VMware Site Recovery Manager 8.1 Release Notes

Updated on 02/15/2021

VMware Site Recovery Manager 8.1.0.4 | 24 AUG 2018 | Build 9569154

VMware Site Recovery Manager 8.1.0.3 | 12 JUN 2018 | Build 8738384

VMware Site Recovery Manager 8.1.0.2 | 18 MAY 2018 | Build 8527244

VMware Site Recovery Manager 8.1.0.1 | 20 APR 2018 | Build 8311425

Note: VMware Site Recovery Manager 8.1.0.1 | 20 APR 2018 | Build 8311425 replaces the previously released VMware Site Recovery Manager 8.1 | 17 APR 2018 | Build 8255892

VMware Site Recovery Manager 8.1 | 17 APR 2018 | Build 8255892

Check for additions and updates to these release notes.

For information about the VMware Site Recovery Manager 8.1 patch releases, see the corresponding section of these release notes.

- VMware Site Recovery Manager 8.1.0.4 Express Patch
- VMware Site Recovery Manager 8.1.0.3 Express Patch
- VMware Site Recovery Manager 8.1.0.2 Express Patch
- VMware Site Recovery Manager 8.1.0.1 Express Patch

What's in the Release Notes

These release notes cover the following topics:

What's New in Site Recovery Manager 8.1

VMware Site Recovery Manager 8.1 provides the following new features:

- VMware Site Recovery Manager 8.1 is compatible with VMware vSphere 6.7. In addition, Site Recovery Manager 8.1 introduces backward compatibility with previous versions of vCenter and vSphere, as detailed in the **Compatibility Matrixes for VMware Site Recovery Manager 8.1**
- Streamlined HTML 5 user interface. New HTML 5 UI enhances the overall user's experience by simplifying the deployment and usage, and enabling streamlined workflows - unified replication and protection, site pairing, and more.
- VMware Site Recovery Manager 8.1 Configuration Import/Export Tool. You can use the VMware Site Recovery Manager 8.1 Configuration Import/Export Tool to export and import configuration data. The tool supports the export of inventory mappings, recovery plans, protection groups, and the related objects into an XML file, and import from a previously exported file. For more information on the new feature, see the **Site Recovery Manager 8.1 Installation and Configuration.**
- Support for Symmetric Multi-Processing Fault Tolerance (SMP-FT) with array-based replication. For more information, see Protecting Microsoft Cluster Server and Fault Tolerant Virtual Machines.
- Increase in the number of array-based replication protection groups and vSphere Replication protection groups to 500.
- Unified Disaster Recovery and Protection for on-premises and VMware Cloud on AWS. VMware Site Recovery Manager 8.1 enables orchestrated recovery or migration of workloads across on premises sites or between on premises and VMware Cloud on AWS.
- Enhancements to Site Recovery Manager public API. Site Recovery Manager 8.1 introduces new methods in the product's Public API:
  - IP customization
  - Modifying array-based Protection groups
- With the public API, you have programmatic access to a wider range of product functionality and more extensive product documentation.

- vRealize Operations Management Pack for Site Recovery Manager 8.1. For information about the management pack, see **VMware vRealize Operations Management Pack for Site Recovery Manager 8.1 Release Notes**.
- Ability to show related devices and datastores in a Protection Group.

Note: For interoperability with earlier or later releases of VMware vSphere, see the Compatibility Matrixes for VMware Site Recovery Manager 8.1.

For information about the features of vSphere 6.7, see the *vSphere 6.7* documentation.

For information about the supported databases, see the Compatibility Matrixes for VMware Site Recovery Manager 8.1.

Localization

VMware Site Recovery Manager 8.1 is available in the following languages:

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

Compatibility

Site Recovery Manager Compatibility Matrix

Site Recovery Manager 8.1 is compatible with vSphere 6.0 Update 3, vSphere 6.5, vSphere 6.5 Update 1, vSphere 6.7, and supports ESXi versions that vCenter Server 6.7 supports.

If you use VMware Tools 10.1 and ESXi 6.5 or 6.0, ensure the time synchronization between the ESXi host and vCenter Single Sign-On on the recovery site.

For interoperability and product compatibility information, including supported guest operating systems and support for guest operating system customization, see the Compatibility Matrices for VMware Site Recovery Manager 8.1.

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.

VMware vSAN Support

Site Recovery Manager 8.1 can protect virtual machines that reside on VMware vSAN by using vSphere Replication. vSAN does not require a Storage Replication Adapter (SRA) to work with Site Recovery Manager 8.1.

VMware VSA Support

Site Recovery Manager 8.1 can protect virtual machines that reside on the vSphere Storage Appliance (VSA) by using vSphere Replication. VSA does not require a Storage Replication Adapter (SRA) to work with Site Recovery Manager 8.1

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:

- Upgrading Site Recovery Manager from version 5.8.x directly to version 8.1 is not supported. You must first upgrade Site Recovery Manager from 5.8.x to 6.1.2.x. After upgrading Site Recovery Manager to 6.1.2.x, you must reconfigure the pairing between the Site Recovery Manager instances on the protected and the recovery site, before you continue with the upgrade to 8.1.
- Upgrading Site Recovery Manager from version 6.0.x directly to version 8.1 is not supported. To upgrade Site Recovery Manager 6.0.x to Site Recovery Manager 8.1, you must first upgrade Site Recovery Manager from 6.0.x to 6.1.2. If you use vSphere Replication with Site Recovery Manager 6.0.x, and you upgrade vSphere Replication from version 6.0.x to version 8.1 directly, when you attempt the interim upgrade of Site Recovery Manager from version 6.0.x to version 6.1.2, the Site Recovery Manager upgrade fails with an error because of an incompatible version of vSphere Replication. Upgrade vSphere Replication to version 6.1.2 before you upgrade Site Recovery Manager from 6.0.x to 6.1.2.
- After upgrading Site Recovery Manager, Site Recovery Manager does not retain any advanced settings that you configured in the previous installation. This is by design. Due to changes in default values or improvements in performance, advanced settings that you set in a previous version of Site Recovery Manager might not be required by or compatible with the new version. Advanced settings are also not retained if you uninstall and then reinstall the same version of Site Recovery Manager.
- If the vCenter Server instances on the protected and recovery sites are in Enhanced Linked Mode, they must be direct replication partners.

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 8.1

For the operational limits of Site Recovery Manager 8.1, 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 8.1 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 vCenter Site Recovery Manager.

Caveats and Limitations

- Site Recovery Manager 8.1 offers limited support for vCloud Director environments. Using Site Recovery Manager to protect virtual machines within vCloud resource pools (virtual machines deployed to an Organization) is not supported. Using Site Recovery Manager to protect the management structure of vCD is supported. For information about how to use Site Recovery Manager to protect the vCD Server instances, vCenter Server instances, and databases that provide the management infrastructure for vCloud Director, see VMware vCloud Director Infrastructure Resiliency Case Study.
- 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 8.1 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 http://kb.vmware.com/kb/2109813.
- vSphere Replication 8.1 supports replication of virtual machines on VMware vSphere Virtual Volumes with limitations. Site Recovery Manager 8.1 supports vSphere Replication 8.1 with vSphere Virtual Volumes with the following limitations.
    - You cannot use Site Recovery Manager 8.1 with vSphere Virtual Volumes array-based replication.
    - 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 8.1 does not support NFS v 4.1 datastores for array-based replication. You can use Site Recovery Manager 8.1.x with NFS v 4.1 datastores for vSphere Replication.
- Site Recovery Manager does not support reconfiguration of storage profile protection groups, such as changing the set of associated storage policies, group name, or descriptions. To modify a storage profile protection group, you must delete it and recreate it with the new configuration.
- Site Recovery Manager cannot protect RDM disks or fault-tolerant virtual machines in storage policy protection groups.
- Site Recovery Manager does not support the mapping or exclusion of nonreplicated virtual devices in storage policy protection groups.
- To use Two-factor authentication with RSA SecureID or Smart Card (Common Access Card) authentication your environment must meet the following requirements:
    1. Use the administrator credentials of your Platform Services Controller to install Site Recovery Manager 8.1 and to pair your Site Recovery Manager 8.1 sites.
    2. The vCenter Server instances on both Site Recovery Manager 8.1 sites must work in Enhanced Linked Mode. To prevent failures during upgrade of Site Recovery Manager from 8.1 to a newer version of Site Recovery Manager, the vCenter Server instances on both sites must be direct replication partners.
- Site Recovery Manager 8.1 supports protection of encrypted VMs with Storage Policy Protection Groups only, but does not support the customization of encrypted VMs. In Site Recovery Manager 8.1 IP customization and in-guest commands do not work on encrypted VMs. For information about how to configure protection of Encrypted VMs, see the *Site Recovery Manager Administration* documentation.

Available Patch Releases

VMware Site Recovery Manager 8.1.0.4 Express Patch

Released 24 AUG 2018 | Build 9569154

- The VMware Site Recovery Manager 8.1.0.4 Express Patch Release adds support for VMware Cloud on AWS SDDC Version 1.5 and provides bug fixes.

Installation and Upgrade Notes

If you are running Site Recovery Manager 8.1.0.1, 8.1.0.2, or 8.1.0.3, upgrade to Site Recovery Manager 8.1.0.4. See Upgrading Site Recovery Manager in *Site Recovery Manager 8.1 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 8.1.0.x, upgrade the vSphere Replication appliance to version 8.1.0.4. See the vSphere Replication 8.1 Release Notes for information about vSphere Replication 8.1.0.4.

VMware Site Recovery Manager 8.1.0.3 Express Patch

Released 12 JUN 2018 | Build 8738384

- The VMware Site Recovery Manager 8.1.0.3 Express Patch Release provides bug fixes.

Installation and Upgrade Notes

If you are running Site Recovery Manager 8.1.0.1 or 8.1.0.2, upgrade to Site Recovery Manager 8.1.0.3. See Upgrading Site Recovery Manager in *Site Recovery Manager 8.1 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 8.1, upgrade the vSphere Replication appliance to version 8.1.0.3. See the vSphere Replication 8.1 Release Notes for information about vSphere Replication 8.1.0.3.

VMware Site Recovery Manager 8.1.0.2 Express Patch

Released 18 MAY 2018 | Build 8527244

- The VMware Site Recovery Manager 8.1.0.2 Express Patch Release provides bug fixes.
- The VMware Site Recovery Manager 8.1.0.2 Express Patch Release enhances the VMware Site Recovery Manager 8.1 Configuration Import/Export Tool.

Installation and Upgrade Notes

If you are running Site Recovery Manager 8.1 or 8.1.0.1, upgrade to Site Recovery Manager 8.1.0.2. See Upgrading Site Recovery Manager in *Site Recovery Manager 8.1 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 8.1, upgrade the vSphere Replication appliance to version 8.1.0.2. See the vSphere Replication 8.1 Release Notes for information about vSphere Replication 8.1.0.2.

VMware Site Recovery Manager 8.1.0.1 Express Patch

Released 20 APR 2018 | Build 8311425

- The VMware Site Recovery Manager 8.1.0.1 Express Patch Release replaces the previously released VMware Site Recovery Manager 8.1.

Installation and Upgrade Notes

If you are running Site Recovery Manager 8.1, upgrade to Site Recovery Manager 8.1.0.1. See Upgrading Site Recovery Manager in *Site Recovery Manager 8.1 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 8.1, upgrade the vSphere Replication appliance to version 8.1.0.1. See the vSphere Replication 8.1 Release Notes for information about vSphere Replication 8.1.0.1.

Resolved Issues

The resolved issues are grouped as follows.

- Site Recovery Manager
- VMware Site Recovery Manager 8.1 Configuration Import/Export Tool

Site Recovery Manager

- **NEW When you install Site Recovery Manager with a CA-signed certificate and a non-English locale, the installer fails to import the CA-signed certificate to the Tomcat web server that serves the Site Recovery Manager HTML 5 user interface and generates a self-signed certificate**

  When you install Site Recovery Manager with a non-English locale and a CA-signed certificate, the installer fails to import the certificate to the

`VMware: Srm::Installation::SrmClientHandler::InstallSrmClientCertificateFromP12File: ERROR: FindCertificateAliases() failed. VMware: Srm::Installation::VMConfigureSrmClient: ERROR: Failed to install SRM Server certificate in SRM Client (Tomcat) keystore. Trying to generate new certificate for SRM Client (Tomcat).`

This issue is fixed in Site Recovery Manager 8.1.0.4.

- **NEW When you configure virtual machines for replication, the Site Recovery user interface might show an error "Server Error Response with status: 0 for URL: null"**

  When you are using the Site Recovery HTML5 user interface to select VMs to replicate to the recovery site, the UI might throw an error `"Server Error Response with status: 0 for URL: null"`

  This issue is fixed in Site Recovery Manager 8.1.0.4.

- **NEW If you use a Firefox browser, you cannot configure for replication multiple virtual machines**

  If you use a Firefox browser, you receive an error when you attempt to configure for replication multiple virtual machines.

  This issue is fixed in Site Recovery Manager 8.1.0.4.

- **Site Recovery Manager installation fails with "Error 61" when the "phone home global configuration" endpoint registration is missing**

  The possible removal of the "phone home global configuration" endpoint registration is related to load balancing configurations. In the case of load balancing, there are scripts that go over all registered endpoints and replace all URLs to point to the load balancer. These scripts remove the registration of the "phone home global configuration" endpoint and the Site Recovery Manager installation fails to discover it. The Site Recovery Manager installation is searching for this endpoint because it must store its thumbprints.

  This issue is fixed.

- **When configuring a reverse replication, despite selecting a target datastore, you cannot continue because an error message says that you must select a datastore**

  If there is a single datastore on the target site on a slow network, a race condition occurs, which causes the datastore validation and lookup for seeds to occur before the necessary VM data is delivered. This breaks the page logic and the data remains invalid, which causes the validation error.

  This issue is fixed.

- **Site Recovery Manager server crashes if chained certificate is installed and the telemetry functionality is enabled**

  If you install a certificate with chain with 2 or more intermediate certificate authorities and telemetry is enabled, the Site Recovery Manager server crashes when trying to connect to the telemetry service.

  This issue is fixed.

- **Site Recovery Manager installation fails when the Platform Services Controller user has double quotes in the password**

  When you attempt to install Site Recovery Manager and provide a password for the PSC user that contains double quotes, for example `"*#2klm'gSY"~Ov?OTKqS"`, the installation fails.

  This issue is fixed.

- **Cross-vCenter Server vMotion on stretched storage fails on vCenter Server 6.7 with com.vmware.sdrs.disk.dsunspecified, if a virtual machine is migrated to a cluster**

  Cross-vCenter Server vMotion on stretched storage fails on vCenter Server 6.7 with com.vmware.sdrs.disk.dsunspecified, if a virtual machine is migrated to a cluster.

  This issue is fixed.

- **Upgrade of Site Recovery Manager with Oracle database fails with Error: Failed to create database.**

  If you upgrade from Site Recovery Manager version 6.1.2.1, 6.5.1, or 8.0 using Oracle database, the upgrade fails with `Error: Failed to create database.`

  This issue is fixed.

- **Configure Protection for virtual machine with distributed virtual portgroup fails to open**

  If you create a virtual machine on a replicated datastore on one vCenter Server, and then unregister the virtual machine and register it to another vCenter Server, when you attempt to Configure Protection it fails with with the following error.
  `Error: Retrieve properties failed for MoRefData: type = DistributedVirtualPortgroup, value = dvportgroup-270537, serverGuid = 797960a9-91cd-4d78-9b13-4b868032e7f0`
  This is a result of the portgroup key not matching the portgroup moid.

  This issue is fixed.

VMware Site Recovery Manager 8.1 Configuration Import/Export Tool

- **The VMware Site Recovery Manager 8.1 Configuration Import/Export Tool cannot export or import configuration data with Non-ASCII user name**

  When you try to export of import configuration data by using a VMware Site Recovery Manager 8.1 Configuration Import/Export Tool properties file that contains Non-ASCII user name, the operation fails.

- **When importing settings from the recovery site, the VMware Site Recovery Manager 8.1 Configuration Import/Export Tool log contains false warnings**

  When you use the VMware Site Recovery Manager 8.1 Configuration Import/Export Tool to import configuration data from the recovery site, the log contains false warnings like:

  `“ERROR com.vmware.srm.client.impex.importers.vmSettings.VmSettingsImporter - Vm key '501a16d4-53dc-9db5-9504-81acdbe2be64' not found for plan '' with status 'OK'”`

  This issue is fixed.

- **If you try to import a file which does not contain any protection groups, the import operation fails**

  When you use the VMware Site Recovery Manager 8.1 Configuration Import/Export Tool to import configuration data from a file that contains no protection groups the import operation fails.

  This issue is fixed.

- **After importing the configuration data with VMware Site Recovery Manager 8.1 Configuration Import/Export Tool, some virtual machine recovery settings are missing for array-based protection groups and storage policy protection groups**

  When you import the configuration data with VMware Site Recovery Manager 8.1 Configuration Import/Export Tool, some recovery settings for the virtual machines in array-based protection groups and storage policy protection groups are missing.

  This issue is fixed.

- **Recovery settings for storage policy protection group virtual machines are lost when importing the configuration with VMware Site Recovery Manager 8.1 Configuration Import/Export Tool**

  When you import the configuration with VMware Site Recovery Manager 8.1 Configuration Import/Export Tool, the recovery settings for the virtual machines in storage policy protection groups are lost.

  This issue is fixed.

- **Virtual machines included in Protection Groups appear twice in the exported configuration file**

  When you use the VMware Site Recovery Manager 8.1 Configuration Import/Export Tool to export configuration data, the virtual machines included in Protection Groups appear twice in the exported configuration file.

  This issue is fixed.

- **Import fails if you try to import configuration data from a file with exported Default storage policy**

  When you use the VMware Site Recovery Manager 8.1 Configuration Import/Export Tool to export configuration data and there is a mapping with a Default storage policy, the exported XML file contains an empty tag <StorageProfileMapping/>. When you try to import configuration data from that XML file, the import fails.

  This issue is fixed.

Known Issues

- **NEW Site Recovery Manager cannot apply IP subnet rules during failback of a virtual machine to a protected site if the virtual machine was recovered on an opaque network on the recovery site**

  When Site Recovery Manager recovers a vNIC to an NSX-T opaque nework on a recovery site, after performing reprotect and failback to the original protected site, Site Recovery Manager is unable to apply IP subnet rules for this vNIC.

  Workaround 1: Remove the protection of the virtual machine and protect it again. This action defaults your VM Recovery settings and they must be specified again, if needed.

  Workaround 2: Temporary attach the virtual machine NICs to other network and then attach them again to the desired opaque network.

- **NEW 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**

  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.

  Workaround 1:

  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.

  Workaround 2: Update your Chrome browser to version 85.0.4183.83 or later.

- **NEW If the source VM for a replication runs on ESXi 6.7, replication synchronization seems to progress, but the replication instance never completes successfully**

  In ESXi 6.7, it is possible that more demand log chunks be scheduled for parallel transfer than the actual number that can be transmitted. If you are replicating a VM that is running on such a host and this coincides with a slow target host or temporary network errors, this might result in

Workaround:

1. Migrate all the VMs to another ESXi host.
2. Edit the value of the HBR.DemandlogTransferMaxNetwork ESXi Advanced setting to 63 instead of the default 64.
3. Place the ESXi host in maintenance mode.
4. Reboot the ESXi host.

- **NEW If the source VM for a replication runs on ESXi 6.7 or ESXi 6.7 U1, an initial or full synchronization might stop progressing before completion**

  If you are using vSphere Replication and you are running a protected VM on ESXi 6.7 or ESXi 6.7 U1, an initial or full synchronization of replications might stop progressing before completion. The synchronization of replications remains in progress, but the checksum bytes value in the replication details information does not progress. The power off, take a snapshot, revert to snapshot, and migration VM operations fail with a timeout or Task in progress errors.

  Workaround:

  1. In the ESXi Advanced settings, disable the checksum for vSphere Replication by setting HBR.ChecksumUseChecksumInfo = 0.
  2. Migrate all VMs and power off the ones that cannot be migrated on the ESXi host.
  3. Place the host in maintenance mode.
  4. Reboot the ESXi host.

  Note: This workaround disables the checksum part of the sync process and all of the allocated blocks will be sent to the remote site, regardless of whether they are different or not. This workaround disables the seed functionality.

- **NEW vSphere Client displays wrong number of VMs that you can protect while Site Recovery Manager is in evaluation mode**

  The **Administration > Licensing>Assets** tab in the vSphere Client wrongly states that while in evaluation mode, Site Recovery Manager can protect up to 100 virtual machines per site. The correct number of virtual machines that you can protect with a Site Recovery Manager evaluation license is 75 VMs per site.

  Workaround: Protect up to 75 virtual machines while the product is in evaluation mode.

- **NEW The reprotect operation finishes successfully, but you observe an error in the Site Recovery Manager user interface**

  When you run Recovery Plan Reprotect, the reprotect operation finishes successfully, but you might observe the following error in the Site Recovery Manager user interface.

  `"The object 'dr.recovery.RecoveryTask:<SRM_GUID>:dr.recovery.RecoveryManager.reprotect<TASK_ID>' has already been deleted or has not been completely created"`

  Workaround: Discard the error. The reprotect operation finishes successfully.

- **NEW Site Recovery Manager might create dummy networks from the protection vCenter Server on the recovery vCenter Server when the network names are different form the recovery ones**

  When you have protected VMs attached to networks with network labels different from the ones that exist on the recovery site, during Test\Recovery\Reprotect the operations succeed, but dummy networks with same network labels from protected site might be created on the recovery vCenter Server. Dummy networks are created only once, not every time you execute the Test\Recovery\Reprotect.

  Workaround 1: Disable the preservation of VM snapshots by changing the value of `vrReplication.preserveMpitImagesAsSnapshots` in the Site Recovery Manager advance settings.

  Workaround 2: Discard the dummy network and continue working with Site Recovery Manager.

- **During the installation of Site Recovery Manager, you receive a warning message for overwriting the Site Recovery Manager registration**

  If you use a vCenter Server instance with a Site Recovery Manager already registered, when you try to install another Site Recovery Manager instance with a different plug-in ID, a warning message for overwriting the Site Recovery Manager extension appears.

  Workaround: Ignoring the warning message and finishing the installation results in an installation with the correct plug-in ID.

- **VMware Site Recovery Manager 8.1 Configuration Import/Export Tool might error out when you import a configuration with protected VMs in no recovery plans**

  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 8.1 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 like:

  `Error while importing VM settings for server with guid '6f81a31e-32e0-4d35-b329-783933b50868'.`

  The rest of your exported configuration is properly imported.

  Workaround: 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.

- **If you use VMware Cloud on AWS as a disaster recovery site and you have configured Hybrid Linked Mode, the Site Recovery plug-in for the vSphere client shows UI error Not installed**

  If you use VMware Cloud on AWS as a disaster recovery site and you have configured Hybrid Linked Mode, the Site Recovery plug-in for the vSphere Client shows the `UI error Not installed` error for vSphere Replication and Site Recovery Manager services. Opening the Configure Replication wizard from the vSphere client shows the `Cannot find healthy Site Recovery UI` error.

Workaround:

1. Ignore the error and open the Site Recovery user interface at the cloud site - either from the VMC UI Add Ons tab, or directly at https://<VR_SDDC_URL>/dr.
2. Open the Configure Replication wizard from the Site Recovery user interface.

- **When using vSphere 6.7 the Site Recovery Manager server stops working after upgrading Site Recovery Manager 8.1 to Site Recovery Manager 8.1.0.1 or later in an Enhanced Linked Mode**

  When you are using vSphere 6.7 and you upgrade Site Recovery Manager 8.1 to Site Recovery Manager 8.1.0.1 or later in an Enhanced Linked Mode, if the SRM service is restarted after the upgrade, the Site Recovery Manager server stops working. You receive the following error.

  ```
  YYYY-MM-DDT12:12:09.983+03:00 panic vmware-dr[04364] [SRM@6876 sub=Default] Application error: (sso.fault.NoPermission) {
  --> faultCause = (vmodl.MethodFault) null,
  --> faultMessage =
  --> msg = "Received SOAP response fault from [ ]: getDomains
  --> "
  --> }
  ```

  The Site Recovery Manager solution user must be recreated after upgrading from 8.1 to 8.1.0.1 or later versions.

  Workaround: Start the Site Recovery Manager installer and go through the modify workflow to recreate the user.

- **Virtual machines protected in a Storage Profile Protection Groups are not listed in the CSV file created when running the DR IP Customizer tool.**

  When you use the DR IP Customizer tool in a multiple vCenter Server environment, for example setup with federated PSCs where more then one vCenter Server instance is available on each site, you must specify the option `'--vcid UUID'` to be used to gather networking information about the virtual machines protected by Site Recovery Manager. If you provide the secondary site `vcid`, the DR IP Customizer tool connects to the secondary Site Recovery Manager server which does not store the network information for VMs protected with SPPGs. Providing the vcid from the secondary site results in connecting to the wrong vCenter Server and the VMs are not listed in the generated CSV file.

  Workaround: When using the DR IP Customizer tool, provide only the primary vCenter Server `vcid` and `uri`.

- **If you have Site Recovery Manager and vCenter Server deployment in Enhanced Linked Mode, after you run Site Recovery Manager installer in modify mode, the Site Recovery Manager servers are not connected**

  If you have Site Recovery Manager and vCenter Server deployed in Enhanced Linked Mode and you run the Site Recovery Manager installer in modify mode, it recreates the Site Recovery Manager solution users and this requires the reconfiguration of the SRM paring.

  Workaround: Reconfigure the pairing of the Site Recovery Manager servers.

- **Customization via IP subnet mapping rules is not fully supported for Linux VMs using multiple NICs with mixed DHCP and static IP configuration.**

  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 were observed for Red Hat Enterprise Linux 6.x/7.x and CentOS 6.x/7.x, where SRM 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.

  Workaround: For correct IP customization for Linux VMs using multiple NICs with mixed DHCP and static IP configuration, use the Manual IP Customization SRM option.

- **IP customization fails when you use special characters in the Recovery Plan name**

  When you run a Test Recovery for a Recovery Plan with special characters in the name and configured IP customization, the IP customization fails.

  Workaround: 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, especially in the Configure Recovery dialog.**

  You might experience performance degradation in the HTML 5 user interface on the recovery site, especially in the Configure Recovery dialog, if the protected vCenter Server is down.

  Workaround: Refresh the HTML 5 user interface on the recovery site and re-try your operation.

- **Remote vCenter Server is not displayed in the Summary tab after Site Recovery Manager upgrade**

  After you upgrade Site Recovery Manager to version 8.1 from an older SRM version, the remote vCenter Server field might be empty in the Site Pair>Summary screen.

  Workaround: Repair the corresponding site pair.

- **Storage DRS SRM warning is not displayed in the recommendations in a SDRS datastore cluster**

  When you run Storage DRS on a datastore cluster consisting of datastores that are from different consistency groups, SDRS does not display the Site Recovery Manager warning in the recommendations

- **Site Recovery Manager privileges are not localized in the vSphere 6.7 Client**

  Site Recovery Manager privileges are not localized in the vSphere 6.7 Client.

  Workaround: None.

- **When you restart the vCenter Server (vpxd) service, for a virtual machine that is already configured for replication with vSphere Replication, you are unable to reconfigure it**

  When you restart the vCenter Server (vpxd) service, for a virtual machine that is already configured for replication with vSphere Replication, the Site Recovery plug-in for vSphere Client wrongly reports that the VM is not configured for replication. As a result the Site Recovery plug-in is unable to reconfigure it. It allows only the Configure action, but its validation fails, because the VM is already configured for replication.

  Workaround: Use the Site Recovery HTML 5 standalone client to reconfigure the virtual machine.

- **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.

- **Folder names on VSAN datastores are displayed with UUIDs instead of friendly names in the virtual machine protection properties dialog**

  When you open the virtual machine protection properties dialog, the folder names on VSAN datastores are displayed with UUIDs instead of friendly names.

  Workaround: None

- **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

- **After you perform a failover, the virtual machine NICs at the disaster recovery site might remain disconnected**

  When you re-run a failover after an IP customization failure, the NICs of the VM on which the customization failed during the previous run might remain disconnected even after a successful customization in the current failover.

  Workaround: None. Manually reconnect the NICs by reconfiguring the VM devices.

- **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.

- **Configuring a new site pairing or a virtual machine for replication in the Site Recovery HTML 5 user interface might fail with an error**

  In the Site Recovery HTML 5 user interface, when configuring a new site pairing or a virtual machine for vSphere Replication, you might see the following error:

  ```
  "[PairSetupImpl { _server = HmsServerImpl { _guid = 9452f18d-e78c-49d2-afe4-d8374df60b7c _url = https://IP_ADDRESS:8043 } _pairServerGuid =
  6452f88d-e48c-49d2-afe4-d8374df90b7c _pairLsppUrl = https://FQDN:443/lookupservice/sdk _pairLsppsThumbprint =
  A9:57:9C:A7:C3:A8:31:2B:10:02:32:DC:9D:F7:AC:65:60:94:6A:E1:DF:FE:04:1C:D5:FD:A5:32:7C:E1:08:B3 }]"
  ```

  The issue is a result of legacy vSphere Replication Management Server registrations with field value vcUUID instead of vcUuid or improper cleanup of duplicate entries of old vSphere Replication Management Server registrations in the vCenter Server services.

  Workaround: Restart the vSphere Replication service on both sites. If you still see the issue, re-configure the site pairing.

- **When using Internet Explorer 11 or Edge browsers, you might notice slow performance in rendering while interacting with the Site Recovery UI.**

  You experience slow performance in rendering of the Site Recovery UI in Internet Explorer 11 and Edge browsers.

  Workaround: Use Chrome or Firefox browsers.

- **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 Recovey 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.

- **If a consistency group is skipped on a storage policy protection group failover, the reprotect might fail**

The reprotect operation searches for the skipped consistency group and fails to reverse replication on it.

Workaround: Delete the storage policy protection group and recreate it only with the recovered LUNs.

- **Site Recovery Manager Server might crash if you re-enable recovery of a VM**

  You can disable recovery of a VM if the recovery operation for the VM fails. If you run a recovery plan and the recovery fails, you can re-enable the recovery of the VM and rerun the recovery, but Site Recovery Manager Server crashes.

  Workaround: Start Site Recovery Manager Server and disable the recovery of the VM.

- **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.

- **Site Recovery Manager uses the default value of the remoteSiteStatus.drPanicDelay setting even if you changed the value**

  Even if you set a custom value for the delay between a not responding event and a site down event, the drPanicDelay has a default value in the Tasks view.

  Workaround: Change the value of the remoteSiteStatus.drPanicDelay setting and restart Site Recovery Manager Server.

- **Site Recovery Manager uses the default value of the remoteSiteStatus.drPingFailedDelay setting even if you set a custom value**

  Even if you set a custom value for remoteSiteStatus.drPingFailedDelay, the setting has a default value in the Tasks view.

  Workaround: Set the custom value for the remoteSiteStatus.drPingFailedDelay setting and restart Site Recovery Manager Server.

- **A VM and a consistency group assigned to a deleted storage policy appear in the Virtual Machines and Consistency Groups tabs**

  If you delete a storage policy, the VMs and the consistency group that are assigned to the storage policy appear in the Virtual Machines and Consistency Groups tabs to the SPPG group.

  Workaround: Recreate the storage policy protection group. After you recreate the group the VMs and consistency group do not appear in the Virtual Machines and Consistency Groups tabs.

- **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.

- **A Test Recovery Fails with the `Cannot create a test bubble image for group` message**

  If you have a VM with multiple disks that are replicated with vSphere Replication to different vSphere Virtual Volumes datastores on the secondary site, a test recovery operation fails. During a test recovery, vSphere Replication tries to create Linked Clones for the vSphere Virtual Volumes replica disks, but the operation fails because Linked Clones across different datastores are not supported. vSphere Replication creates Linked Clones only during a test recovery. The planned recovery, unplanned recovery, and reprotect complete successfully.

  Workaround: A test recovery operation using vSphere Virtual Volumes disks pass successfully only if all disks are replicated to the same vSphere Virtual Volumes datastore on the secondary site.

- **The First Attempt for Recovery of VMs placed on vSphere Virtual Volumes might fail during the customization steps**

  Site Recovery Manager cannot recognize old VMware Tools versions installed on VMs placed on vSphere Virtual Volumes storage during the first recovery attempt. You might observe the following failures that depend on the VMware Tools version installed on the recovered VMs.
  `Vim::Fault::OperationNotSupportedByGuest : "The guest operating system does not support the operation." Vim::Fault::InvalidGuestLogin : "Failed to authenticate with the guest operating system using the supplied credentials.`

1. Rerun the failed recovery plan or clean the test plan up and rerun the test recovery again.
2. Update VMware Tools to the latest version for all VMs placed on vSphere Virtual Volumes storage.

- **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.
    1. Right-click the recovered VM.
    2. Click **Edit** Settings.
    3. In the **Options** tab, click **General**.
    4. Click **Configuration** to update the configuration parameters.
    5. Click **Add Row** and enter `time.synchronize.tools.startup.backward` in the **Name** text box and `TRUE` in the **Value** text box.
    6. 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 8.1 Administration* guide.

- **Valid vCenter Server addresses might not be listed as possible targets when you install Site Recovery Manager**

  If there are duplicated vCenter Server addresses in your environment due to multiple service registrations of one vCenter Server with different versions, a valid address might not be listed. Site Recovery Manager writes an error for duplicated key in its installation log file.

  The following error message appears in the installation log file of your Site Recovery Manager:

  ```
  VMware: Srm::Installation::XmlFileHandler::GetElementMap: INFORMATION: Inserted key 'xxxxxx' and value '76B00E54-9A6F-4C13-8DD9-5C5A4E6101E3'

  VMware: Srm::Installation::XmlFileHandler::GetElementMap: INFORMATION: Inserted key 'xxxxxx' and value 'default-first-site:b84bcef3-85fb-4d92-8204-2392acf0088d'

  VMware: Srm::Installation::XmlFileHandler::GetElementMap: ERROR: Duplicate key 'xxxxxx' exists
  ```

  Workaround: See https://kb.vmware.com/kb/2145520.

- **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.

- **Disaster recovery for a VM that is attached to a VSS network shows the protected site network in the UI for temporary placeholder network mappings.**

  If you use a VSS network for which you have not configured a regular network mapping and you run disaster recovery on a recovery plan that contains a storage policy protection group, Site Recovery Manager creates a temporary placeholder mapping for this network. When you complete the temporary placeholder mapping, a network might appear on the secondary site that has the same name as the network on the primary site. If you did not explicitly create this network, it is not a genuine network. However, it is possible to select it as the target for the temporary placeholder mapping and recovery will succeed. The network is then displayed as inaccessible after the recovery completes, even though the recovered VMs are shown as being connected to this network on the recovery site.

  Workaround: After the recovery, manually map the VMs to a different network and connect them to a genuine network.

- **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 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.
- **When you edit a temporary placeholder mapping, you might see error `The specified key, name, or identifier '6458aed1-6c80-4565-907f-189e6a102046' already exists.`**

  This error can occur when a regular mapping for the same protected site inventory object exists.
- **Renaming a datastore associated with a protected virtual machine can result in loss of protection and recovery settings.**

  A protected virtual machine can lose its protection status as well as recovery settings when you rename the datastore associated with the virtual machine. First shut down the Site Recovery Manager server, then rename datastores to avoid losing recovery settings for the virtual machine.

  Workaround: To restore the protection status, restart the protected site Site Recovery Manager server or remove the affected datastore from the protection group and then add it back, then reconfigure recovery settings.
- **Site Recovery Manager displays incorrect names for some protected site objects in placeholder mappings.**
    - Datacenters display the name **vm** instead of the user-defined datacenter name.
    - Resource pools display the name **Resources** instead of the user-defined resource pool name.
    - If you move a virtual machine to another folder or resource pool after protecting the virtual machine in a storage profile protection group, the placeholder mappings generated after the move display internal IDs such as **folder-3** or **resgroup-5** instead of the user-defined object names.

  Workaround: There is no workaround for incorrect object names in inventory mappings. Check the history report from the failed test or recovery workflow that caused the placeholder mappings to be created. For example, if you know the protected site inventory, you can determine the protected site datacenter, folder, and resource pool that contained the protected virtual machine that failed to recover due to a missing mapping.
- **When you run a planned migration with vMotion disabled on a stretched storage with static site bias, the operation might fail during the storage sync step.**

  Workaround: After the planned migration fails in the first attempt, manually run discover devices and rerun the operation.
- **After the recovery plan workflow completes, the last recovery steps continue to show a "Running" status.**

  The incorrect status is a transient UI problem. Site Recovery Manager executes all the steps to completion.

  Workaround: 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.**

  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.

  Workaround: Click the global refresh icon to refresh the interface. All callouts reappear in the list of steps.
- **When the storage array fails at the protected site, Site Recovery Manager cannot recover virtual machines in storage profile protection groups.**

  The virtual machines become unprotected but the data is still protected.

  Workaround: Manually recover the datastores and virtual machines at the recovery site.
- **Site Recovery Manager installation fails if the Platform Services Controller certificate has expired.**

  When connecting to Platform Services Controller during Site Recovery Manager installation, you can accept the Platform Services Controller certificate even if it has expired or is not yet valid. The installation then fails at the step when you select the vCenter Server instance to connect to, with the error `Failed to validate vCenter Server. Details: Internal error: unexpected error code: -1`. The same error occurs if the Platform Services Controller certificate expires after you install Site Recovery Manager and you run the Site Recovery Manager installer in Modify mode. If

Workaround: Replace the Platform Services Controller certificate and attempt installation again.

- **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 SRM 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.

  Workaround: Delete the placeholder virtual machine and remove the orphaned virtual machine, then create the protection group with the same virtual machine.

- **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.

- **Rerunning reprotect fails with error: `Protection Group '{protectionGroupName}' has protected VMs with placeholders which need to be repaired.`**

  If a **ReloadFromPath** operation does not succeed during the first reprotect, the corresponding protected virtual machines enter a **repairNeeded** state. 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 **ReloadFromPath** operation failed.

  Workaround: Rerun reprotect with the **force cleanup** option enabled. This option completes the reprotect operation and enables the **Recreate placeholder** option. Click **Recreate placeholder** to repair the protected virtual machines and to restore the placeholder virtual machines.

- **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 then cancel 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.

- **Cancellation of Recovery Plan Not Completed**

  When a recovery plan is run, 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. The following options can be used 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, the recovery plan can be run 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.

- **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.

- **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.

- **Running a planned migration of a recovery plan with no protected virtual machines leaves the environment in an unusable state.**

  When a protection group contains no virtual machines and you run a recovery plan of this protection group in planned migration mode from the remote Site Recovery Manager server, the operation fails. The plan goes into Incomplete Recovery state and cannot be deleted and the LUN disconnects from both protection and recovery hosts.

  Workaround: To restore the environment, delete the protection group and recovery plan and manually reconfigure the LUN using SAN management interface.

- **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.

- **Running a recovery plan fails with a virtual machine error in the Configure Storage step.**

  Subsequent runs of the recovery plan fail at the same Configure Storage step for the same virtual machine with the error `The specified key, name, or identifier already exists.`. If you look in the vCenter Server Inventory, you see two virtual machines with the same name as the failed virtual machine, one of which is in the Discovered Virtual Machines folder. This problem is caused by a known communication issue between vCenter Server and the ESXi Server instance.

  Workaround: Unregister the duplicate virtual machine in the Discovered Virtual Machines folder from vCenter Server. After completing this for all affected virtual machines, re-run the recovery plan.