VMware Site Recovery Manager 6.1.1 Release Notes

Updated on 02/15/2021

Site Recovery Manager 6.1.1.1 | 10 NOV 2016 | Build 4535903

Site Recovery Manager 6.1.1 | 26 MAY 2016 | Build 3884620

Last updated: 24 FEB 2017

Check for additions and updates to these release notes.

For information about Site Recovery Manager 6.1.1.x patch releases, see the corresponding section of these release notes.

- Site Recovery Manager 6.1.1.1 Express Patch Release

What's in the Release Notes

These release notes cover the following topics:

What's New in Site Recovery Manager 6.1.1

VMware Site Recovery Manager 6.1.1 delivers new bug fixes described in the Resolved Issues section.

Updated VMware Site Recovery Manager 6.1.1 provides the following new features:

- Support for Two-factor authentication with RSA SecurID for vCenter Server 6.0U2.
- Support for Smart Card (Common Access Card) authentication for vCenter Server 6.0U2.
- Site Recovery Manager 6.1.1 now supports the following external databases:
  - Microsoft SQL Server 2012 Service Pack 3
  - Microsoft SQL Server 2014 Service Pack 1
- Adding localization support for Spanish language.

VMware Site Recovery Manager 6.1.1 is compatible with VMware vSphere 6.0 update 2.

Note: For interoperability with earlier or later releases of VMware vSphere, see the Compatibility Matrixes for VMware Site Recovery Manager 6.1.

For information about the features of vSphere 6.0 update 2 and the authentication methods for vCenter Server update 2, see the *vSphere 6.0* documentation.

For information about the supported databases, see the Compatibility Matrixes for VMware Site Recovery Manager 6.1.

Localization

VMware Site Recovery Manager 6.1.1 is available in the following languages:

- English
- French
- German

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

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 Site Recovery Manager 6.1.

Compatible Storage Arrays and Storage Replication Adapters

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

VMware Virtual SAN Support

Site Recovery Manager 6.1.1 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 6.1.1.

VMware VSA Support

Site Recovery Manager 6.1.1 can protect virtual machines that reside on the vSphere Storage Appliance (VSA) by using vSphere Replication. VSA does not require a Storage Replication Adapter (SRA) to work with Site Recovery Manager 6.1.1.

Installation and Upgrade

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

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

NOTES:

- Upgrading Site Recovery Manager from version 5.8.x directly to version 6.1.1 is not supported. To upgrade Site Recovery Manager 5.8.x to Site Recovery Manager 6.1.1, you must first upgrade Site Recovery Manager from 5.8.x to 6.0.x. Upgrading vSphere Replication from version 5.8.x directly to version 6.1.1 is not supported. If you use vSphere Replication with Site Recovery Manager 5.8.x, and you upgrade vSphere Replication from version 5.8.x to version 6.1 directly, when you attempt the interim upgrade of Site Recovery Manager from version 5.8.x to version 6.0.x, the Site Recovery Manager upgrade fails with an error about an incompatible version of vSphere Replication. Make sure that you upgrade vSphere Replication to version 6.0.x before you upgrade Site Recovery Manager from 5.8.x to 6.0.x. If you have already upgraded vSphere Replication from 5.8.x to 6.1 directly, see KB 2136677.
- 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 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/2119329.

Operational Limits for Site Recovery Manager 6.1.1

For the operational limits of Site Recovery Manager 6.1.1, see http://kb.vmware.com/kb/2119336.

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 6.1.1 are available at VMware 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 6.1.1 offers limited support for vCloud Director environments. Using Site Recovery Manager to protect virtual machines within vCloud resource pools (virtual machines deployed to an Organization) is not supported. Using Site Recovery Manager to protect the management structure of vCD is supported. For information about how to use Site Recovery Manager to protect the vCD Server instances, vCenter Server instances, and databases that provide the management infrastructure for vCloud Director, see VMware vCloud Director Infrastructure Resiliency Case Study.
- vSphere Flash Read Cache is disabled on virtual machines after recovery and the reservation is set to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take a note of 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 6.1.1 does not support the protection of virtual machines that are configured with multiple-CPU vSphere Fault Tolerance (FT). Site Recovery Manager 6.1.1 supports the protection of virtual machines with uni-processor vSphere FT, but deactivates uni-processor vSphere FT on the virtual machines on the recovery site after a recovery.
    - If you 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 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 6.1.1 supports replication of virtual machines on Virtual Volumes (vVols) with limitations. Site Recovery Manager 6.1.1 does not support the protection of virtual machines on Virtual Volumes, even if you use vSphere Replication as the replication technology for protection.
- Site Recovery Manager 6.1.1.x does not support NFS v 4.1 datastores for array-based replication. You can use Site Recovery Manager 6.1.1.x with NFS v 4.1 datastores for vSphere Replication.
- Site Recovery Manager does not support reconfiguration of storage profile protection groups, such as changing the set of associating storage policies, group name, or descriptions. If you need 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 6.1.1 and to pair your Site Recovery Manager 6.1.1 sites.
    2. The vCenter Server instances on both Site Recovery Manager 6.1.1 sites must work in Enhanced Linked Mode. To prevent failures during upgrade of Site Recovery Manager from 6.1.1 to a newer version of Site Recovery Manager, the vCenter Server instances on both sites must be direct replication partners.

Available Patch Releases

The Site Recovery Manager 6.1.1.x express patch releases resolve problems that have been encountered after the initial 6.1.1 release. You obtain the patch releases from the Site Recovery Manager Downloads page at http://www.vmware.com/go/download-srm.

Site Recovery Manager 6.1.1.1 Express Patch Release

Released 10 NOV 2016 | Build 4535903

The Site Recovery Manager 6.1.1.1 Express Patch Release enables the ECDHE cipher.

The Site Recovery Manager 6.1.1.1 Express Patch Release resolves the following issues:

- **Recovery plan history report cannot be exported if there are special characters in the name**

  If there are special characters in the name of the recovery plan such as `/`, `*` or `%`, when you press **Download report** nothing happens. You are unable to donwload the history report. If you remove the special character from the plan name, the report is exported successfully.

- **When performing failover tasks using RDM devices, SRM crashes or fails with the following error:** `The virtual disk is either corrupted or not a supported format.`

- **When performing failover tasks, SRM might fail with the following error message:** `Unable to copy the configuration file "[datastore]machine/*.vmx from host`

  This issue is resolved by built-in delays and retries for the Network File Copy (NFC) commands. The default NFC command delay is set to 3 seconds and the default retry is set to 5.
  If you want to modify the parameters, navigate to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` and open the file `vmware-dr.xml`. Add the following items and set their values:

  ```
  <nfc>
  <retryCount>5</retryCount>
  <retryDelaySeconds>3</retryDelaySeconds>
  </nfc>
  ```

Installation and Upgrade Notes

If you are running Site Recovery Manager 6.1.1, upgrade to Site Recovery Manager 6.1.1.1. See Uprading Site Recovery Manager in *Site Recovery Manager 6.1 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 6.1.1, upgrade the vSphere Replication appliance to version 6.1.1.1. See the vSphere Replication 6.1.1.x Release Notes for information about vSphere Replication 6.1.1.1.

Resolved Issues

The following issues from previous releases have been resolved in this release.

- **Site Recovery Manager service crashes if the NIC information for your VM is invalid**

  If your protected VM is part of two VM networks and you delete one of its MAC addresses from the `.vmx` file or an issue in your environment corrupts the NIC information, the IP customization of the VM fails and the Site Recovery Manager service at the recovery site crashes.

  The issue is resolved. The service does not crash and Site Recovery Manager writes an error in its logs.

  For example, if you delete `ethernet1.present` and `ethernet1.generatedAddress` from the `.vmx` file, the following error appears in the Site Recovery Manager logs:

  ```
  Failed to customize IP for that VM
  ```

- **The `SrmLoginSites` method of the public Site Recovery Manager API returns an InvalidLoginFault error**

  If your Site Recovery Manager sites are paired and work in Enhanced Linked Mode, the `SrmLoginSites` method throws an error even if you call the method with the correct `username` and `password` parameters.

  The following error appears in your execution log:

  ```
  "com.vmware.vim.binding.vim.fault.InvalidLogin: Cannot complete login due to an incorrect user name or password."
  ```

  Site Recovery Manager Server records the following error in its logs:

  ```
  Cannot authenticate user Unknown
  ```

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

  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.

- **The Site Recovery Manager service crashes if your host does not have an allocated vmkernel IP**

  The Site Recovery Manager service crashes if there is an error in the vmkernel IP allocation or the connection between your host, vCenter Server, and Site Recovery Manager temporarily fails.

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.

- **IP Customization and Callout fails when SRM 6.1.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.

- **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 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.

- **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.

- **Storage policy protection groups with non-protected VMs do not reflect and pick up changes when a planned migration is in the Incomplete Recovery state.**

  If planned migration fails in the Incomplete Recovery state because a non-protected VM that is not associated with the appropriate storage policy is in the protected datastore, and if you then associate the non-protected VM with the correct storage policy and run the planned migration again, the storage policy protection group is not updated to reflect and pick up the changes you made. The planned migration continues to fail in the Incomplete Recovery state due to the non-protected VM, even though this VM should now be part of the protection group.

Workarounds: Perform one of the following workarounds to move the virtual machine out of the protection group:

- If the non-protected VM is accessible and is not read-only, migrate it out the consistency group.
- Copy the non-protected VM and use `VirtualMachine.ReloadFromPath` from the vCenter Server API to reload the VM on a datastore that is not in the consistency group.
- Copy the non-protected VM, unregister the old VM from vCenter Server, then register the new VM on a datastore that is not in the consistency group. The virtual machine loses its MoRef but keeps its UUID.
- If the non-protected VM exists on the failed over datastore, unregister the VM from vCenter Server and manually recover the VM on the recovery site.

- **Recovery plans fail at the Unregister VMs at protected site step if Site Recovery Manager attempts to unregister a non-protected VM.**

  A recovery plan that includes a non-protected virtual machine can fail at the Unregister VMs at protected site step when Site Recovery Manager attempts to unregister that virtual machine. Changing the non-protected VM's storage policy to add it to the storage policy protection group after you have attempted to run the recovery does not resolve the issue, as described in the issue above.

  Workaround: Move the non-protected VM to a different datastore.

- **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.

- **When you use Storage DRS to migrate a virtual machine to a datastore that does not match its storage policy's tags, Site Recovery Manager does not modify the virtual machine's storage policy. If this virtual machine is protected in a storage policy protected group, it might lose protection.**

  Workaround: First modify the policy to **Datastore Default** and then the storage policy corresponding to the new datastore, so that the virtual machine is automatically protected by the corresponding storage policy protection group.

- **Virtual machine is not protected or associated with any protected storage policies after using Storage vMotion.**

  If you use Storage vMotion on a virtual machine that is protected by a storage policy protection group from one datastore to a datastore in a different consistency group, and then use Storage vMotion to return to the original datastore, the virtual machine is not protected.

  Workaround: Reapply the storage policy on the virtual machine. The virtual machine is protected again under the original storage policy protection group.

- **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.

- **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

- **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 6.1.1 Release Notes.

- **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.

- **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 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.

- **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 in to 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.

- **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.

- **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.

- **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.

- **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.

- **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 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...`**

  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.
- **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 twice, 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

- **After you upgrade Site Recovery Manager 6.1 to 6.1.1, virtual machines recovered by Site Recovery Manager 6.1 still have the 'managed by SRM' flag on the protected site**

  For a virtual machine that has the `Reserve all guest memory (All locked)` option set in Site Recovery Manager 6.1 and recovered by Site Recovery Manager 6.1 the virtual machine still has the `Managed by SRM` flag on the protected site. It should be shown as a normal virtual machine.

  Workaround: To clean the flag, run the recovery plan after you upgrade Site Recovery Manager 6.1 to 6.1.1.

- **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.