

VMware Site Recovery Manager 8.3 Release Notes

 Updated on 01/04/2024

- VMware Site Recovery Manager 8.3.0.2 | 18 JUN 2020 | Build 16356494 | [Download](#)
- VMware Site Recovery Manager 8.3.0.2 Virtual Appliance | 18 JUN 2020 | Build 16356473 | [Download](#)
- VMware Site Recovery Manager 8.3.0.1 | 14 MAY 2020 | Build 16168268 | [Download](#)
- VMware Site Recovery Manager 8.3.0.1 Virtual Appliance | 14 MAY 2020 | Build 16168265 | [Download](#)
- VMware Site Recovery Manager 8.3 | 02 APR 2020 | Build 15928802 | [Download](#)
- VMware Site Recovery Manager 8.3 Virtual Appliance | 02 APR 2020 | Build 15929234 | [Download](#)
- VMware Site Recovery Manager 8.3 Configuration Import/Export Tool | 02 APR 2020 | Build 15928802 | [Download](#)
- Check for additions and updates to these release notes.

For information about the VMware Site Recovery Manager 8.3 patch releases, see the corresponding section of these release notes.

- [VMware Site Recovery Manager 8.3.0.2 Express Patch](#)
- [VMware Site Recovery Manager 8.3.0.1 Express Patch](#)

What's in the Release Notes

These release notes cover the following topics:

- [What's New in Site Recovery Manager 8.3](#)
- [Localization](#)
- [Compatibility](#)
- [Product Support Notice](#)
- [Installation and Upgrade](#)
- [Migration to Site Recovery Manager Virtual Appliance](#)
- [Network Security](#)
- [Operational Limits of Site Recovery Manager](#)
- [Open Source Components](#)
- [Caveats and Limitations](#)
- [Available Patch Releases](#)
- [Resolved Issues](#)
- [Known Issues](#)

What's New in Site Recovery Manager 8.3

- VMware Site Recovery Manager 8.3 adds compatibility with VMware vSphere 7.0.
- Support for VMware vSphere Virtual Volumes through array-based replication. Site Recovery Manager 8.3 supports protection and orchestrated recovery of virtual machines that are located on Virtual Volume datastores and replicated by array-based replication.
- Accelerate protection - automatic protection of virtual machines, part of array-based and Virtual Volumes replication.
- Enhanced security. Site Recovery Manager adds support for vSphere Trust Authority with array based replication.
- VMware Site Recovery Manager Appliance FIPS 140-2 validation. You can enable Federal Information Processing Standard 140-2 by following the steps in [KB 78280](#).
- VMware Site Recovery Manager is compatible with N-1 version of VMware Site Recovery Manager on the paired site. For example, if the current version of VMware Site Recovery Manager is 8.3, the supported versions for the paired site is 8.2 and later.
- Enhancements to the Site Recovery User Interface:
 - Export all DataGrids in .csv format
 - Show and Hide columns
 - Add and Remove Datastores actions in array-based Protection Groups
 - vSphere Replication details and reporting
- Enhancements to Site Recovery Manager public API. Site Recovery Manager 8.3 introduces new methods in the product [public API](#).

- Site Recovery Manager Appliance Management Interface APIs
 - Configuration: PSC, SSO, ports, extension, VC address
 - Access: SSH, certificates
 - Networking and Time servers
 - Services: retrieve status, stop, start and restart services
 - Update Site Recovery Manager Appliance via update repository
 - Configure Syslog
 - Storage Replication Adapters - retrieving information, upgrade, download or upload configuration

For information about Site Recovery Manager public APIs and more extensive product automation, see [Site Recovery Manager API Developer's Guide](#).

- vRealize Operations Management Pack for Site Recovery Manager 8.3. For information about the management pack, see [VMware vRealize Operations Management Pack for Site Recovery Manager 8.3 Release Notes](#).
- vRealize Orchestrator Plug-In for VMware Site Recovery Manager 8.3. For information about the new workflows, see [VMware vRealize Orchestrator Plug-In for VMware Site Recovery Manager 8.3 Release Notes](#).

Note: For interoperability with earlier or later releases of VMware vSphere, see the [Compatibility Matrices for VMware Site Recovery Manager 8.3](#).

For information about the features of vSphere 7.0, see the [vSphere 7.0 documentation](#).

For information about the supported databases, see the [Compatibility Matrices for VMware Site Recovery Manager 8.3](#).

Localization

VMware Site Recovery Manager 8.3 is available in the following languages:

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

Compatibility

Site Recovery Manager Compatibility Matrix

Site Recovery Manager 8.3 is compatible with vSphere 6.5, vSphere 6.5 Update 1, vSphere 6.5 Update 2, vSphere 6.5 Update 3, vSphere 6.7, vSphere 6.7 Update 1, vSphere 6.7 Update 2, vSphere 6.7 Update 3, vSphere 7.0, and supports ESXi versions that vCenter Server 7.0 supports.

Site Recovery Manager 8.3 requires a supported vCenter Server version on both the protected site and the recovery site.

If you use VMware Tools 10.1 and ESXi 6.5 or 6.0, ensure the time synchronization between the ESXi host and vCenter Single Sign-On on the recovery site.

For interoperability and product compatibility information, including supported guest operating systems and support for guest operating system customization, see the [Compatibility Matrices for VMware Site Recovery Manager 8.3](#).

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](#).

Compatible vVols Partner VASA Providers

For the current list of compatible vVols Partner VASA providers, see the [VMware Compatibility Guide](#).

VMware vSAN Support

Site Recovery Manager 8.3 can protect virtual machines that reside on VMware vSAN by using vSphere Replication. vSAN does not require a Storage Replication Adapter (SRA) to work with Site Recovery Manager 8.3

Product Support Notice

This is the final release, that supports VMware Site Recovery Manager for Windows.

Installation and Upgrade

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

NOTES:

- To install or upgrade to VMware Site Recovery Manager 8.3 on Windows Server 2008 x64, Windows Server 2008 R2 x64, Windows Server 2012 x64, or Windows Server 2012 R2 x64, you must update Windows to [KB2999226](#).
- After upgrading Site Recovery Manager, Site Recovery Manager does not retain any advanced settings that you configured in the previous installation. This is by design. Due to changes in default values or improvements in performance, advanced settings that you set in a previous version of Site Recovery Manager might not be required by or compatible with the new version. Advanced settings are also not retained if you uninstall and then reinstall the same version of Site Recovery Manager.
- If the vCenter Server instances on the protected and recovery sites are in Enhanced Linked Mode, they must be direct replication partners. Otherwise, upgrade might fail.

Migration to Site Recovery Manager Virtual Appliance

You can migrate your Site Recovery Manager 8.3 instance from Windows to the Site Recovery Manager Virtual Appliance. For information about the migration procedure, see [Migrate from Site Recovery Manager for Windows to Site Recovery Manager Virtual Appliance](#).

Network Security

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

For the list of network ports that Site Recovery Manager requires to be open on both sites, see [Network Ports for Site Recovery Manager](#).

Operational Limits for Site Recovery Manager 8.3

For the operational limits of Site Recovery Manager 8.3, see [Operational Limits of Site Recovery Manager](#).

Open Source Components

The copyright statements and licenses applicable to the open source software components distributed in Site Recovery Manager 8.3 are available at [VMware Site Recovery Manager Downloads](#). You can also download the source files for any GPL, LGPL, or similar licenses that require the source code or modifications to the source code to be made available for the most recent generally available release of vCenter Site Recovery Manager.

Caveats and Limitations

- Site Recovery Manager does not support the protection of virtual machines using persistent memory (PMem) devices.
- If you use vVols replication, use a local VMFS datastore as the placeholder datastore.
- When a linked clone virtual machine is created, some of its disks continue to use the base virtual machine disks. If you use vVols replication, you must replicate the linked clone virtual machine on the same replication group as the base virtual machine, otherwise you get the following error message: "Virtual machine '{vmName}' is replicated by multiple replication groups." If you have to replicate the base virtual machine in a different replication group than the linked clone virtual machines, or the base virtual machine cannot be replicated at all, the linked clone virtual machines must be converted to full clones.
- Encrypted virtual machines in vVols protection groups are not supported when the vCenter Server is version 6.7 Update 3.
- Enabling the SHA-1 hashing function in Site Recovery Manager 8.3 for Windows is not supported. To enable SHA-1, you must use the Site Recovery Manager 8.3 Appliance.
- The Site Recovery Manager virtual appliance supports configuration with a single network adapter.
- Network auto-mapping for storage policy protection groups is not supported on NSX-T Data Centers.
- The protection and recovery of encrypted virtual machines with array-based replication requires VMware vSphere 6.7 or later.
- The protection and recovery of encrypted virtual machines with vSphere Replication requires VMware vSphere 6.7 Update 1 or later.
- Site Recovery Manager 8.3 does not support the recovery of encrypted virtual machines in array-based replication protection groups on vCenter Server 6.5 Update 2.
- The VMware Site Recovery Manager 8.3 Configuration Import/Export Tool Importing attempts to import the recovery settings of protected virtual machines only once no matter whether the protected virtual machines are part of one or many recovery plans.
- vSphere Flash Read Cache is disabled on virtual machines after recovery and the reservation is set to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take a note of the virtual machine's cache reservation from the vSphere Web Client. You can reconfigure vSphere Flash Read Cache on the virtual machine after the recovery.
- Site Recovery Manager 8.3 supports the protection of virtual machines with uni-processor vSphere FT, but deactivates uni-processor vSphere FT on the virtual machines on the recovery site after a recovery.
 - If you use uni-processor vSphere FT on virtual machines, you must configure the virtual machines on the protected site so that Site Recovery Manager can deactivate vSphere FT after a recovery. For information about how to configure virtual machines for uni-processor vSphere FT on the protected site, see <https://kb.vmware.com/kb/2109813>.

- You cannot use vSphere Replications Point-in-Time Snapshots with virtual machines where the replication target is a Virtual Volumes datastore.
- When using vSphere Virtual Volumes storage as a replication target all disks belonging to the virtual machine must be replicated to a single vSphere Virtual Volumes datastore.
- When a replicated virtual machine is located on vSphere Virtual Volumes storage, all disks belonging to that virtual machine must be located on a single vSphere Virtual Volumes datastore.
- Site Recovery Manager 8.3 does not support NFS v 4.1 datastores for array-based replication and vVols replication. You can use Site Recovery Manager 8.3.x with NFS v 4.1 datastores for vSphere Replication.
- Site Recovery Manager does not support reconfiguration of storage profile protection groups, such as changing the set of associated storage policies, group name, or descriptions. To modify a storage profile protection group, you must delete it and recreate it with the new configuration.
- Site Recovery Manager cannot protect RDM disks or fault-tolerant virtual machines in storage policy protection groups.
- Site Recovery Manager does not support the mapping or exclusion of nonreplicated virtual devices in storage policy protection groups.
- To use Two-factor authentication with RSA SecureID or Smart Card (Common Access Card) authentication your environment must meet the following requirements:
 1. Use the administrator credentials of your Platform Services Controller to install Site Recovery Manager 8.3 and to pair your Site Recovery Manager 8.3 sites.
 2. The vCenter Server instances on both Site Recovery Manager 8.3 sites must work in Enhanced Linked Mode. To prevent failures during upgrade of Site Recovery Manager from 8.3 to a newer version of Site Recovery Manager, the vCenter Server instances on both sites must be direct replication partners.

Available Patch Releases

VMware Site Recovery Manager 8.3.0.2 Express Patch

VMware Site Recovery Manager 8.3.0.2 | 18 JUN 2020 | Build 16356494

VMware Site Recovery Manager 8.3.0.2 Virtual Appliance | 18 JUN 2020 | Build 16356473

- The VMware Site Recovery Manager 8.3.0.2 Express Patch Release provides bug fixes.

Installation and Upgrade Notes

If you are running Site Recovery Manager 8.3.0.x, upgrade to Site Recovery Manager 8.3.0.2. See [Upgrading Site Recovery Manager](#) in *Site Recovery Manager 8.3 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 8.3.0.x, upgrade the vSphere Replication appliance to version 8.3.0.2. See the [vSphere Replication 8.3 Release Notes](#) for information about vSphere Replication 8.3.0.2.

VMware Site Recovery Manager 8.3.0.1 Express Patch

VMware Site Recovery Manager 8.3.0.1 | 14 MAY 2020 | Build 16168268

VMware Site Recovery Manager 8.3.0.1 Virtual Appliance | 14 MAY 2020 | Build 16168265

- The VMware Site Recovery Manager 8.3.0.1 Express Patch Release provides bug fixes.
- The VMware Site Recovery Manager 8.3.0.1 Express Patch Release adds support for IP customization of Windows Server 2019 Guest OS.

Installation and Upgrade Notes

If you are running Site Recovery Manager 8.3, upgrade to Site Recovery Manager 8.3.0.1. See [Upgrading Site Recovery Manager](#) in *Site Recovery Manager 8.3 Installation and Configuration* for instructions about upgrading Site Recovery Manager.

If you use vSphere Replication with Site Recovery Manager 8.3.0.x, upgrade the vSphere Replication appliance to version 8.3.0.1. See the [vSphere Replication 8.3 Release Notes](#) for information about vSphere Replication 8.3.0.1.

Resolved Issues

- **NEW** Upgrading the Site Recovery Manager 8.2 virtual appliance to Site Recovery Manager 8.3 by using the URL option does not complete successfully

You can upgrade Site Recovery Manager 8.2 virtual appliance to Site Recovery Manager 8.3 by using the ISO file without any issues. When you attempt to upgrade by using the URL option, Site Recovery Manager shows that upgrade in progress and closes without any error but the upgrade process does not complete successfully.

This issue is fixed in Site Recovery Manager 8.3.0.2.

- **NEW** Planned migration with vMotion on a stretched storage on vCenter Server 6.5 fails during the "Live migration of VMs to recovery site" step

When performing a planned migration with vMotion on a stretched storage on vCenter Server 6.5, the operation fails during the **Live migration of VMs to recovery site** step with the following error: "A general system error occurred: Invalid argument : Thumbprint too long (max 60) for SSL connection".

This issue is fixed in Site Recovery Manager 8.3.0.2.

- **NEW The Site Recovery Manager server crashes when there is a protected virtual machine with fault tolerance enabled on an NFS datastore**

If you enable fault tolerance on a protected virtual machine on an NFS datastore, when the fault tolerance monitor activates the Site Recovery Manager server crashes.

This issue is fixed in Site Recovery Manager 8.3.0.2.

- **Test recovery fails at the 'Create writable storage snapshot' step**

When you create a vVols protection group to protect a vVols datastore on a Pure storage array, the test recovery fails at the 'Create writable storage snapshot' step with the following error: 'Cannot find point-in-time replica.'

This issue is fixed in Site Recovery Manager 8.3.0.1.

- **All Recovery Plans and History Reports are deleted**

If you have simultaneous restarts from both sites and multiple sequenced restarts in a single site within less than a minute, some of the Site Recovery Manager plug-ins might timeout during shutdown. As a result the remote site might delete the recovery plans and history reports.

This issue is fixed in Site Recovery Manager 8.3.0.1.

- **Recovery operation fails with "Unable to find a viable replica for VR replication group '<group name>'"**

If you add a new disk to a source virtual machine, which is configured for replication with multiple points in time, when you run a recovery plan, the recovery fails with the error message "Unable to find a viable replica for VR replication group '<group name>'".

This issue is fixed in Site Recovery Manager 8.3.0.1.

- **IP customization for Red Hat Enterprise Linux 7.4 is failing with "Cannot complete customization, possibly due to a scripting runtime error or invalid script parameters (Error code: 255). IP settings may have been partially applied."**

In rare cases, Planned Migration, Disaster Recovery or Test Recovery IP customization for Red Hat Enterprise Linux 7.4 virtual machines might fail with "Cannot complete customization, possibly due to a scripting runtime error or invalid script parameters (Error code: 255). IP settings may have been partially applied.". You can find the concrete reason for the failure in the target recovered virtual machine's `/var/log/vmware-imc/toolsDeployPkg.log` file. Two known issues related to Red Hat Enterprise Linux 7.4 are observed. In the `/var/log/vmware-imc/toolsDeployPkg.log` file, you see similar entries:

```
1. 2020-03-24T18:28:56 INFO: Customization completed.
2020-03-24T18:28:56 DEBUG: Removing lock file /var/lock/vmware/gosc.
'.
: [error] Customization command failed with stderr: 'rm: cannot remove '/var/lib/dhclient/ntp.conf.predhclient.ens192': Is a directory
...
2. 2020-03-24T18:28:56 INFO: Customization completed.
2020-03-24T18:28:56 DEBUG: Removing lock file /var/lock/vmware/gosc.
'.
: [error] Customization command failed with stderr: 'Database /etc/iproute2/rt_scopes is corrupted at ...
...
```

This issue is fixed in Site Recovery Manager 8.3.0.1

- **Site Recovery Manager recovery plan fails to recover a virtual machine on High Availability enabled cluster with "Unable to write VMX file: ..." error and the virtual machine is powered on**

This error can appear when you perform a disaster recovery without a planned migration of a virtual machine on a High Availability (HA) enabled cluster. The virtual machine was protected with Site Recovery Manager on site A, failed over to site B, then failed back to site A again on a HA configured cluster without a clean shut down on site B. In such a scenario HA on site A can power on the recovering virtual machine while Site Recovery Manager adjusts its properties.

Workaround: This issue is fixed in Site Recovery Manager 8.3.x.

Known Issues

- **Site Recovery Manager workflow fails with a NotAuthenticated error**

Every 8 hours, there is a 0-60 seconds period when a remote operation might wrongly fail with a `NotAuthenticated` error. When running a Site Recovery Manager workflow, for example, Reprotect or Failover, if you hit that time window, the workflow might fail with a `NotAuthenticated` error. Although all connections are up when you start the workflow, the active login token might expire during the execution of the workflow, causing the error.

Workaround: Re-run the workflow.

- **A CD/DVD device is not connected after the recovery of a Virtual Volumes protected VM. when the device points to an image file on a**

When a virtual machine with a CD/DVD device pointing to an image file on a datastore is recovered, you receive the following error "**Connection control operation failed for disk 'sata0:0'.**" and the device is not connected.

Workaround: Recreate the device pointing to the desired image file.

- **Exporting Site Recovery Manager configuration by using a remote Site Recovery Manager solution user fails with an error**

In a Site Recovery Manager environment with only array-based replication, when you attempt to export the Site Recovery Manager configuration by using a script without credentials, the export fails. The Impex log contains the following error:

```
2022-05-02 04:35:57,061 [srm-reactive-thread-13] ERROR com.vmware.srm.client.impex.Main - Export SRM configuration ended.
(vim.fault.NoPermission) {
  faultCause = null,
  faultMessage = null,
  object = ManagedObjectReference: type = Folder, value = group-d1, serverGuid = e288c277-4377-4abe-80ad-0e981d64badf,
  privilegeId = StorageProfile.View }
```

Workaround 1: Add "policy-driven storage view" to the remote SRM solution user role.

Workaround 2: Export the Site Recovery Manager configuration by either using a properties file or in interactive mode with credentials. See, [Use a Properties File to Export Site Recovery Manager Configuration Data](#) and [Export Site Recovery Manager Configuration Data with the Standalone Import/Export Tool](#).

- **After performing a failover, the recovered virtual machine icon shows 3 dots**

If you manually map the protected disk of a virtual machine to another disk or detach the disk in the VM protection properties under the protection group, the recovered VM icon shows 3 dots after performing a failover as if it is still a placeholder VM.

Workaround: None.

- **After upgrading vCenter Server, you might observe errors messages in the Site Recovery UI**

When you open the Site Recovery UI after upgrading your vCenter Server to version 6.7 Update 3p, you might observe the following error message: "**User is not logged in. Terminating method execution due to lack of privileges.**" The same error is observed in the dr.log and the HMS logs.

Workaround: None. Discard the error.

- **The Edit Recovery Plan wizard shows a maximum of 20 Protection Groups**

When you attempt to edit a Recovery Plan that contains more than 20 Protection Groups, the Edit Recovery Plan wizard shows only a single page with a maximum of 20 Protection Groups.

Workaround:

1. In the Protection Groups page of the Edit Recovery Plan wizard, click the filter button located to the right of the Name column or Description column.
2. Enter any text, then clear the entered text. You can now see the full list of Protection Groups.

- **Site Recovery Manager cannot apply IP subnet rules during failback of a virtual machine to a protected site if the virtual machine was recovered on an opaque network on the recovery site**

When Site Recovery Manager recovers a vNIC to an NSX-T opaque network on a recovery site, after performing reprotect and failback to the original protected site, Site Recovery Manager is unable to apply IP subnet rules for this vNIC.

Workaround 1: Remove the protection of the virtual machine and protect it again. This action defaults your VM Recovery settings and they must be specified again, if needed.

Workaround 2: Temporary attach the virtual machine NICs to other network and then attach them again to the desired opaque network.

- **If you use Chromium-based browser and you try to resize a column of a grid, the Site Recovery user interface freezes and becomes unresponsive**

LayoutNG in Chromium is having a bug that causes performance issues. For more information, see

<https://bugs.chromium.org/p/chromium/issues/detail?id=1008523> and <https://bugs.chromium.org/p/chromium/issues/detail?id=1098231>.

Workaround 1:

1. Close all Chrome windows.
2. Edit the Chrome shortcut link and update it to: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-blink-features=LayoutNG
3. Open Chrome again.

Workaround 2: Update your Chrome browser to version 85.0.4183.83 or later.

- **VMware vCenter Server 7.0 and VMware vCenter Server 7.0.0b show an error that Site Recovery Manager 8.3 and vSphere Replication 8.3 are not compatible**

If you have Site Recovery Manager 8.3 and/or vSphere Replication 8.3 installed on a vCenter Server 7.0 or a vCenter Server 7.0.0b, when you navigate to **vCenter>Monitor Tab>vCenter Server>Interoperability** Site Recovery Manager 8.3 and vSphere Replication 8.3 are displayed as "No

Workaround: None. Site Recovery Manager 8.3 and vSphere Replication 8.3 are compatible as indicated in the interoperability matrix.

- **Generation of vSphere Replication Replications report might fail**

If you delete the source virtual machine from the vCenter Server inventory before you stop the active replication, the generation of vSphere Replication Replications report (export to CVS) might fail. When a source virtual machine of an active vSphere Replication replication is deleted, vSphere Replication removes the outgoing replication on the source site and retains the incoming replication on the target site.

Workaround:

1. To make a successful vSphere Replication replications export in the Outgoing replications from the source site, you must first refresh the view to clean up the stale data.
2. To make a successful vSphere Replication replications export in the Incoming replications from the target site, you must force stop the orphaned replications if you do not need to recover them. If you cannot stop these replications, you must individually select the replications to export and exclude the orphaned ones.

- **Site Recovery Manager might not install or configure correctly if you use non-ascii characters for the vCenter Single Sign-On user name**

If your vCenter Single Sign-On user name contains non-ascii characters, when you try to install Site Recovery Manager, the installation might fail with an error: `Error 25239. Failed to configure Site Recovery Manager. Details: Provided credentials are not valid.`

Workaround: Use a vCenter Single Sign-On user name with ascii characters.

- **The Site Recovery Manager Configuration Import/Export Tool does not import all Network Mappings if the network names are the same**

If you have duplicate network names in your inventory exported with the Site Recovery Manager Configuration Import/Export Tool and you try to import the configuration data, only data related to one of the networks with such name is imported.

Workaround: Rename the networks so there are no duplicate names and export and import the configuration data again.

- **Some of the recovered virtual machines throw the following alarm 'vSphere HA virtual machine failover failed'**

During a Site Recovery Manager workflow, post Test Recovery or Failover operations, some of recovered virtual machines might throw the following alarm: `vSphere HA virtual machine failover failed`. From Site Recovery Manager perspective, there is no functional impact as all virtual machines are recovered successfully.

Workaround: None. You must acknowledge the alarm.

- **Site Recovery Manager 8.3 plug-in does not appear in the vCenter Server web client or HTML5 client**

When you install or upgrade to Site Recovery Manager 8.3 and register it with a vCenter Server version 6.5.x or 6.7.x which installed on a Windows Server, the Site Recovery Manager 8.3 plug-in does not appear in the vCenter Server web client or HTML5 client.

Workaround: See <https://kb.vmware.com/s/article/78678>.

- **After changing the vCenter Server certificates, you cannot unregister the Site Recovery Manager virtual appliance**

If you change the vCenter Server certificates and then attempt to unregister the Site Recovery Manager virtual appliance from the vCenter Server, the operation fails with the following error: `A specified parameter was not correct: connection.thumbprint`. The Site Recovery Manager Virtual Appliance Management Interface displays the thumbprint for the old certificate.

Workaround: Restart the config-service. SSH to the Site Recovery Manager virtual appliance host machine and run `sudo systemctl restart dr-configurator`.

- **Virtual machines created while a test recovery is running are not automatically protected after the test completes**

When you create a virtual machine on a protected datastore while there is a test recovery is running on an array-based protection group, the virtual machine might not be automatically protected if the test recovery process is not cleaned up within 15 minutes after the virtual machine provisioning.

Workaround 1: To initiate automatic protection, restart the Site Recovery Manager server on the protected site.

Workaround 2: Use manual protection for virtual machines in a Not configured state after a test recovery.

- **DNS servers are available in the network configuration of the Site Recovery Manager Appliance Management Interface, even if you selected static DNS without DNS servers**

When the requirements of the network settings are for No DNS servers but with automatic DHCP adapter configuration, the setting static DNS and DHCP in the adapter configuration results in DNS servers acquired from DHCP.

Workaround: Use 127.0.0.1 or ::1 in the static DNS servers list, depending on the selected IP protocol.

- **After a successful login in the Single Sign-On, you are unable to login in the Site Recovery user interface**

The Site Recovery user interface log contains the following error message `"Certificate for <host> doesn't match any of the subject alternative names: <subjectAltlist>"`. When you attempt to do a remote login within the Site Recovery user interface by using the remote login dialog, you receive similar error message in the user interface.

The Site Recovery user interface might not be able to connect to the Platform Services Controller hosts because of the way the host certificate is generated:

- If the Platform Services Controller certificate does not have a host's address (IP or FQDN) as a subject alternative name;
- If Platform Services Controller certificate lacks subject alternative names and the host name is not matched in the certificate's CN fields.

1. Reconfigure the Platform Services Controller with a certificate with a SAN (Subject Alternative Name Field) that contains an entry for the Platform Services Controller address (the '<host>' string from the error message).
2. If the certificate is properly generated, but the address used by user interface is not, you must reconfigure the user interface and the corresponding Site Recovery Manager and vSphere Replication Appliances to use the correct Platform Services Controller address.
3. Reconfigure the existing pairings for the appliances.

- **Reprotect fails when using stretch storage on some storage arrays**

The command to reverse the replication on some devices is skipped intentionally when the devices are already in the expected state. As a result the storage array are not getting required notifications and this causes the reprotect operation to fail.

Workaround:

1. Navigate to the vmware-dr.xml file and open it in a text editor.
2. Set the configuration flag `storage.forcePrepareAndReverseReplicationForNoopDevices` to true.

```
<storage >
<forcePrepareAndReverseReplicationForNoopDevices>true</forcePrepareAndReverseReplicationForNoopDevices>
</storage>
```
3. Save the file and restart the Site Recovery Manager server service.

- **When you attempt to configure IPv6 through the Site Recovery Manager Appliance Management Interface you receive an invalid property - dns error**

When you attempt to configure IPv6 through the Site Recovery Manager Appliance Management Interface and select the 'Obtain IPv6 settings automatically through router advertisement' option with auto assigned dns, the following error occurs `invalid property - dns`.

Workaround: SSH to the Site Recovery Manager Appliance host machine and run `$netmgr ip6_address --set --interface --dhcp 0 --autoconf 1 .` To receive an IP address through DHCP run `$netmgr ip6_address --set --interface --dhcp 1 --autoconf 1` instead.

- **You cannot reconfigure the IPv6 settings through the Site Recovery Manager Appliance Management Interface**

If you have configured the IPv6 network with the 'Obtain IPv6 settings automatically through router advertisement' or 'Obtain IPv6 settings automatically through DHCP' option, you are unable to reconfigure the IPv6 settings with only 'Obtain IPv6 settings automatically through DHCP'. Either both options must be selected or none of them.

Workaround: SSH to the Site Recovery Manager Appliance host machine and run `$netmgr ip6_address --set --interface --dhcp 0 --autoconf 1 .` To receive an IP address through DHCP run `$netmgr ip6_address --set --interface --dhcp 1 --autoconf 1` instead.

- **During a test recovery one of the ESXi hosts crashes**

While you are running a test recovery one of the ESXi hosts might crash with PSOD: `Assert bora/vmkernel/main/bh.c:981`.

Workaround: Restart the ESXi host.

- **When you attempt to pair a Site Recovery Manager 8.3 instance with a Site Recovery Manager 8.2 instance, you receive a warning in the Site Recovery 8.3 User Interface**

If you break the pairing of two Site Recovery Manager 8.3 instances on two different vCenter Server instances, and then attempt to pair one of the Site Recovery Manager 8.3 instance with a Site Recovery Manager 8.2 instance on another vCenter Server, you receive a `"SRM Server cannot connect to SSO Server"` warning.

Workaround: Restart the Site Recovery Manager 8.3 server.

- **Sometimes after starting the Site Recovery Manager virtual appliance, the VMware Console is not visible in the vSphere UI**

There is no blue screen, that shows information about the appliance. Because of a circular dependency and a race in the boot order, the service that is responsible for the appliance information might be scheduled off and as a result fail to provide information about the appliance. All other VMware related services in the Site Recovery Manager appliance are up and running.

Workaround: Restart the Site Recovery Manager appliance.

- **vSphere Replication appliances are not working correctly after converging vCenter Server instances in Enhanced Linked Mode with external Platform Services Controllers to embedded vCenter Sever instances in Enhanced Linked Mode**

If you have an Enhanced Linked Mode environment with external Platform Services Controllers and you converge it to embedded node, your vSphere Replication appliances might not work correctly.

Workaround: Re-register the solution user or manually add the solution user to the required groups.

- **Exporting grids is not working in the Microsoft Edge browser**

When you open a view with a grid, select **Export**, and click **All rows/Selected rows** no file is downloaded. When you attempt to export and download the history of a recovery plan, you receive an error in the console and the download files are corrupted.

Workaround: Upgrade to the latest version of the Microsoft Edge browser based on the Chromium engine.

- **You cannot remove or force stop a replication**

Workaround: Use the vSphere Replication Management Server Managed Object Browser by opening https://vrms_address:8043/mob/?vmodl=1.

1. For incoming replications, navigate to **content > replica-manager > getIncomingReplications**. For outgoing replications, navigate to **content > replication-manager > getOutgoingReplications**.

2. Change the **parameters** as follows:

start: 0

count: 2000

Clear **sorters** and **filter** and leave them blank, then click **Invoke Method**.

3. Find the replication that you need to remove by looking for the VM name and copy the replication ID (GID-<uuid> value).

4. Click on the replication ID **value > destroy > Invoke method**.

5. Click on **val > info** and ensure that the **state** value is **success** and the **error** value is **Unset**.

If the task is still in progress, refresh the info window and wait until it completes.

- **Site Recovery Manager does not populate all replicated virtual machines in a vSphere Replication protection group**

When you edit a vSphere Replication protection group and add new replicated virtual machines, Site Recovery Manager does not populate all the replicated virtual machines but only the selected VMs.

Workaround: Use the filter option in the list to find the required replicated virtual machines. When you clean-up the filter, all virtual machines appear in the protection group.

- **You cannot create alarms for Site Recovery Manager in the HTML5-based vSphere Client when using vCenter Server 6.5 Update 2 and earlier**

If you attempt to configure Site Recovery Manager alarms in the HTML5-based vSphere Client in vCenter Server 6.5 Update 2 and earlier, you receive an error message and the alarms are not created.

Workaround: Use the Flex-based vSphere Web Client for vCenter Server 6.5 Update 2 and earlier. The issue is fixed in vCenter Server 6.7 Update 1.

- **PowerCLI Connect-SrmServer command fails to connect to the Site Recovery Manager appliance using the default port**

When you try to connect to the Site Recovery Manager appliance by using the PowerCLI [Connect-SrmServer](#) command, the connection fails with the following error: [Unable to connect to the remote server](#). This is not an issue if you use the Windows version of Site Recovery Manager.

Workaround: Specify port 443 to the Site Recovery Manager appliance by using the following command [Connect-SrmServer -Port 443](#). For a complete list of all Site Recovery Manager network ports, see [Network Ports for Site Recovery Manager](#).

- **When recovering a storage policy protection group, the recovery plan might fail with the following error "Cannot fetch hosts associated with placeholder VMs. Mapping for resourcePool 'XXXXXX' missing in resource mappings." The 'XXXXXX' resourcePool' is a compute resource (host or cluster) that does not contain virtual machines protected by the storage policy protection group.**

The error appears when there is no resource inventory mapping for the compute resource, but some hosts belonging to the same compute resource have mounted some of the datastores protected by the storage policy protection group. By design, storage policy protection groups require existing resource inventory mappings for all such compute resources.

Workaround 1: Do not remove the compute resource from the vSphere inventory. Create a resource inventory mapping for the mentioned compute resource and re-run the recovery.

Workaround 2: If you have already removed the compute resource from the vSphere inventory, perform the following steps:

1. Stop the protection Site Recovery Manager server to make placeholder mappings appear in the Site Recovery user interface, and create a placeholder mapping for the same compute resource.
2. Re-run the recovery.
3. After the recovery succeeds, you might still get errors when running reprotect. If the errors persist:
 - a. Delete the affected storage policy protection group from Site Recovery Manager.
 - b. If Site Recovery Manager reprotect failed to reverse the storage replication, reverse the replication for the affected LUNs by using storage administration tools.
 - c. Run Discover Devices on the involved Site Recovery Manager array pair and verify that replication direction for the affected LUNs is correctly detected by Site Recovery Manager.
 - d. Recreate the affected storage policy protection group in the reverse direction and add it back to the affected recovery plan.

- **After migrating the Windows Site Recovery Manager server to Site Recovery Manager Virtual Appliance, the srm-server service fails to start**

After a successful migration from Site Recovery Manager for Windows to Site Recovery Manager Virtual Appliance in a federated IPv6 environment, the srm-server service of the virtual appliance fails to start.

Workaround: Reconfigure the Site Recovery Manager Virtual Appliance through the Site Recovery Manager Appliance Management Interface.

- **The pairing of the Site Recovery Manager instances fails after you install a new certificate in the Site Recovery Manager appliance**

When you change the certificate of one of the Site Recovery Manager appliances in a site pair, the connection between the sites is lost. When you attempt to reconnect the site pair from the site where the certificate is changed, the pairing operation fails.

Workaround 1: Reconnect the site pair from the site where the certificate is not changed.

Workaround 2: Restart the srm-server service in the appliance with the changed certificate and reconnect the site pair.

- **When you run a Test Recovery of a recovery plan that contains storage policy protection groups on a stretched storage cluster, you receive a**

During the Test Recovery operation Site Recovery Manager attempts to rename a test recovered stretched storage devices with the same name as the actual production stretched storage devices that is already mounted. As a result you receive a warning message **The name <Datastore_name> already exists.**

Workaround: Ignore the warning. The Site Recovery Manager workflow is not affected by the warning messages

- **The planned migration of a storage policy protection group constantly fails with ProtectionGroupNotSynced fault**

The planned migration of a storage policy protection group might fail with a **ProtectionGroupNotSynced fault: "The peer site has not finished synchronizing changes to protection group 'SP_protection_group_name'. If this is a planned migration, wait for the peer site to synchronize and then retry the workflow."**

If you continue to observe this issue after multiple planned migration re-runs, you can disable this check to complete the planned migration process successfully.

Workaround:

1. Edit the vmware-dr.xml file for both the protection and the recovery Site Recovery Manager servers with the following additional configuration:

```
<replication>  
  <failPlannedMigrationIfSitesNotSynced>false</failPlannedMigrationIfSitesNotSynced>  
</replication>
```
2. Restart both Site Recovery Manager servers.
3. Re-run the planned migration of the storage policy protection group.

- **vCenter Server shows a warning for expiring evaluation license of an on-premises Site Recovery Manager instance even when paired with a Site Recovery Manager instance in VMware Cloud on AWS**

When you pair your on-premises instance of Site Recovery Manager with a Site Recovery Manager instance in VMware Cloud on AWS, the Site Recovery Manager server uses the cloud license.

Workaround: When the on-premises instance of Site Recovery Manager is paired with a cloud site, you can ignore the warning for expiring on-premises license.

- **When you run Test Recovery on a storage policy protection group with stretched storage, you receive a warning message about possible failure of live migration**

When you run Test Recovery, you observe a warning message for a virtual machines configured for storage policy protection with stretched storage, the vpxd service restarts, and might create a core dump.

Workaround: Ignore the warning. The Site Recovery Manager workflow is not affected by the warning messages.

- **Recovery plan execution might fail to power on a virtual machine with 'InvalidArgument:path'**

When you run a recovery plan, Site Recovery Manger might fail to power on a VM with **(vmodl.fault.InvalidArgument:path)** error. The following error message appears in the Site Recovery Manager recovery site server logs:

```
YYYY-MM-DDT20:24:35.996-08:00 error vmware-dr[02448] [SRM@6876 sub=Recovery ...] Plan execution (test workflow) failed;  
plan id: 34f86036-3bc7-4c2d-a841-e15c5d781532, plan name: HBRRP_LIMITS, error: (vmodl.fault.InvalidArgument) {  
-->   faultCause = (vmodl.MethodFault) null,  
-->   faultMessage = <unset>,  
-->   invalidProperty = "path"  
-->   msg = "A specified parameter was not correct: path"  
--> }  
-->
```

This error is a result of a failing 'Relocating VM before powered on' operation on the target destination ESXi host. The related error message in the ESXi vpxa service logs is:

```
YYYY-MM-DDT03:56:48.255Z error vpxa[2099931] [Originator@6876 sub=vpxaVmprov opID=failedOpId]  
Failed to canonicalize vm register path;  
/vmfs/volumes/.../recoveredVm.vmx, err: 16(Device or resource busy)  
...  
YYYY-MM-DDT03:56:48.256Z info vpxa[2099931] [Originator@6876 sub=Default opID=failedOpId]  
[VpxLRO] -- ERROR task-1824 -- vpxa -- vpxapi.VpxaService.registerVm: vmodl.fault.InvalidArgument:  
--> Result:  
--> (vmodl.fault.InvalidArgument) {  
-->   faultCause = (vmodl.MethodFault) null,  
-->   faultMessage = <unset>,  
-->   invalidProperty = "path"
```

- **Devices and Datastores information is missing during the failover of a recovery plan with array-based replication protection groups**

When you run a recovery plan failover, depending on the SAN type and whether it detaches the datastore from the host during recovery, the information in the Devices and the Datastores tabs might disappear during the failover process.

Workaround: None. The information in both tabs appears again after a successful reprotect.

- **Reprotect fails with Internal error: Received unexpected exception during prepare phase. The session is not authenticated**

When you run reprotect, the operation fails with the following error.

Internal error: Received unexpected exception during prepare phase. The session is not authenticated.

Workaround: Re-run the reprotect operation.

- **If the source VM for a replication runs on ESXi 6.7, replication synchronization seems to progress, but the replication instance never completes successfully**

In ESXi 6.7, it is possible that more demand log chunks be scheduled for parallel transfer than the actual number that can be transmitted. If you are replicating a VM that is running on such a host and this coincides with a slow target host or temporary network errors, this might result in replication failure with **DiskQueue is full** errors.

Workaround:

1. Migrate all the VMs to another ESXi host.
2. Edit the value of the HBR.DemandlogTransferMaxNetwork ESXi Advanced setting to 63 instead of the default 64.
3. Place the ESXi host in maintenance mode.
4. Reboot the ESXi host.

- **If the source VM for a replication runs on ESXi 6.7 or ESXi 6.7 Update 1, an initial or full synchronization might stop progressing before completion**

If you are using vSphere Replication and you are running a protected VM on ESXi 6.7 or ESXi 6.7 Update 1, an initial or full synchronization of replications might stop progressing before completion. The synchronization of replications remains in progress, but the checksum bytes value in the replication details information does not progress. The power off, take a snapshot, revert to snapshot, and migration VM operations fail with a timeout or Task in progress errors.

Workaround:

1. In the ESXi Advanced settings, disable the checksum for vSphere Replication by setting HBR.ChecksumUseChecksumInfo = 0.
2. Migrate all VMs and power off the ones that cannot be migrated on the ESXi host.
3. Place the host in maintenance mode.
4. Reboot the ESXi host.

Note: This workaround disables the checksum part of the sync process and all of the allocated blocks will be sent to the remote site, regardless of whether they are different or not. This workaround disables the seed functionality.

- **vSphere Client displays wrong number of VMs that you can protect while Site Recovery Manager is in evaluation mode**

The **Administration > Licensing > Assets** tab in the vSphere Client inaccurately states that while in evaluation mode, Site Recovery Manager can protect up to 100 virtual machines per site. The correct number of virtual machines that you can protect with a Site Recovery Manager evaluation license is 75 VMs per site.

Workaround: Protect up to 75 virtual machines while the product is in evaluation mode.

- **Site Recovery Manager might create dummy networks from the protection vCenter Server on the recovery vCenter Server when the network names are different from the recovery ones**

When you have protected VMs attached to networks with network labels different from the ones that exist on the recovery site, during Test\Recovery\Reprotect the operations succeed, but dummy networks with same network labels from protected site might be created on the recovery vCenter Server. Dummy networks are created only once, not every time you execute the Test\Recovery\Reprotect.

Workaround 1: Disable the preservation of VM snapshots by changing the value of **vrReplication.preserveMpitImagesAsSnapshots** in the Site Recovery Manager advanced settings.

Workaround 2: Discard the dummy network and continue working with Site Recovery Manager.

- **VMware Site Recovery Manager 8.3 Configuration Import/Export Tool might error out when you import a configuration with protected VMs in no recovery plans**

If you put protected virtual machines in recovery plans, then delete all recovery plans containing these VMs, and export your configuration with the VMware Site Recovery Manager 8.2 Configuration Import/Export Tool, the VM recovery settings for those VMs are exported but you are unable to import them later. If you try to import your settings, you see errors like:

Error while importing VM settings for server with guid '6f81a31e-32e0-4d35-b329-783933b50868'.

The rest of your exported configuration is properly imported.

Workaround: Recreate your recovery plan, reconfigure the desired recovery settings, and export your configuration again. Do not delete recovery plans if you want to export and import VM recovery settings.

- **Virtual machines protected in a Storage Profile Protection Groups are not listed in the CSV file created when running the DR IP Customizer tool.**

When you use the DR IP Customizer tool in a multiple vCenter Server environment, for example setup with federated PSCs where more than one vCenter Server instance is available on each site, you must specify the option '`--vcid UUID`' to be used to gather networking information about the virtual machines protected by Site Recovery Manager. If you provide the secondary site `vcid`, the DR IP Customizer tool connects to the secondary Site Recovery Manager server which does not store the network information for VMs protected with SPPGs. Providing the `vcid` from the secondary site results in connecting to the wrong vCenter Server and the VMs are not listed in the generated CSV file.

Workaround: When using the DR IP Customizer tool, provide only the primary vCenter Server `vcid` and `uri`.

- **If you have Site Recovery Manager and vCenter Server deployment in Enhanced Linked Mode, after you run Site Recovery Manager installer in modify mode, the Site Recovery Manager servers are not connected**

If you have Site Recovery Manager and vCenter Server deployed in Enhanced Linked Mode and you run the Site Recovery Manager installer in modify mode, it recreates the Site Recovery Manager solution users and this requires the reconfiguration of the SRM pairing.

Workaround: Reconfigure the pairing of the Site Recovery Manager servers.

- **Customization through IP subnet mapping rules is not fully supported for Linux VMs using multiple NICs which are named ethX**

Site Recovery Manager does not fully support IP rule-based customization for Linux virtual machines that have multiple NICs, if the NICs have mixed DHCP and static IP settings. Site Recovery Manager customizes only the NICs with static IP addresses for which it has matching IP subnet mapping rule and might clear some configuration settings for the other NICs configured with DHCP. Known issue related to this scenario was observed for Red Hat Enterprise Linux 6.x/7.x and CentOS 6.x/7.x, where Site Recovery Manager customization deletes `/etc/sysconfig/network-scripts/ifcfg-ethX` files for the NICs configured with DHCP and successfully customizes the rest with static IP settings according to the matched IP subnet mapping rule. This issue also happens when the VM's NICs are all configured with static IP addresses, but some of them have a matching IP subnet rule while others do not. Some configuration settings for those NICs without a matching IP subnet rule might be cleared after IP customization.

Workaround: For correct IP customization for Linux VMs using multiple NICs with some of them having a matching IP subnet mapping rule while the others do not, use the Manual IP Customization Site Recovery Manager option.

- **IP customization fails when you use special characters in the Recovery Plan name**

When you run a Test Recovery for a Recovery Plan with special characters in the name and configured IP customization, the IP customization fails.

Workaround: Remove any OS-specific special symbols from the Recovery Plan name.

- **If the protected vCenter Server is down, you might experience performance degradation in the HTML 5 user interface on the recovery site, especially in the Configure Recovery Settings dialog.**

You might experience performance degradation in the HTML 5 user interface on the recovery site, especially in the Configure Recovery Settings dialog, if the protected vCenter Server is down.

Workaround: Refresh the HTML 5 user interface on the recovery site and re-try your operation.

- **Remote vCenter Server is not displayed in the Summary tab after Site Recovery Manager upgrade**

After you upgrade Site Recovery Manager to version 8.2 from an older Site Recovery Manager version, the remote vCenter Server field might be empty in the Site Pair>Summary screen.

Workaround: Repair the corresponding site pair.

- **Site Recovery Manager privileges are not localized in the vSphere 6.7 Client**

Site Recovery Manager privileges are not localized in the vSphere 6.7 Client.

Workaround: None. The issue is resolved in vSphere 6.7 Update 1.

- **The Site Recovery UI becomes unusable showing a constant stream of 403 - OK error message**

The Site Recovery UI shows no data and an error 403 - OK.

Workaround:

1. Log out from Site Recovery UI and log in again.
2. Disable the browser's 'Restore last session' checkbox. For Chrome disable the 'Continue where you left off' option.

- **Folder names on VSAN datastores are displayed with UUIDs instead of friendly names in the virtual machine protection properties dialog**

When you open the virtual machine protection properties dialog, the folder names on VSAN datastores are displayed with UUIDs instead of friendly names.

Workaround: None

- **Datastore cluster that consists of datastores that are not replicated or are from different consistency groups visible to Site Recovery Manager does not have an SRM warning.**

You create a datastore cluster that consists of datastores that are not all in a same consistency group or are not replicated. A Site Recovery Manager warning should exist but does not.

Workaround: None

- **After you perform a failover, the virtual machine NICs at the disaster recovery site might remain disconnected**

Workaround: None. Manually reconnect the NICs by reconfiguring the VM devices.

- **Export report from the Recovery Plan History or the Recovery Steps screens does not work when using Microsoft Edge browser**

When you try to export the report from the Recovery Plan History or the Recovery Steps screens using MS Edge browser, you get the following error in the dev console.

```
ERROR XML5610: Quote character expected.
```

```
ERROR Error: Invalid argument.
```

This is a known Microsoft Edge browser issue with XSLTProcessor used to transform server's xml into html.

Workaround: Use Chrome, Microsoft Internet Explorer, or Firefox browser.

- **When you right-click on a replicated VM and select Reconfigure Replication in the vSphere UI, the pop-up window for the Site Recovery UI is blocked without notification in Mozilla Firefox browser**

By default the Site Recovery UI opens in a new tab. When you right-click on a replicated VM and select Reconfigure Replication in the vSphere UI, the pop-up window for the Site Recovery UI is blocked without notification in Mozilla Firefox browser.

Workaround: From the Options menu in Mozilla Firefox, select the Content tab and add the URL of the vCenter Server to the Pop-ups exception list.

- **Site Recovery Manager Server might crash if you re-enable recovery of a VM**

You can disable recovery of a VM if the recovery operation for the VM fails. If you run a recovery plan and the recovery fails, you can re-enable the recovery of the VM and rerun the recovery, but Site Recovery Manager Server crashes.

Workaround: Start Site Recovery Manager Server and disable the recovery of the VM.

- **The Test and Recovery operations fail if a vSAN stretched cluster has one fault domain that is not available**

If you test or recover a VM on a vSAN stretched cluster with one fault domain that is not available, the operation fails. The cause is that the vSAN Default Storage Policy cannot be satisfied and provisioning a VM with Site Recovery Manager on the storage fails.

Workaround: Register the recovered VM on the vSAN stretched cluster manually. The VM becomes compliant with the vSAN Default Storage Policy when the fault domain is available.

- **Your datastore might appear as inactive in the inventory of the original protected site after reprotect**

If you use a stretched storage and run reprotect after a disaster recovery, you might receive the following warning.

```
The requested object was not found or has already been deleted.
```

After reprotect, the datastore in the inventory of the original protected site appears as inactive.

Workaround: Refresh or rescan the storage adapters.

1. Click the **Configure** tab and click **Storage Adapters**.
2. Click the **Refresh** or **Rescan** icon to refresh or rescan all storage adapters.

- **Site Recovery Manager uses the default value of the remoteSiteStatus.drPanicDelay setting even if you changed the value**

Even if you set a custom value for the delay between a not responding event and a site down event, the drPanicDelay has a default value in the Tasks view.

Workaround: Change the value of the remoteSiteStatus.drPanicDelay setting and restart Site Recovery Manager Server.

- **Site Recovery Manager uses the default value of the remoteSiteStatus.drPingFailedDelay setting even if you set a custom value**

Even if you set a custom value for remoteSiteStatus.drPingFailedDelay, the setting has a default value in the Tasks view.

Workaround: Set the custom value for the remoteSiteStatus.drPingFailedDelay setting and restart Site Recovery Manager Server.

- **A VM and a consistency group assigned to a deleted storage policy appear in the Virtual Machines and Consistency Groups tabs**

If you delete a storage policy, the VMs and the consistency group that are assigned to the storage policy appear in the Virtual Machines and Consistency Groups tabs to the SPPG group.

Workaround: Recreate the storage policy protection group. After you recreate the group the VMs and consistency group do not appear in the Virtual Machines and Consistency Groups tabs.

- **Recovery of an encrypted VM might fail during the Power On step if the encryption key is not available on the recovery site**

If you recover an encrypted VM and the encryption key used on the protected site is not available on the recovery site during the recovery process, the recovery fails when Site Recovery Manager powers on the VM.

Workaround: Complete the following steps.

1. Remove the encrypted VM from the inventory of the recovery site.
2. Ensure that the Key Management Server on the recovery site is available and that the encryption key used on the protected site is available on the recovery site.
3. Register the encrypted VM to the inventory of the recovery site.
4. In the Site Recovery Manager user interface, open the recovery settings of the encrypted VM and disable power on of the VM during recovery.
5. Rerun recovery.

If you have a VM with multiple disks that are replicated with vSphere Replication to different vSphere Virtual Volumes datastores on the secondary site, a test recovery operation fails. During a test recovery, vSphere Replication tries to create Linked Clones for the vSphere Virtual Volumes replica disks, but the operation fails because Linked Clones across different datastores are not supported. vSphere Replication creates Linked Clones only during a test recovery. The planned recovery, unplanned recovery, and reprotect complete successfully.

Workaround: A test recovery operation using vSphere Virtual Volumes disks pass successfully only if all disks are replicated to the same vSphere Virtual Volumes datastore on the secondary site.

- **The First Attempt for Recovery of VMs placed on vSphere Virtual Volumes might fail during the customization steps**

Site Recovery Manager cannot recognize old VMware Tools versions installed on VMs placed on vSphere Virtual Volumes storage during the first recovery attempt. You might observe the following failures that depend on the VMware Tools version installed on the recovered VMs.

`Vim::Fault::OperationNotSupportedByGuest : "The guest operating system does not support the operation." Vim::Fault::InvalidGuestLogin : "Failed to authenticate with the guest operating system using the supplied credentials."`

Workaround:

1. Rerun the failed recovery plan or clean the test plan up and rerun the test recovery again.
2. Update VMware Tools to the latest version for all VMs placed on vSphere Virtual Volumes storage.

- **Planned Migration might fail with an error for VMs protected on vSphere Virtual Volumes datastore**

If you have VMs protected on vSphere Virtual Volumes datastores, the planned migration of the VMs might fail with the following error on the Change recovery site storage to writable step.

`Error - Storage policy change failure: The vSphere Virtual Volumes target encountered a vendor specific error. Invalid virtual machine configuration. A specified parameter was not correct: path.`

Workaround: Rerun the recovery plan.

- **The IP customization or in-guest callout operations might fail with Error - Failed to authenticate with the guest operating system using the supplied credentials**

If the time of the ESXi host where the VM is recovered and running is not synchronized with vCenter Single Sign-On servers on the recovery site you might receive an error.

Workaround:

When `recovery.autoDeployGuestAlias` option in Advanced Settings is TRUE (default).

- If the guest OS of the recovered VM is Windows, ensure the time synchronization between the ESXi host and vCenter Single Sign-On on the recovery site, and rerun the failed recovery plan.
- If the guest OS of the recovered VM is Linux and the time is ahead from the ESX host on which the recovered VM is running, update the configuration parameters of the VM by using the following procedure and rerun the failed recovery plan.
 1. Right-click the recovered VM.
 2. Click **Edit** Settings.
 3. In the **Options** tab, click **General**.
 4. Click **Configuration** to update the configuration parameters.
 5. Click **Add Row** and enter `time.synchronize.tools.startup.backward` in the **Name** text box and **TRUE** in the **Value** text box.
 6. Click **OK** to confirm.

When the `recovery.autoDeployGuestAlias` option in Advanced Settings is FALSE.

- Ensure proper time synchronization between your guest OS on the protected VM and vCenter Single Sign-On servers on the recovery site.
- Ensure that your protected VMs have correct guest aliases configured for the Solution User on the recovery site SRM server. For more information see, the description of `recovery.autoDeployGuestAlias` option in [Change Recovery Settings](#).

For more information, see the related troubleshooting sections in the *Site Recovery Manager 8.3 Administration* guide.

- **Valid vCenter Server addresses might not be listed as possible targets when you install Site Recovery Manager**

If there are duplicated vCenter Server addresses in your environment due to multiple service registrations of one vCenter Server with different versions, a valid address might not be listed. Site Recovery Manager writes an error for duplicated key in its installation log file.

The following error message appears in the installation log file of your Site Recovery Manager:

`VMware: Srm::Installation::XmlFileHandler::GetElementMap: INFORMATION: Inserted key 'xxxxxx' and value '76B00E54-9A6F-4C13-8DD9-5C5A4E6101E3'`

`VMware: Srm::Installation::XmlFileHandler::GetElementMap: INFORMATION: Inserted key 'xxxxxx' and value 'default-first-site:b84bcef3-85fb-4d92-8204-2392acf0088d'`

`VMware: Srm::Installation::XmlFileHandler::GetElementMap: ERROR: Duplicate key 'xxxxxx' exists`

Workaround: See <https://kb.vmware.com/kb/2145520>.

- **Replacing the SSL certificate of vCenter Server causes certificate validation errors in Site Recovery Manager.**

If you replace the SSL certificate on the vCenter Server system, a connection error might occur when Site Recovery Manager attempts to connect to vCenter Server.

Workaround: For information about how to update vCenter Server certificates and allow solutions such as Site Recovery Manager to continue to

- **Disaster recovery for a VM that is attached to a VSS network shows the protected site network in the UI for temporary placeholder network mappings.**

If you use a VSS network for which you have not configured a regular network mapping and you run disaster recovery on a recovery plan that contains a storage policy protection group, Site Recovery Manager creates a temporary placeholder mapping for this network. When you complete the temporary placeholder mapping, a network might appear on the secondary site that has the same name as the network on the primary site. If you did not explicitly create this network, it is not a genuine network. However, it is possible to select it as the target for the temporary placeholder mapping and recovery will succeed. The network is then displayed as inaccessible after the recovery completes, even though the recovered VMs are shown as being connected to this network on the recovery site.

Workaround: After the recovery, manually map the VMs to a different network and connect them to a genuine network.

- **Test network mappings are not deleted when the corresponding network mapping is deleted.**

If, when you create network mappings, you configure a specific network mapping for testing recovery plans, and if you subsequently delete the main network mapping, the test network mapping is not deleted, even if the recovery site network that you configured is not the target of another mapping. For example:

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

Workaround: Delete the test network mapping manually.

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

Workarounds: Remove dependency between virtual machines and rerun planned migration with vMotion. Manually re-enable dependency for future recovery workflows.

If you want to preserve the dependency between virtual machines, then run planned migration without vMotion. Both virtual machines migrate as regular virtual machines according to the dependency order.

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

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

Workaround: Restart the Site Recovery Manager server.

- **When you edit a temporary placeholder mapping, you might see error `The specified key, name, or identifier '6458aed1-6c80-4565-907f-189e6a102046' already exists.`**

This error can occur when a regular mapping for the same protected site inventory object exists.

- **Renaming a datastore associated with a protected virtual machine can result in loss of protection and recovery settings.**

A protected virtual machine can lose its protection status as well as recovery settings when you rename the datastore associated with the virtual machine. First shut down the Site Recovery Manager server, then rename datastores to avoid losing recovery settings for the virtual machine.

Workaround: To restore the protection status, restart the protected site Site Recovery Manager server or remove the affected datastore from the protection group and then add it back, then reconfigure recovery settings.

- **Site Recovery Manager displays incorrect names for some protected site objects in placeholder mappings.**

- Datacenters display the name **vm** instead of the user-defined datacenter name.
- Resource pools display the name **Resources** instead of the user-defined resource pool name.
- If you move a virtual machine to another folder or resource pool after protecting the virtual machine in a storage profile protection group, the placeholder mappings generated after the move display internal IDs such as **folder-3** or **resgroup-5** instead of the user-defined object names.

Workaround: There is no workaround for incorrect object names in inventory mappings. Check the history report from the failed test or recovery workflow that caused the placeholder mappings to be created. For example, if you know the protected site inventory, you can determine the protected site datacenter, folder, and resource pool that contained the protected virtual machine that failed to recover due to a missing mapping.

- **After the recovery plan workflow completes, the last recovery steps continue to show a "Running" status.**

The incorrect status is a transient UI problem. Site Recovery Manager executes all the steps to completion.

Workaround: Click the global refresh icon to refresh the interface. All steps display the correct completed status.

- **Prompts and commands disappear from the list of steps in recovery view.**

After you add a prompt or command in **Recovery Steps > Recovery View**, you can see the same prompt or command in test view. However if you try to edit a prompt or command in test view, the prompt or command specific to the recovery view might disappear from the list of steps.

Disappearing prompts or commands is a transient UI problem that affects only the detailed list of recovery steps. Site Recovery Manager

Workaround: Click the global refresh icon to refresh the interface. All callouts reappear in the list of steps.

- **When the storage array fails at the protected site, Site Recovery Manager cannot recover virtual machines in storage profile protection groups.**

The virtual machines become unprotected but the data is still protected.

Workaround: Manually recover the datastores and virtual machines at the recovery site.

- **Site Recovery Manager installation fails if the Platform Services Controller certificate has expired.**

When connecting to Platform Services Controller during Site Recovery Manager installation, you can accept the Platform Services Controller certificate even if it has expired or is not yet valid. The installation then fails at the step when you select the vCenter Server instance to connect to, with the error **Failed to validate vCenter Server. Details: Internal error: unexpected error code: -1**. The same error occurs if the Platform Services Controller certificate expires after you install Site Recovery Manager and you run the Site Recovery Manager installer in Modify mode. If the Platform Services Controller certificate expires after you have installed Site Recovery Manager, different errors can also appear in the Site Recovery Manager interface.

Workaround: Replace the Platform Services Controller certificate and attempt installation again.

- **The placeholder virtual machine on the recovery site still exists after you delete the protection group and recovery plan.**

When you delete the recovery plan and protection group from the SRM inventory, the placeholder VM is still visible on the recovery site. An error occurs when you try to create a new protection group with the same datastore and virtual machine. When you try to manually delete the placeholder virtual machine from the vCenter Server inventory, an error occurs. Site Recovery Manager marks the virtual machine as orphaned.

Workaround: Delete the placeholder virtual machine and remove the orphaned virtual machine, then create the protection group with the same virtual machine.

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

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

Workaround: Wait for 10 minutes and attempt cleanup again.

- **Rerunning reprotect fails with error: Protection Group '{protectionGroupName}' has protected VMs with placeholders which need to be repaired.**

If a **ReloadFromPath** operation does not succeed during the first reprotect, the corresponding protected virtual machines enter a **repairNeeded** state. When Site Recovery Manager runs a reprotect on the protection group, Site Recovery Manager cannot repair the protected virtual machines nor restore the placeholder virtual machines. The error occurs when the first reprotect operation fails for a virtual machine because the corresponding **ReloadFromPath** operation failed.

Workaround: Rerun reprotect with the **force cleanup** option enabled. This option completes the reprotect operation and enables the **Recreate placeholder** option. Click **Recreate placeholder** to repair the protected virtual machines and to restore the placeholder virtual machines.

- **Recovery Fails to Progress After Connection to Protected Site Fails**

If the protection site becomes unreachable during a deactivate operation or during RemoteOnlineSync or RemotePostReprotectCleanup, both of which occur during reprotect, then the recovery plan might fail to progress. In such a case, the system waits for the virtual machines or groups that were part of the protection site to complete those interrupted tasks. If this issue occurs during a reprotect operation, you must reconnect the original protection site and then cancel and restart the recovery plan. If this issue occurs during a recovery, it is sufficient to cancel and restart the recovery plan.

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

This error might occur due to a latency between vCenter, ESXi, and Site Recovery Manager Server.

Workaround: Rerun the recovery plan.

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

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

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

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

- **Cancellation of Recovery Plan Not Completed**

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

- Pause vSphere Replication, causing synchronization to fail. After recovery enters an error state, use the vSphere Client to restart vSphere Replication in the vSphere Replication tab. After replication is restarted, the recovery plan can be run again, if desired.
 - Wait for synchronization to complete or time out. This might take considerable time, but does eventually finish. After synchronization finishes or expires, cancellation of the recovery plan continues.
- **Error in recovery plan when shutting down protected virtual machines: Error - Operation timed out: 900 seconds during Shutdown VMs at Protected Site step.**

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

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

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

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

Workaround: Rerun recovery.

- **Test cleanup fails with a datastore unmounting error.**

Running cleanup after a test recovery can fail with the error **Error - Cannot unmount datastore 'datastore_name' from host 'hostname'. The operation is not allowed in the current state..** This problem occurs if the host has already unmounted the datastore before you run the cleanup operation.

Workaround: Rerun the cleanup operation.

- **Running a planned migration of a recovery plan with no protected virtual machines leaves the environment in an unusable state.**

When a protection group contains no virtual machines and you run a recovery plan of this protection group in planned migration mode from the remote Site Recovery Manager server, the operation fails. The plan goes into Incomplete Recovery state and cannot be deleted and the LUN disconnects from both protection and recovery hosts.

Workaround: To restore the environment, delete the protection group and recovery plan and manually reconfigure the LUN using SAN management interface.

- **When you remove permission for a user on a protected site while logged in as that user, the following error message appears: Unable to retrieve Permissions data. The session is already logged in. A similar error appears on the Advanced Settings tab.**

This error appears when you remove your own permissions at the site level. Instead, the message should inform you that you do not have permissions to view the page.

- **Running a recovery plan fails with a virtual machine error in the Configure Storage step.**

Subsequent runs of the recovery plan fail at the same Configure Storage step for the same virtual machine with the error **The specified key, name, or identifier already exists..** If you look in the vCenter Server Inventory, you see two virtual machines with the same name as the failed virtual machine, one of which is in the Discovered Virtual Machines folder. This problem is caused by a known communication issue between vCenter Server and the ESXi Server instance.

Workaround: Unregister the duplicate virtual machine in the Discovered Virtual Machines folder from vCenter Server. After completing this for all affected virtual machines, re-run the recovery plan.



Company

About Us

Executive Leadership

News & Stories

Investor Relations

Security, Safety & Compliance

Environment, Social & Governance

AI at VMware

Careers

Blogs

Communities

Acquisitions

Office Locations

VMware Cloud Trust Center

COVID-19 Resources

Support

VMware Customer Connect

Support Policies

Product Documentation


Compatibility Guide

Terms & Conditions

California Transparency Act Statement

Hands-on Labs & Trials

 Twitter

 YouTube

 Facebook

 LinkedIn

 Contact Sales

Copyright © 2005-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Terms of Use

Your California Privacy Rights

Privacy

Accessibility

Trademarks

