# VMware vSphere Replication Administration

vSphere Replication 8.4

vmware by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

**VMware by Broadcom**
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

# Contents

# About VMware vSphere Replication

1

VMware vSphere Replication is an extension to VMware vCenter Server that provides a hypervisor-based virtual machine replication and recovery.

vSphere Replication is an alternative to storage-based replication. It protects virtual machines from partial or complete site failures by replicating the virtual machines between the following sites:

- From a source site to a target site
- Within a single site from one cluster to another
- From multiple source sites to a shared remote target site

vSphere Replication provides several benefits as compared to storage-based replication.

- Data protection at a lower cost per virtual machine.
- A replication solution that allows flexibility in the storage vendor selection at the source and target sites.
- Lower overall cost per replication.

## vSphere Replication Use and Compatibility

You can use vSphere Replication with the vCenter Server Appliance or with a standard vCenter Server installation. You can have a vCenter Server Appliance on one site and a standard vCenter Server installation on the other.

vSphere Replication is compatible with N-1 version of vSphere Replication on the paired site. For example, if the current version of vSphere Replication is 8.4, the supported versions for the paired site is 8.3 and later.

## vSphere Replication Functionalities

With vSphere Replication, you can replicate virtual machines from a source data center to a target site quickly and efficiently.

You can deploy additional vSphere Replication servers to meet your load-balancing needs.

After you set up the replication infrastructure, you can select the virtual machines to be replicated at a different recovery point objective (RPO). You can enable the multi-point-in-time retention policy to store more than one instance of the replicated virtual machine. After recovery, the retained instances are available as snapshots of the recovered virtual machine.

You can use VMware vSAN datastores as target datastores and select destination storage profiles for the replica virtual machine and its disks when configuring replications.

You can configure all vSphere Replication features in the Site Recovery user interface like managing sites, registering additional replication servers monitoring and managing replications.

## Site Recovery Client Plug-In

The vSphere Replication appliance adds a plug-in to the vSphere Web Client and vSphere Client. The plug-in is also shared with Site Recovery Manager and is named Site Recovery.

You use the Site Recovery client plug-in to perform all vSphere Replication actions.

- View the vSphere Replication status for all vCenter Server instances that are registered with the same vCenter Single Sign-On.
- Open the Site Recovery user interface.
- View a summary of the replication configuration parameters on the **Summary** tab of virtual machines that are configured for replication.
- Reconfigure the replications of one or more virtual machines by selecting the VMs and using the context menu.
- vSphere Replication Appliance Components

  The vSphere Replication appliance provides all the components that vSphere Replication requires.
- Local and Remote Sites

  In a typical vSphere Replication installation, the local site provides business-critical data center services. The remote site is an alternative facility to which you can migrate these services.
- How vSphere Replication Works

  With vSphere Replication, you can configure the replication of a virtual machine from a source site to a target site, monitor and manage the status of the replication, and recover the virtual machine at the target site.
- Replication Data Compression

  You can configure vSphere Replication to compress the data that it transfers through the network.

# vSphere Replication Appliance Components

The vSphere Replication appliance provides all the components that vSphere Replication requires.

- Site Recovery user interface that provides a full functionality for working with vSphere Replication.
- A plug-in to the vSphere Web Client and vSphere Client that provides a user interface for troubleshooting vSphere Replication health status and links to the Site Recovery standalone user interface.
- A VMware standard embedded vPostgreSQL database that stores the replication configuration and management information. vSphere Replication does not support external databases.
- A vSphere Replication management server:
  - Configures the vSphere Replication server.
  - Enables, manages, and monitors replications.
  - Authenticates users and checks their permissions to perform vSphere Replication operations.
- A vSphere Replication server that provides the core of the vSphere Replication infrastructure.

The vSphere Replication appliance provides a virtual appliance management interface (VRMS Appliance Management Interface.) You can use the VRMS Appliance Management Interface to configure the appliance after deployment. For example, you can use the VRMS Appliance Management Interface to change the appliance security settings or change the network settings. You can deploy additional vSphere Replication Servers using a separate .ovf package.

# Local and Remote Sites

In a typical vSphere Replication installation, the local site provides business-critical data center services. The remote site is an alternative facility to which you can migrate these services.

The local site can be any site where vCenter Server supports a critical business need. The remote site can be in another location, or in the same facility to establish a redundancy. The remote site is typically located in a facility where environmental, infrastructure, or other disturbances are unlikely to occur and affect the local site.

vSphere Replication has the following requirements for the vSphere® environments at each site:

- Ensure that each site has at least one data center.
- Ensure that the remote site has hardware, network, and storage resources that can support the same virtual machines and workloads as the local site.
- Ensure that the sites are connected by a reliable IP network.

- Ensure that the remote site accesses networks (public and private) comparable to the ones on the local site. It is not necessary for them to be in the same range of network addresses.

## Connecting Local and Remote Sites

Before you replicate virtual machines between two sites, you must connect the sites. When connecting sites, users at both sites must have the **VRM remote.Manage VRM** privilege assigned.

When you connect sites that are part of the same vCenter Single Sign-On domain, you must select the remote site only, without providing authentication details, because you are already logged in.

When you connect sites that belong to different vCenter Single Sign-On domains, the vSphere Replication Management Server must register with the Platform Services Controller on the remote site. You must provide authentication details for the remote site, including IP or FQDN of the server where Platform Services Controller runs, and user credentials. See Configure vSphere Replication Connections.

After connecting the sites, you can monitor the connectivity state between them in the Site Recovery user interface.

# How vSphere Replication Works

With vSphere Replication, you can configure the replication of a virtual machine from a source site to a target site, monitor and manage the status of the replication, and recover the virtual machine at the target site.

When you configure a virtual machine for replication, the vSphere Replication agent sends changed blocks in the virtual machine disks from the source site to the target site. The changed blocks are applied to the copy of the virtual machine. This process occurs independently of the storage layer. vSphere Replication performs an initial full synchronization of the source virtual machine and its replica copy. You can use replication seeds to reduce the network traffic that data transfer generates during the initial full synchronization.

During replication configuration, you can set a recovery point objective (RPO) and enable retention of instances from multiple points in time (MPIT).

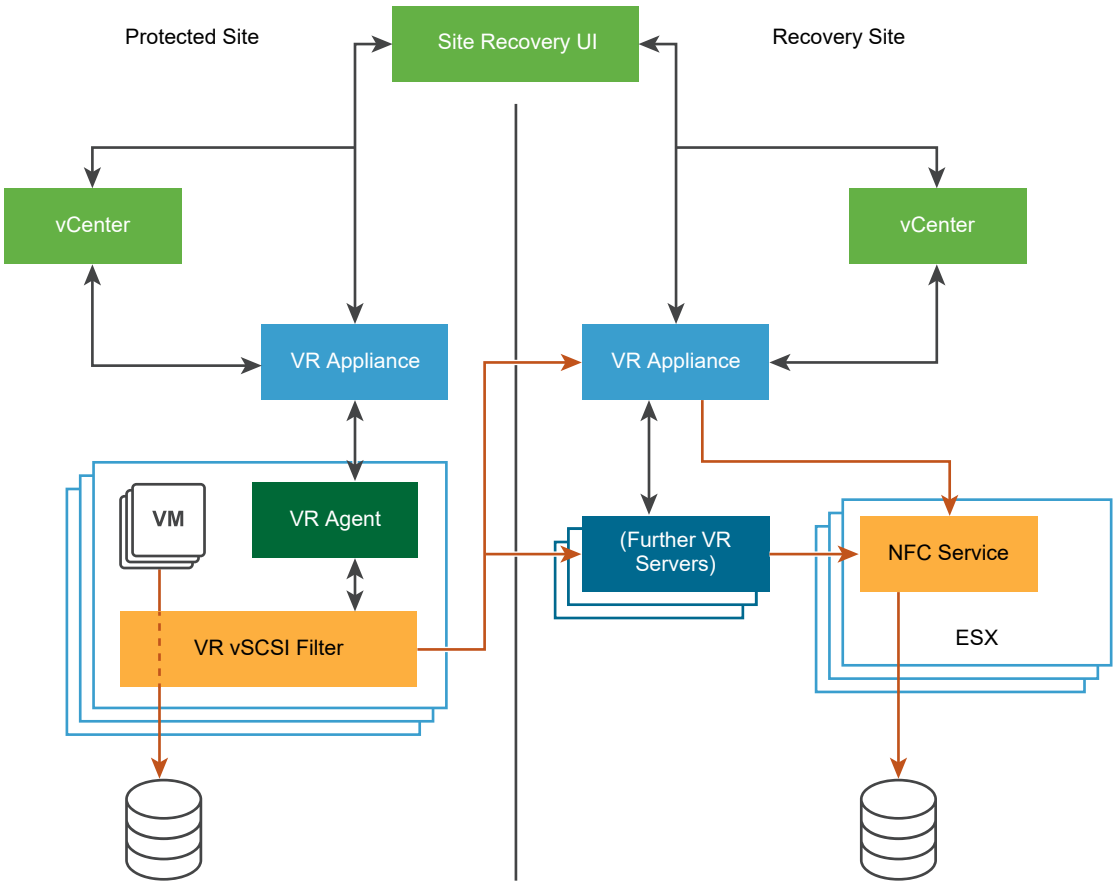
As administrator, you can monitor and manage the status of the replication. You can view information for outgoing and incoming replications, local and remote site status, replication issues, and for warnings and errors.

When you manually recover a virtual machine, vSphere Replication creates a copy of the virtual machine connected to the replica disk, but does not connect any of the virtual network cards to port groups. You can review the recovery and status of the replica virtual machine and attach it to the networks. You can recover virtual machines at different points in time, such as the last known consistent state. vSphere Replication presents the retained instances as ordinary virtual machine snapshots to which you can revert the virtual machine.

vSphere Replication stores replication configuration data in its embedded database.

You can replicate a virtual machine between two sites. vSphere Replication is installed on both source and target sites. Only one vSphere Replication appliance is deployed on each vCenter Server. You can deploy additional vSphere Replication Servers.

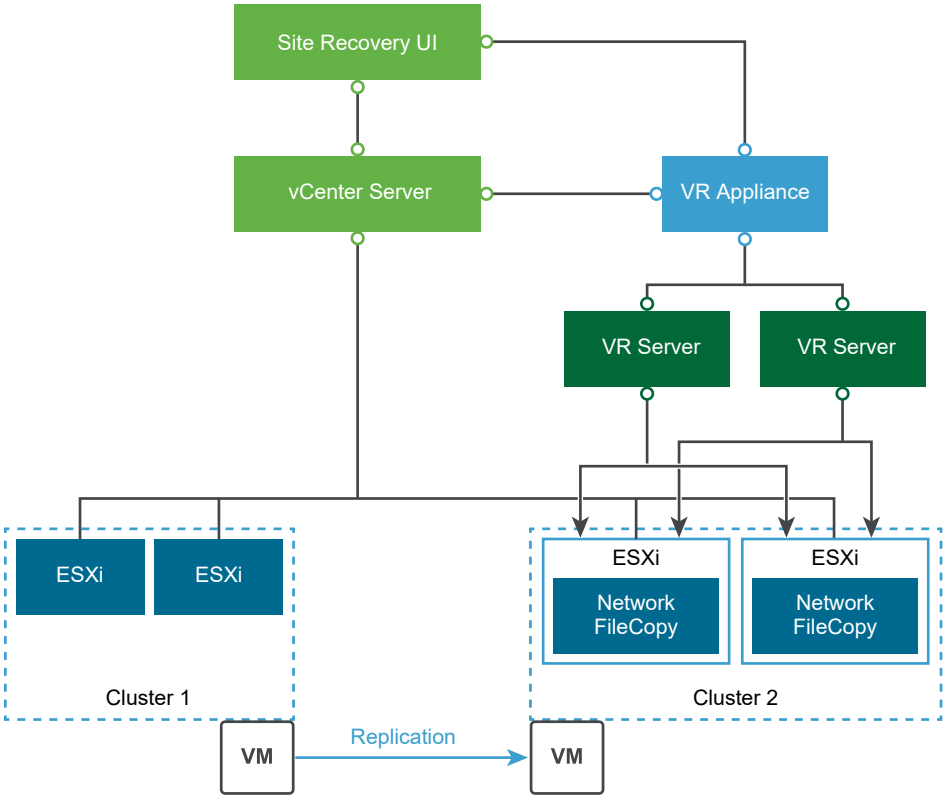
Figure 1-1. Replication Between Two Sites




You can also replicate a virtual machine between datastores at the same vCenter Server. In that topology one vCenter Server manages hosts at the source and at the target. Only one vSphere Replication appliance is deployed on the single vCenter Server. You can add multiple Additional vSphere Replication servers in a single vCenter Server to replicate virtual machines to other clusters.

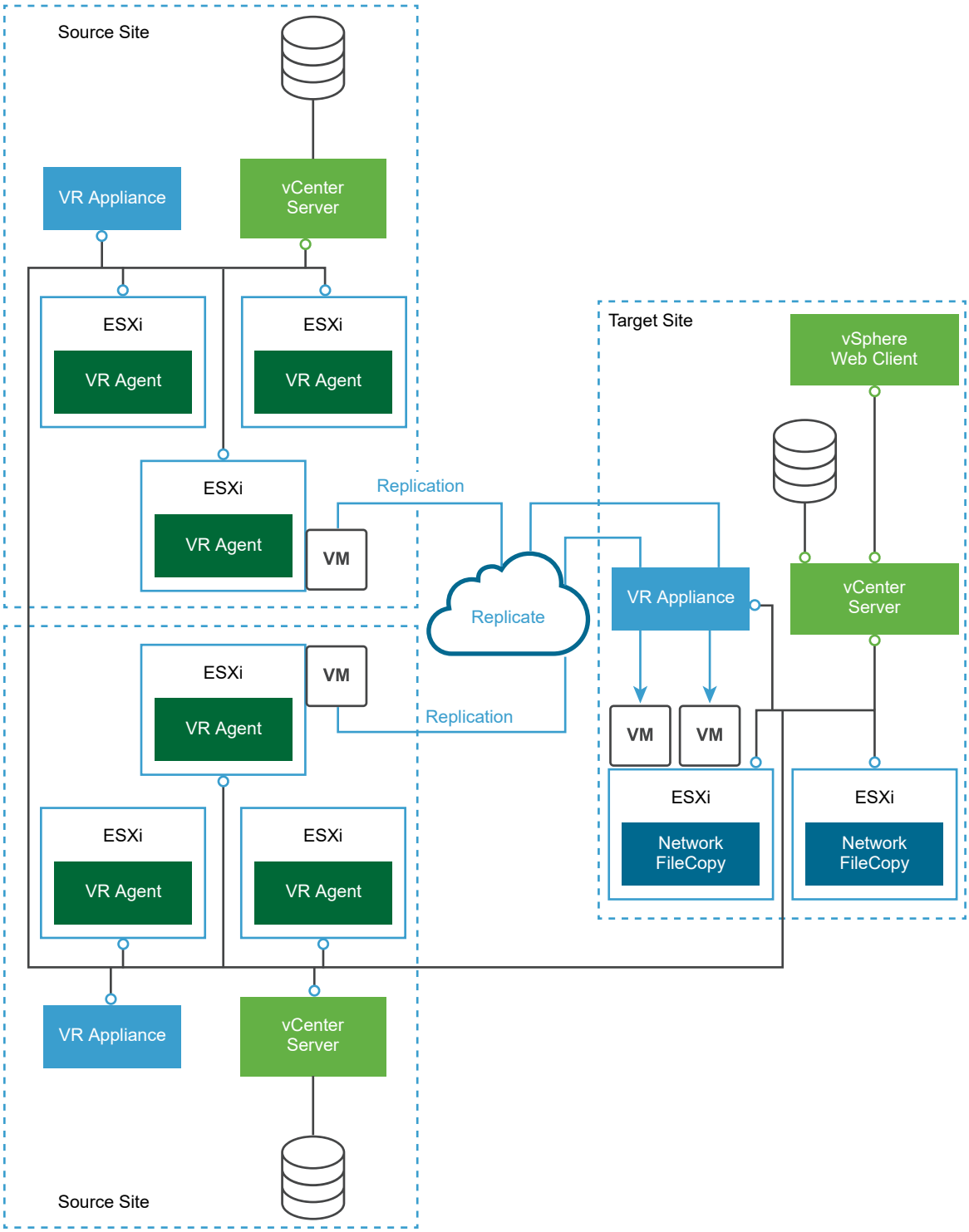
To perform recovery, the vCenter Server managing the target datastore, the vSphere Replication appliance, and any additional vSphere Replication Servers managing the replication must be up and running.

Figure 1-2. Replication in a Single vCenter Server




You can replicate virtual machines to a shared target site.

Figure 1-3. Replication to a Shared Target Site




# Replication Data Compression

You can configure vSphere Replication to compress the data that it transfers through the network.

Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

The ESXi host on the source site compresses the data, and the vSphere Replication server on the target site passes off the data to the ESXi host, where the host decompresses the data, and writes it to disk.

# vSphere Replication System Requirements

2

The environment in which you run the vSphere Replication virtual appliance must meet certain hardware requirements.

vSphere Replication is distributed as a 64-bit virtual appliance packaged in the `.ovf` format. It is configured to use a dual-core or quad-core CPU, a 16 GB and a 17 GB hard disk, and 8 GB of RAM. Additional vSphere Replication servers require 1 GB of RAM.

You must deploy the virtual appliance in a vCenter Server environment by using the OVF deployment wizard on an ESXi host.

vSphere Replication consumes negligible CPU and memory on the source host ESXi and on the guest OS of the replicated virtual machine.

**Note** vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

The operation of vSphere Replication depends on certain services, ports, and external interfaces. For more information, see Services, Ports, and External Interfaces That the vSphere Replication Virtual Appliance Uses.

Read the following topics next:

- vSphere Replication Licensing
- Operational Limits of vSphere Replication
- vSphere Replication Compatibility Information
- Bandwidth Requirements for vSphere Replication

# vSphere Replication Licensing

You can use vSphere Replication with certain editions of vSphere that include vSphere Replication in the license.

vSphere Replication does not have a separate license as it is a feature of certain vSphere license editions.

- vSphere Essentials Plus
- vSphere Standard
- vSphere Enterprise
- vSphere Enterprise Plus
- vSphere Desktop

If you have the correct vSphere license, there is no limit on the number of virtual machines that you can replicate by using vSphere Replication.

You cannot use vSphere Replication to replicate virtual machines on ESXi hosts that do not have the correct vSphere license. If you install vSphere Replication on an ESXi host that does not have the correct license and try to configure a replication for virtual machines on that host, the replication fails with a licensing error.

If you configure a virtual machine for a replication on a host with the correct vSphere license and move it to a host with an unsupported license, vSphere Replication stops the replication of that virtual machine. You can deactivate vSphere Replication on a configured virtual machine on the unlicensed host.

# Operational Limits of vSphere Replication

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

The following operational limits apply to vSphere Replication:

- You can only deploy one vSphere Replication appliance on a vCenter Server instance. After you deploy another vSphere Replication appliance, during the initial configuration process in the VRMS Appliance Management Interface, vSphere Replication detects another appliance already deployed and registered as an extension to vCenter Server. You must confirm if you want to proceed with the new appliance.
- Each newly deployed vSphere Replication appliance can manage a maximum of 3000 replications, of which up to a 1000 can be within the same vCenter Server instance. See https://kb.vmware.com/kb/2102453 for more information.
- vSphere Replication 8.4 uses only an embedded database and requires additional configuration to enable the support of a maximum of 3000 replications. See https://kb.vmware.com/kb/2102463.

Table 2-1. Replication Maximums for vSphere Replication 8.4

| Item | Maximum |
|---|---|
| vSphere Replication appliances per vCenter Server instance. | 1 |
| Maximum number of additional vSphere Replication servers per vSphere Replication. | 9 |
| Maximum number of virtual machines per vCenter Server instance. | 3000 |
| Maximum number of protected virtual machines per vSphere Replication appliance (by using the embedded vSphere Replication server.) | 300 |
| Maximum number of protected virtual machines per vSphere Replication server. | 300 |
| Maximum number of virtual machines configured for one replication at a time. | 20 |
| Maximum number of protected disks per virtual machine on ESXi 8.0 or earlier version. | 64 |
| Maximum number of protected disks per host. | 8192 |

# vSphere Replication Compatibility Information

vSphere Replication is compatible with certain other vSphere management features and other VMware software.

## vSphere Replication Compatibility with Other vSphere Features

You can safely use vSphere Replication with certain vSphere features, such as vSphere vMotion. Some other vSphere features, for example, vSphere Distributed Power Management, require a special configuration for use with vSphere Replication.

**Note** To upgrade VMware Tools, you must upgrade the vSphere Replication appliance.

Table 2-2. Compatibility of vSphere Replication with Other vSphere Features

| vSphere Feature | Compatible with vSphere Replication | Description |
|---|---|---|
| vSphere vMotion | Yes | You can migrate replicated virtual machines by using vMotion. Replication continues at the defined recovery point objective (RPO) after the migration is finished. |
| vSphere Storage vMotion | Yes | You can move the disk files of a replicated virtual machine on the source site using Storage vMotion with no impact on the ongoing replication. |
| vSphere High Availability | Yes | You can protect a replicated virtual machine by using HA. Replication continues at the defined RPO after HA restarts a virtual machine. vSphere Replication does not perform any special HA handling. You can protect the vSphere Replication appliance itself by using HA. |

Table 2-2. Compatibility of vSphere Replication with Other vSphere Features (continued)

| vSphere Feature | Compatible with vSphere Replication | Description |
|---|---|---|
| vSphere Fault Tolerance | No | You cannot replicate virtual machines that have Fault Tolerance activated. You cannot protect the vSphere Replication appliance itself with FT. |
| vSphere DRS | Yes | Replication continues at the defined RPO after the resource redistribution is finished. |
| vSphere Storage DRS | Yes | On the source site, Storage DRS can move the disk files of replicated virtual machines with no impact on the ongoing replication.<br>On the target site, you must register the vSphere Replication appliance with the vCenter Single Sign-On service to activate the communication between Storage DRS and the vSphere Replication Management server. See Configure the vSphere Replication Appliance to Connect to a vCenter Server. |
| vSAN datastore | Yes | You can use vSAN datastores as the source and target datastore when configuring replications. |
| vSphere Distributed Power Management | Yes | vSphere Replication coexists with DPM on the source site. vSphere Replication does not perform any special DPM handling on the source site. You can deactivate DPM on the target site to allow enough hosts as replication targets. |
| VMware vSphere Flash Read Cache | Yes | You can protect virtual machines that contain disks that use the VMware vSphere Flash Read Cache storage. Since the host to which a virtual machine recovers might not be configured for Flash Read Cache, vSphere Replication deactivates Flash Read Cache on disks when it starts the virtual machines on the recovery site. vSphere Replication sets the reservation to zero. Before performing a recovery on a virtual machine that is configured to use vSphere Flash Read Cache, take note of the virtual machine's cache reservation from the vSphere Web Client. After the recovery, you can migrate the virtual machine to a host with Flash Read Cache storage and restore the original Flash Read Cache setting on the virtual machine manually. |
| vSphere Life Cycle Manager | No | You must not run vSphere Replication and vSphere Life Cycle Manager (vLCM) in the same data center, because vLCM causes vSphere Replication to stop. |
| vCloud APIs | Not applicable | No interaction with vSphere Replication. |
| vCenter Chargeback | Not applicable | No interaction with vSphere Replication |
| VMware Data Recovery | Not applicable | No interaction with vSphere Replication. |

## vSphere Replication Compatibility with Other Software

vSphere Replication is compatible with certain versions of ESXi, vCenter Server, Site Recovery Manager, and Web browsers.

For information about the vSphere Replication compatibility, see the following documents:

- Compatibility Matrices for vSphere Replication 8.4 at https://docs.vmware.com/en/vSphere-Replication/8.4/rn/vsphere-replication-compat-matrix-8-4.html.
- vSphere Replication interoperability with backup software when using VSS at https://kb.vmware.com/kb/2040754.
- VMware Compatibility Guide at https://partnerweb.vmware.com/comp_guide2/search.php
- Browser compatibility at vSphere Client and vSphere Web Client Software Requirements in the *vSphere Installation and Setup* guide.

# Bandwidth Requirements for vSphere Replication

To replicate virtual machines efficiently, before configuring a replication you can determine the storage and network bandwidth requirements for vSphere Replication.

Storage and network bandwidth requirements can increase when using vSphere Replication. The following factors play a role in the amount of network bandwidth that vSphere Replication requires for an efficient replication.

## Network-Based Storage

Network bandwidth requirements increase if all storage is network-based, because data operations between the host and the storage also use network. When you plan your deployment, be aware of the following levels of traffic:

- Between the host running the replicated virtual machine and the vSphere Replication server.
- Between the vSphere Replication server and a host with access to the replication target datastore.
- Between the host and storage.
- Between storage and the host, during redo log snapshots.

Network-based storage is a concern when you are replicating virtual machines within a single vCenter Server instance, that shares the network for the levels of traffic listed. When you have two sites, each with a vCenter Server instance, the link speed between the two sites is the most important as it can slow down the replication traffic between the two sites.

## Dataset Size

vSphere Replication might not replicate every virtual machine or every VMDK file in the replicated virtual machines. To evaluate the dataset size that vSphere Replication replicates, calculate the percentage of the total storage used for virtual machines, then calculate the number of VMDKs within that subset that you have configured for replication.

For example, you might have 2 TB of virtual machines on the datastores and use vSphere Replication to replicate half of these virtual machines. You might only replicate a subset of the VMDKs and the maximum amount of data for replication is 1 TB.

## Data Change Rate and Recovery Point Objective

Recovery point objective (RPO) affects the data change rate. To estimate the size of the data transfer for each replication, you must evaluate how many blocks change in a given RPO for a virtual machine. The data change rate within the RPO period provides the total number of blocks that vSphere Replication transfers. This number might vary throughout the day, which alters the traffic that vSphere Replication generates at different times.

vSphere Replication transfers blocks based on the RPO schedule. If you set an RPO of one hour, vSphere Replication transfers any block that has changed in that hour. vSphere Replication only transfers the block once in its current state, at the moment that vSphere Replication creates the bundle of blocks for transfer. vSphere Replication only registers that the block has changed within the RPO period, not how many times it changed. The average daily data change rate provides an estimation of how much data vSphere Replication transfers or how often the transfers occur.

If you use Volume Shadow Copy Service (VSS) to quiesce the virtual machine, replication traffic cannot be spread out in small sets of bundles throughout the RPO period. Instead, vSphere Replication transfers all the changed blocks as one set, when the virtual machine is idle. Without VSS, vSphere Replication can transfer smaller bundles of changed blocks on an ongoing basis as the blocks change, spreading the traffic throughout the RPO period. The traffic changes if you use VSS and vSphere Replication handles the replication schedule differently, leading to varying traffic patterns.

If you change the RPO, vSphere Replication transfers more or less data per replication to meet the new RPO.

## Link Speed

If you have to transfer an average replication bundle of 4 GB in a one hour period, you must examine the link speed, to determine if the RPO can be met. If you have a 10Mb link, under ideal conditions on a dedicated link with little overhead, 4GB takes about an hour to transfer. Meeting the RPO saturates a 10Mb WAN connection. The connection is saturated even under ideal conditions, with no overhead or limiting factors such as retransmits, shared traffic, or excessive bursts of data change rates.

You can assume that only about 70% of a link is available for traffic replication. This means that on a 10Mb link you obtain a link speed of about 3GB per hour. On a 100Mb link, you obtain a speed of about 30GB per hour.

To calculate the bandwidth, see Calculate Bandwidth For vSphere Replication.

There is no hard requirement about the minimal latency across the Wide Area Network (WAN) caused by the geographic distance between the data centers. However, when the WAN connecting the two data centers has latency, out-of-order or dropped packets, the replication throughput can be affected resulting in RPO violations.

# Calculate Bandwidth For vSphere Replication

To determine the bandwidth that vSphere Replication requires to replicate virtual machines efficiently, you calculate the average data change rate within an RPO period, divided by the link speed.

If you have groups of virtual machines that have different RPO periods, you can determine the replication time for each group of virtual machines. For example, you might have four groups with RPO of 15 minutes, 1 hour, 4 hours, and 24 hours. If you want to calculate the bandwidth requirements for vSphere Replication, consider the following factors:

- All the different RPOs in the environment.
- The subset of virtual machines in your environment that is replicated.
- The change rate of the data within that subset.
- The number of data changes within each configured RPO.
- The link speeds in your network.

### Prerequisites

- Examine how data change rate, traffic rates, and the link speed meet the RPO.
- Look at the aggregate of each group.

### Procedure

1. Identify the average data change rate within the RPO by calculating the average change rate over a longer period, then dividing it by the RPO.
2. Calculate how much traffic this data change rate generates in each RPO period.
3. Measure the traffic against your link speed.

### Example

For example, a data change rate of 100GB requires approximately 200 hours to replicate on a T1 network, 30 hours to replicate on a 10Mbps network, 3 hours on a 100Mbps network.

# Installing and Setting Up vSphere Replication

3

To ensure a successful vSphere Replication deployment, follow the sequence of tasks required.

vSphere Replication uses the replication technologies included in ESXi with the assistance of virtual appliances to replicate virtual machines between source and target sites.

To use vSphere Replication, you must deploy the vSphere Replication appliance on an ESXi host by using the vSphere Web Client.

The vSphere Replication appliance registers as an extension with the corresponding vCenter Server instance. For example, on the source site, the vSphere Replication appliance registers with the vCenter Server instance on the source site. Only one vSphere Replication appliance is allowed per vCenter Server.

The vSphere Replication appliance contains an embedded vSphere Replication server that manages the replication process. To meet the load balancing needs of your environment, you might need to deploy additional vSphere Replication servers at each site. Additional vSphere Replication servers that you deploy are themselves virtual appliances. You must register any additional vSphere Replication server with the vSphere Replication appliance on the corresponding site.

The vSphere Replication appliance automatically installs an encryption agent VIB on all ESXi hosts from the vCenter Server inventory. The encryption agent is used to encrypt the outgoing replicated data of the virtual machines that run on these ESXi hosts.

The vSphere Replication appliance provides a virtual appliance management interface (VRMS Appliance Management Interface). You can use the VRMS Appliance Management Interface to perform initial configuration and reconfigure the vSphere Replication database, network settings, public-key certificates, and passwords for the appliances.

Read the following topics next:

- Prepare Your Environment to Install vSphere Replication
- Deploy the vSphere Replication Virtual Appliance
- Configure the vSphere Replication Appliance to Connect to a vCenter Server
- Configure vSphere Replication Connections
- Use the OVF Tool to Deploy vSphere Replication Virtual Appliance
- Uninstall vSphere Replication

# Prepare Your Environment to Install vSphere Replication

Before you deploy the vSphere Replication appliance, you must prepare the environment.

### Prerequisites

Verify that you have vSphere and vSphere Web Client installations for the source and target sites.

**Note** vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

### Procedure

1. In the vSphere Web Client, select the vCenter Server instance on which you are deploying vSphere Replication, click **Configure > Settings > Advanced Settings**, and verify that the `VirtualCenter.FQDN` value is set to a fully qualified domain name or a literal address.
2. If you configure vSphere Replication in an IPv6 network, verify that the IPv6 address of the vSphere Replication appliance, vCenter Server, and the ESXi hosts are mapped to fully qualified domain names on the DNS server. Install the vSphere Replication appliance by using FQDN and post installation, make sure that the **Local Host** text box in the VRMS Appliance Management Interface is set to the FQDN of the vSphere Replication appliance. Do not use a static IPv6 address.

### What to do next

You can deploy the vSphere Replication appliance.

# Deploy the vSphere Replication Virtual Appliance

vSphere Replication is distributed as an OVF virtual appliance. To deploy vSphere Replication successfully, follow the sequence of instructions.

You deploy the vSphere Replication appliance by using the standard vSphere OVF deployment wizard.

**Note** vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

Prerequisites

- Download the vSphere Replication ISO image and mount it on a system in your environment.

Procedure

1. Log in to the vSphere Client on the source site.

   If you use the HTML5-based vSphere Client to deploy the OVF virtual appliance, on vSphere version earlier than vSphere 6.7 Update 1, the deployment succeeds, but vSphere Replication fails to start.
2. On the home page, select **Hosts and Clusters**.
3. Right-click a host and select **Deploy OVF template**.
4. Provide the location of the OVF file from which to deploy the vSphere Replication appliance, and click **Next**.
   - Select **URL** and provide the URL to deploy the appliance from an online URL.
   - If you downloaded and mounted the vSphere Replication ISO image on a system in your environment, select **Local file > Browse** and navigate to the `\bin` directory in the ISO image, and select the `vSphere_Replication_OVF10.ovf`, `vSphere_Replication_OVF10.cert`, `vSphere_Replication_OVF10.mf`, `vSphere_Replication-system.vmdk`, and `vSphere_Replication-support.vmdk` files.
5. Accept the name, select or search for a destination folder or data center for the virtual appliance, and click **Next**.

   You can enter a new name for the virtual appliance. The name must be unique within each vCenter Server virtual machine folder.
6. Select a cluster, host, or resource pool where you want to run the deployed template, and click **Next**.
7. Review the virtual appliance details and click **Next**.
8. Accept the end-user license agreements (EULA) and click **Next**.

9 Select the number of vCPUs for the virtual appliance and click **Next**.

**Note** Selecting higher number of vCPUs ensures the better performance of the vSphere Replication Management Server, but might slow down the replications that run on ESXi host systems that have 4 or less cores per NUMA node. If you are unsure what the hosts in your environment are, select 2 vCPUs.

10 Select a destination datastore and disk format for the virtual appliance and click **Next**.

Encrypting the vSphere Replication appliance VM is not necessary to replicate encrypted VMs with vSphere Replication.

11 Select a network from the list of available networks, set the IP protocol and IP allocation, and click **Next**.

vSphere Replication supports both DHCP and static IP addresses. You can also change network settings by using the VRMS Appliance Management Interface after installation.

12 On the **Customize template** page, enter one or more NTP server host names or IP addresses.

13 Set the password for the root account and enter the hostname or IP address of at least one NTP server.

The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.

14 Click **Next**.

15 Review the binding to the vCenter Extension vService and click **Next**.

16 Review the settings and click **Finish**.

The vSphere Replication appliance is deployed.

17 Power on the vSphere Replication appliance. Take a note of the IP address of the appliance and log out of the vSphere Client.

18 To deploy vSphere Replication on the target site, repeat the procedure.

### What to do next

Configure the vSphere Replication Appliance to connect to a vCenter Server.

## Configure the vSphere Replication Appliance to Connect to a vCenter Server

To start replicating virtual machines, you must configure the vSphere Replication Appliance to connect to a vCenter Server instance on both the source and the target sites.

### Prerequisites

Deploy the vSphere Replication Virtual Appliance and power it on.

Procedure

1 Log in to the VRMS Appliance Management Interface as admin.

2 Click on **Summary**, then click **Configure Appliance**.

3 On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.

| Menu Item | Description |
|---|---|
| PSC host name | Enter the host name (in lowercase letters) or IP address of the Platform Services Controller for the vCenter Server with which to register vSphere Replication. |
| PSC port | Accept the default value of `443`, or enter a new value if Platform Services Controller uses a different port.<br>Platform Services Controller only supports connections over HTTPS. |
| User name | Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the Platform Services Controller instance. |
| Password | The password for the specified vCenter Single Sign-On user name. |

4 If prompted, click **Connect** to verify the Platform Services Controller certificate.

5 On the **vCenter Server** page, select the vCenter Server instance with which to register the vSphere Replication Appliance, and click **Next**.

Caution The drop-down menu includes all the vCenter Server instances that are registered with the Platform Services Controller. In an environment that uses Enhanced Linked Mode, it might also include vCenter Server instances from other Platform Services Controller instances. Make sure that you select the correct vCenter Server instance. After you configure the vSphere Replication Appliance, you cannot select a different vCenter Server instance.

6 On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.

| Menu Item | Description |
|---|---|
| Site name | A name for this vSphere Replication site, which appears in the vSphere Replication interface. The vCenter Server address is used by default. Use a different name for each vSphere Replication instance in the pair. |
| Administrator email | The email address of the vSphere Replication administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for vSphere Replication events. |

| Menu Item | Description |
| --- | --- |
| Local host | The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the vSphere Replication Appliance detects is not the interface that you want to use.<br>**Note** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address. |
| Extension ID | The unique identifier of the vSphere Replication Appliance. The Extension ID is not customizable. |
| Storage Traffic IP | The IP address of a VM NIC to be used by the vSphere Replication Server for incoming replication data. |

7 On the **Ready to Complete** page, review your settings and click **Finish**.

8 To configure the vSphere Replication Appliance on the target site, repeat the procedure.

## Understanding the States of vSphere Replication Displayed in the vSphere Web Client or vSphere Client

You can see the vSphere Replication status on each vCenter Server in your environment and if vSphere Replication does not function properly, you can find the appropriate remediation.

Before you begin using vSphere Replication, you must configure the vSphere Replication Appliance to Connect to a vCenter Server.

After the configuration, in the vSphere Web Client or vSphere Client, when you click **Site Recovery**, you can see the list of vCenter Server instances and the status of vSphere Replication on each vCenter Server instance. If you have Site Recovery Manager deployed in your environment, you can also see the status of Site Recovery Manager. You can change the configuration of each vSphere Replication appliance by clicking the **Configure** icon next to the status icon.

The following table lists the vSphere Replication states that you can observe, their meanings, and what you can do to change a state back to normal.

Table 3-1. vSphere Replication States on vCenter Server Instances

| Status | Description | Remediation |
|---|---|---|
| Not installed | The vSphere Replication extension is not registered in the vCenter Server Extension Manager.<br>The vSphere Replication appliance is either not deployed or the vSphere Replication extension has been deleted from the vCenter Server Extension Manager. | If a vSphere Replication appliance is deployed on this vCenter Server, restart the appliance or the vSphere Replication Management service on the appliance.<br>1 Use a supported browser to log in to the VRMS Appliance Management Interface as the admin user.<br>The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.<br>2 Click **Services**, then select **hms** and click **Restart**. |
| Not configured | A configuration error occurred.<br>The configuration of the vSphere Replication Management Server is incorrect and must be updated.<br>You cannot manage existing replications, or configure new replications to this server . | Configure the vSphere Replication appliance.<br>1 Point to the `Enabled (Configuration issue)` status.<br>The detailed error message appears in a tooltip.<br>2 Click the **Configure** icon.<br>The VRMS Appliance Management Interface opens.<br>3 Click **Summary**, then click **Reconfigure**, and enter the parameters indicated in the error message.<br>4 Click **Restart** . |
| Not compatible | There is a vSphere Replication appliance with earlier version than 8.0, registered in the vCenter Server. | Install vSphere Replication 8.0 or later. |

Table 3-1. vSphere Replication States on vCenter Server Instances (continued)

| Status | Description | Remediation |
|---|---|---|
| Not accessible | The vSphere Replication Management Server is not accessible.<br>The vSphere Replication extension is registered in the vCenter Server Extension Manager, but the vSphere Replication appliance is missing or powered off, or the vSphere Replication Management service is not running.<br>You cannot manage existing replications, or configure new replications to this server . | ■ Verify that the vSphere Replication appliance exists on the vCenter Server.<br>■ Verify that the vSphere Replication appliance is powered on.<br>■ Restart the VRM service.<br>a Use a supported browser to log in to the VRMS Appliance Management Interface as the admin user.<br>The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.<br>b Click **Services**, then select **hms** and click **Restart**. |
| OK | The vSphere Replication appliance is installed, configured, and functioning properly. | Not needed. |

# Configure vSphere Replication Connections

To use vSphere Replication between two sites managed by different vCenter Server instances, you must configure a connection between the two vSphere Replication appliances.

If the source and target vCenter Server instances use the same vCenter Single Sign-On domain, the connection is considered local. vSphere Replication uses the vCenter Single Sign-On service on the local site to authenticate with each vCenter Server in the vCenter Single Sign-On domain.

If the source and the target vCenter Server instances use different vCenter Single Sign-On domains, the connection is considered remote. The vSphere Replication Management Server on the source site registers with the Platform Services Controller of the remote vCenter Single Sign-On domain.

You can use vSphere Replication to replicate virtual machines between ESXi hosts that the same vCenter Server manages. In this case, you deploy only one vSphere Replication appliance and do not need to connect the local and remote sites.

You can configure a connection on either site on which you have installed a vSphere Replication appliance. If you are using an untrusted certificate, certificate warnings might appear during the process.

You can also set up a connection between two sites while you configure a replication between them.

Prerequisites

- Verify that you have installed vSphere Replication at the local and remote sites.
- If you plan to configure a remote connection, obtain the IP address or FQDN of the PSC server where the remote vSphere Replication Management Server is registered.

Procedure

1. On the home page, click **Site Recovery** and click **Open Site Recovery**.
2. On the Site Recovery home page, click the **New Site Pair** button.
3. Select a local vCenter Server from the list, select a pair type, and click **Next**.
   - Pair with a peer vCenter Server located in a different Single Sign-On domain
   - Pair with a peer vCenter Server located in the same Single Sign-On domain
4. Enter the address of the Platform Services Controller for the vSphere Replication Server on the second site, provide the user name and password, and click **Find vCenter Server Instances**.

   The address that you provide for the Platform Services Controller must be an exact match of the of address that you provided when you installed vSphere Replication Server on the target site.

   **Important** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address.
5. Select the vCenter Server and the services you want to pair, and click **Next**.
6. On the Ready to complete page, review your settings selection, and click **Finish**.

Results

The local and the remote sites are connected. The pair appears under on the home page of the Site Recovery user interface.

## Understanding the vSphere Replication Site Connection States

You can view the states of the connections to target sites in the Site Recovery user interface.

The following table lists the states that you can observe, their meanings, and what you can do to change a state back to normal. You can view the states by clicking **View Details** for a site pair in the Site Recovery user interface.

Table 3-2. Replication Server Connection States

| Icon | Status | Description | Remediation |
|---|---|---|---|
|  | Connected | The connection between the local and remote vSphere Replication management servers is working properly. | Not needed. |
|  | Not Connected | ■ The SSL certificate on the local or remote vSphere Replication Management Server has been changed.<br>■ The network connection between the local and remote vSphere Replication Management Servers is not functioning properly or one of the servers is offline.<br>■ The user that is used for authentication with the Lookup Service or the VRMS extension user in the vCenter Single Sign-On might be deactivated or deleted.<br>In this state, configured replications might not be running. | ■ To reconnect the site connection, click the **Reconnect** button in the upper-right corner of the **Summary** page.<br>■ In the vSphere Client or vSphere Web Client, navigate to the vCenter Server, select the **Monitor** tab, and select **Events** under **Tasks and Events** to search for events related to vSphere Replication.<br>■ Verify the status of the remote vSphere Replication appliances in the Site Recovery plug-in for vSphere Client or vSphere Web Client. |

## Reconnect to a Remote Site

If the state of the connection to a target site is `Not connected`, you must repair the connection to manage existing replications, and to enable the creation of new replications.

The states of the connections to the target sites appear in the Site Recovery user interface.

If the source and the target vCenter Server instances use different vCenter Single Sign-On domains, the connection is considered remote. The vSphere Replication Management Server on the source site registers with the Platform Services Controller of the remote vCenter Single Sign-On domain. To establish a connection to a remote site, you provide the address of the

vCenter Server and the Platform Services Controller, and enter the credentials of a user that has the **VRM remote.VRM Server.Manage VRM** privilege assigned. If the Platform Services Controller address changes or there is a change in the certificate, the connection status changes to `Not connected` and you must reconnect the two sites.

**Note** You cannot use the **Reconnect** action to add a missing pairing or a pairing that was manually broken with **Break Site Pair**. If your site pair is missing a pairing, you must use **New Site Pair** to configure it.

### Prerequisites

Verify that the vCenter Server and the vSphere Replication Management Server on the local site are up and running, and that there is no network problem that can cause the `Not connected` status.

### Procedure

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Select **Site Pair > Summary**, and click **Reconnect**.

   You can initiate the reconnect from either site, even if you only changed the installation on one of the sites.
5. Select the services you want to pair. Enter the address of the Platform Services Controller on the remote site, provide the vCenter Single Sign-On user name and password, and click **Reconnect**.

   If the Platform Services Controller manages more than one vCenter Server instance, the other vCenter Server instances appear in the list but you cannot select a different instance. You can only select the vCenter Server instance that vSphere Replication already extends.

### Results

The connection status changes to `Connected`.

# Use the OVF Tool to Deploy vSphere Replication Virtual Appliance

You can use the VMware OVF tool to deploy the vSphere Replication Virtual Appliance from an OVF template.

VMware OVF Tool (`ovftool`) is a flexible command-line utility that you can use to import and export OVF packages to and from a wide variety of VMware products. For more information about `ovftool`, see the OVF Tool Documentation.

### Prerequisites

- Verify that you have downloaded and mounted the vSphere Replication `.iso` image.
- Verify that you have downloaded and installed on your computer the VMware OVF tool 4.2 or later.

### Procedure

1 To deploy the vSphere Replication Virtual Appliance with the VMware OVF Tool, use one of the following command lines.

- If you want to obtain network settings through DHCP:

```
ovftool
--acceptAllEulas
-ds="DATASTORE NAME"
-n="VIRTUAL MACHINE NAME"
--net:"Management Network"="NETWORK NAME"
--prop:"varoot-password"="ROOT USER PASSWORD"
--prop:"vaadmin-password"="ADMIN USER PASSWORD"
--prop:"ntpserver"="NTP SERVER IP OR FQDN"
--vService:installation=com.vmware.vim.vsm:extension_vservice
${VSPHERE_REPLICATION_OVF_FILEPATH}
vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VCENTER_SERVER_ADDRESS}/?ip=$
{ESX_HOST_NAME}
```

- If you want to obtain network settings through a static IP address:

```
ovftool
--acceptAllEulas
-ds="DATASTORE NAME"
-n="VIRTUAL MACHINE NAME"
--net:"Management Network"="NETWORK NAME"
--prop:"varoot-password"="ROOT USER PASSWORD"
--prop:"vaadmin-password"="ADMIN USER PASSWORD"
--prop:"ntpserver"="NTP SERVER IP OR FQDN"
--prop:"network.ip0.vSphere_Replication_Appliance"="VRMS SERVER IP ADDRESS"
--prop:"network.netprefix0.vSphere_Replication_Appliance"="SUBNET MASK"
--prop:"network.gateway.vSphere_Replication_Appliance"="GATEWAY IP ADDRESS"
--prop:"network.DNS.vSphere_Replication_Appliance"="DNS IP ADDRESSES"
--prop:"network.searchpath.vSphere_Replication_Appliance"="DOMAIN SEARCH PATH"
--prop:"network.netmode.vSphere_Replication_Appliance"='static'
--ipAllocationPolicy="fixedPolicy"
--vService:installation=com.vmware.vim.vsm:extension_vservice
${VSPHERE_REPLICATION_OVF_FILEPATH}
vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VCENTER_SERVER_ADDRESS}/?ip=$
{ESX_HOST_NAME}
```

2 Replace the variables in the example with values from your environment.

| Variable | Description |
|---|---|
| *DATASTORE NAME* | The target datastore name. |
| *VIRTUAL MACHINE NAME* | Specify the vSphere Replication Management Server name. |
| *NETWORK NAME* | The name of the network to which you attach the vSphere Replication Appliance. |
| *ROOT USER PASSWORD* | The password for the **root** account. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters. |
| *ADMIN USER PASSWORD* | The password for the **admin** account, which you use to log in to the vSphere Replication Management Server. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters. |
| *NTP SERVER IP OR FQDN* | The IP address or FQDN of the NTP server. |
| *VRMS SERVER IP ADDRES* | The IP address of the vSphere Replication Management Server. |
| *SUBNET MASK* | The subnet mask address of the vSphere Replication Management Server. |
| *GATEWAY IP ADDRESS* | The Gateway address of the vSphere Replication Management Server. |
| *DNS IP ADDRESS* | The DNS address of the vSphere Replication Management Server. |
| *DOMAIN SEARCH PATH* | The domain search path for this virtual machine (use a comma or a space to separate the different names.) |
| *VSPHERE_REPLICATION_OVF_FILEPATH* | The path to the OVF package. To get access to the vSphere Replication OVF files, navigate to the `\bin` directory in the ISO image. |
| *VSPHERE_USER* | The user name for the target vCenter Server. |
| *VSPHERE_USER_PASSWORD* | The password for the target vCenter Server. |
| *VCENTER_SERVER_ADDRESS* | The address of the target vCenter Server. |
| *ESX_HOST_NAME* | The name of the target ESX host. |

### What to do next

Configure the vSphere Replication Appliance to Connect to a vCenter Server service.

# Uninstall vSphere Replication

Uninstall vSphere Replication from your environment.

**Note** If a vSphere Replication appliance is deleted before all replications that it manages are stopped, target datastores remain tagged with the `com.vmware.vr.HasVrDisks` tag. If a target datastore that is tagged with `com.vmware.vr.HasVrDisks` is part of a datastore cluster where Storage DRS is enabled, some operations, like Enter maintenance mode, might not succeed when the vSphere Replication Management server is missing. To prevent errors, you must remove the tags from all target datastores that were used for replications by the deleted vSphere Replication appliance. See Remove the vSphere Replication Tag from Target Datastores.

To uninstall vSphere Replication from your environment, you must unregister the appliance from the vCenter Single Sign-On service and from the vCenter Server, and then delete the vSphere Replication appliance.

If you delete the vSphere Replication appliance before unregistering it from the vCenter Single Sign-On server and the vCenter Server, a special procedure must be performed to clean up your environment. See Clean up the vCenter Server Extension Manager.

### Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Stop all existing outgoing or incoming replications to the site.
- Disconnect any connections to other vSphere Replication sites.

### Procedure

1. Use a supported browser to log in to the VRMS Appliance Management Interface.

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.
2. Click on **Summary**, then click **Unregister**.
3. In the vSphere Web Client, power off and delete the vSphere Replication appliance.

   The Site Recovery plug-in is uninstalled automatically.

### Results

You removed vSphere Replication from your environment.

## Remove the vSphere Replication Tag from Target Datastores

If you delete the vSphere Replication appliance before stopping all its replications, target datastores remain tagged with the `com.vmware.vr.HasVrDisks` tag. To prevent errors, remove the tags from all target datastores that that were used for replications by the deleted vSphere Replication appliance.

If a target datastore that is tagged with `com.vmware.vr.HasVrDisks` is part of a datastore cluster where Storage DRS is enabled, some operations, like Enter maintenance mode, might not succeed when the vSphere Replication Management server is missing.

Prerequisites

- Verify that the vSphere Replication appliance is deleted.
- Verify that you have the required privilege on the root vCenter Server instance (**Inventory Service.vSphere Tagging.Assign or Unassign vSphere Tag**.)

Procedure

1. Log in to the vSphere Client on the target site.
2. In the search box enter **`com.vmware.vr.HasVrDisks`**, press enter and click the tag.
3. Click the **Objects** tab.
4. Right-click a datastore and select **Tags & Custom Attributes > Remove Tag**.
5. In the Remove Tag dialog box, select the row that contains com.vmware.vr.HasVrDisks and click **Remove**.
6. Repeat steps 4 and 5 for all datastores that are assigned the `com.vmware.vr.HasVrDisks` tag.

# Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted

If you delete the vSphere Replication appliance before unregistering it from the environment, you cannot use the VRMS Appliance Management Interface to unregister vSphere Replication from vCenter Server

Before you deploy a new vSphere Replication Appliance, you must clean up your environment by using the Managed Object Browser (MOB).

## Clean up the vCenter Lookup Service

Use the Managed Object Browser (MOB) to clean up the old vSphere Replication registration in Lookup Service after deleting the vSphere Replication Appliance.

If you delete the vSphere Replication Appliance before you unregister it from the environment, you cannot use the VRMS Appliance Management Interface to unregister vSphere Replication from vCenter Server

Prerequisites

Verify that you have the credentials of a vSphere administrator.

### Procedure

1 Log in with vCenter Server credentials to `https://<vCenter_Server_address>:443/lookupservice/mob/?moid=ServiceRegistration&method=List&vmodl=1`.

**Note** If you have external Platform Services Controller (PSC), use the PSC address instead of the vCenter Server address.

2 To search for the VRMS registrations, replace the value in the **Value** field with the following text and click **Invoke Method**.

```
<filterCriteria>
<siteId></siteId>
<nodeId></nodeId>
<serviceType>
<product></product>
<type>com.vmware.vr.vrms</type>
</serviceType> <endpointType>
<protocol></protocol>
<type></type>
</endpointType>
</filterCriteria>
```

3 Look for the old VRMS registration and copy its **serviceId** value.

4 Navigate to `https://<vCenter_Server_address>:443/lookupservice/mob/?moid=ServiceRegistration&method=Delete`.

5 To delete the service registration, enter the **serviceId** value and click **Invoke Method**.

## Clean up the vCenter Server Extension Manager

Use the Managed Object Browser (MOB) to clean up vSphere Replication from vCenter Extension Manager after deleting the vSphere Replication Appliance.

The procedures on removing the permissions for a solution user and on removing a solution user from the vCenter Single Sign-On domain are documented in the *vSphere 6.5 Security* document. See topics Remove Permissions and Delete vCenter Single Sign-On Solution Users.

### Prerequisites

Verify that you have the credentials of a vSphere administrator.

### Procedure

1 Log in to `https://<vCenter_Server_address>/mob/?moid=ExtensionManager` with vCenter Server credentials.

2 In the extensionList property, click the link for the com.vmware.vcHms extension key to check the key details.

3 Verify that the displayed data is for a vSphere Replication appliance that is already lost.

4 In ExtensionManager, click **unregisterExtension**.

5 Enter **`com.vmware.vcHms`** for the extension key value, and click **Invoke Method**.

6 Verify that the result displays `void` and not an error message.

An error message might appear if the specified extension is not registered, or if an unexpected runtime error occurs.

7 Close the window.

8 Refresh the ExtensionManager page and verify that the extensionList entry does not include com.vmware.vcHms.

9 Remove the permissions for the HMS solution user from all vCenter Server instances in the Single Sign-On domain.

10 Remove the HMS solution user from the vCenter Single Sign-On domain.

#### What to do next

You can deploy a new vSphere Replication appliance.

**Note** If a vSphere Replication appliance is deleted before all replications that it manages are stopped, target datastores remain tagged with the `com.vmware.vr.HasVrDisks` tag. If a target datastore that is tagged with `com.vmware.vr.HasVrDisks` is part of a datastore cluster where Storage DRS is enabled, some operations, like Enter maintenance mode, might not succeed when the vSphere Replication Management server is missing. To prevent errors, you must remove the tags from all target datastores that were used for replications by the deleted vSphere Replication appliance. See Remove the vSphere Replication Tag from Target Datastores.

# Participate in the Customer Experience Improvement Program

4

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

Details regarding the data collected by CEIP and the purposes for which it is used by VMware are available at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

You can choose to join the Customer Experience Improvement Program (CEIP), or leave the CEIP at any time.

### Prerequisites

- CEIP participation requires connection from the vSphere Replication virtual appliance to `https://vcsa.vmware.com:443`.
- If the system uses a firewall or a proxy to connect to the Internet, you must specify a firewall or a proxy rule allowing outbound traffic through for `https://vcsa.vmware.com:443/ph/api/*`.
- Verify that you are a member of the Administrators@vsphere.local group.

### Procedure

1. Log in to the vCenter Server instance as a member of Administrators@vsphere.local by using the vSphere Web Client.
2. On the vSphere Web Client Home page, under Administration, click **Customer Experience Improvement Program**.
3. To activate the CEIP, click **Join**. To deactivate the CEIP, click **Leave**.

# Exporting and Importing Replication Configuration Data

5

You can use the vSphere Replication 8.4 Configuration Import/Export Tool to export and import configuration data about the replications created in vSphere Replication.

If you plan to migrate vSphere Replication to a different host, you can use the tool to export replication settings and the related objects into an XML file. You can then import the configuration data from the previously exported file.

The vSphere Replication 8.4 Configuration Import/Export Tool creates new outgoing replications only for the local site. It does not create incoming replications and it does not modify the existing replications. For example, if you export 10 outgoing replications and delete 6 of them, the import operation configures only the six deleted replications. It skips processing the four existing replications.

When you deploy the vSphere Replication appliance, the vSphere Replication 8.4 Configuration Import/Export Tool is also deployed with the appliance. The tool is located in the `/opt/vmware/vr-impex-tool` directory.

## Requirements for Using the vSphere Replication 8.4 Configuration Import/Export Tool

- You must have Java 1.8.x installed.
- The `JAVA_HOME` environment variable must be properly configured. For example, `JAVA_HOME=C:\Program Files\Java\jre1.8.0_152` for Windows, or `JAVA_HOME=/usr/java/jre1.8.0_152` for Linux.

## Requirements for Exporting and Importing Replication Groups Configuration Data

- Before you can export a configuration, you must have a site pair with vSphere Replication 8.4.x up and running on both the protected and the recovery site.
- Import is supported in a clean vSphere Replication 8.4.x installation, registered to the same vCenter Server instance or to a vCenter Server instance which contains the same inventory.

## Input Parameters Required for Import

- Lookup Service host name. The host name of the Platform Services Controller or the vCenter Server host name, if you are using vCenter Server with an Embedded Platform Services Controller.
- vCenter Single Sign-On administrator user name and password for both sites.

## Exported Information

The vSphere Replication 8.4 Configuration Import/Export Tool exports the host folder information, compute resources, network and datastore information, datastore paths, RPO settings, multiple points in time (MPIT), quiescing, network compression, and so on.

## Network Requirements

You must verify that the following network ports are open.

| Default Port | Target | Description |
|---|---|---|
| 443 | On-premises vCenter Server | vCenter Server HTTPS port |
| 443 | On-premises Platform Services Controller / Lookup service | Platform Services Controller HTTPS port |
| 8043 | On-premises vSphere Replication | vSphere Replication port |

Read the following topics next:

- Export Replication Configuration Data
- Use a Properties File to Export vSphere Replication Configuration Data
- Import Replication Configuration Data
- Import Large Numbers of Replications
- Properties for Automated Export and Import of vSphere Replication Configuration Data
- Syntax of the Import/Export Tool

## Export Replication Configuration Data

You use the vSphere Replication 8.4 Configuration Import/Export Tool to export replication configuration data in an XML file.

### Prerequisites

- Verify that you have Java 1.8.x installed and environment variables configured.
- Verify that you have a site pair with vSphere Replication running on both the protected and the recovery sites.

### Procedure

1. Open a command shell, navigate to `/opt/vmware/vr-impex-tool` directory, and run the following command.

   ```
   java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
   ```

   To make the XML file more human-readable, add the `format` option. Adding the `format` option significantly increases the XML file size.

   ```
   java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
   --format
   ```

2. Enter the host name or the IP address of the Lookup Service.
3. Enter the port number or press Enter, if you use the default port.
4. Accept the SHA-1 Thumbprint.
5. Enter user name and password for the local vCenter Server instance.
6. Select a paired vSphere Replication instance.
7. Enter user name and password for the remote vCenter Server instance.

### Example

Example for Export of Outgoing Replications

```
 java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
 ***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating CMD interaction.
Enter host name or IP address of a Lookup Service:
10.92.228.236
Enter port (or press Enter in case you use the default - 443):

Host 10.92.228.236 has untrusted certificate with SHA-1 Thumbprint:
63:50:89:60:76:5C:78:C9:B0:1A:A6:B6:D0:08:D7:8E:31:46:BF:A7 .
Accept thumbprint? (y/n):
y
Enter username for wdc-rdops-vm09-dhcp-228-236.eng.vmware.com:
administrator@vsphere.local
Enter password for wdc-rdops-vm09-dhcp-228-236.eng.vmware.com:
Establishing connection...
Available HMS servers:
[0] wdc-rdops-vm08-dhcp-221-15.eng.vmware.com
[1] wdc-rdops-vm09-dhcp-228-236.eng.vmware.com

0
One HMS server found: wdc-rdops-vm09-dhcp-228-236.eng.vmware.com
Enter username for pair site 'wdc-rdops-vm08-dhcp-221-15.eng.vmware.com':
administrator@vsphere.local
Enter password for pair site 'wdc-rdops-vm08-dhcp-221-15.eng.vmware.com':
Collecting data...
Starting export...
2019-09-03 16:28:14,771 DEBUG - Hms inventory export started.
2019-09-03 16:28:14,993 DEBUG - Replication groups export started.
```

```
2019-09-03 16:28:15,627 DEBUG - Hms inventory export ended.
2019-09-03 16:28:23,680 DEBUG - Replication groups export ended.
Writing to file started.
Writing to file finished.
Export ended successfully.
```

# Use a Properties File to Export vSphere Replication Configuration Data

You can use a properties file to simplify or automate the export of vSphere Replication configuration data.

### Prerequisites

- Verify that you have Java 1.8.x installed on the vSphere Replication host machine.
- Verify that you have a site pair with vSphere Replication running on both the protected and the recovery site.
- Prepare an *export_vr_configuration*.properties file. See Properties for Automated Export and Import of vSphere Replication Configuration Data.

### Procedure

- Open a command shell, navigate to /opt/vmware/vr-impex-tool directory, and run the following command.

  ```
  java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --
  exportPropererties=Path_to_properties_file
  ```

  To make the XML file more human-readable, add the format option. Adding the format option significantly increases the XML file size.

  ```
  java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --
  exportProperties=Path_to_properties_file
  ```

### Example

Example of Export with Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --
exportProperties=/opt/vmware/vr-impex-tool/sample.properties --exportPath=/opt/vmware/vr-
impex-tool/
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***

Initiating using properties file.

Establishing connection...

Collecting data...

Starting export...
```

```
2019-10-28 07:56:52,529 DEBUG - VR inventory export started.

2019-10-28 07:56:52,632 DEBUG - Replication groups export started.

2019-10-28 07:56:52,668 DEBUG - VR inventory export ended.

2019-10-28 07:56:53,329 DEBUG - Replication groups export ended.

Writing to file started.

Writing to file finished.

Export ended successfully.
```

# Import Replication Configuration Data

You can use the vSphere Replication 8.4 Configuration Import/Export Tool to import replication configuration data from a previously exported XML file.

### Prerequisites

- Provide a clean vSphere Replication installation, registered with the same vCenter Server instance or with a vCenter Server instance with the same inventory as the exported.

### Procedure

1. Open a command shell, navigate to the folder of the `/opt/vmware/vr-impex-tool` directory, and run the following command.

   ```
   java -jar vr-impex-tool-<version>.jar --importInteractive --
   path=Path_toexported_XML_file
   ```

2. (Optional) To automate the import process by using a *sample.properties* file, run the following command instead.

   ```
   java -jar vr-impex-tool-<version>.jar --importProperties=sample.properties --
   path=Path_toexported_XML_file
   ```

3. Enter the host name or the IP address of the Lookup Service.
4. Enter the port number or press Enter, if you use the default port.
5. Accept the SHA-1 Thumbprint.
6. Enter user name and password for the local vCenter Server instance.
7. Select a paired vSphere Replication instance.
8. Enter user name and password for the remote vCenter Server instance.

### Results

The vSphere Replication 8.4 Configuration Import/Export Tool creates replications using the exported XML file.

#### Example

Example of Importing the Configuration by Using a Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --
importProperties=/opt/vmware/vr-impex-tool/sample.properties --path=/opt/vmware/vr-impex-tool/
sample.xml
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating using properties file.
Establishing connection...
Collecting data...
2019-08-23 02:13:10,246 INFO - Importing hms data.
Reading file...
Reading file done.
2019-08-23 02:13:10,636 INFO - Import hms configurables started.
2019-08-23 02:13:11,478 DEBUG - Getting profiles for server with guid 'd83b4ce0-4530-4a45-
b493-5f137598d3f2'.
2019-08-23 02:13:11,510 DEBUG - Getting profiles for server with guid '1c0f9490-3ac3-4546-
af4a-10ab4ee634c7'.
2019-08-23 02:13:11,525 DEBUG - Starting import of replications.
2019-08-23 02:13:11,619 DEBUG - Importing Replication Group for server with guid
'd83b4ce0-4530-4a45-b493-5f137598d3f2' is complete.
2019-08-23 02:13:13,834 DEBUG - Importing Replication Group for server with guid
'1c0f9490-3ac3-4546-af4a-10ab4ee634c7' is complete.
2019-08-23 02:13:13,834 INFO - Import VR configurables ended. Imported : 2 .
Import ended successfully.
```

## Import Large Numbers of Replications

You can use the vSphere Replication 8.4 Configuration Import/Export Tool to import the replication configuration data for over 200 replications. You can import the data from a previously exported XML file.

When you have an environment with over 200 replications, the replications are spread on more than one vSphere Replication server. After you export the replication configuration data, you must change the exported XML file to balance the replication workload.

#### Prerequisites

- Verify that you have Java 1.8.x installed and environment variables configured.
- The `JAVA_HOME` environment variable must be properly configured. For example, `JAVA_HOME=C:\Program Files\Java\jre1.8.0_152` for Windows, or `JAVA_HOME=/usr/java/jre1.8.0_152` for Linux.
- Verify that you have a site pair with vSphere Replication 8.4.x up and running on both the protected and the recovery site.

#### Procedure

1 Copy the exported XML file, so that you have two identical files.

  For example, `exported_vr_config.xml` and `exported_vr_config.1.xml`.

2 Open `exported_vr_config.xml` in a text editor and change the replication number to 200 or less.

3 Open `exported_vr_config.1.xml` in a text editor and change the replication number to the remaining replications in your environment.

4 Change the target vSphere Replication server name in `targetHbrServerName` to `vrs-<No.>`.

5 Import `exported_vr_config.xml` that contains 200 replication configurations or less.

6 Deploy a second vSphere Replication server on the target site.

7 Import `exported_vr_config.1.xml`.

# Properties for Automated Export and Import of vSphere Replication Configuration Data

You use the vSphere Replication 8.4 Configuration Import/Export Tool properties file to automate the export and import of replication configuration data.

The vSphere Replication 8.4 Configuration Import/Export Tool properties file must follow a specific structure.

Table 5-1. Parameters for the Properties File

| Parameter | Description |
|---|---|
| `lookup.service.address` | The local Lookup Service address. For a cloud to cloud pairing, use the internal vCenter Server IP address. |
| `port` | The port number for the Lookup Service. The default value is `443`. This parameter is optional. |
| `local.vc.address` | The local vCenter Server name. |
| `local.auth.credentials.vc.username` | The user name of the local vCenter Server. |
| `local.auth.credentials.vc.password` | The password for the local vCenter Server. |
| `local.vr.name` | The name of the local vSphere Replication Management server.<br>**Note** The name of the vSphere Replication management server is customizable and can be different from the host name of the FQDN. Retrieve the name from the Site Recovery UI. |
| `remote.vc.address` | The remote vCenter Server name. |
| `remote.auth.credentials.vc.username` | The user name for the remote vCenter Server. Required if your environment is not federated. |

Table 5-1. Parameters for the Properties File (continued)

| Parameter | Description |
| --- | --- |
| `remote.auth.credentials.vc.password` | The password for the remote vCenter Server. Required if your environment is not federated. |
| `remote.vr.name` | The name of the remote vSphere Replication Management server.<br>**Note** The name of the vSphere Replication management server is customizable and can be different from the host name of the FQDN. Retrieve the name from the Site Recovery UI. |

## Example: Sample Properties File

```
lookup.service.address=10.193.15.152
local.auth.credentials.vc.username=administrator@vsphere.local
local.auth.credentials.vc.password=
remote.auth.credentials.vc.username=administrator@vsphere.local
remote.auth.credentials.vc.password=
local.vr.name=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
remote.vr.name=sc-rdops-vm12-dhcp-109-104.eng.vmware.com
```

# Syntax of the Import/Export Tool

The vSphere Replication 8.4 Configuration Import/Export Tool includes different options that you can use to import or export configuration data.

Table 5-2. vSphere Replication 8.4 Configuration Import/Export Tool Options

| Option | Description |
| --- | --- |
| `--export` | Required when doing an export. Cannot be used together with `--import`. |
| `--exportProperties` | Used to start an export by using a properties file. |
| `--exportInteractive` | Used to start an export interactively with prompts for the required information. |
| `--exportPath` | Used to specify the directory in which to create the exported file. When the directory is not specified, the file is exported in the location of the import/export tool. |
| `--importInteractive` | Used to start an import interactively with prompts for the required information. |
| `--importProperties` | Used to start an import by using a properties file. |
| `--path` | Used for importing data. Path to the previously exported file. |
| `--lspp` | The Platform Services Controller address. Can be an IP address or FQDN. For vSphere Replication, it must match the `lookup.service.address` property. |

Table 5-2. vSphere Replication 8.4 Configuration Import/Export Tool Options (continued)

| Option | Description |
|---|---|
| `--port <[1, 2147483647]>` | The port number for the Lookup Service. The default value is *443*. |
| `--localVrName` | The name of the local vSphere Replication Management server. It must match the `local.vr.name` property. |
| `--remoteVrName` | The name of the remote vSphere Replication Management server. It must match the `remote.vr.name` property. |
| `--localAuthCredsUsername` | The user name for the local vCenter Server. |
| `--localAuthCredsPass` | The password for the local vCenter Server. |
| `--remoteAuthCredsUsername` | The user name for the remote vCenter Server. |
| `--remoteAuthCredsPass` | The password for the remote vCenter Server. |
| `--format` | Used to make the exported XML file better formatted and human-readable. The `--format` option significantly increases the file size. |

### Sample Commands with Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --format --
exportProperties=/opt/vmware/vr-impex-tool/sample.properties --exportPath=/opt/vmware/vr-
impex-tool/
```

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --importProperties=/opt/
vmware/vr-impex-tool/sample.properties --path=/opt/vmware/vr-impex-tool/sample.xml
```

### Sample Properties File

```
lookup.service.address=10.193.15.152
local.auth.credentials.vc.username=administrator@vsphere.local
local.auth.credentials.vc.password=
remote.auth.credentials.vc.username=administrator@vsphere.local
remote.auth.credentials.vc.password=
local.vr.name=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
remote.vr.name=sc-rdops-vm12-dhcp-109-104.eng.vmware.com
```

### Sample Commands in Interactive Mode

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
```

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --importInteractive --
path=Path_toexported_XML_file
```

### Sample of Using Interactive Mode

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --exportInteractive
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating CMD interaction.
Enter host name or IP address of a Lookup Service:10.193.15.152
Enter port (or press Enter in case you use the default - 443):
Host sc2-rdops-vm08-dhcp-15-152.eng.vmware.com has untrusted certificate with SHA-1
Thumbprint: 82:CF:58:F2:E7:C6:A1:4C:
89:FC:7B:05:31:DD:13:00:28:21:DA:F3 .
Accept thumbprint? (y/n):y
Enter username for sc2-rdops-vm08-dhcp-15-152.eng.vmware.com:administrator@vsphere.local
Enter password for sc2-rdops-vm08-dhcp-15-152.eng.vmware.com:
Establishing connection...
Available VR servers:
[0] sc-rdops-vm12-dhcp-109-104.eng.vmware.com
[1] sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
0
One VR server found: sc2-rdops-vm08-dhcp-15-152.eng.vmware.com
Enter username for pair site 'sc-rdops-vm12-
dhcp-109-104.eng.vmware.com':administrator@vsphere.local
Enter password for pair site 'sc-rdops-vm12-dhcp-109-104.eng.vmware.com':
Collecting data...
Starting export...
2019-10-30 04:21:18,464 DEBUG - VR inventory export started.
2019-10-30 04:21:18,548 DEBUG - Replication groups export started.
2019-10-30 04:21:18,585 DEBUG - VR inventory export ended.
2019-10-30 04:21:19,228 DEBUG - Replication groups export ended.
Writing to file started.
Writing to file finished.
Export ended successfully.
```

### Sample of Using Commands without Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --
localVrName=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com --remoteVrName=sc-rdops-vm12-
dhcp-109-104.eng.vmware.com --lspp=10.193.15.152 --format --exportPath=/opt/
vmware/vr-impex-tool/ --localAuthCredsUsername=administrator@vsphere.local --
remoteAuthCredsUsername=administrator@vsphere.local --localAuthCredsPass=***** --
remoteAuthCredsPass=*****
```

### Sample of Using Commands without Properties File

```
java -jar /opt/vmware/vr-impex-tool/vr-impex-tool-<version>.jar --
localVrName=sc2-rdops-vm08-dhcp-15-152.eng.vmware.com --remoteVrName=sc-rdops-vm12-
dhcp-109-104.eng.vmware.com --lspp=10.193.15.152 --format --exportPath=/opt/
vmware/vr-impex-tool/ --localAuthCredsUsername=administrator@vsphere.local --
remoteAuthCredsUsername=administrator@vsphere.local --localAuthCredsPass=Admin!23 --
remoteAuthCredsPass=Admin!23
***Copyright (c) 2018-2019 VMware, Inc. All rights reserved.***
Initiating CMD interaction.
Establishing connection...
Collecting data...
Starting export...
```

```
2019-10-30 04:28:54,426 DEBUG - VR inventory export started.
2019-10-30 04:28:54,508 DEBUG - Replication groups export started.
2019-10-30 04:28:54,543 DEBUG - VR inventory export ended.
2019-10-30 04:28:55,230 DEBUG - Replication groups export ended.
Writing to file started.
Writing to file finished.
Export ended successfully.
```

# Isolating the Network Traffic of vSphere Replication

6

You can isolate the network traffic of vSphere Replication from all other traffic in a data center's network.

Isolating the replication traffic helps you ensure that sensitive information is not routed to the wrong destination. It also helps you enhance the network performance in the data center, because the traffic that vSphere Replication generates does not impact other types of traffic. Traffic isolation also facilitates monitoring and troubleshooting. You isolate the network traffic to the vSphere Replication Server by dedicating a VMkernel NIC on each ESXi host on the primary site that sends data to the vSphere Replication Server. See Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host.

**Note** You cannot enable the vSphere Replication traffic on a custom TCP/IP stack on the ESXi host. vSphere Replication uses the default stack on the ESXi host. To isolate the network traffic, you must use a VMkernel adapter tagging or configure static routes.

If you are using a distributed network switch, you can take advantage of the vSphere Network I/O Control feature to set limits or shares for incoming and outgoing replication traffic on each ESXi host. The feature allows you to manage the network resources that vSphere Replication uses.

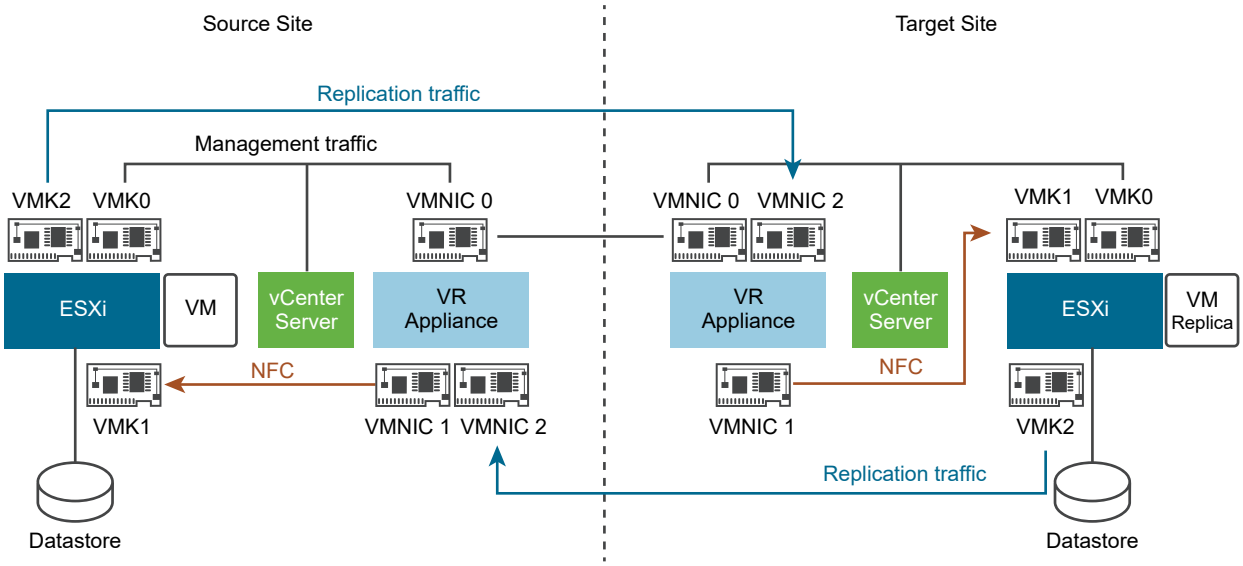
By default, the vSphere Replication appliance has one VM network adapter that is used for various traffic types.

- Management traffic between vSphere Replication Management Server and vSphere Replication Server.
- Replication traffic from the source ESXi hosts to the vSphere Replication Server.
- Traffic between vCenter Server and vSphere Replication Management Server.
- NFC (Network File Copy) traffic, which is the traffic from the vSphere Replication Server appliance at the target site to the destination datastores.

You can add network adapters to the vSphere Replication appliance and use the VRMS Appliance Management Interface to configure a separate IP address to use for each traffic type.

You can isolate the vSphere Replication NFC traffic from the vSphere Replication Server to the target datastore. By default, the NFC traffic is sent to the target ESXi host from the vSphere Replication Server through the management network. You can isolate the NFC traffic from the management traffic by sending it through the replication network. In this case, the vSphere Replication server handles the replication and NFC traffic together, by using the same interface. To isolate the replication and NFC traffic from the management traffic, you must add a second vNIC to separate them. Alternatively, you can add a third vNIC for the NFC traffic only. This option provides security isolation with a dedicated vSphere Replication VLAN for the replication traffic and another one for the NFC traffic, depending on the security requirements in your environment.

Figure 6-1. vSphere Replication Traffic Isolation




In the vSphere Replication appliance, the IP address that is used for management traffic between the vSphere Replication Management Server and vSphere Replication Server is localhost 127.0.0.1. Therefore, you do not need to add network adapters for this type of traffic.

When the vSphere Replication Management Server and the vSphere Replication Server run on separate appliances, you can specify a non-localhost IP address to be used by the vSphere Replication Management Server.

**Note** After the IP address of the vSphere Replication server on the target site changes, the replications are automatically reconfigured with the new IP address.

In addition, you must configure the relevant static routes on each ESXi host at the source site to communicate with the target site. For replications to flow in the opposite direction, you must configure reverse routes on the ESXi hosts on the target site. See https://kb.vmware.com/kb/2001426. Depending on the complexity of your environment, if you want to isolate the NFC traffic, you must configure the relevant vSphere Replication and NFC vSphere Replication static routes after you configure the VMkernel adapters for vSphere Replication and NFC traffic.

Read the following topics next:

- Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host
- Set Up a VMkernel Adapter for vSphere Replication Traffic on a Target Host
- Create a VM Network Adapter to Use for Incoming Replication Traffic on the Combined vSphere Replication Appliance
- Create VM Network Adapters to Isolate the Network Traffic of an Additional vSphere Replication Server
- Configure a Static Route on an Additional VM Network Adapter

# Set Up a VMkernel Adapter for vSphere Replication Traffic on a Source Host

You create VMkernel adapters to isolate the outgoing replication traffic on source ESXi hosts.

**Note** One VMkernel adapter must handle one traffic type.

Perform this procedure for every ESXi host that is used as a replication source, and for which you want to isolate the replication traffic.

### Prerequisites

- Verify that the vSphere Replication virtual appliance is deployed and registered with the vCenter Server.
- For distributed network switches, verify that you have a port group that you can dedicate to the new VMkernel adapter.

### Procedure

1. In the vSphere Web Client, navigate to the ESXi host.
2. Click the **Configure** tab and under **Networking**, select **VMkernel adapters**.
3. Click the **Add networking** icon  .

   The **Add Networking** wizard opens.
4. On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.
5. On the Select target device page, select a port group or a standard switch and click **Next**.
6. On the Port properties page, under VMkernel port settings, configure the IP settings and TCP/IP stack to comply with your environment.

   **Note** vSphere Replication requires that all components in your environment, such as vCenter Server, ESXi hosts, and the vSphere Replication appliance use the same IP version, IPv4 or IPv6.

7 Under Available services, select **vSphere Replication** and click **Next**.

8 Apply the IP settings, click **Next**, and **Finish** to complete the wizard.

### Results

The VMkernel adapter that you created for outgoing vSphere Replication traffic appears in the list of adapters. The outgoing replication data from the ESXi host is sent to the vSphere Replication server through this adapter.

### What to do next

You can add a vNIC to the vSphere Replication appliance and use the VRMS Appliance Management Interface to configure an IP address to use for incoming replication data.

## Set Up a VMkernel Adapter for vSphere Replication Traffic on a Target Host

You create VMkernel adapters to isolate the incoming replication traffic on target ESXi hosts.

**Note** One VMkernel adapter must handle one traffic type.

Perform this procedure for every ESXi host that is used as a replication target, and for which you want to isolate the replication traffic.

### Prerequisites

- For distributed network switches, verify that you have a port group that you can dedicate to the new VMkernel adapter.

### Procedure

1 In the vSphere Web Client, navigate to the ESXi host.

2 Click the **Configure** tab and under **Networking**, select **VMkernel adapters**.

3 Click the **Add networking** icon  .

The **Add Networking** wizard opens.

4 On the Select connection type page, select **VMkernel Network Adapter** and click **Next**.

5 On the Select target device page, select a port group or a standard switch and click **Next**.

6 On the Port properties page, under VMkernel port settings, configure the IP settings and TCP/IP stack to comply with your environment.

**Note** vSphere Replication requires that all components in your environment, such as vCenter Server, ESXi hosts, and the vSphere Replication appliance use the same IP version, IPv4 or IPv6.

7 Under Available services, enable the service for either **vSphere Replication**, **vSphere Replication NFC**, or both on the dedicated vSphere Replication VMkernel adapter.

8 Click **Next**.

9 Apply the IP settings, click **Next**, and **Finish** to complete the wizard.

### Results

The VMkernel adapter that you tagged for NFC traffic appears in the list of adapters. The vSphere Replication Server routes the replication data to the adapter, and the ESXi host saves the data to a datastore.

### What to do next

1 Apply the configuration of the VMkernel Adapters for each ESXi host in your environment.

2 Configure the relevant static routes on each ESXi host at the source site to communicate with the target site. For replications to flow in the opposite direction, you must configure reverse routes on the ESXi hosts on the target site. See https://kb.vmware.com/kb/2001426. Depending on the complexity of your environment, if you want to isolate the NFC traffic, you must configure the relevant vSphere Replication and NFC vSphere Replication static routes after you configure the VMkernel adapters for vSphere Replication and NFC traffic.

## Create a VM Network Adapter to Use for Incoming Replication Traffic on the Combined vSphere Replication Appliance

By default, the combined vSphere Replication appliance has one VM network adapter. You can add a second adapter to the appliance, and configure vSphere Replication to use the second adapter only for the incoming replication traffic.

The IP address that is used for the vSphere Replication management traffic is localhost 127.0.0.1. The default VM network adapter is used by the vSphere Replication server for the replication traffic, and for managing the add-on replication servers. Use the following procedure to add a second adapter to the vSphere Replication appliance only for the incoming replication traffic.

### Prerequisites

- Verify that the vSphere Replication virtual appliance is deployed and registered with the vCenter Server.
- Make a note of the IP address of the VM network adapter.

Procedure

1 Power off the vSphere Replication appliance and edit the **VM Hardware** settings to add a new VM NIC.

   a Right-click the VM and select **Edit Settings**.

   b From the **New Device** drop-down menu at the bottom of the **Virtual Hardware** tab, click **Network Adapter**.

      The new network adapter appears in the list of devices at the right.

   c Expand the properties of the new network adapter to verify that **Connect At Power On** is selected.

      You can assign a static MAC address or leave the text box empty to obtain an MAC address automatically.

   d Click **OK** to close the Edit Setting dialog box.

2 Power on the vSphere Replication appliance.

3 From the **Summary** tab of the vSphere Replication appliance, take a note of the IP address of the new network adapter.

   You can click **View all *XX* IP addresses** to see the IP address of the new NIC.

4 (Optional) If you need to configure a static route on the new NIC, see Configure a Static Route on an Additional VM Network Adapter.

5 Use a supported browser to log in to the VRMS Appliance Management Interface .

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.

   **Note** After powering on the vSphere Replication, the VRMS Appliance Management Interface address might change to the new network adapter's IP address.

6 Click on **Summary**, then click **Change**.

7 In the **IP Address for Incoming Storage Traffic** text box, enter the IP address of the new network adapter that you added and click **Save**.

Results

The vSphere Replication appliance uses the IP address that you assigned only for the incoming replication traffic.

# Create VM Network Adapters to Isolate the Network Traffic of an Additional vSphere Replication Server

By default, the vSphere Replication Server appliance has one VM network adapter. You can add network adapters to the appliance and configure vSphere Replication to use a separate adapter for each traffic type.

The default VM network adapter that is used by the vSphere Replication Server for management and replication traffic. Use the following procedure to add a second adapter to the vSphere Replication appliance for each traffic type.

### Prerequisites

- Verify that you have deployed the vSphere Replication Server appliance in your environment and that it is registered as a vSphere Replication Server in the vSphere Web Client.
- Verify that you have at least one additional vSphere Replication server in your environment.

### Procedure

1. Power off the vSphere Replication appliance and edit the **VM Hardware** settings to add a new VM NIC.
   a. Right-click the VM and select **Edit Settings**.
   b. From the **New Device** drop-down menu at the bottom of the **Virtual Hardware** tab, click **Network Adapter**.

      The new network adapter appears in the list of devices at the right.
   c. (Optional) If you want to isolate the NFC traffic from the replication traffic, click **Add** again to add another VM NIC to handle the NFC traffic separately.

      The first network adapter must be attached to the replication traffic port group and the other network adapter is for the NFC traffic port group.
   d. To verify that **Connect At Power On** is selected, expand the properties of the new network adapter or adapters, if you want to isolate the NFC from the replication traffic.

      You can assign a static MAC address or leave the text box empty to obtain an IP address automatically.
   e. Click **OK** to close the Edit Setting dialog box.
2. Power on the vSphere Replication appliance.
3. From the **Summary** tab of the vSphere Replication appliance, take note of the IP address of the new network adapters.

   You can click **View all *XX* IP addresses** to see the IP addresses of the new VM NICs.
4. (Optional) If you need to configure a static route on the new NIC, see Configure a Static Route on an Additional VM Network Adapter.
5. Use a supported browser to log in to the VRMS Appliance Management Interface of an additional vSphere Replication server.

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.
6. Click **Summary**, then click **Change**.

7 Enter the IP addresses of the new VM NICs that you want to use to isolate the network traffic of vSphere Replication.

| Option | Description |
|---|---|
| **IP Address for Incoming Storage Traffic** | The IP address of a VM NIC to be used by the vSphere Replication Server for incoming replication data. |
| **IP Address for VRMS Management Traffic** | The IP address of a VM NIC to be used by the vSphere Replication Management Server to manage the vSphere Replication Server. |

8 Click **Apply Network Settings**.

### Results

Separate NICs handle the different types of traffic that vSphere Replication generates.

# Configure a Static Route on an Additional VM Network Adapter

To manage replication traffic by using an additional VM NIC, you must configure a static route for the VM NIC.

### Prerequisites

- Verify that you have added a new VM NIC.
- Make a note of the number of the new VM NIC.

### Procedure

1 Establish an SSH connection to the vSphere Replication appliance.

2 To locate the network configuration file, navigate to `/etc/systemd/network`.

3 Open the `10-eth<NIC_Number>.network` file in a text editor and update it.

   a Navigate to the `[Route]` section.

   If you are unable to locate this section in the configuration file, you can manually add it.

   b Set the `Gateway` parameter to the IP address of the next gateway through which the target network can be reached.

   c Set the `Destination` parameter to Classless Inter-Domain Routing (CIDR) notation for the IP range of the target network.

4 Restart the systemd-networkd service by running the `systemctl restart systemd-networkd` command.

5 Validate the static route by running the `ip r` command for IPv4 or the `ip -6 r` command for IPv6.

   a (Optional) If you are not able to validate the route, the network is inaccessible. To force the kernel routing table to accept the network, set the `GatewayOnLink` parameter to `yes` in the `[Route]` section.

   b (Optional) Restart the systemd-networkd service by running the `systemctl restart systemd-networkd` command.

**Example**

```
[Route]
Gateway=10.71.239.253
Destination=10.71.232.0/21
```

# Deploying Additional vSphere Replication Servers

7

Depending on replication traffic, you might need to deploy one or more additional vSphere Replication servers.

Read the following topics next:

- Deploy an Additional vSphere Replication Server
- Register an Additional vSphere Replication Server
- Replication Server Connection States
- Reconfigure vSphere Replication Server Settings
- Unregister and Remove a vSphere Replication Server
- Deactivate the Embedded vSphere Replication Server
- Use the OVF Tool to Deploy an Additional vSphere Replication Server

## Deploy an Additional vSphere Replication Server

The vSphere Replication appliance includes a vSphere Replication server. However, you might need to deploy multiple vSphere Replication servers to meet your load-balancing needs.

You can deploy multiple vSphere Replication servers to route traffic from source hosts to target datastores without traveling between different sites managed by the same vCenter Server. You cannot deploy a second management server on the same vCenter Server.

For information about the loads that a vSphere Replication management server and a vSphere Replication server can support, see https://kb.vmware.com/s/article/2102453.

### Prerequisites

- Deploy vSphere Replication appliances on the source and target sites.
- Deploy vSphere Replication servers on a network that allows them to communicate with the vSphere Replication appliances on the source and target sites.
- Verify that the vSphere Replication servers can communicate with the ESXi Server instances on the source site that hosts the replicated virtual machines.

### Procedure

1. Log in to the vSphere Client on the site where you want to deploy the additional vSphere Replication server.
2. On the home page, select **Hosts and Clusters**.
3. Right-click on a data center, host or cluster, and select **Deploy OVF Template**.
4. Provide the location of the OVF file from which to deploy the additional vSphere Replication server, and click **Next**.
   - Select **URL** and provide the URL to deploy the appliance from an online URL.
   - If you downloaded and mounted the vSphere Replication ISO image on a system in your environment, select **Local file > Browse** and navigate to the `\bin` directory in the ISO image, and select the `vSphere_Replication_AddOn_OVF10.ovf`, `vSphere_Replication_AddOn_OVF10.cert`, `vSphere_Replication_AddOn_OVF10.mf`, `vSphere_Replication-system.vmdk`, and `vSphere_Replication-support.vmdk` files. Make sure that you do not select the `vSphere_Replication_OVF10.ovf` file.
5. Accept the name, select or search for a destination folder or data center for the virtual appliance, and click **Next**.

   You can enter a new name for the virtual appliance. The name must be unique within each vCenter Server virtual machine folder.
6. Select a cluster, host, or resource pool where you want to run the deployed template, and click **Next**.
7. Review the virtual appliance details and click **Next**.
8. Select a destination datastore and disk format for the virtual appliance and click **Next**.

   Encrypting the additional vSphere Replication server VM is not necessary to replicate encrypted VMs with vSphere Replication.
9. Set the network properties. Select DHCP or set a static IP address.

   You can change network settings after deployment in the VRMS Appliance Management Interface.
10. Enter a password for the appliance.

    The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.
11. Review your settings and click **Finish**.
12. Power on the vSphere Replication appliance.

### What to do next

When the OVF file has deployed, register the vSphere Replication server with the vSphere Replication appliance.

# Register an Additional vSphere Replication Server

After you deploy additional vSphere Replication servers, you must register these servers with the vSphere Replication appliance to enable them as traffic handlers at the recovery site.

**Note** You can register additional vSphere Replication servers that run within the same vSphere environment.

### Prerequisites

- Verify that the vSphere Replication appliance is deployed and configured.
- Verify that an additional vSphere Replication Server is deployed.

### Procedure

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. On the **Site Pair** tab, select **Configure > Replication Servers**.
5. Click the **Register** icon.
6. From the list, select a virtual machine that is a working vSphere Replication server and click **Select**.

### Results

The newly registered vSphere Replication server appears in the list of vSphere Replication servers.

# Replication Server Connection States

You can view the states of the connections with the replication servers and determine if they need a remediation.

The following table lists the states that you can observe, their meanings, and what you can do to change a state back to normal.

Table 7-1. Replication Server Connection States

| Icon | Status | Description | Remediation |
|---|---|---|---|
|  | Connected | The connection between the source replication server and the target replication server is working properly. | Not needed. |
|  | Disconnected | ■ The SSL certificate on the remote replication server has been changed.<br>■ The network connection between the source site and the target site is not functioning properly, or the remote site is offline. | ■ Click the **Reconnect** icon.<br>■ Verify that the replication server has network connectivity. |

# Reconfigure vSphere Replication Server Settings

The vSphere Replication appliance contains a vSphere Replication server. If you deploy additional vSphere Replication servers, the server settings are established during deployment. You can modify the settings after you deploy the server.

A vSphere Replication server does not require additional configuration through the VRMS Appliance Management Interface after deployment. To increase security, you can change the root password of the vSphere Replication server and install a new certificate. You can use a self-signed certificate, which provides public-key based encryption and authentication, however it does not provide the level of assurance offered when you use a certificate signed by a certificate authority.

You can also reconfigure the network settings for the vSphere Replication server virtual appliance.

**Note** vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

### Prerequisites

Verify that the additional vSphere Replication server is powered on.

Procedure

1 Use a supported browser to log in to the VRMS Appliance Management Interface of the additional vSphere Replication Server that you deployed.

The URL for the VRMS Appliance Management Interface is https://*vr-server-address*:5480.

Use the root password that you set when you deployed the vSphere Replication server.

2 (Optional) Click **Certificates**, then click **Change**.

3 (Optional) Select a certificate type.

| Menu item | Description |
|---|---|
| **Generate a self-signed certificate** | Use an automatically generated certificate.<br>a Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company.<br>b Accept the default FQDN and IP values.<br>**Note** Using self-signed certificate is not recommended for production environments. |
| **Use a PKCS #12 certificate file** | Use a custom certificate.<br>a Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate.<br>b (Optional) Enter the optional private key encryption password. |
| **Use a CA-signed certificate generated from CSR** | Use a CA-signed certificate generated from a CSR.<br>a In the **Certificate file** row, click **Browse**, navigate to the certificate file, and click **Open**.<br>b (Optional) In the **CA chain** row, click **Browse**, navigate to the CA chain, and click **Open**. |

4 (Optional) Click **Change**.

5 (Optional) To change the password for the vSphere Replication server, click **Access** and then **VRMS appliance password > Change**.

6 (Optional) To change the network settings, click **Networking**, and then **Edit**.

7 (Optional) Configure the DNS settings in the **Hostname and DNS** pane.

| Menu Item | Description |
|---|---|
| **Obtain DNS settings automatically** | Obtains the DNS settings automatically from the network. |
| **Enter DNS settings manually** | Uses the DNS address settings that you set manually. If you select this option, you must provide the IP addresses for a primary and a secondary DNS server. |

8 (Optional) In the **eth0** pane, select the IPv4 or theIPv6 protocol type and configure the IP address settings.

- Configure the IPv4 address settings.

| Option | Description |
|---|---|
| Obtain IPv4 settings automatically | Obtains the IP address for the appliance from the network. |
| Enter IPv4 settings manually | Uses an IPv4 address that you set manually.<br>1 Enter the IPv4 address<br>2 Enter subnet prefix length.<br>3 Enter the default IPv4 gateway. |

- Configure the IPv6 address settings.

| Option | Description |
|---|---|
| Obtain IPv6 settings automatically using DHCP | Assigns IPv6 addresses to the appliance from the network by using DHCP.<br>**Note** To apply this setting, you must restart the vSphere Replication Appliance. |
| Obtain IPv6 settings automatically using router advertisement | Assigns IPv6 addresses to the appliance from the network by using router advertisement. |
| Use static IPv6 addresses | Uses static IPv6 addresses that you set up manually.<br>1 Enter the IPv6 address and the subnet prefix length in the address box.<br>2 To enter additional IPv6 addresses, click **Add**.<br>3 Enter the default IPv6 gateway. |

9 (Optional) Click **Save**.

10 (Optional) To restart the vSphere Replication service, click **Services > hms > Restart**.

11 (Optional) To reboot the vSphere Replication server appliance, click **Summary** and click **Restart**.

# Unregister and Remove a vSphere Replication Server

If you deployed additional vSphere Replication server instances that you no longer require, you must unregister them from the vSphere Replication appliance before you delete them.

### Prerequisites

Verify that the vSphere Replication server that you want to unregister does not serve any replications, otherwise the operations fails.

### Procedure

1 On the Site Recovery home page, select a site pair and click **View Details**.

2 On the **Site Pair** tab, select **Replication Servers** and find the vSphere Replication server in the list.

   If you have both vSphere Replication and Site Recovery Manager installed, you can find **Replication Servers** on the **Site Pair** tab, under **Configure**.

3 Select the server and click the **Unregister** icon.

4 In the **Hosts and Clusters** view of the vSphere Client, power off and delete the vSphere Replication server virtual machine.

# Deactivate the Embedded vSphere Replication Server

The vSphere Replication appliance includes an embedded vSphere Replication Server by default. If you want to deactivate the embedded vSphere Replication server, you can do so using SSH.

### Prerequisites

Verify that no replications are using the embedded server. Stop the replications or move them to a different server.

### Procedure

1 Use SSH into the vSphere Replication appliance and enter:

```
# /opt/vmware/hms/bin/hms-configtool -cmd reconfig -property hms-embedded-hbr=false
```

2 Restart the HMS service.

```
# service hms restart
```

3 Unregister the embedded vSphere Replication server from the **Replication Servers** view.

   a On the Site Recovery home page, select a site pair and click **View Details**.

   b On the **Site Pair** tab, select **Replication Servers** and find the vSphere Replication server in the list.

      If you have both vSphere Replication and Site Recovery Manager installed, you can find **Replication Servers** on the **Site Pair** tab, under **Configure**.

   c Select the server and click the **Unregister** icon.

### What to do next

Rebooting vSphere Replication does not automatically register the embedded server. To restore the default behavior to register automatically the embedded vSphere Replication server, enter:

```
# /opt/vmware/hms/bin/hms-configtool -cmd reconfig -property hms-embedded-hbr=true
# service hms restart
```

# Use the OVF Tool to Deploy an Additional vSphere Replication Server

You can use the VMware OVF tool to deploy an additional vSphere Replication server from an OVF template.

VMware OVF Tool (`ovftool`) is a flexible command-line utility that you can use to import and export OVF packages to and from a wide variety of VMware products. For more information about `ovftool`, see the OVF Tool Documentation.

### Prerequisites

- Verify that you have downloaded and mounted the vSphere Replication .iso image.
- Verify that you have downloaded and installed on your computer the VMware OVF tool 4.2 or later.

### Procedure

1. To deploy an additional vSphere Replication server with the VMware OVF Tool, use one of the following command lines.
   - If you want to obtain network settings through DHCP:

     ```
     ovftool
     -ds="DATASTORE NAME"
     -n="VIRTUAL MACHINE NAME"
     --net:"Management Network"="NETWORK NAME"
     --prop:"varoot-password"="ROOT USER PASSWORD"
     --prop:"vaadmin-password"="ADMIN USER PASSWORD"
     --prop:"ntpserver"="NTP SERVER IP OR FQDN"
     ${VSPHERE_REPLICATION_ADD-ON_OVF_FILEPATH}
     vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VCENTER_SERVER_ADDRESS}/?ip=$
     {ESX_HOST_NAME}
     ```

   - If you want to obtain network settings through a static IP address:

     ```
     ovftool
     -ds="DATASTORE NAME"
     -n="SERVER NAME"
     --net:"Management Network"="NETWORK NAME"
     --prop:"varoot-password"="ROOT USER PASSWORD"
     --prop:"vaadmin-password"="ADMIN USER PASSWORD"
     --prop:"ntpserver"="NTP SERVER IP OR FQDN"
     --prop:"vami.ip0.vSphere_Replication_Appliance"="IP ADDRESS"
     --prop:"vami.netmask0.vSphere_Replication_Appliance"="SUBNET MASK"
     --prop:"vami.gateway.vSphere_Replication_Appliance"="GATEWAY IP ADDRESS"
     --prop:"vami.DNS.vSphere_Replication_Appliance"="DNS IP ADDRESSES"
     --prop:"vami.searchpath.vSphere_Replication_Appliance"="DOMAIN SEARCH PATH"
     --ipAllocationPolicy="fixedPolicy"
     ${VSPHERE_REPLICATION_ADD-ON_OVF_FILEPATH}
     vi://${VSPHERE_USER}:${VSPHERE_USER_PASSWORD}@${VCENTER_SERVER_ADDRESS}/?ip=$
     {ESX_HOST_NAME}
     ```

2 Replace the variables in the example with values from your environment.

| Variable | Description |
|---|---|
| *DATASTORE NAME* | The target datastore name. |
| *VIRTUAL MACHINE NAME* | Specify the additional vSphere Replication Server name. |
| *NETWORK NAME* | The name of the network to which you attach the additional vSphere Replication server. |
| *ROOT USER PASSWORD* | The password for the **root** account. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters. |
| *ADMIN USER PASSWORD* | The password for the **root** account, which you use to log in to the vSphere Replication Server. The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters. |
| *NTP SERVER IP OR FQDN* | The IP address or FQDN of the NTP server. |
| *SUBNET MASK* | The subnet mask address of the additional vSphere Replication Server. |
| *GATEWAY IP ADDRESS* | The Gateway address to the additional vSphere Replication Server. |
| *DNS IP ADDRESSES* | The DNS address of the additional vSphere Replication Server. |
| *DOMAIN SEARCH PATH* | The domain search path for this virtual machine (use a comma or a space to separate the different names.) |
| *VSPHERE_REPLICATION_ADD-ON_OVF_FILEPATH* | The path to the vSphere Replication Add-On OVF package. To get access to the vSphere Replication OVF files, navigate to the `\bin` directory in the ISO image. |
| *VSPHERE_USER* | The user name for the target vCenter Server. |
| *VSPHERE_USER_PASSWORD* | The password for the target vCenter Server. |
| *VCENTER_SERVER_ADDRESS* | The address of the target vCenter Server. |
| *ESX_HOST_NAME* | The name of the target ESX host. |

### What to do next

When the OVF file has deployed, register the vSphere Replication server with the vSphere Replication appliance.

# Upgrading vSphere Replication

8

You upgrade the vSphere Replication appliance and any additional vSphere Replication servers by using a downloaded ISO image and the virtual appliance management interface (VAMI).

## Example: vSphere Replication Upgrade Scenarios

You use the ISO file and the VAMI to upgrade from vSphere Replication 8.2.x or 8.3.x to vSphere Replication 8.4.

These examples of upgrade and update scenarios are not exhaustive. For the full list of supported upgrade paths, see the *Compatibility Matrices for vSphere Replication 8.4.x* at https://docs.vmware.com/en/vSphere-Replication/8.4/rn/vsphere-replication-compat-matrix-8-4.html.

- You can upgrade vSphere Replication 8.2.x or 8.3.x to 8.4 by using the ISO file for vSphere Replication 8.4.
- You cannot upgrade vSphere Replication 6.5.1 to 8.4 by using the VAMI.
- You can upgrade between minor versions of vSphere Replication, for example 8.1.1 to 8.1.2, by using the ISO file and the VAMI.

Read the following topics next:

- Order of Upgrading vSphere and vSphere Replication Components
- Upgrade Additional vSphere Replication Servers
- Increase the Hard Disk 1 Disk After Upgrading the vSphere Replication Additional Servers
- Upgrade vSphere Replication Appliance
- Increase the Hard Disk 1 Disk After Upgrading the vSphere Replication Appliance
- Update the vCenter Server IP Address in the vSphere Replication Management Server

## Order of Upgrading vSphere and vSphere Replication Components

There are alternative strategies for the upgrade of vSphere Replication sites.

You can upgrade all components of one of your sites before upgrading all components on the other site. It is best practice to upgrade the vSphere Replication components before the Platform Services Controller and the vCenter Server components.

An alternative strategy is to upgrade the vSphere Replication components on both sites before upgrading the Platform Services Controller appliances and vCenter Server components.

**Note** To avoid replication failures, you must restart the HMS service after you upgrade the vCenter Server components.

You can upgrade the ESXi hosts at any time.

## Upgrading vSphere Replication by Sites

By upgrading the protected site first, you can perform a disaster recovery on the recovery site if you encounter problems during the upgrade that render the protected site unusable.

**Note** To upgrade VMware Tools, you must upgrade the vSphere Replication appliance.

1. Upgrade any additional vSphere Replication server deployments on the protected site.
2. Upgrade the vSphere Replication appliance on the protected site.
3. (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the protected site.
4. (Optional) Upgrade the ESXi host on the protected site
5. Upgrade any additional vSphere Replication server deployments on the recovery site.
6. Upgrade the vSphere Replication appliance on the recovery site.
7. (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the recovery site.
8. (Optional) Upgrade the ESXi host on the recovery site.
9. Verify the connection between the vSphere Replication sites.
10. (Optional) Upgrade the virtual hardware of the virtual machines on the ESXi hosts if there is a specific reason for the upgrade.

## Upgrading vSphere Replication by Components

With this strategy, you can decide when to upgrade certain components. For example, you can delay the upgrade of the Platform Services Controller appliances and vCenter Server components or the ESXi hosts. Verify which new functionalities are available with earlier versions of vCenter Server.

**Note** To upgrade VMware Tools, you must upgrade the vSphere Replication appliance.

1. Upgrade any additional vSphere Replication server deployments on the protected site.
2. Upgrade the vSphere Replication appliance on the protected site.
3. Upgrade any additional vSphere Replication server deployments on the recovery site.
4. Upgrade the vSphere Replication appliance on the recovery site.

5 (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the protected site.

6 (Optional) Upgrade the Platform Services Controller and all components of vCenter Server on the recovery site.

7 (Optional) Upgrade the ESXi host on the protected site.

8 (Optional) Upgrade the ESXi host on the recovery site.

9 Verify the connection between the vSphere Replication sites.

10 (Optional) Upgrade the virtual hardware of the virtual machines on the ESXi hosts if there is a specific reason for the upgrade.

# Upgrade Additional vSphere Replication Servers

If you want to upgrade the additional vSphere Replication servers, you must use a downloadable ISO image. To ensure a successful upgrade, follow the sequence of instructions.

### Prerequisites

- Download the `VMware-vSphere_Replication-8.4.x.x-build_number.iso` image from the vSphere Downloads page. Copy the ISO image file to a datastore that is accessible from the vCenter Server instance that you use with vSphere Replication.
- Verify that you are currently running a version, which allows you to upgrade directly to vSphere Replication 8.4.
  - You can directly upgrade to vSphere Replication 8.4, only if the version of vSphere Replication you currently run is 8.2.x or 8.3.x.
  - If you run an earlier version of vSphere Replication, you must upgrade your vSphere Replication instance to version 8.3 first. For example, to upgrade vSphere Replication 6.5.1 to version 8.4, you must first upgrade 6.5.1 to 8.3.

### Procedure

1 In the vSphere Client, right-click the vSphere Replication Additional Server virtual machine and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **Memory** and change the memory size from 716 MB to 1024 MB.

3 In the vSphere Client, right-click the vSphere Replication virtual machine and select **Edit Settings**.

4 On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.

5 Navigate to the ISO image in the datastore.

6 For **File Type**, select **ISO Image** and click **OK**.

7 Follow the prompts to add the CD/DVD drive to the vSphere Replication virtual machine.

8 In a Web browser, log in to the virtual appliance management interface (VAMI).

The URL for the VAMI is https://*vr_appliance_address*:5480.

9 Click the **Update** tab.

10 Click **Settings**, select **Use CDROM Updates**, and click **Save Settings**.

11 Click **Status** and click **Check Updates**.

The appliance version appears in the list of available updates.

12 Click **Install Updates** and click **OK**.

The VAMI remains in Installation in Progress state. The installation process automatically performs system reboot. You can check if the installation is complete by going to the virtual machine console in the vSphere UI and verifying the vSphere Replication Appliance version, which must be 8.4.

To open the new VRMS Appliance Management Interface, you must refresh your browser.

13 Configure a password for the admin account by using the virtual machine console in the vSphere UI.

a Login to the vSphere Replication console with the root user and the old password.

b Assign the admin user password from the console by using the `passwd admin` command.

### What to do next

- Increase the size of the Hard Disk 1 virtual disk. See Increase the Hard Disk 1 Disk After Upgrading the vSphere Replication Additional Servers.
- Upgrade the vSphere Replication appliance. See Upgrade vSphere Replication Appliance.
- Delete the virtual machine of the old vSphere Replication server.

## Increase the Hard Disk 1 Disk After Upgrading the vSphere Replication Additional Servers

After you upgrade the vSphere Replication Additional Servers, you must increase the size of the Hard Disk 1 disk of the vSphere Replication Additional Server virtual machine.

### Prerequisites

You must increase the size of the Hard Disk 1 disk of the vSphere Replication Additional Server virtual machine from 9 GB to 16 GB.

### Procedure

1 Stop the vSphere Replication Additional Server virtual machine.

2 Increase the virtual disk size of Hard Disk 1 to 16 GB.

3 Start the vSphere Replication Additional Server virtual machine.

4 Open the vSphere Replication Additional Server virtual machine console and run the following command:

```
/opt/vmware/bin/extend_system_partition.sh
```

# Upgrade vSphere Replication Appliance

If you are using vSphere Replication 8.2.x, or 8.3.x you can directly upgrade to version 8.4.

### Prerequisites

- Download the `VMware-vSphere_Replication-8.4.x.x-build_number.iso` image from the vSphere Downloads page. Copy the ISO image file to a datastore that is accessible from the vCenter Server instance that you use with vSphere Replication.
- Verify that you are currently running a version, which allows you to upgrade directly to vSphere Replication 8.4.
  - You can directly upgrade to vSphere Replication 8.4, only if the version of vSphere Replication you currently run is 8.2.x or 8.3.x.
  - If you run an earlier version of vSphere Replication, you must upgrade your vSphere Replication instance to version 8.3 first. For example, to upgrade vSphere Replication 6.5.1 to version 8.4, you must first upgrade 6.5.1 to 8.3, then upgrade 8.3 to 8.4.

**Important** After you upgrade to vSphere Replication 8.4, you must use the admin account to access the virtual appliance console and the VRMS Appliance Management Interface, instead of the root account. See step 12 of the procedure.

### Procedure

1 In the vSphere Client, right-click the vSphere Replication virtual machine and select **Edit Settings**.

2 On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.

3 Navigate to the ISO image in the datastore.

4 For **File Type**, select **ISO Image** and click **OK**.

5 Follow the prompts to add the CD/DVD drive to the vSphere Replication virtual machine.

6 In a Web browser, log in to the virtual appliance management interface (VAMI).

The URL for the VAMI is https://*vr_appliance_address*:5480.

7 Click the **Update** tab.

8 Click **Settings**, select **Use CDROM Updates**, and click **Save Settings**.

9 Click **Status** and click **Check Updates**.

The appliance version appears in the list of available updates.

10 Click **Install Updates** and click **OK**.

The VAMI remains in Installation in Progress state. The installation process automatically performs system reboot. You can check if the installation is complete by going to the virtual machine console in the vSphere UI and verifying the vSphere Replication Appliance version, which must be 8.4.

To open the new VRMS Appliance Management Interface, you must refresh your browser.

11 Configure a password for the admin account by using the virtual machine console in the vSphere UI.

a Login to the vSphere Replication console with the root user and the old password.

b Assign the admin user password from the console by using the `passwd admin` command.

12 After the vSphere Replication appliance reboots, repeat the steps in the Configure the vSphere Replication Appliance to Connect to a vCenter Server topic.

### What to do next

- Increase the size of the Hard Disk 1 virtual disk. See Increase the Hard Disk 1 Disk After Upgrading the vSphere Replication Appliance.
- You might need to re-enable the SSH connections. See Unable to Establish an SSH Connection to the vSphere Replication Appliance.
- If your infrastructure uses more than one vSphere Replication Server, you must upgrade all vSphere Replication Server instances to version 8.4 on the on-premises site.
- If you plan to upgrade the vCenter Server next, you must restart the HMS service after you upgrade the vCenter Server components.

**Important** As of vSphere Replication 8.3, external databases are no longer supported. If you were using an external database in the previous version of vSphere Replication that you were running, all your data will be migrated to the embedded database. You must apply additional configuration to enable the support of up to 3000 replications in the embedded database. See http://kb.vmware.com/kb/2102463.

## Increase the Hard Disk 1 Disk After Upgrading the vSphere Replication Appliance

After you upgrade the vSphere Replication Appliance, you must increase the size of the Hard Disk 1 disk of the vSphere Replication Management Server virtual machine.

### Prerequisites

You must increase the size of the Hard Disk 1 disk of the vSphere Replication Management Server virtual machine from 9 GB to 16 GB.

### Procedure

1. Stop the vSphere Replication Management Server virtual machine.
2. Increase the virtual disk size of Hard Disk 1 to 16 GB.
3. Start the vSphere Replication Management Server virtual machine.
4. Open the vSphere Replication Management Server virtual machine console and run the following command:

   ```
   /opt/vmware/bin/extend_system_partition.sh
   ```

## Update the vCenter Server IP Address in the vSphere Replication Management Server

If during the upgrade process of vCenter Server and the vSphere Replication appliance you changed the vCenter Server certificate or IP address, you must perform additional steps.

To update the vCenter Server certificate, see vSphere Replication Is Inaccessible After Changing vCenter Server Certificate.

You must update the IP address in the vSphere Replication Management Server when the vCenter Server uses a DHCP address that changed during the upgrade and the vSphere Replication Management Server is configured to use the vCenter Server IP address and not FQDN.

If vCenter Server uses a static IP address, it preserves the IP address by default after upgrade.

### Prerequisites

Verify that the vCenter Server and vSphere Replication components are upgraded. For more information, see Order of Upgrading vSphere and vSphere Replication Components.

### Procedure

1. Power off the vSphere Replication appliance and power it on to retrieve the OVF environment.
2. Use a supported browser to log in to the VRMS Appliance Management Interface.

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.
3. Click **Summary**, and click **Reconfigure**.
4. On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.
5. If prompted, click **Connect** to verify the Platform Services Controller certificate.
6. On the **vCenter Server** page, select the new vCenter Server instance, and click **Next**.
7. On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.

8 On the **Ready to Complete** page, review your settings and click **Finish**.

# Reconfiguring the vSphere Replication Appliance

9

If necessary, you can reconfigure the vSphere Replication appliance settings by using the VRMS Appliance Management Interface.

You provide the settings for the vSphere Replication appliance in the **Deploy OVF** wizard when you deploy the appliance. If you selected automatic configuration of the appliance using an embedded database, you can use the vSphere Replication appliance immediately after deployment. If necessary, you can modify the configuration settings of the vSphere Replication appliance after you deploy it.

- Reconfigure General vSphere Replication Settings

  You can use vSphere Replication immediately after you deploy the vSphere Replication appliance. If necessary, you can reconfigure the general settings after deployment in the VRMS Appliance Management Interface.

- Change the Password of the vSphere Replication Appliance

  You set the password of the vSphere Replication appliance when you deploy the appliance. You can change the password after installation by using the VRMS Appliance Management Interface.

- Change the Keystore Passwords of the vSphere Replication Appliance

  To increase security, you can change the passwords of the vSphere Replication appliance keystore. If you copy the keystores from the appliance to another machine, you must change the passwords before the copy operation.

- Change the Truststore Passwords of the vSphere Replication Appliance

  To increase security, you can change the passwords of the vSphere Replication appliance truststore.

- Activate or Deactivate SSH Access to the vSphere Replication Appliance

  You can use the VRMS Appliance Management Interface to edit the appliance SSH access settings.

- Change the SSL Certificate of the vSphere Replication Appliance

  You can change the initial vSphere Replication SSL certificate by generating a new self-signed certificate or uploading an SSL certificate signed by a trusted Certificate Authority.

- Generate and Download a Certificate Signing Request for the vSphere Replication Appliance

  A certificate signing request (CSR) is an encrypted text file that contains specific information, such as organization name, common name, locality, and country. You send the CSR file to a certificate authority (CA) to apply for a digital identity certificate.

- Configure vSphere Replication Network Settings

  You can review your current network settings and change the address and proxy settings for vSphere Replication. If you want to match network configurations, these changes might be necessary.

- Configure the Time Zone and Time Synchronization Settings for the vSphere Replication Appliance

  When you deploy the vSphere Replication, you either use the time settings of the ESXi host on which the appliance is running, or you configure time synchronization with an NTP server. If the time settings in your network change, you can edit the time zone and time synchronization settings of the appliance.

- Start, Stop, and Restart vSphere Replication Appliance Services

  If changes in your environment require the restart of certain services, you can use the VRMS Appliance Management Interface to view the state of the services and to start, stop, and restart them.

- Forward vSphere Replication Appliance Log Files to Remote Syslog Server

  You can forward the vSphere Replication Appliance log files to a remote syslog server to conduct an analysis of your logs.

- Enable the SHA-1 Hashing Function

  You can install certificates, signed with the SHA-1 hashing function in case your environment requires it.

# Reconfigure General vSphere Replication Settings

You can use vSphere Replication immediately after you deploy the vSphere Replication appliance. If necessary, you can reconfigure the general settings after deployment in the VRMS Appliance Management Interface.

The general settings of the vSphere Replication appliance include:

- The name and IP address of the vSphere Replication appliance
- The address and port of the vCenter Server instance to which it connects
- An administrator email address

You can change the general settings from the default values in the VRMS Appliance Management Interface.

For example, you can reconfigure the address of the vSphere Replication appliance if you did not specify a fixed IP address when you deployed the appliance, and DHCP changes the address after deployment. Similarly, you can update the address of the vCenter Server instance if the address changes after deployment.

### Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

### Procedure

1. Log in to the VRMS Appliance Management Interface as admin.
2. Click **Summary**, and click **Reconfigure**.
3. On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.

| Menu Item | Description |
|---|---|
| PSC host name | Enter the host name (in lowercase letters) or IP address of the Platform Services Controller for the vCenter Server with which to register vSphere Replication. |
| PSC port | Accept the default value of `443`, or enter a new value if Platform Services Controller uses a different port.<br>Platform Services Controller only supports connections over HTTPS. |
| User name | Enter the vCenter Single Sign-On user name for the vCenter Single Sign-On domain to which this Platform Services Controller instance belongs. This user account must be a member of the vCenter Single Sign-On administrator group on the Platform Services Controller instance. |
| Password | The password for the specified vCenter Single Sign-On user name. |

4. If prompted, click **Connect** to verify the Platform Services Controller certificate.
5. On the **vCenter Server** page, click **Next**.

   After the initial configuration of the vSphere Replication Appliance, you cannot select a different vCenter Server instance.

6 On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.

| Menu Item | Description |
|---|---|
| Site name | A name for this vSphere Replication site, which appears in the vSphere Replication interface. The vCenter Server address is used by default. Use a different name for each vSphere Replication instance in the pair. |
| Administrator email | The email address of the vSphere Replication administrator. This information is required even though you use the standard vCenter Server alarms to configure email notifications for vSphere Replication events. |
| Local host | The name or IP address of the local host. Only change the value if the IP address is not the one that you want to use. For example, the local host might have more than one network interface, and the one that the vSphere Replication Appliance detects is not the interface that you want to use.<br>**Note** To facilitate IP address changes in your infrastructure, provide a fully qualified domain name (FQDN) whenever possible, rather than an IP address. |
| Extension ID | The unique identifier of the vSphere Replication Appliance. The Extension ID is not customizable. |
| Storage Traffic IP | The IP address of a VM NIC to be used by the vSphere Replication Server for incoming replication data. |

7 On the **Ready to Complete** page, review your settings and click **Finish**.

8 To configure the vSphere Replication Appliance on the target site, repeat the procedure.

### Results

You reconfigured the general settings of the vSphere Replication appliance.

## Change the Password of the vSphere Replication Appliance

You set the password of the vSphere Replication appliance when you deploy the appliance. You can change the password after installation by using the VRMS Appliance Management Interface.

### Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

Procedure

1 Use a supported browser to log in to the VRMS Appliance Management Interface.

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.

2 Enter the admin user name and password for the appliance.

   You configured the admin password during the OVF deployment of the vSphere Replication appliance.

3 Click **Access** and go to **VRMS appliance password > Change**.

4 Enter the current password in the **Current Password** text box.

5 Enter the new password in the **New Password** and the **Confirm New Password** text boxes.

   The password must be at least eight characters long and must contain characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters.

6 Click **Change** to change the password.

# Change the Keystore Passwords of the vSphere Replication Appliance

To increase security, you can change the passwords of the vSphere Replication appliance keystore. If you copy the keystores from the appliance to another machine, you must change the passwords before the copy operation.

The keystore passwords might be stored in an access restricted configuration file. vSphere Replication has the following keystores:

- `/opt/vmware/hms/security/hms-keystore.jks`, which contains the vSphere Replication appliance private key and certificate.
- `/opt/vmware/hms/security/hms-truststore.jks`, which contains additional CA certificates besides the ones that Java already trusts.

Procedure

1 To change the password for the `hms-keystore.jks` keystore, open the remote console of your vSphere Replication virtual machine and log in as root.

2 Obtain the current keystore password.

```
# /opt/vmware/hms/bin/hms-configtool -cmd list | grep keystore
```

   Example of the output `hms-keystore-password = old_password`

3 Change the keystore password.

```
 # /usr/java/default/bin/keytool -storepasswd -storepass old_password -new new_password
-keystore /opt/vmware/hms/security/hms-keystore.jks
```

4 Change the vSphere Replication appliance private key password.

The following command is a long, single command and must be run at once. There are breaks in the command for better visibility. Verify that the command returns a success message.

```
# /usr/java/default/bin/keytool -keypasswd -alias jetty -keypass
old_password -new new_password -storepass new_password -keystore
/opt/vmware/hms/security/hms-keystore.jks
```

5 Update the configuration with the new password.

```
/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property 'hms-keystore-
password=new_password'
```

6 Update the tomcat `server.xml` file with the new password.

```
sed -i 's/old_password/new_password/g' /var/opt/apache-tomcat/webapps/dr/WEB-INF/classes/
h5dr.properties
```

7 Reboot the appliance for the changes to take effect.

```
# reboot
```

8 Use a supported browser to log in to the VRMS Appliance Management Interface.

The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.

9 Click **Configure**, and click **Restart**.

### What to do next

If you want to change the truststore passwords of the vSphere Replication appliance, see Change the Truststore Passwords of the vSphere Replication Appliance.

# Change the Truststore Passwords of the vSphere Replication Appliance

To increase security, you can change the passwords of the vSphere Replication appliance truststore.

The truststore passwords might be stored in an access restricted configuration file.

### Procedure

1 To change the password for the `hms-truststore.jks` keystore, open the remote console of your vSphere Replication virtual machine and log in as root.

2 Obtain the current truststore password.

```
# /opt/vmware/hms/bin/hms-configtool -cmd list | grep truststore
```

Example of the output: `hms-truststore-password = old_password`

3 Change the truststore password.

The following command is a long, single command and must be run at once. There are breaks in the command for better visibility. Verify that the command returns a success message.

```
# /usr/java/default/bin/keytool -storepasswd -storepass
old_password -new new_password -keystore
/opt/vmware/hms/security/hms-truststore.jks
```

4 Update the configuration with the new password.

```
/opt/vmware/hms/bin/hms-configtool -cmd reconfig -property 'hms-truststore-
password=new_password'
```

5 Restart the vSphere Replication service.

```
# service hms restart
```

### What to do next

If you want to change the keystore passwords of the vSphere Replication appliance, see Change the Keystore Passwords of the vSphere Replication Appliance.

## Activate or Deactivate SSH Access to the vSphere Replication Appliance

You can use the VRMS Appliance Management Interface to edit the appliance SSH access settings.

You can activate or deactivate an SSH access to the appliance only for the **admin** account.

### Procedure

1 Log in to the VRMS Appliance Management Interface as admin.

2 Click the **Access** tab.

3 In the **SSH** pane, click **Enable** or **Disable**.

## Change the SSL Certificate of the vSphere Replication Appliance

You can change the initial vSphere Replication SSL certificate by generating a new self-signed certificate or uploading an SSL certificate signed by a trusted Certificate Authority.

vSphere Replication generates a standard SSL certificate when the appliance first boots and registers with vCenter Server. The vSphere Replication self-signed certificate expires after five years from the first boot of the appliance. When your certificate is due to expire in 30 days, you see a warning under **Issues** on the **Site Pair** tab of vSphere Replication. The default certificate policy uses trust by thumbprint.

You can change the SSL certificate, for example if your company's security policy requires that you use trust by validity and thumbprint or a certificate signed by a certification authority. You change the certificate by using the VRMS Appliance Management Interface of the vSphere Replication appliance. For information about the SSL certificates that vSphere Replication uses, see vSphere Replication Certificate Verification and Requirements When Using a Public Key Certificate with vSphere Replication.

See vSphere Replication Certificate Verification for details on how vSphere Replication handles certificates.

### Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

### Procedure

1. Use a supported browser to log in to the VRMS Appliance Management Interface.

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.
2. Enter the admin user name and password for the appliance.

   You configured the admin password during the OVF deployment of the vSphere Replication appliance.
3. Click **Certificates**.
4. (Optional) To enforce verification of a certificate validity, see How to Activate the Verification of Certificate Validity.
5. Click on **Change**.

| Menu item | Description |
|---|---|
| **Generate a self-signed certificate** | Use an automatically generated certificate.<br>a Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company.<br>b Accept the default FQDN and IP values.<br>**Note** Using a self-signed certificate is only recommended for non-production environments. |
| **Use a PKCS #12 certificate file** | Use a custom certificate.<br>a Click **Browse**, navigate to the certificate file, and click **Open**. The certificate file must contain exactly one certificate with exactly one private key matching the certificate.<br>b (Optional) Enter the optional private key encryption password. |
| **Use a CA-signed certificate generated from CSR** | Use a CA-signed certificate generated from a CSR.<br>a In the **Certificate file** row, click **Browse**, navigate to the certificate file, and click **Open**.<br>b (Optional) In the **CA chain** row, click **Browse**, navigate to the CA chain, and click **Open**. |

6 Click **Change**.

7 Restart the **vSphere Replication** appliance.

**Results**

You changed the SSL certificate and optionally changed the security policy to use trust by validity and certificates signed by a certificate authority.

**Note** If you change a certificate on one of the source or target sites, the connection status to this site changes to `Connection issue`. In the vSphere Web Client, you can check the list of target sites under **vSphere Replication** on the **Manage** tab, and reconnect the sites.

## How to Activate the Verification of Certificate Validity

Activate the verification of the certificate validity by activating vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority.

When you activate vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority, vSphere Replication refuses to communicate with a server with an invalid certificate. You cannot use a self-signed certificate if you activate vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority.

**Note** If you reconfigure vSphere Replication through the VRMS Appliance Management Interface after you activate the verification of certificate validity, the verification gets deactivated and you must activate it again.

**Procedure**

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-trust-mode=0`.

3 Restart the HMS Service.

## vSphere Replication Certificate Verification

vSphere Replication verifies the certificates of vCenter Server and remote vSphere Replication servers.

All communication between vCenter Server, the local vSphere Replication appliance, and the remote vSphere Replication appliance goes through a vCenter Server proxy at port 80. All SSL traffic is tunneled.

vSphere Replication can trust remote server certificates either by verifying the validity of the certificate and its thumbprint or by verifying the thumbprint only. The default is to verify by thumbprint only. You can activate the verification of the certificate validity. See How to Activate the Verification of Certificate Validity.

### Thumbprint Verification

vSphere Replication checks for a thumbprint match. vSphere Replication trusts remote server certificates if it can verify the thumbprints through secure vSphere platform channels or, in some rare cases, after the user confirms them. vSphere Replication only takes certificate thumbprints into account when verifying the certificates and does not check the certificate validity.

**Verification of Thumbprint and Certificate Validity**

vSphere Replication checks the thumbprint and checks that all server certificates are valid. If you enabled vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority, vSphere Replication refuses to communicate with a server with an invalid certificate. When verifying certificate validity, vSphere Replication checks expiration dates, subject names, and the certificate issuing authorities.

In both modes, vSphere Replication retrieves thumbprints from vCenter Server. vSphere Replication refuses to communicate with a server if the automatically determined thumbprint differs from the actual thumbprint that it detects while communicating with the respective server.

You can mix trust modes between vSphere Replication appliances at different sites. A pair of vSphere Replication appliances can work successfully even if you configure them to use different trust modes.

## Requirements When Using a Public Key Certificate with vSphere Replication

If you enforce a verification of certificate validity by enabling vSphere Replication to accept only SSL certificates signed by a trusted Certificate Authority, some fields of the certificate request must meet certain requirements.

vSphere Replication can only import and use certificates and private keys from a file in the PKCS#12 format. Sometimes these files have a `.pfx` extension.

- The certificate must be issued for the same server name as the value in the **Local Host** setting in the VRMS Appliance Management Interface. Setting the certificate subject name accordingly is sufficient, if you put a host name in the **Local Host** setting or if any of the Subject Alternative Name certificate fields of the certificate matches the **Local Host** setting.
- vSphere Replication checks the issue and expiration dates of the certificate against the current date, to ensure that the certificate is not expired.
- If you use your own certificate authority, for example one that you create and manage with the OpenSSL tools, you must add the fully qualified domain name or IP address to the OpenSSL configuration file.
  - If the fully qualified domain name of the appliance is `VR1.example.com`, add `subjectAltName = DNS: VR1.example.com` to the OpenSSL configuration file.
  - If you use the IP address of the appliance, add `subjectAltName = IP:` *`vr-appliance-ip-address`* to the OpenSSL configuration file.

- vSphere Replication requires a trust chain to a well-known root certificate authority. vSphere Replication trusts all the certificate authorities that the Java Virtual Machine trusts. Also, you can manually import additional trusted CA certificates in `/opt/vmware/hms/security/hms-truststore.jks` on the vSphere Replication appliance.
- vSphere Replication accepts MD5 and SHA1 and SHA256 signatures. It is a best practice to use SHA156 signatures.
- vSphere Replication does not accept RSA or DSA certificates with 512-bit keys. vSphere Replication requires at least 1024-bit keys. It is a best practice to use 2048-bit public keys.

# Generate and Download a Certificate Signing Request for the vSphere Replication Appliance

A certificate signing request (CSR) is an encrypted text file that contains specific information, such as organization name, common name, locality, and country. You send the CSR file to a certificate authority (CA) to apply for a digital identity certificate.

You generate a CSR and a matching private key. The private key remains on the vSphere Replication Appliance.

**Attention** Generating a new private key invalidates any existing CSR configuration.

### Procedure

1. Use a supported browser to log in to the VRMS Appliance Management Interface.

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.
2. Enter the admin user name and password for the appliance.

   You configured the admin password during the OVF deployment of the vSphere Replication appliance.
3. Click **Certificates**, and click **Generate CSR**.
4. Enter text values for your organization and organization unit, typically your company name, and the name of your group in the company.
5. Accept the default FQDN and IP values and click **Generate and download**.

### What to do next

To submit a certificate request to the CA in accordance with the CA enrollment process, use the contents of the CSR file.

The CA creates a server certificate based on the information in the CSR file, signs it with its private key, and sends you the certificate, which you can then import to the vSphere Replication Appliance.

# Configure vSphere Replication Network Settings

You can review your current network settings and change the address and proxy settings for vSphere Replication. If you want to match network configurations, these changes might be necessary.

**Note** vSphere Replication can be deployed with either IPv4 or IPv6 address. Mixing IP addresses, for example having a single appliance with an IPv4 and an IPv6 address, is not supported. To register as an extension, vSphere Replication relies on the `VirtualCenter.FQDN` property of the vCenter Server. When an IPv6 address is used for vSphere Replication, the `VirtualCenter.FQDN` property must be set to a fully qualified domain name that can be resolved to an IPv6 address or to a literal address. When operating with an IPv6 address, vSphere Replication requires that all components in the environment, such as vCenter Server and ESXi hosts are accessible using the IPv6 address.

### Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

### Procedure

1. Use a supported browser to log in to the VRMS Appliance Management Interface.

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.
2. Enter the admin user name and password for the appliance.

   You configured the admin password during the OVF deployment of the vSphere Replication appliance.
3. Click on **Networking**.
4. To configure your network settings, click **Edit**.
5. Configure the DNS settings in the **Hostname and DNS** pane.

| Menu Item | Description |
|---|---|
| **Obtain DNS settings automatically** | Obtains the DNS settings automatically from the network. |
| **Enter DNS settings manually** | Uses the DNS address settings that you set manually. If you select this option, you must provide the IP addresses for a primary and a secondary DNS server. |

6 In the **eth0** pane, select the IPv4 or theIPv6 protocol type and configure the IP address settings.

- Configure the IPv4 address settings.

| Option | Description |
|---|---|
| Obtain IPv4 settings automatically | Obtains the IP address for the appliance from the network. |
| Enter IPv4 settings manually | Uses an IPv4 address that you set manually.<br>1 Enter the IPv4 address<br>2 Enter subnet prefix length.<br>3 Enter the default IPv4 gateway. |

- Configure the IPv6 address settings.

| Option | Description |
|---|---|
| Obtain IPv6 settings automatically using DHCP | Assigns IPv6 addresses to the appliance from the network by using DHCP.<br>**Note** To apply this setting, you must restart the vSphere Replication Appliance. |
| Obtain IPv6 settings automatically using router advertisement | Assigns IPv6 addresses to the appliance from the network by using router advertisement. |
| Use static IPv6 addresses | Uses static IPv6 addresses that you set up manually.<br>1 Enter the IPv6 address and the subnet prefix length in the address box.<br>2 To enter additional IPv6 addresses, click **Add**.<br>3 Enter the default IPv6 gateway. |

7 Click **Save**.

### What to do next

If you modified the IP address of the vSphere Replication appliance, you must update and verify certain settings:

- Update the general vSphere Replication settings. See Reconfigure General vSphere Replication Settings.
- Verify that the **IP Address for Incoming Storage Traffic** value is updated with the new IP address.
- Verify that the appliance certificate is valid for the new IP address. You must verify the certificate if you have activated the verification of the certificate validity.

# Configure the Time Zone and Time Synchronization Settings for the vSphere Replication Appliance

When you deploy the vSphere Replication, you either use the time settings of the ESXi host on which the appliance is running, or you configure time synchronization with an NTP server. If the time settings in your network change, you can edit the time zone and time synchronization settings of the appliance.

### Procedure

1 Log in to the VRMS Appliance Management Interface as admin.

2 Click the **Time** tab.

3 Configure vSphere Replication Appliance time zone settings.

   a On the **Time zone** pane, click **Edit**.

   b From the **Time zone** drop-down menu, select a location or a time zone and click **Save**.

4 On the **Time synchronization** pane, click **Edit**.

5 Configure the time synchronization settings and click **Save**.

| Mode | Description |
|---|---|
| **Disabled** | No time synchronization. Uses the system time zone settings. |
| **Host** | Uses VMware Tools to synchronize the time of the appliance with the time of the ESXi host. |
| **NTP** | Enables NTP synchronization. You must enter the IP address or FQDN of one or more NTP servers. |

# Start, Stop, and Restart vSphere Replication Appliance Services

If changes in your environment require the restart of certain services, you can use the VRMS Appliance Management Interface to view the state of the services and to start, stop, and restart them.

You can start, stop, and restart the vSphere Replication management server service, the vSphere Replication server service, the embedded database service, and the `tomcat` server service.

### Procedure

1 Log in to the VRMS Appliance Management Interface as admin.

2 In the VRMS Appliance Management Interface, click **Services**.

   The Services page displays a table of the installed services that can be sorted by name, startup type, and state.

3 Select a service and click **Start**, **Stop**, or **Restart**.

Restarting some services might lead to functionality becoming temporarily unavailable.

4 Restart the appliance for the changes to take effect.

# Forward vSphere Replication Appliance Log Files to Remote Syslog Server

You can forward the vSphere Replication Appliance log files to a remote syslog server to conduct an analysis of your logs.

Procedure

1 Log in to the VRMS Appliance Management Interface as admin.

2 In the VRMS Appliance Management Interface, select **Syslog Forwarding**.

3 Click **New**, and enter the server address of the destination host in the **New Syslog Forwarding** pane.

4 From the **Protocol** drop-down menu, select the protocol to use.

5 In the **Port** text box, enter the port number to use with the destination host.

The default port number is **514**.

6 Click **OK**.

7 Verify that the remote syslog server is receiving messages.

8 In the **Syslog Forwarding** section, click **Send Test Message**.

9 Verify that the test message is received on the remote syslog server.

# Enable the SHA-1 Hashing Function

You can install certificates, signed with the SHA-1 hashing function in case your environment requires it.

By default, the vSphere Replication server rejects installation of new certificates, which are signed with the SHA-1 hashing function. To install a certificate, signed with the SHA-1 hashing function, you must enable it in the vSphere Replication appliance.

Procedure

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-allow-legacy-hash-algo>` value to **`true`**.

4 Restart the vSphere Replication service.

# vSphere Replication Roles and Permissions

10

You can use any predefined roles or clone an existing role, and add or remove privileges from it based on your needs.

Read the following topics next:

- vSphere Replication Roles Reference
- Assign VRM Replication Viewer Role
- Assign VRM Virtual Machine Replication User Role
- Assign VRM Virtual Machine Recovery User Role and Perform a Recovery Operation
- Clone an Existing VRM Administrator Role and Modify Privileges

## vSphere Replication Roles Reference

vSphere Replication includes a set of roles. Each role includes a set of privileges, which enable users with those roles to complete different actions.

For information about how to assign roles, see *Assigning Roles in the vSphere Web Client* in *vSphere Security*.

**Note** When assigning permissions with no propagation, make sure that you have at least Read-only permission on all parent objects.

Table 10-1. vSphere Replication Roles

| Role | Actions that this Role Permits | Privileges that this Role Includes | Objects in vCenter Server Inventory that this Role Can Access |
|---|---|---|---|
| VRM replication viewer | ■ View replications.<br>■ Cannot change replication parameters. | **VRM remote.View VR**<br>**VRM remote.View VRM**<br>**VRM datastore mapper.View**<br>**VRM replication.View replications**<br>**Virtual machine.vSphere Replication.Monitor replication** | vCenter Server root folder with propagation, at the source site (outgoing replications) and the target site (incoming replications).<br>Alternatively, vCenter Server root folder without propagation on both sites and virtual machine without propagation on the source site. |
| VRM virtual machine replication user | ■ View replications.<br>■ Manage datastores.<br>■ Configure and unconfigure replications.<br>■ Manage and monitor replications.<br>■ View defined storage capabilities and storage profiles.<br>Requires a corresponding user with the same role on the target site and also vSphere Replication target datastore user role on the target data center, or datastore folder or each target datastore. | **Datastore.Browse Datastore**<br>**VRM remote.View VR**<br>**VRM remote.View VRM**<br>**VRM replication.View replications**<br>**VRM datastore mapper.Manage**<br>**VRM datastore mapper.View**<br>**Host.vSphere Replication.Manage replication**<br>**Virtual machine.vSphere Replication.Configure replication**<br>**Virtual machine.vSphere Replication.Manage replication**<br>**Virtual machine.vSphere Replication.Monitor replication**<br>**Profile-driven storage .Profile-driven storage view** | vCenter Server root folder with propagation on both sites.<br>Alternatively, vCenter Server root folder without propagation on both sites, virtual machine without propagation on the source site, source datastores without propagation on the source site. |

Table 10-1. vSphere Replication Roles (continued)

| Role | Actions that this Role Permits | Privileges that this Role Includes | Objects in vCenter Server Inventory that this Role Can Access |
|---|---|---|---|
| VRM administrator | Incorporates all vSphere Replication privileges. | **VRM remote.Manage VR**<br>**VRM remote.View VR**<br>**VRM remote.Manage VRM**<br>**VRM remote.View VRM**<br>**VRM datastore mapper.Manage**<br>**VRM datastore mapper.View**<br>**VRM diagnostics .Manage**<br>**VRM replication.View replications**<br>**VRM session .Terminate**<br>**Datastore.Browse datastore**<br>**Datastore.Configure datastore**<br>**Datastore.Low level file operations**<br>**Host.vSphere Replication.Manage replication**<br>**Resource.Assign virtual machine to resource pool**<br>**Virtual machine.Configuration.Add existing disk**<br>**Virtual machine.Configuration.Add or remove device**<br>**Virtual machine.Interaction.Power On**<br>**Virtual machine.Interaction.Device connection**<br>**Virtual machine.Inventory.Register**<br>**Virtual machine.Inventory.Unregister**<br>**Virtual machine.vSphere Replication.Configure replication**<br>**Virtual machine.vSphere Replication.Manage replication**<br>**Virtual machine.vSphere Replication.Monitor replication**<br>**Virtual machine.Snapshot management.Remove snapshot**<br>**Profile-driven storage .Profile-driven storage view** | vCenter Server root folder with propagation on both sites.<br>Alternatively, vCenter Server root folder without propagation on both sites, virtual machine without propagation on the source site, target datastore, target virtual machine folder with propagation on the target site, target host or cluster with propagation on the target site. |
| VRM diagnostics | Generate, retrieve, and delete log bundles. | **VRM remote.View VR**<br>**VRM remote.View VRM**<br>**VRM replication .View replication**<br>**VRM diagnostics .Manage** | vCenter Server root folder on both sites. |

Table 10-1. vSphere Replication Roles (continued)

| Role | Actions that this Role Permits | Privileges that this Role Includes | Objects in vCenter Server Inventory that this Role Can Access |
|---|---|---|---|
| VRM target datastore user | Configure and reconfigure replications.<br>Used on the target site in on the VRM virtual machine replication user role on both sites. | **Datastore.Browse datastore**<br>**Datastore.Low level file operations** | Datastore objects on the target site, or datastore folder with propagation at the target site, or target data center with propagation. |
| VRM virtual machine recovery user | Recover virtual machines. | **Datastore.Browse datastore**<br>**Datastore.Low level file operations**<br>**Host.vSphere Replication.Manage replication**<br>**Virtual machine.Configuration.Add existing disk**<br>**Virtual machine.Configuration.Add or remove device**<br>**Virtual machine.Interaction.Power On**<br>**Virtual machine.Interaction.Device connection**<br>**Virtual machine.Inventory.Register**<br>**Virtual machine.Inventory.Unregister**<br>**Virtual machine.Snapshot management. Remove snapshot**<br>**Resource.Assign virtual machine to resource pool** | Secondary vCenter Server root folder with propagation.<br>Alternatively, secondary vCenter Server root folder without propagation, target datastore without propagation, target virtual machine folder with propagation, target host, or cluster with propagation. |

# Assign VRM Replication Viewer Role

Assign the VRM Replication View role to a user so that they can view replication sites and the replications configured between them, but cannot perform modifications.

### Prerequisites

- Verify that you have two sites connected and replication configured between them.
- Verify that you have another user account for each site.

### Procedure

1. Log in as Administrator on the source site.
2. Select **vCenter > Permissions** and assign the **VRM replication viewer** role with the propagate option to this user.
3. Assign the same privilege on the target replication site.

4 Log in as the user with the assigned VRM replication viewer role.

### Results

The user with the VRM replication viewer role cannot perform modifications on the configured replication, nor on the replication sites. The following error message appears when this user tries to run an operation: `Permission to perform this operation was denied`.

## Assign VRM Virtual Machine Replication User Role

Create a vSphere Replication user who can only configure a replication between sites and use a specific datastore on the target site.

### Prerequisites

- Verify that two sites are connected.
- Verify that you have another user account for each site.

### Procedure

1 Log in as the Administrator user on the source site.

2 Select **vCenter > Permissions** and assign to this user the **VRM virtual machine replication user** role with the propagate option.

3 Assign the same privilege on the target replication site.

4 On the target site, select the datastore to store your replica files, and select **Manage > Permissions**.

5 Edit the assigned permission and assign the **VRM target datastore user** role.

6 Log in as that user on the source site, select the virtual machine, and click **Configure Replication** to start the configuration wizard.

7 Select the target site and enter the same user credentials.

8 Accept the default selections until **Target Location**.

9 For the target location, select the datastore to which you granted permission.

## Assign VRM Virtual Machine Recovery User Role and Perform a Recovery Operation

You assign specific permissions to a vSphere Replication user, so that they can perform only recovery operations.

### Prerequisites

- Verify that you have two sites connected and replication configured between them.

- Verify that you have another user account for the target site apart from the Administrator user.

Procedure

1. Log in as the Administrator user on the target site.
2. Select **vCenter > Permissions** and assign to a different user account the **VRM virtual machine recovery user** role with the propagate option.
3. Log in as that user on the target site.
4. On the home page, click **Site Recovery** and click **Open Site Recovery**.
5. On the Site Recovery home page, select a site pair and click **View Details**.
6. Click the **Replications** tab and select **Incoming**.
7. Select a replication from the list.
8. To finish the recovery, click the **Recover** icon and follow the prompts.

# Clone an Existing VRM Administrator Role and Modify Privileges

Create a vSphere Replication user who can modify the replication infrastructure, but cannot register additional vSphere Replication servers.

Prerequisites

- Verify that you have a replication site.
- Verify that you have another user account to which you can assign the modified privileges.

Procedure

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Administration** and click **Roles.**
3. Select the **VRM Administrator** role and click the **Clone role action** icon.
4. In the cloned role, deselect the **VRM Remote > VR Server > Manage VR Server** privilege.
5. Navigate to the vCenter Server instance.
6. On the **Permissions** tab, click the **Add permission** icon.
7. Select the user that must have the privileges defined by the selected role.
8. Select the cloned **VRM Administrator** role from the **Assigned Role** drop-down menu.
9. Select the **Propagate to children** check box.

### Results

Trying to register a vSphere Replication server results in the error message `Permission to perform this operation was denied.`

# Replicating Virtual Machines

11

You can replicate virtual machines from a source site to a target site with vSphere Replication.

To replicate a virtual machine using vSphere Replication, you must deploy the vSphere Replication appliance at the source and target sites. A vSphere Replication infrastructure requires one vSphere Replication appliance at each site.

If you want to configure replications, the source and target sites must be connected. You cannot perform replications if one of the sites is in the `Not Connected` state. See Understanding the vSphere Replication Site Connection States.

You can configure replications for powered-off virtual machines, but the data synchronization begins when the virtual machine is powered on. While the source virtual machine is powered off, the replication appears in the `Not active` status.

You can set a recovery point objective (RPO) to a certain time interval depending on your data protection needs. vSphere Replication applies all changes made to virtual machines configured for a replication at the source site to their replicas at the target site. This process reoccurs periodically to ensure that the replicas at the target site are not older than the RPO interval that you set. See Recovery Point Objective.

vSphere Replication does not support the recovery of multiple virtual machines from the same workflow. Each recovery workflow is for an individual virtual machine.

You cannot use vSphere Replication to replicate virtual machine templates.

Read the following topics next:

- Recovery Point Objective
- How the Retention Policy Works
- Replicating a Virtual Machine and Enabling Multiple Point in Time Instances
- Using vSphere Replication with vSAN Storage
- Using vSphere Replication with vSphere Storage DRS
- How vSphere Replication Synchronizes Data Between vCenter Server Sites During Initial Configuration
- How vSphere Replication Synchronizes Data Between the Source and the Target Sites During Incremental Sync

- Replicating Virtual Machines Using Replication Seeds
- Replicating a Virtual Machine in a Single vCenter Server Instance
- Replicating Encrypted Virtual Machines
- Network Encryption of Replication Traffic
- How vSphere Replication Works When Using Guest OS Trim/Unmap Commands
- Best Practices for Using and Configuring vSphere Replication
- Configure a Replication
- Move a Replication to a New vSphere Replication Server
- Stop Replicating a Virtual Machine
- Reconfiguring Replications
- Enable VM Encryption for an Already Replicated VM
- Stopping a Virtual Machine Offline Synchronization Task

# Recovery Point Objective

When you set a Recovery Point Objective (RPO) value during replication configuration, you determine the maximum data loss that you can tolerate.

## How the Recovery Point Objective Affects Replication Scheduling

The RPO value affects replication scheduling, but vSphere Replication does not adhere to a strict replication schedule. For example, when you set the RPO to 15 minutes, you instruct vSphere Replication that you can tolerate losing the data for up to 15 minutes. This does not mean that data is replicated every 15 minutes.

If you set an RPO of x minutes, and the RPO is not violated, the latest available replication instance can never reflect a state that is older than x minutes. A replication instance reflects the state of a virtual machine at the time the synchronization starts.

You set the RPO to 15 minutes. If the synchronization starts at 12:00 and it takes five minutes to transfer to the target site, the instance becomes available on the target site at 12:05, but it reflects the state of the virtual machine at 12:00. The next synchronization can start no later than 12:10. This replication instance is then available at 12:15 when the first replication instance that started at 12:00 expires.

If you set the RPO to 15 minutes and the replication takes 7.5 minutes to transfer an instance, vSphere Replication transfers an instance all the time. If the replication takes more than 7.5 minutes, the replication encounters periodic RPO violations.

If the replication starts at 12:00 and takes 10 minutes to transfer an instance, the replication finishes at 12:10. You can start another replication immediately, but it finishes at 12:20. During the time interval 12:15-12:20, an RPO violation occurs because the latest available instance started at 12:00 and is too old.

The replication scheduler tries to satisfy these constraints by overlapping replications to optimize bandwidth use and might start replications for some virtual machines earlier than expected.

To determine the replication transfer time, the replication scheduler uses the duration of the last few instances to estimate the next one.

### Recovery Point Objective Violations After the Initial Full Synchronization

The initial full synchronization of the virtual machine disks is a time-consuming process. As soon as it is complete, vSphere Replication begins to replicate the changed in the meantime disk blocks (first incremental sync), which might require longer transfer time than the set RPO time.

After the first incremental sync, vSphere Replication detects a staleness of the generated replica instance and starts reporting RPO violations. Since the replication is behind the RPO schedule, the second incremental sync begins as soon as the first one completes.

This process of immediate subsequent incremental syncs continues until vSphere Replication creates a replica instance that satisfies the RPO schedule, and does not report an RPO violation. The replication status becomes OK.

### How the 5 Minute Recovery Point Objective Works

If the target and the source sites use VMFS 6.0, VMFS 5.x, NFS 4.1, NFS 3, vVol, or vSAN 6.2 Update 3 storage and later, you can use the 5 minute RPO.

vSphere Replication displays the 5 minute RPO setting when the target and the source site use VMFS 6.0, VMFS 5.x, NFS 4.1, NFS 3, vVol, or vSAN 6.2 Update 3 storage and later.

If you are using different datastore types between the source and the target site, you can use the 5 minute RPO setting .

The 5 minute RPO requires the source host to be ESXi 6.5 or later.

The 5 minute RPO can be applied to a maximum of 100 VMs on VMFS 6.0, VMFS 5.x, NFS 4.1, NFS 3, and vSAN 6.2 Update 3 storage and later. The maximum for vVol datastore is 50 VMs.

**Note** RPO lower than 15 minutes is not supported when you select the OS quiescing option.

## How the Retention Policy Works

When you configure a replication, you can enable the retention of up to 24 virtual machine replica instances from Multiple Points in Time (MPIT).

After you recover a replicated virtual machine, the retained replicas appear as snapshots of the virtual machine in the vSphere Web Client. The list of snapshots includes the retained instances according to the retention policy that you set, and the latest instance. You can use the snapshots to revert to an earlier state of the recovered virtual machine.

You can configure the retention of three instances per day for the last five days. The list of snapshots contains 15 snapshots and the latest saved instance of the virtual machine, or a total of 16 snapshots.

Administrators cannot configure the precise time when replica instances are created, because the retention policy is not directly related to the replication schedule and RPO. As a consequence, replications with the same retention policy might not result in replicas retained at the same time instants.

## RPO Without Retention Policy

By default, vSphere Replication is configured to a one-hour RPO, so the latest available replica instance can never reflect a state of the virtual machine that is older than one hour. You can adjust the RPO interval when you configure or reconfigure a replication.

When the age of the latest replication instance approaches the RPO interval, vSphere Replication starts a sync operation to create an instance on the target site. The replication instance reflects the state of the virtual machine at the time the synchronization starts. If no retention policy is configured, when the new instance is created, the previous instance expires and the vSphere Replication Server deletes it.

## How RPO and the Retention Policy Combine

To save some of the replica instances that are created during RPO synchronizations, you can configure vSphere Replication to keep up to 24 instances per replication. The exact instances that vSphere Replication keeps are determined by applying a specific algorithm. Using this algorithm, the vSphere Replication Server tries to match each instance to a slot of the retention policy. Instances that do not match any slot expire and are deleted. If a slot contains more than one instance, the instances that do not match the retention criteria are also deleted. vSphere Replication always keeps the latest created instance and it is not included when determining the number of instances to keep.

When the age of the latest instance approaches the RPO interval, vSphere Replication starts creating a replica instance. The start time of the sync operation is the time of the new instance. When the sync operation completes, vSphere Replication assesses the existing replica instances to determine which ones to keep:

1 The granularity of the retention policy is determined based on the replication settings. For example, if you configured vSphere Replication to keep three instances for the last one day, it means that you want to keep three replica instances that are relatively evenly distributed over 24 hours. This equals approximately one instance in an eight-hour interval, or the granularity of this retention policy is 8 hours.

2 The time of the last saved instance is rounded down to the nearest slot time. If the granularity is eight hours, the slot times are 0:00, 8:00, and 16:00.

3 The instances that are between the nearest slot time and the last saved instance are traversed. Let us assume that the time of the last saved instance is 10:55. Following our example, the nearest slot time is 8:00 o'clock. Let us also assume that the RPO is 1 hour, and each sync operation takes 5 minutes to complete. Between 8:00 o'clock and 10:55, the slot contains an 8:55 instance, and a 9:55 instance.

4 The earliest instance that is newer than the nearest slot time is saved, and the rest of the instances in this slot are deleted, except for the latest created instance that vSphere Replication always keeps. Following our example, the 8:55 instance is saved, and the 9:55 instance is deleted. The 10:55 instance is the latest created instance, so it is also saved.

5 The granularity of the retention policy decrements the slot time and a check is performed for the earliest instance between the beginning of the current slot and the beginning of the previous slot. If the slot contains expiring instances, they are deleted.

6 The number of slots that contain saved instances is analyzed. If the number of slots with saved instances is higher than the number of slots determined by the retention policy, the oldest saved instance expires and is deleted. The last saved instance is not included in this count. In our example, if we had an instance saved for the interval 8:00 - 16:00 o'clock of the previous day, that instance would be deleted.

The number of replication instances that vSphere Replication keeps depends on the configured retention policy, but also requires that the RPO period is short enough for these instances to be created. Because vSphere Replication does not verify whether the RPO settings creates enough instances to keep, and does not display a warning message if the instances are not enough, you must ensure that you set vSphere Replication to create the instances that you want to keep. For example, if you set vSphere Replication to keep six replication instances per day, the RPO period must not exceed four hours, so that vSphere Replication can create six instances in 24 hours.

## Replicating a Virtual Machine and Enabling Multiple Point in Time Instances

You can recover virtual machines at specific points in time (PIT), such as the last known consistent state.

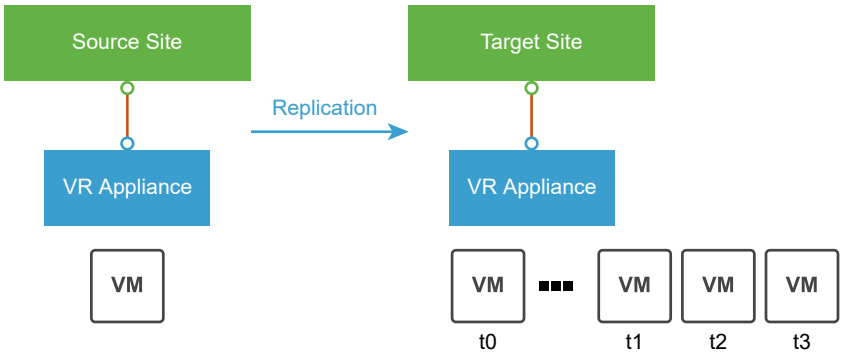
When you configure a replication, you can enable multiple point in time (MPIT) instances in the recovery settings. vSphere Replication keeps several snapshot instances of the virtual machine on the target site, based on the retention policy that you specify. vSphere Replication supports a maximum of 24 snapshot instances. After you recover a virtual machine, you can revert it to a specific snapshot.

During the replication process, vSphere Replication replicates all aspects of the virtual machine to the target site, including any potential viruses and corrupted applications. If a virtual machine has a virus or a corruption and you have configured vSphere Replication to keep PIT snapshots, you can recover the virtual machine and then revert it to a snapshot in its uncorrupted state.

You can also use the PIT instances to recover the last known good state of a database.

**Note** vSphere Replication does not replicate virtual machine snapshots.

Figure 11-1. Recovering a Virtual Machine at Points in Time




# Using vSphere Replication with vSAN Storage

When configuring replications, you can use VMware vSAN datastores as target datastores. Follow the guidelines when using vSphere Replication with vSAN storage.

User-friendly names of directories on vSAN datastores might change and cause errors during replication or recovery operations. Because of this reason, vSphere Replication automatically replaces the user-friendly name of a directory with its UUID, which is constant. As a result you may see the UUID displayed in the Site Recovery user interface instead of a human-readable name.

## Limits of Using vSphere Replication with vSAN Storage

Because of load and I/O latency, vSAN storage has limits for the numbers of hosts that you can include in a vSAN cluster and the number of VMs that you can run on each host. See the Limits section in the *VMware vSAN Design Guide* at https://core.vmware.com/resource/vmware-vsan-design-guide.

Using vSphere Replication adds to the load on the storage. Every virtual machine generates regular read and write operations. Configuring replications on those virtual machines adds another read operation to the regular read and write operations, which increases the I/O latency on the storage. The precise number of virtual machines that you can replicate to vSAN storage by using vSphere Replication depends on your infrastructure. If you notice slower response times when you configure replications for virtual machines in vSAN storage, monitor the I/O latency of the vSAN infrastructure. Potentially, reduce the number of virtual machines that you replicate in the vSAN datastore.

## Retaining Point-in-Time Snapshots When Using vSAN Storage

vSAN storage stores virtual machine disk files as a set of objects and components. Each disk object in vSAN storage has mirror and witness objects. In the default vSAN storage policy, a disk object has two mirrors and one witness. The number of mirror components is determined by the size of the virtual machine disk and the number of failures to tolerate that you set in your vSAN storage policy. A mirror object is divided into components of a maximum size of 256 GB each.

- If a virtual machine has one 256 GB disk and you use the default vSAN storage policy, the disk object has two mirror components of 256 GB each and one witness - a total of three components.
- If a virtual machine has one 512 GB disk and you use the default vSAN storage policy, the disk object has four mirror components of 256 GB each and one witness - a total of five components.

See the *VMware vSAN Design Guide* at https://core.vmware.com/resource/vmware-vsan-design-guide for explanations of objects, components, mirrors, witnesses, and vSAN storage policies.

If you enable multiple point-in-time (MPIT) snapshots, you must make allowances for the additional components that each snapshot creates in the vSAN storage. You must consider the number of disks per virtual machine, the size of the disks, the number of PIT snapshots to retain, and the number of failures to tolerate. When retaining PIT snapshots and using vSAN storage, you must calculate the number of extra components that you require for each virtual machine:

*Number of disks* x *number of PIT snapshots* x *number of mirror and witness components*

Examples of using this formula demonstrate that retaining PIT snapshots rapidly increases the number of components in the vSAN storage for every virtual machine that you configure for vSphere Replication:

- You have a virtual machine with two 256 GB disks for which you retain 10 MPIT snapshots, and you set the default vSAN storage policy:
  - 2 (number of disks) x 10 (number of PIT snapshots) x 3 (two mirror components + 1 witness) = 60 components for this one virtual machine.
- You have a virtual machine with two 512 GB disks for which you retain 10 PIT snapshots, and you set the default vSAN storage policy:
  - 2 (number of disks) x 10 (number of PIT snapshots) x 5 (four mirror components of 256 GB each + 1 witness) = 100 components for this one virtual machine.

The number of PIT snapshots that you retain can increase I/O latency on the vSAN storage.

# Using vSphere Replication with vSphere Storage DRS

vSphere Replication can operate with target sites that have VMware vSphere® Storage DRS™ enabled.

Storage DRS (SDRS) can detect the data that vSphere Replication copies on the target site and can move replications without affecting the replication process. SDRS on the source site does not impact the replication process.

If there is SDRS enabled on the target site and the target datastore is included in a datastore cluster with SDRS enabled, SDRS communicates with vSphere Replication and does not automatically move the replica files from one datastore to another. vSphere Replication triggers a reconfigure replication that moves the replication data to the new datastore in the cluster. Initially, the replica files might be on one datastore and then they might split to several datastores or to a different datastore.

vSphere Replication manages all SDRS operations.

# How vSphere Replication Synchronizes Data Between vCenter Server Sites During Initial Configuration

When you configure a virtual machine for replication, vSphere Replication starts an initial configuration task. During this task a replica virtual machine is created on the target site, and data synchronization occurs between the source and the target vCenter Server sites.

The speed of data synchronization depends on the availability of information about the block allocation of the VMDK files. vSphere Replication uses this information to find empty regions of the disks and accelerate the sync operations by skipping these regions. The speed of data synchronization also depends on the site for which block allocation information is available.

- If the allocation information is available at both sites, data synchronization occurs at the highest possible speed.
- If the allocation information is available only at the source or the target site, vSphere Replication skips the empty regions on the VMDK disks at that site, but processes the entire disk at the site where the allocation information is not available. Therefore, data synchronization is slower.
- If the allocation information is not available at either site, data synchronization is done by comparing all blocks between the source site and the target site, even if many of the blocks are not allocated on the disk by the guest OS. This is the slowest method for data synchronization.

**Note** The availability of block allocation information has little effect on the speed of data synchronization for VMDK disks that are almost full.

## Factors That Affect the Availability of Block Allocation Information

The availability of allocation information and the degree to which vSphere Replication can use it to accelerate data synchronization depend on:

- The ESXi versions.
- The vSphere Replication Management server versions.

- The type of VMDK disks, and the type of volumes on which the disks reside.

### Version Support

Table 11-1. Product Versions at the Source and the Target Site

| Source Site | | Target Site | | Result | |
|---|---|---|---|---|---|
| ESXi Host | vSphere Replication Management Server | ESXi Host | vSphere Replication Management Server | | |
| 6.x or later | 6.x or later | 6.x or later | 6.x or later | The acceleration of initial synchronization is supported. | |
| 6.x or later | 6.x or later | Earlier than 6.x | Earlier than 6.x | The allocation information is available only on the source site. | |
| 6.x or later | 6.x or later | Earlier than 6.x | 6.x or later | | |
| 6.x or later | 6.x or later | 6.x or later | Earlier than 6.x | | |

### The Type of the Datastore

Disks on VMFS or vSAN datastores provide full allocation information.

NFS datastores cannot provide allocation information for the disks that are located on them.

Replication disks on the source and the target site can be on different datastore types. The acceleration of the initial synchronization depends on whether both sites can provide allocation information, or only one site. If none of the sites can provide allocation information, no acceleration occurs.

### The Type of Virtual Disk

Lazy zeroed thick disks, thin disks, and vSAN sparse disks, Space-Efficient sparse disks, and VMDK sparse snapshots provide allocation information.

Eager zeroed thick disks do not provide allocation information.

Virtual disks that are based on vVols are native to the volume. vSphere Replication 8.4.x can get allocation information from them only when they are on the target site. For this reason, the acceleration of the initial synchronization is partial.

## How vSphere Replication Synchronizes Data Between the Source and the Target Sites During Incremental Sync

After the initial full synchronization is complete, vSphere Replication starts to track the changed blocks on the source site and periodically transfers them to the target site. This process is called an incremental sync. As a result of the incremental sync completion, vSphere Replication creates a new replica instance on the target site. The following removal of the old instance is a time-consuming process.

During the old instance removal process, vSphere Replication might start transferring new changed blocks to the target site. This activity further increases the storage consumption on the target site. When the old instance removal is complete, vSphere Replication frees the storage space occupied by the old instance. If the source disk has a high data change rate, while the old replica instance is being removed, the storage consumption on the target site might temporarily exceed several times the size of the source disk.

**Note** If due to the temporary spikes in the storage consumption on the target site the space is not enough, you might observe "Insufficient storage space" errors in the Site Recovery user interface. vSphere Replication might start reporting recovery point objective (RPO) violations.

# Replicating Virtual Machines Using Replication Seeds

Reduce the amount of network traffic and time during the initial full synchronization. You can copy the virtual disk files in the target datastore and using them as replication seeds.

When you configure a replication for the first time, vSphere Replication performs an initial full synchronization of the virtual machine's disk. This operation is network and time intensive.

vSphere Replication compares the differences on the source and target site, and replicates only the changed blocks.

When, during replication configuration, you select a target datastore for the virtual machine or a specific disk, vSphere Replication looks for disks with the same filename in the target datastore. If a file with the same name exists, a warning appears in the wizard. You can review and configure the replication seeds or choose not to use any replication seeds. If you choose not to use the discovered seeds, then replica files are placed in a new directory with a unique name. If you choose to configure seeds by selecting the **Select seeds** check box, then a new page appears in the wizard where you can configure seeds for each disk on each virtual machine.

**Note** If you plan to copy files from the source to the target datastore, the source virtual machine must be powered off before downloading the VMDK files that will be used as seeds for the replication.

## Using vSphere CLI for Storage Operations

To create a copy of a virtual disk, you can use the vSphere CLI to manage VMFS volumes, `vmkfstools`.

To prevent performance and data management issues on ESXi hosts, avoid using standard Linux commands for storage operations.

For more information, see https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.storage.doc/GUID-01D3CF47-A84A-4988-8103-A0487D6441AA.html.

# Replicating a Virtual Machine in a Single vCenter Server Instance

You can use vSphere Replication to replicate a virtual machine in a single vCenter Server even if the vCenter Server instance has only one host in its inventory.

When you configure a replication in a single vCenter Server instance, you can select the source site as the target site for the replication. You then configure a replication in the same way as for an infrastructure with a source and a target site. For example, you can replicate a virtual machine to a different datastore attached to the same host or another host. vSphere Replication prevents you from using the source or replicated virtual machine's VMDK files as the target of the replication.

The virtual machine name must be unique and in the same folder in the vCenter Server inventory. In the recovery wizard, vSphere Replication does not allow you to select a folder if there is already a virtual machine with the same name registered to it. During recovery if there is a virtual machine with the same name, you might see an error message. See Error Recovering Virtual Machine in a Single vCenter Server Instance for more information.

# Replicating Encrypted Virtual Machines

You can improve security and protection of your data by replicating encrypted virtual machines.

**Warning** You cannot replicate encrypted virtual machines if you are running vSphere 7.0 Update 2. vSphere Replication 8.4 does not support vSphere 7.0 Update 2 if virtual machine encryption is switched on.

You can replicate virtual machines if you are running vSphere 6.7 Update 1 or later. Ensure that you either use a common Key Management Server (KMS) or that the Key Management Server clusters at both sites use common encryption keys. Ensure that the KMS server is registered with the same name both at the source and target sites. For information about how to set up a Key Management Server cluster, see the *VMware vSphere ESXi and vCenter Server 6.7 documentation*.

An encrypted virtual machine can have both encrypted and unencrypted disks and you must follow different policies for each type.

When you specify the VM Storage Policy for target disks in a replication, you must set a storage policy with VM Encryption enabled at the target if the source disks are encrypted. For unencrypted source disks, you must set a storage policy without VM Encryption enabled at the target.

If you use replication seeds, target disks for encrypted source disks must be encrypted and target disks for unencrypted source disks must be unencrypted. Replica disks can have different encryption keys from the source disks.

If you do not use seed disks, replica disks are encrypted with the same encryption key as the source VM disks.

When you configure a replication of an encrypted VM, encryption of the transferred data is automatically switched on to enhance data security and you cannot switch it off.

For more information on VM encryption, see Virtual Machine Encryption in the *vSphere Security* documentation.

For information about enabling virtual machine encryption for an already replicated VM, see Enable VM Encryption for an Already Replicated VM.

## vSphere Native Key Provider

VMware vSphere® Native Key Provider™ enables encryption-related functionality without requiring an external key server (KMS). Initially, vCenter Server is not configured with a vSphere Native Key Provider. You must manually configure a vSphere Native Key Provider. See Configuring and Managing vSphere Native Key Provider in the *VMware vSphere Product Documentation*.

Requirements for using vSphere Native Key Provider for encrypting virtual machines and virtual disks:

- You need vSphere 7.0 Update 2 or later.
- You must purchase the vSphere Enterprise+ edition.

You must configure a vSphere Native Key Provider on both the local and remote sites. The vSphere Native Key Provider ID of the encrypted VM on the local site must match the vSphere Native Key Provider ID on the remote site.

To use encryption with a vSphere Native Key Provider for replicated virtual machines, the replica disks must be located on datastores, which are accessible through at least one host, which is a part of a vCenter cluster.

For more information, see *Configuring and Managing vSphere Native Key Provider* in the VMware vSphere 7.0 Product Documentation.

# Network Encryption of Replication Traffic

You can activate the network encryption of the replication traffic data for new and existing replications to enhance the security of data transfer.

You can activate encryption of replication traffic flows from the source ESXi host to the datastore at the target site.

The vSphere Replication appliance automatically installs an encryption agent on the source ESXi hosts in vSphere environments of version 6.0 or later.

The encrypted replication traffic uses mutual certificate-based authentication between the source ESXi host and target site vSphere Replication server.

When configuring or reconfiguring a replication, the vSphere Replication Management Server (VRMS) updates the source virtual machine configuration with a thumbprint of the target vSphere Replication server certificate. VRMS registers each vSphere Replication server at the target site with the certificates of all ESXi hosts from the source site. The registration is done separately for each paired vSphere Replication site.

VRMS exchanges data for the leaf certificates of the endpoints of the encrypted replication traffic, regardless of the certificate authorities for the source ESXi host and the target vSphere Replication server.

You can run the shell command `esxcli software vib list` on the source ESXi host and look for the `vmware-hbr-agent` VIB to make sure the agent is available in your system.

When the network encryption feature is switched on, the agent encrypts the replication data on the source ESXi host and sends it to the vSphere Replication appliance on the target site. The vSphere Replication server decrypts the data and sends it to the target datastore.

Unencrypted traffic goes through port 31031 on the source ESXi hosts and the vSphere Replication appliance on the target site.

Encrypted traffic goes through port 32032 on the source ESXi hosts and the vSphere Replication appliance on the target site.

If you configure a replication of an encrypted VM, the network encryption is automatically turned on and cannot be deactivated.

# How vSphere Replication Works When Using Guest OS Trim/Unmap Commands

Storage and network bandwidth requirements might increase when using the trim/unmap Guest OS commands with vSphere Replication. You might also observe RPO violations.

## Incremental Sync After Using Guest OS Trim/Unmap Commands

Calling the trim/unmap commands might increase the storage consumption on the target site.

After using the trim/unmap commands on the source site disk, the free space available on the disk is added to the data blocks that vSphere Replication transfers to the target site during the next RPO cycle. As a result, when the source site disk is less full, the size of the changed blocks that are transferred to the target site is larger.

For example, if the source site disk is 10 TB, and only 1 TB is allocated, calling the trim/unmap commands results in a transfer of at least 9 TB to the target site.

If the source site disk is 10 TB, 9 TB of which are allocated, and if you delete 2 TB of data, calling the trim/unmap commands results in a transfer of at least 3 TB of data to the target site.

Because of the incremental sync and depending on the RAID configuration defined by the VM storage policy at the target site, the storage consumption by the replicated VM can be more than two times as high as the consumption by the source VM.

**Note** If you use the trim/unmap commands at the source site, it is a best practice to configure the replication with an activated network compression to reduce the network bandwidth. See: Replication Data Compression and Configure a Replication.

**Note** If you use the trim/unmap commands, and the target datastore is vSAN, to reduce the actual physical storage space consumption at the target site, you must activate deduplication and compression of vSAN. If you do not use deduplication and compression, no storage space is reclaimed at the target site. Even after deduplication and compression, you might still see storage consumption spikes at the target location, but after the sync and the reconciliation, the storage space is freed. For more information about deduplication and compression, see Using Deduplication and Compression.

You can't see the storage consumption by the replicated VM at the target site. You can only see the overall consumption of the entire vSAN datastore. So, you can't track the reclaimed storage space at the VM disk level, but you can track it by looking at the overall free space left on the vSAN datastore.

## Recovery Point Objective Violations After Using the Trim/Unmap Commands on the Source Virtual Machine

You can call the trim/unmap commands manually or they can be called by the guest OS at certain intervals of time. In both cases, the synchronization after the command might take a significant amount of time.

The usage of the trim/unmap commands to reclaim the unused space on the source virtual machine might generate a large number of changed disk blocks. The synchronization of these changes might take longer than the configured RPO, and vSphere Replication starts reporting RPO violations.

Since the replication is behind the RPO schedule, to synchronize the changed disk blocks, a new incremental sync begins as soon as the synchronization of the previous instance completes. This process of immediate subsequent incremental syncs continues until vSphere Replication creates a replica instance that satisfies the RPO schedule, and does not report an RPO violation. The replication status becomes OK.

# Best Practices for Using and Configuring vSphere Replication

Best practices for using and configuring vSphere Replication can prevent your environment from possible issues during replication.

**Important** You mustn't change the source VM hardware while you are in the process of configuring a replication. For example, don't add or remove hard disk to the source VM before you finish configuring the replication.

## Setting the Optimal Recovering Point Objective (RPO) Time

The replication of several thousand virtual machines is a bandwidth consuming process. One of the many factors that influence bandwidth requirements for vSphere Replication is the RPO configuration for each replicated virtual machine.

You can set the RPO to 5 minutes, but you must estimate the optimal RPO time to save bandwidth for the replication, and to cover your business requirements for the protection of your VMs.

For instance, if a block changes only once per day, it is replicated only once regardless of the RPO configuration. However, if a block changes many times during the day, and the RPO is set to a low number such as 30 minutes, the block might be replicated as many as 48 times in one day.

vSphere Replication tracks larger blocks on disks over 2 TB. Replication performance on a disk over 2 TB might be different than replication performance on a disk under 2 TB for the same workload depending on how much of the disk goes over the network for a particular set of changed blocks.

A network with the appropriate bandwidth available to transfer the system’s data ingest rate is required to support the desired replication interval.

If you have a dataset of 1 TB with a daily change rate of 2 GB per hour and RPO set to one hour, this means vSphere Replication must transfer 2 GB in 1 hour or 4.7 Mbps. This is the minimum theoretical bandwidth required to complete the vSphere Replication transfer.

The data change rate is not uniform throughout the day even though the above example assumes it. Use the peak data change rate in your scenario to calculate the minimum bandwidth requirement

See Calculate Bandwidth For vSphere Replication for details.

## Using Multiple Point in Time (MPIT) Recovery

Each point in time snapshot consumes storage. The amount consumed depends on the data change rate in the VM. When you set multiple point in time instances for replication of a VM between two vCenter Server sites, vSphere Replication presents the retained instances as standard snapshots after recovery. The time required to consolidate snapshots after recovery, increases with the number of snapshots.

Although vSphere Replication supports up to 24 recovery points, you must set the MPIT to the lowest number of recovery points that meets your business requirements. For example, if the business requirement is for 10 recovery points, you must set up vSphere Replication to save only 10 snapshots. You can set up two recovery points per day for the last five days. As a result, the consumed storage and the time needed to consolidate the snapshots after recovery are less than if you use the maximum number of recovery points.

## Configuring Quiescing

For VMs with high levels of storage I/O, quiescing of the file system and applications can take several minutes and impact the performance of the VM . When quiescing a file system and applications for Windows VMs, vSphere Replication requires a regular VM snapshot before replication. When you estimate the RPO time, consider the time and resource consumption for the quiescing and for the consolidation of the snapshots. For example, if you configure a replication of a Windows VM with an RPO of 15 minutes and quiescing is enabled, vSphere Replication generates a VM snapshot and consolidates it every 15 minutes.

Quiescing options are available only for virtual machines that support quiescing. For more information on which operating systems are supported, see the Guest OS Quiescing Support section in Compatibility Matrices for vSphere Replication 8.4.x.

**Note** Quiescing for vSphere Replication and backup operations for the same virtual machine is not supported.

## Configuring Replication Seeds

You can copy virtual disk files of source VMs to the target location and use these files as replication seeds. By using replication seeds, vSphere Replication reduces the amount of time and network bandwidth required for the initial full sync process. The UUID of the source and target VMDK files must match for the replication to be successful and to prevent unintentional overwrites of disk files that belong to other VMs at the target location.

## Monitoring a Datastore on the Target Site

vSphere Replication requires enough disk space at the target site to replicate a VM. If the available space is not enough to save the replication files, the replication might fail. You can create an alarm that alerts you about insufficient storage capacity at the target site.

# Configure a Replication

vSphere Replication can protect one or more virtual machines and their virtual disks by replicating them from one vCenter Server instance to another. Configure the replications with your desired settings by using the following procedure.

When you configure a replication, you set a recovery point objective (RPO) to determine the maximum data loss that you can tolerate. For example, an RPO of one hour seeks to ensure that a virtual machine loses the data for no more than one hour during the recovery. For smaller RPO values, less data is lost in a recovery, but more network bandwidth is consumed keeping the replica up to date. The RPO value affects replication scheduling, but vSphere Replication does not adhere to a strict replication schedule. See Recovery Point Objective.

vSphere Replication guarantees crash consistency among all the disks that belong to a virtual machine. If you use quiescing, you might obtain a higher level of consistency. The available quiescing types are determined by the operating system of the virtual machine. See Compatibility Matrices for vSphere Replication 8.4 for quiescing support for Windows and Linux virtual machines.

You can configure virtual machines to replicate from and to vSAN datastores. See Using vSphere Replication with vSAN Storage for the limitations when using vSphere Replication with vSAN.

### Prerequisites

- Verify that the vSphere Replication appliance is deployed at the source and the target sites.
- To enable the quiescing of virtual machines that run Linux guest OS, install the latest version of VMware Tools on each Linux machine that you plan to replicate.
- If you want to replicate an encrypted VM or to activate the network encryption of a replication, verify that your environment meets the requirements. See Replicating Encrypted Virtual Machines.

### Procedure

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab, select **Outgoing** or **Incoming**, and click the **Create new replication** icon.
5. Accept the automatic assignment of a vSphere Replication server or select a particular server on the target site and click **Next**.
6. On the **Virtual machines** page of the **Configure Replication** wizard, select the virtual machines you want to replicate and click **Next**.

7 On the **Target datastore** page, select a datastore on which to replicate files.

When replicating multiple virtual machines, you can configure a different target datastore for each virtual machine.

**Note** All datastores that are selected as the target of the replicated disks must be read and write accessible by at least one host on the target site.

If after configuring the replication the read and write access gets broken, the replication will get into an unrecoverable state.

8 (Optional) Select the **Select seeds** check box.

Replication seeds can reduce the network traffic during the initial full synchronization, but unintended use of replication seeds might lead to data loss.

9 (Optional) Select or deselect the **Auto-include new disks in replication** check box.

Keep the check box selected to automatically include new disks in the replication, with the same replication configuration as the source virtual machine. Disk format for the automatically included disks is determined the following way: If all replicated disks use the **Same as source** format, the **Same as source** format is applied to the automatically included disks. If that is not the case, but all replicated disks use the same format, for example **Thin provision**, the same format (**Thin provision**) is applied to the automatically included disks. If all replicated disks use different formats, the **Same as source** format is applied to the automatically included disks.

10 (Optional) Activate or deactivate the **Configure datastore per disk** view.

If you activate the **Configure datastore per disk** view, you can specify a different datastore for each disk. You can also include or exclude existing disks from replication, and you can also activate or deactivate the automatic replication of new disks. To include or exclude a new or existing disk from being replicated, select or deselect the respective disk.

11 Click **Next**.

12 (Optional) On the **Select seed** page, review the suggested replication seeds and change them if necessary.

You can select seed files for each virtual machine disk and search for seeds by using the drop-down menu and clicking **Browse**.

The replica files for the disk are written in the seeds file directory.

13 Select the **The selected seeds are correct** check box and click **Next**.

14 On the **Replication settings** page, use the RPO slider to set the acceptable period for which data can be lost if a site failure occurs.

The available RPO range is from 5 minutes to 24 hours.

15 (Optional) To save multiple replication instances that can be converted to snapshots of the source virtual machine during recovery, select **Enable point in time instances** and adjust the number of instances to keep.

**Note** You can keep up to 24 instances for a virtual machine. For example, if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is four days.

The number of replication instances that vSphere Replication keeps depends on the configured retention policy, but also requires that the RPO period is short enough for these instances to be created. Because vSphere Replication does not verify whether the RPO settings creates enough instances to keep, and does not display a warning message if the instances are not enough, you must ensure that you set vSphere Replication to create the instances that you want to keep. For example, if you set vSphere Replication to keep six replication instances per day, the RPO period must not exceed four hours, so that vSphere Replication can create six instances in 24 hours.

16 (Optional) Activate quiescing for the guest operating system of the source virtual machine.

**Note** Quiescing options are available only for virtual machines that support quiescing. vSphere Replication does not support VSS quiescing on vVOL.

17 (Optional) Select **Enable network compression for VR data**.

Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication server. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

18 (Optional) Activate the network encryption of the replication traffic.

If you configure a replication of an encrypted VM, this option is automatically turned on and cannot be deactivated.

19 On the Ready to complete page, review the replication settings, and click **Finish**.

### Results

vSphere Replication starts an initial full synchronization of the virtual machine files to the designated datastore on the target site.

## Move a Replication to a New vSphere Replication Server

After configuring vSphere Replication, you can move replications to other vSphere Replication Server instances. You might do this to complete maintenance tasks on existing servers or to balance the load on the servers if one server becomes overloaded with replications.

### Prerequisites

You must have an additional vSphere Replication Server deployed and registered, apart from the embedded vSphere Replication Server.

### Procedure

1. Log in to the vSphere Client or vSphere Web Client on the source site.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
5. Click the **Reconfigure** icon.
6. On the **Target site** page of the **Reconfigure Replication** wizard, select **Manually select vSphere Replication Server**.
7. Select a different vSphere Replication Server instance from the list and click **Next** until you finish the wizard.

   **Note** You can see the list of replications handled by each vSphere Replication Server and if some load balancing is needed, the replications can switch to a less loaded vSphere Replication Server.

   If you use the **Auto-assign vSphere Replication Server** option, the vSphere Replication Server will not be changed and the load balancing will not be autotriggered.

### Results

The newly assigned server is updated in the **Replication Server** column.

## Stop Replicating a Virtual Machine

If you do not need to replicate a virtual machine, you can stop that replication by removing it.

Take a note of the target datastore and the name of the replication that you are about to stop. You need this information to clean up your environment after you stop the replication.

### Prerequisites

Verify that you are logged in the vSphere Web Client or vSphere Client as a VRM virtual machine replication user or a VRM administrator user. See vSphere Replication Roles Reference.

### Procedure

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.

5 Click the **Remove** icon.

vSphere Replication asks you if you want to stop permanently the replication for the selected virtual machine.

**Note** The connection between the vSphere Replication sites must be working to stop a replication on both sites. Alternatively, you can force stop the replication on the local site by selecting **Force stop replication**. If the remote site is available, you must also use the Site Recovery user interface to force stop the corresponding replication on the remote site. If you force stop an outgoing replication, the replication can still be recovered by using the Site Recovery user interface on the remote site.

6 To confirm that you want to stop replicating this virtual machine, click **Remove** .

If you want to retain your replica disks, select the **Retain replica disks** check box.

7 Inspect the target datastore for any leftover replica disks and files. Delete them if you do not plan to use them as seeds in the future.

### Results

The virtual machine does not replicate to the target site.

When you stop a replication, the following operations are performed at the replication target site.

- If the VMDK files were created when the replication was first configured, the VMDK files are deleted from the target site datastore.
- If you configured the replication to use existing disks at the target site as seeds, the VMDK files are not deleted and remain on the target datastore.

# Reconfiguring Replications

You can reconfigure a replication to modify its settings.

For example, you can reconfigure the replication to activate or deactivate a virtual machine disk file for replication, modify replication options, such as RPO, MPIT retention policy, or quiescing method. You can also specify a different target datastore for replica configuration and disk files.

**Important** You mustn't change the source VM hardware while you are in the process of reconfiguring a replication. For example, don't add or remove hard disk to the source VM before you finish the reconfiguration of the replication.

## Reconfigure Recovery Point Objective in Replications

You can modify the settings for already configured replications to specify different recovery point objective (RPOs).

### Procedure

1 Log in to the vSphere Client or vSphere Web Client.

2 On the home page, click **Site Recovery** and click **Open Site Recovery**.

3 On the Site Recovery home page, select a site pair and click **View Details**.

4 Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.

5 Click the **Reconfigure** icon.

6 Click **Next** until you reach the **Replication settings** page of the **Reconfigure Replication** wizard.

7 Modify the RPO settings for this replication and click **Next**.

8 Click **Finish** to save your changes.

## Change the Point in Time Settings of a Replication

You can reconfigure a replication to activate or deactivate the saving of point in time instances, or to change the number of instances that vSphere Replication keeps.

vSphere Replication can save replication instances that can be used as snapshots after recovery or planned migration operations. You can save up to 24 point in time instances per VM.

Procedure

1 Log in to the vSphere Client or vSphere Web Client.

2 On the home page, click **Site Recovery** and click **Open Site Recovery**.

3 On the Site Recovery home page, select a site pair and click **View Details**.

4 Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.

5 Click the **Reconfigure** icon.

6 Click **Next** until you reach the **Replication settings** page of the **Reconfigure Replication** wizard.

7 In the **Point in time instances** pane, make the changes that you want to apply and click **Next**.

| Action | Procedure |
| --- | --- |
| **Enable the saving of point in time instances** | Select the **Enable point in time instances** check box. |
| **Disable the saving of point in time instances** | Deselect the **Enable point in time instances** check box. |
| **Adjust the number of instances to keep and for how long to keep them** | Use the spin-boxes to adjust the number of instances (no more than 24 per virtual machine) to keep per day and the number of past days for which you want to keep replication instances. |

8 Click **Finish** to save your changes.

Results

If you selected to deactivate the saving of point in time instances, the instances that exist on the target site are deleted when the next replication instance appears on the target site. The moment when a new replication instance is saved on the target site depends on the RPO setting.

## Increasing the Size of Replicated Virtual Disks

If you run out of disk space, you can seamlessly increase the virtual disks of virtual machines that are configured for replication without triggering an initial full synchronization.

You can resize the virtual disk of a replicated virtual machine while the virtual machine is powered on or powered off.

**Important** As a best practice, resize the virtual disk of a replicated virtual machine while the virtual machine is powered on. If you increase the disk size of a virtual machine that is powered off, full synchronization is performed the next time you power on the replicated virtual machine.

After you increase the virtual disk on the source site, the virtual disk on the target site automatically resizes and the ongoing replication enters `Resizing disk` state, until the task completes.

**Note** After you resize the virtual disk, vSphere Replication clears all available multiple points in time. You can modify this behavior by changing the virtual disk resizing configuration options.

When the target datastore for a replication is NFS and you want to increase a thick-provisioned virtual disk, if the available storage space on the target datastore is not enough for the new size, then the resized replica disk is of a thin type.

To use this feature, you need vSphere 7.0 or later on the source site and vSphere 6.5 or later on the target site.

For more information about disk resizing, see *Change the Virtual Disk Configuration in the VMware Host Client* in the vSphere Product Documentation.

## Configure the Virtual Disk Resizing

You can determine the behavior of vSphere Replication during disk resizing, by choosing one of the three configuration options. To activate your preferred option, you must change the value of three different parameters in the `/etc/vmware/hbrsrv.xml` configuration file.

- vSphere Replication can follow two approaches to perform the disk resizing on the target site. To configure the way the server handles the resizing, change the value of the `extendDiskPITHierarchyPolicy` parameter.

  **Table 11-2.** `extendDiskPITHierarchyPolicy` **Parameter Values**

  | Value | Description |
  |---|---|
  | `extendDiskPITHierarchyPolicy` = `auto` | vSphere Replication selects `preserve` or `collapse`, depending on the current datastore storage consumption and the requested new virtual disk size. This is the default value of the parameter. |
  | `extendDiskPITHierarchyPolicy` = `collapse` | vSphere Replication collapses the disk hierarchy of the replica disk and extends the resulting base disk. All PITs created before the start of the virtual disk resizing are lost. You cannot perform recovery until you create a PIT after resizing the virtual disk. |
  | `extendDiskPITHierarchyPolicy` = `preserve` | vSphere Replication creates a new base disk, which is a full clone of the latest PIT. vSphere Replication extends the new disk to the new size. The original base disk still exists. The extra consumed storage is freed, after vSphere Replication removes all PITs, which contain the original disk. Then the vSphere Replication removes the original replica base disk. |

- To adjust the behavior when the `extendDiskPITHierarchyPolicy` is set to `auto`, you can use the `extendDiskPITHierarchyPolicyAutoThreshold` parameter. You can change the property value to a number between 0 and 1 (the default value is 0.9). This way you set a limit to the datastore capacity. vSphere Replication calculates this limit by multiplying the size of the datastore capacity by the `extendDiskPITHierarchyPolicyAutoThreshold` parameter value.

  For example, if the datastore capacity is 5 TB and the `extendDiskPITHierarchyPolicyAutoThreshold` parameter is set to 0.8, then the datastore capacity limit is 4 TB.

  vSphere Replication calculates what is the final storage consumption, if the `preserve` mode is active. If the storage consumption is below the threshold, vSphere Replication uses the `preserve` mode and if it is above the threshold, it uses the `collapse` mode.

- To reduce the period of extended storage consumption, when `extendDiskPITHierarchyPolicy` is set to `preserve` mode, change the value of the `removeMPITsBeforeBaseDisks` parameter.

  **Table 11-3.** `removeMPITsBeforeBaseDisks` **Parameter Values**

| Value | Description |
|---|---|
| `removeMPITsBeforeBaseDisks` = `true` | The vSphere Replication server drops all PITs, which are based on the original disk size, after a new PIT which is based on the extended disk appears. |
| `removeMPITsBeforeBaseDisks` = `false` | The retention policy of the PITs determines the expiration of the older PITs. The storage consumption drops, after all PITs, which refer to the original disk, are expired. |

## Change the Target Datastore Location of a Replication

You can reconfigure a replication to change the datastore where replicated data is saved.

To change the target datastore, the old target datastore from which you want to move the replication data must be online. If the old datastore is inaccessible, the reconfiguration task fails. To change the target datastore when the old datastore is inaccessible, you must stop the replication to the old datastore and configure another replication to the new datastore.

**Note** You cannot change the target datastore, while you are performing a test recovery. To change the target datastore, you must wait for the test cleanup to be complete.

**Procedure**

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
5. Click the **Reconfigure** icon.
6. Click **Next** to reach the **Target datastore** page of the **Reconfigure Replication** wizard.
7. Select the new target datastore.

   **Note** All datastores that are selected as the target of the replicated disks must be read and write accessible by at least one host on the target site.

   If after reconfiguring the replication the read and write access gets broken, the replication will get into an unrecoverable state.

8. Click **Next** until you reach the **Ready to complete** page and click **Finish** to save your settings.

### Results

vSphere Replication moves all replicated instances and configuration files to the new target datastore according to your settings.

# Enable VM Encryption for an Already Replicated VM

You can enable the virtual machine encryption for an already replicated VM.

### Procedure

1. Recover the virtual machine.
2. Stop the replication.
3. Encrypt the disk on the source site.
4. Encrypt the disk of the recovered virtual machine on the target site.
5. Unregister the recovered virtual machine on the target site, but do not delete the disks.
6. Configure a replication by using the disks of the recovered virtual machine as seeds.

# Stopping a Virtual Machine Offline Synchronization Task

You can stop an ongoing offline synchronization task for a powered off virtual machine by using two different methods: by establishing an SSH connection to the ESXi host of the source VM or by using the vCenter Server Managed Object Browser (MOB).

## Stop a Virtual Machine Offline Synchronization Task by Using an SSH Connection

### Procedure

1. Establish an SSH connection to the ESXi host that hosts the source virtual machine.
2. To get the list of all VMs, and to find the ID of the VM whose offline sync you want to stop, run the following command: `vim-cmd vmsvc/getallvms`.
3. To check the progress of the sync task, run the following command: `vim-cmd hbrsvc/vmreplica.queryReplicationState <vmid>`.
4. To stop the offline sync task, run the following command: `vim-cmd hbrsvc/vmreplica.stopOfflineInstance <vmid>`.

## Stop a Virtual Machine Offline Synchronization Task by Using the vCenter Server MOB

### Prerequisites

Verify that you have the credentials of a vSphere administrator.

Procedure

1 To get the Managed Object ID (MOID) of the source VM:
   a Log in to the vSphere Client or vSphere Web Client on the source site.
   b Navigate to the source VM.
   c Copy the *vm-...* value from the URL.
2 Log in to `https://<vc_ip>/mob/?moid=hbrManager&method=stopOfflineInstance&vmodl=1` with vCenter Server credentials.
3 In the **Value** text box, replace the MOID text with the MOID of the VM, and click **Invoke Method**.
4 To check the state of the stopOfflineInstance task:
   a In the **Value** text box of the **Method Invocation Result: ManagedObjectReference** panel, click the displayed task session.
   b On the **Managed Object Type: vim.Task** window, click the **Info** value.
   c Optional: Refresh the page.

# Monitoring and Managing Replications in vSphere Replication

12

vSphere Replication provides a management interface where you can monitor and manage virtual machine replication and connectivity states for local and remote sites.

On the home page of the Site Recovery user interface, you can see all vSphere Replication site connections and the number of outgoing and incoming replications between the sites.

To see details about the status of a connection, replication problems, and to manage and monitor replications between a site pair, click the **View Details** button.

Read the following topics next:

- Monitor the Status of a Replication
- View Replication Reports for a Site
- Identifying Replication Problems
- Manage vSphere Replication Connections
- Manage vSphere Replication Servers

## Monitor the Status of a Replication

You can monitor the status of your replications, view information about the virtual machines configured for replication, or get a remediation plan for some replication states.

For more information about how to identify replication errors, see Identifying Replication Problems.

### Prerequisites

- Verify that vSphere Replication is running.
- Verify that the virtual machines are configured for replication.

### Procedure

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.

4 To see details of the virtual machines replicated from this site, select the **Replications** tab and click **Outgoing** or **Incoming**.

Table 12-1. Replication Statuses

| Status | Description | Remediation |
|---|---|---|
| OK | The replication is running. | Not needed. |
| Not Active | The replication is not running at the moment.<br>■ The source virtual machine is powered off.<br>■ A communication problem might have occurred between the source ESXi host and the target site.<br>■ At target site, the vSphere Replication server cannot access the datastore using an ESXi host. | ■ Power on the source virtual machine.<br>■ Check the network connectivity between source and target site. |
| Paused | The replication is not running at the moment. A vSphere Replication user has paused the replication. | From the list of replications, select the paused replication and click the **Resume** icon. |
| Error | The replication is not running at the moment.<br>■ A configuration error occurred.<br>■ A replication error occurred. For example, the target site infrastructure is not accessible. | ■ Reconfigure the replication.<br>■ Verify whether some problem occurred on the virtual machine by clicking the **Site Pair** tab and clicking **Issues**. |
| Status (RPO violation) | For replication status `OK`, `Sync`, or `Full Sync`, the replication is running, but the RPO that is set for the replication is not met and is violated.<br>For replication status `Not Active` or `Error`, the replication is not running, and the RPO that is set for the replication is violated.<br>■ The network connection between the source and the target site is dropping intermittently.<br>■ The bandwidth of the connection between the source and the target site is too low.<br>■ The replication is not running, so data cannot be replicated on the target site. | ■ Improve the network connection between the source and target site.<br>■ Increase the RPO period.<br>■ For replication status `Not Active` or `Error`, address the cause for the status and wait for the next sync. |

**Note** If a replication is in the `Not Active` replication state, you might have connected the source and target sites using network address translation (NAT). vSphere Replication does not support NAT. Use credential-based authentication and network routing without NAT when connecting the sites. Another cause for a `Not Active` replication state might be that the source virtual machine is powered off. Automatic replication works only on virtual machines that are powered on.

# View Replication Reports for a Site

If you observe frequent RPO violations, want to learn more about the network usage of vSphere Replication, or verify the status of your outgoing replications, you can view replication statistics for source and target vCenter Server sites.

You can view statistics for the replications for a certain time period. The transferred bytes statistics do not include the transferred data for the initial full synchronization, only the data transferred after the initial synchronization is complete. The update of the information in the statistics might occur in the end of the selected RPO period. For example, if you configure a replication with the default RPO of 1 hour, you might not see any transferred data for this VM in the statistics for up to 1 hour.

The granularity of the statistical data depends on the `rrd-updater-interval` parameter. The parameter is defined in the `the/opt/vmware/hms/conf/hms-configuration.xml` configuration file. This parameter controls the interval, at which the statistical data is saved. By default, the value is set to 5 minutes, but it can be changed if needed.

**Note** Data is collected in 10 minute intervals and the graphs represent aggregated data for each interval. Therefore, you cannot see the exact moment when a peak value occurred and there might be an additional delay of up to 10 minutes before the Transferred Bytes statistics display the data. The displayed data combines all site pairs.

- Transferred Bytes - total bytes transferred for all outgoing replications, excluding the data from the initial full synchronization.
- Replications Count - number of outgoing replications.
- RPO Violation Count - number of RPO violations.
- Target Sites Count - number of vSphere Replication site connections.
- VR Sites Count - number of registered replication servers.

### Prerequisites

Verify that vSphere Replication is running.

### Procedure

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.

3 On the Site Recovery home page, select a site pair and click **View Details**.

4 Click the **Site Pair** tab and click **vSphere Replication reports**.

#### Results

The **Reports** page displays historic data for vSphere Replication for a certain time period.

#### What to do next

- You can use the drop-down menu above the reports to change the time range of the reports.
- You can zoom in the data.
- Export any chart as a CSV file.

## Interpreting Replication Statistics for a Site

You can use the reports that vSphere Replication compiles to optimize your environment for replication, identify problems in your environment, and reveal their most probable cause.

As an administrator, you can get the necessary information to diagnose various replication issues by using the server and site connectivity, number of RPO violations, and other metrics.

The following sections contain examples of interpreting the data displayed under **vSphere Replication reports** on the **Site Pair** tab of vSphere Replication.

### RPO Violations

The large number of RPO violations can occur due to by various problems in the environment, on both the protected and the recovery site. With more details on historical replication jobs, you can make educated decisions on how to manage the replication environment.

Table 12-2. Analyzing RPO Violations

| Probable Cause | Solution |
| --- | --- |
| ■ The network bandwidth cannot accommodate all replications.<br>■ The replication traffic might have increased.<br>■ The initial full sync for a large virtual machine is taking longer than the configured RPO for the virtual machine. | ■ To allow the lower change rate virtual machines to meet their RPO objectives, deactivate the replication on some virtual machines with a high change rate.<br>■ Increase the network bandwidth for the selected host.<br>■ Check if the replication traffic has increased. If the traffic has increased, investigate possible causes, for example the usage of an application might have changed without you being informed.<br>■ Check the historical data for average of transferred bytes for a notable and sustained increase. If an increase exists, contact application owners to identify recent events that might be related to this increase.<br>■ Adjust to a less aggressive RPO or look at other ways to increase bandwidth to accommodate the current RPO requirements. |
| ■ A connectivity problem exists between the protected and the recovery site.<br>■ An infrastructure change might have occurred on the recovery site. | ■ To verify the connection between the protected and recovery site, check the site connectivity data.<br>■ Check if the infrastructure on the recovery site has changed or is experiencing problems that prevent vSphere Replication from writing on the recovery datastores. For example, storage bandwidth management changes made to recovery hosts might result in storage delays during the replication process.<br>■ Check on the vSphere Replication Management Server appliance and the vSphere Replication Server appliance. Someone might have shut down the appliance or it might have lost connection. |

## Transferred Bytes

Corelating the total number of transferred bytes and the number of RPO violations can help you decide on how much bandwidth might be required to meet RPO objectives.

Table 12-3. Analyzing the Rate of Transferred Bytes and RPO Violations

| Graph Values | Probable Cause | Solution |
|---|---|---|
| ■ High rate of transferred bytes and high number of RPO violations<br>■ Low rate of transferred bytes and high number of RPO violations | The network bandwidth might be insufficient to accommodate all replications. | ■ Check the **transferred bytes** graph and use the drop-down menus to filter the data by virtual machine and time period. To let virtual machines with a lower change rate meet their RPO objectives, you can deactivate the replication on some virtual machines with a high change rate.<br>■ Increase the network bandwidth for the selected host. |
| ■ High rate of transferred bytes and a few or no RPO violations<br>■ Low rate of transferred bytes and a few or no RPO violations | The environment operates as expected. | N/A |

# Identifying Replication Problems

You can view and troubleshoot possible vSphere Replication problems that might occur during replication.

Under **Issues** on the **Site Pair** tab of vSphere Replication, you can view and identify possible replication problems.

Table 12-4. Possible Replication Problems

| Problem | Cause | Solution |
|---|---|---|
| Not Active | The replication is not active because the virtual machine is powered off and a warning icon appears. Replication is not running for that virtual machine. | Power on the virtual machine to resume the replication. |
| Paused | If you paused the replication, a warning icon appears. | Resume the paused replication from the **Issues** tab. |
| Error | If you added a disk on a virtual machine which is already configured for replication with deactivated automatic replication for new disks, the replication pauses and goes to an error state. | Reconfigure the replication and activate or deactivate the newly added disk. |

Table 12-4. Possible Replication Problems (continued)

| Problem | Cause | Solution |
|---|---|---|
| Error | While configuring replication, the replication fails with the incorrect UUID. For example, the replication seed found and intended for use has a different UUID from the original hard disk. | Reconfigure the replication. |
| RPO Violation | A replication contains an RPO violation. | See Reconfigure Recovery Point Objective in Replications. |

# Manage vSphere Replication Connections

You can reconnect a site pair or break the connections between vSphere Replication sites.

If you have problems with an existing site pair, you can attempt to reconnect the site pair with the **Reconnect** action. When you provide the required credentials, the reconnection operation attempts to repair the existing site pair.

With the **Break Site Pair** action, you can disconnect vSphere Replication sites.

**Note** You cannot use the **Reconnect** action to add a missing pairing or a pairing that was manually broken with **Break Site Pair**. If your site pair is missing a pairing, you must use **New Site Pair** to configure it.

### Prerequisites

Verify that you have paired your protected site with at least one recovery site. To create a connection to a new recovery site, see Configure vSphere Replication Connections.

### Procedure

1. Log in to the vSphere Client or vSphere Web Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Site Pair** tab and click **Summary**.

5 Manage the site pair.

| Option | Description |
| --- | --- |
| **Reconnect** | a Select **Site Pair > Summary**, and click **Reconnect**.<br>b Select the services you want to pair. Enter the address of the Platform Services Controller on the remote site, provide the vCenter Single Sign-On user name and password, and click **Reconnect**. |
| **Break a site pair** | a Click **Break Site Pair**.<br>b Select the services you want to disconnect.<br>c Click **Disconnect**. |

# Manage vSphere Replication Servers

You can view, configure, reconnect, and unregister vSphere Replication Server instances that are registered in your environment.

### Prerequisites

Verify that vSphere Replication is running.

### Procedure

1 Log in to the vSphere Client or vSphere Web Client.

2 On the home page, click **Site Recovery** and click **Open Site Recovery**.

3 On the Site Recovery home page, select a site pair and click **View Details**.

4 Click the **Site Pair** tab, click **Replication Servers**, and select a server from the list.

5 To manage the vSphere Replication servers, select an option.

| Option | Description |
| --- | --- |
| **Register a virtual machine as vSphere Replication Server.** | Click to register a virtual machine as a vSphere Replication Server. See Register an Additional vSphere Replication Server. |
| **Unregister the selected vSphere Replication Server.** | Click to unregister the vSphere Replication Server that you selected from the list. See Unregister and Remove a vSphere Replication Server. |
| **Reconnect the selected vSphere Replication Server.** | Click if the status of the vSphere Replication Server that you selected from the list is `Disconnected`. |
| **Configure the selected vSphere Replication Server.** | Click to access the VRMS Appliance Management Interface of the vSphere Replication Server that you selected from the list. |

# Performing a Recovery with vSphere Replication

13

With vSphere Replication, you can recover virtual machines that were successfully replicated at the target site.

vSphere Replication performs a sequence of steps to recover replicated virtual machines.

- vSphere Replication prepares for the recovery operation.
  - If you perform a synchronization of the latest changes, vSphere Replication checks that the source site is available and source virtual machine is powered off before recovering the virtual machine on the target site. Then vSphere Replication synchronizes the changes from the source to the target site.
  - If you skip the synchronization and recover with the latest data available, for example, if the source site is not available, vSphere Replication uses the latest available data at the target site.
- vSphere Replication rebuilds the replicated `.vmdk` files.
- vSphere Replication reconfigures the newly replicated virtual machine with the correct disk paths.
- vSphere Replication registers the virtual machine with vCenter Server at the target site.

You can recover one virtual machine at a time in **Incoming** replications on the **Replications** tab at the target site. Optionally, you can power on the recovered virtual machine. The network devices of the recovered virtual machine are disconnected. You might need to configure the recovered virtual machine to render it fully operational.

If you enabled the saving of point in time instances, those instances are converted to snapshots of the recovered virtual machine. You can use the vSphere Web Client to revert to a snapshot from the list.

Read the following topics next:

- Recover Virtual Machines with vSphere Replication
- Failback of Virtual Machines in vSphere Replication

# Recover Virtual Machines with vSphere Replication

With vSphere Replication, you can recover virtual machines that were successfully replicated at the target site. You can recover one virtual machine at a time.

**Note** If you have replications, configured to automatically replicate newly added disks, then you perform a recovery, and add a new disk to the recovered VM, this disk will not be replicated upon reprotect operation. You must include the new disk to the replication manually.

### Prerequisites

Verify that the virtual machine at the source site is powered off. If the virtual machine is powered on, an error message reminds you to power it off.

### Procedure

1. Log in to the target site by using the vSphere Web Client or vSphere Client.
2. On the home page, click **Site Recovery** and click **Open Site Recovery**.
3. On the Site Recovery home page, select a site pair and click **View Details**.
4. Click the **Replications** tab and select a replication from **Incoming**.
5. Click the **Recover** icon.
6. Select whether to recover the virtual machine with all the latest data, or to recover the virtual machine with the most recent data available on the target site.

| Option | Description |
|---|---|
| **Synchronize recent changes** | Performs a full synchronization of the virtual machine from the source site to the target site before recovering the virtual machine. Selecting this option avoids data loss, but it is only available if the data of the source virtual machine is accessible. You can only select this option if the virtual machine is powered off. |
| **Use latest available data** | Recovers the virtual machine by using the data from the most recent replication on the target site, without performing synchronization. Selecting this option results in the loss of any data that has changed since the most recent replication. Select this option if the source virtual machine is inaccessible or if its disks are corrupted. |

7. (Optional) Select the **Power on the virtual machine after recovery** check box.
8. Click **Next**.
9. Select the recovery folder and click **Next**.
10. Select the target compute resource and click **Next**.

    The selected host must have read and write access to all datastores that are used as targets for the replica disks.

11 (Optional) If the virtual machine contains hard disks for which you have not activated replication, select a target destination to attach an existing disk or detach the disk, and click **Next**.

   This page only appears if the virtual machine contains hard disks for which you have not activated replication.

   - To select a target destination, click **Browse** and navigate to a folder on a datastore in which disk file is placed.
   - To detach the disk and exclude disk files from the recovery, click **Detach**.

12 Click **Finish**.

### Results

vSphere Replication validates the provided input and recovers the virtual machine. If successful, the virtual machine status changes to `Recovered`. The virtual machine appears in the inventory of the target site.

If you activated multiple point in time instances when you configured replication for the virtual machine, vSphere Replication presents the retained instances as standard snapshots after a successful recovery. You can select one of these snapshots to revert the virtual machine. vSphere Replication does not preserve the memory state when you revert to a snapshot.

If the recovery fails, the replication of the virtual machines reverts to the replication state before the attempted recovery. For more information about the failed recovery attempt, check the last recovery error message in the replication details pane or check vCenter Server tasks.

The recovery might also fail if you use the same name for the virtual machine in a scenario where you use vSphere Replication to replicate a virtual machine in a single vCenter Server and the vCenter Server instance has only one host in its inventory. See Error Recovering Virtual Machine in a Single vCenter Server Instance for more information.

After a successful recovery, vSphere Replication deactivates the virtual machine for replication if the source site is still available. When the virtual machine is powered on again, it does not send replication data to the recovery site. To unconfigure the replication, click the **Remove** icon.

When the source virtual machine is no longer in the vCenter Server inventory, the replication is removed from the **Outgoing** tab, but it can still be found in the **Incoming** tab on the target site.

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. To attach it to the correct network, edit the recovered virtual machine settings.

vSphere Replication disconnects virtual machine network adapters to prevent damage in the production network. After recovery, you must connect the virtual network adapters to the correct network. A target host or cluster might lose access to the DVS the virtual machine was configured with at the source site. In this case, manually connect the virtual machine to a network or other DVS to successfully power on the virtual machine.

# Failback of Virtual Machines in vSphere Replication

Failback of virtual machines between vCenter Server sites is a manual task in vSphere Replication. Automated failback is not available.

After performing a successful recovery on the target vCenter Server site, you can perform failback. Click **Incoming** and manually configure a new replication in the reverse direction, from the target site to the source site. The disks on the source site are used as replication seeds, so that vSphere Replication only synchronizes the changes made to the disk files on the target site. For more information on replication seeds, see Replicating Virtual Machines Using Replication Seeds.

Before you configure an incoming replication, you must unregister the virtual machine from the inventory on the source site.

# Troubleshooting vSphere Replication

14

Known troubleshooting information can help you diagnose and correct problems that occur while replicating and recovering virtual machines with vSphere Replication.

If you have problems with deploying vSphere Replication, replicating or recovering virtual machines, or connecting to databases, you can troubleshoot them. To help identify the problem, you might need to collect and review vSphere Replication logs and send them to VMware Support.

See Chapter 12 Monitoring and Managing Replications in vSphere Replication to learn about replication states and how to identify replication issues.

You can also search for solutions to problems in the VMware knowledge base at http://kb.vmware.com.

Read the following topics next:

- Generate vSphere Replication Support Bundle
- vSphere Replication Events and Alarms
- Solutions for Common vSphere Replication Problems

## Generate vSphere Replication Support Bundle

If you need a vSphere Replication support bundle for system monitoring and troubleshooting, you can use the vSphere Replication VRMS Appliance Management Interface to generate one. A VMware support engineer might request the bundle during a support call.

To access and download the vSphere Replication logs, you need access to the vSphere Replication VRMS Appliance Management Interface. vSphere Replication rotates its logs when the log file reaches 50 MB and keeps 50 compressed log files at most. For more options on how to collect automatically vSphere Replication logs, see https://kb.vmware.com/s/article/2013091.

**Note** You can save up to three support bundles at any time. If you generate three support bundles and you try to create a new one, the oldest support bundle is deleted. To save more than one support bundle on large environments, you might need to manually enlarge the support disk on the vSphere Replication Management Server VM. See Increase the Support Volume for Support Bundles.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.

Procedure

1. Use a supported browser to log in to the VRMS Appliance Management Interface.

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.
2. Click **Summary**, and then click **Download Support Bundle** to generate a `.zip` package of the current vSphere Replication logs.

   A link to the package containing the replication and system logs appears. Log files from the vSphere Replication appliance and all connected Additional vSphere Replication Servers are included in the same package.
3. Click **Download** to download the package.

## Increase the Support Volume for Support Bundles

To save more than one support bundle on large environments, you might need to manually increase the support disk on the vSphere Replication Management Server VM.

You can save up to three support bundles at any time. If you generate three support bundles and you try to create a new one, vSphere Replication deletes the oldest one.

If you want to save more than one support bundle on large environments, you might need to manually increase the support disk on the vSphere Replication Management Server VM. On environments with nine additional vSphere Replication servers, each support bundle can be over 1 GB in size, but the support volume for the support bundles is 2 GB.

Procedure

1. Edit the settings of the vSphere Replication Management Server VM and increase the size of the second virtual disk with 3 GB, from 17 GB to 20 GB.
2. Establish an SSH connection to the vSphere Replication Appliance.
3. Verify that the size of the `/dev/sdb` partition is increased by running the following command:

   ```
   fdisk -l
   ```

   This process can take up to several minutes until the OS detects the changes. If the changes remain undetected, reboot thevSphere Replication Management Server VM.
4. Once the OS detects the disk size change, increase the physical volume of the disk by running the following command:

   ```
   pvresize /dev/sdb
   ```
5. Verify the new volume by running the following command:

   ```
   pvs
   ```

`PSize` must be 20 GB and `PFree` must be 3 GB.

6 (Optional) If the sizes are not updated, rescan the physical volume and volume groups by running the following commands:

```
pvscan
vgscan
```

7 (Optional) To verify the size of the `support_vg` volume group, run the following command:

```
vgs
```

8 Increase the size of the support volume by running the following command:

```
lvextend -l +100%FREE -r /dev/support_vg/support
```

9 Verify that the logical volume is created by running the following command:

```
lvscan
```

Verify that `/dev/support_vg/`support volume is `ACTIVE` and verify its disk size.

10 (Optional) To see more information about the new logical volume, run the following command:

```
lvdisplay
```

## Manually Access the vSphere Replication Logs

You can copy and use the vSphere Replication logs for system monitoring and troubleshooting. A VMware support engineer might request these logs during a support call.

Use SCP or Win SCP to copy log folders and files from the vSphere Replication appliance and all Additional vSphere Replication Servers.

- `/opt/vmware/hms/logs/`
- `/opt/vmware/var/log/lighttpd/`
- `/var/log/vmware/`
- `/var/log/boot.msg`
- `/var/opt/apache-tomcat/logs/dr.log`

# vSphere Replication Events and Alarms

vSphere Replication supports event logging. You can define alarms for each event that can trigger if the event occurs. This feature provides a way to monitor the health of your system and to resolve potential problems, ensuring reliable virtual machine replication.

You can define and edit alarms to alert you when a specific vSphere Replication event occurs, such as after you configure a virtual machine for replication. See *View and Edit Alarm Settings in the vSphere Web Client* in the vSphere Web Client documentation.

# List of vSphere Replication Events

vSphere Replication Replication monitors replications and the underlying replication infrastructure, and generates different types of events. The events can be informative, they can give you a warning or notify you there is an error in your environment.

Table 14-1. vSphere Replication Events

| Event Name | Event Description | Event Type | Category | Event Target |
|---|---|---|---|---|
| vSphere Replication configured | Virtual machine is configured for vSphere Replication | com.vmware.vcHms.replicationConfiguredEvent | Info | Virtual Machine |
| vSphere Replication unconfigured | Virtual machine was unconfigured for vSphere Replication | com.vmware.vcHms.replicationUnconfiguredEvent | Info | Virtual Machine |
| Host configured for vSphere Replication | Host is configured for vSphere Replication | com.vmware.vcHms.hostConfiguredForHbrEvent | Info | Host System |
| Host unconfigured for vSphere Replication | Host with managed object id <Host Moid> was unconfigured for vSphere Replication | com.vmware.vcHms.hostUnconfiguredForHbrEvent | Info | Folder |
| Virtual machine is not configured for vSphere Replication | Virtual machine is experiencing problems with vSphere Replication and must be reconfigured | com.vmware.vcHms.vmMissingReplicationConfigurationEvent | Error | Virtual Machine |
| VM cleaned up from vSphere Replication | Virtual machine cleaned up from vSphere Replication configuration | com.vmware.vcHms.vmReplicationConfigurationRemovedEvent | Info | Virtual Machine |
| RPO violated | Virtual machine vSphere Replication RPO is violated by <x> minutes | com.vmware.vcHms.rpoViolatedEvent | Error | Virtual Machine |
| RPO restored | Virtual machine vSphere Replication RPO is not longer violated | com.vmware.vcHms.rpoRestoredEvent | Info | Virtual Machine |
| Remote vSphere Replication site is disconnected | Connection to the remote vSphere Replication site <siteName> is down | com.vmware.vcHms.remoteSiteDownEvent | Error | Folder |

Table 14-1. vSphere Replication Events (continued)

| Event Name | Event Description | Event Type | Category | Event Target |
|---|---|---|---|---|
| Remote vSphere Replication site is connected | Connection to the remote vSphere Replication site <siteName> is established | com.vmware.vcHms.remoteSiteUpEvent | Info | Folder |
| VR Server disconnected | vSphere Replication server <VR Server> disconnected | com.vmware.vcHms.hbrDisconnectedEvent | Info | Folder |
| VR Server reconnected | vSphere Replication server <VR Server> reconnected | com.vmware.vcHms.hbrReconnectedEvent | Info | Folder |
| Invalid vSphere Replication cleaned up | Virtual machine <VM name> was removed from vCenter Server and its vSphere Replication state was cleaned up | com.vmware.vcHms.replicationCleanedUpEvent | Info | Folder |
| Virtual machine recovered from replica | Recovered virtual machine <VM Name> from vSphere Replication image | com.vmware.vcHms.vmRecoveredEvent | Info | Virtual Machine |
| vSphere Replication cannot access datastore | Datastore is not accessible for vSphere Replication Server | com.vmware.vcHms.datastoreInaccessibleEvent | Error | Datastore |
| vSphere Replication handled a disk addition on a virtual machine | vSphere Replication detected and handled the addition of a disk to virtual machine <VM name>. Disks added are <Disk name> | com.vmware.vcHms.handledVmDiskAddEvent | Info | Virtual Machine |
| vSphere Replication handled a disk removal on a virtual machine | vSphere Replication detected and handled the addition of a disk to virtual machine <VM name>. Disks added are <Disk name> | com.vmware.vcHms.handledVmDiskRemoveEvent | Info | Virtual Machine |

Table 14-1. vSphere Replication Events (continued)

| Event Name | Event Description | Event Type | Category | Event Target |
|---|---|---|---|---|
| Failed to resolve storage policy | Failed to resolve a specific storage policy for the provided storage profile ID <profile ID> and datastore with managed object ID <Moid> | com.vmware.vcHms.failedResolvingStoragePolicyEvent | Error | Datastore |
| vSphere Replication paused | vSphere Replication was paused as a result of a configuration change, such as a disk being added or reverting to a snapshot where disk states are different | hbr.primary.SystemPausedReplication | Error | Virtual Machine |
| Invalid vSphere Replication configuration | Invalid vSphere Replication configuration | hbr.primary.InvalidVmReplicationConfigurationEvent | Error | Virtual Machine |
| Sync started | Sync started | hbr.primary.DeltaStartedEvent | Info | Virtual Machine |
| Application consistent sync completed | Application consistent sync completed | hbr.primary.AppQuiescedDeltaCompletedEvent | Info | Virtual Machine |
| File-system consistent sync completed | File-system consistent sync completed | hbr.primary.FSQuiescedDeltaCompletedEvent | Info | Virtual Machine |
| Unquiesced crash consistent sync completed | Quiescing failed or the virtual machine is powered off. Unquiesced crash consistent sync completed. | hbr.primary.UnquiescedDeltaCompletedEvent | Warning | Virtual Machine |
| Crash consistent sync completed | Crash consistent sync completed | hbr.primary.DeltaCompletedEvent | Info | Virtual Machine |
| Sync failed to start | Sync failed to start | hbr.primary.FailedToStartDeltaEvent | Error | Virtual Machine |
| Full-sync started | Full-sync started | hbr.primary.SyncStartedEvent | Info | Virtual Machine |
| Full-sync completed | Full-sync completed | hbr.primary.SyncCompletedEvent | Info | Virtual Machine |
| Full-sync failed to start | Full-sync failed to start | hbr.primary.FailedToStartSyncEvent | Error | Virtual Machine |

Table 14-1. vSphere Replication Events (continued)

| Event Name | Event Description | Event Type | Category | Event Target |
|---|---|---|---|---|
| Sync aborted | Sync aborted | hbr.primary.DeltaAbortedEvent | Warning | Virtual Machine |
| No connection to VR Server | No connection to vSphere Replication Server | hbr.primary.NoConnectionToHbrServerEvent | Warning | Virtual Machine |
| Connection to VR Server restored | Connection to VR Server has been restored | hbr.primary.ConnectionRestoredToHbrServerEvent | Info | Virtual Machine |
| vSphere Replication configuration changed | vSphere Replication configuration has been changed | hbr.primary.VmReplicationConfigurationChangedEvent | Info | Virtual Machine |

# Solutions for Common vSphere Replication Problems

Known troubleshooting information can help you diagnose and correct problems with vSphere Replication.

## Error at vService Bindings When Deploying the vSphere Replication Appliance

When you deploy the vSphere Replication appliance, you get an error at vService bindings in the Deploy OVF Template wizard.

### Problem

When you deploy the vSphere Replication, an error appears at vService bindings in the Deploy OVF Template wizard.

```
Unsupported section '{http://www.vmware.com/schema/ovf}vServiceDependencySection'(A vService dependency)
```

### Cause

This error is typically the result of the VMware vService Manager service being paused or stopped.

### Solution

Attempt to start the VMware vService Manager service. If vCenter Server is running as a Linux virtual appliance, reboot the appliance.

## OVF Package Is Invalid and Cannot Be Deployed

When you attempt to deploy OVF for the vSphere Replication appliance, an OVF package error might occur.

#### Problem

The error `OVF package is invalid and cannot be deployed` might appear while you attempt to deploy the vSphere Replication appliance.

#### Cause

This problem is due to the vCenter Server port being changed from the default of 80.

#### Solution

If possible, change the vCenter Server port back to 80.

## vSphere Replication Service Fails with Unresolved Host Error

If the address of vCenter Server is not set to a fully qualified domain name (FQDN) or to a literal address, the vSphere Replication service can stop unexpectedly or fail to start after a reboot.

#### Problem

The vSphere Replication service stops running or does not start after a reboot. The error `unable to resolve host: non-fully-qualified-name` appears in the vSphere Replication logs.

#### Solution

1. In the vSphere Web Client or vSphere Client, select the vCenter Server instance and click the **Configure** tab.
2. Under **Settings**, click **Advanced Settings** and verify that the `VirtualCenter.FQDN` key is set to either a fully qualified domain name or to a literal address.
3. Use a supported browser to log in to the VRMS Appliance Management Interface.

   The URL for the VRMS Appliance Management Interface is https://*vr-appliance-address*:5480.
4. (Optional) Review and confirm the browser security exception to proceed to the login page.
5. Enter the admin user name and password for the appliance.

   You configured the admin password during the OVF deployment of the vSphere Replication appliance.
6. Click **Summary**, and click **Reconfigure**.
7. On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.
8. If prompted, click **Connect** to verify the Platform Services Controller certificate.
9. On the **vCenter Server** page, select the new vCenter Server instance, and click **Next**.
10. On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.
11. On the **Ready to Complete** page, review your settings and click **Finish**.

## Error Recovering Virtual Machine in a Single vCenter Server Instance

You might receive an error message when you are recovering a virtual machine with the same name in a single vCenter Server instance.

### Problem

```
Unable to register the recovered virtual machine VM_name with configuration file
<path_to_vmx_config_file>.
```

### Cause

You cannot recover virtual machines with the same name in the same source and destination folder in the vCenter Server inventory.

### Solution

Recover the virtual machine in a different `VMs and Templates` folder in the same data center. Optionally, after successful recovery, you can remove the old virtual machine from the vCenter inventory and drag the recovered virtual machine to the required virtual machine folder.

## vSphere Replication RPO Violations

You might encounter RPO violations even if vSphere Replication is running successfully at the recovery site.

### Problem

When you replicate virtual machines, you encounter RPO violations.

### Cause

RPO violations might occur for one of the following reasons:

- Network connectivity problems between source hosts and vSphere Replication servers at the target site.
- As a result of changing the IP address, the vSphere Replication server has a different IP address.
- The vSphere Replication server cannot access the target datastore.
- Slow bandwidth between the source hosts and the vSphere Replication servers.

  To calculate bandwidth requirements, see Calculate Bandwidth For vSphere Replication.

### Solution

- Search the `vmkernel.log` at the source host for the vSphere Replication server IP address to see any network connectivity problems.
- Verify that the vSphere Replication server IP address is the same. If it is different, reconfigure all the replications, so that the source hosts use the new IP address.

- Check `/var/log/vmware/*hbrsrv*` at the vSphere Replication appliance at the target site for problems with the server accessing a target datastore.
- Verify that you have sufficient bandwidth.

## vSphere Replication Appliance Extension Cannot Be Deleted

If you delete the vSphere Replication appliance virtual machine, the VRMS Appliance Management Interface is not available to delete the appliance extension that still exists in vCenter Server.

### Problem

Deleting the vSphere Replication appliance does not remove the vSphere Replication extension from vCenter Server.

### Solution

1. Use the Managed Object Browser (MOB) to delete the vSphere Replication extension manually.
2. Redeploy the appliance and reconfigure the replications.

   For more information, see Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted.

## vSphere Replication Does Not Start After Moving the Host

If you move the ESXi Server on which the vSphere Replication appliance runs to the inventory of another vCenter Server instance, vSphere Replication operations are not available. If you reinstall vCenter Server, vSphere Replication operations are also unavailable.

### Problem

If the ESXi Server instance on which vSphere Replication runs is disconnected from vCenter Server and is connected to another vCenter Server instance, you cannot access vSphere Replication functions. If you try to restart vSphere Replication, the service does not start.

### Cause

The OVF environment for the vSphere Replication appliance is stored in the vCenter Server database. When the ESXi host is removed from the vCenter Server inventory, the OVF environment for the vSphere Replication appliance is lost. This action deactivates the mechanisms that the vSphere Replication appliance uses to authenticate with vCenter Server.

### Solution

1. (Optional) If possible, redeploy the vSphere Replication appliance and configure all replications and if possible, reuse the existing .vmdk files as initial copies.
   a. Power off the old vSphere Replication appliances.
   b. Remove any temporary `hbr*` files from the target datastore folders.

c Deploy new vSphere Replication appliances and connect the sites.

d Configure all replications, reusing the existing replica .vmdk files as initial copies.

2 (Optional) If you cannot redeploy the vSphere Replication appliance, use the VRMS Appliance Management Interface to connect vSphere Replication to the original vCenter Server instance.

a Reconnect the ESXi host to vCenter Server.

b Connect to the VRMS Appliance Management Interface of the vSphere Replication server at https://*vr-server-address*:5480 .

3 Click **Summary**, and click **Reconfigure**.

4 On the **Platform Services Controller** page, enter the information about the site where you deployed the vSphere Replication Appliance.

5 If prompted, click **Connect** to verify the Platform Services Controller certificate.

6 On the **vCenter Server** page, select the new vCenter Server instance, and click **Next**.

7 On the **Name and Extension** page, enter the necessary information to register the vSphere Replication Appliance with vCenter Server, and add a storage traffic IP address.

8 On the **Ready to Complete** page, review your settings and click **Finish**.

9 If you use the VRMS Appliance Management Interface solution, you must repeat the steps each time that you change the vSphere Replication certificate.

## Unexpected vSphere Replication Failure Results in a Generic Error

vSphere Replication includes a generic error message in the logs when certain unexpected failures occur.

### Problem

Certain unexpected vSphere Replication failures result in the error message

```
A generic error occurred in the vSphere Replication Management Server.
```

In addition to the generic error, the message provides more detailed information about the problem, similar to the following examples.

- `A generic error occurred in the vSphere Replication Management Server. Exception details: 'org.apache.http.conn.HttpHostConnectException: Connection to https://vCenter_Server_address refused'`. This error relates to problems connecting to vCenter Server.
- `Synchronization monitoring has stopped. Please verify replication traffic connectivity between the source host and the target vSphere Replication Server. Synchronization monitoring will resume when connectivity issues are resolved`. This problem relates to a synchronization operation error.

### Cause

vSphere Replication sends this message when it encounters configuration or infrastructure errors. For example, network issues, or host overload.

### Solution

Check the `Exception details` message for information about the problem. Depending on the details of the message, you can choose to retry the failed operation, restart vSphere Replication, or correct the infrastructure.

## Reconnecting Sites Fails If One of the vCenter Server Instances Has Changed Its IP Address

When the vCenter Server address of one site changes, the connection status between two sites is displayed as `Not connected` and you cannot reconnect the sites.

### Problem

If you have two connected sites, and the vCenter Server address of either site changes, the connection status `Not connected` appears and you cannot reconnect the sites.

### Solution

1. Log in the VRMS Appliance Management Interface for the vSphere Replication appliance that is registered to the vCenter Server whose address has changed.
2. Reconfigure the vSphere Replication appliance with the new vCenter Server address. See Configure the vSphere Replication Appliance to Connect to a vCenter Server.
3. In the vSphere Replication user interface, from the list of target sites, select the connection that indicates the `Not connected` status.
4. Select **Site Pair > Summary**, and click **Reconnect**.
5. Select the services you want to pair. Enter the address of the Platform Services Controller on the remote site, provide the vCenter Single Sign-On user name and password, and click **Reconnect**.

   If the Platform Services Controller manages more than one vCenter Server instance, the other vCenter Server instances appear in the list but you cannot select a different instance. You can only select the vCenter Server instance that vSphere Replication already extends.
6. Verify that the connection between the two sites is successfully restored and the status is `Connected`.

## vSphere Replication Server Registration Takes Several Minutes

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

#### Problem

If the vCenter Server inventory contains a few hundred or more hosts, the Register VR Server task takes more than a few minutes to complete.

#### Cause

vSphere Replication updates the SSL thumbprint registry of each host. The vCenter Server Events pane displays `Host is configured for vSphere Replication` for each host as the vSphere Replication server registration task progresses.

#### Solution

1. Wait for the registration task to complete.

   After it finishes, you can use vSphere Replication for incoming replication traffic.

2. Alternatively, edit `/opt/vmware/hms/conf/hms-configuration.xml` and change the `hms-config-host-at-hbr-threadpool-size` parameter to a higher value to enable parallel processing of more hosts at a time and restart the vSphere Replication management server `/etc/init.d/hms restart`

## Generating Support Bundles Disrupts vSphere Replication Recovery

If you generate a vSphere Replication log bundle and at the same time attempt to run a recovery, the recovery might fail.

#### Problem

In heavily loaded environments, generating log bundles can cause vSphere Replication connection problems during recovery operations. Recovery fails with the error

```
A generic error occurred in the vSphere Replication Management Server. Exception details:
'Failed write-locking object: object_ID'.
```

#### Cause

vSphere Replication server is blocked when the log bundle is generated. This situation occurs if the storage for the vSphere Replication virtual machine is overloaded.

#### Solution

Rerun the recovery. If the recovery still fails, reevaluate the storage bandwidth requirements of the cluster on which vSphere Replication is running, and the network bandwidth if the storage is NAS.

## vSphere Replication Operations Take a Long Time to Complete

Some vSphere Replication operations might take a long time to complete during a heavy load.

#### Problem

Operations such as recovering virtual machines fail with the following error:

```
Object object_GUID is locked by another ongoing operation in vSphere Replication Management
Server. Try again later.
```

#### Cause

When running under heavy load, some vSphere Replication operations might take a longer time to complete and other operations can fail with this error because a background update operation on the replication group is slow and holds a lock on the replication for a long time.

#### Solution

Retry the failed operation after a few minutes.

## vSphere Replication Operations Fail with Authentication Error

An error message appears when you try to configure a replication between two sites, though the sites are paired.

#### Problem

If two sites are paired, and, while the vSphere Web Client is open on the source site, you restart the vCenter Server and the vSphere Replication Management Server on the target site, when you try to configure a replication from the source to the target site, the configuration task fails with the following error message:

```
Cannot verify login credentials. The authentication service infrastructure is
not responding..
```

The following error message appears in the HMS log file on the restarted target site:

```
The VMOMI call does not contain an HMS session ID.
```

The following error message appears in the HMS log file on the source site:

```
Cannot check login credentials. Authentication service infrastructure failed.
```

#### Cause

When you establish a connection between two sites, the connection is cached in the user session on both sites. When you restart the vCenter Server and the vSphere Replication Management Server on the target site, the information about user sessions is discarded. Because the vSphere Web Client is open and connected to the source site, the login data remains cached in the vSphere Replication Management Server. When you configure a replication, the source site tries to connect to the target site using the cached login data. The target site interprets that data as stale and stops the reconnecting thread.

#### Solution

- Refresh the Site Recovery user interface.

- Log out the Site Recovery user interface and log back in.

## vSphere Replication Does Not Display Incoming Replications When the Source Site Is Inaccessible

The list of incoming replications between two remote sites fails to populate when the connection to the local site is refused.

### Problem

When you refresh the incoming replications list on a remote site soon after the connection to the local site has become unavailable, the replications do not display due to a communication error between the two sites.

### Solution

Refresh the Site Recovery user interface. Alternatively, log out and log in again.

## vSphere Replication Is Inaccessible After Changing vCenter Server Certificate

If you change the SSL certificate of vCenter Server, you cannot access vSphere Replication.

### Problem

vSphere Replication uses certificate-based authentication to connect to vCenter Server. If you change the vCenter Server certificate, vSphere Replication is inaccessible.

### Cause

The vSphere Replication database contains the old vCenter Server certificate.

### Solution

1. In the vSphere Web Client, right-click the vSphere Replication Management Server virtual machine and power it off and on.
2. Log into the VRMS Appliance Management Interface of the vSphere Replication appliance and click **Summary > Restart**.

   Do not change any configuration information before clicking **Restart**.

   vSphere Replication restarts with the new vCenter Server certificate.

## vSphere Replication Cannot Establish a Connection to the Hosts

Replications fail because vSphere Replication cannot connect to the hosts.

### Problem

vSphere Replication needs access to port 80. You might see forbidden HTTP connections in the vSphere Replication logs.

### Solution

Make sure the vSphere Replication appliance has access to port 80 on the storage hosts.

For a list of ports that must be open for vSphere Replication, see Services, Ports, and External Interfaces That the vSphere Replication Virtual Appliance Uses.

## Anti-Virus Agent in Firewall Stops Virtual Machine Replication

If a virtual machine contains virus information, an anti-virus agent in the firewall might detect the virus data and stop the connection during replication.

### Problem

When you reconfigure the replication and start a full sync, the replication stops in the same data block with the virus information in it unless the virus data has moved on the disk. Clones of the disk fail, but other virtual machines of the same size and configuration from the same host replicating to the same destination datastore replicate successfully.

### Solution

Remove the virus information from the replicated guest to avoid replicating virus information.

Make an exception in the anti-virus rules in the firewall to allow the replication to proceed.

## Initial Full Synchronization of Virtual Machine Files to VMware vSAN Storage Is Slow

When using VMware vSAN storage and configuring vSphere Replication on multiple virtual machines, the initial full synchronization takes a long time to complete.

### Problem

Configuring vSphere Replication on a large number of virtual machines simultaneously when using vSphere Replication with vSAN storage causes the initial full synchronization of the virtual machine files to run very slowly.

### Cause

Initial full synchronization operations generate heavy I/O traffic. Configuring too many replications at the same time can overload the vSAN storage.

### Solution

Configure vSphere Replication in batches of a maximum of 20 virtual machines at a time.

## Configuring Replication Fails Because Another Virtual Machine Has the Same Instance UUID

You cannot configure a replication because another virtual machine already exists at the target site.

### Problem

You might see the following error message:

```
Unable to configure replication for virtual machine VM_name because group group_name cannot
be created.
Another virtual machine configured_VM_name}' that has the same instance UUID instance_UUID
already exists on protection site source_site_name.
```

### Cause

This error message might appear on the following occasions.

- If, due to a connectivity issue or some other problem, an orphaned replication remains on one of the sites while it is deleted from the other site, the orphaned replication prevents you from configuring a new replication for the same virtual machine.
- If you have paired two sites and reinstall the vSphere Replication Management server appliance, the other site contains information about the old appliance and database, and prevents you from configuring new replications.

### Solution

- If you have not reinstalled the vSphere Replication Management server, an orphaned replication exists in your environment. You can force stop this replication to delete it.
  a Log in to the vSphere Client or vSphere Web Client.
  b On the home page, click **Site Recovery** and click **Open Site Recovery**.
  c On the Site Recovery home page, select the site pair which contains the protected site, mentioned in the error message that you received.
  d Click the **Replications** tab and select a replication from **Outgoing** or **Incoming**.
  e Click the **Remove** icon and select **Force stop replication(s)**.
- Alternatively, you can use the Managed Object Browser (MOB) of the vSphere Replication Management server to delete the replication.
  a Navigate to https://*vrms_address*:8043/mob/?vmodl=1

  Where *vrms_address* is the IP address of the vSphere Replication Management server.
  b Click the **content** value.
  c Select the replicaManager or replicationManager value, depending on the type of replication you want to delete.
  - For an outgoing replication, click **replication-manager > getOutgoingReplications**.
  - For an incoming replication, click **replica-manager > getIncomingReplications**.

d Set the relevant **start**, **count**, **sorters**, and **filter** values.

**Note** You must set the **start** value to *0* and delete the **sorters** and **filter** values, to invoke the first page of maximum 50 listed replications. For more than 50 replications, you can use paging and make additional calls for the next pages of replications or use the **sorters** and **filter** values.

e Click **Invoke Method**.

f Locate the replication and click the GID link under **replication** value.

g Invoke the **destroy** method to remove the replication.

- If the vSphere Replication Management server on one of the sites was reinstalled or otherwise reset:
  a Reinstall the vSphere Replication Management server at the other site or reset its database.
  b Connect the sites and register any additional vSphere Replication server appliances.
  c Remove any temporary `hbr*` files left over from the target datastore folders.
  d Configure all replications, reusing the existing replica .vmdk files as replication seeds.

## vSphere Replication Operations Run Slowly as the Number of Replications Increases

As you increase the number of virtual machines that you replicate, vSphere Replication operations can run more slowly.

### Problem

Response times for vSphere Replication operations can increase as you replicate more virtual machines. You possibly experience recovery operation timeouts or failures for a few virtual machines, and RPO violations.

### Cause

Every virtual machine in a datastore generates regular read and write operations. Configuring vSphere Replication on those virtual machines adds another read operation to the regular read and write operations, which increases the I/O load on the storage. The performance of vSphere Replication depends on the I/O load of the virtual machines that you replicate and on the capabilities of the storage hardware. If the load generated by the virtual machines, combined with the extra I/O operations that vSphere Replication introduces, exceeds the capabilities of your storage hardware, you might experience slow response times.

### Solution

When running vSphere Replication, if response times are greater than 30 ms, reduce the number of virtual machines that you replicate to the datastore. Alternatively, increase the capabilities of your hardware. If you suspect that the I/O load on the storage is an issue and you are using VMware vSAN storage, monitor the I/O latency by using the monitoring tool in the vSAN interface.

## Unable to Establish an SSH Connection to the vSphere Replication Appliance

SSH connections to the vSphere Replication appliance are deactivated.

### Prerequisites

Verify that you have the root user credentials to log in to the vSphere Replication appliance.

### Problem

To apply custom settings to vSphere Replication, you must establish an SSH connection to the vSphere Replication appliance, and modify certain configuration files.

To transfer files from and to the vSphere Replication appliance, you use SCP or SFTP protocol.

Because the SSH connections are deactivated, you cannot apply the changes that you need, and you cannot transfer files.

### Cause

By default, SSH connections to the vSphere Replication appliance are deactivated to strengthen the security in your environment.

### Solution

1. In the vSphere Web Client, right-click the vSphere Replication Management (HMS) virtual machine, and select **Open Console**.
2. Log in as the root user, and run the following script.

   ```
   /opt/vmware/bin/enable-sshd.sh
   ```

### Procedure

The script configures the vSphere Replication appliance to activate SSH connections.

## The Replication Pauses When You Add a New Disk to the Source VM

The replication pauses when you add a new disk to the source virtual machine.

### Problem

When you add a new disk to the source VM and you have deactivated the automatic replication of new disks, the replication pauses.

#### Cause

vSphere Replication detects the addition of a disk to a VM and generates an event such as `vSphere Replication handled a disk addition on a virtual machine`.

#### Solution

Include or exclude the new disk in the replication.

You can set up and view an alarm for the event by using the vSphere Web Client. See the *vSphere Administration with the vSphere Client* documentation for details.

## The vSphere Replication Appliance Root File System Switches to Read-Only Mode and Login Fails

The vSphere Replication appliance root file system switches to `read-only` mode, and you cannot log in.

#### Problem

vSphere Replication server cannot update its database and becomes unresponsive. Log in through VRMS Appliance Management Interface, SSH, or console fails. Attempts to use the appliance console to log in result in the following error message:

`Read-only file system`.

#### Cause

To prevent data corruption the vSphere Replication appliance is configured to put its root file system in `read-only` mode when it detects a problem with the underlying storage.

#### Solution

1. Resolve the storage problem or use Storage vMotion to migrate the vSphere Replication appliance to another storage.
2. Reboot the vSphere Replication appliance.
3. Verify that you can log in by using the VRMS Appliance Management Interface and the appliance console.

## Configuration of an Encrypted VM Fails with an Error

When you try to configure a replication for an encrypted virtual machine, the process fails with an error.

The message that you see is: "`The replication of encrypted virtual machines requires Secure LWD support. Secure LWD is not available for this VM.`".

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 you deployed the appliance. The automatic installation of the VIB file might fail due to different reasons.

To configure a replication for the encrypted VM, you must verify that the VIB file is installed and running on the ESXi host of the source virtual machine. If not, you must manually install it.

## Verify the VIB File Installation

### Procedure

1. Run the shell command `esxcli software vib list` on the source ESXi host.
2. In the results, look for the `vmware-hbr-agent` VIB file.

### What to do next

If the VIB file is not available on the source ESXi host, you must install it manually. See Manually Install the VIB File.

## Manually Install the VIB File

### Solution

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. Enable the firewall on the ESXi host.