VMware vSphere Replication 8.4 Release Notes

Updated on 01/04/2024

VMware vSphere Replication 8.4 | 09 MAR 2021 | Build 17703102 | Download

VMware vSphere Replication 8.4 Configuration Import/Export Tool | 09 MAR 2021 | Build 17703114 | Download

Check for additions and updates to these release notes.

What's in the Release Notes

These release notes cover the following topics:

Localization

VMware vSphere Replication 8.4 is available in the following languages:

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

What's New

- **Reprotect optimization** when vSphere Replication is used with Site Recovery Manager. Checksum is no longer used for reprotect run soon after a planned migration. Instead, changes are tracked at the site of the recovered VM and only those changes are replicated when reprotect is run. For details about using optimized reprotect, see Using vSphere Replication Optimized Reprotect.
- New config service/management UI.
- Support for **vSphere Native Key Provider** - **VRMS Appliance Management Interface**.
- Support for virtual **NVMe controller**.
- Ability to select multiple VMs to move between vSphere Replication servers and to reconfigure replications.
- vSphere Replication 8.4 continues to release accessibility enhancements based on **VPAT** (Voluntary Product Accessibility Template) tests. For more information and to stay up to speed on accessibility efforts at VMware, visit the VMware Accessibility home page.

Product Documentation

In addition to the current release notes, you can use the documentation set for vSphere Replication 8.4 that includes the following deliverables.

- vSphere Replication 8.4 Documentation Center
- Compatibility Matrices for vSphere Replication 8.4

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 8.3 or 8.4.

vSphere Replication 8.4 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 and the VAMI to upgrade to vSphere Replication 8.2.x or 8.3.x to vSphere Replication 8.4.

You cannot upgrade vSphere Replication from version 6.5.1 to version 8.4 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.

See Upgrade Additional vSphere Replication Servers and Upgrade the vSphere Replication Appliance for the procedures on upgrading to vSphere Replication 8.4.

Notes:

- If you have ongoing Disaster Recovery to Cloud replications and you try to upgrade to vSphere Replication 8.4 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 8.4 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 3000 Replications.

Open Source Components

The copyright statements and licenses applicable to the open source software components distributed in vSphere Replication 8.4 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.

- **NEW** vSphere Replication can replicate virtual machines with virtual NVMe. vSphere Replication supports NVMe over Fabrics (NVMe-oF) datastores as a source and a target of a replication. vSphere Replication supports virtual NVMe controllers only if both the source and the target ESXi hosts are version 7.0 Update 2 or later. For more information about using the NVMe technology with the VMware products, see VMware NVMe Concepts in the VMware vSphere 7.0 Documentation.
- **NEW** vSphere Replication 8.4 does not support vSphere 7.0 Update 2 if virtual machine encryption is switched on.
- **NEW** vSphere Replication 8.4 does not provide support bundle management in the VRMS Appliance Management Interface. This includes lists with support bundles and deleting support bundles. To manage the support bundles through SSH, establish an SSH connection to to the vSphere

- **NEW** vSphere Replication will stop working correctly if you run the vSphere *Prevent Guest Operating System Processes from Sending Configuration Messages to the Host* procedure on the vSphere Replication Appliance.
- Resizing a replicated disk of a virtual machine by non-multiple of 512 bytes is not supported. If the disk is resized by non-multiple of 512 bytes, the replication fails. To return to the OK state, the disk size must be set to a multiple of 512 bytes.
- vSphere Replication does not support the protection of virtual machines using persistent memory (PMem) devices.
- 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 during the initial configuration process in the VRMS Appliance Management Interface. This requires user confirmation to proceed with the new appliance. This situation does not occur when deploying more than one vSphere Replication servers.
- Each vSphere Replication Management Server can manage a maximum of 3000 replicated virtual machines. See Configuring Upgraded vSphere Replication Appliances to Support up to 3000 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.
- The 5 minute RPO requires the source host to be ESXi 6.5.
- 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 supports Standard Key Provider and VMware vSphere® Native Key Provider™.
- 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

- **After upgrading to vSphere Replication 8.4 an unexpected error appears in the Site Recovery UI**

  After you upgrade to vSphere Replication 8.4, you might observe the following recurring error in the Site Recovery UI:

  ```
  Bad actionId exportVrLogs
  ```

  Workaround:

  1. Log out from the Site Recovery UI.
  2. Clear the cache of your browser.
  3. Log in to the Site Recovery UI.

- **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.

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.

- **The hms-vpostgres service cannot start after an upgrade attempt through VAMI from vSphere Replication version 8.2.1 to version 8.4**

  The `hms-vpostgres` service cannot start after an upgrade attempt through VAMI from vSphere Replication version 8.2.1 to version 8.4. 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 Reverting a recovered encrypted VM to a snapshot fails with an error**

  When you recover a replication of an encrypted VM with enabled multiple point in time (MPIT) snapshots, the VM encryption is not applied to the point in time (PIT) snapshots that are created after the recovery. The attempt to revert to a snapshot of the recovered encrypted VM fails with the following error: `Unable to open the snapshot file.`

  Workaround: None.

- **NEW Moving seed replica disks from different datastores into one datastore fails**

  When you try to move seed replica disks with identical names from different datastores into one datastore, the process fails. Seed replica disks with the same names cannot exist in the same location.

  Workaround: Rename the seed replica disks before the move.

- **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 logs.

  Workaround: None. Discard the error.

- **NEW You cannot configure a replication for an encrypted VM**

  When you try to configure a replication for an encrypted VM, the process fails with the following error:

  ```
  there are VMCrypt keys not accessible at the destination site
  ```

  Workaround: None.

- **NEW Reprotect operation fails**

  If you configure a replication with an activated quiescing feature and the ESXi host on the target site is version 7.0 or 7.0 Update 1, the reprotect operation fails.

  Workaround: Deactivate the optimized reprotect feature.

  1. Establish an SSH connection to the vSphere Replication Appliance.
  2. Run the following command: `/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property reprotect-optimization-enabled=false`
  3. Restart the HMS service.

- **NEW You cannot configure the network card settings in the VRMS Appliance Management Interface**

  You cannot see the second and/or third network card in the Networking page of the VRMS Appliance Management Interface.

  Workaround:

  1. Power off the VM.
  2. Add a new Network card.
  3. Power on the VM.
  4. In the virtual appliance console, run the `ip addr` command to see the network details and the name of the newly added network card. The network card should have a state `DOWN` and a name `eth1`, for example.
  5. In the virtual appliance console, run the following command:

  ```
  sudo /opt/vmware/bin/create_nic_config.sh <new network card name>
  ```

  For example:

  ```
  sudo /opt/vmware/bin/create_nic_config.sh eth1
  ```

  Note that new NIC will be configured with DHCP IPv4 address by default.
  6. Use the VRMS Appliance Management Interface to configure the network settings for the newly added network card, if required.

- **NEW Protected VMs become unresponsive, when configuring a new replication with large virtual disks or adding large disks to an existing replication**

  If you are running vSphere 7.0 Update 2 and you configure a new replication with large virtual disks or add large disks to an existing replication, the protected VMs become unresponsive.

  Workaround: Deactivate the TRIM/UNMAP feature of vSAN.

  1. Establish an SSH connection to the vCenter Server Appliance.
  2. Run the following command:

  ```
  rvc localhost
  ```

  3. Navigate to the `/localhost/Datacenter/computers` folder.
  4. Run the following command:

  ```
  vsan.unmap_support -d <cluster name>
  ```

- **NEW If you try to run a sync operation after disk resizing, the operation fails.**

  If you perform disk resizing, depending on the size of the disk, the operation might take up to a few hours. When you try to run a sync operation in the meantime, the operation fails, even if the replication is in OK state.

  Workaround: Wait for the disk resizing operation to complete. You can verify the completion by checking the `/var/log/vmware/hbrsrv.log` log file, where you should be able to see this entry:

  ```
  Resizing disk <replicated disk ID>
  ```

- **NEW The recovery of a replication of a VM, encrypted with vSphere Native Key Provider, fails**

  If you remove from the cluster, which is configured with Native Key Provider, all hosts to which the target datastore is attached, the existing replications remain in OK state. However, if you try to perform a recovery, the recovery fails and the replication goes into Error state.

  Workaround: Make the datastore accessible in the cluster again. If you did not attempted recovery and the replication is still in OK state, reconfigure the replication and change the target datastore to a datastore, which is accessible in the cluster.

- **NEW Newly added virtual disk is not replicated upon reprotect operation**

  If you perform recovery and add a new disk to the recovered VM, the new disk is not replicated upon reprotect operation. The new disk is not automatically replicated if the initial replication was configured to automatically replicate new disks either.

  Workaround: Manually include the new disk to the replication.

- **NEW Generating a support bundle fails**

  If the vSphere Replication Appliance is not configured and you try to generate a support bundle, the process fails.

  Workaround: Manually generate the support bundles for the vSphere Replication Appliance and the embedded vSphere Replication Server. The generated files are `/tmp/hms-bundle.tar.gz` and `/tmp/embedded-hbr-bundle.tgz`.

  1. Establish an SSH connection to the vSphere Replication Appliance.
  2. Run the following commands:

  ```
  /bin/tar --force-local --ignore-failed-read -chvpf /tmp/hms-bundle.tar /opt/vmware/hms/logs /opt/vmware/var/log /opt/vmware/support/logs/dr
  /opt/vmware/support/logs/drconfigui /opt/vmware/support/logs/envoy
  /usr/bin/gzip --no-name --quiet --stdout /tmp/hms-bundle.tar > /tmp/hms-bundle.tar.gz
  /urs/bin/rm /tmp/hms-bundle.tar
  /usr/bin/sudo -u root /usr/bin/hbrsrv-support-bundle.sh -f /tmp/embeded-hbr-bundle.tgz
  ```

  3. Navigate to the VMware VRMS Appliance Management for the respective embedded vSphere Replication Server and generate the support

If, within a short period of time, you exclude a virtual disk with a vVOL target datastore from the replication, and then incluce it again, this might affect a subsequent recovery operation. If you attempt to perform the recovery, it might not progress.

Workaround 1

If you already started the recovery operation:

1. Remove the replication, retaining the replica disks.
2. Configure the replication again, using seeds.
3. Perform recovery.

Workaround 2:

If you have not yet started the recovery operation:

1. Exclude the disk with a vVOL target datastore.
2. Sync the replication.
3. Include the disk again.
4. Perform recovery.

- **NEW Replication sync does not progress**

  If, within a short period of time, you exclude a virtual disk with a vVOL target datastore from the replication, and then incluce it again, this might affect a subsequent replication sync operation. If you attempt to perform a replication sync, it might not progress.

  Workaround:

  1. Exclude the disk with a vVOL target datastore.
  2. Sync the replication.
  3. Include the disk again.

- **NEW You cannot use network encryption for vSphere Replication**

  When you try to configure network encryption for a replication, the option in the Configure replication wizard is inactive. If you are using ESX version 6.5, the hbr-agent.vib is not automatically installed on the ESX 6.5 hosts and you cannot configure network encryption for these replications.

  Workaround:

  1. Establish an SSH connection to the vSphere Replication Appliance.
  2. Run the following command: `/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property hms-auto-install-hbragent-vib=false`
  3. Restart the HMS service.
  4. Download and install the hbr-agent.vib for vSphere Replication 8.4 and install it on the ESX 6.5 hosts. See https://kb.vmware.com/s/article/2110304.

- **NEW When you attempt to configure IPv6 through the VMware VRMS Appliance Management you receive an invalid property - dns error**

  When you attempt to configure IPv6 through the VMware VRMS Appliance Management 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 vSphere Replication 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.

- **NEW You cannot reconfigure the IPv6 settings through the VMware VRMS Appliance Management**

  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 vSphere Replication 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.

- **NEW Reconfiguring a replication fails after removing and then adding the same disk to a different Virtual Device Node on the source VM**

  If you remove a virtual disk and add a new one with the same VMDK file, and then you try to perform a manual or an automatic (if you enabled the Auto include new disks option) reconfiguration of the replication, the process fails with the following error:

  ```
  Cannot reconfigure replication group '<VM_ID>' (managed object ID: 'GID-<group-ID>'). Details: 'Duplicate key (hms.Disk) { dynamicType = null, dynamicProperty = null, deviceKey = <DEVICE_KEY>, destination = (hms.ExtendedDatastorePath) { dynamicType = null, dynamicProperty = null, datastore = MoRef: type = Datastore, value = <DATASTORE>, serverGuid = null, path = <PATH>, fileName = <FILENAME>, dsCluster = null }, storageProfileId = null, useOfflineCopy = false, virtualDiskType = thin, skipDiskUuidValidation = true, replicationDiskId = null, contentId = null, capacityInKb = <CAPACITY> }'. ThrowableProxy.cause The operation is not allowed in the current state.
  ```

  Workaround

  1. Stop the replication and preserve the replica disks.
  2. Configure the replication again by using the disks as seeds.

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 mismsatched (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.

- **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:

     ```
     ./embedded_db_connect.sh --no-align --tuples-only -c "update diskentity set isnativesnapshotsupported = false from secondaryvirtualmachineentity where secondaryvirtualmachineentity.movalue = diskentity.vm_movalue;"
     ```

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

- **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.

- **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 the replication source VM.

  1. Temporarily deactivate the firewall on the ESXi host.
  2. Establish an SSH connection to the ESXi Server.

```
$ 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**

  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 deactivate 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. Activate 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 deactivated.

- **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, deactivate 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 deactivate 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 Recovey UI is blocked without notification in Mozilla Firefox browser**

  By default the Site Recovey 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 Recovey 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**

Workaround:

1. Log out from Site Recovery UI and log in again.

2. Deactivate the browser's 'Restore last session' checkbox. For Chrome deactivate the 'Continue where you left off' option.

- **Configuring a replication that uses seeds on a vVol target datastore succeeds, but the replication is in `Error` state**

  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: retriable): Class: NFC Code: 10; NFC error: NFC_DISKLIB_ERROR (Input/output error); Set error flag: retriable; 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: retriable, 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: retriable; 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

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 appear 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 activate quiescing is deactivate 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 "... UnmarshallException"**

  When the vSphere Replication Management Server experiences high load or transient network errors, operations can fail with UnmarshallException 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.
2. Open the file `/usr/java/jre-vmware/lib/security/java.security` in an editor.
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

- **NEW Configuring a replication to a newly registered VM fails with an error**

  If after performing a successful failover, you remove the recovered VM and then re-register it, when you attempt to configure a replication for this VM, the process fails with the following error:

  ```
  VM '<VM_ID>' was recovered in optimized reprotect mode in another replication group. To configure new replication for the VM, you must first remove the existing recovered replication.
  ```

  Workaround: Deactivate vSphere Replication on this VM. See https://kb.vmware.com/s/article/2106946.

- **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 appliance can take several minutes.
  This is because the vSphere Replication server must register with each ESXi Server host.