VMware Site Recovery Manager 6.0.0.x Release Notes

Updated on 02/15/2021

Site Recovery Manager 6.0.0.1 | 30 APR 2015 | Build 2700459

Site Recovery Manager 6.0 | 12 MAR 2015 | Build 2580226

Last updated: 24 FEB 2017

Check for additions and updates to these release notes.

For information about Site Recovery Manager 6.0.0.x patch releases, see the corresponding section of these release notes.

- Site Recovery Manager 6.0.0.1 Express Patch Release

What's in the Release Notes

These release notes cover the following topics:

What's New in Site Recovery Manager 6.0

VMware vCenter Site Recovery Manager 6.0 provides the following new features:

- Support for VMware vSphere 6.0, including integration with shared infrastructure components such as Platform Services Controller and vCenter Single Sign On.
- Support for Storage vMotion and Storage DRS on both the protected and recovery sites.
- Protection and recovery of virtual machines in IPv6 environments.
- IP customization enhancements to support dual-protocol IP configurations and independent IPv4 and IPv6 configurations.

Localization

VMware vCenter Site Recovery Manager 6.0 is available in the following languages:

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

Compatibility

Site Recovery Manager Compatibility Matrix

For interoperability and product compatibility information, including supported guest operating systems and support for guest operating system customization, see the Compatibility Matrixes for VMware vCenter Site Recovery Manager 6.0.

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 Virtual SAN Support

Site Recovery Manager 6.0 can protect virtual machines that reside on VMware Virtual SAN by using vSphere Replication. Virtual SAN does not require a Storage Replication Adapter (SRA) to work with Site Recovery Manager 6.0.

VMware VSA Support

Site Recovery Manager 6.0 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 6.0.

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 **Solution Upgrade Path** and **VMware vCenter Site Recovery Manager** in the VMware Product Interoperability Matrixes.

NOTE: 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. For information about uninstalling then reinstalling Site Recovery Manager, see http://kb.vmware.com/kb/2110280.

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 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 http://kb.vmware.com/kb/2103394.

Operational Limits for Site Recovery Manager 6.0

For the operational limits of Site Recovery Manager 6.0, see http://kb.vmware.com/kb/2105500.

Site Recovery Manager SDKs

For a guide to using the Site Recovery Manager SOAP-based API, see VMware vCenter Site Recovery Manager API.

Open Source Components

The copyright statements and licenses applicable to the open source software components distributed in Site Recovery Manager 6.0 are available at VMware vCenter Site Recovery Manager Downloads. You can also download the source files for any GPL, LGPL, or other similar licenses that require the source code or modifications to source code to be made available for the most recent generally available release of vCenter Site Recovery Manager.

Caveats and Limitations

- Site Recovery Manager 6.0 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 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 6.0 does not support the protection of virtual machines that are configured with multiple-CPU vSphere Fault Tolerance (FT). Site Recovery Manager 6.0 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 do use multi-CPU vSphere FT on virtual machines, Site Recovery Manager does not deactivate vSphere FT on the recovered

  - If you do use multi-CPU vSphere FT on virtual machines, Site Recovery Manager does not deactivate vSphere FT on the recovered virtual machines and powering on those virtual machines fails. You must manually deactivate vSphere FT on the recovered virtual machines by removing FT properties and run the recovery plan again.
  - If you use uni-processor vSphere FT on a virtual machine, you must configure the virtual machine 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.
- **NEW** vSphere Replication 6.0 supports replication of virtual machines on Virtual Volumes (vVols) with limitations. Site Recovery Manager 6.0 does not support the protection of virtual machines on Virtual Volumes, even if you use vSphere Replication as the replication technology for protection.
- **NEW** Site Recovery Manager 6.0 does not support NFS v 4.1 datastores for array-based replication. You can use Site Recovery Manager 6.0 with NFS v 4.1 datastores for vSphere Replication.
- **NEW** An adjustment of **+1 second** is scheduled for **23:59 UTC** on **30th June 2015**. This adjustment does not affect Site Recovery Manager but it does affect the vSphere Replication appliance. For more information, see http://kb.vmware.com/kb/2115818.

Available Patch Releases

The Site Recovery Manager 6.0.0.x express patch releases resolve problems that have been encountered after the initial 6.0.0 release. You obtain the patch releases from the Site Recovery Manager Downloads page at http://www.vmware.com/go/download-srm.

Site Recovery Manager 6.0.0.1 Express Patch Release

Released 30 APR 2015 | Build 2700459

The Site Recovery Manager 6.0.0.1 Express Patch Release resolves the following issue:

When upgrading from Site Recovery Manager 5.8 to Site Recovery Manager 6.0, the upgrade might fail with the error `VMware vCenter Site Recovery Manager service failed to start. Check that all required Windows services are running. View the server log for more information.`

Alternatively, the upgrade might succeed but then the Site Recovery Manager Server on both sites stops unexpectedly soon after the upgrade. The error `Panic: VERIFY d:\build\ob\bora-2580226\srm\public\common/typedMoRef.h:498` appears in the Site Recovery Manager Server logs.

This issue occurs if you had protected virtual machines in the following fashion in your Site Recovery Manager 5.8 installation:

- You protected a virtual machine that includes a non-replicated, file-backed, or disk-backed device.
- You specified a recovery location for any of these non-replicated devices.

The devices that are affected by this issue include ISO images, floppy images, hard disks, and RDMs.

The Site Recovery Manager 6.0.0.1 express patch release resolves the issue described in KB 2111069.

Installation Notes

If you are running Site Recovery Manager 6.0.0, upgrade to Site Recovery Manager 6.0.0.1. See Upading Site Recovery Manager in *Site Recovery Manager 6.0 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you have already upgraded from Site Recovery Manager 5.8 to Site Recovery Manager 6.0.0 and you have encountered this issue, contact VMware Support.

If you use vSphere Replication with Site Recovery Manager 6.0.0, upgrade the vSphere Replication appliance to version 6.0.0.1. See the vSphere Replication 6.0.0.x Release Notes for information about vSphere Replication 6.0.0.1.

Known Issues

The following known issues have been discovered through rigorous testing and will help you understand some behavior you might encounter in this release.

- **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.
- **NEW IP Customization and Callout fails when SRM 6.0.x recovers virtual machines with installed VMTools 10.1.x.**

  When Site Recovery Manager is running IP customization and Callouts on recovered virtual machines with installed VMTools 10.1.x, you see the following error: `"Unexpected error '3051' when communicating with ESX or guest VM: The authentication type used was disabled in the guest operating system"`.

  Workaround: Upgrade to Site Recovery Manager 6.1.2 or 6.5, or use VMTools 10.0.9 on the recovered virtual machines.
- **When the protected site is offline, newly created recovery plans only appear in the Inventory Trees view.**

If the protected site is offline and you create a new recovery plan from the recovery site, the new plan does not appear in the Inventories > Recovery Plans view in the Site Recovery Manager interface. The new plan is visible in the Inventory Trees > Recovery Plans view.

Workaround: None

- **Site Recovery Manager messages in the vSphere Web Client are malformed and not localized.**

  If you have installed vCenter Server 6.0 with non-default ports, and you install Site Recovery Manager 6.0 or upgrade Site Recovery Manager 5.x to Site Recovery Manager 6.0, Site Recovery Manager messages in the vSphere Web Client are malformed and are not localized correctly.

  Workaround:

  1. Log into the vCenter Server host machine.
  2. In a text editor, open the `SRM_GUID_com.vmware.vcDr.properties` file for the vCenter Server instance.

     You find the `SRM_GUID_com.vmware.vcDr.properties` file in the following location:
     - vCenter Server on Windows:

       `C:\ProgramData\VMware\vCenterServer\cfg\sca\services\`

       `SRM_GUID_com.vmware.vcDr.properties`
     - vCenter Server Appliance:

       `/etc/vmware-sca/services/`

       `SRM_GUID_com.vmware.vcDr.properties`
  3. Update the `resourcebundle.location` value to add the custom port:
     - Old value:

       `resourcebundle.location=`

       `https\://SRM_Server_address/catalog/com.vmware.vcDr_catalog.zip`
     - New value:

       `resourcebundle.location=`

       `https\://SRM_Server_address:custom_port/catalog/com.vmware.vcDr_catalog.zip`
  4. Log out of the vSphere Web Client and log back in again.

- **Virtual machine recovery properties wizard displays an error when dependent virtual machines are not present in a recovery plan.**

  If you have configured dependencies between virtual machines, and a dependent virtual machine is in a protection group that is not included in the same recovery plan, when you open the virtual machine recovery properties wizard for the virtual machine with the dependency, the wizard displays the error `com.vmware.vim.vmomi.core.exception.MarshallException: Invalid value for field "vmIdentities": array contains null at index 0`.

  For example, this situation can occur in the following circumstances:

  - VM-1 is in protection group PG-1, which is included in recovery plan RP-1.
  - VM-2 is in protection group PG-2, which is not included in recovery plan RP-1.
  - VM-1 has a dependency on VM-2.
  - You attempt to edit the recovery properties of VM-1

  This error only affects the recovery properties wizard, and does not affect recovery itself because Site Recovery Manager skips invalid dependencies during recovery.

  Workaround: Add the protection group that contains the virtual machine that another virtual machine depends upon to the recovery plan that contains the dependent virtual machine. The recovery properties wizard functions correctly when both protection groups are in the same recovery plan. If you do not want the two protection groups to be in the same recovery plan, you must remove the dependency. You can temporarily move the protection group into the same recovery plan so that you can remove the dependency:

  1. Add the protection groups that contain virtual machines that other virtual machines depend on to the same recovery plan as the dependent virtual machines. For example, add PG-2 to RP-1.
  2. Edit the recovery properties of the dependent virtual machines to remove the dependencies. For example, edit VM-1 to remove the dependency on VM-2.
  3. Remove the protection groups that contain the virtual machines that other virtual machines previously depended on from the recovery plan. For example, remove PG-2 from RP-1.

- **vSphere Replication operations fail when there is heavy replication traffic.**

  If you recover virtual machines that you protect by using vSphere Replication, reprotect might fail with the error `Unable to reverse replication` and other operations might fail with `java.net.UnknownHostException`. These errors occur because DNS requests get dropped due to network congestion.

  Workaround: See the vSphere Replication 6.0 Release Notes.

- **Cannot add or edit array managers when multiple Site Recovery Manager pairs exist and the Site Recovery Manager user account does not have privileges for all Site Recovery Manager instances on a site.**

If you have multiple Site Recovery Manager pairs, each of which is accessed by a different user account, and if user accounts do not have privileges for all Site Recovery Manager instances on a site, none of the users can add or edit array managers on any of the pairs. This is true even if the user has the correct privileges for the pair on which they are attempting to add or edit an array manager.

Workaround: Assign privileges to each user for all Site Recovery Manager instances on a site.

- **Site Recovery Manager fails to trust certificates from vCenter Server after upgrading from version 5.1 or earlier to 6.0.**

  If you upgrade vCenter Server and Site Recovery Manager from version 5.1 or earlier to version 6.0, vCenter Server upgrade might fail because version 6.0 fails to trust the certificate from the older version of vCenter Single Sign-On.

  After you successfully upgrade vCenter Server to 6.0 and perform the two-step upgrade of Site Recovery Manager from version 5.1 or earlier to version 5.5 then to version 6.0, reconfiguring the connection between the sites might fail.

  Workaround:

  1. To allow the vCenter Server upgrade to succeed, copy the root vCenter Single Sign-On certificate into the vCenter Server certificate store.
  2. After upgrading vCenter Server and Site Recovery Manager to version 6.0, attempt to connect the sites by running **Repair Connection** from the other site.
  3. If connection still fails, import the trusted CA certificates for the vCenter Single Sign-On and vCenter Server instances on the recovery site into the truststore of the Site Recovery Manager Server on the protected site, and the reverse. This allows both Site Recovery Manager Server instances to trust their respective remote vCenter Single Sign-On and vCenter Server.
- **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 results 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.
- **Changing the Site Recovery Manager license from one type to another causes the usage count in the Licensing view of vSphere Web Client to become out-dated.**

  If you change the Site Recovery Manager license type, for example from a virtual machine-based license to a per-CPU license, the license usage count that the Licensing view of the vSphere Web Client displays can continue to display the old information. This is a UI error, and Site Recovery Manager functions correctly with the new license.

  Workaround: Attempt whichever of the following workarounds is most appropriate.

  - Delete the affected Site Recovery Manager solution asset from the **Licensing** > **Licenses** > **Assets** view in the vSphere Web Client, then wait 5 to 10 minutes for vCenter Server to automatically restore Site Recovery Manager in the Licenses view.
  - Protect a virtual machine, if your license permits it.
  - Remove protection from a virtual machine, if you have virtual machines that are already protected.
  - Restart the Site Recovery Manager service.
- **Planned migration after recovery and reprotect fails with the error `Failed to recover datastore` *`datastore_name`*`. VMFS volume residing on recovered devices` *`device_name`* `cannot be found`.**

  If you use Site Recovery Manager to protect datastores on arrays that support dynamic swap, running a disaster recovery when the protected site is partially down or running a force recovery can lead to errors when you attempt to restore the protected site by running planned migration after the recovery and reprotect operations. If you were obliged to manually shut down virtual machines on the protected site during the disaster recovery or forced recovery, Site Recovery Manager is unable to locate the datastore that contains the protected virtual machines.

  Workaround: Reboot the ESXi hosts on the protected site that includes the datastores and run planned migration again.
- **Site Recovery Manager operations fail to unmount datastores.**

  When you run Site Recovery Manager operations that unmount datastores, such as planned migration or test cleanup, the cleanup operation fails to unmount the datastores on the recovery site, with the error `Cannot unmount datastore` *`datastore_name`* `from host` *`host_name`*.

  Workaround: Run the operation again.
- **Inventory Mapping wizard shows an empty inventory after you change a trusted vCenter Server certificate on the remote site.**

  If you have a setup that uses trusted certificates for vCenter Server on both the protected and recovery sites, and if you change the vCenter Server certificate for one of the sites while logged into the Site Recovery Manager interface for the other site and then attempt to configure resource mappings, the Inventory Mapping wizard shows an empty inventory on the remote site.

  Workaround: Log out of the vSphere Web Client and log in again.
- **Adding an array manager fails when the remote site is down or the remote Site Recovery Manager Server has stopped.**

  When you log in to the vSphere Web Client at the primary site and authenticate with Site Recovery Manager at the remote site, if the remote site is down or the remote SRM Server has stopped, you cannot add an array manager and the array manager wizard waits indefinitely. In a setup of multiple Site Recovery Manager servers registered to a single vCenter Server and the local Site Recovery Manager server is down, the array manager wizard waits indefinitely.

Workaround: Log out and log in to the vSphere Web Client and add the array manager again.

- **Virtual machines in a vSphere Replication protection group show up erroneously as Not Configured in the protection group Summary tab in vSphere Web Client.**

  Information about the protection status of virtual machines in a vSphere Replication protection group can differ in different views in vSphere Web Client.

  - If you view the protection status of the virtual machines in a vSphere Replication protection group in the **Site Recovery** > **Protection Groups** > *Protection Group* > **Related Objects** > **Virtual Machines** view of the vSphere Web Client, all correctly configured virtual machines show the status OK.
  - If you look at the **Site Recovery** > **Protection Groups** > *Protection Group* > **Summary** tab for the same protection group, the Protection Group Details panel might erroneously show a number of virtual machines in the Not Configured row, even if the status of all of the virtual machines in the **Related Objects** > **Virtual Machines** view was OK.

  An error in the caching of information from the vSphere Replication server by vSphere Web Client can sometimes cause the Summary tab to display out-dated error information.

  Workaround: Check the **Site Recovery** > **Protection Groups** > *Protection Group* > **Related Objects** > **Virtual Machines** view of the vSphere Web Client. The virtual machine statuses presented in this view are always correct.

- **Site Recovery Manager disappears from the vSphere Web Client.**

  In a setup with federated vCenter Single Sign-On, Site Recovery Manager can disappear from the vSphere Web Client for one of the following reasons:

  - You log in to either the protected site or the recovery site and the Platform Services Controller for that site is offline. The plug-in that was loaded last time you logged in is not deployed because a Platform Services Controller, vCenter Server, or Site Recovery Manager Server instance on that site that serves the Site Recovery Manager plug-in might be offline.
    Workaround: Restart the vSphere Web Client service.
  - You installed Site Recovery Manager in a shared recovery site configuration, and you uninstalled one of the Site Recovery Manager instances that is registered with vCenter Server on the shared site. If you deleted all Site Recovery Manager data when you uninstalled the Site Recovery Manager Server instance, Site Recovery Manager disappears from the vSphere Web Client. None of the remaining Site Recovery Manager instances is available.
    Workaround: Restart the vSphere Web Client service.
  - Site Recovery Manager Server on either the protected or the recovery site is offline. In this case, vSphere Web Client should download the Site Recovery Manager client plug-in from the remaining active site, but does not do so.
    Workarounds: Attempt these workarounds in order.
    1. Restart the Site Recovery Manager Server instance that is offline, or repair the connection between Site Recovery Manager Server and Platform Services Controller.
    2. If you cannot bring Site Recovery Manager Server online, uninstall and reinstall this instance of Site Recovery Manager Server.
    3. If you cannot uninstall Site Recovery Manager Server, for example because the virtual machine that it runs in cannot be started, unregister the Site Recovery Manager Server extension from the Managed Object Browser (MOB) of the vCenter Server instance for this site. You must then reinstall Site Recovery Manager.

- **Site Recovery Manager installer shows misleading message if vSphere Replication validation fails.**

  If the vCenter Server instance on which you are installing Site Recovery Manager has a vSphere Replication extension, the Site Recovery Manager installer checks the version of vSphere Replication and stops the installation if the vSphere Replication version is incompatible. The installer then checks whether vSphere Replication is running. If vSphere Replication is not running, the installer displays the error `Failed to validate HMS. Cannot connect to HMS. Perhaps the network is down or the host is powered off. Press Retry to try again or press Cancel to exit installation.` Clicking Retry shows the message again. Clicking Cancel dismisses the warning and allows the Site Recovery Manager installation to continue. The error message is incorrect. Continuing the Site Recovery Manager installation if vSphere Replication is of the correct version but is not running is the correct behavior.

- **Operations fail but Site Recovery Manager does not issue a warning or error when the vCenter Server certificate has expired.**

  If the vCenter Server certificate has expired, Site Recovery Manager operations fail but no warning or error appears in the vSphere Web Client. The following error appears in the Site Recovery Manager logs:

```
[01460 warning 'Default'] Dr::Internal::StubExcTranslator :
Error while calling stub for 'dataservice.authentication.SessionManager:sessionManager'
[...]
--> The remote host certificate has these problems:
-->
```

```
--> * A certificate in the host's chain is not time-valid.
-->
--> * The certificate is not time-valid.
-->
--> * unable to get local issuer certificate"
```

- **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 happens 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 the Platform Services Controller certificate expires after you have installed Site Recovery Manager, different errors can also appear in the Site Recovery Manager interface.

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

- **Site Recovery Manager does not issue a warning or error when its certificate has expired or is about to expire.**

  If the Site Recovery Manager certificate has expired, no warnings or errors are displayed when you log into Site Recovery Manager. Certain operations become impossible if the certificate has expired.

  Workaround: Configure vCenter Server to trigger alarms for the following Site Recovery Manager events related to certificate validity:

  - `SrmCertificateNotValidEvent`
  - `SrmCertificateExpiredEvent`
  - `SrmCertificateEvent`

  See Site Status Events for information about these events. You can also adjust the time period before a certificate expires that Site Recovery Manager issues a certificate expiry event by modifying the `localSiteStatus.minCertRemainingTime` advanced setting. See Change Local Site Settings in *Site Recovery Manager Administration* for information about this setting.

- **Certain Site Recovery Events do not display correctly.**

  When viewing Site Recovery Manager events in the Events view in vSphere Web Client, certain events include the text [data.planName] instead of the name of the recovery plan. This issue affects the following storage events:

  - `SPVmDsProtConflictEvent`
  - `SPVmDsProtMissingEvent`
  - `SPVmDsReplicationLostEvent`
  - `SPVmProtRestoredEvent`
  - `StorageRdmDiscoveredEvent`
  - `StorageRdmLostEvent`

  In addition, the following events display correctly in English but do not display correctly in non-English locales:

  - `PlanVmCommandBegin`
  - `PlanVmCommandEnd`
  - `RecoveryVmBegin`
  - `RecoveryVmEnd`

- **In a setup with federated vCenter Single Sign-On, if a vCenter Server instance is offline, no information appears in the Site Recovery Manager interface for this site.**

  When you connect to vSphere Web Client in a federated vCenter Single Sign-On setup, if one of the vCenter Server instances is offline, this vCenter Server instance does not appear, and no warning or error is displayed. This results in empty views in the Site Recovery Manager interface for this site. The vCenter Server instance does not reappear in the interface even if it comes back online. All calls to this vCenter Server instance from Site Recovery Manager fail.

  Workaround: Log out of the vSphere Web Client and log in again.

- **Site Recovery Manager log files fail to download when the site name contains special characters \ / : ? * | " < >.**

  Workaround: Rename the site without using special characters.

- **In a setup with federated vCenter Single Sign-On, Site Recovery Manager fails to initiate recovery on any plan when the protection node is down in the same session.**

  Workaround: When a topology changes in a setup with federated vCenter Single Sign-On, log out and log in to the vSphere Web Client.

- **In a setup with federated vCenter Single Sign-On, if the remote site or remote Platform Services Controller service is down, Site Recovery Manager fails to load objects in the inventory.**

  Workaround: Log out and log in to the remote vSphere Web Client.

- **In a setup with federated vCenter Single Sign-On when pairing sites, Site Recovery Manager does not show an error when one of the**

solution users fails to replicate to the secondary vCenter Single Sign-On instance.

Workaround: Reboot the virtual machine with primary and secondary Platform Services Controllers.

- **Virtual machine status does not change after restoring placeholder.**

  Virtual machines and protection groups stop monitoring changes to their peers when they complete the deactivate operation. If the placeholder VM is missing when the deactivate operation runs, the protected site always reports it missing even if the placeholder VM is repaired on the recovery site for that protected VM. The recovery site UI should be aware of the placeholder being repaired and allow failover to succeed.

  Workaround: For a deactivated protected VM that says the placeholder is missing even if you repaired it, check the protected VM status on the recovery site instead of on the protected site.
- **vSphere Replication UI does not appear in vSphere Web Client if you upgraded vCenter Server and vSphere Replication to version 6.0 but you did not upgrade Site Recovery Manager to 6.0.**

  When you upgrade vCenter Server 5.5U2 to 6.0, vSphere Replication 5.8 to 6.0, and Site Recovery Manager 5.8 is registered with vCenter Server but not upgraded, vSphere Replication starts successfully but the vSphere Replication interface does not appear in vSphere Web Client.

  Workaround: Upgrade Site Recovery Manager 5.8 to 6.0, or uninstall Site Recovery Manager 5.8. Restart the vSphere Web Client.
- **Placeholder virtual machine on 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 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.
- **In a setup with federated vCenter Single Sign-On, Site Recovery Manager roles do not appear in the list of roles.**

  During Site Recovery Manager installation, the installer creates privileges and roles for Site Recovery Manager that do not synchronize successfully between sites. vCenter Server receives the list of roles before the list of privileges and rejects the roles.

  Workaround: Restart the vpxd services that failed to register the Site Recovery Manager roles.
- **When moving protection groups in the root folder, Site Recovery Manager throws a flex exception.**

  Workaround: Dismiss the exception and perform a global refresh to reload the vSphere Web Client.
- **When Site Recovery Manager server disconnects with vCenter inventory service, the Site Recovery Manager user interface does not display the appropriate error notification.**

  You can perform actions such as removing protection from a virtual machine, but Site Recovery Manager Server fails to push data to the inventory server and sends errors. However, the actions do succeed.

  Workaround: Check the vCenter Server instance that posted the event that the inventory service cannot connect to Site Recovery Manager. Investigate the cause of the broken connection between Site Recovery Manager and the inventory service, and restore the connection.
- **On Windows 8 or Windows 8.1 using Internet Explorer versions 10 and 11, when you change the user locale to Chinese, the vSphere Web Client displays Site Recovery Manager in English.**

  Workaround: Use Chrome or Firefox.
- **Site Recovery Manager plugin does not display in the vSphere Web Client if Site Recovery Manager service stops.**

  After you install Site Recovery Manager and the service stops for any reason, the vSphere Web Client does not display the Site Recovery Manager plugin.

  Workaround: Restart the vSphere Web Client.
- **Site Recovery Manager stops during an attempt to protect an already reprotected array-based virtual machine using vSphere Replication.**

  If you run a recovery, then try to use vSphere Replication to protect a virtual machine already protected by an array-based protection group, Site Recovery Manager Server asserts a licensing alert.

  Workaround: Restart Site Recovery Manager Server and unprotect the array-based protected virtual machine first before protecting with vSphere Replication. Alternatively, continue with array-based protection and do not not protect with vSphere Replication. Site Recovery Manager does not support protecting with both providers.
- **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 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.
- **When protection site LUNs encounter All Paths Down (APD) or Permanent Device Loss (PDL), Site Recovery Manager might not recover raw disk mapping (RDM) LUNs in certain cases.**

  During the first attempt at planned migration you might see the following error message when Site Recovery Manager attempts to shut down the protected virtual machine:

  ```
  Error - The operation cannot be allowed at the current time because the virtual machine has a question pending:
  'msg.hbacommon.askonpermanentdeviceloss:The storage backing virtual disk VM1-1.vmdk has permanent device loss. You might be able to hot
  remove this virtual device from the virtual machine and continue after clicking Retry. Click Cancel to terminate this session.
  ```

  If the protected virtual machines have RDM devices, in some cases Site Recovery Manager does not recover the RDM LUN.

  Workaround:

  1. When LUNs enter APD/PDL, ESXi Server marks all corresponding virtual machines with a question that blocks virtual machine operations.
     a. In the case of PDL, click **Cancel** to power off the virtual machine.
     b. In the case of APD, click **Retry**.

     If you run planned migration, Site Recovery Manager fails to power off production virtual machines.
  2. If the virtual machines have RDM devices, Site Recovery Manager might lose track of the RDM device and not recover it. Rescan all HBAs and make sure that the status for all of the affected LUNs has returned from the APD/PDL state.
  3. Check the vCenter Server inventory and answer the PDL question that is blocking the virtual machine.
  4. If you answer the PDL question before the LUNs come back online, Site Recovery Manager Server on the protected site incorrectly detects that the RDM device is no longer attached to this virtual machine and removes the RDM device. The next time you run a recovery, Site Recovery Manager does not recover this LUN.
  5. Rescan all HBAs to make sure that all LUNs are online in vCenter Server inventory and power on all affected virtual machines. vCenter Server associates the lost RDMs with protected virtual machines.
  6. Check the **Array Managers** tab in the Site Recovery Manager interface. If all the protected datastores and RDM devices do not display, click **Refresh** to discover the devices and recompute the datastore groups.
  7. Make sure that **Edit Group Settings** shows all of the protected datastores and RDM devices and that the virtual machine protection status does not show any errors.
  8. Start a planned migration to recover all protected LUNs, including the RDM devices.
- **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 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

    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 re-running 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.

- **IP Customization fails due to a timeout when uploading customization scripts to virtual machines via the VIX API.**

  Uploading IP customization scripts to virtual machines by using VIX when running recovery plans fails with a timeout.

  Workaround: None.

- **New users with native high-ASCII password cannot log in using vSphere Web Client.**

  When a new user attempts to log in for the first time using the vSphere Web Client with a high-ASCII password in French and German locales, the log in attempt fails.

  Workaround: Log in as a vSphere Single Sign On (SSO) administrator and add any single ASCII character to the new user's existing high-ASCII password.

- **Planned migration fails during vSphere vMotion with an error at the "Shutdown VMs at protected site" step.**

  During planned migration, if an vSphere vMotion of a protected virtual machine is in progress when the "Shutdown VMs at protected site" step starts, the step might fail with the error `Error - The attempted operation cannot be performed in the current state (powered on)`. This occurs because `hostd` fails the shut down and power off operations during virtual machine migration. This has been fixed.

- **The embedded database server stores the database credentials in plain text in a configuration file.**

  Workaround: Back up and delete `%APPDATA%\postgresql\pgpass.conf` file after installation.

- **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.

- **Virtual machines still have the 'managed by SRM' flag on the protected site after recovery and reprotect.**

  For a virtual machine that has the `Reserve all guest memory(All locked)` option set, after running recovery and reprotect the virtual machine still has the `Managed by SRM` flag on the protected site. It should be shown as a normal virtual machine.

  Workaround: None.

- **When you run a test failover on a Windows virtual machine that is configured for IP customization, you see the following error in the logs: `Error accessing guestcust.log`.**

  This error can occur if either the folder `%TMP%` does not exist or the file `%TMP%\vmware-imc\guestcust.log` does not exist.

  Workaround: Run the IP customization manually.

- **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.

- **Protect virtual machine task appears to remain at 100%.**

  The vSphere Web Client Recent Tasks pane shows a virtual machine stuck at 100% during the **Protect VM** task. Site Recovery Manager marks the virtual machine as **Configured**, indicating that it was protected. You do not need to take action as Site Recovery Manager successfully protected the virtual machine.