:

Field	Description
`key`	Key to look up translation for the string. This key is made optional to accommodate SRAs which do not support localization. These SRAs will just return strings in default locale (English).
`text`	String text in default locale

`OpaquePrompt` extends `DataPrompt`. It contains additional information about the opaque parameters. It has the following fields:

Field	Description
`optional`	Boolean indicating whether or not this parameter is optional.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Storage

This section shows a method that you can use to rescan storage.

DiscoverDevices

The `discoverDevices` method starts a loop through the array managers on the local and remote sites, and for each array pair call `discoverDevices`. If the user does not have enough privileges, the array managers are skipped.

Synopsis

```
DiscoverDevicesTask discoverDevices()
```

The method returns a `DiscoverDevicesTask` object that contains information about the status of the operation. Site Recovery Manager Server retains the object for 30 minutes after the task finishes.

`IsDiscoverDevicesTaskComplete` returns true if the `DiscoverDeviceTask` is complete.

`GetDiscoverDevicesTaskFailures` returns a list of failures that occurred while performing `DiscoverDevices` on array managers. The entire set of failures can be retrieved when the task is complete. If no failures occurred, the array is empty or null.

`DiscoverDevicesFailure.name` is a string that contains the array pair name.

`DiscoverDevicesFailure.fault` is an MethodFault object that indicates the failure.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

QueryArrayManagers

The `queryArrayManagers` method returns a list of all the available array managers.

Synopsis

```
@optional ArrayManager[] queryArrayManagers()
```

`ArrayManager[]` is an array of available array managers. For more inforamtion, see ArrayManager.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

CreateArrayManager

Creates `ArrayManager` object. Performs array discovery as part of array manager creation and fails if array discovery fails.

Synopsis

```
@task ArrayManager createArrayManager(
   String name,
   String uuid,
   AdapterConnectionSpec[] connectionSpec)
```

`createArrayManager` returns a task instance to monitor the asynchronous operation of this method. `ArrayManager` object is returned as task result. The `createArrayManager` has the following parameters:

Field	Description
`name`	The name of the Array Manager
`uuid`	Universally unique identifier of the SRA
`connectionSpec`	SRA-specific connection parameters for the underlying storage management system. For more information, see GetAdapterConnectionSpec.

NOTE
When getting the `AdapterConnectionSpec` with `getAdapterConnectionSpec` , all the optional opaques will be returned. However, some vendors do not allow not setting the optional opaques. Ensure that they are excluded from the spec.

If a task fails, its error field may contain one of the following:

- `drextapi.fault.DuplicateName` - if an array manager with the same name already exists.
- `drextapi.fault.InvalidAdapterConnectionSpec` - if connectionSpec does not match the internal StorageAdapter connection spec typically, a more specific fault is thrown.
- `drextapi.fault.CommandFailed` - if the command for creating an array manager fails.
- `drextapi.fault.DuplicateArray` - if there is another array manager that already discovered a given array.

Faults

- vim.fault.InvalidArgument
- StorageAdapterNotFound
- StringArgumentTooLong
- RuntimeFault

See Faults in Site Recovery Manager API for more details.

QueryStorageAdapters

List of Storage Replication Adapters (SRAs) information successfully loaded into SRM.

Synopsis

```
@optional StorageAdapter[] queryStorageAdapters();
```

`StorageAdapter` provides information about the Storage Adapter. For more information see Storage Adapter.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

RemoveArrayManager

Deletes `ArrayManager` object. Array managers deletion is deferred until all the tasks currently in progress are complete.

Synopsis

```
@task void removeArrayManager(ArrayManager arrayManager);
```

`removeArrayManager` returns a task instance to monitor the asynchronous operation of this method. `removeArrayManager` has the following parameters:

Field	Description
`arrayManager`	ArrayManager object to delete. For more information, see ArrayManager.

If a task fails, its error field may contain the following:

- `drextapi.fault.ArrayManagerInUse` - if there are array pairs configured for this array manager.

Faults

- RuntimeFault
- TaskInProgress
- vim.fault.InvalidArgument

See Faults in Site Recovery Manager API for more details.

ReloadAdapters

Scans SRA installation directory and reloads SRAs. It returns a task object to monitor the process.

Synopsis

```
@task void reloadAdapters();
```

Faults

- RuntimeFault
- TaskInProgress

See Faults in Site Recovery Manager API for more details.

ArrayManager

This section presents methods to interact with the SRM array managers.

ReadInfo

The `ReadInfo` method returns information specific to the `ArrayManager` instance.

Synopsys

```
ArrayManagerInfo readInfo()
```

Returns `ArrayManagerInfo` which contains information for the ArrayManager instance. It has the `name` field, which is the name of the `ArrayManager`.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

QueryReplicatedArrayPairs

The `queryReplicatedArrayPairs` method returns a list of all the replicated array pairs in the `ArrayManager`.

Synopsis

```
@optional ReplicatedArrayPair[] queryReplicatedArrayPairs()
```

`ReplicatedArrayPair[]` is an array of the replicated array pairs in the `ArrayManager`. For more information, see ReplicatedArrayPair.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetArrayInfo

This method gets the list of discovered storage arrays. This list is populated by `discoverArrays` API.

Synopsis

```
@optional ArrayInfo[] getArrayInfo();
```

`ArrayInfo` class describes the storage array configured for replication. It has the following fields:

Field	Description
`key`	Storage array identifier. The 'key' name is used to allow partial property updates for ArrayManager.arrayInfo[]. This is passed to `ArrayManager#addArrayPair` arrayId.
`name`	User-friendly name of the storage.
`@optional PeerArrayInfo peerArray[]`	Describes a peer array. It has a property named key. This is passed to `addArrayPair peerArrayId.`

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetAdapter

Returns the corresponding storage adapter to the ArrayManager. If the `ArrayManager` does not have a storage adapter then, the unset value is returned.

Synopsis

```
@optional StorageAdapter getAdapter();
```

`StorageAdapter` is a managed object that provides information about the Storage Adapter. For more information, see Storage Adapter.

NOTE
In a scenario where the `ArrayManager` may not have a storage adapter, the `unset` value is returned.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

AddArrayPair

Creates ReplicatedArrayPair object for a given pair of storage arrays.

Synopsis

```
@task ReplicatedArrayPair addArrayPair(String arrayId, String peerArrayId)
```

`addArrayPair` returns task instance to monitor the asynchronous operation of this method. `ReplicatedArrayPair` object is returned as task result. `addArrayPair` has the following parameters:

Field	Description
`arrayId`	Array identifier of the local storage
`peerArrayId`	Identifier of the storage array at the remote site

If a task fails, its error field may contain one of the following:

- `drextapi.fault.ArrayNotFound` - if array with ID arrayId cannot be found at local site, or if array with ID peerArrayId cannot be found at remote site.
- `drextapi.fault.ReplicatedArrayPairAlreadyExists` - if an array pair involving same arrayId and peerArrayId already exists.
- `drextapi.fault.PeerArrayNotFound` - if peerArrayId is not a valid peer of array pointed by arrayId on local site, or if arrayId is not a valid peer of array pointed by peerArrayId on remote site.
- `drextapi.fault.ConnectionDownFault` - if the other site involved in the operation could not be reached.

Faults

- RemoteSiteNotEnabled
- RuntimeFault
- TaskInProgress
- vim.fault.InvalidArgument

See Faults in Site Recovery Manager API for more details.

RemoveArrayPair

Deletes specified ReplicatedArrayPair object. Returns a task instance to monitor the asynchronous operation of this method.

Synopsis

```
@task void removeArrayPair(ReplicatedArrayPair arrayPair)
```

`removeArrayPair` has the following parameters:

Field	Description
`arrayPair`	`ReplicatedArrayPair` to be removed

If a task fails, its error field may contain one of the following:

- `drextapi.fault.ArrayPairInUse` - if array pair is in use by protection group(s).
- `drextapi.fault.ConnectionDownFault` - if the other site involved in the operation could not be reached.

Faults

- RuntimeFault
- TaskInProgress
- vim.fault.InvalidArgument

See Faults in Site Recovery Manager API for more details.

DiscoverArrays

Discovers storage arrays configured for replication by executing SRA command discoverArrays. Ids of discovered array must be unique across all array managers that use the same SRA.

Synopsis

```
@task ArrayInfo[] discoverArrays()
```

`discoverArrays` returns a task instance to monitor the asynchronous operation of this method. Array of `ArrayInfo` objects is returned as task result.

`ArrayInfo` class describes storage array configured for replication. For more information, see GetArrayInfo.

If a task fails, its error field may contain one of the following:

- `drextapi.fault.CommandFailed` - if SRA failed to execute discoverArrays command.
- `drextapi.fault.StorageAdapterNotFound` - if SRA was not found for this array manager.
- `drextapi.fault.DuplicateArray` - if an array, which is already discovered by another array manager with the same SRA, was discovered.
- `drextapi.fault.ArrayPairNotFound` - if arrays are not found for already configured array pair.

Faults

- RuntimeFault
- TaskInProgress

See Faults in Site Recovery Manager API for more details.

Reconfigure

Updates array manager name and connection parameters for the SRA. Performs array discovery as part of reconfigure operation. Ensures that all existing configured array pairs are not affected by the connection specs changes and are still discovered. Array discovery is not performed if only name change is requested and connection specs are unchanged.

Synopsis

```
@task void reconfigure(
   String name,
   @optional AdapterConnectionSpec[] connectionSpec)
```

`reconfigure` returns a task instance to monitor the asynchronous operation of this method. It has the following parameters:

Field	Description
`name`	New name.
`connectionSpec`	New connection parameters.
`AdapterConnectionSpec`	Connection parameters for the SRA provided by the user. For more information, see GetAdapterConnectionSpec.

If a task fails, its error field may contain one of the following:

- `drextapi.fault.ArrayPairNotFound` - if arrays are not found for already configured array pair.
- `drextapi.fault.CommandFailed` - if SRA failed to execute discoverArrays command.
- `drextapi.fault.DuplicateName` - if an array manager with the same name already exists.
- `drextapi.fault.DuplicateArray` - if array, which is already discovered by another array manager with the same SRA, was discovered
- `drextapi.fault.InvalidAdapterConnectionSpec` - if connectionSpec doesn't match the internal StorageAdapter connection spec typically, a more specific fault is thrown.
- `drextapi.fault.StringArgumentTooLong` - if the size of the name parameter is too long.
- `drextapi.fault.StorageAdapterNotFound` - if SRA was not found for this array manager.

Faults

- RuntimeFault
- TaskInProgress

See Faults in Site Recovery Manager API for more details.

GetArrayDiscoveryStatus

Returns the status and timestamp information of latest array discovery. This can be an unset value if no array discovery is still executed.

Synopsis

```
@optional ArrayDiscoveryStatus getArrayDiscoveryStatus()
```

`ArrayDiscoveryStatus` describes the status of the most recent array discovery. Array discovery can be initiated by calling discoverArrays API. Additionally, there is a periodic auto-discovery executed in the background. It has the following the fields:

Field	Description
`fault`	Fault occurred during the most recent array discovery if any.
`startTimestamp`	Start time of the most recent discovery of storage devices.
`completeTimestamp`	Completion time of the most recent discovery of storage devices. This property is not set if discovery task is currently in progress.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

ReplicatedArrayPair

This section presents methods to interact with the replicated array pairs.

QueryReplicatedRdms

The `queryReplicatedRdms` method returns information about all the replicated RDMs in the `ReplicatedArrayPair`.

Synopsis

```
@optional ReplicatedRdmInfo[] queryReplicatedRdms()
```

`ReplicatedRdmInfo[]` is an array and it contains the following information about all the replicated RDMs in the `ReplicatedArrayPair`:

Table 173:

Field	Description
key	Unique key identifying this object. The value is constructed from virtual machine MoID and virtual device key.
device	Storage device identifier.
deviceGroup	Consistency group identifier, if any.
stretchedStorage	Indicates if this is a stretched RDM device.
sitePreference	For stretched RDM devices, indicates whether this device has the site preference or not.
vm	Virtual machine to which the RDM is attached.
deviceKey	Virtual device key of the attached RDM.
lunUuid	UUID of the RDM LUN.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetDevices

Returns list of storage devices configured for replication.

Synopsis

```
@optional StorageDevice[] getDevices()
```

`StorageDevice` is data object that describes storage device configured for replication. It has the following fields:

Field	Description
`groupId`	SRA-specific identifier of a consistency group of the device if any. This property must be set if device is part of a consistency group.
`groupName`	User-friendly name of the consistency group. SRA capabilities determine whether this property is set or not. It is either set for all devices or none. This property is set if StorageDevice#groupId is set and StorageDeviceGroupBase#name is set.
`@optional DeviceProperty[] details`	Describes SRA-specific device property.
`@optional MethodFault queryDetailsFault`	Error occurred while querying SRA for device properties, if any.

`DeviceProperty` describes the SRA-specific device property. It has the following fields:

Field	Description
`LocalizableString name`	User-friendly property name.

`StorageDevice` extends `StorageDeviceGroupBase`, a base class for storage devices and storage groups. It has the following fields:

Field	Description
`id`	SRA-specific identifier.
`name`	User-friendly name. SRA capabilities determine whether this property is set or not. It is either set for all devices or none.
`role`	Role of devices and groups in the replication relationship. See `drextapi.StorageDeviceRole`.
`targetKey`	Key of the promoted replication target if role is promotedTarget. This property is set only for groups and devices with role `drextapi.StorageDeviceRole#promotedTarget`.
`replicationSettings`	Replication settings opaque to SRM.
`@optional MethodFault queryReplicationSettingsFault`	Error occurred while querying SRA for replication settings, if any.

`StorageDeviceGroupBase` extends `StorageItemBase`, a base class for replicated datastores, storage devices and storage groups. It has the following fields:

Field	Description
`stretchedStorage`	Boolean true if stretched storage is enabled.
`staticSitePreference`	Boolean. This property is set for stretched devices, device groups and replicated datastores. True if static site preference is supported.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetDeviceGroups

Returns list of consistency groups of storage devices configured for replication.

Synopsis

```
StorageDeviceGroup[] getDeviceGroups()
```

`StorageDeviceGroup` describes a consistency group of storage devices. The `StorageDeviceGroup` data class extends the `StorageDeviceGroupBase`. It has the following fields:

Field	Description
`devices`	SRA specific identifiers of the storage devices in the group.

`StorageDeviceGroupBase` is a base class for storage devices and storage groups. For information, see GetDevices.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetReplicatedDatastores

Returns list of datastores residing on replicated storage devices. This list is populated by scanning all datastores in local vCenter inventory and matching underlying storage devices to replicated storage devices, discovered by SRM's discoverDevices operation.

Synopsis

```
@optional ReplicatedDatastore[] getReplicatedDatastores();
```

`ReplicatedDatastore` data class describes a datastore residing on replicated storage devices. It extends the `StorageItemBase`. `ReplicatedDatastore` has the following fields:

Field	Description
`key`	Unique key identifying this object.
`datastore`	datastore residing on replicated storage devices.
`StorageDevicePartition[] extent`	List of device partitions corresponding to datastore extents.
`stretchedStorage`	Indicates if this is a stretched datastore.
`staticSitePreference`	For stretched datastore indicates whether this datastore has a static site preference or a dynamic site preference.
`sitePreference`	For a stretched datastore, indicates whether this datastore has the site preference or not. This attribute is relevant for datastore with a static site preference.
`array`	array Reference to the array holding storage devices backing the datastore.

`StorageDevicePartition` describes a partition of a storage device. It has the following fields:

Field	Description
`device`	Storage device identifier.
`deviceGroup`	Consistency group identifier, if any.
`partition`	Partition number.

`StorageItemBase` is the base class for replicated datastores, storage devices, and storage groups. For more information, see GetDevices.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetDeviceDiscoveryStatus

Gets the storage device discovery status. Contains timestamp and faults data for the most recent device discovery.

Synopsis

```
@optional DeviceDiscoveryStatus getDeviceDiscoveryStatus();
```

`DeviceDiscoveryStatus` describes status of the most recent storage device discovery. It has the following fields:

Field	Description
`fault`	Fault occurred during the most recent discovery of storage devices if any.
`peerMatchingFault`	Local to remote peer device and device group matching faults, if any.
`startTimestamp`	Start time of the most recent discovery of storage devices.

Field	Description
completeTimestamp	Completed time of the most recent discovery of storage devices. This property is not set if discovery task is currently in progress.

GetOwner

Returns the local ArrayManager for this pair.

Synopsis

```
ArrayManager getOwner()
```

This method returns the ArrayManager managed object.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Vvol Replication

vVol Replication API provides information about the local vVol topology replicated to the SRM peer site.

GetDomains

Returns a list of local vVol fault domains with their replication groups which target fault domains matching SRM peer site.

Synopsis

```
@optional DomainInfo[] getDomains()
```

`DomainInfo[]` is a list of fault domain information data objects describing the currently available vVol fault domains. It has the following fields:

Field	Description
id	ID of the fault domain.
name	Name of the fault domain.
description	Description of the fault domain. The description is expected to be already localized by the VASA provider and the VC.
vasaProviderUid	Identifier of the vendor of the VASA provider for this fault domain.
vasaProviderVendor	Name of the vendor of the VASA provider for this fault domain.
vasaProviderModel	VASA provider model name for this fault domain.
vasaProviderVersion	VASA provider version string for this fault domain.
@optional ReplicationGroupInfo[] sourceReplicationGroups	Source replication groups in this fault domain. Empty if no replication groups are in SOURCE state.

`ReplicationGroupInfo[]` is the information about a vVol replication group. For more information, see GetVvolGroupDetails.

NOTE
`DomainInfo` and `ReplicationGroupInfo` extends `FaultInfo`. For more information, see GetVvolGroupDetails.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

GetUnprotectedVms

Returns a list of unprotected vVol replicated virtual machines part of vVol replication groups that target the SRM peer site.

Synopsis

```
@optional UnprotectedVmInfo[] getUnprotectedVms(@optional FaultDomainId[] domains);
```

`domains` is an optional list of domains to filter the result. If not set the server will return all protectable VMs.

`UnprotectedVmInfo[]` is a list containing information about unprotected vVol replicated virtual machines part of vVol replication groups that target the SRM peer site. It includes empty Replication Groups that are not part of any SRM protection group and with no virtual machines. It has the following fields:

Field	Description
`ReplicationGroupInfo replicationGroup`	Inforomation about a vVol replication group with SRM peer site as target.
`protectionGroup`	SRM Protection group which protects this replication group. Unset if the replication group is not protected by any SRM protection group.
`VmInfo[] unprotectedVms`	List of vVol replicated virtual machines that are unprotected from SRM point of view and replicated with this replication group. This list might include VMs with vVol configuration errors. Only VMs with no errors are suitable for protection by SRM.

ReplicationGroupInfo is the information about a vVol replication group. For more information, see GetDomains.

`VmInfo` is the information about a local vVol replicated `vim.VirtualMachine`. It has the following fields:

Field	Description
`key`	The `vim.VirtualMachine` object at the local site.
`name`	Name of the virtual machine.
@optional ReplicationGroupInfo[] replicationGroups	Replication groups for this VM. Virtual machines sharing the same replication groups belong to the same consistency group. They will be added or removed from a protection group together. For information about `ReplicationGroupInfo`, see GetDomains.

NOTE
`VmInfo` and `ReplicationGroupInfo` extends `FaultInfo`. For more information, see GetVvolGroupDetails.

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Rescan

Initiates a rescan of the server's local vVol configuration. The server keeps updating its view of the local vVol configuration periodically. This results in the newly provisioned vVol virtual machines being available for protection only after the passage of update interval. This function is called to force an update.

Synopsis

```
Task rescan()
```

`Task` returns an object to the operation. For more information, see SrmExtApiTask

Faults

- RuntimeFault

For information about the faults that Site Recovery Manager throws, see Faults in Site Recovery Manager API.

Placeholder Datastore Manager

This section describes the used method to manage placeholder datastores.

AddDatastore

Adds datastore to the list of placeholder datastores.

Synopsis

```
@task @optional AddDatastoreResult[] addDatastore(@optional vim.Datastore[] datastore);
```

`AddDatastoreResult` structure is returned as task result. It has the following properties:

Field	Description
`key`	The datastore that could not be used as a placeholder datastore.
`fault`	The list of errors for this datastore.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

RemoveDatastore

Removes datastore(s) from the list of placeholder datastores.

Synopsis

```
@task RemoveDatastoreResult removeDatastore(@optional vim.Datastore[] datastore);
```

`RemoveDatastoreResult` structure is returned as task result. It has the following fields:

Field	Description
`notConfigured`	The list of datastores that are not configured as placeholder datastores.

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

GetPlaceholderDatastores

Gets the list of all configured placeholder datastores.

Synopsis

```
@optional PlaceholderDatastoreInfo[] getPlaceholderDatastores()
```

`PlaceholderDatastoreInfo` has the following fields:

Field	Description
`fault`	The list of errors for this datastore. If this property is not empty, this datastore can not be used as a placeholder datastore.

`PlaceholderDatastoreInfo` extends `DatastoreInfo`. It has the following fields:

Field	Description
`key`	reference to the actual vim.Datastore object in VC.
`capacity`	The total capacity of this datastore in bytes.
`freeSpace`	The amount of free space in bytes available on this datastore.
`reservedSpace`	The amount of additional storage space in bytes on this datastore that could potentially be used by all virtual machines on this datastore. A non-zero value in this field is associated with virtual machines having Thin Provisioned disks.
`type`	The type of the file system on this datastore, such as VMFS, NFS or CIFS. @see vim.host.FileSystemVolume#type

Field	Description
`@optional ComputeResourceInfo[] visibleTo`	The list of hosts and clusters that can access this datastore. If a cluster is included in this list, it means that this datastore is accessible to all hosts in this cluster. In most cases this list can not be empty. The only reason for this field to be optional is to be able to return placeholder datastores that have become invalid because there are no clusters or hosts that can see this datastore. This could happen, for example, if the user were to add a host to a cluster and this host could not see some of the datastores that were previously visible to all hosts in the cluster.

`ComputeResourceInfo` has the following properties:

Field	Description
`key`	The reference to the actual `vim.ComputeResource` object in VC. Hosts will be represented by `vim.ComputeResource` with a single `vim.HostSystem` in it. Clusters will be represented by `vim.ClusterComputeResource`.

`DatastoreInfo` and `ComputeResourceInfo` extend `ObjectInfo` which has the following properties:

Field	Description
`name`	The name of the object.
`status`	The status of the object, such as green, red or yellow. @see vim.ManagedEntity.Status

Faults

- RuntimeFault

See Faults in Site Recovery Manager API for more details.

Deprecated APIs

Deprecated Site Recovery Manager APIs

Table 174: Replaced APIs

SrmApi	Replacement API
`ListRecoveryPlans`	`SrmRecovery.ListPlans`
`RecoveryPlanAnswerPrompt`	`SrmRecoveryPlan.AnswerPrompt`
`RecoveryPlanSettings`	`SrmRecoveryPlan.RecoveryPlanGetInfo`
`RecoveryPlanStart, RecoveryPlanCancel`	`SrmRecoveryPlan.Start, SrmRecoveryPlan.Cancel`
`GetFinalStatus`	`SrmRecoveryHistory.GetRecoveryResult`
`GetApiVersion`	no replacement

SrmApi	Replacement API
SrmApi.SrmLogin	SrmServiceInstance.SrmLoginLocale
SrmApi.SrmLoginByToken	SrmServiceInstance.SrmLoginByTokenLocale
SrmApi.SrmLogout	SrmServiceInstane.SrmLogoutLocale
SrmApi.GetApiVersion	ServiceInstanceContent.apiVersion
SrmApi.ListRecoveryPlans	SrmRecovery.ListPlans
SrmApi.RecoveryPlanSettings	SrmRecoveryPlan.RecoveryPlanGetInfo
SrmApi.RecoveryPlanStart	SrmRecoveryPlan.Start
SrmRecoveryPlan.Start	SrmRecoveryPlan.StartEx
SrmApi.RecoveryPlanPause	no replacement
SrmApi.RecoveryPlanResume	no replacement
SrmApi.RecoveryPlanCancel	SrmRecoveryPlan.Cancel
SrmApi.RecoveryPlanAnswerPrompt	SrmRecoveryPlan.AnswerPrompt
SrmApi.GetFinalStatus	SrmRecoveryHistory.GetRecoveryResult
RemoteSite.vcHost, RemoteSite.vcPort	RemoteSite.lkpUrl and RemoteSite.vcInstanceUuid
SrmServiceInstance.getSiteName	SrmServiceInstance.GocalSiteInfo.siteName
SrmProtection.listReplicatedDatastores	SrmProtection.listUnassignedReplicatedDatastores
createHbrProtectionGroup	createHbrProtectionGroup2

Site Recovery Manager Faults

This chapter lists the various faults thrown by the Site Recovery Manager Virtual Appliance Management APIs and the Site Recovery Manager APIs.

Faults in Site Recovery Manager Appliance Management API

This section lists the various faults thrown by the Site Recovery Manager Appliance Management APIs.

Table 175: Faults thrown by Site Recovery Manager Appliance Management functions

Fault	Description
CannotCreateSraLogDirectory	Thrown when the SRA directory cannot be created.
CannotExecuteDockerCommand	Thrown when there are issues executing the 'docker' CLI inside the SRM VA, that is there is no 'docker' command in the '/usr/bin/' directory; there are no permissions to execute the 'docker' command, and so on.
CannotGenerateSystemLogBundle	Thrown when bundle generation fails and we cannot narrow it down to a more precise result.
CertificateBadKeyPair	Thrown when the private key does not match the certificate's public key.
CertificateCaNotAllowed	Thrown when certification authority certificate is provided.
CertificateCtlNotValidForUsage	Thrown when a certificate trust list used to create this chain is not valid for this usage.

Fault	Description
CertificateCtlSignatureNotValid	Thrown when a certificate trust list used to create this chain did not have a valid signature.
CertificateCtlTimeNotValid	Thrown when a certificate trust list used to create this chain was not time-valid.
CertificateCyclicError	Thrown when a cycle in the certificate chain of trust was detected.
CertificateDnsMismatch	Thrown when the certificate's Subject Alternative Name does not meet certain conditions.
CertificateHasExpired	Thrown when the certificate has expired.
CertificateInvalidKeyLength	Thrown when the certificate does not have the minimum required key length.
CertificateMd5NotAllowed	Thrown when certificate signed with MD5 is provided.
CertificateNotTimeNested	Thrown when certificates in the host's certificate chain are not properly time-nested.
CertificateNotTrustedByDrConfig	DrConfig cannot validate SSL certificate.
CertificateNotValidForUsage	Thrown when a certificate in the host's chain is not valid in its proposed usage.
CertificateNotYetValid	Thrown when the certificate is not yet valid.
CertificateParseError	Thrown when certificate can't be parsed due to incorrect format or password.
CertificatePartialChain	Thrown when the host certificate chain is not complete.
CertificateRevocStatusUnknown	Thrown when a certificate in the host's chain has an unknown revocation status.
CertificateRevokedError	Thrown when trust for a certificate in the host's chain has been revoked.
CertificateSha1NotAllowed	Thrown when certificate signed with SHA-1 is not allowed.
CertificateSignatureNotValid	Thrown when a certificate in the host's chain does not have a valid signature.
CertificateTimeNotValid	Thrown when a certificate in the host's chain is not time-valid.
CertificateUnknownError	Thrown when an unknown certificate trust error occurs.
CertificateUntrustedRoot	Thrown when a certificate in the host's chain is based on an untrusted root.
ChangePasswordFault	Thrown when change pass operation fails.
CommandFailed	Thrown when the SRA command execution fails.
CommandResponseMissing	Thrown when a request is made involving a non-existent docker image.
ConnectionError	Thrown during a failed TCP connection when accessing an address using a port number.
ConnectionRefusedFault	Thrown when the connection was refused by the target.
CreateDbSchemaFault	Thrown when there is an error during database schema creation.
DatabaseConnectionFault	Thrown when there's an error while connecting to database.
DnsLookupFault	Thrown when failed to look up the server in DNS

Fault	Description
DockerCommandFailed	Thrown when the 'docker' command execution failed. The contents of the command's 'stderr' can be found in the reason field.
DockerImageDoesNotExist	Thrown when a request is made involving a non-existent docker image.
DrConfigMethodFault	Root type for all DrConfig faults
DrConfigRuntimeFault	Base type for DrConfig faults extending RuntimeFault
DropDbSchemaFault	Thrown when there is an error during db schema drop.
ExcessiveTimeSkewFault	Thrown when the time skew between this machine
FailedToRetrieveUpdateFault	Thrown when check for update fails to retrieve avaivable updates from the repository.
HostUnreachableFault	Thrown when the host could not be contacted.
IncompatibleVcFault	Occurs when attempting to connect to a Virtual Center server with incompatible protocol version.
InstallUpdateFailedFault	Thrown when install update fails.
InternalError	Occurs when the fault is not better described by a more specific DrConfig fault.
InvalidLocale	Thrown when a locale name is invalid or unavailable.
InvalidLogin	Thrown when the login is incomplete due to an incorrect token, user name, or password.
IncompatibleVmomiServer	Thrown when a VMOMI server has an incompatible version.
InvalidCaCertificate	Thrown when provided certificate cannot be decoded from PEM format or when it is not CA certificate.
InvalidCertificate	Thrown when certificate is not suitable. For example when it is expired, not yet valid, contains a weak key etc.
InvalidNetworkConfiguration	Thrown when network configuration provided by client is not valid. For example when static IP address is configured but DNS is dynamic.
NoPermission	Thrown when an operation is denied because of a privilege not held on a managed object.
NotAuthenticated	Thrown when an operation is denied because the session has not yet successfully logged in.
NotAuthorized	Failed to authorize account.
OutOfBounds	Thrown if a parameter exceeds the acceptable range of values.
PrivateKeyNotFound	Thrown when certificate does not match the generated private key.
ReadDbStatusFault	Thrown when there is an error during db status read.
RecreateDbSchemaFault	Thrown when there is an error during db
ServiceBusy	Thrown if another configuration task is already running.
ServiceIdle	Thrown when cancel is called and thereis no running task.
ServiceNotFound	Thrown when an attempt is made to retrieve service information for a non-existent service.

Fault	Description
SraOperationsDisabled	Thrown when SRA operation are disabled through the configuration. Used in VMC case.
SraUuidMismatch	Thrown when an operation involves two SRA images which have different vendor UUIDs. Some operations only make sense between SRA images which represent different version of the same SRA. For example, copying the SRA configuration. By the SRA spec, such images must have the same vendor UUID.
SrmAlreadyRunning	Thrown when configure is called on an already running SRM server.
SrmNotConfigured	Thrown when the operation's prerequisite of a configured SRM is not met.
SsoTokenNotAcquired	Thrown when SSO token could not be acquired.
SystemLogBundleNotFound	Thrown when an attempt is made to access a system log bundle that does not exist
UpdateNotAvailableFault	Thrown when install operation is invoked without avaivable update.
UpgradeDbFault	Thrown when there is an error during db schema upgrade.

Faults in Site Recovery Manager API

This section lists the various faults thrown by the Site Recovery Manager APIs.

Table 176: Faults thrown by Site Recovery Manager functions

Fault	Description
AgentVmNotSupported	Thrown when an agent VM is used in an operation that does not support it.
AlreadyExists	The name, key, or identifier of the element already exists in the collection.
AlreadyLoggedInFault	The session is already logged in, and Login was called again.
AlreadyPairedFault	Thrown if an attempt to pair already paired SRM was made.
ArrayManagerInUse	Thrown when removing an array manager in use.
ArrayNotFound	Thrown when storage array with the specified ID cannot be found.
ArrayPairInUse	Thrown when removing an array pair in use.
ArrayPairNotFound	Thrown when existing array pair is not found in discoverArrays response.
CannotMapDvsUplinkPortgroup	Invalid DVPortgroup network specified for the mapping). Use this fault when site context is obvious from used mapping type(test mappings) or the operation itself.
CannotProtectDatastore	Base fault for failure to add a datastore to protection group. To fix remove the datastore from the protection group.
CannotUnprotectDatastoreInUse	Cannot remove a datastore from protection group because it is used by protected VM(s).

Fault	Description
CannotProtectFTSecondaryVm	Fault thrown when a user tries to protect a VM which is a fault tolerance secondary VM.
CannotProtectVm	Cannot add virtual machine to the protection group.
CertificateCtlSignatureNotValid	Thrown when a certificate trust list used to create this chain did not have a valid signature.
CommandFailed	Failed to execute SRA command.
ConfigFileNotReplicated	The VM's config file is located on a datastore which is either not replicated or not protected by the protection group in which the VM is being protected.
ConnectionDownFault	Thrown if the VMOMI connection to the remote server is down.
ConnectionLimitReached	Thrown when the configured connection limit has been reached.
DatastoreAlreadyProtected	Datastore cannot be added to this group because it is already part of another protection group.
DatastoreMissingProtection	Base fault for datastore missing from the protection group.
DatastoreNotReplicated	Cannot protect datastore because underlying storage devices are not configured for replication.
DatastoreProtectionIssue	Base fault for datastore-specific protection issues.
DependencyConflict	UpdateVmSettings operation was attempted that might cause a dependency cycle.
DeviceBackingConflict	If the caller specified a device locator, or explicitly excluded, a device which the provider would like to protect.
DeviceBackingConflict	Fault thrown when a user attempts to protect or reconfigure protection for a VM, specifying one or more backing locators which conflict with those chosen by the provider.
DeviceGroupMatchingFault	Reported when a device group cannot be matched to a peer device group.
DeviceMatchingFault	Reported when a device cannot be matched to a peer device.
DevicesNotResolved	Fault thrown when a user attempts to protect or reconfigure protection for a VM without resolving all of its devices
DirectionError	The direction of the recovery plan cannot be determined.
DomainDatastoreNotFound	No existing datastore could be matched to a fault domain.
DomainNotFound	No storage container could be matched to a fault domain. A storage container links the domain to its datastore.
DomainPeerNotFound	Domains does not have their peer domains reported by the paired SRM. One of the reasons may be no VASA provider is registered at the paired site.
DomainReplicationGroupNotFound	Replication group is part of a protection group but could not be found in the configuration.
DomainScNotFound	No storage container could be matched to a fault domain. The storage container links the domain to its datastore.
DuplicateArray	There is already another array manager that discovered a given array.

Fault	Description
DuplicateName	Call is unable to determine which object to use due to name conflict.
GroupProtectionOverlapped	Thrown when more than one protection group contain VMs replicated by the same vVol replication groups. If recovery is started in this situation, all colocated VMs might be broken. To resolve this make sure that all VMs located on a certain replication group are protected by the same protection group.
GroupStateMissmatch	Sate of the protection group does not match the state of a replication group protected by it. This is possible when the replication group state is changed by an external tool. The error can be corrected by restoring the replication group to the expected state using the storage array instruments and tools.
GroupTargetsNotFound	Target replication groups cannot be found. This occurs when the group is not in the correct state. Check storage policy assignment.
IllegalMove	Thrown when a folder is moved to an invalid place in the folder hierarchy. This can be because the move would create a cycle or the destination is the wrong kind of container.
ImmutableFolder	Thrown when an operation is attempted upon a Folder that cannot be changed. For example, moving or deleting the root folder.
InsufficientLicensesFault	Thrown by a method that cannot acquire licenses for the object to create.
InternalError	An internal error occurred that cannot be described by a more specific fault or if the hbr provider cannot be found(null reference).
InvalidAdapterConnectionSpec	An AdapterConnectionSpec doesn't match the corresponding AdapterConnectionPrompt defined by the SRA.
InvalidArgument	Base class for invalid argument exceptions. Thrown if the username format invalid, or user or user group does not exist, or if the user is a global vCenter administrator, or if the name of the protection group is empty or if the list of virtual machines is empty or null.
InvalidFolder	Thrown when a node is moved to an invalid place in the hierarchy. This can be because it is a child of the current node, or a wrong kind of container.
InvalidLogin	Cannot complete login due to an incorrect user name or password.
InvalidPrimaryFolder	Thrown for an attempt to create a primary site folder that cannot contain VMs.
InvalidPrimaryNetwork	Invalid primary network specified for mapping, such as uplink DVPortgroup
InvalidSecondaryFolder	Thrown for an attempt to create a secondary site folder that cannot contain VMs.
InvalidSecondaryNetwork	Invalid secondary network specified for mapping (such as uplink DVPortgroup)
InvalidState	Base class for invalid state exceptions

Fault	Description
InvalidTokenLifetime	SSO token is either expired or not yet valid. This exception is generally thrown if there is a time skew between the local clock and the SSO server. This exception is not supported from methods with version prior to 8. However it is translated to Vim::Fault::InvalidLogin::Exception.
IpMappingFault	A base class for all IpMapping related faults. Thrown if problems are found while validating IP subnet mapping rules.
ManagedObjectNotFound	The destination folder does not exist.
MatchingFault	Reported when a device/device group cannot be matched to a peer device/device group.
MissingFolderMapping	Thrown when a user attempts to protect a VM, but the folder inventory mapping for the VM is not present in the InventoryMapper.
MissingFolderAndResourcePoolMapping	Thrown when a user attempts to protect a VM, but both the folder and resourcepool inventory mapping for the VM is not present in the InventoryMapper.
MissingInventoryMapping	Thrown when a user attempts to protect a VM, but the inventory mappings for the VM are not present in the InventoryMapper.
MissingNetworkMapping	Thrown when user attempts to add an IP mapping, but a network mapping between protectedNetwork and recoveryNetwork is missing.
MissingNetworkMappingEx	Thrown when a user attempts to protect a VM, but the network inventory mapping for the VM is not present in the InventoryMapper.
MissingResourcePoolMapping	Thrown when a user attempts to protect a VM, but the resourcePool inventory mapping for the VM is not present in the InventoryMapper.
MultipleFault	Multiple faults occur.
NetworkNotFound	Thrown if the test network mapping does not exist in the recovery plan.
NoPermission	Operation denied because of a privilege not held on a managed object.
NotEmpty	Thrown when an operation cannot be performed because the object is not empty.
NotSuitablePlaceholderDatastoreCluster	Thrown if the Placeholder Datastore Manager determines that a datastore should not be used as a placeholder datastore because it is not visible to all hosts in the cluster.
NotSuitablePlaceholderDatastore	Thrown if the Placeholder Datastore Manager determines that a datastore should not be used as a placeholder datastore for a variety of reasons, for example, it becomes replicated or is not visible to all hosts in the cluster. This fault is a parent for several other faults, which determine the exact reason why this datastore should not be used as a placeholder datastore.

Fault	Description
NotSupported	ProtectionGroup is being moved into a folder whose childType() property is not set to the appropriate value. For example, a ProtectionGroup cannot be moved into a folder whose ChildType property value does not contain "ProtectionGroup".
NotAuthenticated	Operation denied because the session has not successfully logged in.
PairOperationInProgress	Thrown when another pair, repair or break pairing operation is in progress and the request is rejected.
PeerArrayNotFound	Thrown when peer array with specified ID not found for a storage array.
PeerDeviceGroupNotMatched	Reported when a local device group cannot be matched to a remote peer device group.
PeerDeviceGroupNotStretched	Reported when a local stretched device group is matched to a remote peer device group but the local device group is not stretched.
PeerDeviceGroupWithoutStaticSitePreference	Reported when a local stretched device group is matched to a remote stretched peer device group but the local device group has no static site preference.
PeerDeviceNotMatched	Reported when a local device cannot be matched to a remote peer device.
PeerDeviceNotStretched	Reported when a local stretched device is matched to a remote peer device but the local device is not stretched.
PeerDeviceWithoutStaticSitePreference	Reported when a local stretched device is matched toa remote stretched peer device but the local device has no static site preference.
ProductionVmDeleted	Production VM was deleted.
PromptNotFound	Thrown when a RecoveryPrompt cannot be found.
ProtectionGroupNotEmpty	Thrown after attempt to remove a protection group that contains protected VMs.
ProtectionGroupNotFound	Thrown when an operation on protection group cannot find the protection group.
ProtectionIssue	Base class for faults describing protection group configuration issues.
ProtectionStillActive	Thrown when an attempt is made to remove a Primary/ SecondarySite that is being replicated from/to.
ProviderFault	Thrown if either ReplicationProvider rejected the operation. This can occur when the settings are incorrect.
RecoveredDatastoreNotAvailableForPdm	Thrown if the Placeholder Datastore Manager determines that a datastore should not be used as a placeholder datastore because it was recovered.
RecoveryPlanLocked	An attempt was made to change a RecoveryPlan that is locked.
RecoveryPlanNotFound	Thrown when the requested recovery plan was not found
RecoveryResultNotFound	Thrown when a RecoveryResult cannot be found.

Fault	Description
RemotePeerDeviceGroupNotMatched	Reported when a remote device group cannot be matched to a local peer device group.
RemotePeerDeviceGroupNotStretched	Reported when a local stretched device group is matched to a remote peer device group but the remote device group is not stretched.
RemotePeerDeviceGroupWithoutStaticSitePreference	Reported when a local stretched device group is matched to a remote stretched peer device group but the remote device group has no static site preference.
RemotePeerDeviceNotMatched	Reported when a remote device cannot be matched to a local peer device.
RemotePeerDeviceNotStretched	Reported when a local stretched device is matched toa remote peer device but the remote device is not stretched.
RemotePeerDeviceWithoutStaticSitePreference	Reported when a local stretched device is matched to a remote stretched peer device but the remote device has no static site preference.
RemoteSiteNotAuthenticated	Thrown if the remote site or the session is not authenticated.
RemoteSiteNotEnabled	An attempt was made to use a remote site that is not enabled.
RemoteSiteNotInitialized	An attempt is made to use a remote site that is not initialized.
ReplicatedArrayPairAlreadyExists	Thrown when a replicated array pair already exists for a pair of arrays for a given SRA.
ReplicatedDatastoreNotAvailableForPdm	Thrown if the Placeholder Datastore Manager determines that a datastore should not be used as a placeholder datastore because it is replicated.
ReplicationGroupFault	ExtApi representation of dr.vvolProvider.fault.ReplicationGroupFault.
ReplicationProviderFault	Thrown when an unspecified error was returned from the replication provider.
SelfPairFault	Thrown when an attempt to pair with ourselves was made.
SitePairingFault	Thrown when one of the site pairing operations failed.
SnapshotDirectoryNotReplicated	The VM's snapshot directory is not replicated.
SourceDeviceGroupsWithStaticSitePreference	Reported when a local stretched device group is matched to a remote stretched peer device group but both the local device group and the remote device group have static site preference.
SourceDevicesWithStaticSitePreference	Reported when a local stretched device is matched to a remote stretched peer device but both the local device and the remote device have static site preference.
StorageAdapterNotFound	Thrown when storage adapter is not found.
StorageProviderFault	Corresponds to dr.vvolProvider.fault.StorageProviderFault.
StretchedDeviceGroupMatchingFault	Reported when a stretched device group is matched to a peer device group but only one device group is stretched.
StretchedDeviceMatchingFault	Reported when a stretched device is matched to a peer device but only one device is stretched.
StringArgumentTooLong	Thrown when a string argument exceeds {maxSize} characters

Fault	Description
SuOperationInProgress	Thrown when another create, update or delete solution user operation is in progress and the request is rejected.
SuspendDirectoryNotReplicated	The VM's suspend directory is not replicated.
SystemError	Thrown in case of internal SRM error.
TaskInProgress	Array cannot be found.
TestDatastoreNotAvailableForPdm	Thrown if the Placeholder Datastore Manager determines that a datastore should not be used as a placeholder datastore because it is created for test recovery.
UnableToFindPlaceholderDatastore	Thrown if the Placeholder Datastore Manager is unable to find a placeholder datastore for a host or a cluster.
UnknownPrimaryFolder	Secondary site tried operation on a folder that is nonexistent on primary site (protected site)
UnknownPrimaryNetwork	Thrown when the secondary site tries to perform an operation involving a network that does not exist on the primary site.
UnknownSecondaryNetwork	Secondary site tried operation on a network that is nonexistent on secondary site (recovery site)
UnknownPrimaryResourcePool	Secondary site tried operation on resource pool that is nonexistent on primary site.
UnknownSecondaryFolder	Primary site tried operation on a folder that is nonexistent on secondary site.
UnknownSecondaryNetwork	Primary site tried operation on a network that is nonexistent on secondary site.
UnknownSecondaryResourcePool	Primary site tried operation on resource pool that is nonexistent on secondary site.
VersionConflict	Attempt to reconfigure with a changeVersion that does not match the current value.
vim.fault.ConcurrentAccess	Thrown if another operation has modified the object and the change version no longer matches.
VmAlreadyProtected	Thrown when a user tries to protect a VM which is already protected by SRM.
VmAlreadyProtectedEx	Thrown when a user tries to protect a VM which is already protected by SRM. Contains extra info about the PG currently holding the VM protection.
VmFileNotReplicated	A virtual machine file is not replicated.
VmNotFoundInRecoveryPlan	Attempt to retrieve settings for virtual machine that does not exist in RecoveryPlan.
VmNotReplicated	No virtual machine files are replicated. Check and fix the storage policy assignment.
VmNotSupported	Thrown when the type VM used in an operation is not supported by the operation.
VmPiggybackError	A virtual machine is detected on a replication group that is already protected by one of the protection groups. Either protect the VM or reconfigure it out of the replication group.

Fault	Description
VmReconfigureRequired	The virtual machine configuration has changed and reconfiguration is required. Reconfigure is started automatically without user intervention.
VmReplicationGroupError	Attempting to protect a virtual machine that belongs to one replication group into a protection group that is configured to use a different set of replication groups.
VmSplitReplicated	In order to guarantee the consistency, SRM protects only virtual machines replicated by a single replication group. This situation occurs when the configuration file and the virtual disk files do not share the same storage policy assignments.
VmTemplateFault	vVol provider does not support protection of template VMs. This fault is throw when attempt to protect template VM with vVol provider is made.
VvolDomainFault	Base class for all fault domain related VvolProvider faults.
VvolProviderFault	Base class for all VvolProvider faults.
VvolVmFault	Base class for all virtual machine related VvolProvider faults.
WrongDrServerFault	Thrown if an attempt to repair connection of a paired SRM with wrong remote SRM.

SSL Certificates and SNMP Traps

This appendix contains information for the requirements and work with SSL certificates and Simple Network Management Protocol (SNMP) Traps.

SSL Certificates

The Site Recovery Manager uses SSL to encrypt communications between a client application and the server. The SSL certificate of the target server must reside on the client machine. To access the Web service programmatically, use its URN from a Web services client application.

The Web service listens to the following ports:

- Site Recovery Manager Appliance Management API
  Port - 5480
- Site Recover Manager APIs for Windows
  Port - 9086
- Site Recover Manager APIs for Photon Virtual Appliance (VA)
  Port - 443

Get vCenter Server Certificate

The Site Recovery Manager API or Site Recovery Manager Virtual Appliance is a secure Web service running on the Site Recovery Manager Server. To develop client applications, you must obtain the VMware vCenter Server certificate,

which is used by the Site Recovery Manager Server, and import it into the certificate store of the workstation where you develop client applications.

1. From your development workstation, open Internet Explorer (IE).
2. Navigate to the vCenter Server using HTTPS protocol – `https://<servername>`.
   A Security Alert message displays a warning regarding the certificate's certifying authority.
3. Click **View Certificate**.
4. Click **Install Certificate** to launch the Certificate Import wizard. Keep the default settings and click **Next**.
5. Click **Finish**. A security warning message displays concerning the certificate's certifying authority.
6. Click **Yes**.
   A Certificate Import wizard "success" message displays.
7. Click **OK** to dismiss the success message.
   The Certificate Properties page becomes active again.
8. Click **OK** in the Certificate dialog box to continue to the server.
   The initial Security Alert message presented in step 2 becomes active again.
9. Click **Yes** in the Security Alert message to continue with the original HTTPS request.
   The server Welcome page displays. The certificate is now installed in the IE certificate cache.

Now that you have the certificate, your next task depends on what programming language you use to develop your client applications.

For C# developers, you can continue setting up your development environment by following the instructions at "Setting Up for Microsoft C# Development" in the Developer's Setup Guide located at VMware's Web site developer support page under the vSphere Web Services SDK.

For Java developers, you must export the certificates from the IE cache to a local directory. Minimize the IE browser window, and export the certificates as detailed in the following procedure.

Export Cached Certificates to a Local Directory

For Java development in a Windows environment, you must export the certificate to a local directory.

1. Create a directory for the certificate, using the name set in the various batch files for the vSphere Web Services SDK: `C:\VMware-Certs`.
2. From the IE Tools menu, select Internet Options to open the Internet Options properties page.
3. Click the **Content** tab to activate the content advisor.
4. Click **Certificates** to open the Certificate manager.
5. Click the **Trusted Root Certificate Authorities** tab to display the list of trusted certificates.
6. Scroll through the list of certificates to find the certificate. For the vCenter Server, the certificate name is VMware.
7. Click the certificate to select it.
8. Click **Export...** to launch the Certificate Export Wizard.
9. Click **Next** to continue. The Export File Format dialog displays.
10. Keep the defaults ("DER encoded binary X.509 (.CER)") and click **Next** to continue.
    The File To Export dialog displays, enabling you to enter a unique name for the certificate.

11. Choose a filename and enter it, along with the complete path to the directory: `C:\VMware#Certs\<servername>.cer`

    If you do not enter the complete path, the certificate is stored in your Documents and Settings folder.

12. Click **Next** to continue with the export.

    A Completing the Certificate Export Wizard page displays, summarizing the information about the certificate.

13. Click **Finish** to complete the export.

    A Certificate Export Wizard “success” message displays.

14. Click **OK** to dismiss the success message.

15. Click **Close**.

16. Click **Cancel** to close the Internet Options properties page.

For more information about setting up your Java development environment, see “Setting Up for Java Development” in the Developer’s Setup Guide located at the VMware Web site developer support page under the vSphere Web Services SDK.

About the Virtual Machine Keystore

A Java KeyStore (JKS) is a repository of security certificates – either authorization certificates or public key certificates – used for SSL encryption and related activities. The Java Development Kit (JDK) maintains a keystore in `jre/lib/security/cacerts`, and provides the `keytool` command to manipulate it.

The `VMKEYSTORE` environment variable specifies the path to the JKS. The `run.sh` and `run.bat` scripts both refer to it. If you use the `--ignorecert` argument to run Java samples, you must still set the `VMKEYSTORE` variable, but you can set it to any location, not the actual JKS location.

Sample paths, Windows and Linux:

```
VMKEYSTORE=C:\VMware-Certs\vmware.keystore
```

```
VMKEYSTORE=/root/vmware-certs/vmware.keystore
```

SNMP Traps

Site Recovery Manager provides Simple Network Management Protocol (SNMP) traps that collect information sent by the API. All traps are compliant with the SNMPv1 type. Information provided by the traps can be used to initiate actions by client applications.Callers of the Site Recovery Manager API interface should listen for the SNMP traps. You might need to configure the vCenter Server to forward the SNMP traps to the registered SNMP Server. The MIB file is located in the following directory:`<installdir>\www\VMWARE-SRM-TRAPS-5_0.MIB`

There are two ways to generate SNMP traps from Site Recovery Manager. The first is the method presented here and in other Site Recovery Manager documentation. The second method to generate traps is by configuring SNMP actions on the events and alarms that Site Recovery Manager adds to vCenter Server. Alarms with SNMP traps configured are all raised using the generic alarm definition in `VMWARE-VC-EVENT.mib`. Consequently alarm-based traps do not have explicit definitions. To manage them, you would need to synthesize the trap, capture its contents, parse the trap, then determine how to filter it.

Look at MIB Names for SNMP Traps for more details.

MIB Names for SNMP Traps

The listed SNMP traps originate from the Site Recovery Manager, not from vCenter Server. Descriptions of SNMP traps are given according to their names in the MIB file. The names in this list can be prefaced by either `vmwareSrm` (Site Recovery Manager) or `oidDr` (object ID data recovery)

Table 177: SNMP Traps in the MIB

SNMP Trap	What Trap Indicates
RecoveryPlanExecuteTestBegin	Signaled on the recovery site when a recovery test is initiated.
RecoveryPlanExecuteTestEnd	Signaled on the recovery site when a recovery test has completed. If an error occurred it is available as [data.Error]
RecoveryPlanExecuteBegin	Signaled on the recovery site when a recovery is initiated.
RecoveryPlanExecuteEnd	Signaled on the recovery site when a recovery has completed. If an error occurred it is available as [data.Error]
RecoveryVmBegin	Signaled when the recovery virtual machine was successfully created. If an error occurs before the virtual machine's ID is known, the event is not fired.
RecoveryVmEnd	Signaled after the last post-power on script has completed, or after a recovery-stopping error has occurred for the virtual machine.
RecoveryPlanPromptDisplay	The recovery plan is displaying prompt [data.PromptKey] and is waiting for user input. PromptKey is a unique identifier.
RecoveryPlanPromptResponse	The recovery plan received an answer to prompt [data.PromptKey] and is no longer paused waiting for user input.
RecoveryPlanServerCommandBegin	Signaled on the recovery site when Site Recovery Manager starts to run a Callout command on the Site Recovery Manager server.
RecoveryPlanServerCommandEnd	Signaled on the recovery site when Site Recovery Manager has finished running a Callout command on the Site Recovery Manager server.
RecoveryPlanVmCommandBegin	Signaled on the recovery site when Site Recovery Manager has started to run a Callout command on a recovered virtual machine.
RecoveryPlanVmCommandEnd	Signaled on the recovery site when Site Recovery Manager has finished running a Callout command on a recovered virtual machine.
RecoveryPlanExecuteReprotectBegin	Signaled on the recovery site when a reprotect is initiated.
RecoveryPlanExecuteReprotectEnd	Signaled on the recovery site when a reprotect has completed. If an error occurred it is available as [data.Error]
RecoveryPlanExecuteCleanupBegin	Signaled on the recovery site when a test cleanup is initiated.
RecoveryPlanExecuteCleanupEnd	Signaled on the recovery site when a test cleanup has completed. If an error occurred it is available as [data.Error]

Configuring SNMP Receivers in vCenter Server

For a simple procedure to configure SNMP receivers, see the section "Configure SNMP Settings in the vSphere Web Client" in the vSphere vCenter Server and Host Management manual, available in the VMware vSphere 5.5 Documentation Center. For details about configuring the SNMP receiver URL, receiver port, and community, see the section "Configure SNMP Settings for vCenter Server by Using the vSphere Web Client" in the vSphere Monitoring and Performance manual, also in the VMware vSphere 5.5 Documentation Center.

SNMP Traps and Object IDs

The MIB objects are listed below with IDs, then the SMNP traps themselves with IDs.

Table 178: MIB objects with IDs

MIB_OBJECT	ID
oidDrVmName	1.3.6.1.4.1.6876.51.1.1
oidDrRecoveryName	1.3.6.1.4.1.6876.51.1.2
oidDrPromptString	1.3.6.1.4.1.6876.51.1.3
oidDrRecoveryType	1.3.6.1.4.1.6876.51.1.4
oidDrRecoveryState	1.3.6.1.4.1.6876.51.1.5
oidDrSiteString	1.3.6.1.4.1.6876.51.1.6
oidDrVmUuid	1.3.6.1.4.1.6876.51.1.7
oidDrResult	1.3.6.1.4.1.6876.51.1.8
oidDrCommandName	1.3.6.1.4.1.6876.51.1.9

Table 179: SMNP traps with IDs

MIB_TRAP	ID
RecoveryPlanExecuteTestBegin	1.3.6.1.4.1.6876.51.0.1
RecoveryPlanExecuteTestEnd	1.3.6.1.4.1.6876.51.0.2
RecoveryPlanExecuteBegin	1.3.6.1.4.1.6876.51.0.3
RecoveryPlanExecuteEnd	1.3.6.1.4.1.6876.51.0.4
RecoveryVmBegin	1.3.6.1.4.1.6876.51.0.5
RecoveryVmEnd	1.3.6.1.4.1.6876.51.0.6
RecoveryPlanPromptDisplay	1.3.6.1.4.1.6876.51.0.7
RecoveryPlanPromptResponse	1.3.6.1.4.1.6876.51.0.8
RecoveryPlanServerCommandBegin	1.3.6.1.4.1.6876.51.0.9
RecoveryPlanServerCommandEnd	1.3.6.1.4.1.6876.51.0.10
RecoveryPlanVmCommandBegin	1.3.6.1.4.1.6876.51.0.11
RecoveryPlanVmCommandEnd	1.3.6.1.4.1.6876.51.0.12
RecoveryPlanExecuteReprotectBegin	1.3.6.1.4.1.6876.51.0.13
RecoveryPlanExecuteReprotectEnd	1.3.6.1.4.1.6876.51.0.14
RecoveryPlanExecuteCleanupBegin	1.3.6.1.4.1.6876.51.0.15
RecoveryPlanExecuteCleanupEnd	1.3.6.1.4.1.6876.51.0.16

Documentation Legal Notice


vmware®
by Broadcom