

VMware Site Recovery Manager 5.5.1.x Release Notes



Updated on 08/25/2016

VMware vCenter Site Recovery Manager 5.5.1.7 | 25 AUG 2016 | Build 4265224

VMware vCenter Site Recovery Manager 5.5.1.6 | 24 FEB 2016 | Build 3572851

VMware vCenter Site Recovery Manager 5.5.1.5 | 16 APR 2015 | Build 2653439

VMware vCenter Site Recovery Manager 5.5.1.4 | 22 OCT 2014 | Build 2215373

VMware vCenter Site Recovery Manager 5.5.1.3 | 01 OCT 2014 | Build 2170717

VMware vCenter Site Recovery Manager 5.5.1.2 | 30 JUL 2014 | Build 2000438

VMware vCenter Site Recovery Manager 5.5.1.1 | 17 JUL 2014 | Build 1964818

VMware vCenter Site Recovery Manager 5.5.1 | 11 MAR 2014 | Build 1647061

Last updated: 25 AUG 2016

Check for additions and updates to these release notes.

For information about the Site Recovery Manager 5.5.1.x patch releases, including details of any required vSphere Replication 5.5.1.x patches, see the corresponding knowledge base articles.

- [Site Recovery Manager 5.5.1.7 Express Patch Release \(KB 2146508\)](#)
- [Site Recovery Manager 5.5.1.6 Express Patch Release \(KB 2144234\)](#)
- [Site Recovery Manager 5.5.1.5 Express Patch Release \(KB 2111994\)](#)
- [Site Recovery Manager 5.5.1.4 Express Patch Release \(KB 2092268\)](#)
- [Site Recovery Manager 5.5.1.3 Express Patch Release \(KB 2091038\)](#)
- [Site Recovery Manager 5.5.1.2 Express Patch Release \(KB 2084603\)](#)
- [Site Recovery Manager 5.5.1.1 Express Patch Release \(KB 2081861\)](#)

What's in the Release Notes

These release notes cover the following topics:

- [What's New in SRM 5.5.1](#)
- [Localization](#)
- [Compatibility](#)
- [Installation and Upgrade](#)
 - [Install SRM 5.5.1](#)
 - [Upgrade an Existing SRM 4.1.2 Installation to SRM 5.5.1](#)
 - [Upgrade an Existing SRM 5.0.x or 5.1.x Installation to SRM 5.5.1](#)
 - [Upgrading Sites that Include Virtual Machines with RDM](#)
 - [Update an Existing SRM 5.5 Installation to SRM 5.5.1](#)
 - [Upgrade vSphere Replication to vSphere Replication 5.5.1](#)
- [Operational Limits of SRM and vSphere Replication](#)
- [SRM SDKs](#)
- [Open Source Components](#)
- [Caveats and Limitations](#)
- [Resolved Issues](#)
- [Known Issues](#)

What's New in SRM 5.5.1

VMware vCenter Site Recovery Manager 5.5.1 adds the following new features and improvements.

- Full support of using vSphere Replication with VMware Virtual SAN datastores. See [Using vSphere Replication with Virtual SAN Storage](#)

in *SRM Administration*.

- Bug fixes described in [Resolved Issues](#).

Localization

VMware vCenter Site Recovery Manager 5.5.1 is available in the following languages:

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

Compatibility

There are no SRM 5.5.2 or 5.5.3 releases to correspond with the vCenter Server 5.5u2 and 5.5u3 releases. SRM 5.5.1.x has been fully tested with and fully supports vCenter Server 5.5u1, 5.5u2, and 5.5u3.

SRM 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 5.5](#).

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 Virtual SAN Support

SRM 5.5.1 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 SRM 5.5.1.

VMware VSA Support

SRM 5.5.1 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 SRM 5.5.1.

Installation and Upgrade

For an evaluation guide to assist with a technical walkthrough of major features and capabilities of Site Recovery Manager 5.5.1, see the [VMware vCenter Site Recovery Manager Resources](#).

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

Install SRM 5.5.1

To create a new installation of SRM 5.5.1, download and run the installer `VMware-srm-5.5.1-1647061.exe`.

See [Installing SRM](#) in *Site Recovery Manager 5.5 Installation and Configuration*.

Upgrade an Existing SRM 4.1.2 Installation to SRM 5.5.1

Upgrade SRM 4.1.2 to SRM 5.0.x before you upgrade to SRM 5.5.1.

See *Upgrading SRM* in the [Site Recovery Manager 5.0 Administration Guide](#).

IMPORTANT: Upgrading vCenter Server directly from 4.1.2 to 5.5.1 is a supported upgrade path. However, upgrading SRM directly from 4.1.2 to 5.5.1 is not a supported upgrade path, and you must upgrade to SRM 5.0.x before you can upgrade to 5.5.1. When upgrading a vCenter Server 4.1.2 instance that includes an SRM 4.1.2 installation, you must also upgrade vCenter Server to version 5.0.x before you upgrade SRM to 5.0.x. If you upgrade vCenter Server from 4.1.2 to 5.5.1 directly, when you attempt to upgrade SRM from 4.1.2 to 5.0.x, the SRM upgrade fails. SRM 5.0.x cannot connect to a vCenter Server 5.5 instance.

Upgrade an Existing SRM 5.0.x or 5.1.x Installation to SRM 5.5.1

To upgrade an existing SRM 5.0.x or 5.1.x installation to SRM 5.5.1, download and run the installer `VMware-srm-5.5.1-1647061.exe`.

See [Upgrading SRM](#) in *Site Recovery Manager 5.5 Installation and Configuration*.

If you protect virtual machines that use raw disk mapping (RDM), upgrading Site Recovery Manager 5.0.x or 5.1.x to Site Recovery Manager 5.5.1 on the recovery site can fail during the creation of the database tables. Upgrade fails with the error: **Failed to create database tables. Could not perform the upgrade: Not initialized.** This issue occurs if you use RDM and your Site Recovery Manager environment is in either of the following states when you attempt the upgrade:

1. You performed a test recovery but test cleanup has not been completed before you attempt to upgrade.
2. You performed a recovery but did not perform reprotect before you attempt to upgrade.

To avoid this issue, run cleanup after a test recovery or reprotect after a recovery before you attempt to upgrade.

Workaround: If you encounter this issue, you can resolve it by modifying database tables manually. **NOTE:** This workaround depends on you having backed up the database on the recovery site before you attempted the failed upgrade.

1. Restore the database on the recovery site from the back up that you made before you attempted the failed upgrade.
2. Connect to the database on the recovery site and delete the entries in the `pds_rdmrecoveryinfo` table.
3. Upgrade Site Recovery Manager Server on the recovery site again.
IMPORTANT Do not back up the database again before attempting to upgrade again. Keep the original backup that you took before you attempted the initial failed upgrade.
4. When the upgrade completes, stop the Site Recovery Manager service.
5. Insert the rows from the `pds_rdmrecoveryinfo` table in the backup database into the `pds_rdmrecoveryinfo` table in the upgraded database.
6. Obtain the `unique_key` by selecting the ID from the `sequence_table` where `name = 'global_sequence'`.
7. For each of the n-rows that you inserted in step 5, update the values of the columns as follows:

<code>recovereddeviceinfo</code>	<code>unique_key + n</code>
<code>peerdevicegroup</code>	<code>''</code>
<code>peerdevicegrouphasvalue</code>	<code>0</code>

8. For each of the n-rows inserted in step 5, create a new row in the `pds_recovereddeviceinfo` table as follows:

<code>db_id</code>	<code>unique_key + n</code>
<code>mo_id</code>	<code>''</code>
<code>ref_count</code>	<code>1</code>
<code>device</code>	<code>(value of pds_rdmrecoveryinfo.device n)</code>
<code>peerdevice</code>	<code>''</code>
<code>peerdevicehasvalue</code>	<code>0</code>

9. Start the Site Recovery Manager service.

Update an Existing SRM 5.5 Installation to SRM 5.5.1

You perform the following steps to update an existing SRM 5.5 installation to SRM 5.5.1.

1. Log into the machine on which you are running SRM Server on the protected site.
2. Back up the SRM database using the tools that your database software provides.
3. Download and run the installer `VMware-srm-5.5.1-1647061.exe`.
4. Click **Yes** when prompted for confirmation that you want to upgrade SRM.
5. Click **Yes** to confirm that you have backed up the SRM database.
6. Click **Finish** when the installation completes.
7. Repeat the upgrade process on the recovery site.

After you have updated SRM Server, you must reinstall the SRM client plug-in.

1. Log into a machine on which you are running a vSphere Client instance that you use to connect to SRM.
2. Uninstall the SRM 5.5 client plug-in.
3. Log into a vSphere Client instance and connect to the vCenter Server to which SRM Server is connected.
4. Select **Plug-ins > Manage Plug-ins**.
5. Click **Download and Install** to install the SRM 5.5.1 client plug-in.
6. When the plug-in installation completes, log into SRM and verify that the configuration from the previous version has been retained.
7. Repeat the process for all vSphere Client instances that you use to connect to SRM Server.

Upgrade vSphere Replication to vSphere Replication 5.5.1

If you have installed vSphere Replication with a previous release of SRM and you upgrade to SRM 5.5.1, you must also upgrade vSphere Replication to version 5.5.1. You must also upgrade vSphere Replication servers to version 5.5.1. You must make sure that you have upgraded SRM to version 5.5.1 and vCenter Server to at least version 5.5 before you upgrade vSphere Replication to version 5.5.1.

IMPORTANT: vSphere Update Manager 5.5u3 is not supported. To upgrade vSphere Replication you must use either the downloadable ISO, or the virtual appliance management interface (VAMI) of the vSphere Replication appliance.

- To upgrade vSphere Replication from version 1.0.x or 5.1.x to 5.5.1, use the downloadable ISO file for vSphere Replication 5.5.1.

NOTE: If you are upgrading from vSphere Replication 1.0.3.3 or 5.1.3.1, you must upgrade to at least version 5.5.1.5. You cannot upgrade from vSphere Replication 1.0.3.3 or 5.1.3.3 to vSphere Replication releases between 5.5.0.0 and 5.5.1.4.

- To update vSphere Replication from version 5.5 to 5.5.1, use either the downloadable ISO file for vSphere Replication 5.5.1, vSphere Update Manager, or the virtual appliance management interface (VAMI) of the vSphere Replication appliance.
- To update vSphere Replication from version 5.5 to 5.5.1 when a later update release is already available, use the downloadable ISO file for vSphere Replication 5.5.1, or set the Use Specified Repository option in the VAMI to <https://vapp-updates.vmware.com/vai-catalog/valm/vmw/05d561bc-f3c8-4115-bd9d-22baf13f7178/5.5.1.0>.

NOTE: To obtain the VAMI upgrade URL for a vSphere Replication 5.5.1.x patch release, see the knowledge base article for the corresponding Site Recovery Manager 5.5.1.x patch release.

See [Upgrading vSphere Replication](#) in *Site Recovery Manager Installation and Configuration*.

IMPORTANT: Do not select the option in **Update > Settings** in the VAMI to automatically update vSphere Replication. If you select automatic updates, VAMI updates vSphere Replication to the latest 5.x version, which might be incompatible with SRM and vCenter Server 5.5.x. Leave the update setting set to **No automatic updates**.

Operational Limits for SRM and vSphere Replication

For the operational limits of SRM 5.5.x and vSphere Replication 5.5.x, see <http://kb.vmware.com/kb/2034768>.

For the protection and recovery limits when using SRM 5.5.x and vSphere Replication 5.5.x in a shared recovery site configuration, see <http://kb.vmware.com/kb/2008061>.

SRM SDKs

For a guide to using the SRM 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 5.5.1 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

- SRM 5.5.1 offers limited support for vCloud Director environments. Using SRM to protect virtual machines within vCloud resource pools (virtual machines deployed to an Organization) is not supported. Using SRM to protect the management structure of vCD is supported. For information about how to use SRM 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](#).
- Windows Server 2003 is not a supported platform for SRM Server but the SRM installer allows you to install SRM on Windows Server 2003.
- 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.

Resolved Issues

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

- **If SRM stops unexpectedly while testing a recovery plan, SRM stops again when you attempt to rerun the test.**

SRM stopping unexpectedly when testing a recovery plan results in SRM always stopping when you attempt to rerun the plan. This is due to an assertion check on the state of a virtual machine, which, as the result of the prematurely terminated test recovery, is in an invalid state. This has been fixed.

- **Reconfiguring replication to include a disk that was previously excluded, and using a replication seed for this disk, results in vSphere Replication erroneously removing the replication seed.**

If you have a replication with an excluded disk and later reconfigure the replication to include that disk, and then you manually copy a disk file to use as a replication seed, vSphere Replication removes the copied .vmdk file, ignoring the fact that it was an initial copy that was not created by vSphere Replication. This requires you to copy the .vmdk file to the target site again. This has been fixed.

- **Unconfiguring replications or running reprotect fails after upgrading SRM and vSphere Replication.**

If you have run a test recovery without performing cleanup and then you upgraded vSphere Replication to version 5.5, unconfiguring a replication or performing reprotect fails with the error `VRM Server generic error ... 'Error while committing the transaction'`. This error occurs because vSphere Replication fails to clean up the data for the test image in the vSphere Replication database during upgrade.

Secure because Replicator's replication fails to clean up the data for the test image in the Replicator's database during upgrade, preventing further removal of the replication. This has been fixed.

- **IP Customization fails during a recovery or test recovery.**

When running a recovery or test recovery of a recovery plan, IP customization fails for some or all virtual machines, for either of the following reasons:

- On some Windows virtual machines that have altered paths for temporary folders, IP customization looks in the wrong place for the result logs. See [KB 2021083](#) for details. This has been fixed.
- If an intermediate result log was inaccessible while performing IP Customization on Windows virtual machines, the customization completes successfully but reports the error **Error - Cannot complete customization, possibly due to a scripting runtime error or invalid script parameters (Error code: -1). IP settings may have been partially applied.** This has been fixed. IP customization now correctly reports success.

- **SRM fails to mount VMFS volumes with the error **Already Mounted.****

When SRM gets information from vCenter Server, SRM shows that the volume that contains a virtual machine is not mounted. However, at the same time, ESXi Server mounts the volume successfully. SRM tries to mount the volume based on previous information from vCenter Server and shows that the volume is in an invalid state, and says that it is already mounted. This has been fixed.

- **SRM installation leads to an MsiExec error on Windows Server 2012, and can fail with the error **ERROR: Could not open service: ProtectedStorage.****

SRM installer attempts to start the Protected Storage service, which does not exist on Server 2012. In most cases, installation succeeds, but the Windows event log records an MsiExec error. If Windows error reporting is set to "I don't want to participate, and don't ask again", the SRM installation fails and is rolled back. This has been fixed.

- **vSphere Replication management server becomes unresponsive due to a potential memory leak when attempting to connect several times to vCenter Server or vSphere Replication Server.**

This issue has been resolved in this release.

- **SRM service stops at the Attach SCSI LUN step during a test recovery.**

When running a test of a recovery plan, the SRM service stops unexpectedly during the Attach SCSI LUN step. The recovery plan test starts correctly and proceeds to the Create Writeable Storage Snapshot step, at which point the test plan does not progress further. The system eventually reports that the SRM service is no longer available. The SRM logs include the error **Panic: Assert Failed: "_completions.find(tag) == _completions.end() (Operation added with duplicate tag)".** After restarting the SRM service, the test of the recovery plan shows up as incomplete. Rerunning the test fails, and the only option is to perform cleanup. This issue occurs when SCSI LUNs have duplicate device IDs, for example two LUNs on different arrays have the same ID. This has been fixed.

- **Invoking failover from the SRM API performs disaster recovery.**

In SRM 5.0.x and 5.1.x, if you invoked failover by using the SRM API, SRM performed planned migration. This was inconsistent with the API documentation. In SRM 5.5, SRM insures consistency between the documentation and implementation of the API by performing disaster recovery. This is the correct behavior.

- **Planned migration fails during shutdown of some virtual machines because they are in an invalid state.**

Planned migration fails for some virtual machines with the error **Error - Received SOAP response fault from [virtual machine]: shutdownGuest The attempted operation cannot be performed in the current state (Powered on).** This error is caused by SRM attempting to shut down a virtual machine while it is still in the process of changing state. SRM now attempts to shut down a virtual machine 3 times before sending the error. If you still see this error, run the recovery again.

- **SRM Server stops unexpectedly during reprotect forced recovery.**

When using vSphere Replication and running reprotect after running a recovery with the forced recovery option selected, the SRM Server stops unexpectedly with the error **Panic: Assert Failed: "!peerHmsServerRef.IsNull()".** SRM Server was unable to find the remote vSphere Replication management server. This has been fixed.

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.

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

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

- **Datastore browser does not show datastore folders if the datastore name contains certain characters.**

When selecting a target datastore folder for vSphere Replication, if the datastore name contains certain characters, such as opening or closing parentheses or a space, the datastore browser window does not show the subfolders of the datastore.

Workaround: To select a subfolder of a datastore that contains a parenthesis character or a space, select the datastore and click the

Open button in the datastore browser. This opens the datastore and displays the datastore folders.

- **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.

- **Cannot configure a virtual machine with physical mode RDM disk even if the disk is excluded from replication.**

If you configure vSphere Replication on a virtual machine with a physical mode RDM disk, you might see the following error:

VRM Server generic error. Check the documentation for any troubleshooting information. The detailed exception is: HMS can not set disk UUID for disks of VM : MoRef: type = VirtualMachine, value = , serverGuid = null'.

Workaround: None. You cannot configure vSphere Replication on virtual machines that contain physical mode RDM disks.

- **Non-ASCII passwords not accepted by virtual appliance management interface (VAMI)**

Attempts to log in to VAMI with an account with a password that uses non-ASCII character fails. This occurs even when correct authentication information is provided. This issue occurs in all cases where non-ASCII passwords are used with VAMI. To avoid this issue, use ASCII passwords or connect using SSH.

- **Reprotect fails with an error message that contains `Unable to communicate with the remote host, since it is disconnected`.**

This error might be due to the fact that the protected side cluster has been configured to use Distributed Power Management (DPM), and one of the ESX hosts required for the operation was put into standby mode. This could happen if DPM detected that the host had been idle, and put it in the standby mode. SRM had to communicate to the host in order to access the replicated datastore managed by this host. SRM does not manage the DPM state on the protected site but does, however, manage the DPM state during recovery, test, and cleanup on the recovery site.

Workaround: If the error persists, temporarily turn off DPM and ensure the ESX hosts managing the replicated datastores on the protected side are turned on before attempting to run reprotect.

- **Datastores Fail to Unmount When on Distributed Power Management (DPM) Enabled Clusters**

Planned migrations and disaster recoveries fail to unmount datastores from hosts that are attached to a DPM cluster if the host enters standby mode. The error Error: Cannot unmount datastore *datastorename* from host *hostname*. Unable to communicate with the remote host, since it is disconnected might appear. To resolve this issue, turn off DPM at the protected site before completing planned migrations or disaster recoveries. You can choose to turn DPM back on after completing recovery tasks.

- **SRM 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, SRM Server asserts.

Workaround: Restart SRM 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. SRM 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, SRM does not update the information in the SRM 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, SRM must have access to raw disk mapping and parent disk files. Without this access, SRM cannot determine disk types during recovery. In such a case, SRM 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.

- **Running reprotect fails with error: Protection Group '{*protectionGroupName*}' has protected VMs with placeholders which need**

- 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 SRM runs a reprotect on the protection group, SRM 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.

- **vSphere Replication Appliance Fails to Support Valid ESX Hosts**

During vSphere Replication configuration, when a datastore is being selected on a supported version of ESX, the message VR server *Server Name* has no hosts through which to access destination datastore ... appears. This occurs when adding a new host to vCenter Server or during registration of vSphere Replication server, if there is a temporary interruption of communication between the vSphere Replication appliance and the vSphere Replication server. Communication problems typically arise due to temporary loss of connectivity or to the server services being stopped.

To resolve this issue, restart the vSphere Replication management server service.

1. Log into the virtual appliance management interface (VAMI) of the vSphere Replication appliance at `https://vr_appliance_address:5480`.
2. Click **Configuration** > **Restart** under **Service Status**.

- **Recovered VMFS volume fails to mount with error: Failed to recover datastore.**

This error might occur due to a latency between vCenter, ESXi and SRM Server.

Workaround: Rerun the recovery plan.

- **When protection site LUNs encounter All Paths Down (APD) or Permanent Device Loss (PDL), SRM 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 SRM 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 SRM 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, SRM fails to power off production virtual machines.

2. If the virtual machines have RDM devices, SRM 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, SRM 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, SRM 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 SRM 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 SRM 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 SRM 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.

- **Replication stalls after reverting to a snapshot if this snapshot was taken while replication was paused.**

When you configure replication for a virtual machine and pause the replication, take a snapshot, then resume the replication and revert to the snapshot, instead of going into the paused state, the replication status in the UI does not change and makes no progress.

Workaround: Pause and then resume the replication.

- **Operations on vSphere Replication sometimes fail with a read timed out error.**

Operations on vSphere Replication sometimes fail with root cause error **java.net.SocketTimeoutException: Read timed out**. This can happen if the ESXi Server host is slow or is running many other operations, such as Storage vMotion, at the same time as vSphere Replication is configuring, reconfiguring, stopping, or reversing replications. The following error is encountered in case of reverse replication: **Unable to reverse replication for the virtual machine virtual_machine. VRM Server generic error. Please check the documentation for any troubleshooting information. The detailed exception is: 'java.net.SocketTimeoutException: Read timed out'**

Workaround: Rerun the operation when other operations on the ESXi Server have finished.

- **vSphere Replication operations fail with a Not Authenticated error.**

If you start an operation on one SRM site, for example configuring vSphere Replication on a virtual machine, and then restart vCenter

Server and the vSphere Replication appliance on the other site, vSphere Replication operations can fail with the error **VRM Server generic error. Please check the documentation for any troubleshooting information. The detailed exception is:**

'com.vmware.vim.binding.vim.fault.NotAuthenticated'. This problem is caused by the fact that the vSphere Replication server retains in its cache the connection session from before you restarted vCenter Server and the vSphere Replication appliance.

Workaround: Clear the vSphere Replication connection cache by logging out of the SRM client or vSphere Web Client and logging back in again.

- **Cleanup of a test recovery fails after ESXi hosts are put into and taken out of maintenance mode.**

If you perform a test recovery when ESXi hosts on the recovery site are in maintenance mode, the test recovery fails as expected. If you take the ESXi hosts out of maintenance mode and perform cleanup, the cleanup fails with errors that state that the hosts are still in maintenance mode.

Workaround: After you take the hosts out of maintenance mode, wait for approximately 10 minutes before running cleanup. Alternatively, restart the SRM Server after taking the hosts out of maintenance mode and before running cleanup.

- **Cannot install vSphere Client on a domain controller.**

In previous releases, it was possible to install vSphere Client on a host machine that is an Active Directory domain controller. In vSphere 5.5, if the vSphere installer detects Active Directory services, it does not permit you to install vSphere Client.

Workaround: Install the vSphere Client before you install the Active Directory Services role or before you promote the server to be an Active Directory domain controller.

- **SRM Server on the protected site stops unexpectedly during reprotect operations.**

SRM Server on the protected site can unexpectedly stop if you start a reprotect operation immediately after a successful planned migration. This is caused by a delay in discovering the list of replicated devices on the storage array after a planned migration. If you run into this issue, the following error appears in the logs:

Error - Failed to reverse replication for failed over devices. SRA command 'prepareReverseReplication' failed. Address of the storage array is not reachable. Storage array might be down or IP address entered might be incorrect. Ensure that the storage array is up and running and the IP address of the storage array is reachable through the command line interface.

Workaround: Wait for approximately 10 minutes after performing recovery before you perform reprotect.

- **vSphere Replication server registration might take a long time depending on the number of hosts in the vCenter Server inventory.**

If the vCenter Server inventory contains a few hundred or more hosts, the **Register VR server** task takes 10 to 20 minutes to complete, as vSphere Replication updates each host's SSL thumbprint registry.

Workaround: Wait for the registration task to complete. After it finishes, you can use vSphere Replication for incoming replication traffic. See also [vSphere Replication Server Registration Takes Several Minutes](#).

- **Running reprotect on recovered virtual machines with snapshots fails with a datastore locked error, when you use ESXi Server 5.0.**

If you recover a virtual machine that you protect with vSphere Replication, and if the virtual machine has snapshots, running reprotect after the recovery results in a datastore locked error. This error only occurs if you are running ESXi Server 5.0 and if you have not selected the advanced setting to preserve multiple point-in-time (MPIT) snapshots on recovery.

Workaround: Remove replication from the recovered virtual machine then reconfigure vSphere Replication. You can then perform reprotect.

- **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 SRM interface.

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

- **Running multiple vCenter Server instances in linked mode causes duplicate SRM roles to appear**

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

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

- **Configuring protection fails with placeholder creation error**

Configuring protection on a large number of virtual machines at the same time fails with either a placeholder creation timeout error or a placeholder creation naming error:

- Placeholder VM creation error:Operation timed out:300 seconds
- Placeholder VM creation error:The name 'placeholder_name' already exists

Workaround: See [Configuring Protection fails with Placeholder Creation Error](#) in *SRM 5.5 Administration*.

- In a shared recovery site configuration, operations fail with the error The connection to the remote server is down.**

Test recovery, recovery, and reprotect operations can fail in a shared recovery site configuration if the vSphere Replication server experiences a heavy load.

Workaround: Do not perform concurrent operations on more than 200 virtual machines, with a maximum of number of 20 virtual machines per protected site.

- During replication of multiple virtual machines, a vSphere Replication server might enter a state where it does not accept any further VRMS connections but continues to replicate virtual machines.**

Workaround: Reboot the vSphere Replication server.

- Moving multiple replications from one vSphere Replication server to another results in error.**

vSphere Replication reconfigure or move operations fail with the error `SocketTimeoutException: Read timed out` and replications go into the Error state. When the source or target vSphere Replication server and the storage are under heavy load, moving a replication can take more than a few minutes and can result in the timeout error.

Workaround: Reconfigure the replication on the new vSphere Replication server.

- Test recovery of a virtual machine with RDM fails at the Configure Storage step while powering on the virtual machine.**

Test recovery fails in the following situations:

- A virtual machine with RDM configured is protected on the primary site.
- In Sites > Resource Mappings, the protected site resource that contains the virtual machine is mapped to a vApp as the secondary site resource.

Workaround: Map the virtual machine to a type of resource that is not a vApp, such as a host, on the secondary site.

- 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.

- Virtual machine VNIC's MAC address is usually preserved during recovery.**

Under very rare circumstances, test or recovery might fail to recover a specific virtual machine because vCenter unexpectedly assigns a new MAC address to the virtual machine's VNIC on the recovery site. The error message in the result column in the recovery steps is the following: `Error - Cannot complete customization, possibly due to a scripting runtime error or invalid script parameters (Error code: 255). IP settings might have been partially applied.` The SRM logs contain a message: `Error finding the specified NIC for MAC address = xx:xx:xx:xx:xx:xx` where `xx:xx:xx:xx:xx:xx` is the expected MAC address.

Workaround: Modify the affected virtual machine's MAC address manually in the vSphere Client virtual machine Properties to "xx:xx:xx:xx:xx:xx" and restart the recovery plan.

- Events Not Displayed Properly for Traditional Chinese Operating Systems**

When the vSphere Client starts, it determines the locale on which it is running, and then chooses the set of messages to display based on the locale. When the vSphere Client is installed on a Traditional Chinese operating system, the client requests messages from the zh_TW folder from the vCenter Server installation because the vCenter Server and the vSphere Client are localized for Traditional Chinese. While the vCenter Server and vSphere Client are localized for Traditional Chinese, SRM is not. Therefore, XXX messages are displayed, instead of SRM Server messages.

Workaround:

- Create a copy of the en folder which in `C:\Program Files\VMware\Infrastructure\VirtualCenter Server\extensions\com.vmware.vcDr\locale\`.
- Rename the folder from en to zh_TW.
- Restart the vCenter Server and SRM services.

- **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.

- **SRM Server stops unexpectedly if you run test cleanup after upgrading to SRM 5.5.1 without upgrading the SRAs.**

If you use array-based replication and upgrade SRM to version 5.5.1 but do not upgrade the SRAs, SRM Server stops unexpectedly when you run a test cleanup.

Workaround: Upgrade the SRAs to their appropriate version for 5.5.1.

- **Per-CPU license count is incorrect**

Some customers who purchased SRM 1.x and SRM 4.0 might still be using per-CPU allocated licenses rather than per-VM licenses. It is possible that fewer per-CPU licenses than are required by SRM 5.5 will be granted.

Workaround: None.

- **Reprotect fails after reconfiguring replication of a virtual machine to the virtual machine's original placeholder folder.**

If you remove vSphere Replication from a virtual machine that you have included in a protection group and recovery plan, then reconfigure replication on the virtual machine and use **Specify the Target Folder** to select the virtual machine's original placeholder datastore folder, recovery succeeds but reprotect fails with the error **Error: Unable to reverse replication for the VM 'virtual_machine', A recovered disk was not found for replicated disk with UUID.**

Workaround: If you reconfigure vSphere Replication on virtual machines that are already included in an SRM protection group, recreate the protection group. Do not use **Specify the Target Folder** when configuring replication.

- **X-vMotion of a virtual SAN virtual machine from a High Availability (HA) cluster might result in an alarm.**

When you perform a X-vMotion of a virtual SAN virtual machine from HA cluster to a different cluster and to a different storage, the virtual machine reports an alarm similar to **vSphere HA virtual machine failover failed.**

Workaround: None.