VMware Site Recovery Manager 6.5 Release Notes

Updated on 02/15/2021

Site Recovery Manager 6.5 | 15 NOV 2016 | Build 4613745

Last updated: **10 OCT 2017**

Check for additions and updates to these release notes.

What's in the Release Notes

These release notes cover the following topics:

What's New in Site Recovery Manager 6.5

VMware Site Recovery Manager 6.5 is compatible with VMware vSphere 6.5.

VMware Site Recovery Manager 6.5 provides the following new features:

- vRealize Operations Management Pack for Site Recovery Manager 6.5. Site Recovery Manager 6.5 delivers integration with vRealize Operations Manager through a new management pack. With the management pack installed on vRealize Operations Manager, you can monitor key Site Recovery Manager health metrics such as Site Recovery Manager Server connectivity, and protection group and recovery plan status. For information about the management pack, see VMware vRealize Operations Management Pack for Site Recovery Manager 6.5 Release Notes.
- Support for VMware vSphere Virtual Volumes through vSphere Replication. Site Recovery Manager 6.5 supports protection and orchestrated recovery of virtual machines that are located on Virtual Volume datastores and replicated by vSphere Replication.
- Support for silent installation, upgrade, and uninstallation.
- Enhancements to Site Recovery Manager public API. Site Recovery Manager 6.5 introduces new methods in the product's Public API. With the public API, you have programmatic access to a wider range of product functionality and more extensive product automation. For information about the new and updated API methods, see *Site Recovery Manager API Developer's Guide*.
- Enhancements and new workflows in the vRealize Orchestrator plug-in for Site Recovery Manager 6.5
  - The vRealize Orchestrator plug-in for Site Recovery Manager can work with vRealize Orchestrator configured with LDAP authentication.
  - Site Recovery Manager 6.5 introduces 18 new workflows available through the vRealize Orchestrator plug-in for Site Recovery Manager 6.5. For information about the new workflows, see VMware vRealize Orchestrator Plug-In for Site Recovery Manager 6.5 Release Notes.
- Support for the vCenter Server HA feature. Site Recovery Manager works normally in the event that vCenter Server HA fails over to another vCenter Server node.
- Support for migration of a vCenter Server installation on Windows to a vCenter Server Appliance installation during upgrade. You can use VMware Migration Assistant to upgrade and migrate your environment from vCenter Server 6.0 for Windows to vCenter Server 6.5 Appliance. The procedure is fully compatible with a standard Site Recovery Manager direct upgrade.
- Support for the Virtual Machine Encryption feature. Site Recovery Manager 6.5 supports the protection and recovery of encrypted virtual machines with Storage Policy Protection Groups (SPPGs). For information about the protection of encrypted VM[illegible] *Site Recovery Manager 6.5 Administration*.

- Site Recovery Manager API support for Test Recovery operation when the protected and recovery sites are disconnected.
- Participation in the VMware Customer Experience Improvement Program (CEIP). Details regarding the data collected by CEIP and the purposes for which it is used by VMware are available at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

Note: For interoperability with earlier or later releases of VMware vSphere, see the Compatibility Matrixes for VMware Site Recovery Manager 6.5.

For information about the features of vSphere 6.5, see the *vSphere 6.5* documentation.

For information about the supported databases, see the Compatibility Matrixes for VMware Site Recovery Manager 6.5.

Localization

VMware Site Recovery Manager 6.5 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 6.5 is compatible with vSphere 6.5 and supports ESXi versions that vCenter Server 6.5 supports.

Site Recovery Manager 6.5 does not support IP customization and in-guest callout operations for VMs that are placed on ESXi 5.5 and use VMware Tools 10.1.

To use IP customization and in-guest callout operations for VMs placed on ESXi 5.5, ensure that the VMs use VMware Tools version earlier than 10.1.

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 Matrixes for VMware Site Recovery Manager 6.5.

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 6.5 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 6.5.

VMware VSA Support

Site Recovery Manager 6.5 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 6.5.

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 Matrixes.

NOTES:

- Upgrading Site Recovery Manager from version 6.0.x directly to version 6.5 is not supported. To upgrade Site Recovery Manager 6.0.x to Site Recovery Manager 6.5, you must first upgrade Site Recovery Manager from 6.0.x to 6.1.x. If you use vSphere Replication with Site Recovery Manager 6.0.x, and you upgrade vSphere Replication from version 6.0.x to version 6.5 directly, when you attempt the interim upgrade of Site Recovery Manager from version 6.0.x to version 6.1.x, the Site Recovery Manager upgrade fails with an error because of an incompatible version of vSphere Replication. Upgrade vSphere Replication to version 6.1.x before you upgrade Site Recovery Manager from 6.0.x to 6.1.x.

- 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. Otherwise, upgrade might fail.

Network Security

Site Recovery Manager requires a management network connection between paired sites. The Site Recovery Manager Server instances on the protected site and on the recovery site must be able to connect to each other. In addition, each Site Recovery Manager instance requires a network connection to the Platform Services Controller and the vCenter Server instances that Site Recovery Manager extends at the remote site. Use a restricted, private network that is not accessible from the Internet for all network traffic between Site Recovery Manager sites. By limiting network connectivity, you limit the potential for certain types of attacks.

For the list of network ports that Site Recovery Manager requires to be open on both sites, see http://kb.vmware.com/kb/2147112.

Operational Limits for Site Recovery Manager 6.5

For the operational limits of Site Recovery Manager 6.5, see http://kb.vmware.com/kb/2147110.

Site Recovery Manager SDKs

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

Open Source Components

The copyright statements and licenses applicable to the open source software components distributed in Site Recovery Manager 6.5 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 6.5 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 6.5 does not support the protection of virtual machines that are configured with multiple-CPU vSphere Fault Tolerance (FT). Site Recovery Manager 6.5 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 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 running the recovery plan again.
    - 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 6.5 supports replication of virtual machines on VMware vSphere Virtual Volumes with limitations. Site Recovery Manager 6.5 supports vSphere Replication 6.5 with vSphere Virtual Volumes with the following limitations.
    - You cannot use Site Recovery Manager 6.5 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 6.5.x does not support NFS v 4.1 datastores for array-based replication. You can use Site Recovery Manager 6.5.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 6.5 and to pair your Site Recovery Manager 6.5 sites.
  2. The vCenter Server instances on both Site Recovery Manager 6.5 sites must work in Enhanced Linked Mode. To prevent failures during upgrade of Site Recovery Manager from 6.5 to a newer version of Site Recovery Manager, the vCenter Server instances on both sites must be direct replication partners.
- The DR IP Customizer tool does not support storage policy protection groups.
- Site Recovery Manager 6.5 supports protection of encrypted VMs only with Storage Policy Protection groups. For information about how to configure protection of Encrypted VMs, see the *Site Recovery Manager Administration* documentation.

Known Issues

The following known issues have been discovered through rigorous testing and will help you understand some behavior that 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.

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

  If an issue occurs with the VMs in a consistency group during a storage policy protection group failover, and you skip the consistency group, the reprotect operation 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.

- **Site Recovery Manager in a high change environment might experience database identifier exhaustion**

  High change environment might cause database identifier exhaustion in Site Recovery Manager. As a result Site Recovery Manager might stop working with a back trace recorded in the `vmware-dr.log`.

  ```
  2017-08-04T11:57:52.065-04:00 [06292 panic 'Default']
  Panic: VERIFY d:\build\ob\bora5077693\srm\public\persistence/AssociationDBAdapter.h:465
  Backtrace:
  [backtrace begin] product: VMware vCenter Site Recovery Manager, version: 6.1.2, build: build-5077693, tag: - backtrace[00]
  vmacore.dll[0x001B937A]
  ```

  Workaround: See https://kb.vmware.com/s/article/54754.

- **vSphere Web Client works slow and the OutOfMemory error appears**

  vSphere Web Client works slow, if you use vCenter Server Appliance environment deployed in a Tiny configuration, and use Site Recovery Manager and vSphere Replication plug-ins in the vSphere Web Client. The cause is that the memory reserved for vSphere Web Client is not enough to support the plug-ins.

  Workaround: Deploy the vCenter Server appliance with at least Small configuration.

- **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 Related Objects tab**

  If you delete a storage policy, the VMs and the consistency group that are assigned to the storage policy appear as related objects 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 Related Objects tab.

- **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 virtual disks of recovered VMs are associated with the default storage policy regardless of their association on the protected VMs**

  The same applies to the VMs after a full reprotect cycle. All virtual disks are in the correct locations, VMs can be powered on and are still protected by Site Recovery Manager. The virtual disks of encrypted VMs are encrypted even after the association with the encryption storage profile is lost.

  Workaround: Apply the correct storage policies after the VMs are recovered.

- **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.`

  Workaround:

  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 Recovery Plan fails if your recovered VM uses the latest VMware Tools version and is not synchronized with the ESXi host on the recovery site**

  If you use an IP customization or in-guest callout operations and the time of your guest OS on the recovered VM is not synchronized with your ESXi host on the recovery site, you receive the following error.

  ```
  Error - Failed to authenticate with the guest operating system using the supplied credentials.
  ```

  Workaround: If the recovery.autoDeployGuestAlias option in Advanced Settings is FALSE, ensure the time synchronization between the recovered VM and vCenter Single Sign-On on the recovery site, and rerun the recovery plan.

  If the recovery.autoDeployGuestAlias option in Advanced Settings is TRUE and the guest OS of the recovered VM is Windows, ensure the time synchronization between the ESXi host and vCenter Single Sign-On on the recovery site, and rerun the failed recovery plan.

  If the recovery.autoDeployGuestAlias option in Advanced Settings is TRUE and the guest OS of the recovered VM is Linux, ensure the time synchronization between the ESXi host and vCenter Single Sign-On on the recovery site, 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.

- **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 network mapping from *Protected_Network_Main* on the protected site to *Recovery_Network_Main* on the recovery site.

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

- The test network mapping from *Recovery_Network_Main* to *Recovery_Network_Test* is not deleted.

Workaround: Delete the test network mapping manually.

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

  Workarounds: Remove dependency between virtual machines and rerun planned migration with vMotion. Manually re-enable dependency for future recovery workflows.
  If you want to preserve the dependency between virtual machines, then run planned migration without vMotion. Both virtual machines migrate as regular virtual machines according to the dependency order.

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

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

  Workaround: Restart the Site Recovery Manager server.

- **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.

- **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 in to 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.

- **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 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 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.

- **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.

- **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.

- **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.**

Web Client displays Site Recovery Manager in English.

Workaround: Use Chrome or Firefox.

- **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.

  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`**

- **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.

- **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.