

VMware vSphere Replication 8.3.1 Release Notes

 Updated on 01/04/2024

VMware vSphere Replication 8.3.1 | 15 SEP 2020 | Build 16877246 | [Download](#)

VMware vSphere Replication 8.3.1 Configuration Import/Export Tool | 15 SEP 2020 | Build 16880382 | [Download](#)

Check for additions and updates to these release notes.

What's in the Release Notes

These release notes cover the following topics:

- [Localization](#)
- [Earlier Releases of vSphere Replication 8.3](#)
- [What's New](#)
- [Product Documentation](#)
- [Installation](#)
- [Upgrading vSphere Replication](#)
- [Operational Limits of vSphere Replication](#)
- [Open Source Components](#)
- [Caveats and Limitations](#)
- [Known Issues](#)

Localization

VMware vSphere Replication 8.3.1 is available in the following languages:

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

Earlier Releases of vSphere Replication 8.3.x

Features, known issues, and resolved issues of vSphere Replication are described in the release notes for each release. Release notes for earlier releases of vSphere Replication 8.3.x are:

[vSphere Replication 8.3.0.2 Express Patch Release](#)

[vSphere Replication 8.3.0.1 Express Patch Release](#)

[vSphere Replication 8.3 Release Notes](#)

What's New

- Automatically add new disks to replication, without interruption of ongoing replication.
- vRealize Operations Management Pack for vSphere Replication 8.3.1. For information about the management pack, see the **VMware vRealize Operations Management Pack for vSphere Replication 8.3.1 Release Notes**.
- vRealize Orchestrator Plug-In for vSphere Replication 8.3.1. For information about the new workflows, see the **VMware vRealize Orchestrator Plug-In for vSphere Replication 8.3.1 Release Notes**.

- [vSphere Replication 8.3 Documentation Center](#)
- [Compatibility Matrices for vSphere Replication 8.3.x](#)

Installation

Download the vSphere Replication `.iso` image and mount it. You can deploy the vSphere Replication appliance by using the Deploy OVF wizard in the vSphere Web Client or the vSphere Client. Navigate to the `\bin` directory in the `.iso` image and use the corresponding OVF file:

1. `vSphere_Replication_OVF10.ovf`: Use this file to install all vSphere Replication components, including the vSphere Replication Management Server and a vSphere Replication Server.
2. `vSphere_Replication_AddOn_OVF10.ovf`: Use this file to install an optional additional vSphere Replication Server.

For more information on installation, see section Installing vSphere Replication in the [vSphere Replication Documentation Center](#).

For vCenter Server to vCenter Server replications, the version of the vSphere Replication Management server on the source and the target site can be either 8.2 or 8.3.

vSphere Replication 8.3.1 requires a supported vCenter Server version on both the source site and the target site. For more information, see [VMware Product Interoperability Matrices](#).

Upgrading vSphere Replication

You use the ISO file or the VAMI to upgrade to a major version of vSphere Replication, for example from 8.1 or 8.2 to 8.3.x.

You cannot upgrade vSphere Replication from version 6.5.1 to version 8.3.1 by using the official VMware Update Repository from the VAMI of the vSphere Replication appliance. See the [compatibility matrices](#) for further information on supported versions.

Important: Before you initiate an upgrade, verify that the vSphere Replication appliance has an OVF environment, or context. See [Checking and Restoring the OVF Context of the vSphere Replication Appliance \(2106709\)](#).

Verify that you read the Upgrade and General sections under [Known Issues](#).

Make sure that you deploy the new vSphere Replication 8.3.x OVF first. In the console of the newly deployed vSphere Replication appliance, make sure that you select the **Upgrade Option**.

See [Upgrade Additional vSphere Replication Servers](#) and [Upgrade the vSphere Replication Appliance](#) for the procedures on upgrading to vSphere Replication 8.3.1

Notes:

- If you have ongoing Disaster Recovery to Cloud replications and you try to upgrade to vSphere Replication 8.3.x through the VAMI, the upgrade will fail, to prevent you from losing these replications. To avoid the upgrade failure, unconfigure all Disaster Recovery to Cloud replications before the upgrade. To continue using cloud recovery, you can use VMware vCloud Availability for vCloud Director. For more information, see the [VMware vCloud Availability](#) product page.
- When you use vSphere Replication with Site Recovery Manager, upgrade vSphere Replication on both of the protected and the recovery sites before you upgrade the Site Recovery Manager Server. After upgrading vSphere Replication, you must restart the Site Recovery Manager Server. For more information, see the *VMware Site Recovery Manager Documentation*.

Operational Limits of vSphere Replication

The operational limits of vSphere Replication 8.3.x are documented in the VMware Knowledge Base. See [Operational Limits for vSphere Replication 6.x and 8.x \(KB 2102453\)](#).

Note: vSphere Replication requires additional configuration to support more than 500 replications per a vSphere Replication Management server. See [Operational Limits for vSphere Replication 6.x and 8.x](#) and [Configuring Upgraded vSphere Replication Appliances to Support up to 2000 Replications](#).

Open Source Components

The copyright statements and licenses applicable to the open source software components distributed in vSphere Replication 8.3.1 are available at the [vSphere Replication Open Source Disclosure page](#).

Caveats and Limitations

To ensure successful virtual machine replication, you must verify that your virtual infrastructure respects certain limits before you start the replication.

the disk to a different type of storage controller.

- You cannot configure the vSphere Replication appliance when the Platform Services Controller is installed with a custom port.
- The 5 minute RPO scales to a maximum supported limit of 50 VMs on a provisional vVol datastore.
- vSphere Replication does not support VSS quiescing on Virtual Volumes.
- vSphere Replication cannot replicate virtual machines that share vmdk files.
- vSphere Replication does not support vSphere APIs for IO Filtering on both the source and the target sites. You cannot replicate a virtual machine that is assigned a VM Storage Policy that contains IOFilters, nor can you assign such a policy to the replication target VM. Before configuring a virtual machine for replication, verify that the VM Storage Policy that is assigned to it does not contain IOFilters. Do not assign VM Storage policies with IOFilters to virtual machines that are already configured for replication.
- Deploying more than one vSphere Replication appliance produces a warning on the boot screen. This requires user confirmation to either continue and configure all replications again or shut down the new appliance so that it does not interfere with the old one. This situation does not occur when deploying more than one vSphere Replication servers.
- Each vSphere Replication Management Server can manage a maximum of 2000 replicated virtual machines. See [Configuring Upgraded vSphere Replication Appliances to Support up to 2000 Replications \(KB 2102463\)](#) and [Requirements to the Environment... \(KB 2107869\)](#).
- vSphere Replication supports a maximum disk size of 62TB. If you attempt to enable replication on a virtual machine with a disk larger than 62TB, the virtual machine will not perform any replication operation and will not power on.
- vSphere Replication tracks larger blocks on disks over 2TB. Replication performance on a disk over 2TB might be different than replication performance on a disk under 2TB for the same workload depending on how much of the disk goes over the network for a particular set of changed blocks.
- vSphere Replication does not support upgrading the VMware Tools package in the vSphere Replication appliance.
- vSphere Replication supports replicating RDMs in Virtual Compatibility Mode. RDMs in Physical Compatibility Mode cannot be configured for replication.
- vSphere Replication does not replicate virtual machine snapshot hierarchy at the target site.
- You can configure virtual machines that are powered off for replication. However, actual replication traffic begins when the virtual machine is powered on.
- When using Storage DRS at a replication site, ensure that you have homogeneous host and datastore connectivity to prevent Storage DRS from performing resource consuming cross-host moves (changing both the host and the datastore) of replica disks.
- For VMware vCloud Availability for vCloud Director, a seed vApp can be used for only one replication.
- The 5 minute RPO requires the source host to be ESXi 6.0 Update 3 or later for VSAN, and ESXi 6.5 for other supported datastores.
- To use the network isolation feature, vSphere Replication requires the host to be ESXi 6.0 or later.
- vSphere Replication does not support VMware vSphere® Trust Authority™.
- vSphere Replication 8.3 Configuration Import/Export Tool fully supports vSphere Replication 8.3.1 to vSphere Replication 8.3.1 pairing. In a vSphere Replication 8.2 to vSphere Replication 8.3 pairing, the vSphere Replication 8.3 Configuration Import/Export Tool imports only the outgoing replications.
- vSphere Replication is not integrated with vSphere Life Cycle Manager (vLCM). You must not run vSphere Replication and vLCM in the same data center, because vLCM causes vSphere Replication to stop.
- When using the TRIM/UNMAP commands to reclaim space, if the UNMAP command is used at the source site, the replication traffic sends the command as a large stream of zeroes, unless compression is used on the replication. The data is stored as zeroes at the target site and space on the replica disks is not reclaimed.

Known Issues

The known issues are grouped as follows.

- [Upgrade](#)
- [General](#)
- [Replications to vCenter Server](#)

Upgrade

• Replication falls into error state

After you upgrade vSphere Replication 8.1.2.1 to vSphere Replication 8.3 and run Disaster Recovery while the source site is active, the replication might fall into an error state.

Workaround: Remove the replication which is in error state and configure it again.

• You cannot use network encryption for vSphere Replication

After upgrading from vSphere Replication 8.1 to version 8.3, you cannot use the network encryption feature.

Workaround 1:

1. Establish an SSH connection to the vSphere Replication Appliance.
2. Navigate to `/opt/vmware/hms/conf/`.
3. Open `hms-configuration.xml` in a text editor and set the `<hms-auto-install-hbragent-vib>` value to **true**.
4. Restart the HMS service.

Workaround 2:

- **The vSphere Replication Management service does not start after the upgrade**

After you upgrade vSphere Replication, the vSphere Replication Management (VRM) service appears as stopped in the VAMI, and the `/opt/vmware/hms/logs/hms-configtool.log` file in the virtual appliance contains `java.net.ConnectException: Connection refused` error messages. This problem is observed if the upgrade procedure of the embedded DB schema fails because the vPostgreSQL service was not fully started. Workaround:

1. In the virtual appliance console, log in as the root user.
2. Run the following command: `$ /opt/vmware/hms/bin/hms-configtool -cmd upgrade -configfile /opt/vmware/hms/conf/hms-configuration.xml`
The DB schema upgrade starts.
3. Wait for the DB upgrade procedure to complete.
4. In the vSphere Replication VAMI, navigate to the **Configuration** tab, and complete the SSO registration of the appliance.

- **Missing vSphere Replication permissions after upgrading the vSphere Replication appliance, certificate or IP change**

If you upgrade the vSphere Replication appliance, or if for some other reason the certificate or the IP address of the vSphere Replication appliance changes, the permissions that are assigned to the default VRM user roles are deleted. This problem is observed every time the vSphere Replication extension is unregistered and registered with the vCenter Server extension manager.

Workaround: Clone the predefined VRM roles and create your custom roles before upgrading the vSphere Replication appliance, or changing its certificate or IP address. The permissions that are assigned to custom roles are not removed.

- **The vSphere Replication Virtual Appliance Management Interface (VAMI) becomes inaccessible after upgrade**

After the upgrade, the vSphere Replication VAMI changes and you cannot access it in the same browser window that you used before the upgrade.

Workaround: Do one of the following.

- Change the browser that you use to open the VAMI.
- Close the entire browser and open a new browser window to connect to the VAMI.
- Clear the cache of your browser.
- Open an incognito tab in your browser.

- **After an upgrade of the vCenter Server and vSphere Replication, configuring the SSO in the vSphere Replication VAMI fails with error Bad exit code: 1**

After you upgrade the vCenter Server to version 7.0 and vSphere Replication to version 8.3, you must register the appliance with vCenter Single Sign-on. On the Configuration tab of the vSphere Replication VAMI, you enter the LookupService address and the credentials of an SSO administrator, and click **Save and Restart Service**. The following error message appears: `Bad exit code: 1`.

This problem is observed because the upgraded vCenter Server changes its IP address or certificate, but the vSphere Replication Management server preserves the old IP address and certificate of the vCenter Server in its OVF environment. As a result, the validation of the vCenter Server fails.

Workaround: In the vSphere Web Client, right-click the vSphere Replication Management server VM and power it off and on. This operation forces the update of the OVF environment on the vSphere Replication Management server VM.

- **Site Recovery Manager cannot be upgraded after upgrading vSphere Replication**

On upgrade of vSphere Replication to version 6.5, Site Recovery Manager cannot be upgraded as the vSphere Replication version is detected as incompatible. Under solutions manager in vCenter, the vSphere Replication version appears not to have been upgraded though the appliance reports the upgrade is successful.

Workaround: Register the vSphere Replication appliance with vCenter Single Sign-On.

1. Connect to the VAMI interface of the vSphere Replication appliance by using a supported browser.
2. On the **Configuration** tab, enter the user name and password of an SSO administrator.
Note: The text boxes for the SSO credentials will not be visible if you are using an unsupported browser.

- **The hms-vpostgres service cannot start after an upgrade attempt through VAMI from vSphere Replication version 8.2.1 to version 8.3.1**

The `hms-vpostgres` service cannot start after an upgrade attempt through VAMI from vSphere Replication version 8.2.1 to version 8.3.1. The update process deletes all configurations from the postgres directory `/var/lib/vrmsdb`.

Workaround:

1. Open `/opt/vmware/hms/conf/embedded_db.cfg` file.
2. Update the `EMB_DB_INSTALL_DIR=/opt/vmware/vpostgres/XXX` value to `EMB_DB_INSTALL_DIR=/opt/vmware/vpostgres/current`.
3. Run the upgrade.

General

- **NEW 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

Workaround: None. Discard the error.

- **NEW Reconfiguring a replication fails after a new disk is added to the source VM**

Auto include new disks option is enabled. When you add a new disk to the source VM, vSphere Replication attempts to automatically reconfigure the replication, but the process fails with the following error:

Cannot reconfigure replication group '<group-name>' (managed object ID: '<group-mo-id>'). Details: 'The vSphere Replication configuration of the virtual machine has an issue: Generation number is mismatched (stale).'

Workaround:

1. Reconfigure the replication manually in the Site Recovery UI and exclude the newly added disk.
2. Reconfigure the replication again and include the previously excluded disk.

- **NEW Data does not sync properly after reverting to a snapshot**

If a full synchronization is in progress and you revert the protected VM to a snapshot, the data may not sync properly.

Workaround to prevent the issue:

1. Establish an SSH connection to the vSphere Replication Server virtual machine.
2. Navigate to `/etc/vmware`.
3. Open `hbrsrv.xml` in a text editor, uncomment the property and change the `<optimizeInitialSync>` value to false.
4. Restart the HBR service by using the command `systemctl restart hbrsrv`.

Workaround if you have hit the issue:

Perform full synchronization by using the vSphere Replication Management Server Managed Object Browser.

1. Go to `https://vrms_address:8043/mob/?vmodl=1`.
2. Navigate to **content > replication-manager > getOutgoingReplications**.
3. Change the **parameters** as follows:

start: 0

count: 200

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

4. Find the replication that you need to fully synchronize by looking for the VM name and click on the replication ID (GID-<uuid> value).
5. Click on **fullSync > Invoke method**.

In the Site Recovery plug-in, you will now see that the state of this replication has changed to *Initial Sync*.

- **Configuring replication fails after switching from vSphere Trust Authority to KMS as an encryption mechanism**

If you are using vSphere Trust Authority as an encryption mechanism, but switch back to the old encryption mechanism using KMS servers, and then try to configure a replication, the process might fail. The problem is observed, because the encryption keys might not be properly distributed to the target hosts, after switching the encryption mechanisms.

Workaround: Restart the HMS service.

- **Reconfiguring replication at the remote site fails with an error**

When you attempt to reconfigure replication at the remote site, the process fails with the following error:

Failed to reconfigure replication because of java.lang.NullPointerException at
com.vmware.hms.replication.SecondaryGroupImpl.reconfigureVirtualMachine(SecondaryGroupImpl.java:3163) at
com.vmware.hms.replication.SecondaryGroupImpl.scheduledReconfigure(SecondaryGroupImpl.java:2840) at
com.vmware.hms.replication.SecondaryGroupImpl.access\$3(SecondaryGroupImpl.java:2812) at
com.vmware.hms.replication.SecondaryGroupImpl\$2.go(SecondaryGroupImpl.java:2780) at com.vmware.hms.task.TaskRunnable.run(TaskRunnable.java:71) at
com.vmware.hms.HmsTaskManager\$2.run(HmsTaskManager.java:519) at
com.vmware.hms.util.executor.LoggerOpIdConfigurator\$RunnableWithDiagnosticContext.run(LoggerOpIdConfigurator.java:133) at
com.vmware.hms.util.executor.LoggerOpIdConfigurator\$2.run(LoggerOpIdConfigurator.java:100)

This problem only happens with vSphere Replication appliance which is upgraded from an older versions than 8.1.0, for example from 6.5 and earlier.

Workaround:

1. Establish an SSH connection to the HMS appliance.
2. Navigate to `/opt/vmware/hms/bin/`.
3. To check if the issue is coming from a particular replication, run this command:

```
./embedded_db_connect.sh --no-align --tuples-only -c "select diskentity.isnativesnapshotsupported, secondaryvirtualmachineentity.name from diskentity, secondaryvirtualmachineentity where secondaryvirtualmachineentity.movalue = diskentity.vm_movalue;"
```

4. If the running the command from step 3 gives any results, also run the following command:


```
secondaryvirtualmachineentity where secondaryvirtualmachineentity.movalue = diskentity.vm_movalue;"
```

5. Restart the HMS service by using the `systemctl restart hms` command.

- **Reconfiguring a replication fails after changing the Virtual Device Node on the source VM**

If you change the Virtual Device Node settings on a replicated disk and then you attempt a manual or automatic reconfiguration (in case you have enabled automatic replication of new disks) of the replication, the process fails with the following error:

```
Unable to complete the reconfiguration task at remote site for replication group '<VM_ID>' (managed object ID: 'GID-<group-ID>'): task 'HTID-<hms-task-ID>'. Details: 'A runtime error occurred in the vSphere Replication Management Server. Exception details: 'VR Server error: 'Error for (diskId: "RDID-<replica-disk-ID>"): SQLite error 19: UNIQUE constraint failed: ReplicatedDisk.diskID; Returned error message: UNIQUE constraint failed: ReplicatedDisk.diskID; Code set to: A disk with the given ID already exists.; Disk ID already in database!; Adding replica disk RDID-<replica-disk-ID> (groupID=GID-<group-ID>) to database; Adding disk RDID-<replica-disk-ID>; Adding disk info to database.'.'. '.
```

Workaround:

1. Reconfigure the replication manually in the Site Recovery UI and exclude the disk, whose Virtual Device Node settings you changed.
2. Reconfigure the replication again and include the previously excluded disk.

- **Automatic reconfiguration of a replication fails with an error after disk is added or Virtual Device Node on excluded disk is changed**

If you have a replicated VM and the option for automatic replication of new disks is enabled, then you might receive the following error:

```
Unable to complete the reconfiguration task at remote site for replication group '<vm-ID>' (managed object ID: 'GID-<group-ID>'): task 'HTID-<hms-task-ID>'. Details: 'Disk file name '<vmdk-name>.vmdk' already exists.
```

The error might be due to one of the following two scenarios:

- a) You deleted a disk on the source VM and then added a new disk.
- b) You changed the Virtual Device Node settings of a disk on the source VM, which is excluded from the replication.

Workaround: Wait for a time period, which is greater than the RPO and then manually reconfigure the replication using the DR UI. If you have enabled MPIT, you must wait until all replication instances, which contain references to the deleted/modified disk, expire.

- **Reconfiguring a replication fails with an error**

If you exclude a disk from a replication and then try to include it again, the reconfiguration fails with the following error:

```
Unable to complete the reconfiguration task at remote site for replication group '<vm_id>' (managed object ID: 'GID-<group-id>'): task 'HTID-<hms-task-id>'. Details: 'Disk file name '<vm_id2>.vmdk' already exists.
```

Workaround: Wait for a time period, which is greater than the RPO, after you exclude the disk, to be able to include it again. If you have enabled MPIT, you must wait until all replication instances, which contain references to the excluded disk, expire. Alternatively, you can manually delete the vmdk file from the destination datastore (you can see the name of the vmdk file in the error message.)

- **Test recovery fails with an error**

If you configure a replication to a VMFS datastore and then reconfigure any disk of this group to be replicated to a vSAN datastore (while the VM home is still configured to a VMFS datastore), when you try to perform a test recovery, it fails with the following error:

```
Cannot create a test bubble image for group '<group-ID>' on vSphere Replication Server...
```

Workaround 1: Reconfigure all replica disks back to using a VMFS datastore.

Workaround 2: Reconfigure the VM home to be replicated to a vSAN datastore.

- **Auto-replicate new disks appears as Disabled**

When you go to **Replications > Incoming**, **Auto-replicate new disks** appears as **Disabled**, even though you have enabled it.

Workaround: Go to the remote site and check the status from **Replications > Outgoing**.

- **Replications with network encryption appear in Not Active state**

By default, when you power on the vSphere Replication appliance, a vSphere Installation Bundle (VIB) is installed on all supported ESXi hosts in the vCenter Server inventory where the appliance is deployed. The automatic installation of the VIB file might fail due to different reasons.

Workaround:

Install the vSphere Replication VIB file on each ESXi instance that hosts replication source VM.

1. Temporarily disable the firewall on the ESXi host.
2. Establish an SSH connection to the ESXi Server.
3. Run the following command:

```
$ esxcli software vib install -v https://VR_APPLIANCE_IP:8043/vib/vmware-hbr-agent.vib
```

4. Enable the firewall on the ESXi host.

- **You cannot configure new replications with network encryption**

Workaround:

Install the vSphere Replication VIB file on each ESXi instance that hosts replication source VM.

1. Temporarily disable the firewall on the ESXi host.
2. Establish an SSH connection to the ESXi Server.
3. Run the following command:

```
$ esxcli software vib install -v https://VR_APPLIANCE_IP:8043/vib/vmware-hbr-agent.vib
```

4. Enable the firewall on the ESXi host.

- **Importing or exporting replication configuration data with the vSphere Replication Import/Export tool fails with an error**

If you are using vSphere 6.5 with a vVol datastore and you try to import or export replication configuration data, the operation will fail with the following error:

```
Unable to configure replication: A general system error occurred: Invalid fault
```

Workaround 1: Use a different type of datastore, such as vSAN, VMFS or NFS.

Workaround 2: Upgrade to vSphere 6.7 or vSphere 7.0.

- **Replications change state to Not Active if you try to configure a replication to use both the network encryption and network traffic isolation features**

If you try to configure a replication to use both the network encryption and network traffic isolation features, the replication changes state to Not Active. For example, if you try to use network traffic isolation on the replication of encrypted virtual machines, where network encryption is not optional.

Workaround: Until a future vSphere Replication release to enable the full use of both features, you can only partially combine network encryption and traffic isolation. For example, if you go to the settings of the VMkernel network adapters on the source host and switch off the vSphere Replication tags, the replication state changes to OK, and only traffic isolation of the outgoing traffic from the source site is disabled.

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

The synchronization of replications for which the source VM is running on ESXi 6.7 or 6.7 Update 1 remains in progress, but the checksum bytes value in the replication details information does not progress. Operations such as powering off, taking a snapshot, reverting to a snapshot, and migrations 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.

With these steps, you disable the checksum part of the sync process and all of the allocated blocks are sent to the remote site, regardless of whether they are different or not. Also, you cannot use seeds.

- **If the source VM for a replication runs on ESXi 6.7 or 6.7 Update 1, replication synchronization seems to be in progress, but the replication instance never completes successfully**

In ESXi 6.7 and 6.7 Update 1, 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. Move 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.

- **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.

- **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.

If you configure a replication to use as a seed a VM that has snapshots, the configure operation succeeds, but the replication goes into the **Error** state at the end of the **Initial Full Sync**. An issue with a similar error description appears:

```
"A replication error occurred at the vSphere Replication Server for replication 'vmname'. Details: 'Error for (datastoreUUID:
"vvol:9148a6192d0349de-94149524b5f52bc4"), (diskId: "RDID-fd3ed4de-2356-43c7-a0e2-7bc07a7da012"), (hostId: "host-33"), (pathname:
"vmname/vmname.vmdk"), (flags: retrieable): Class: NFC Code: 10; NFC error: NFC_DISKLIB_ERROR (Input/output error); Set error flag: retrieable;
Can't write (multiEx) to remote disk; Can't write (multi) to remote disk'."
```

Workaround: Delete the snapshots from the seed VM.

- **During full synchronization vSphere Replication fails with error: A replication error occurred at the vSphere Replication Server**

During full synchronization vSphere Replication might fail with the following error.

```
A replication error occurred at the vSphere Replication Server for replication <group_name>. Details: 'Error for (datastoreUUID: "..."), (diskId:
"..."), (hostId: "..."), (pathname: "..."), (flags: retrieable, pick-new-host, nfc-no-memory): Class: NFC Code: 5; NFC error: NFC_NO_MEMORY; Set
error flag: nfc-no-memory; Code set to: Host unable to process request.; Set error flag: retrieable; Set error flag: pick-new-host; Can't write
(single) to remote disk'.
```

Usually, this error is transient and the operation succeeds after some time.

- **Replacing the SSL certificate of vCenter Server causes certificate validation errors in vSphere Replication**

If you replace the SSL certificate on the vCenter Server system, a connection error occurs when vSphere Replication attempts to connect to vCenter Server.

Workaround: For information about how to update vCenter Server certificates and allow solutions such as vSphere Replication to continue to function, see <http://kb.vmware.com/kb/2109074>.

- **Data synchronization fails and the log file of the source vSphere Replication Management Server contains error `DeltaAbortedException`**

If your environment experiences connectivity issues during data synchronization, you might observe the following problems.

- Replication group synchronizations fail and the `hms<n>.log` file in the vSphere Replication Management server at the source site contains the following error message:
`DeltaAbortedException`.
- In Site Recovery Manager, replication group synchronizations fail with the following error message:
`VR synchronization failed for VRM group <group_name>. A generic error occurred in the vSphere Replication Management Server. Exception details: 'com.vmware.hms.replication.sync.DeltaAbortedException' .`

Workaround: Resolve the connectivity issues in your environment before you proceed.

- **Failover with "Sync latest changes" might fail with `SocketTimeoutException` when multiple replications are recovered concurrently and there is a huge accumulated delta since the latest synchronization**

The vSphere Replication Management server might not receive due responses through the vCenter reverse proxy when there is heavy replication traffic at the same network. Some replication management or monitoring operations might fail with the following error message:

```
'com.vmware.vim.vmomi.client.exception.ConnectionException: java.net.SocketTimeoutException: Read timed out'
```

Workaround: Configure network traffic isolation for vSphere Replication traffic, so that the management communication between vCenter and the vSphere Replication Management server is not affected by the heavy replication traffic. See [Isolating the Network Traffic of vSphere Replication](#).

- **Virtual machines that are located in the target folder are overwritten during recovery**

If the target folder contains a registered virtual machine with the same name as the replicated virtual machine, the registered virtual machine is overwritten during the recovery. When you start the Recovery wizard, vSphere Replication checks the target folder and displays a dialog box for you to confirm the overwrite operation. On rare occasions, after the target check is complete, and while the wizard is still open, a virtual machine might be registered to the target folder. On these occasions, the virtual machine that was copied to the target folder will be overwritten without further notice.

Workaround: None.

- **Replications appear in Not Active (RPO violation) status after changing the IP address of the vSphere Replication server at the target site**

If the IP address of the vSphere Replication server at the target site changes, the status of all replications to this site turns to Not Active (RPO violation). This problem is observed because replications on the source site are not reconfigured automatically when the IP address changes.

Workaround: Reconfigure all replications, so that the source hosts use the new IP address of the target vSphere Replication server.

- **Transient Error state during the initial full synchronization**

During the initial synchronization, you might observe that the state of the synchronization changes temporarily to **Error** and back to normal multiple times. The error state might indicate resource deficiency at the target site. If the IO workload caused by the sync operation is higher than the load that target hosts can handle, the state of the replication will turn to **Error**. When the IO workload decreases, the error disappears.

Workaround: Reduce the value of the host configuration option called **HBR.TransferMaxContExtents** on each ESXi host where replication source VMs are running. The default value is 8, and a lower value decreases the size of data blocks that are sent during one sync update, but increases the duration of the initial full sync. After the initial full sync, change the value back to its default (8) to achieve maximum RPO performance. If transient errors continue to occur during delta synchronizations, it might mean that a lot of changed blocks are transferred during each delta, and the

hosts at the target site cannot accommodate the incurred IO workload. In such cases, keep the value of the `HBR.TransferMaxContExtents` configuration option low.

Alternatively, you can add more hosts to the secondary site.

- **Users that are assigned the VRM administrator or VRM virtual machine replication role cannot access the Configure Replication wizard**

The Configure Replication wizard is not launched if a user that is assigned the predefined VRM administrator or VRM virtual machine replication role logs in the Site Recovery user interface and attempts to configure a replication.

Workaround: Clone the default role to add the **Profile-driven storage -> Profile-driven storage view** privilege to it, and assign the cloned role to the user.

- **The option to enable quiescing is disabled in Configure Replication wizard for a powered off replication source VM, though the guest OS supports quiescing**

For both Linux and Windows sources, the Enable Quiescing option is enabled based on the information about the guest OS. If a virtual machine has never been powered on, ESXi hosts always report no support for quiescing, because the guest OS information is not available.

Workaround: Verify that replication source VMs have been powered on at least once before you configure replications.

- **vSphere Replication Management Server (VRMS) might leak a partially recovered virtual machine in the target vCenter Server after a failed recovery**

In rare cases VRMS might stop during recovery immediately after registering the recovered virtual machine in the target vCenter Server. The last recovery error in the replication details panel says `VRM Server was unable to complete the operation`. When VRMS restarts, it cleans up the files for the partially recovered virtual machine. In some cases, it fails to unregister the virtual machine from the target vCenter Server. Subsequent recovery attempts show an error in the recovery wizard that the selected virtual machine folder already contains an entity with the same name.

Workaround: Manually remove the virtual machine from the target vCenter Server, but keep its disks as they point to the replica placeholder files.

- **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.

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

If you start an operation on one 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 vSphere Web Client and logging back in again.

- **Operation in vSphere Replication Management Server fails with error "... UnmarshalException"**

When the vSphere Replication Management Server experiences high load or transient network errors, operations can fail with `UnmarshalException` due to errors in the communication layer.

Workaround: Try the failed operation again.

- **The VAMI might not respond when you install an update**

When you upgrade vSphere Replication, a status message 'Installing Updates' might not disappear even after the updates install successfully because the VAMI is not responding.

Workaround: Refresh the VAMI UI in the browser or open it in a new tab.

- **A virtual machine recovered in vSphere Replication does not power on in vCenter Server**

When you use vSphere Replication to run a recovery on a virtual machine, it fails, and the status of the replication is not 'Recovered'. The virtual machine is registered in the vCenter inventory, but when you try to power it on, it fails with error: `File [datastorename] path/vmname.vmx was not found`. The virtual machine registration as part of the vSphere Replication recovery workflow can succeed in vCenter Server, but the response might not reach the vSphere Replication Management Server due to a transient network error. vSphere Replication reverts the replication image and reports a failed recovery task due to virtual machine registration error. If you initiate another recovery, it fails with a message that a virtual machine with the same name is already registered in vCenter Server.

Workaround: Remove the partially recovered virtual machine from the vCenter Server inventory. Do not delete the files from disk. Try the recovery again.

- **vSphere Replication operations fail when there is heavy replication traffic**

vSphere Replication operations might fail with error `java.net.UnknownHostException`. These errors occur because DNS requests are dropped due to network congestion.

Workaround: Configure your network to ensure that management traffic is not dropped, by configuring traffic shaping, quality of service, or DNS on the vSphere Replication appliance. One possible solution is to modify the network address caching policy for the vSphere Replication appliance.

1. Log into the vSphere Replication appliance as root.

3. Uncomment the line `networkaddress.cache.ttl` and set its value to at least 86400 seconds (24 hours) or to the longest time that is required for an initial full sync to complete.
4. Save the file and reboot the vSphere Replication appliance.
5. Repeat the procedure for all remaining vSphere Replication appliances.

Replications to vCenter Server

- **You cannot encrypt an unencrypted source VM in an active replication**

If you try to encrypt an unencrypted virtual machine in an active replication configuration, the encryption fails.

Workaround: Recover the unencrypted virtual machine and configure a new replication with encrypted seed disks.

1. Recover the VM on the remote site, but do not power the VM on.
2. Remove the replication of the source VM.
3. Edit the settings of the VM on the target site and change the VM storage policy to VM Encryption Policy.
4. Edit the settings of the source VM on the source site and change the VM storage policy to VM Encryption Policy.
5. Unregister the recovered virtual machine on the target site, but do not delete the disks.
6. Configure a new replication and select the disks of the recovered VM on the target site as seeds.

- **If you reconfigure a replication to assign a new vSAN storage policy to some virtual machine disks, the policy is not applied to the replicas at the target site**

vSAN storage policy is applied to replicas at the recovery site at the time you first configure or recover a replication. If you reconfigure the replication with a new storage policy, the change is not automatically reflected to the pair site.

Workaround:

1. Recover the virtual machines with reconfigured replication.
2. By using the vSphere Client, change the storage policy of the recovered virtual machines to the new policy.
3. Unregister the recovered virtual machines from the vCenter Server inventory.
4. Configure replication again by using seeds and with the new storage policy.

- **Reconfiguring a replication fails if a Storage DRS cluster is selected as destination for the replication**

If you try to reconfigure a replication and move the replication to a datastore part from a Storage DRS cluster, the reconfiguration fails.

Workaround: Remove the replication and configure a new replication to the desired datastore.

- **You cannot use custom defined users and roles with vSphere Replication**

You are unable to configure a replication with a custom user, even if that custom user is assigned all required VRM privileges on both sites. The error message `Permission to perform this operation is denied` appears on the Target Location page in Configure Replication wizards.

Workaround: None. All vSphere Replication operations must be performed with the SSO administrator user on both sites.

- **A recovered virtual machine with multiple point-in-time instances enabled can lose the attached disks to the latest snapshot when you revert to a previous snapshot and then revert to latest snapshot again**

When you recover a virtual machine for which you enabled point-in-time instances and attach a disk for unresolved disks, if any, the disks attach to the latest snapshot. If you revert to a previous snapshot and then revert to the latest one, the attached disks are not available.

Workaround: Edit settings of the virtual machine and add the required disks as existing hard disks.

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

If you configure a replication for a virtual machine with physical mode, 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.

- **Recovering a virtual machine with vSphere Replication 8.3 fails to power on the recovered virtual machine**

If a replicated virtual machine is attached to a distributed virtual switch and you attempt to perform a recovery in an automated DRS cluster, the recovery operation succeeds but the resulting virtual machine cannot be powered on.

Workaround: Edit the recovered virtual machine settings to attach it to the correct network.

- **Registering additional vSphere Replication servers takes a long time**

If vCenter Server manages several hundred ESXi Server hosts, registering an additional vSphere Replication server with the vSphere Replication appliances can take several minutes.



Company

[About Us](#)

[Executive Leadership](#)

[News & Stories](#)

[Investor Relations](#)

[Customer Stories](#)

[Diversity, Equity & Inclusion](#)

[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](#)

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](#)

[Glossary](#)

[Help](#)

[Feedback](#)