VMware Site Recovery Manager 5.5 Release Notes

Updated on 03/31/2015

VMware vCenter Site Recovery Manager 5.5 | 22 SEP 2013 | Build 1315893

Last updated: 31 MAR 2015

Check for additions and updates to these release notes.

What's in the Release Notes

These release notes cover the following topics:

What's New in SRM 5.5

VMware vCenter Site Recovery Manager 5.5 adds the following new features and improvements.

- Use Storage DRS and Storage vMotion on sites that SRM protects:
  - vSphere Replication supports movement of virtual machines by Storage DRS and Storage vMotion on the protected site. See Using SRM with vSphere Replication on Sites with Storage DRS or Storage vMotion.
  - Array-based replication supports movement of virtual machines by Storage DRS and Storage vMotion within a consistency group. See Using SRM with Array-Based Replication on Sites with Storage DRS or Storage vMotion.
- Preserve multiple point-in-time (PIT) images of virtual machines that are protected with vSphere Replication. See Replicating a Virtual Machine and Enabling Multiple Point in Time Instances.
- Protect virtual machines that reside on VMware vSphere Flash Read Cache storage. vSphere Flash Read Cache is disabled on virtual machines after recovery.

Localization

VMware vCenter Site Recovery Manager 5.5 is available in the following languages:

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

Compatibility

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 VSA Support

SRM 5.5 can protect virtual machines that reside on the vSphere Storage Appliance (VSA) by using vSphere Replication. VSA does not require a Storage Replication Adapter (SRA) to work with SRM 5.5.

Installation and Upgrade

For an evaluation guide to assist with a technical walkthrough of major features and capabilities of Site Recovery Manager 5.x, see the VMware vCenter Site Recovery Manager Resources for Business Continuity.

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

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

IMPORTANT: When upgrading vSphere Replication, do not select the option in **Update** > **Settings** in the virtual appliance management interface VAMI to automatically update vSphere Replication. If you select automatic updates, VAMI updates vSphere Replication to the latest version, which might not be compatible with SRM 5.5 and vCenter Server 5.5. Leave the update setting set to **No automatic updates**.

Upgrading Sites that Include Virtual Machines with RDM

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 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:

```
recovereddeviceinfo       unique_key + n
peerdevicegroup           ''
peerdevicegrouphasvalue   0
```

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

```
db_id                 unique_key + n
mo_id                 ''
ref_count             1
device                (value of pds_rdmrecoveryinfo.device  n)
peerdevice            ''
peerdevicehasvalue    0
```

9. Start the Site Recovery Manager service.

Operational Limits for SRM and vSphere Replication

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

For the protection and recovery limits when using SRM 5.5 and vSphere Replication 5.5 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 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

- vSphere 5.5 includes VMware Virtual SAN as an experimental feature. You can perform testing with Virtual SAN, but it is not supported for use in a production environment. Using SRM and vSphere Replication with VMware Virtual SAN is possible but it is not supported. See Using vSphere Replication with Virtual SAN Storage for the limitations when using Virtual SAN with SRM and vSphere Replication. See the Virtual SAN Public Beta Community for information about how to enable Virtual SAN. VMware cannot troubleshoot, provide workarounds or provide fixes for Virtual SAN. If you experiment with Virtual SAN, VMware is interested in any feedback that you are willing to share. Please submit a support request through the access methods outlined in the Virtual SAN Public Beta Community pages:
  - Virtual SAN Public Beta URL for existing customers
  - Virtual SAN Public Beta URL for new customers
- SRM 5.5 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.
- SRM 5.5 no longer supports IBM DB2 as the SRM database, in accordance with the removal of support for DB2 as a supported database for vCenter Server 5.5. If you use DB2 as the SRM database or as an external vSphere Replication database, contact VMware support for instructions about how to migrate your data to a supported database.
- 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.
- Limitations apply when you use SRM 5.5 in a shared recovery site (N:1) configuration. See Known Issues when Using SRM 5.5 in a Shared Recovery Site Configuration.
- You can use array-based protection with SRM 5.5 to protect a maximum of 50 LUNs. See Limitations to Using SRM with Array-Based Replication in Large-Scale Environments.

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.

- **NEW Running recovery on multiple LUNs simultaneously results in errors and timeouts.**

  If you have a large-scale SRM 5.5.0 environment, that involves between 50 to 255 Fibre Channel LUNs, and if you run recovery on more than 50 LUNs simultaneously, you might notice recovery timeouts, errors, and failures related to the LUNs and in some cases to the virtual machines. In some cases, you might have to run the recovery plan multiple times before it succeeds. This occurs whether you are protecting the LUNs in a single recovery plan or in multiple recovery plans.

  Workaround: See KB 2059498.

- **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.

- **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.

- **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.

- **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.

- **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

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_applliance_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.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 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.

- **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.

- **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.

- **Internal error occurs during recovery.**

  SRM retrieves various information from vCenter during the recovery process. If it does not receive critical information required to proceed, an internal error `CannotFetchVcObjectProperty` can occur. This error might occur when vCenter is under heavy stress or an ESXi host becomes unavailable due to heavy stress. This error might also occur when SRM tries to look up information of an ESXi host that is in a disconnected state or has been removed from vCenter inventory.

  Workaround: Rerun the recovery plan.

- **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`.

- **SRM Might Encounter Errors Mounting Datastores During Recoveries**

  During a test recovery or actual failover, SRM waits for recovered datastores to become available. After datastores become available, SRM attempts to mount any datastores that are not mounted. In rare instances, these datastores are automatically mounted before SRM can mount them. If this occurs during a test failover, the failover does not complete. If this occurs during an actual recovery, the recovery completes with an error. To resolve this issue, retry the recovery.

- **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.

  Workaround: Rerun the planned migration again after vSphere vMotion of the virtual machine has finished.

- **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.

- **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.

- **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.

- **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.

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

  If you perfom 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.
- **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.
- **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.**

  If you perform a recovery on a virtual machine that includes one empty thin-provisioned disk, and if you have configured SRM not to wait for VMware tools or power on this virtual machine, performing reprotect within a few seconds after the recovery causes SRM Server on the protected site to stop unexpectedly. When you restart SRM Server, 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.
  ```

  Running cleanup results in the same error. This error does not occur for virtual machines with disks that are not empty and that have an operating system installed. This problem usually only occurs if you start reprotect by using the SRM API. If you start reprotect from the SRM interface, the time between the end of the recovery and the moment that you start reprotect is sufficient for this issue not to occur.

  Workaround: Wait for a few seconds 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.
- **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, preventing further removal of the replication.

  Workaround: Run test cleanup before you upgrade SRM and vSphere Replication to version 5.5. If you have already upgraded SRM and vSphere Replication to version 5.5, you must manually delete the test data from the vSphere Replication database on the recovery site.

  External SQL Server or Oracle Server database:

  1. Log into the host machine for the vSphere Replication database on the recovery site.
  2. Run the following SQL statements on the vSphere Replication database:

     ```
     delete from DiskImageEntity where vmImage_dbId in (select dbId from VmImageEntity where groupImage_dbId not in (select COALESCE(committedImage_dbId, 0) from SecondaryGroupEntity));
     delete from ConfigFileImageEntity where vmImage_dbId in (select dbId from VmImageEntity where groupImage_dbId not in (select COALESCE(committedImage_dbId, 0) from SecondaryGroupEntity));
     delete from VmImageEntity where groupImage_dbId not in (select COALESCE(committedImage_dbId, 0) from SecondaryGroupEntity);
     delete from GroupImageEntity where dbId not in (select COALESCE(committedImage_dbId, 0) from SecondaryGroupEntity);
     ```

  Embedded PostgreSQL vSphere Replication database:

  1. Log into the vSphere Replication appliance on the recovery site.
  2. Type the following command:

     ```
     /opt/vmware/vpostgresql/1.0/bin/psql -U vrmsdb
     ```

  3. Run the following SQL statements:

```
delete from DiskImageEntity where vmImage_dbId in (select dbId from VmImageEntity where groupImage_dbId not in (select
COALESCE(committedImage_dbId, 0) from SecondaryGroupEntity));
delete from ConfigFileImageEntity where vmImage_dbId in (select dbId from VmImageEntity where groupImage_dbId not in (select
COALESCE(committedImage_dbId, 0) from SecondaryGroupEntity));
delete from VmImageEntity where groupImage_dbId not in (select COALESCE(committedImage_dbId, 0) from SecondaryGroupEntity);
delete from GroupImageEntity where dbId not in (select COALESCE(committedImage_dbId, 0) from SecondaryGroupEntity);
```

4. Type `\q` or press CTRL+D to exit.

- **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.

Known Issues when Using SRM 5.5 in a Shared Recovery Site Configuration

If you use SRM 5.5 with a shared recovery site configuraton, also known as an N:1 configuration, the following known issues apply. See http://kb.vmware.com/kb/2008061 for the protection and recovery limits when using SRM and vSphere Replication in a shared recovery site configuration.

- **vSphere Replication recovery fails with the error `Sync monitoring aborted.`**

  When running a vSphere Replication recovery in a shared recovery site configuration, the recovery can fail with the error `Error - VR synchronization failed for VRM group replication_group. Sync monitoring aborted. Please verify replication traffic connectivity between source host and target VR server. Sync will automatically resume when connectivity issues are resolved`. This problem might occur if the recovery site is loaded as follows:

  - There are virtual machines with disks of greater than 2TB
  - There are many virtual machines to recover

  Workaround:

  1. Log into the vSphere Replication appliance as root.
  2. Open the `/opt/vmware/hms/conf/hms-configuration.xml` file.
  3. Change the value in the `<hms-sync-secondary-passive-state-toleration-period>` tag to 900000 milliseconds.
  4. Save the changes and restart the vSphere Replication service:

     ```
     service hms restart
     ```

- **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` where 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" and restart the recovery plan.

- **SRM reports timeout errors while powering on the virtual machines on the shared recovery site.**

  In a large SRM setup, if a single vCenter Server manages a large number of virtual machines on the shared recovery site, for example 1000 or more, SRM can report timeout errors while powering on the virtual machines on the shared recovery site. The error message is `Error:Operation timed out:900 seconds`.

  Workaround:

  1. Go to `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` on the SRM Server host machine on the recovery site.
  2. Open the `vmware-dr.xml` in a text editor.
  3. Increase the default `RemoteManager` timeout value from 900 to a larger number, for example 1200.

     ```
     <RemoteManager>
         <DefaultTimeout>900</DefaultTimeout>
      </RemoteManager>
     ```

  4. Restart the SRM Server service.

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

- **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.