

# VMware Site Recovery Manager 5.8 Release Notes



Updated on 07/27/2015

Site Recovery Manager 5.8.0.1 | 09 DEC 2014 | Build 2336305

Site Recovery Manager 5.8 | 09 SEP 2014 | Build 2056894

Last updated: 27 JUL 2015

Check for additions and updates to these release notes.

For information about the Site Recovery Manager 5.8.0.1 patch release, see [Site Recovery Manager 5.8.0.1 Express Patch Release \(KB 2096080\)](#).

## What's in the Release Notes

These release notes cover the following topics:

- [What's New in Site Recovery Manager 5.8](#)
- [Localization](#)
- [Compatibility](#)
- [Installation and Upgrade](#)
- [Operational Limits of Site Recovery Manager](#)
- [Site Recovery Manager SDKs](#)
- [Open Source Components](#)
- [Caveats and Limitations](#)
- [Known Issues](#)

## What's New in Site Recovery Manager 5.8

VMware vCenter Site Recovery Manager 5.8 provides the following new features.

- Integration of the Site Recovery Manager UI in vSphere Web Client.
- A vCenter Orchestrator plug-in for Site Recovery Manager that allows you to automate certain Site Recovery Manager operations by including them in vCenter Orchestrator workflows. For information about the vCenter Orchestrator plug-in for Site Recovery Manager, see [Site Recovery Manager and vCenter Orchestrator](#) in the Site Recovery Manager 5.8 Documentation Center and the [vCenter Orchestrator Plug-In for Site Recovery Manager 5.8 Release Notes](#).
- Increased scale that allows you to use Site Recovery Manager to protect and recover larger numbers of virtual machines. See [Operational Limits of Site Recovery Manager 5.8 \(KB 2081158\)](#).
- Subnet-level IP customization rules that allow you to manage the customization of IP addresses across multiple virtual machines from the Site Recovery Manager UI. For information about subnet-level IP customization rules, see [Customize IP Properties for Multiple Virtual Machines by Defining IP Customization Rules](#) in the Site Recovery Manager 5.8 Documentation Center.
- An optional embedded vPostgreSQL database that you can use instead of a dedicated external database with minimal configuration. For information about the embedded database, see [Creating the Site Recovery Manager Database](#) and [Install Site Recovery Manager Server](#) in the Site Recovery Manager 5.8 Documentation Center.
- Improved support for Integrated Windows Authentication when using Microsoft SQL Server as the Site Recovery Manager database. For information about using Integrated Windows Authentication with SQL Server, see [Requirements when Using Microsoft SQL Server with Site Recovery Manager](#) and [Install Site Recovery Manager Server](#) in the Site Recovery Manager 5.8 Documentation Center.

## Localization

VMware vCenter Site Recovery Manager 5.8 is available in the following languages:

- English
- French
- German
- Japanese

- Korean
- Simplified Chinese
- Traditional Chinese

## Compatibility

### Site Recovery Manager Compatibility Matrix

For interoperability and product compatibility information, including supported guest operating systems and support for guest operating system customization, see the [Compatibility Matrixes for VMware vCenter Site Recovery Manager 5.8](#).

### Compatible Storage Arrays and Storage Replication Adapters

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

### VMware Virtual SAN Support

Site Recovery Manager 5.8 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 5.8.

### VMware VSA Support

Site Recovery Manager 5.8 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 5.8.

## Installation and Upgrade

For information about installing and upgrading Site Recovery Manager, see [Site Recovery Manager Installation and Configuration](#).

For the supported upgrade paths for Site Recovery Manager, see the [VMware Product Interoperability Matrixes](#) and select **Solution Upgrade Path** and **VMware vCenter Site Recovery Manager**.

## Operational Limits for Site Recovery Manager 5.8

For the operational limits of Site Recovery Manager 5.8, see <http://kb.vmware.com/kb/2081158>.

For the protection and recovery limits when using Site Recovery Manager 5.8 in a shared recovery site configuration, see <http://kb.vmware.com/kb/2081866>.

## Site Recovery Manager SDKs

For a guide to using the Site Recovery Manager SOAP-based API, see [VMware vCenter Site Recovery Manager API](#).

## Open Source Components

The copyright statements and licenses applicable to the open source software components distributed in Site Recovery Manager 5.8 are available at [VMware vCenter Site Recovery Manager Downloads](#). You can also download the source files for any GPL, LGPL, or other similar licenses that require the source code or modifications to source code to be made available for the most recent generally available release of vCenter Site Recovery Manager.

## Caveats and Limitations

- Site Recovery Manager 5.8 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.

## 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.

- **Cannot start virtual machine after recovery if the virtual machine has disk files at the top level of a nonreplicated datastore.**

If a virtual machine has a disk file at the top level in a nonreplicated datastore, you might not be able to power on the virtual machine after you run a test recovery, planned migration, or disaster recovery. You might see the following error message in the log file: **Failed to**

After you run a test recovery, planned migration, or disaster recovery, you might see the following error message in the log: `Failed to resolve file locator for backing of device 2001: (dr.storageProvider.fault.ResolvedVmFileNotFound)'`.

Workaround: Move the disk file out of the top level of the datastore. Do not use a disk file at the top level of the datastore when mapping to a placeholder datastore on the recovery site.

- **Performing a recovery reports the error: `Failed to connect Site Recovery Manager Server(s)`.**

If the vCenter Server instances on the protected site and recovery site are configured in Linked Mode and the protected site is offline or the vSphere Web Client server is unable to communicate with the vCenter Server Inventory Service on the protected site, you cannot perform a recovery using the vSphere Web Client because there are no Recovery Plans visible in the user interface. Recovery fails with the error `Failed to connect Site Recovery Manager Server(s). Cause: Failed to retrieve pairs from Site Recovery Manager Server at https://vcenter_server_hostname:8095/dr`.

Workaround: See [KB 2093902](#).

- **Planned migration with vSphere Replication and Virtual SAN can fail if Virtual SAN stores logs on a datastore that Site Recovery Manager protects.**

If you use Virtual SAN storage, and you store the Virtual SAN logs on a datastore that is included in a Site Recovery Manager protection group, planned migration can fail with the error `Cannot unmount volume datastore_name because file system is busy`.

Workaround: See [KB 2069171](#).

- **Reprotect remains in progress for 2-3 days then shows as Reprotect Interrupted.**

If the network connection between the protected and recovery sites fails after the "Restore protected site hosts from standby" step completes during a reprotect operation, the reprotect operation remains in progress indefinitely for 2-3 days. After this time, the status of the recovery plan is set to Reprotect Interrupted.

Workaround: Restart Site Recovery Manager Server and rerun reprotect. If the error still occurs, contact VMware support.

- **Uninstalling then reinstalling Site Recovery Manager 5.8 resets the embedded vPostgres database.**

If you use the embedded vPostgres database with Site Recovery Manager 5.8 and you uninstall Site Recovery Manager, retaining the database contents, then reinstall Site Recovery Manager, connecting to the embedded vPostgres database from the previous installation, the Site Recovery Manager installer resets the embedded database. This causes the loss of all inventory mappings from the previous installation.

Workaround: Upgrade to Site Recovery Manager 5.8.0.1, which fixes this issue. For information about Site Recovery Manager 5.8.0.1, see [KB 2096080](#).

If you cannot upgrade to Site Recovery Manager 5.8.0.1, see [KB 2092565](#) for details of an alternative workaround.

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

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

Workaround: None.

- **Connecting to an existing database and selecting the Recreate the database option when installing a new Site Recovery Manager Server instance for use with a new vCenter Server instance causes installation to fail.**

Recreating an existing Site Recovery Manager database for use with a new instance of Site Recovery Manager Server and a new instance of vCenter Server causes installation to fail with the error `Failed to clear Inventory Service registration`. This problem occurs in the following scenario:

1. You install a new instance of vCenter Server.
2. You attempt to install a new instance of Site Recovery Manager to connect to the new vCenter Server instance.
3. During installation of Site Recovery Manager, you select an existing Site Recovery Manager database from a previous Site Recovery Manager installation.
4. You select the **Recreate the database** option.

In this scenario, installation fails with the error and rolls back.

Workaround: When installing a new instance of Site Recovery Manager Server to use with a new instance of vCenter Server, connect Site Recovery Manager to a new database instance.

- **History reports generated for the support bundles do not render correctly on Internet Explorer versions 8 and 9.**

Workaround: Use Firefox.

- **Incorrect error message 'Failed to Install Certificate' appears when the Site Recovery Manager extension fails to register with vCenter.**

When you use a trusted user-generated certificate and Site Recovery Manager Installer shows an error of failing to install the certificate, the error might also mean Site Recovery Manager failed to register with vCenter Server.

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

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

- **Recovery operation fails with error: Cannot unmount volume '(datastore name)' because file system is busy. Correct the problem and retry the operation.**

This error occurs when you run a recovery plan with a protection group containing a virtual machine whose virtual CDROM device filename property is set to `emptyBackingString`. The volumes are in open state and one or more process on the host are using them. You cannot force unmount the volume.

Workaround: Find the user and stop accessing the volume using `lssof` output.

- **When you uninstall Site Recovery Manager server, Site Recovery Manager removes default Site Recovery Manager roles but you can still see and assign Site Recovery Manager privileges on roles.**

Workaround: None.

- **Planned migration for a recovery plan fails with error `VR synchronization failed for VRM group`.**

If, during planned migration, the infrastructure (hosts, network, or storage) is under heavy load, running a recovery plan might fail with the error `VR synchronization failed for VRM group <group_name>`. A replication error occurred at the vSphere Replication Server for replication `<group_name>`. Details: 'Error for (datastoreUUID: "..."), (diskId: "..."), (hostId: "..."), (pathname: "..."), (flags: retrieable): Class: NFC Code: 10; NFC error: The operation completed successfully; Set error flag: retrieable; ...'

Usually, this error is transient and the operation succeeds if you retry running it.

Workaround: If the error occurs frequently in your environment, you can increase the toleration period for replication synchronizations on the vSphere Replication Management Server (VRMS).

1. Log in to the VRMS appliance as the root user and navigate to `/opt/vmware/hms/conf/`.
2. Open the `hms-configuration.xml` file for editing and set the value of the `hms-sync-replication-error-toleration-period` property to `300000`.
3. Try running the planned migration task again.

- **When you select the option to reserve all guest memory on a virtual machine, then perform a failover, the placeholder virtual machine on the protected site changes to 32M memory and loses the selected option.**

This issue does not occur when there is no memory reservation on the virtual machine.

Workaround: Set memory reservations manually on the placeholder virtual machine on the recovery site.

- **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.

- **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.

- **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.

- **After you upgrade vCenter Server and Site Recovery Manager servers to version 5.8, log in to a shared recovery site and start a test recovery plan on one pair, then start a test recovery plan on the other pair, the second test plan fails with a message that the plan is locked.**

Workaround: Start the test plan again.

- **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.

- **When moving protection groups in the root folder, Site Recovery Manager throws a flex exception.**

Workaround: Dismiss the exception and perform a global refresh to reload the vSphere Web Client.

- **When Site Recovery Manager server disconnects with vCenter inventory service, the Site Recovery Manager user interface does not display the appropriate error notification.**

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

Workaround: Check the vCenter Server instance that posted the event that the inventory service cannot connect to Site Recovery Manager. Investigate the cause of the broken connection between Site Recovery Manager and the inventory service, and restore the connection.

- **Site Recovery Manager creates a core dump when it cannot connect to vCenter Server during shutdown.**

During the shutdown sequence, Site Recovery Manager server fails to connect to vCenter Server within the default time of 5 minutes, throws an exception which yields a core dump.

Workaround: None. This does not affect the ability of Site Recovery Manager to restart and connect with vCenter Server when it is available.

- **Removing permission does not disable mapping creation action.**

If you remove permissions for a user with Administrator role, instead of disabling the action to create mappings, Site Recovery Manager continues to allow the user to create mappings.

Workaround: None.

- **When you install Site Recovery Manager and protect a virtual machine with ABR, then switch to a vSphere Replication-only license, the protected virtual machine does not change to unprotected. The protected virtual machine counts against your license, but the error message that you exceeded your license restriction does not appear.**

- **After a global refresh, the Summary tab might not update a disconnected site pairing on the remote site.**

When you pair sites, log into the remote site, select the remote site, navigate to the Summary tab and break the pairing, the Summary tab does not update the information and continues to display the sites as paired.

Workaround: Navigate away from the Summary tab, perform a global refresh, then return to the Summary tab to see the correct information.

- **On Windows 8 or Windows 8.1 using Internet Explorer versions 10 and 11, when you change the user locale to Chinese, the vSphere Web Client displays Site Recovery Manager in English.**

Workaround: Use Chrome or Firefox.

- **Site Recovery Manager plugin does not display in the vSphere Web Client if Site Recovery Manager service stops.**

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

Workaround: Restart the vSphere Web Client.

- **Site Recovery Manager might fail to restart while external processes are in progress.**

Site Recovery Manager uses external processes for some operations, such as recovery workflows and storage array management. If you restart the server while an external process is in progress, the operating system might not release these resources to allow Site Recovery Manager to restart immediately. The expected delay for releasing resources is about two minutes.

Workaround: Verify the external processes are terminated and network ports used by Site Recovery Manager are not in a lingering state, then restart Site Recovery Manager.

- **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.

- **Stopping datastore replication for protected virtual machines produces incorrect error messages**

It is possible to protect a virtual machine that has disks on multiple datastores and then subsequently disable replication for one of the datastores. In such a case, the virtual machine's status in the protection group changes to Invalid: Virtual machine 'VM' is no longer protected. Internal error: Cannot create locator for disk '2001'... This information is incorrect. The status should change to Datastore '[datastore name]' is no longer replicated.

- **Recovery of a vSphere Replication protection group fails with the error The specified key, name, or identifier already exists.**

If you choose the same datastore when you configure the placeholder for a virtual machine and when you configure vSphere Replication on that virtual machine, the placeholder and the recovered virtual machine files might be located on the same path. This can cause errors during recovery.

Workaround: Choose different datastores for placeholder virtual machines and vSphere Replication.



- **Site Recovery Manager stops during an attempt to protect an already reprotected array-based virtual machine using vSphere Replication.**

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

Workaround: Restart Site Recovery Manager Server and unprotect the array-based protected virtual machine first before protecting with vSphere Replication. Alternatively, continue with array-based protection and do not not protect with vSphere Replication. Site Recovery Manager does not support protecting with both providers.

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

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

- **Virtual Machine Recovery Fails Due to Disk Configuration Error**

It is possible to place different disks and configuration files for a single protected virtual machine on multiple datastores. During recovery, Site Recovery Manager must have access to raw disk mapping and parent disk files. Without this access, Site Recovery Manager cannot determine disk types during recovery. In such a case, Site Recovery Manager might assume that a Raw Disk Mapping (RDM) disk is a non-RDM disk, resulting in a failed reconfiguration. To avoid this issue, ensure all hosts that can access recovered virtual machine configuration files can also access RDM mapping files and any parent disks, if such disks exist.

- **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.askonpermanentdevice loss: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

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.

- **While reprotecting a virtual machine, the following error might occur during the "Configure protection to reverse direction" step: Error - The operation was only partially completed for the protection group 'pg\_name' since a protected VM belonging to it was not successful in completing the operation. VM 'vm\_name' is not replicated by VR.**

This error occurs during the second reprotect run if the first run failed with **Operation Timed out** error during "Configure storage to reverse direction" step.

Workaround: Manually configure reverse replication for the affected virtual machines and rerun reprotect. For information on reverse replication, see [vSphere Replication Administration: Failback of Virtual Machines in vSphere Replication](#).

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

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

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

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

- **Cancellation of Recovery Plan Not Completed**

When a recovery plan is run, an attempt is made to synchronize virtual machines. It is possible to cancel the recovery plan, but attempts to cancel the recovery plan run do not complete until the synchronization either completes or expires. The default expiration is 60 minutes. The following options can be used to complete cancellation of the recovery plan:

- Pause vSphere Replication, causing synchronization to fail. After recovery enters an error state, use the vSphere Client to restart vSphere Replication in the vSphere Replication tab. After replication is restarted, the recovery plan can be run again, if desired.
- Wait for synchronization to complete or time out. This might take considerable time, but does eventually finish. After synchronization finishes or expires, cancellation of the recovery plan continues.

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

If you use Site Recovery Manager to protect datastores on arrays that support dynamic swap, for example Clariion, running a disaster recovery when the protected site is partially down or running a force recovery can lead to errors when re-running the recovery plan to complete protected site operations. One such error occurs when the protected site comes back online, but Site Recovery Manager is unable to shut down the protected virtual machines. This error usually occurs when certain arrays make the protected LUNs read-only, making ESXi unable to complete I/O for powered on protected virtual machines.

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

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

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

Workaround: Rerun recovery.

- **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.

- **Performing test recovery rapidly after running a cleanup results in an error.**

If you perform a test recovery too rapidly after performing a cleanup following a previous test recovery, the recovery can fail with the error **File already exists**. This usually occurs if you run the test recovery from automation code, rather than from the Site Recovery Manager interface.

Workaround: Wait for a few minutes and try the operation again.

- **Running multiple vCenter Server instances in linked mode causes duplicate Site Recovery Manager roles to appear**

If you configure the vCenter Server instances on the protected and recovery sites to run in linked mode, duplicate Site Recovery Manager roles appear in the Assign Permissions window.

Workaround: Edit the Site Recovery Manager roles on each vCenter Server instance to provide them with unique names.

- **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.

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

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

- **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.