VMware vSphere Replication Administration

vSphere Replication 6.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001462-01

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2012–2015 VMware, Inc. All rights reserved. Copyright and trademark information.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

vSphere Replication Administration 5

Updated Information 7

1 Overview of VMware vSphere Replication 9
- Contents of the vSphere Replication Appliance 10
- vSphere Replication Client Plug-In 10
- Source and Target Sites 11
- How vSphere Replication Works 11
- Isolating the Network Traffic of vSphere Replication 13
- Replication Data Compression 17

2 vSphere Replication Roles and Permissions 19
- Assign vSphere Replication Roles to Users 19
- Assign VRM Replication Viewer Role 19
- Assign VRM Virtual Machine Replication User Role 20
- Assign VRM Virtual Machine Recovery User Role 20
- Clone Existing VRM Administrator Role and Modify Privileges 21
- vSphere Replication Roles Reference 21

3 vSphere Replication System Requirements 25
- vSphere Replication Licensing 25
- vSphere Replication Network Ports 26
- Operational Limits of vSphere Replication 26
- Compatibility of vSphere Replication with Other vSphere Features 26
- vSphere Replication Compatibility with Other Software 28
- Bandwidth Requirements for vSphere Replication 28

4 Installing and Uninstalling vSphere Replication 31
- Install vSphere Replication 32
- Uninstall vSphere Replication 39
- Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted 40

5 Deploying Additional vSphere Replication Servers 43
- Deploy an Additional vSphere Replication Server 43
- Register an Additional vSphere Replication Server 44
- Reconfigure vSphere Replication Server Settings 44
- Unregister and Remove a vSphere Replication Server 45
- Disable the Embedded vSphere Replication Server 46

6 Upgrading vSphere Replication 47
Upgrade vSphere Replication by Using the Downloadable ISO Image 47
Update the vCenter Server IP Address in the vSphere Replication Management Server 49

7 Reconfigure the vSphere Replication Appliance 51
Reconfigure General vSphere Replication Settings 52
Change the SSL Certificate of the vSphere Replication Appliance 52
Change the Password of the vSphere Replication Appliance 55
Change Keystore and Truststore Passwords of the vSphere Replication Appliance 55
Configure vSphere Replication Network Settings 56
Configure vSphere Replication System Settings 58
Reconfigure vSphere Replication to Use an External Database 58
Use the Embedded vSphere Replication Database 61

8 Replicating Virtual Machines 63
How the Recovery Point Objective Affects Replication Scheduling 64
How Retention Policy Works 64
Replicating a Virtual Machine and Enabling Multiple Point in Time Instances 66
Using vSphere Replication with Virtual SAN Storage 66
Using vSphere Replication with vSphere Storage DRS 68
How vSphere Replication Synchronizes Data Between vCenter Server Sites During Initial Configuration 68
Replicating Virtual Machines Using Replication Seeds 69
Replicating a Virtual Machine in a Single vCenter Server Instance 70
Configure Replication for a Single Virtual Machine to vCenter Server 70
Configure Replication for Multiple Virtual Machines to vCenter Server 72
Move a Replication to a New vSphere Replication Server 74
Stop Replicating a Virtual Machine 74
Reconfiguring Replications 76

9 Performing a Recovery with vSphere Replication 79
Recover Virtual Machines by Using vSphere Replication 79
Failback of Virtual Machines in vSphere Replication 81

10 Monitoring and Managing Replications in vSphere Replication 83
View the Replication Summary for a Site 83
View Replication Reports for a Site 84
Identifying Replication Problems in the Issues Tab 87
Manage Target Sites 87
Manage vSphere Replication Servers 88

11 Troubleshooting vSphere Replication 89
vSphere Replication Limitations 89
Access the vSphere Replication Logs 90
vSphere Replication Events and Alarms 91
Solutions for Common vSphere Replication Problems 94

Index 109

vSphere Replication Administration

vSphere Replication Administration provides information about installing, configuring, and using VMware vSphere Replication.

Intended Audience

This information is intended for anyone who wants to protect the virtual machines in their virtual infrastructure by using vSphere Replication. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Updated Information

vSphere Replication Administration is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Replication Administration*.

Revision	Description
EN-001462-01	■ Updated the information about the change of the IP address of the vSphere Replication server in topics "Configure vSphere Replication Network Settings," on page 56, "Reconfigure vSphere Replication Server Settings," on page 44, and "Isolating the Network Traffic of vSphere Replication," on page 13. ■ Updated the information in topic "vSphere Replication Limitations," on page 89. ■ Corrected the information in the topic "Configuring Replication Fails Because Another Virtual Machine has the Same Instance UUID," on page 105. ■ Corrected the Prerequisites in "Configure vSphere Replication Connections," on page 36. ■ Added information about the consequences of stopping a replication in "Stop Replicating a Virtual Machine," on page 74. ■ Added troubleshooting topic"The Replication Pauses When You Add a New Disk To the Source VM," on page 108.
EN-001462-00	Initial release.

Overview of VMware vSphere Replication 1

VMware vSphere Replication is an extension to VMware vCenter Server that provides 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 lower cost per virtual machine.
- A replication solution that allows flexibility in storage vendor selection at the source and target sites.
- Overall lower cost per replication.

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.

With vSphere Replication, you can replicate virtual machines from a source datacenter 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 choose the virtual machines to be replicated at a different recovery point objective (RPO). You can enable 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 Virtual SAN datastores as target datastores and choose destination storage profiles for the replica virtual machine and its disks when configuring replications.

NOTE VMware Virtual SAN is a fully supported feature of vSphere 5.5 Update 1 and later.

You can configure all vSphere Replication features in the vSphere Web Client. You can manage sites monitor the status of a replication through the replication management and monitoring dashboard.

- Contents of the vSphere Replication Appliance on page 10

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

- vSphere Replication Client Plug-In on page 10

  The vSphere Replication appliance adds a plug-in to the vSphere Web Client.

- Source and Target Sites on page 11

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

- How vSphere Replication Works on page 11

  With vSphere Replication, you can configure 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.

- Isolating the Network Traffic of vSphere Replication on page 13

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

- Replication Data Compression on page 17

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

Contents of the vSphere Replication Appliance

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

- A plug-in to the vSphere Web Client that provides a user interface for vSphere Replication.
- An embedded database that stores replication configuration and management information.
- 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.

You can use vSphere Replication immediately after you deploy the appliance. The vSphere Replication appliance provides a virtual appliance management interface (VAMI) that you can use to reconfigure the appliance after deployment, if necessary. For example, you can use the VAMI to change the appliance security settings, change the network settings, or configure an external database. You can deploy additional vSphere Replication Servers using a separate .ovf package.

vSphere Replication Client Plug-In

The vSphere Replication appliance adds a plug-in to the vSphere Web Client.

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

- Configure connections between vSphere Replication sites.
- View all vCenter Server instances that are registered with the same SSO and status of each vSphere Replication extension.
- Deploy and register additional vSphere Replication servers.
- Configure the replication of individual or multiple virtual machines.
- View incoming and outgoing replications.
- Monitor and manage the status of the replications.
- Recover virtual machines.

Source and Target Sites

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

The source site can be any site where vCenter Server supports a critical business need. The target site can be in another location, or in the same facility to establish redundancy. The target site is usually located in a facility that is unlikely to be affected by environmental, infrastructure, or other disturbances that might affect the source site.

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

- Each site must have at least one data center.
- The target site must have hardware, network, and storage resources that can support the same virtual machines and workloads as the source site.
- The sites must be connected by a reliable IP network.
- The target site must have access to networks (public and private) comparable to those on the source site, although not necessarily the same range of network addresses.

Connecting Source and Target 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 SSO domain, you need to select the target site only, without providing authentication details, because you are already logged in.

When you connect sites that belong to different SSO domains, the vSphere Replication Management Server must register with the Platform Services Controller (PSC) on the target site. You must provide authentication details for the target site, including IP or FQDN of the server where PSC runs, and user credentials. See "Configure vSphere Replication Connections," on page 36.

After connecting the sites, you can monitor the connectivity state between them on the **Target Sites** tab.

How vSphere Replication Works

With vSphere Replication, you can configure 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, where they 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 amount of time and bandwidth required for the initial replication.

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

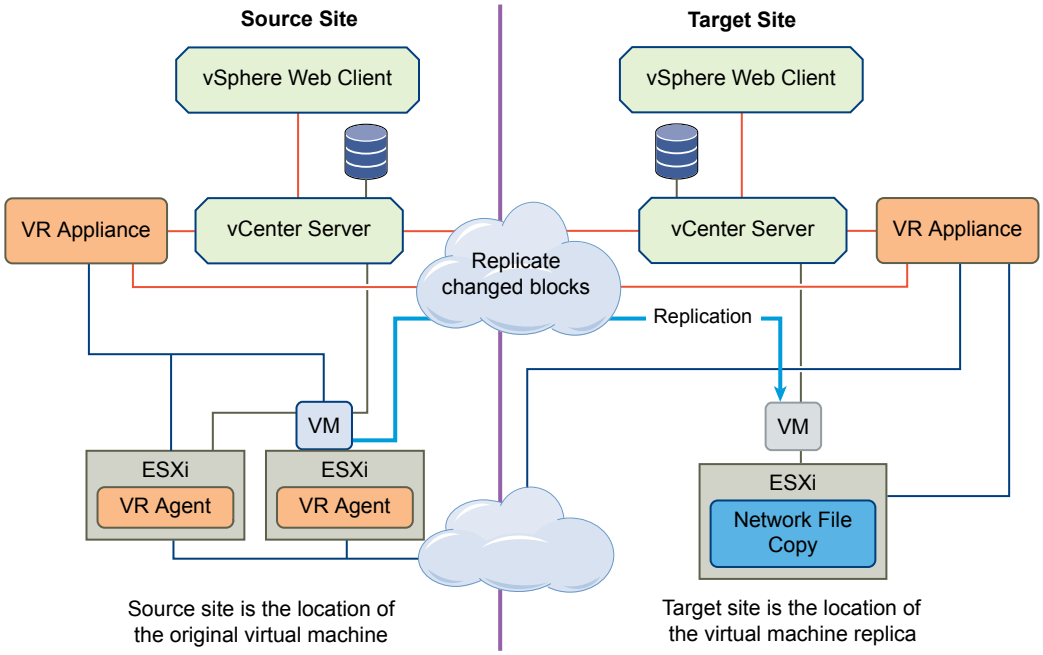
As administrator, you can monitor and manage the status of the replication. You can view information for incoming and outgoing replications, source and target site status, replication issues, and for warnings and errors.

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 also configure vSphere Replication to use an external database.

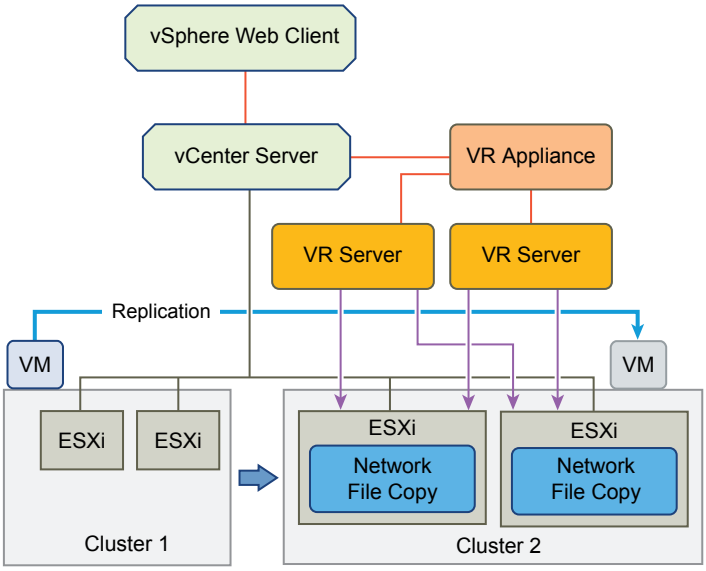
You can replicate a virtual machine between two sites. vSphere Replication is installed on both source and target sites. Only one vSphere Replication appliance is deployed on each vCenter Server. You can deploy additional vSphere Replication Servers.

Figure 1-1. Replication Between Two Sites



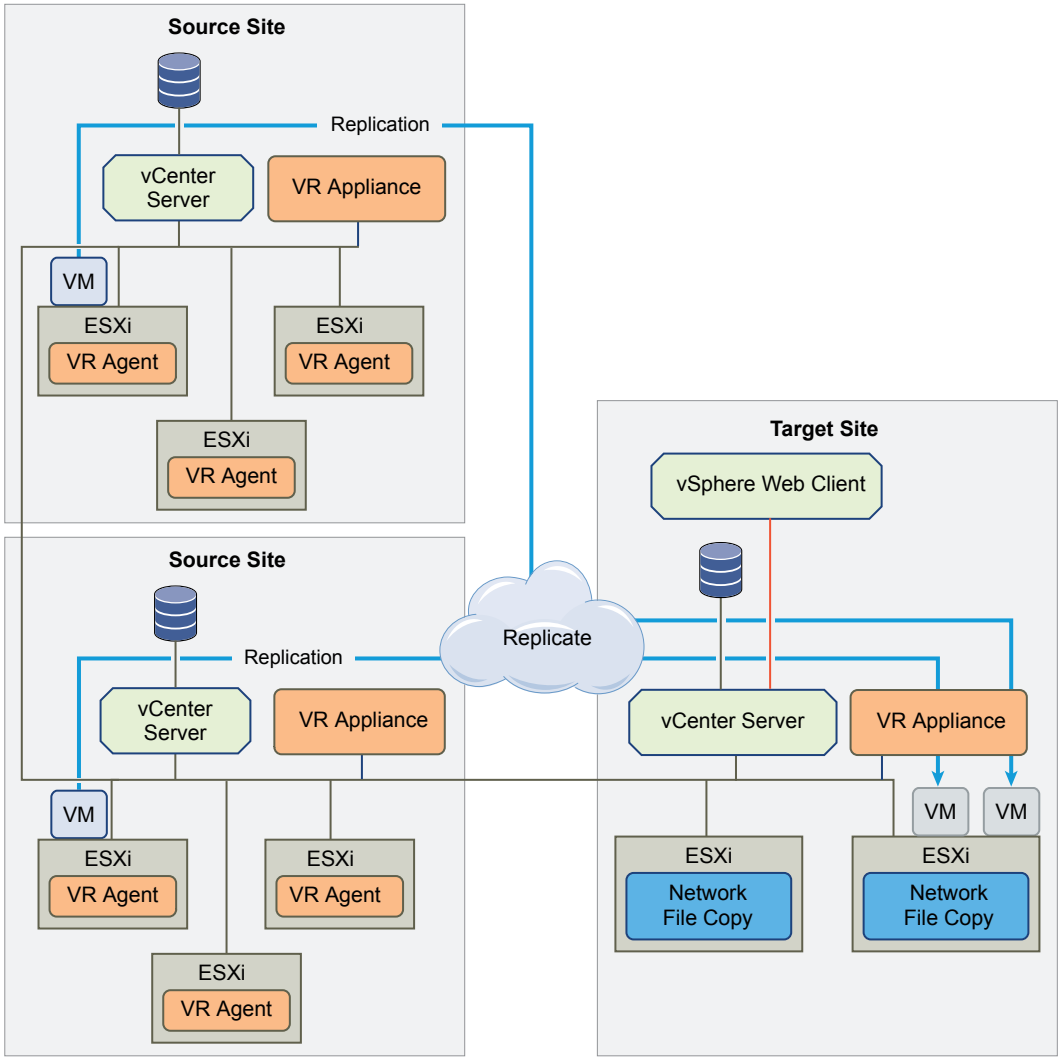
You can add multiple Additional vSphere Replication servers in a single vCenter Server to replicate virtual machines to other clusters.

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



Isolating the Network Traffic of vSphere Replication

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, and helps you enhance the network performance in the data center, because the traffic that vSphere Replication generates does not impact other types of traffic. 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," on page 14.

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.

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

In the combined 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, you must manually reconfigure replications on the source site to point to the new IP address.

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 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. Under **Manage**, select **Networking**, and select **VMkernel adapters**.
3. Click the **Add host 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 traffic** and click **Next**.
8. Apply the IP settings, click **Next**, and **Finish** to complete the wizard.

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 VAMI 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 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. Under **Manage**, select **Networking**, and select **VMkernel adapters**.
3. Click the **Add host 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 NFC traffic** and click **Next**.
8. Apply the IP settings, click **Next**, and **Finish** to complete the wizard.

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.

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 that is used by the vSphere Replication server for replication traffic, and by the vCenter Server for virtual machine management.

The IP address that is used for vSphere Replication management traffic is localhost 127.0.0.1. Because the default VM network adapter is used for different types of traffic, you can add a second adapter to the appliance, and configure vSphere Replication to use the second adapter only for incoming replication traffic.

Prerequisites

- Verify that the vSphere Replication virtual appliance is deployed and registered with the vCenter Server.

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, select **Network**, and click **Add**.

      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 IP 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 check the IP address of the new NIC.

4 Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.

5 On the **VR** tab, click **Configuration**.

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

7 Click **Apply Network Settings**.

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

Create VM Network Adapters to Isolate the Network Traffic of a vSphere Replication Server

By default, the vSphere Replication Server appliance has one VM network adapter that is used by the vSphere Replication Server for management and replication traffic.

Because the default VM network adapter is used for different types of traffic, you can add network adapters to the appliance, and configure vSphere Replication to use a separate adapter 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.

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, select **Network**, and click **Add**.

      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 IP address automatically.

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

2 Repeat Step 1 to add another VM NIC.

3 Power on the vSphere Replication appliance.

4 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 check the IP addresses of the new NICs.

5 Use a supported browser to log in to the vSphere Replication VAMI.

The URL for the VAMI is https://*vr-appliance-address*:5480.

6 On the **VRS** tab, click **Configuration**.

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 to be used by the vSphere Replication Server for incoming replication data.
IP Address for VRMS Management Traffic	The IP address to be used by the vSphere Replication Management Server to manage the vSphere Replication Server.

8 Click **Apply Network Settings**.

The different types of traffic that vSphere Replication generates are handled by separate NICs.

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.

Data Compression Support

vSphere Replication 6.0 supports end-to-end compression when the source and target ESXi hosts are also version 6.0. The support of data compression for all other use cases depends on the versions of source and target ESXi hosts. The vSphere Replication servers on both the source and target sites must be 6.0.

Table 1-1. Support for Data Compression Depending on Other Product Versions

Source ESXi host	ESXi Host that Manages the Target Datastore	Data Compression Support
Earlier than 6.0	Any supported version	vSphere Replication does not support data compression for the source ESXi host, so the option **Enable network compression for VR data** is disabled in the Configure Replication wizard.
6.0	Earlier than 6.0	The ESXi host on the source site sends compressed data packets to the vSphere Replication server on the target site. The vSphere Replication server searches the target site for ESXi 6.0 hosts that can decompress the data. If no 6.0 hosts are available for the target datastore, the vSphere Replication server uses the resources of the vSphere Replication appliance to decompress the data, and sends the uncompressed data to the ESXi host.
6.0	6.0	This is an environment that supports full end-to-end compression. The ESXi host on the source site compresses the data, and the vSphere Replication server on the target site passes the data off to the ESXi host where the host decompresses the data and writes it to disk.

Data Compression and vSphere vMotion

If data compression is disabled, you can perform vMotion operations on replication source machines between any pair of hosts that support vMotion and vSphere Replication.

When data compression is enabled, if both the source and the target ESXi hosts support data compression, vMotion operations can be performed as usual. However, if the target ESXi host is earlier than 6.0, vSphere Replication prevents vMotion from moving replication source VMs to that host because it does not support data compression. This prevents DRS from performing automated vMotion operations to hosts that do not support compression. Therefore, if you need to move a replication source VM to an ESXi host earlier than 6.0, before you perform the vMotion operation, you must reconfigure the replication to disable data compression.

vSphere Replication Roles and Permissions

2

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

This chapter includes the following topics:

- "Assign vSphere Replication Roles to Users," on page 19
- "Assign VRM Replication Viewer Role," on page 19
- "Assign VRM Virtual Machine Replication User Role," on page 20
- "Assign VRM Virtual Machine Recovery User Role," on page 20
- "Clone Existing VRM Administrator Role and Modify Privileges," on page 21
- "vSphere Replication Roles Reference," on page 21

Assign vSphere Replication Roles to Users

You create roles and assign permissions for vSphere Replication in the same way as you do in vCenter.

See vSphere Users and Permissions in vSphere Security.

Assign VRM Replication Viewer Role

In this example, you create a vSphere Replication user that can view replication sites and 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 > Manage > 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.

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

In this example, you create a vSphere Replication user who can only configure 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 > Manage > 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.

Selecting a datastore for which the user lacks the **Target datastore user** role results in the error message `Permission to perform this operation was denied.`

Assign VRM Virtual Machine Recovery User Role

In this example, you create a vSphere Replication user who 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.

Procedure

1. Log in as the Administrator user on the target site.
2. Select **vCenter > Manage > Permissions** and assign to this user the **VRM virtual machine recovery user** role with the propagate option.
3. Log in as that user on the target site.
4. Select **Monitor > vSphere Replication > Incoming Replications**, select the replication, and start recovery.
5. Select **Recover with latest available data** and follow the prompts to finish the recovery.

Clone Existing VRM Administrator Role and Modify Privileges

In this example, you create a vSphere Replication user who cannot modify the replication infrastructure. The user cannot register additional vSphere Replication servers.

Prerequisites

- Verify that you have a replication site.
- Verify that you have another user account.

Procedure

1. Log in as the Administrator user and clone the **VRM Administrator** role.
2. In the cloned role, remove the **Manage VR** privileges.
3. Select **vCenter > Manage > Permissions** and assign the cloned user with **Propagate** privilege.
4. Log in as the cloned user and select **Manage > vSphere Replication > Replication Servers**.

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

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 2-1. 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. ■ Cannot change replication parameters.	**VRM remote.View VR** **VRM remote.View VRM** **VRM datastore mapper.View** **Host.vSphere Replication.Manage replication** **Virtual machine.vSphere Replication.Monitor replication**	vCenter Server root folder with propagation, at source site (outgoing replications) and target site (incoming replications). 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. ■ Manage datastores. ■ Configure and unconfigure replications. ■ Manage and monitor replications. ■ View defined storage capabilities and storage profiles. Requires a corresponding user with the same role on the target site and additionally vSphere Replication target datastore user role on the target datacenter, or datastore folder or each target datastore.	**Datastore.Browse Datastore** **VRM remote.View VR** **VRM remote.View VRM** **VRM datastore mapper.Manage** **VRM datastore mapper.View** **Host.vSphere Replication.Manage replication** **Virtual machine.vSphere Replication.Configure replication** **Virtual machine.vSphere Replication.Manage replication** **Virtual machine.vSphere Replication.Monitor replication** **Profile-driven storage .Profile-driven storage view**	vCenter Server root folder with propagation on both sites. 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 2-1. 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** **VRM remote.View VR** **VRM remote.Manage VRM** **VRM remote.View VRM** **VRM datastore mapper.Manage** **VRM datastore mapper.View** **VRM diagnostics .Manage** **VRM session .Terminate** **Datastore.Browse datastore** **Datastore.Low level file operations** **Host.vSphere Replication.Manage replication** **Resource.Assign virtual machine to resource pool** **Virtual machine.Configuration.Add existing disk** **Virtual machine.Configuration.Add or remove device** **Virtual machine.Interaction.Power On** **Virtual machine.Interaction.Device connection** **Virtual machine.Inventory.Register** **Virtual machine.vSphere Replication.Configure replication** **Virtual machine.vSphere Replication.Manage replication** **Virtual machine.vSphere Replication.Monitor replication** **Profile-driven storage .Profile-driven storage view**	vCenter Server root folder with propagation on both sites. 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** **VRM remote.View VRM** **VRM diagnostics .Manage**	vCenter Server root folder on both sites.

Table 2-1. 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. Used on target site in combination with the VRM virtual machine replication user role on both sites.	**Datastore.Browse datastore** **Datastore.Low level file operations**	Datastore objects on target site, or datastore folder with propagation at target site, or target datacenter with propagation.
VRM virtual machine recovery user	Recover virtual machines.	**Datastore.Browse datastore** **Datastore.Low level file operations** **Host.vSphere Replication.Manage replication** **Virtual machine.Configuration.Add existing disk** **Virtual machine.Configuration.Add or remove device** **Virtual machine.Interaction.Power On** **Virtual machine.Interaction.Device connection** **Virtual machine.Inventory.Register** **Resource.Assign virtual machine to resource pool**	Secondary vCenter Server root folder with propagation. Alternatively, secondary vCenter Server root folder without propagation, target datastore without propagation, target virtual machine folder with propagation, target host or cluster with propagation.

vSphere Replication System Requirements

3

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 CPU, a 16 GB and a 2 GB hard disk, and 4 GB of RAM. Additional vSphere Replication servers require 716 MB 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.

This chapter includes the following topics:

- "vSphere Replication Licensing," on page 25
- "vSphere Replication Network Ports," on page 26
- "Operational Limits of vSphere Replication," on page 26
- "Compatibility of vSphere Replication with Other vSphere Features," on page 26
- "vSphere Replication Compatibility with Other Software," on page 28
- "Bandwidth Requirements for vSphere Replication," on page 28

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

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 replication for virtual machines on that host, the replication fails with a licensing error.

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

vSphere Replication Network Ports

vSphere Replication uses default network ports for intrasite communication between hosts at a single site and intersite communication between hosts at the protected and recovery sites.

For a list of all the ports that must be open for vSphere Replication, see http://kb.vmware.com/kb/2087769.

For the list of default ports that all VMware products use, see http://kb.vmware.com/kb/1012382.

Operational Limits of vSphere Replication

vSphere Replication has certain operational limits.

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

- You can only deploy one vSphere Replication appliance on a vCenter Server instance. When you deploy another vSphere Replication appliance, during the boot process vSphere Replication detects another appliance already deployed and registered as an extension to vCenter Server. You have to confirm if you want to proceed with the new appliance and recreate all replications or shut it down and reboot the old appliance to restore the original vSphere Replication extension thumbprint in vCenter Server.
- Each newly deployed vSphere Replication appliance can manage a maximum of 2000 replications. See http://kb.vmware.com/kb/2102453 for more information.
- Upgraded vSphere Replication appliances that use the embedded vSphere Replication database require additional configuration to enable the support of a maximum of 2000 replications. See http://kb.vmware.com/kb/2102463. No additional configuration is required for vSphere Replication appliances that are configured to use an external database.

Compatibility of vSphere Replication with Other vSphere Features

vSphere Replication is compatible with certain other vSphere management features.

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

NOTE You cannot upgrade VMware Tools in the vSphere Replication appliance.

Table 3-1. 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.
vSphere Fault Tolerance	No	vSphere Replication cannot replicate virtual machines that have fault tolerance enabled. You cannot protect the vSphere Replication appliance itself with FT.
vSphere DRS	Yes	Replication continues at the defined RPO after 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. On the target site, you must register the vSphere Replication appliance with the SSO service to enable the communication between Storage DRS and the vSphere Replication Management server. See "Register the vSphere Replication Appliance with vCenter Single Sign-On," on page 34.
VMware Virtual SAN datastore	Yes	You can use VMware Virtual SAN datastores as the source and target datastore when configuring replications. **Note** VMware Virtual SAN is a fully supported feature of vSphere 5.5 Update 1 and later.
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 disable 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 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 disables 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.
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, databases, and Web browsers.

vSphere Replication is compatible with the same versions as vCenter Server, except for ESXi: vSphere Replication requires ESXi 5.0 or later. See the following documents for more information.

- Compatibility Matrixes for vSphere Replication 6.0 at http://www.vmware.com/support/vsphere-replication/doc/vsphere-replication-compat-matrix-6-0.html .
- For vSphere Replication interoperability with backup software when using VSS, see http://kb.vmware.com/kb/2040754.
- VMware Compatibility Guide at http://partnerweb.vmware.com/comp_guide2/search.php
- Browser compatibility at vSphere Client and vSphere Web Client Software Requirements in *vSphere Installation and Setup*.
- Browser compatibility of the VAMI depends on browsers supported by VMware Studio. See https://www.vmware.com/support/developer/studio/studio25/release_notes.html.

Bandwidth Requirements for vSphere Replication

Before configuring replications, VMware recommends that determine storage and network bandwidth requirements for vSphere Replication to replicate virtual machines efficiently.

Storage and network bandwidth requirements can increase when using vSphere Replication. The following factors play a role in the amount of network bandwidth vSphere Replication requires for 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 with a vCenter Server instance on each site, the link speed between the two sites is the most important as it can slow down replication traffic between the two sites.

Dataset Size

vSphere Replication might not replicate every virtual machine nor 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 2TB of virtual machines on the datastores and usevSphere Replication to replicate half of these virtual machines. You might only replicate a subset of the VMDKs and assuming all the VMDKs are replicated, the maximum amount of data for replication is 1TB.

Data Change Rate and Recovery Point Objective

The data change rate is affected by the recovery point objective (RPO). 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 to meet that RPO. 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 4GB 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 completely 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," on page 29.

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, one hour, four hours, and 24 hours. Factor in 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 amount of data changes within each configured RPO, and the link speeds in your network.

Prerequisites

Examine how data change rate, traffic rates, and the link speed meet the RPO. Then 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.

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 Uninstalling vSphere Replication

4

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

Installing vSphere Replication

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 provides a virtual appliance management interface (VAMI). You can use this interface to reconfigure the vSphere Replication database, network settings, public-key certificates, and passwords for the appliances.

Uninstalling vSphere Replication

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

In the event of deleting the vSphere Replication appliance before unregistering it from the SSO server and the vCenter Server, a special procedure must be performed to clean your environment up.

This chapter includes the following topics:

- "Install vSphere Replication," on page 32
- "Uninstall vSphere Replication," on page 39
- "Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted," on page 40

Install vSphere Replication

The installation procedure of vSphere Replication involves several steps.

Procedure

1 Prepare Your Environment to Install vSphere Replication on page 32

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

2 Deploy the vSphere Replication Virtual Appliance on page 33

vSphere Replication is distributed as an OVF virtual appliance.

3 Register the vSphere Replication Appliance with vCenter Single Sign-On on page 34

You must register the vSphere Replication Management Server with vCenter Single Sign-On on both the source and the target sites.

4 Configure vSphere Replication Connections on page 36

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

Prepare Your Environment to Install vSphere Replication

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

Procedure

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

2 Download and install the Client Integration Plug-in from the login page of the vSphere Web Client.

If the plug-in is already installed, the link does not appear.

3 In the vSphere Web Client, select the vCenter Server instance on which you are deploying vSphere Replication, click **Manage > Settings > Advanced Settings**, and verify that the `VirtualCenter.FQDN` value is set to a fully-qualified domain name or a literal address.

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.

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.

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 installation package to a local directory or obtain its online URL.

Procedure

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

2 Select **vCenter > 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.
- Select **Local file > Browse** to locate the `.ovf` file if you downloaded the installation package to a local machine.

5 Review the virtual appliance details and click **Next**.

6 Accept the end user license agreements (EULA) and click **Next**.

7 Accept the name, select or search for a destination folder or datacenter 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.

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

   NOTE Selecting higher number of vCPUs ensures 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.

   ---

9 Select a cluster, host, or resource pool where you want to run the deployed template, and click **Next**.

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

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 virtual appliance management interface (VAMI) after installation.

12 Set the password for the root account for the customized template, and click **Next**.

   The password must be at least eight characters long.

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

14 Review the settings, select the check box to power on the virtual appliance after deployment, and click **Finish**.

   The vSphere Replication appliance is deployed.

15 Take a note of the IP address of the appliance, log out of the vSphere Web Client and close the browser.

16 Repeat the procedure to deploy vSphere Replication on the target site.

What to do next

Register the vSphere Replication appliance with the SSO service.

Register the vSphere Replication Appliance with vCenter Single Sign-On

You must register the vSphere Replication Management Server with vCenter Single Sign-On on both the source and the target sites.

After you deploy the vSphere Replication appliance, you use the Virtual Appliance Management Interface (VAMI) to register the endpoint and the certificate of the vSphere Replication Management Server with the vCenter Lookup Service, and to register the vSphere Replication solution user with the vCenter Single Sign-On administration server.

If you do not register vSphere Replication with vCenter Single Sign-On on the target site, vSphere Replication cannot operate as expected. In addition, storage DRS does not detect the replicated data that vSphere Replication stores on the target site and might destroy it.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.
- Verify that the vSphere Replication management server is synchronized with the time of the Single Sign-On server.

Procedure

1 Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.

2 Type the root user name and password for the appliance.

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

3 Click the **Configuration** tab.

4 In the **LookupService Address** text box, enter the IP address or domain name of the server where the lookup service runs.

5 Enter the credentials of a user with administrator privileges to vCenter Single Sign-On.

   Initially, only the user administrator@vsphere.local has these privileges.

6 Click **Save and Restart Service**.

7 Repeat the procedure to register vSphere Replication on the target site.

vSphere Replication appears on the **Home** tab in the vSphere Web Client.

What to do next

NOTE If you registered the vSphere Replication appliance with SSO as part of the upgrade procedure, all existing connections will turn into `Connection issue` status. See "Reconnect to a Remote Site," on page 38.

If you competed this procedure as part of the installation process, you can configure connections between the source and target sites.

Perform optional reconfiguration of the vSphere Replication appliance by using the VAMI. You can install a certificate, change the appliance root password, change the trust policy, or configure vSphere Replication to use an external database.

States of vSphere Replication Displayed in the vSphere Web Client

Before you can start using vSphere Replication, you must register the vSphere Replication appliance with the vCenter Lookup Service and the Single Sign-On administration server in the environment.

In the vSphere Web Client, on the vSphere Replication **Home** tab, you can check the list of vCenter Server instances in the Single-Sing On domain, and the status of vSphere Replication on each vCenter Server instance.

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 4-1. 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. 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. 1 Use a supported browser to log in to the vSphere Replication VAMI as the root user. The URL for the VAMI is https://*vr-appliance-address*:5480. 2 On the **Configuration** tab, click **Save and Restart Service**.
Enabled (Configuration issue)	A configuration error occurred. The vSphere Replication Management Server is either not registered with the vCenter SSO components, or the configuration is incorrect and must be updated. You cannot manage existing replications, or configure new replications to this server .	Configure the vSphere Replication appliance. 1 Select the row that indicates the `Enabled (Configuration issue)` status. 2 Point to the `Enabled (Configuration issue)` status. The detailed error message appears in a tooltip. 3 Click the **Configure** icon ( ) above the list of vCenter Server instances. The vSphere Replication VAMI opens. 4 On the **Configuration** tab, enter the parameters that were indicated in the error message and click **Save and Restart Service** .

Table 4-1. vSphere Replication States on vCenter Server Instances (Continued)

Status	Description	Remediation
Enabled (Not accessible)	The vSphere Replication Management Server is not accessible. 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. You cannot manage existing replications, or configure new replications to this server .	■ Verify that the vSphere Replication appliance exists on the vCenter Server. ■ Verify that the vSphere Replication appliance is powered on. ■ Restart the VRM service. a On the vSphere Replication **Home** tab, select the row that indicates the `Enabled (Not accessible)` status and click the **Configure** icon ( ) above the list of replication servers. b On the **Configuration** tab, restart the VRM service.
Enabled (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 need to configure a connection between the two vSphere Replication appliances.

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

If the source and the target vCenter Server instances use different SSO domains, the connection is considered remote. The vSphere Replication Management Server on the source site registers with the Platform Services Controller (PSC) of the remote SSO 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 source and target 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

If you plan to configure a remote connection, obtain the IP address or domain name of the server where the PSC runs. The address appears in the **LookupService Address** text box on the **Configuration** tab under **VR** in the vSphere Replication VAMI on the target site.

Procedure

1 Click **vSphere Replication** in the Navigator tree of the vSphere Web Client.

2 Under **vSphere Replication**, click the **Home** tab.

3 Click **Manage**.

4 Click **Target Sites**, and click the **Connect to target site** icon ( ).

5 Select a target site option.

Option	Description
Connect to a local site	Select this option to connect to a vCenter Server that uses the same SSO domain as the source vCenter Server. If the domain contains no vCenter Server systems to which you can connect, this option is disabled. For local connections, vSphere Replication uses the SSO service on the local site to authenticate with each vCenter Server in the SSO domain. The list of vCenter Server instances to which you can connect appears at the bottom of the dialog box.
Connect to a remote site	Select this option to connect to a vCenter Server that uses a different SSO domain. For remote connections, the vSphere Replication Management Server on the source site registers with the PSC of the remote SSO domain. Therefore, you must enter the IP address or host name of the server where the PSC runs, and provide the credentials of a user that has the **VRM remote.Manage VRM** privilege assigned. When you log in to the remote SSO domain, a list of all vCenter Server instances to which you can connect appears at the bottom of the dialog box.

6 Select the vCenter Server to which you want to connect, and click **OK**.

Site Connection States Displayed in the vSphere Web Client

In the vSphere Web Client, on the **vSphere Replication** tab under **Manage**, you can check the states of the connections to target sites.

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 4-2. Site Connection States

Icon	Status	Description	Remediation
	Connected	The connection between the source site and the target site is working properly.	Not needed.
	Not authenticated	The remote site is online, but your user session has expired. In this state, you must enter credentials to manage replication tasks. Already configured replications are running in the background.	Reconnect the sites. See "vSphere Replication Sites Appear in the Not Authenticated State," on page 98.
	Connection issue	■ The SSL certificate on the remote site has been changed. ■ The network connection between the source site and the target site is not functioning properly, or the remote site is offline. ■ The user that is used for authentication with the Lookup Service or the VRMS extension user in the SSO might be disabled or deleted. In this state, configured replications might not be running.	■ Select the target site that indicates the `Connection issue` status and click the **Reconnect** icon ( ). See "Reconnect to a Remote Site," on page 38. ■ In the inventory tree, click the vCenter Server and navigate to the **Events** tab under **Monitor** to search for events related to vSphere Replication. ■ Verify the status of the remote site.

Reconnect to a Remote Site

If the state of the connection to a target site is **Connection issue**, you must repair the connection to manage existing replications, and to enable the creation of new replications.

The states of connections to target sites appear in the vSphere Web Client, on the **vSphere Replication** tab under **Manage**.

For reconnecting to cloud sites, see topic Reconnect to a Cloud Provider Site in the *vSphere Replication for Disaster Recovery to Cloud* document.

If the source and the target vCenter Server instances use different SSO domains, the connection is considered remote. The vSphere Replication Management Server on the source site registers with the Platform Services Controller (PSC) of the remote SSO domain. To establish a connection to a remote site, you provide the address of the vCenter Server and the PSC, and enter the credentials of a user that has the **VRM remote.Manage VRM** privilege assigned. If the PSC address changes, the connection status changes to `Connection issue` and you must reconnect the two sites.

Prerequisites

Verify that the vCenter Server and the vSphere Replication Management Server on the target site are up and running, and that the `Connection issue` status is not caused by a network problem.

Procedure

1 From the list of target sites, select the connection that indicates `Connection issue` status.

2 Click the **Reconnect to the selected site** icon ( ), and click **Yes** to confirm that you want to reconnect.

The Reconnect to Remote Site dialog box appears.

3 Enter the new PSC address and the credentials of a user that has the **VRM remote.Manage VRM** privilege assigned, and click **OK**.

NOTE If you upgraded from an earlier vSphere Replication version, the text box for the Platform Service Controller address is automatically populated with the IP address of the target vSphere Replication Management server. You must replace it with the address of the Platform Service Controller on the target site before providing the credentials.

The connection status turns into `Connected`.

Uninstall vSphere Replication

You uninstall vSphere Replication by unregistering the appliance from vCenter Server and removing it from your environment.

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 vSphere Replication VAMI.

The URL for the VAMI is https://*vr-appliance-address*:5480.

2 Select the **Configuration** tab.

3 Click **Unregister from vCenter Server**.

4 In the vSphere Web Client, power off and delete the vSphere Replication appliance.

The vSphere Replication plug-in is uninstalled automatically.

You removed vSphere Replication from your environment.

What to do next

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 "Search and Remove the vSphere Replication Tag from Target Datastores," on page 40.

Search and Remove the vSphere Replication Tag from Target Datastores

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.

Prerequisites

- The vSphere Replication appliance is deleted.
- Required privilege: **Inventory Service.vSphere Tagging.Assign or Unassign vSphere Tag** on the root vCenter Server instance.

Procedure

1. Use the vSphere Web Client to log in to the target vCenter Server.
2. In the search text box on the upper right, enter **`com.vmware.vr.HasVrDisks`** and search for the tag.

   The list of users and groups that have permissions to manage the `com.vmware.vr.HasVrDisks` tag appears.
3. Click the **Related Objects** tab.

   The list of datastores that have the `com.vmware.vr.HasVrDisks` tag assigned appears.
4. Right-click a datastore and select **Tags > 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 the vSphere Replication appliance was deleted before you unregistered it form the environment , you cannot use the virtual appliance management interface (VAMI) to unregister vSphere Replication from vCenter Server.

Only a vSphere administrator can clean up the environment.

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 6.0 Security* document. See topics Remove Permissions and Delete vCenter Single Sign-On Solution Users.

Prerequisites

Verify that you know 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 Type **`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 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 "Search and Remove the vSphere Replication Tag from Target Datastores," on page 40.

Deploying Additional vSphere Replication Servers

5

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

This chapter includes the following topics:

- "Deploy an Additional vSphere Replication Server," on page 43
- "Register an Additional vSphere Replication Server," on page 44
- "Reconfigure vSphere Replication Server Settings," on page 44
- "Unregister and Remove a vSphere Replication Server," on page 45
- "Disable the Embedded vSphere Replication Server," on page 46

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.

For information about the loads that a vSphere Replication management server and a vSphere Replication server can support, see http://kb.vmware.com/kb/2034768.

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. In the vSphere Web Client, start the OVF deployment wizard from **Manage > vSphere Replication > Replication Servers**.
2. Browse for the `vSphere_Replication_AddOn_OVF10.ovf` file, select it, and click Next.
3. Review the virtual appliance details and click **Next**.
4. Follow the prompts to select a destination host, datastore, and disk format for the virtual appliance.
5. Enter a password for the appliance that is at least eight characters long.

6 Set the network properties. Select DHCP or set a static IP address.

   You can change network settings after deployment in the VAMI.

7 Review your settings and select **Power on after deployment** to start the appliance immediately after deployment completes.

8 Click **Finish**.

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

If 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 the additional vSphere Replication Server is deployed.

Procedure

1 In the vSphere Web Client, navigate to **Manage > vSphere Replication > Replication Servers**, and click **Register a virtual machine as vSphere Replication Server**.

2 From the inventory, select a virtual machine that is a working vSphere Replication server and click **OK**.

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

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 virtual appliance management interface (VAMI) after deployment. To increase security, you can change the root password of the vSphere Replication server and install a new certificate. Using a self-signed certificate provides the benefit of public-key based encryption and authentication, although using such a certificate 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

You deployed an optional vSphere Replication server in addition to the vSphere Replication appliance, and the server is powered on.

Procedure

1 Use a supported browser to log in to the VAMI of the additional vSphere Replication Server that you deployed.

The URL for the VAMI is https://*vr-server-address*:5480.

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

2 Click the **VRS** tab.

3 (Optional) Click **Configuration** to generate or upload a new certificate.

Option	Action
Generate and install a self-signed certificate	Click **Generate and Install**.
Upload an existing SSL certificate	Click **Browse** next to the **Upload PKCS#12 (*.pfx) file** text box to browse for an existing certificate, and click **Upload and Install**.

4 (Optional) Click **Security** to change the Super User password for the vSphere Replication server.

`root` is the Super User.

5 (Optional) Click the **Network** tab to change the network settings.

Option	Action
View current network settings	Click **Status**.
Set static or DHCP IPv4 or IPv6 addresses	■ Click **Address**, and select **DHCP**, **Static**, or **None** for IPv4 addresses. ■ Select **Auto** or **Static** for IPv6 addresses. If you select **Static**, type the default gateway and DNS server addresses to use.
Configure proxy server	Click **Proxy**, select the **Use a proxy server** check box, and type the proxy server address and port number.
Save Settings	If you do not click **Save Settings**, changes are discarded.

NOTE After the IP address of the vSphere Replication server on the target site changes, you must manually reconfigure replications on the source site to point to the new IP address.

6 (Optional) Select **VRS > Configuration > Restart** to restart the vSphere Replication service.

7 (Optional) Select **System > Reboot** to reboot the vSphere Replication server appliance.

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

You deployed and registered a vSphere Replication server that you no longer require. Make sure it does not serve any replications, otherwise the operations will fail.

Procedure

1 In **Manage > vSphere Replication**, click the **Replication Servers** tab and find the vSphere Replication server in the list.

2 Select the server and click **Unregister the selected vSphere Replication Server.**

3 In the Hosts and Clusters view, power off and delete the vSphere Replication server virtual machine.

Disable the Embedded vSphere Replication Server

vSphere Replication includes an embedded vSphere Replication Server by default. If you want to disable the embedded vSphere Replication server, you can do so using ssh.

Prerequisites

Make sure 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 type:

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

2 Restart the HMS service.

```
# service hms restart
```

You can now unregister the embedded vSphere Replication server from the vSphere Replication user interface.

What to do next

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

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

Upgrading vSphere Replication 6

You upgrade the vSphere Replication appliance and any additional vSphere Replication servers by using a downloaded ISO image.

The downloadable ISO image is the only means of upgrading from vSphere Replication 5.5.1 or 5.8 to vSphere Replication 6.0. You cannot upgrade vSphere Replication from version 5.5.1 or 5.8 to version 6.0 by using vSphere Update Manager or the virtual appliance management interface (VAMI) of the vSphere Replication appliance. After you have installed vSphere Replication 6.0 or upgraded to version 6.0 by using the ISO image, you can use the VAMI or Update Manager to install later 6.0.x update releases.

You cannot downgrade to an earlier version of vSphere Replication.

Example: vSphere Replication Upgrade Scenarios

You use the ISO file to upgrade to a major version of vSphere Replication, for example from 5.5.1 to 6.0.

You use Update Manager, the VAMI, or the ISO file to install an update release of vSphere Replication, for example upgrade 5.5.0 to 5.5.1.

These examples of upgrade and update scenarios are not exhaustive. For the full list of supported upgrade paths, see the *Compatibility Matrixes for vSphere Replication 6.0* at https://www.vmware.com/support/vsphere-replication/doc/vsphere-replication-compat-matrix-6-0.html.

- You can upgrade vSphere Replication 5.5.1 to 6.0 by using the ISO file for vSphere Replication 6.0.
- You cannot upgrade vSphere Replication 5.5.1 to 6.0 by using Update Manager or the VAMI.
- You can upgrade vSphere Replication 5.5.0 to 5.5.1 by using Update Manager, the VAMI, or the ISO file.

This chapter includes the following topics:

- "Upgrade vSphere Replication by Using the Downloadable ISO Image," on page 47
- "Update the vCenter Server IP Address in the vSphere Replication Management Server," on page 49

Upgrade vSphere Replication by Using the Downloadable ISO Image

You upgrade the vSphere Replication appliance and the vSphere Replication server by using a downloadable ISO image.

Prerequisites

- Upgrade the vCenter Server instance that vSphere Replication extends.
- Download the `VMware-vSphere_Replication-6.0.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.

- If the vSphere Replication version that you run is not supported for direct upgrade to vSphere Replication 6.0, upgrade your vSphere Replication instance to a supported version. For example, to upgrade vSphere Replication 5.6 to 6.0, you must upgrade 5.6 to 5.8 first. See the interoperability matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php for solution upgrade paths for vSphere Replication.
- Shut down and power off the vSphere Replication virtual machine.

Procedure

1. Right-click the vSphere Replication virtual machine and select **Edit Settings**.
2. If you are upgrading a vSphere Replication Server appliance, reconfigure the virtual machine to increase its memory from 512 MB to 716 MB RAM.
3. On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.
4. Navigate to the ISO image in the datastore.
5. For **File Type**, select **ISO Image** and click **OK**.
6. Select the option to connect at power on and follow the prompts to add the CD/DVD drive to the vSphere Replication virtual machine.
7. Power on 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**.
11. Click **Status** and click **Check Updates**.

    The appliance version appears in the list of available updates.
12. Click **Install Updates** and click **OK**.
13. After the updates install, click the **System** tab and click **Reboot** to complete the upgrade.
14. Log out of the vSphere Web Client, clear the browser cache, and log in again to see the upgraded appliance.

What to do next

Note If the vSphere Replication deployment that you upgraded was not registered with the vCenter Lookup Service, after the upgrade the status of the vSphere Replication server will turn to `Enabled (Configuration issue)`. You must log in to the VAMI and register the vSphere Replication appliance with the Lookup Service. See "Register the vSphere Replication Appliance with vCenter Single Sign-On," on page 34.

If your infrastructure uses more than one vSphere Replication Server, you must upgrade all vSphere Replication Server instances to version 6.0.

Important If the vSphere Replication appliance that you upgraded uses the embedded database, you must apply additional configuration to enable the support of up to 2000 replications. See http://kb.vmware.com/kb/2102463. No additional configuration is required for vSphere Replication appliances that are configured to use an external database.

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

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

To update the vCenter Server certificate, see "vSphere Replication is Inaccessible After Changing vCenter Server Certificate," on page 104.

If vCenter Server uses a static IP address, it preserves the IP address by default after upgrade. If 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, update the IP address in the vSphere Replication Management Server.

Procedure

1 Upgrade vCenter Server to the new appliance.

2 Upgrade vSphere Replication.

3 Power off the vSphere Replication appliance and power it on to retrieve the OVF environment.

4 Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.

5 On the **Configuration** tab, enter the new IP address of the vCenter Server.

6 Click **Save and Restart**.

Reconfigure the vSphere Replication Appliance 7

If necessary, you can reconfigure the vSphere Replication appliance settings by using the virtual appliance management interface (VAMI).

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 on page 52

  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 virtual appliance management interface (VAMI).

- Change the SSL Certificate of the vSphere Replication Appliance on page 52

  vSphere Replication appliance uses certificate-based authentication for all connections that it establishes with vCenter Server and remote site vSphere Replication appliances.

- Change the Password of the vSphere Replication Appliance on page 55

  You set the password of the vSphere Replication appliance when you deploy the appliance. You can change the password after installation by using the virtual appliance management interface (VAMI).

- Change Keystore and Truststore Passwords of the vSphere Replication Appliance on page 55

  To increase security, you can change the default passwords of the vSphere Replication appliance keystore and truststore. If you copy the keystores from the appliance to another machine, VMware recommends that you change the passwords before the copy operation.

- Configure vSphere Replication Network Settings on page 56

  You can review current network settings and change address and proxy settings for vSphere Replication. You might make these changes to match network reconfigurations.

- Configure vSphere Replication System Settings on page 58

  You can view the vSphere Replication system settings to gather information about the vSphere Replication appliance. You can also set the system time zone, and reboot or shut down the appliance.

- Reconfigure vSphere Replication to Use an External Database on page 58

  The vSphere Replication appliance contains an embedded vPostgreSQL database that you can use immediately after you deploy the appliance, without any additional database configuration. If necessary, you can reconfigure vSphere Replication to use an external database.

- Use the Embedded vSphere Replication Database on page 61

  If you configured vSphere Replication to use an external database, you can reconfigure vSphere Replication to use the embedded database.

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 virtual appliance management interface (VAMI).

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, and an administrator email address. You can change the general settings from the default values in the virtual appliance management interface (VAMI).

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.
- Update the vCenter Server to 6.0.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
2. Review and confirm the browser security exception, if applicable, to proceed to the login page.
3. Type the root user name and password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication appliance.
4. On the **VR** tab, click **Configuration**.
5. Type the address of the vSphere Replication appliance or click **Browse** to select an IP address from a list.
6. Type the address of the vCenter Server instance to use with this installation.

   You must use the same address format that you used when you installed vCenter Server.

   For example, if you used a fully qualified domain name during installation, you must use that FQDN. If you used an IP address, you must use that IP address.
7. Type an administrator email address.
8. Click **Save and Restart Service** to apply the changes.

You reconfigured the general settings of the vSphere Replication appliance.

Change the SSL Certificate of the vSphere Replication Appliance

vSphere Replication appliance uses certificate-based authentication for all connections that it establishes with vCenter Server and remote site vSphere Replication appliances.

vSphere Replication does not use user name and password based authentication. vSphere Replication generates a standard SSL certificate when the appliance first boots and registers with vCenter Server. 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 virtual appliance management interface (VAMI) of the vSphere Replication appliance. For information about the SSL certificates that vSphere Replication uses, see "vSphere Replication Certificate Verification," on page 53 and "Requirements When Using a Public Key Certificate with vSphere Replication," on page 54.

See "vSphere Replication Certificate Verification," on page 53 for details of 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.
- Update the vCenter Server to 6.0.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.

2. Type the root user name and password for the appliance.

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

3. (Optional) Click the **VR** tab and click **Security** to review the current SSL certificate.
4. Click **Configuration**.
5. (Optional) To enforce verification of certificate validity, select the **Accept only SSL certificates signed by a trusted Certificate Authority** check box.
6. Generate or install a new SSL certificate.

Option	Action
Generate a self-signed certificate	Click **Generate and Install**. Using a self-signed certificate provides trust by thumbprint only and might not be suitable for environments that require high levels of security. You cannot use a self-signed certificate if you selected **Accept only SSL certificates signed by a trusted Certificate Authority**.
Upload a certificate	Click **Browse** to select a PKCS#12 certificate and click **Upload and Install**. Public key certificates must meet certain requirements. See "Requirements When Using a Public Key Certificate with vSphere Replication," on page 54.

7. Click **Save and Restart Service** to apply the changes.

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.

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 tunnelled.

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 in the virtual appliance management interface (VAMI) of the vSphere Replication appliance by selecting the option **Accept only SSL certificates signed by a trusted Certificate Authority** when you upload a certificate.

Thumbprint Verification	vSphere Replication checks for a thumbprint match. vSphere Replication trusts remote server certificates if it can verify the 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 certificate validity.
Verification of Thumbprint and Certificate Validity	vSphere Replication checks the thumbprint and checks that all server certificates are valid. If you select the **Accept only SSL certificates signed by a trusted Certificate Authority** option, 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 verification of certificate validity by selecting **Accept only SSL certificates signed by a trusted Certificate Authority** in the virtual appliance management interface (VAMI) of the vSphere Replication appliance, 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 **VRM Host** setting in the VAMI. Setting the certificate subject name accordingly is sufficient, if you put a host name in the **VRM Host** setting. If any of the certificate Subject Alternative Name fields of the certificate matches the **VRM Host** setting, this will work as well.
- vSphere Replication checks the issue and expiration dates of the certificate against the current date, to ensure that the certificate has 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 signatures, but VMware recommends that you use SHA256 signatures.
- vSphere Replication does not accept RSA or DSA certificates with 512-bit keys. vSphere Replication requires at least 1024-bit keys. VMware recommends using 2048-bit public keys. vSphere Replication shows a warning if you use a 1024-bit key.

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 virtual appliance management interface (VAMI).

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.
- Update the vCenter Server to 6.0.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.

2. Type the root user name and password for the appliance.

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

3. Click the **VR** tab and click **Security**.
4. Type the current password in the **Current Password** text box.
5. Type the new password in the **New Password** and the **Confirm New Password** text boxes.

   The password must be a minimum of eight characters. vSphere Replication does not support blank passwords.

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

Change Keystore and Truststore Passwords of the vSphere Replication Appliance

To increase security, you can change the default passwords of the vSphere Replication appliance keystore and truststore. If you copy the keystores from the appliance to another machine, VMware recommends that you change the passwords before the copy operation.

The keystore and truststore passwords might be stored in an access restricted `config` 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 `hms-keystore.jks` password, log in as root.

2 Obtain the current hms-keystore password.

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

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

3 Change the hms-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.

```
# /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/hms-configtool -cmd reconfig -property
'hms-keystore-password=new_password'
```

6 Reboot the appliance for the changes to take effect.

```
# reboot
```

7 To change the hms-truststore.jks password, log in as root.

8 Obtain the current hms-truststore password.

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

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

9 Change the hms-truststore password.

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

10 Update the configuration with the new password.

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

11 Restart the vSphere Replication service.

```
# service hms restart
```

Configure vSphere Replication Network Settings

You can review current network settings and change address and proxy settings for vSphere Replication. You might make these changes to match network reconfigurations.

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.
- Update the vCenter Server to 6.0.

Procedure

1 Use a supported browser to log in to the vSphere Replication VAMI.

The URL for the VAMI is https://*vr-appliance-address*:5480.

2 Type the root user name and password for the appliance.

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

3 Click the **Network** tab.

4 Click **Status** to review current network settings.

5 Click **Address** to review or modify IPv4 and IPv6 address settings.

IP Address Type	Option	Description
IPv4	DHCP	DHCP is not recommended if the IP address of the appliance might change if it reboots.
IPv4	Static	With a static IPv4 address, you can modify the IP settings, DNS settings, net mask, and host name information.
IPv4	None	Disabling IPv4 addresses forces the use of IPv6 addresses only.
IPv6	Auto	Automatic assignment of IPv6 addresses is not recommended if the IP address of the appliance might change if it reboots.
IPv6	Static	With a static IPv6 address, you can modify the IP address and the address prefix.

6 Click **Save Settings**.

If you do not click **Save Settings**, changes are discarded.

Note After the IP address of the vSphere Replication server on the target site changes, you must manually reconfigure replications on the source site to point to the new IP address.

7 Click **Proxy** to review or modify proxy settings.

a Select **Use a proxy server** to use a proxy server.

b Enter a proxy server name in the **HTTP Proxy Server** text box.

c Enter a proxy port in the **Proxy Port** text box.

d (Optional) Enter a proxy server user name and password.

8 Click **Save Settings**.

If you do not click **Save Settings**, changes are discarded.

What to do next

A network address change might require you to reconnect the source and target sites and might also require a change of certificate if you have activated verification of certificate validity.

Configure vSphere Replication System Settings

You can view the vSphere Replication system settings to gather information about the vSphere Replication appliance. You can also set the system time zone, and reboot or shut down the appliance.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.
- Update the vCenter Server to 6.0.

Procedure

1 Use a supported browser to log in to the vSphere Replication VAMI.

The URL for the VAMI is https://*vr-appliance-address*:5480.

2 Type the root user name and password for the server.

3 Click the **System** tab.

4 Click **Information**.

You can review information about vSphere Replication, and reboot or shutdown the appliance.

Option	Description
Vendor	Vendor name
Appliance Name	vSphere Replication appliance name
Appliance Version	vSphere Replication version
Hostname	Hostname of the appliance
OS Name	Operating system name and version
OVF Environment: View	Displays information about the OVF environment
Reboot	Reboots the virtual appliance
Shutdown	Shuts down the virtual appliance

Shutting down the vSphere Replication appliance stops configured replications and prevents you from configuring replication of new virtual machines as well as modifying existing replication settings.

5 Click **Time Zone**.

Option	Description
System Time Zone	Time zones are available from the drop-down list
Save Settings	Saves settings
Cancel Changes	Discards changes

Reconfigure vSphere Replication to Use an External Database

The vSphere Replication appliance contains an embedded vPostgreSQL database that you can use immediately after you deploy the appliance, without any additional database configuration. If necessary, you can reconfigure vSphere Replication to use an external database.

Each vSphere Replication appliance requires its own database. If the database at either site is corrupted, vSphere Replication does not function. vSphere Replication cannot use the vCenter Server database because it has different database schema requirements. However, if you do not use the embedded vSphere Replication database you can use the vCenter database server to create and support an external vSphere Replication database.

You might need to use an external database to improve performance or load balancing, for easier backup, or to meet your company's database standards.

NOTE vSphere Replication server inside the vSphere Replication appliance uses its own embedded database and config files. Configuring VRMS to use external database does not provide protection of losing the vSphere Replication appliance or any Additional vSphere Replication Server appliance.

If you reinitialize the database after you deploy vSphere Replication, you must go to the vSphere Replication virtual appliance management interface (VAMI) to reconfigure vSphere Replication to use the new database connection.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.
- You must create and configure the external database before you connect it to vSphere Replication. See "Databases that vSphere Replication Supports," on page 60 for the configuration requirements for each supported type of database.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.

2. Review and confirm the browser security exception, if applicable, to proceed to the login page.
3. Type the root user name and password for the appliance.

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

4. On the **VR** tab, click **Configuration**.
5. Select **Manual configuration** to specify a configuration or select **Configure from an existing VRM database** to use a previously established configuration.
6. In the DB text boxes, provide information about the database for vSphere Replication to use.

Option	Setting
DB Type	Select **SQL Server** or **Oracle**.
DB Host	IP address or fully qualified domain name of the host on which the database server is running.
DB Port	Port on which to connect to the database.
DB Username	Username for the vSphere Replication database user account that you create on the database server.
DB Password	Password for the vSphere Replication database user account that you create on the database server.
DB Name	Name of the vSphere Replication database instance.
DB URL	Auto-generated and hidden by default. Advanced users can fine-tune other database properties by modifying the URL, for example if you use a named instance of SQL Server.

7. Click **Save and Restart Service** to apply the changes.

You configured vSphere Replication to use an external database instead of the database that is embedded in the vSphere Replication appliance.

Databases that vSphere Replication Supports

The vSphere Replication virtual appliance includes the VMware standard embedded vPostgreSQL database. You can also configure vSphere Replication to use an external database.

Automated migration between the embedded database and any external databases is not supported in any direction. If you must configure an external database, you must manually migrate the data or manually recreate all replications.

You can configure vSphere Replication to use one of the supported external databases.

- Microsoft SQL
- Oracle

External vPostgreSQL databases are not supported. vSphere Replication supports the same database versions as vCenter Server. For supported database versions, see the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

- Configure Microsoft SQL Server for vSphere Replication on page 60

  When you create a Microsoft SQL Server database, you must configure it correctly to support vSphere Replication.

- Configure Oracle Server for vSphere Replication on page 61

  You must configure an Oracle Server database correctly to support vSphere Replication.

Configure Microsoft SQL Server for vSphere Replication

When you create a Microsoft SQL Server database, you must configure it correctly to support vSphere Replication.

You use SQL Server Management Studio to create and configure an SQL Server database for vSphere Replication.

This information provides the general steps that you must perform to configure an SQL Server database for vSphere Replication. For instructions about how to perform the relevant steps, see the SQL Server documentation.

Prerequisites

Verify that the SQL Server Browser service is running.

Procedure

1. Select **Mixed Mode Authentication** when you create the database instance.

   The vSphere Replication appliance and the database server run on different hosts, so you must use mixed mode authentication and not Windows Authentication.

2. Use either a named instance or the default instance of SQL Server.

   If you intend to use dynamic TCP ports, you must use a named instance of SQL Server.

3. Enable TCP on the database instance.

4 Set a TCP port.

Option	Action
Static TCP port	Set the TCP port to the default of 1433.
Dynamic TCP port	a Use a named instance of SQL Server. You can only use dynamic ports with a named instance of SQL Server. b Select the **Show DB URL** check box in the virtual appliance management interface (VAMI) of the vSphere Replication appliance. c Modify the **DB URL** value. Replace port=*port_number* with instanceName=*instance_name* in the URL. d Use the `PortQuery` command from a remote machine to check that the port on which the SQL Server Browser service runs is not blocked by a firewall. The SQL Server Browser runs on port 1434. Type the `PortQuery` command in a terminal window. `PortQry.exe –n Machine_Name –p UDP –e 1434`

5 Verify that the firewall on the database server permits inbound connections on the TCP port.

6 Create the vSphere Replication security login.

7 Create the vSphere Replication database and set the vSphere Replication security login as the database owner.

8 Keep the dbo user and dbo schema settings.

Because the vSphere Replication security login is the database owner, it maps to the database user dbo and uses the dbo schema.

Configure Oracle Server for vSphere Replication

You must configure an Oracle Server database correctly to support vSphere Replication.

You create and configure an Oracle Server database for vSphere Replication by using the tools that Oracle Server provides.

This information provides the general steps that you must perform to configure an Oracle Server database for vSphere Replication. For instructions about how to perform the relevant steps, see the Oracle documentation.

Procedure

1 When creating the database instance, select UTF-8 encoding.

2 Create the vSphere Replication database user account.

3 If they are not selected already, select the **CONNECT** and **RESOURCE** roles.

These roles provide the privileges that vSphere Replication requires.

Use the Embedded vSphere Replication Database

If you configured vSphere Replication to use an external database, you can reconfigure vSphere Replication to use the embedded database.

The vSphere Replication appliance includes an embedded vPostgreSQL database. The embedded database is preconfigured for use with vSphere Replication and is enabled if you accept the default **Performs initial configuration of the appliance using an embedded database** option when you deploy the vSphere Replication appliance. If you reconfigured vSphere Replication to use an external database after

deployment, you can switch to the embedded database. After switching databases, you must manually configure replications again as the replication management data is not migrated to the database. You can use the reset feature in the embedded database to drop replications, site connections and external vSphere Replication registrations.

Prerequisites

- Verify that the vSphere Replication appliance is powered on.
- Verify that you have administrator privileges to configure the vSphere Replication appliance.
- You must have reconfigured vSphere Replication to use an external database.

Procedure

1. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
2. Review and confirm the browser security exception, if applicable, to proceed to the login page.
3. Type the root user name and password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication appliance.
4. On the **VR** tab, click **Configuration**.
5. Select **Configure using the embedded database**.
6. (Optional) Click **Reset Embedded Database** to reset the database.
7. Click **Save and Restart Service** to apply the changes.

You configured vSphere Replication to use the embedded vSphere Replication database.

Replicating Virtual Machines 8

With vSphere Replication you can replicate virtual machines from a source site to a target site.

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 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 "How the Recovery Point Objective Affects Replication Scheduling," on page 64.

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.

The source and target sites must be connected for you to be able to configure replications. You cannot perform replications if one of the sites is in the `Connection issue` state. See "Site Connection States Displayed in the vSphere Web Client," on page 37. If the sites appear in the `Not authenticated` state, scheduled replications continue as normal, but you cannot manage replications. See "vSphere Replication Sites Appear in the Not Authenticated State," on page 98.

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 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 `Not active` status.

You cannot use vSphere Replication to replicate virtual machine templates.

This chapter includes the following topics:

- "How the Recovery Point Objective Affects Replication Scheduling," on page 64
- "How Retention Policy Works," on page 64
- "Replicating a Virtual Machine and Enabling Multiple Point in Time Instances," on page 66
- "Using vSphere Replication with Virtual SAN Storage," on page 66
- "Using vSphere Replication with vSphere Storage DRS," on page 68
- "How vSphere Replication Synchronizes Data Between vCenter Server Sites During Initial Configuration," on page 68
- "Replicating Virtual Machines Using Replication Seeds," on page 69
- "Replicating a Virtual Machine in a Single vCenter Server Instance," on page 70
- "Configure Replication for a Single Virtual Machine to vCenter Server," on page 70
- "Configure Replication for Multiple Virtual Machines to vCenter Server," on page 72

- "Move a Replication to a New vSphere Replication Server," on page 74
- "Stop Replicating a Virtual Machine," on page 74
- "Reconfiguring Replications," on page 76

How the Recovery Point Objective Affects Replication Scheduling

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

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.

Assume that during replication configuration 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. For example, 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.

How Retention Policy Works

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

For example, you can configure the retention of 3 instances per day for the last 5 days.

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. By the example above, the list will contain 15 snapshots and the latest saved instance of the virtual machine, or a total of 16 snapshots. You can use the snapshots to revert to an earlier state of the recovered virtual machine.

Administrators cannot configure the precise time when replica instances are created, because the retention policy is not directly related to 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 4-hour RPO. This means that the latest available replica instance can never reflect a state of the virtual machine that is older than 4 hours. 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 a new instance on the target site. The replication instance reflects the state of the virtual machine at the time the synchronisation 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 synchronisations, 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 taken into account when determining the number of instances to keep.

When the age of the latest instance approaches the RPO interval, vSphere Replication starts creating a new 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 3 instances for the last 1 day, it means that you want to keep 3 replica instances that are relatively evenly distributed over 24 hours. This equals approximately 1 instance in a 8-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 8 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 slot time is decremented by the granularity of the retention policy 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 check whether the RPO settings will create 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 6 replication instances per day, the RPO period should not exceed 4 hours, so that vSphere Replication can create 6 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.

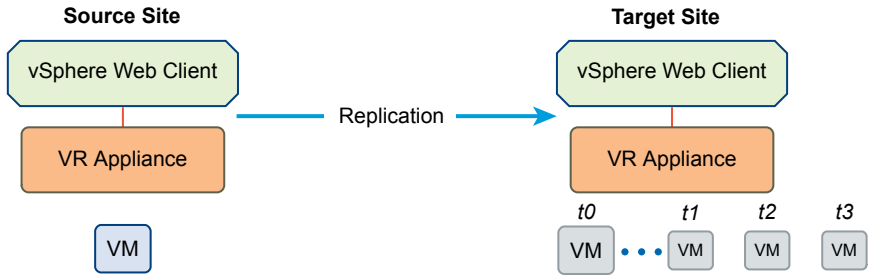
When you configure replication of a virtual machine, you can enable multiple point in time (PIT) instances in the recovery settings in the Configure Replication wizard. vSphere Replication retains a number of snapshot instances of the virtual machine on the target site based on the retention policy that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

During replication, vSphere Replication replicates all aspects of the virtual machine to the target site, including any potential viruses and corrupted applications. If a virtual machine suffers from a virus or corruption and you have configured vSphere Replication to keep PIT snapshots, you can recover the virtual machine and then revert it to a snapshot of the virtual machine 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 8-1. Recovering a Virtual Machine at Points in Time (PIT)



Using vSphere Replication with Virtual SAN Storage

You can use VMware Virtual SAN datastores as target datastores when configuring replications. Follow the guidelines when using vSphere Replication with Virtual SAN storage.

Note VMware Virtual SAN is a fully supported feature of vSphere 5.5 Update 1 and later.

Because user-friendly names of Virtual SAN datastores might change and cause errors during replication or recovery operations, vSphere Replication automatically replaces the user-friendly name of a datastore with its UUID, which is constant. Therefore, the UUID is displayed everywhere in the vSphere Replication user interface, though you selected a human-readable name during replication configuration.

Limits of Using vSphere Replication with Virtual SAN Storage

For reasons of load and I/O latency, Virtual SAN storage is subject to limits in terms of the numbers of hosts that you can include in a Virtual SAN cluster and the number of virtual machines that you can run on each host. See the Limits section in the *VMware Virtual SAN Design and Sizing Guide* at http://www.vmware.com/products/virtual-san/resources.html.

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 Virtual SAN storage by using vSphere Replication depends on your infrastructure. If you notice slower response times when you configure replications for virtual machines in Virtual SAN storage, monitor the I/O latency of the Virtual SAN infrastructure. Potentially, reduce the number of virtual machines that you replicate in the Virtual SAN datastore.

NOTE When you stop a replication, vSphere Replication does not delete the replica directory at the target datastore. As a result, stale directories remain on VMFS and NFS target datastores, and unused namespaces remain on Virtual SAN and Virtual Volume target datastores. Because the maximum number of directories and namespaces on a datastore is limited, you must manually clean them up to free resources on the datastore. See "Clean Up the Target Datastore After You Stop a Replication," on page 75.

Retaining Point-in-Time Snapshots when Using Virtual SAN Storage

Virtual SAN storage stores virtual machine disk files as a set of objects and components. Each disk object in Virtual SAN storage has mirror and witness objects. In the default Virtual SAN storage policy, a disk object has 2 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 Virtual SAN 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 Virtual SAN storage policy, the disk object will have 2 mirror components of 256 GB each and 1 witness, to make a total of 3 components.
- If a virtual machine has one 512 GB disk and you use the default Virtual SAN storage policy, the disk object will have 4 mirror components of 256 GB each and 1 witness, to make a total of 5 components.

See the *VMware Virtual SAN Design and Sizing Guide* at http://www.vmware.com/products/virtual-san/resources.html for explanations of objects, components, mirrors, witnesses, and Virtual SAN storage policies.

If you enable multiple point-in-time (PIT) snapshots, you must make allowances for the additional components that each snapshot creates in the Virtual SAN storage, based on 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 Virtual SAN 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 Virtual SAN 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 Virtual SAN storage policy:
  - 2 (number of disks) x 10 (number of PIT snapshots) x 3 (2 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 Virtual SAN storage policy:
  - 2 (number of disks) x 10 (number of PIT snapshots) x 5 (4 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 Virtual SAN storage.

Using vSphere Replication with vSphere Storage DRS

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

Storage DRS can detect the data that vSphere Replication copies on the target site and can move replications without affecting the replication process.

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 which a replica virtual machine is created on the target site, and data synchronization occurs between the source and the target vCenter Server site.

The speed of data synchronization depends on the availability of information about 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 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 have not been 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.

Product Versions at the Source and the Target Site

The acceleration of initial synchronization is supported only on ESXi hosts 6.0.x or later.

If the ESXi and the vSphere Replication Server on the source site are 6.0, but the vSphere Replication Server or the hosts at the target site are not 6.0, the allocation information will be available only on the source site.

If the vSphere Replication Management servers at the source and at the target site are both 6.0, but one or more ESXi hosts at the target site are not 6.0 or later, if the vSphere Replication Management Server selects a target host that is not 6.0 or later, there will be no allocation information available on the target site.

NOTE Because vSphere Replication Management Server 6.0 cannot select only ESXi 6.0 hosts for the initial synchronization, the acceleration of the operations might vary depending on the selected host. To achieve maximum acceleration, all ESXi hosts at the target site that act as storage servers for vSphere Replication should be ESXi 6.0 or later.

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.

NOTE 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 6.0 can get allocation information from them only when they are on the target site. For this reason, the acceleration of the initial synchronization will be partial.

Replicating Virtual Machines Using Replication Seeds

To reduce the network traffic that is generated by data transfer during the initial full synchronization, vSphere Replication allows you to copy virtual disk files or use files that already exist in the target datastore, and point those as replication seeds when you configure a replication.

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, vSphere Replication looks for a disk with the same filename in the target datastore. If a file with the same name exists, vSphere Replication prompts you with a warning and offers you the option to use the existing disk file as a seed for the replication. If you accept the option, after the virtual machine replication is fully configured and enabled, vSphere Replication compares the differences and replicates only the changed blocks. If you do not accept the prompt, you must change the target location for your replication.

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.

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 replication in a single vCenter Server instance, you can select the source site as the target site for replication. You then configure 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 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," on page 98 for more information.

Configure Replication for a Single Virtual Machine to vCenter Server

vSphere Replication can protect individual virtual machines and their virtual disks by replicating them from one vCenter Server instance to another.

This procedure is for configuring replications to a target vCenter Server. To configure a replication to a cloud provider, see *vSphere Replication for Disaster Recovery to the Cloud*.

When you configure replication, you set a recovery point objective (RPO) to determine the maximum data loss that you can tolerate. For example, an RPO of 1 hour seeks to ensure that a virtual machine loses the data for no more than 1 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 "How the Recovery Point Objective Affects Replication Scheduling," on page 64.

Every time that a virtual machine reaches its RPO target, vSphere Replication records approximately 3800 bytes of data in the vCenter Server events database. If you set a low RPO period, this can quickly create a large volume of data in the database. To reduce the volume of data that is kept in the vCenter Server events database, limit the number of days that vCenter Server retains event data. See Configure Database Retention Policy in the *vCenter Server and Host Management Guide*. Alternatively, set a higher RPO value.

vSphere Replication guarantees crash consistency amongst 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 Matrixes for vSphere Replication 6.0 for quiescing support for Windows and Linux virtual machines.

You can configure virtual machines to replicate from and to Virtual SAN datastores. See "Using vSphere Replication with Virtual SAN Storage," on page 66 for the limitations when using vSphere Replication with Virtual SAN.

NOTE VMware Virtual SAN is a fully supported feature of vSphere 5.5 Update 1 and later.

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.

Procedure

1 On the vSphere Web Client Home page, click **vSphere Replication**.

2 Select a vCenter Server and in the left pane, double-click **Virtual Machines**.

On the **Related Objects** tab, the **Virtual Machines** tab lists the virtual machines.

3 Right-click the virtual machine and select **All vSphere Replication Actions > Configure replication**.

4 Select **Replicate to a vCenter Server**.

5 Select the target site.

- If you want to configure a replication to a local target site, select the target site from the list and click **Next**.

  If the source and target sites are not connected, the connection between the sites is configured when you click **Next**.

- If you want to configure a replication to a remote target site, and the source and target sites are connected, select the target site from the list and click **Next**.

- If you want to configure a replication to a remote target site, and the source and target sites are not connected, click **Add Remote Site**), enter the IP address or host name of the server where the target PSC runs, and provide the credentials of a user that has the **VRM remote.Manage VRM** privilege assigned. When the user is authenticated with the target site, all vCenter Server instances on which the vSphere Replication Management Server is registered with the Lookup Service appear in the list of target sites. Select the target site from the list and click **OK** and **Next**.

6 Accept the automatic assignment of a vSphere Replication server or select a particular server on the target site and click **Next**.

7 On the Target Location page, click **Edit** to select or change the target location datastore.

Optionally, you can select the virtual machine storage policy.

8 (Optional) To configure the replication of individual disks, click the name of the source virtual machine.

The list of disks on the source virtual machine expands.

For each disk, you can select the virtual format, storage policy, and a datastore where it is replicated. You can disable the replication of a disk by clicking **Disable** in its Replication Enabled row.

9 (Optional) On the Replication options page, select the quiescing method 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 Virtual Volumes.

---

10 (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.

11 On the Recovery settings page, use the RPO slider or the time spinners to set the acceptable period for which data can be lost in the case of a site failure.

The available RPO range is from 15 minutes to 24 hours.

12 (Optional) To save multiple replication instances that can be converted to snapshots of the source virtual machine during recovery, select **Enable** in the Point in time instances pane, and adjust the number of instances to keep.

NOTE You can keep up to 24 instances for a virtual machine. This means that if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is 4 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 check whether the RPO settings will create 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 6 replication instances per day, the RPO period should not exceed 4 hours, so that vSphere Replication can create 6 instances in 24 hours.

13 Click **Next**.

14 On the Ready to complete page, review the replication settings, and click **Finish**.

vSphere Replication starts an initial full synchronization of the virtual machine files to the designated datastore on the target site.

Configure Replication for Multiple Virtual Machines to vCenter Server

You can configure replication for multiple virtual machines from one vCenter Server instance to another by using the Multi-VM Configure Replication wizard.

When you configure replication, you set a recovery point objective (RPO) to determine the maximum data loss that you can tolerate. For example, an RPO of 1 hour seeks to ensure that a virtual machine loses the data for no more than 1 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 "How the Recovery Point Objective Affects Replication Scheduling," on page 64.

Every time that a virtual machine reaches its RPO target, vSphere Replication records approximately 3800 bytes of data in the vCenter Server events database. If you set a low RPO period, this can quickly create a large volume of data in the database. To reduce the volume of data that is kept in the vCenter Server events database, limit the number of days that vCenter Server retains event data. See Configure Database Retention Policy in the *vCenter Server and Host Management Guide*. Alternatively, set a higher RPO value.

vSphere Replication guarantees crash consistency amongst 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 Matrixes for vSphere Replication 6.0 for quiescing support for Windows and Linux virtual machines.

You can configure virtual machines to replicate from and to Virtual SAN datastores. See "Using vSphere Replication with Virtual SAN Storage," on page 66 for the limitations when using vSphere Replication with Virtual SAN.

Note VMware Virtual SAN is a fully supported feature of vSphere 5.5 Update 1 and later.

Configuring vSphere Replication on a large number of virtual machines simultaneously when using Virtual SAN storage can cause the initial full synchronization of the virtual machine files to run very slowly. Initial full synchronization operations generate heavy I/O traffic, and configuring too many replications at the same time can overload the Virtual SAN storage. Configure vSphere Replication in batches of a maximum of 30 virtual machines at a time.

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.

Procedure

1 On the vSphere Web Client Home page, click **vSphere Replication**.

2 Select a vCenter Server and in the left pane, double-click **Virtual Machines**.

   On the **Related Objects** tab, the **Virtual Machines** tab lists the virtual machines.

3 Select the virtual machines to replicate by using the Ctrl or Shift keys.

4 Right-click the virtual machines and select **All vSphere Replication Actions > Configure replication**.

   The virtual machines pass a validation check before they can be configured for replication.

5 Click **Next**.

6 Select **Replicate to a vCenter Server**.

7 Select the target site.

   - If you want to configure a replication to a local target site, select the target site from the list and click **Next**.

     If the source and target sites are not connected, the connection between the sites is configured when you click **Next**.

   - If you want to configure a replication to a remote target site, and the source and target sites are connected, select the target site from the list and click **Next**.

   - If you want to configure a replication to a remote target site, and the source and target sites are not connected, click **Add Remote Site**), enter the IP address or host name of the server where the target PSC runs, and provide the credentials of a user that has the **VRM remote.Manage VRM** privilege assigned. When the user is authenticated with the target site, all vCenter Server instances on which the vSphere Replication Management Server is registered with the Lookup Service appear in the list of target sites. Select the target site from the list and click **OK** and **Next**.

8 Accept the automatic assignment of a vSphere Replication server or select a particular server on the target site and click **Next**.

9 On the Target Location page, click **Edit** to select or change the target location datastore.

   Optionally, you can select the virtual machine storage policy.

10 (Optional) On the Replication options page, select the quiescing method 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 Virtual Volumes.

11 (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.

12 On the Recovery settings page, use the RPO slider or the time spinners to set the acceptable period for which data can be lost in the case of a site failure.

   The available RPO range is from 15 minutes to 24 hours.

13 (Optional) To save multiple replication instances that can be converted to snapshots of the source virtual machine during recovery, select **Enable** in the Point in time instances pane, and adjust the number of instances to keep.

   NOTE You can keep up to 24 instances for a virtual machine. This means that if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is 4 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 check whether the RPO settings will create 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 6 replication instances per day, the RPO period should not exceed 4 hours, so that vSphere Replication can create 6 instances in 24 hours.

14 Click **Next**.

15 Choose whether you want to use replication seeds.

This option searches the selected target datastore for replication seeds. If candidate files are found, confirm whether to use the files as seeds.

16 On the Ready to complete page, review the replication settings, and click **Finish**.

vSphere Replication starts an initial full synchronization of the virtual machine files to the designated datastore on the target site.

If a replication source virtual machine is powered off, the replication remains in `Not Active` state until you power on the virtual machine.

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

Other than the embedded vSphere Replication Server, you must have an additional vSphere Replication Server deployed and registered.

Procedure

1 Select a replication from **Outgoing Replications** or **Incoming Replications**.

2 Right-click a replication and select **Move to**.

3 Select a vSphere Replication Server from the list, and click **OK**.

The newly assigned server is updated in the vSphere Replication Server column.

Stop Replicating a Virtual Machine

If you do not need to replicate a virtual machine, you can stop the replication of that virtual machine.

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 as a VRM virtual machine replication user or a VRM administration user. See "vSphere Replication Roles Reference," on page 21.

Procedure

1 In the vSphere Replication Home page, go to the **Monitor** tab and click **Incoming Replications** or **Outgoing Replications**.

2 Right-click a replication and select **Stop**.

vSphere Replication asks you if you want to permanently stop the replication for the selected virtual machine.

NOTE The hosts and vSphere Replication server used by the replication must be accessible to stop a replication on both sites. If a host or the server is not accessible, you can force stop the replication on the accessible site by selecting **Force stop replication**. If you force stop the replication from **Incoming Replications**, you must also force stop the corresponding replication from **Outgoing Replications** if the source site is available. If you force stop the replication from **Outgoing Replications**, you can only recover or force stop the corresponding replication from **Incoming Replications**.

3 Click **Yes** to confirm that you want to stop replicating this virtual machine.

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.

- VMDK files are deleted from the target site datastore if the VMDK files were created when the replication was first configured.

NOTE When you stop a replication, vSphere Replication does not delete the replica directory at the target datastore. As a result, stale directories remain on VMFS and NFS target datastores, and unused namespaces remain on Virtual SAN and Virtual Volume target datastores. Because the maximum number of directories and namespaces on a datastore is limited, you must manually clean them up to free resources on the datastore. See "Clean Up the Target Datastore After You Stop a Replication," on page 75.

- VMDK files are not deleted and remain on the target datastore if you configured the replication to use existing disks at the target site as seeds.

Clean Up the Target Datastore After You Stop a Replication

When you stop a replication, vSphere Replication does not delete the replica directory at the target datastore.

As a result, stale directories remain on VMFS and NFS target datastores, and unused namespaces remain on Virtual SAN and Virtual Volume target datastores. Because the maximum number of directories and namespaces on a datastore is limited, you must manually clean them up to free resources on the datastore.

Prerequisites

Verify that you know the name of the replication that was stopped and its target datastore.

Procedure

1 Log in to the vSphere Web Client as and administrator user and navigate to the datastore that was the target for the stopped replication.

2 Enter the name of the stopped replication in the search text box and locate the folder that corresponds to this name.

3 Verify that the folder is empty and delete it.

Reconfiguring Replications

You can reconfigure a replication to modify its settings.

For example, you can reconfigure the replication to enable or disable 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.

To reconfigure replication parameters, select the replication from **Outgoing Replications** or **Incoming Replications**, and select **Reconfigure**.

Reconfigure Recovery Point Objectives (RPO) in Replications

You can modify the settings for already configured replications to specify different recovery point objectives (RPOs).

Procedure

1 Select a replication from **Outgoing Replications** or **Incoming Replications**.

2 Right-click a replication and select **Reconfigure**.

   You might be prompted to provide login credentials for the target site.

3 Click **Next** until you reach **Recovery settings**.

4 Modify the RPO settings for this replication.

5 Click **Finish** to save your changes.

Resize the Virtual Machine Disk Files of a Replication that Uses Replication Seeds

vSphere Replication prevents you from resizing the virtual machine disk files during replication. If you used replication seeds for the target disk, you can resize the disk manually.

Procedure

1 Stop the replication on the source site.

2 Resize the disk of the source virtual machine.

3 On the target site, resize the disk that is left over after you stopped the replication.

4 Configure the replication on the source virtual machine and use the resized disk on the target site as seed.

Resize Virtual Machine Disk Files of a Replication that Does Not Use Replication Seeds

vSphere Replication prevents you from resizing the virtual machine disk files during replication. If you did not use replication seeds during configuration of the target disk, vSphere Replication deletes the target disk when you stop the replication.

To resize a virtual machine disk if you did not initially use replication seeds, you must perform a recovery, resize the disk on source and target site manually, and use the target disk as a replication seed to configure a new replication.

Procedure

1 Run a planned migration of the replication.

2 Stop the replication.

3 Resize the disk on the source site.

4 Resize 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 replication by using the disks of the recovered virtual machine as seeds.

Change the Point in Time Settings of a Replication

You can reconfigure a replication to enable or disable 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 On the vSphere Replication Home page, click the **Monitor** tab, and click **Outgoing Replications**.

2 Select the replication that you want to reconfigure and click the **Reconfigure replication** icon , or right-click the replication source virtual machine and select **All vSphere Replication Actions > Reconfigure**.

The reconfiguration wizard opens. You might be prompted to provide login credentials for the target site.

3 Click **Next** until you reach the Recovery settings page of the wizard.

4 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** check box.
Disable the saving of point in time instances	Deselect the **Enable** check box.
Adjust the number of instances to keep	Use the spin-boxes to adjust the number of instances to keep per day and the number of past days for which you want to keep replication instances. NOTE You cannot keep more than 24 replication instances per virtual machine.

5 Click **Finish** to save your changes.

If you selected to disable 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.

Change the Target Datastore Location of a Replication

You can reconfigure a replication to change the datastore where replicated data is saved.

NOTE 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.

Procedure

1 In the vSphere Replication Home page, click the **Monitor** tab and click **Outgoing Replications** or **Incoming Replications**.

2 Right-click the replication for which you want to change the target datastore and select **Reconfigure**.

   The reconfiguration wizard open. You might be prompted to provide login credentials for the target site.

3 Click **Next** to reach the Target location page of the wizard.

4 Select the new target datastore.

5 Click **Next** until you reach the Ready to complete page and click **Finish** to save your settings.

vSphere Replication moves all replicated instances and configuration files to the new target datastore according to your settings.

Performing a Recovery with vSphere Replication

9

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 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 on the **Incoming 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 had 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.

This chapter includes the following topics:

- "Recover Virtual Machines by Using vSphere Replication," on page 79
- "Failback of Virtual Machines in vSphere Replication," on page 81

Recover Virtual Machines by Using 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.

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.

2 On the **Incoming Replications** tab, right-click the virtual machine to recover and select **Recover**.

3 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
Recover with 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.
Recover with 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.

4 Select the recovery folder and click **Next**.

5 Select the target compute resource and click **Next**.

6 If the virtual machine contains hard disks for which you have not enabled 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 enabled 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**.

7 (Optional) Select **Power on after recovery**.

8 Click **Finish**.

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 enabled 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," on page 98 for more information.

After a successful recovery, vSphere Replication disables 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, select **Stop replication**.

When the source virtual machine is no longer in the vCenter Server inventory, the replication is unconfigured. Unconfigured replications do not appear in the **Summary** tab nor in the **Incoming Replications** or **Outgoing Replications** tabs. Check vCenter Server task history for information on performed recoveries.

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

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. If target host or cluster has no access to the DVS the virtual machine was configured with at the source site, 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. You log in to the target site 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," on page 69.

Before you configure a reverse replication, you must unregister the virtual machine from the inventory on the source site.

Monitoring and Managing Replications in vSphere Replication 10

vSphere Replication provides a management interface where you can monitor and manage virtual machine replication and connectivity states for local and remote sites.

The **Home** tab in vSphere Replication lists all vCenter Servers that are joined in the same SSO server and the status of each vSphere Replication appliance with the total number of replications.

When you select a vCenter Server and go to the **Summary** tab, you can see vSphere Replication portlet with a summary of the target sites, and outgoing and incoming replications for the vSphere Replication appliance associated with that vCenter Server.

This chapter includes the following topics:

- "View the Replication Summary for a Site," on page 83
- "View Replication Reports for a Site," on page 84
- "Identifying Replication Problems in the Issues Tab," on page 87
- "Manage Target Sites," on page 87
- "Manage vSphere Replication Servers," on page 88

View the Replication Summary for a Site

You can view summarized information for the target sites and the status of incoming and outgoing replications for each site at the **Summary** tab of the vCenter Server to which vSphere Replication is registered.

You can view the following information about a site:

- The target sites and their current status.
- A graphical representation of all incoming and outgoing replications with color-coded states of the replicated virtual machines.

Prerequisites

Verify that vSphere Replication is running.

Procedure

1 Log in to the vSphere Web Client.

2 Select the vCenter Server root folder.

3 Click the **Summary** tab.

Replication States for Virtual Machines

vSphere Replication shows the replication states of virtual machines that you configured for replication.

State	Details for Each State
OK	OK, Moving, Recovering
Warning	Paused, OK(RPO violation), Not Active, Not Active(RPO violation), FullSync(RPO violation), Sync(RPO violation)
In Progress	FullSync, Sync, Initial Full Sync, Configuring
Error	Error, Error(RPO violation)
Recovered	Recovered

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.

Monitor Replication for Virtual Machines

You can monitor the replication status and view information for virtual machines configured for replication.

For more information about how to identify replication errors, see "Identifying Replication Problems in the Issues Tab," on page 87.

Prerequisites

- Verify that vSphere Replication is running.
- Verify that the virtual machines are configured for replication.

Procedure

1. Log in to the vSphere Web Client.
2. Select the vCenter Server to which the vSphere Replication appliance is registered.
3. Click **Monitor**, then click vSphere Replication.
4. Select **Outgoing Replications** to see details of the virtual machines replicated from this site.
5. Select **Incoming Replications** to see details of the virtual machines replicated to this site.

   According to the status of a selected replication, you can perform different actions on the replication.

View Replication Reports for a Site

If you observe frequent RPO violations, want to learn more about the network usage of vSphere Replication, or check the status of your incoming and outgoing replications, you can view replication statistics for source and target vCenter Server sites.

Prerequisites

Verify that vSphere Replication is running.

Procedure

1. In the vSphere Web Client Home view, click **vSphere Replication**.

2 On the vSphere Replication Home tab, click **Monitor**.

3 Click **Reports**.

The Reports page displays two types of data, current and historic. Current data appears in the graphs on the left, and historic data is displayed on the right of the Reports page.

NOTE Data is collected in 5 minute intervals and the graphs represent aggregated data for each interval. Therefore, you cannot see the exact moment when a peak value occurred.

Table 10-1. Types of Data that vSphere Replication Collects

Data Type	Report
Current data	■ Replicated VMs (by VC) ■ Replicated VMs (by Hosts)
Historic data	■ Bytes transferred for all outgoing replications ■ Bytes transferred for a specific outgoing replication ■ RPO violations ■ Replications Count ■ Site connectivity ■ VR server connectivity

What to do next

- You can use the drop-down menu above the historic data reports to limit the time range of the reports.
- You can maximize report widgets to zoom in the data.
- When you maximize the report for transferred bytes, you can use the drop-down menu to filter data by virtual machine. This helps you identify virtual machines that generate the most intense replication traffic in your environment.

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.

Server and site connectivity, number of RPO violations, and other metrics give you, as an administrator, the information you need to diagnose replication issues.

The following sections contain examples of interpreting the data displayed under **Reports** on the **vSphere Replication** tab under **Monitor**.

RPO Violations

The large number of RPO violations can be caused by various problems in the environment, on both the source and the target site. With more details on historical replication jobs, you can make educated decisions on how to manage the replication environment.

Table 10-2. Analysing RPO Violations

Probable Cause	Solution
■ The network bandwidth cannot accommodate all replications. ■ The replication traffic might have increased. ■ The initial full sync for a large virtual machine is taking longer than the configured RPO for the virtual machine.	■ Disable the replication on some virtual machines with high change rate to allow lower change rate virtual machines to meet their RPO objectives. ■ Increase the network bandwidth for the selected host. ■ 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. ■ 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 could be related to this increase. ■ 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 source and the target site. ■ An infrastructure change might have occurred on the target site.	■ Check the site connectivity data to verify the connection between the source and target site. ■ Check if the infrastructure on the target site has changed or is experiencing problems that prevent vSphere Replication from writing on the target datastores. For example, storage bandwidth management changes made to target hosts might result in storage delays during the replication process. ■ 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 make decisions on how much bandwidth might be required to meet RPO objectives.

Table 10-3. Analysing the Rate of Transferred Bytes and RPO Violations

Graph Values	Probable Cause	Solution
■ High rate of transferred bytes and high number of RPO violations ■ Low rate of transferred bytes and high number of RPO violations	The network bandwidth might be insufficient to accommodate all replications.	■ Maximize the transferred bytes graph and use the drop-down menu to filter the data by virtual machine. Disable the replication on some virtual machines with high change rate to allow lower change rate virtual machines to meet their RPO objectives. ■ Increase the network bandwidth for the selected host.
■ High rate of transferred bytes and a few or no RPO violations ■ Low rate of transferred bytes and a few or no RPO violations	The environment operates as expected.	N/A

Replicated Virtual Machines by Host

The number of replicated virtual machines by host help you determine how replication workload is distributed in your environment. For example, if the number of replicated virtual machines on a host is high, the host might be overloaded with replication jobs. You might want to verify that the host has enough resources to maintain all replication jobs. If needed, you can check for hosts with low number of replicated virtual machines and optimize the allocation of resources in your environment.

Identifying Replication Problems in the Issues Tab

You can view and troubleshoot possible vSphere Replication problems that might occur during replication at the **Issues** tab of the corresponding vCenter Server.

Table 10-4. 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 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, the replication pauses and goes to an error state.	Reconfigure the replication and enable or disable the newly added disk.
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.
Error	You do not use replication seeds during configuration, but a disk with the same name is found during configuration.	Reconfigure the replication.
RPO Violation	A replication contains an RPO violation.	See "Reconfigure Recovery Point Objectives (RPO) in Replications," on page 76.

Manage Target Sites

You can reconnect and disconnect target replication sites, and create connections to new target sites.

To create a connection to a new target site, see "Configure vSphere Replication Connections," on page 36.

Prerequisites

Verify that vSphere Replication is running.

Procedure

1 Log in to the vSphere Web Client.

2 On the vSphere Web Client Home page, click **vSphere Replication**.

3 Click **Manage** and click **vSphere Replication**.

4 In **Target Sites**, right-click a site and select **Disconnect** or **Reconnect**.

Manage vSphere Replication Servers

You can deploy and register new vSphere Replication Server instances in addition to the embedded one that is included with the vSphere Replication appliance by default.

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 Web Client.

2 Select the vCenter Server to which the vSphere Replication appliance is registered.

3 Click **Manage** and click the **vSphere Replication** tab.

4 In the **Replication Servers** section, click the icons to manage vSphere Replication servers.

Option	Description
Deploy new vSphere Replication Server from an OVF template	Click to deploy an additional vSphere Replication Server. See Chapter 5, "Deploying Additional vSphere Replication Servers," on page 43.
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," on page 44.
Configure the selected vSphere Replication Server	Click to access the VAMI of the vSphere Replication Server that you selected from the list.
Reconnect	Click if the status of the vSphere Replication Server that you selected from the list is `Disconnected`.
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," on page 45.

Troubleshooting vSphere Replication 11

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 10, "Monitoring and Managing Replications in vSphere Replication," on page 83 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.

This chapter includes the following topics:

- "vSphere Replication Limitations," on page 89
- "Access the vSphere Replication Logs," on page 90
- "vSphere Replication Events and Alarms," on page 91
- "Solutions for Common vSphere Replication Problems," on page 94

vSphere Replication Limitations

vSphere Replication is subject to some limitations when replicating virtual machines.

Replicating Large Volumes

vSphere Replication can replicate virtual machines greater than 2TB with the following limitations:

- If you move a virtual machine with replicated disks larger than 2032GB to an ESXi 5.1 or earlier host, vSphere Replication cannot replicate or power on the virtual machine.
- With ESXi 5.5 or later, vSphere Replication supports a maximum disk size of 62TB.
- Full sync of very large disks can take days.
- vSphere Replication must track changed blocks and can consume more memory depending on the amount of data written on the disk.
- vSphere Replication tracks larger blocks on disks over 2TB. Replication performance on a disk over 2TB might be different than replication performance on a disk under 2TB for the same workload depending on how much of the disk goes over the network for a particular set of changed blocks.
- Replication might consume more or less bandwidth depending on the workload and how it changes blocks on the disk during the RPO interval.

Shared Disk Support

vSphere Replication cannot replicate virtual machines that share vmdk files in this release.

Raw Device Mapping (RDM)

vSphere Replication supports replicating RDMs in Virtual Compatibility Mode. RDMs in Physical Compatibility Mode cannot be configured for replication.

Snapshots

vSphere Replication does not replicate virtual machine snapshot hierarchy at the target site.

Powered off Virtual Machines

You can configure virtual machines that are powered off for replication. However, actual replication traffic begins when the virtual machine is powered on.

Access the vSphere Replication Logs

You can use the vSphere Replication logs for system monitoring and troubleshooting. A VMware support engineer might request these logs during a support call.

To access and download the vSphere Replication logs, you need access to the vSphere Replication virtual appliance management interface (VAMI). vSphere Replication rotates its logs when the log file reaches 50MB and keeps at most 12 compressed log files.

To manually copy log files, see "Manually Access the vSphere Replication Logs," on page 90.

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 vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.

2. Click the **VRM** tab and click **Support**.
3. Click **Generate** 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.

4. Click the link to download the package.
5. (Optional) Click **Delete** next to existing log packages to delete them individually.

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`

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.

Configure vSphere Replication Alarms

You can define and edit alarms to alert you when a specific vSphere Replication event occurs.

You can create an alarm that triggers when a specific 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.

Table 11-1. 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

Table 11-1. vSphere Replication Events (Continued)

Event Name	Event Description	Event Type	Category	Event Target
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
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 11-1. 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
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

Table 11-1. vSphere Replication Events (Continued)

Event Name	Event Description	Event Type	Category	Event Target
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 vCenter Management Web service being paused or stopped.

Solution

Attempt to start the vCenter Management Web 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.

Connection Errors Between vSphere Replication and SQL Server Cannot be Resolved

You cannot resolve a connection error between the vSphere Replication appliance and SQL Server.

Problem

vSphere Replication might not be able to connect to SQL Server, and you have insufficient information to solve this problem.

Cause

Several issues can cause this problem, and initially available information about the problem is insufficient to affect a resolution.

Solution

1 Use a file management tool to connect to the vSphere Replication appliance.

   For example, you might use SCP or WinSCP. Connect using the root account, which is the same account used to connect to the VAMI.

2 Delete any files you find in `/opt/vmware/hms/logs`.

3 Connect to the VAMI and attempt to save the vSphere Replication configuration.

   This action recreates the SQL error.

4 Connect to the vSphere Replication appliance again and find the `hms-configtool.log` file which is in `/opt/vmware/hms/logs`.

   This log file contains information about the error that just occurred. Use this information to troubleshoot the connection issue, or provide the information to VMware for further assistance. See "Reconfigure vSphere Replication to Use an External Database," on page 58.

Application Quiescing Changes to File System Quiescing During vMotion to an Older Host

vSphere Replication can create an application quiesced replica for virtual machines with Windows Server 2008 and Windows 8 guest operating systems running on an ESXi 5.1 or newer host.

Problem

The ESXi 5.1 or newer host is in a cluster with hosts from older versions and you use vMotion to move the replicated virtual machine to an older host. vSphere Replication then creates a file system quiesced replica.

Cause

A mix of ESXi 5.1 (or newer) and older hosts in the cluster creates a file system quiesced replica during vMotion to an older host. The process should instead create an application quiesced replica.

Solution

Make sure that all hosts in the cluster are running ESXi 5.1 or newer before you use vMotion to move a Windows Server 2008 and Windows 8 virtual machine with application quiescing.

Configuring Replication Fails for Virtual Machines with Two Disks on Different Datastores

If you try to configure vSphere Replication on a virtual machine that includes two disks that are contained in different datastores, the configuration fails.

Problem

Configuration of replication fails with the following error:

`Multiple source disks with device keys` *`device_keys`* `point to the same destination datastore and file path` *`disk_path`*`.`

Cause

This problem occurs because vSphere Replication does not generate a unique datastore path or file name for the destination virtual disk.

Solution

If you select different datastores for the VMDK files on the protected site, you must also select different datastores for the target VMDK files on the secondary site.

Alternatively, you can create a unique datastore path by placing the VMDK files in separate folders on a single target datastore on the secondary site.

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, select the vCenter Server instance and click **Manage > Settings > Advanced Settings** to check that the `VirtualCenter.FQDN` key is set to either a fully qualified domain name or to a literal address.
2. Use a supported browser to log in to the vSphere Replication VAMI.

   The URL for the VAMI is https://*vr-appliance-address*:5480.
3. Review and confirm the browser security exception, if applicable, to proceed to the login page.
4. Type the root user name and password for the appliance.

   You configured the root password during the OVF deployment of the vSphere Replication appliance.
5. Enter the same FQDN or literal address for vCenter Server as you set for the `VirtualCenter.FQDN` key.
6. Click **Save and Restart Service** to apply the changes.

Scalability Problems when Replicating Many Virtual Machines with a Short RPO to a Shared VMFS Datastore on ESXi Server 5.0

Performance might be slow if you replicate a large number of virtual machines with a short Recovery Point Objective (RPO) to a single virtual machine file store (VMFS) datastore that is accessible by multiple hosts on the recovery site.

Problem

This problem occurs when running ESXi Server 5.0 on the recovery site. It can result in missed RPO targets.

The number of virtual machines that can successfully replicate to a single, shared VMFS datastore increases if the RPO targets are longer.

Follow the guidelines when calculating the number of virtual machines that you should replicate to a single VMFS volume on the recovery site.

- If all your virtual machines have an RPO of 15 minutes, performance is affected when replicating 50 to 100 virtual machines to the same VMFS datastore.
- If all your virtual machines have an RPO of 30 minutes, performance is affected when replicating 100 to 200 virtual machines to the same VMFS datastore.

If you have heterogeneous RPO targets in a protection group, calculate the harmonic mean of the RPO targets when calculating the number of virtual machines that you can replicate to a single VMFS volume. For example, if you have 100 virtual machines with an RPO of 20 minutes and 50 virtual machines with an RPO of 600 minutes, you calculate the harmonic mean of the RPO as follows:

150/(100/20 + 50/600) = ~30

In this example, the configuration is similar to a setup with 150 virtual machines, each having an RPO of approximately 30 minutes. In this case, performance is affected if these 150 virtual machines replicate to a single VMFS volume.

Cause

This problem affects only VMFS datastores that are shared by multiple hosts. It does not occur on datastores that are local to one host or on other datastore types, such as NFS. This problem affects only installations that are running ESXi Server 5.0.

The number of vSphere Replication servers is not relevant. These limits apply to the number of virtual machines that you can replicate to a single VMFS datastore.

Solution

1. Upgrade ESXi Server to version 5.1 or later on the recovery site.
2. If you cannot upgrade ESXi Server to version 5.1 or later, redistribute the replicated virtual machines or adjust their RPO.
   - Reduce the number of virtual machines with a short RPO that replicate to a single VMFS volume, for example by using a larger number of smaller datastores.
   - Increase the RPO of the virtual machines replicating to a single VMFS volume to create a longer harmonic mean RPO.

vSphere Replication Sites Appear in the Not Authenticated State

vSphere Replication sites that you have connected appear in the `Not authenticated` state.

Problem

In configurations with two vSphere Replication sites where each includes a vCenter Server instance and a vSphere Replication appliance, the vSphere Replication sites can appear in the `Not authenticated` state, even if you have successfully connected the sites.

Cause

Sites that you have successfully connected can appear in the `Not authenticated` state when you establish a new login session to the vSphere Web Client and the previous login session has timed out. In this case, the `Not authenticated` state reflects the connection to the remote site from the vSphere Web Client and not the state of the connection between the sites. If the two sites are running, vSphere Replication still performs replications at the schedules that you have configured. To restore the `Connected` state in the vSphere Web Client, you must provide the login credentials for the remote site.

Solution

1 In the vSphere Web Client, select the vCenter Server to which the vSphere Replication is registered.

2 Click the **Manage** tab, and click **vSphere Replication**.

3 In **Target Sites**, right-click the remote site, select **Reconnect site**, and click **Yes**.

4 Enter the login credentials for the Platform Service Controller (PSC) on the remote site, and click **OK**.

   The address of the PSC is pre-populated, but you can enter a new address if necessary. For example, if the target vCenter Server was moved for load balancing, it might be managed by a new PSC.

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 inventory.

Solution

Recover the virtual machine in a different `VMs and Templates` folder in the same datacenter. 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 might 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.

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.
- To calculate bandwidth requirements, see http://kb.vmware.com/kb/2037268.

vSphere Replication Appliance Extension Cannot Be Deleted

If you delete the vSphere Replication appliance virtual machine, the virtual appliance management interface (VAMI) 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.

   See "Unregister vSphere Replication from vCenter Server if the Appliance Was Deleted," on page 40

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. vSphere Replication operations are also unavailable if you reinstall vCenter Server.

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 disables 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 VAMI to connect vSphere Replication to the original vCenter Server instance.

   a Reconnect the ESXi host to vCenter Server.

   b Connect to the VAMI of the vSphere Replication server at https://*vr-server-address*:5480 .

   c Select the **Configuration** tab.

   d Type **`username:password@vcenter_server_address`** in **vCenter Server Address**, where username and password are credentials of the vCenter Server administrator.

   e Type the correct managed object id of the appliance VM in **Appliance VM MO value**. Use the vCenter Server MOB to obtain the appliance id.

   f Click **Save and Restart Service**.

   If you use the VAMI 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.
- `Error – Unable to reverse replication for the virtual machine 'virtual machine name'. VRM Server generic error. Please check the documentation for any troubleshooting information. Exception details: 'org.hibernate.exception.LockAcquisitionException: Transaction (Process ID 57) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Rerun the transaction.` This problem relates to a deadlock in Microsoft SQL Server.

Cause

vSphere Replication sends this message when it encounters configuration or infrastructure errors. For example, network issues, database connection 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 Servers Has Changed Its IP Address

When the vCenter Server address of one site changes, the connection status between two sites is displayed as `Connection issue` 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 `Connection issue` appears and you cannot reconnect the sites.

Solution

1. Open the VAMI 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.
3. Click **Save and Restart**.
4. In the vSphere Web Client, verify that the status of the connection between the two sites is `Connection issue`.
5. Select **Reconnect to the selected site** ( ).
6. Enter the IP address or host name of the server where the Platform Service Controller (PSC) runs, and provide the credentials of a user that has the **VRM remote.Manage VRM** privilege assigned.

   You can check the PSC address in the vSphere Replication VAMI on the target site, on the **SSO** tab under **VR**, in the **LookupService Address** text box.
7. In the list of available vCenter Server instances, select the vCenter Server with the changed IP address and click **OK**.
8. Verify that the connection between the two sites is successfully restored and the status is `Connected`.

Uploading a Valid Certificate to vSphere Replication Results in a Warning

When you upload a custom certificate to the vSphere Replication appliance, you see a warning even if the certificate is valid.

Problem

When you use the virtual appliance management interface (VAMI) in Internet Explorer to upload certificates to the vSphere Replication appliance, you see a certificate error:

```
The certificate installed with warnings. Remote VRM systems with the 'Accept only SSL
certificate signed by a
trusted CA' option enabled may be unable to connect to this site for the following reason: The
certificate was not issued
for use with the given hostname: vr_appliance_hostname.
```

Solution

Ignore this error, or connect to the VAMI by using a supported browser other than Internet Explorer.

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 each host's SSL thumbprint registry. 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 `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

- Click the global **Refresh** button in the vSphere Web Client.
- Log out the vSphere Web Client 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 source site is refused.

Problem

When you refresh the incoming replications list on a remote site soon after the connection to the source site has become unavailable, the replications do not display due to a communication error between the two sites.

Solution

Refresh the vSphere Web Client. 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

- Log into the virtual appliance management interface (VAMI) of the vSphere Replication appliance and click **Configuration > Save and Restart Service**.

  Do not change any configuration information before clicking **Save and Restart Service**.

  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 "vSphere Replication Network Ports," on page 26.

Anti-virus Agent in Firewall Terminates Virtual Machine Replication

If a virtual machine contains virus information, an anti-virus agent in the firewall might detect the virus data and terminate 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 Virtual SAN Storage Is Slow

When using VMware Virtual SAN 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 Virtual SAN 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 Virtual SAN storage.

Solution

Configure vSphere Replication in batches of a maximum of 30 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 or reset its database on one of the sites, 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, and you know the GID value of that replication, use the Managed Object Browser (MOB) of the vSphere Replication Management server to delete the replication.
  a Navigate to https://*vrms_address*:8043/mob/?moid=GID-*orphaned_replication_GID*&vmodl=1

    Where *vrms_address* is the IP address of the vSphere Replication Management server.

  b Invoke the destroy method to remove the replication from the site on which the vSphere Replication Management server runs.

- If you have not reinstalled the vSphere Replication Management server and orphaned replication exists in your environment, but you do not know the GID value of that replication, the value can be retrieved from the log files or the vSphere Replication Management server database. Contact VMware Global Support Services for assistance.
- 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.

Not Active Replication Status of Virtual Machines

The replication status of a virtual machine might appear as `Not active` without an obvious reason.

Problem

You use a vSphere Replication Server on the target site to manage replications, and the replication status for the virtual machines that this vSphere Replication Server manages is `Not active` though there is no obvious reason for this status.

Cause

The vSphere Replication appliance does not check the connectivity between vSphere Replication Server instances that you register and the ESXi host on the primary site. If you deploy vSphere Replication servers on the target site, but these servers cannot access the ESXi host on the primary site, the vSphere Replication servers register successfully with the vSphere Replication appliance, but cannot operate as expected.

Solution

- If the replication status of a virtual machine is `Not active`, check the network connectivity between the host on which the replicated virtual machine is running and the target vSphere Replication Server.

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 Virtual SAN storage, monitor the I/O latency by using the monitoring tool in the Virtual SAN interface.

Error at Reconfiguring the vSphere Replication Management Server from the Virtual Appliance Management Interface

When you click **Save and Restart** in the virtual appliance management interface (VAMI) of vSphere Replication, the HMS service cannot start, and you can no longer manage replications.

Problem

If you use the virtual appliance management interface (VAMI) to install a new SSL certificate, to change the IP address of the VRM host, or apply another setting on the VR tab, and you click **Save and Restart**, the following error message appears:

```
Missing command-line argument.
```

Cause

The OVF environment of the vSphere Replication appliance might be missing or corrupted.

Solution

1 Establish an SSH connection to the vSphere Replication appliance and navigate to `/opt/vmware/etc/vami/`.

2 Open the `ovfEnv.xml`.

   a If the `ovfEnv.xml` file is not empty, search for the `vServiceEnvironmentSection` element. If the `vServiceEnvironmentSection` element is missing, there might be a problem with the vCenter Management Web Services process on the vCenter Server machine. Verify that the vCenter Management Web Services is running on the vCenter Server machine and then try powering the vSphere Replication appliance off and on. To power the appliance off and on, use the vSphere Web Client while you are connected to the vCenter Server, and not directly to the ESXi host.

   b If the `ovfEnv.xml` file is empty, try to power off and on the vSphere Replication appliance by using the vSphere Web Client while you are connected to the vCenter Server, and not directly to the ESXi host.

3 If powering the vSphere Replication appliance does not resolve the issue, most certainly the appliance has been temporarily removed and re-added in the vCenter Server. There is no solution for restoring the OVF environment in that case. You must re-deploy the vSphere Replication appliance by using an empty database, and configure all replications from scratch.

Unable to Establish an SSH Connection to the vSphere Replication Appliance

SSH connections to the vSphere Replication appliance are disabled.

Problem

To apply custom settings to vSphere Replication, you need to 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 disabled, you cannot apply the changes that you need, and you cannot transfer files.

Cause

By default, SSH connections to the vSphere Replication appliance are disabled to strengthen the security in your environment.

Solution

Prerequisites

Verify that you have the root user credentials to log in to the vSphere Replication appliance.

Procedure

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.

```
/usr/bin/enable-sshd.sh
```

Procedure

The script configures the vSphere Replication appliance to enable SSH connections.

The Replication Pauses When You Add a New Disk To the Source VM

You added a new disk to the source VM, which made the replication pause.

Problem

When you add a new disk to the source VM, 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.

Index

A

accessing the Summary tab **83**
adding disk **108**
adding vSphere Replication servers **88**
Advanced Settings dialog box, vSphere Replication **76**
alarms **91**
anti virus agent terminates replication **104**
Application quiescing during vMotion **95**

B

before installing **32**
block allocation **68**

C

calculating bandwidth for vSphere Replication **29**
causes of RPO violations **98**
change the target datastore location **68**
changing the datastore **77**
changing keystore password; changing truststore password **55**
client plug-in **10**
combined appliance **15**
compatibility with ESXi, compatibility with vCenter Server, compatiblity with Site Recovery Manager, compatibility with Web browsers **28**
compatibility with vSphere features **26**
compression **17**
configure alarms **91**
configuring replication servers **88**
connection issue **38, 63, 101**
connection states **37**
connections
  reconnecting **38**
  repairing **38**

D

data compression **17**
datastore location **77**
datastore tags **40**
datastore clean up **75**
deleting vSphere Replication **40**
deleting vSphere Replication appliance extension **99**
disable embedded vSphere Replication Server **46**
disabled compression **17**
disabling points in time **77**
disconnecting sites **87**
distributed switch **14, 15**

E

enable points in time **77**
enabling SSH **107**
enabling SDRS support **34**
end-to-end compression **17**
endpoint **34**
events **91**

H

HBR server **16**
High Availability **26**

I

incoming replications do not display **103**
initial synchronization **68**
installation overview **32**
installing vSphere Replication **31**
IPv4 **14, 15**
IPv6 **14, 15**
issues tab, identify replication issues **87**

L

latency, and vSphere Replication **106**
licensing **25**
Lookup Service **34**

M

manage replication servers **88**
managing **83**
managing sites **87**
manual reprotection, failback **81**
missing command-line argument **107**
monitoring **83**
MPIT retention **64**

N

network compression **70, 72**
network settings, vSphere Replication appliance **56**
network traffic **13**
network compression disabled **17**
network ports **26**
network traffic isolation **13**
NFS **75**
not authenticated **63**

O

operational limits **26**
outgoing traffic **13**
overview, introduction to vSphere Replication, vSphere Replication and vCenter Server Appliance, vCenter Server Appliance **9**
OVF, cannot be deployed **94**

P

pause **108**
PIT recovery **66**
points in time **70, 72, 77**
port group **14, 15**
pre-installation tasks **32**
public key certificates, vSphere Replication requirements **54**

Q

quiescing **70, 72**

R

reconfiguring
  datastore location **77**
  point in time instances **77**
reconfiguring replication **76**
reconfiguring VRMS **107**
reconnecting sites **38, 87**
reconnecting sites if vCenter Server IP changes **101**
recover virtual machine **79**
recover virtual machines **79**
recovering virtual machines at specific point in time **66**
recovering virtual machines with same name **98**
replicate virtual machines, in a single vCenter Server **70**
replicate virtual machines using vSphere Replication **70**
replicated VMs count **84**
replication
  configuration fails **96**
  missed RPO target **97**
  replication seeds **69**
  scalability issue with VMFS **97**
  troubleshooting **96, 97**
  virtual machines with two disks **96**
replication footprint **75**
replication instances **77**
replication states **84**
replication statistics **85**
replication traffic **14, 15**
replication pause **108**
Replication fails after rebuilding VRMS **105**
replication monitoring, monitor replication **84**
replications count **84**
replications not active **63**
reports **84**
Resize VMDK file, with replication seeds **76**
Resize VMDK file, without replication seeds **76**
retention policy **64**
roles and permissions **19**
RPO violations **85**
RPO and MPIT **64**
RPO and replication scheduling **64**
RPO violation **106**

S

SCP **107**
SDRS on target site **34**
security settings, vSphere Replication appliance **55**
SFTP **107**
Single Sign-On **34**
site
  source **11**
  target **11**
site connectivity **85**
site states
  Enabled (Configuration issue) **35**
  Enabled (Not accessible) **35**
  Not installed **35**
snapshots **77**
sneakernet, replication **69**
solutions for common issues **94**
source site, host compatibility requirements **11**
SSH connections **107**
SSL certificate
  change **52**
  vSphere Replication **52**
SSO **34**
stale directories **75**
standard switch **14, 15**

statistics
  RPO violations **85**
  site connectivity **85**
  transferred bytes **85**
  VR server connectivity **85**
Storage vMotion **26**
Storage DRS **26**
supported databases **60**
synchronization speed **68**
synchronizing data **68**
system requirements **25**
system logs, replication logs **90**

T

target sites
  disconnecting **87**
  managing **87**
  reconnecting **87**
target site, host compatibility requirements **11**
traffic isolation **13–15**
traffic limits **13**
transferred bytes **84, 85**
troubleshooting
  additional servers **106**
  connectivity **106**
  not active **106**
  not-authenticated **103**
  reverse replications **103**
troubleshooting replication, troubleshooting recovery **89**

U

uninstall vSphere Replication **39**
unregistering vSphere Replication **40**
unused namespaces **75**
updated information **7**
upgrading vSphere Replication **47**
upgrading vSphere Replication with ISO image **47**
UUID **66**

V

vCenter Single Sign-On **34**
vCenter Server, change SSL certificate **104**
virtual appliance, unregister **39**
Virtual Volume **75**
Virtual SAN
  and PIT snapshots **66**
  I/O latency **66**
  initial full sync is slow **105**
  limits **66**
  root folders **66**
  supported load **66**
  using with vSphere Replication **66**
VM NIC **15**
VMkernel adapter **14, 15**
VR server connectivity **85**
VRMS reconfiguration **107**
VSAN **26, 66, 105, 106**
vSphere features, compatibility with **26**
vSphere Flash Read Cache **26**
vSphere Replication
  certificate warning **101**
  custom certificates **101**
  deployment **33**
  external database **58**
  features unavailable **94**
  generic error **100**
  host moved **99**
  how it works **11**
  log bundles **102**
  remove replication **74**
  replicate virtual machines **72**
  sites not authenticated **98**
  SQL Server connection fails **95**
  stop replication **74**
vSphere Replication appliance
  certificate verification **53**
  connect **36**
  contents **10**
  embedded database **61**
  general settings **52**
  network settings **56**
  pair **36**
  reboot **58**
  reconfigure **51**
  shutdown **58**
  system settings **58**
  time zone **58**
  VAMI **10**
  virtual appliance management interface **10**
vSphere Replication roles **21**
vSphere Replication server
  change certificate **44**
  deploy **43**
  deploy additional **43**
  move **74**
  network settings **44**
  reconfigure **44**
  remove **45**
  restart **44**
  settings **44**
  unregister **45**
vSphere Replication Server, register **44**

vsphere replication tags **40**
vSphere Replication pairing, unresolved host error **96**
vSphere Replication access to port 80 **104**
vSphere Replication Administration, introduction **5**
vSphere Replication database
configure Oracle Server **61**
configure SQL Server **60**
vSphere Replication limitations, replicating large volumes, shared disk support **89**
vSphere Replication Modified Administrator Role **21**
vSphere Replication network bandwidth **28**
vSphere Replication operations take too long to complete **102**
vSphere Replication Recovery User Role **20**
vSphere Replication Server registration takes several minutes **102**
vSphere Replication solution user **34**
vSphere Replication User Role **20**
vSphere Replication Viewer Role **19**