

vSphere Replication for Disaster Recovery to Cloud

vSphere Replication 8.2



vmware®

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

<https://docs.vmware.com/>

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

docfeedback@vmware.com

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

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 About Disaster Recovery to Cloud 4**
- 2 Disaster Recovery to Cloud System Requirements and Compatibility 5**
 - Roles and Permissions That Disaster Recovery to Cloud Requires 5
- 3 Installing and Configuring vSphere Replication to Cloud 7**
 - Installing vSphere Replication for Disaster Recovery to Cloud 7
 - Upgrading vSphere Replication from Earlier Product Versions 8
 - Configure the NTP Synchronization in Your Environment 8
 - How vSphere Replication Connects to Cloud 9
 - Configuring the Connection to the Cloud 11
- 4 Replicating Virtual Machines to Cloud 17**
 - Configure a Replication to Cloud 17
 - Using Replication Seeds for Replications to Cloud 20
- 5 Reconfiguring Replications to the Cloud 21**
 - Reconfigure a Replication to Cloud 21
- 6 Recovering Virtual Machines to Cloud 23**
 - Test Recovering Virtual Machines to Cloud 23
 - Planned Migration to Cloud 25
- 7 Configuring Replications from Cloud 27**
 - Configure a Replication from Cloud 28
 - Reverse a Replication to Cloud 30
 - Configure Failback Recovery Settings for Replications from the Cloud 31
- 8 Recovering Virtual Machines from Cloud 32**
 - Test Recovering Virtual Machines from Cloud 32
 - Recover a Virtual Machine from Cloud 34
- 9 Monitoring and Managing Replications in vSphere Replication 36**
 - Monitoring the Status of Replications 36
 - Pause or Resume a Replication 37
 - Stop a Replication to Cloud 38
 - Stop a Replication from Cloud 39

About Disaster Recovery to Cloud

1

You can subscribe to a Disaster Recovery service to protect your vSphere workloads.

With Disaster Recovery to Cloud, administrators of small sites can protect their vSphere virtual workloads from a wide class of disasters by replicating those workloads into the cloud. Disaster Recovery to Cloud uses the host-based replication feature of vSphere Replication to copy the protected source virtual machines into the infrastructure of the cloud provider. If a disaster occurs, the Disaster Recovery to Cloud servers can convert the replicated data into vApps and virtual machines in the cloud.

Disaster Recovery to Cloud System Requirements and Compatibility

2

To enable replications to the cloud, your environment must meet certain requirements in terms of additional configuration and specific versions of the VMware products that you use.

System Requirements

Disaster Recovery to Cloud has the same requirements to the environment as vSphere Replication. In addition, Disaster Recovery to Cloud requires that ports 10000–10010 of the ESXi hosts are open for outgoing traffic. The required ports are open automatically when you install a VIB on each supported ESXi host in the environment where the vSphere Replication appliance is deployed. See [How vSphere Replication Connects to Cloud](#).

Product Compatibility

Replications to the cloud require that you run certain versions of VMware products on the local site and on the cloud site. Your cloud provider ensures that the target environment is configured for replications to cloud. You must verify that you run a supported version of the following products on the local site.

Table 2-1. Compatible Product Versions on the Source Site for Replications to the Cloud

Product	Supported Version
vSphere Replication appliance	8.2
ESXi host	5.0, 5.1.x, 5.5.x, 6.0, 6.5, and 6.7
vCenter Server	6.7
vSphere Client	6.7

Roles and Permissions That Disaster Recovery to Cloud Requires

Replications to the cloud require certain users, roles, and permissions.

vSphere Web Client

On the source vSphere site, you need the same credentials as the ones required for vSphere Replication. See [vSphere Replication Roles Reference](#).

vCloud User Credentials

When you create a connection to the target virtual data center, you provide two pairs of credentials.

Connection Credentials Used for authenticating within the cloud organization, these credentials initiate a user session with your cloud provider. Your cloud provider manages the privileges for your user account.

- **com.vmware.hcs.{com.vmware.hcs}:ManageRight**
- **com.vmware.hcs.{com.vmware.hcs}:ViewRight**
- **Organization.View Organization Networks**
- **Organization.View Organizations**
- **Organization VDC.View Organization VDCs**

Credentials to the cloud are required for each target site, once per user session, and not per operation. When the authenticated user session to a target site expires, users are prompted to input their credentials again.

System Monitoring Credentials

Used at runtime to let the source and the target site communicate. These credentials are stored in the vSphere Replication appliance on the source site. The user name that you provide must be assigned the vSphere Replication role, or the following rights in your cloud organization.

- **com.vmware.hcs.{com,vmware.hcs}:ManageRight**
- **com.vmware.hcs.{com,vmware.hcs}:ViewRight**
- **Organization.View Organization Networks**
- **Organization.View Organizations**
- **Organization VDC.View Organization VDCs**

Although you can use the same credentials for both connection and system monitoring, a good practice is to use different pairs of credentials.

Installing and Configuring vSphere Replication to Cloud

3

Before you configure replications to the cloud, you must deploy the vSphere Replication appliance on the source site and set up your environment to enable connections to the cloud.

This chapter includes the following topics:

- [Installing vSphere Replication for Disaster Recovery to Cloud](#)
- [Upgrading vSphere Replication from Earlier Product Versions](#)
- [Configure the NTP Synchronization in Your Environment](#)
- [How vSphere Replication Connects to Cloud](#)
- [Configuring the Connection to the Cloud](#)

Installing vSphere Replication for Disaster Recovery to Cloud

vSphere Replication is distributed as an OVF virtual appliance.

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

Depending on the version of the vCenter Server on which you install vSphere Replication, the deployment procedure might vary.

Table 3-1. vSphere Replication Deployment Procedures

vCenter Server Version	vSphere Replication Deployment Procedure
vCenter Server 5.5.x	See Deploy the vSphere Replication Virtual Appliance in the <i>vSphere Replication 5.5 Administration</i> documentation.
vCenter Server 6.0	See Deploy the vSphere Replication Virtual Appliance .
vCenter Server 6.5	See Deploy the vSphere Replication Virtual Appliance .
vCenter Server 6.7	See Deploy the vSphere Replication Virtual Appliance .

Important In these procedures, the steps for installing vSphere Replication on the target site apply to vCenter Server replications. If you intend to use vSphere Replication only for replications to cloud, do not attempt to install vSphere Replication on the target site. Your cloud provider ensures that the target site is configured for replications to cloud.

After installing the vSphere Replication appliance, you must configure it to synchronize with an external NTP server. See [Configure the NTP Synchronization in Your Environment](#).

Upgrading vSphere Replication from Earlier Product Versions

You can upgrade vSphere Replication 5.5.x, 5.8, and 6.x to vSphere Replication 8.x.

To upgrade a previously installed version of vSphere Replication to vSphere Replication for Disaster Recovery to Cloud, you must mount the vSphere Replication ISO file on a system in your environment. The system must be accessible from the vSphere Replication appliance, and apply the update through the virtual appliance administration interface (VAMI) on port 5480. See [Upgrading vSphere Replication](#).

After upgrading the vSphere Replication appliance, you must configure it to synchronize with an external NTP server. See [Configure the NTP Synchronization in Your Environment](#).

Configure the NTP Synchronization in Your Environment

If you are upgrading the vSphere Replication appliance and the NTP has not been configured yet, you must synchronize the time on the vSphere Replication appliance in your environment with an NTP server.

By default, the vSphere Replication appliance is synchronized with the ESXi host on which it resides. You must disable the NTP synchronization with the host and configure the vSphere Replication appliance and the vCenter Server to synchronize with an external NTP server.

Procedure

- 1 Configure the NTP synchronization on the vSphere Replication appliance.
 - a In the vSphere inventory tree, locate the vSphere Replication appliance, right-click, and select **Edit Settings**.
 - b On the **VM Options** tab, click **VMware Tools**.
 - c Deselect the **Synchronize guest time with host** check box.
 - d In the virtual appliance console, run the command `systemctl enable ntpd` to run NTP synchronization every time the vSphere Replication appliance starts.
 - e To configure the vSphere Replication appliance to synchronize with an NTP server, edit the `/etc/ntp.conf` file to enter the address of an NTP server.

Add the following line in the `ntp.conf` file:

```
server <your_ntp_server_address> iburst
```

- f Run the `systemctl reload-or-restart ntpd` command.
- 2 Configure the vCenter Server on the source site to synchronize with the NTP server that you configured in the vSphere Replication appliance.

How vSphere Replication Connects to Cloud

When you create a connection to the cloud, the vCloud Tunneling Agent in the vSphere Replication appliance creates a tunnel to secure the transfer of replication data to your cloud Organization.

When a tunnel is created, the vCloud Tunneling Agent opens a port on the vSphere Replication appliance. ESXi hosts connect to that port to send replication data to a cloud organization. The port is picked randomly from a configurable range. The default port range is 10000-10010 TCP.

By default, ports 10000-10010 are not open on ESXi hosts. When you power on the vSphere Replication appliance, a vSphere Installation Bundle (VIB) is installed on all supported ESXi hosts in the vCenter Server inventory where the appliance is deployed. The VIB creates a firewall rule, Replication-to-Cloud Traffic, that opens TCP ports 10000 to 10010 for outgoing traffic. The rule is enabled automatically and takes effect immediately when you power on the vSphere Replication appliance, or when a host is registered or connected in the vCenter Server. If an administrator removes the VIB from a host, for example by using the `esxccli` utility, the vSphere Replication appliance reinstalls the VIB the next time you restart the appliance or when a host is restarted or reconnected to the inventory. If you do not want ports 10000 to 10010 to be open on an ESXi host, and if you do not plan to use this host as a replication source, you can disable the Replication-to-Cloud Traffic rule. See [Allow or Deny Access to an ESXi Service or Management Agent with the vSphere Web Client](#).

To reduce the number of open ports or to change the ports that are used for communication between ESXi hosts and the vCloud Tunneling Agent, you can create a custom firewall rule and reconfigure the agent.

Change the Cloud Tunnel Ports on ESXi Hosts

When you power on the vSphere Replication appliance, it automatically configures all ESXi hosts in your environment to open TCP ports 10000–10010 for outgoing data transfers.

The vCloud Tunneling Agent in the vSphere Replication appliance uses ports 10000–10010 to receive data from ESXi instances that host replication sources.

If you do not want to have unused open ports on your ESXi hosts, if the number of open ports is insufficient, or if you want to change which ports are open, you can reconfigure your firewall settings.

You can change the default ports that are used to transfer replication data from ESXi hosts to the vCloud Tunneling Agent. To change the default ports, you must configure each ESXi instance that hosts a replication source virtual machine, and the vCloud Tunneling Agent.

Procedure

- 1 Disable the default **Replication-to-cloud Traffic** rule that the vSphere Replication appliance creates.
For a detailed procedure, see [Manage ESXi Firewall Settings](#).
- 2 Create a custom firewall rule on each ESXi server that hosts replication source machines.
See [Creating custom firewall rules in VMware ESXi 5.0 \(KB 2008226\)](#).

- 3 Enable the custom firewall rule that you created on each ESXi host.

See [Manage ESXi Firewall Settings](#).

What to do next

Configure the vCloud Tunneling Agent to use the ports that you configured on ESXi hosts.

Customize the Ports That vSphere Replication Uses for Tunneling

By default, the vCloud Tunneling Agent in the vSphere Replication appliance is configured to use TCP ports ranging between 10000 and 10010 to create tunnels to the cloud. All ESXi instances that might host replication source virtual machines must have their firewall configured to allow outgoing traffic on these ports.

For each tunnel to cloud, the vCloud Tunneling Agent allocates one unique port from the specified range. You can reconfigure ESXi hosts and the vCloud Tunneling Agent to reduce the number of open ports or to change the ports that are used to create tunnels to cloud.

After you reconfigure the ESXi hosts to use custom ports, you must configure the vCloud Tunneling Agent to use the same custom ports.

Prerequisites

- Verify that the ports you selected to use for cloud tunnels are open for outgoing traffic on all ESXi servers that host replication sources.
- Verify that you know the IP address of the vSphere Replication appliance in your environment. To check the IP address of the vSphere Replication appliance, open the Site Recovery user interface, select **Menu > Replications within the same vCenter Server**, and select the vCenter Server. On the **Site** tab, click **Summary**.
- Verify that you have root user credentials for the vSphere Replication appliance. The IP address of the vSphere Replication appliance is listed on the Server row.
- Verify that TCP port 22 is open on the vSphere Replication appliance, and that SSH connections are enabled. See [Unable to Establish an SSH Connection to the vSphere Replication Appliance](#).

Procedure

- 1 Use an SSH client to connect to the vSphere Replication appliance and log in as the root user.
- 2 Run the following command to configure the ports for tunnel connections.

```
/opt/vmware/vcta/bin/cell-management-tool
  configure-vcta-server -prl LOW -prh HIGH
```

Where *LOW* and *HIGH* define the range of ports to be used for tunnel connections. To use only one port, type the port number as the value for *LOW* and *HIGH*.

For example, the following command configures the vCloud Tunneling Agent to use only port 10001.

```
/opt/vmware/vcta/bin/cell-management-tool
  configure-vcta-server -prl 10001 -prh 10001
```

Note You can designate any free TCP port in your environment for the communication between ESXi hosts and the vCloud Tunneling Agent, but you must verify that all ESXi hosts and the vCloud Tunneling Agent are configured to use the same ports.

- 3 Run the following command to restart the vCloud Tunneling Agent.

```
service vmware-vcd restart
```

Configuring the Connection to the Cloud

In addition to installing and configuring the vSphere Replication appliance, you must configure the connection to your cloud provider.

You can configure a connection to the cloud provider before you start the **Configure Replication** wizard or while you configure a replication task.

Connect to a Cloud Provider Site

Before you configure replication tasks to the cloud, you configure the connections between your vSphere environment and virtual data centers that belong to your cloud organizations.

You can connect a vCenter Server to multiple virtual data centers, and a virtual data center can be connected to multiple vCenter Server instances.

Prerequisites

Verify that you have user credentials for a cloud organization in which vCloud Director is enabled. Your cloud provider enables the Disaster Recovery to Cloud service per your contract.

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 Click the **New Site Pair** button.
The **New Site Pair** wizard starts.
- 4 Select the first site from the list.
- 5 Select the **Cloud provider** radio button.

- 6 To authenticate with the cloud, enter the address of your cloud provider, the organization name, and credentials .

By default, vSphere Replication uses these credentials to establish a user session to the cloud and for system monitoring purposes. To enable system monitoring, these credentials are stored in the vSphere Replication appliance, unless you select to use another user account for system monitoring.

- 7 (Optional) If you do not want to store the credentials that you used for authentication, select the **Use a different account for system monitoring** check box, and enter the credentials to be used for system monitoring.

These credentials are encrypted and stored in the vSphere Replication database.

- 8 Click **Next**.

The **New Site Pair** wizard displays a list of virtual data centers to which you can connect. If a virtual data center is already connected to the vCenter Server, that data center does not appear in the list.

- 9 From the list of virtual data centers, select a target for the connection and click **Next**.

- 10 Review your settings and click **Finish**.

The connection to the cloud organization appears on the Site Recovery home page.

What to do next

Select the networks on the target site that vSphere Replication must use for recovery operations. See [Select Recovery Networks on the Target Virtual Data Center](#).

Reconfiguring a Site Pair and Breaking a Site Pair

You can reconfigure or break an existing site pair.

If you have problems with an existing site pair, you can attempt to reconfigure the site pair with the **Reconfigure Site Pair** action. When you provide the required credentials, the reconfiguration operation attempts to repair the existing site pair.

With the **Break Site Pair** action, you can break the pairing between a vSphere Replication instance on the protected site and the virtual data center on the vCloud Director account of your organization.

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

Select Recovery Networks on the Target Virtual Data Center

To finalize the configuration of a connection to the target site, you must specify the networks that the Disaster Recovery to Cloud service can use for tests and recovery operations.

When you subscribe to the Disaster Recovery to Cloud service, VMware automatically creates two default networks for your service - an isolated network and an external routed network. The Edge Gateway for the routed network has a public IP address on an external interface so that it is accessible through the Internet. You can use these networks for your virtual machines protected by the Disaster Recovery to Cloud service, or create other networks in your cloud organization.

When you run a test recovery, vSphere Replication configures the replicated virtual machine on the target site to connect to the test network. With the test recovery, you can access the target virtual machine and verify that it operates as expected and that data is replicated correctly per your replication settings.

The recovery network is used when you perform planned migrations and recovery operations. vSphere Replication configures the replicated virtual machine on the target site and connects it to the recovery network, so that you can have access.

Note Replicated virtual machines on the target virtual data center are attached to the network selected for recovery operations right after the replication is configured. Replica VM network settings are not changed during planned migration. This means that the recovered virtual machines in a target virtual data center are configured with the network that is initially selected when the replication is configured and not the one that is configured in the mappings.

A good practice is to run test recoveries in a separate network, although you can use the same network for all recovery workflows.

Note You can configure only one pair of networks for a cloud virtual data center.

Prerequisites

Verify that you created a connection to a cloud virtual data center. See [Connect to a Cloud Provider Site](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 Click **View Details** for the connection to a cloud virtual data center that you want to configure.
- 4 On the **Site Pair** tab, click **Network Mappings**.
- 5 Select a local vCenter Server in the locality selector.
- 6 Click **Edit** to select a recovery network and save your selection.

The list displays only the networks that are configured for a vCloud Director based cloud.

- 7 Click **Edit** to select a test network and save your selection.

The list displays only the networks that are configured for a vCloud Director based cloud.

What to do next

When you test a replication or perform a recovery operation, the vCloud Director based cloud automatically attaches the virtual machine to the test or recovery network respectively.

Select Recovery Networks from Cloud to the Local Site

When recovering virtual machines from cloud to your on-premise data center, you can have them attached to the on-premise network if you configure network mappings from cloud.

The configuration of network mappings from cloud assures that during a recovery from cloud, the virtual machine on the on-premise data center connects to the correct vCenter Server network. The network depends on the network mapping and whether you run a test recovery or a recovery operation.

Prerequisites

Verify that you created a connection to a cloud virtual data center. See [Connect to a Cloud Provider Site](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 Click **View Details** for the connection to a cloud virtual data center that you want to configure.
- 4 On the **Site Pair** tab, click **Network Mappings**.
- 5 Select the cloud virtual data center in the locality selector.
- 6 Click the **New** icon.

The **Configure Target Networks** wizard starts.

- 7 On the **Recovery networks** page, select the cloud networks from the left pane and the local recovery networks from the right pane. Click **Add mappings** and click **Next**.

Note You can select a virtual data center (VDC) network or a vApp network. When you select a vApp network, the network mappings are configured only for the selected vApp and override virtual data center network mappings. When you select a VDC network, the network mappings are configured for all VMs in that network.

- 8 On the **Test networks** page, select the cloud networks from the left pane and select the local test networks from the right pane. Click **Add mappings** and click **Next**.
- 9 Review your settings and click **Finish**.

When you test a replication or perform a recovery operation, the vCloud Director-based cloud automatically attaches the virtual machine to the test or recovery network respectively.

Disable the Automatic Export of MAC Addresses During Replication

By default, when you configure a virtual machine for replication to cloud, its NICs and MAC addresses are copied automatically to the target site as part of the provisioning of the placeholder virtual machine.

If the test network is not isolated from the production network and these networks have common routing, a test recovery of a replicated virtual machine might result in duplicate MAC addresses in your virtual data center.

To avoid duplicate MAC addresses in your data center, you can disable the automatic copying of network configurations from the source site to cloud sites.

Note Disabling the automatic copying of network configurations does not delete the configurations that are already replicated to the target site. See <http://kb.vmware.com/kb/2086292> .

Procedure

- 1 Use the vSphere Web Client on the source site to locate the HMS virtual machine and log in as the root user.
- 2 Navigate to folder `/opt/vmware/hms/conf/`.
- 3 Run the `vi hms-configuration.xml` command to open the `hms-configuration.xml` file for editing.
- 4 Locate the `<hms-dr2c-export-mac-address>` parameter, and modify the value to `false`:
`<hms-dr2c-export-mac-address>false</hms-dr2c-export-mac-address>`
- 5 Run the `:wq` command to save the change, and run the following command to restart the HMS service.

```
# service hms restart
```

The automatic copying of network configurations to target cloud sites is disabled for all newly configured replications.

Cloud Connection States

You can view the status of connections between your vSphere environment and the virtual data centers on the remote site by viewing the details of the connection to the cloud provider site.

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

Table 3-2. Cloud Connection States

Icon	Status	Description	Remediation
	Connected	The connection between the local vSphere Replication management servers and the cloud is working properly.	Not needed.
	Not Connected	<ul style="list-style-type: none"> ■ The SSL certificate on the local vSphere Replication Management Server or the cloud endpoint certificate has been changed. ■ The network connection between the local vSphere Replication Management Server and the cloud provider site is not functioning properly. ■ The user that is used for authentication with the Lookup Service or the VRMS extension user in the vCenter Single Sign-On might be disabled or deleted. <p>In this state, configured replications might not be running.</p>	<ul style="list-style-type: none"> ■ To reconfigure the site connection, click Reconfigure Site Pair. ■ Verify the network connectivity to the cloud provider site. ■ In the vSphere Client or vSphere Web Client, navigate to the vCenter Server, select the Monitor tab, and select Events under Tasks and Events to search for events related to vSphere Replication.

Reconnect to a Cloud Provider Site

To protect your environment with Disaster Recovery to Cloud, you must provide authentication details for the cloud provider site.

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, click **Actions > Reconnect Site**.
- 4 Enter the credentials for the cloud provider site and click **Reconnect**.

Replicating Virtual Machines to Cloud

4

You can configure replications from vSphere environments to cloud for a single virtual machine or for multiple virtual machines.

To replicate virtual machines to cloud, you must deploy the vSphere Replication 8.2 appliance at the source site, and your cloud provider must enable replications to the cloud in your cloud organization.

The source and target sites must be connected so that you can configure replications. See [Connect to a Cloud Provider Site](#).

To avoid copying large volumes of data between the source site and the cloud over a network connection, you can create replication seeds on the target site and configure replication tasks to use them. See [Using Replication Seeds for Replications to Cloud](#).

For each replication task, 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 replication source virtual machines to their replicas on the target site. This process reoccurs at the RPO interval that you set.

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:

- [Configure a Replication to Cloud](#)
- [Using Replication Seeds for Replications to Cloud](#)

Configure a Replication to Cloud

You can protect one or more virtual machines and their virtual disks by replicating them to your cloud organization.

When you configure a replication, you set a recovery point objective (RPO) to determine the maximum data loss that you can tolerate. For example, an RPO of 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 the topic *How the Recovery Point Objective Affects Replication Scheduling* in the *vSphere Replication Administration* documentation.

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 crash consistency amongst the disks that belong to a virtual machine. The available quiescing types are determined by the virtual machine's operating system. See [Compatibility Matrices for vSphere Replication 8.2](#) for quiescing support for Windows and Linux virtual machines.

If you plan to use replication seeds, read and understand the information in topic [Using Replication Seeds for Replications to Cloud](#).

Note By default, when you configure a virtual machine for replication to cloud, its NICs and MAC addresses are copied automatically to the target site as part of the provisioning of the placeholder virtual machine. If the test network is not isolated from the production network and these networks have common routing, a test recovery of a replicated virtual machine might result in duplicate MAC addresses in your virtual data center. See [Disable the Automatic Export of MAC Addresses During Replication](#).

Prerequisites

- Verify that the vSphere Replication appliance is deployed in your environment.
- Verify that the Disaster Recovery to Cloud service is enabled in the target cloud organization.
- Configure a connection to the cloud organization to which you want to replicate data. See [Connect to a Cloud Provider Site](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab, select **Forward replications**, and click the **Create new replication** icon. The **Configure Replication** wizard starts.

- 5 On the **Virtual machines** page, select the virtual machines you want to replicate and click **Next**.
- 6 Select a cloud provider site as a target site and click **Next**.
- 7 On the **Target location** page, select the location for the target vApp and click **Next**.

You can use a storage policy or a previously imported vApp on the target site as a replication seed.

- 8 On the **Replication settings** page, use the RPO slider 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.

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

Note You can keep up to 24 instances for a virtual machine. For example, if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is 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 verify 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 must not exceed 4 hours, so that vSphere Replication can create 6 instances in 24 hours.

- 10 (Optional) Enable quiescing for the guest operating system of the source virtual machine.

Note Quiescing options are available only for virtual machines that support quiescing. vSphere Replication does not support VSS quiescing on 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 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 the configuration operation completes successfully, the replication task that you created appears in the list of forward replications.

Note If a replication source virtual machine is powered off, the replication starts after you power on the virtual machine.

What to do next

On the **Replications** tab, under **Forward replications** and **Reverse replications**, you can view the status of each replication. For more information on the replication status, see [Monitoring the Status of Replications](#).

Using Replication Seeds for Replications to Cloud

For each new replication that you configure, an initial full synchronization operation is performed. During this operation, vSphere Replication copies the whole data from the source virtual machine to a placeholder vApp on the target site.

If the source virtual machine is too big, or the bandwidth of your network connection to the cloud is too low, the initial full sync might take a long time. Therefore, you might choose to copy the source virtual machine to the target site by using removable media, or other means of data transfer. Then you can configure a replication and use the virtual machine copy on the target site as a replication seed. When a replication is configured to use a seed vApp, vSphere Replication does not copy the whole source virtual machine to the target site. Instead, it copies to the seed vApp only the different blocks between the source virtual machine and the seed.

Note vSphere Replication stores the replication data in the seed vApp. No copies of the seed vApp are created. Therefore, a seed vApp can be used for only one replication.

Creating Seed vApps in the Cloud

Seed vApps on the target site can be created in the following ways.

- **Offline data transfer:** You can export a virtual machine as an OVF package and let a Cloud service administrator import the package in your cloud organization.
- **Clone a virtual machine:** A virtual machine in the org virtual data center can be cloned to create a seed vApp. vSphere Replication calculates checksum and exchanges the different blocks from the replication source to the seed vApp.
- **Copy over the network:** A source virtual machine can be copied to the cloud organization by using means other than vSphere Replication to copy the initial source data to the target site.

Note The size and number of disks, and their assignment to disk controllers and bus nodes must match between the replication source and the seed virtual machine. For example, if the replication source machine has two disks of 2 GB each, one of them assigned to SCSI controller 0 at bus number 0, and the second one assigned to SCSI controller 1 at bus number 2, the seed vApp that you use must have exactly the same hardware configuration - 2 disks of 2 GB each, at SCSI 0:0 and at SCSI 1:2.

Reconfiguring Replications to the Cloud

5

You can reconfigure cloud replications to change the quiescing method for the guest operating system, the RPO, the network compression, and the retention of point in time instances.

Reconfigure a Replication to Cloud

You reconfigure a replication to change the RPO settings, the number of replication instances to keep, or the quiescing method that is applied when synchronizing the replication source virtual machine to your cloud organization.

Cloud replications appear in the **Forward Replications** list on the **Replications** tab in Site Recovery.

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab and click **Forward replications**.
- 5 Select the replication you want to reconfigure from the list and click the **Reconfigure** icon.
- 6 On the **Replication settings** page of the **Reconfigure Replication** wizard, use the RPO slider to set the acceptable period for which data can be lost if of a site failure occurs.
- 7 (Optional) To save multiple replication instances that can be converted to snapshots of the source virtual machine during recovery, select **Enable point in time instances** and adjust the number of instances to keep.

Note You can keep up to 24 instances for a virtual machine. For example, if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is 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 verify 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 must not exceed 4 hours, so that vSphere Replication can create 6 instances in 24 hours.

- 8 (Optional) Enable quiescing for the guest operating system of the source virtual machine.

Note Quiescing options are available only for virtual machines that support quiescing. vSphere Replication does not support VSS quiescing on Virtual Volumes.

- 9 (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.

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

Recovering Virtual Machines to Cloud

6

You can check if virtual machines are properly replicated in the cloud, and migrate replicated virtual machines to your cloud organization.

This chapter includes the following topics:

- [Test Recovering Virtual Machines to Cloud](#)
- [Planned Migration to Cloud](#)

Test Recovering Virtual Machines to Cloud

You can use test recoveries to verify that source data is replicated correctly on the cloud site.

When you initiate a replication task to cloud, Disaster Recovery to Cloud creates a placeholder virtual machine on the target virtual data center. If the replication uses a seed, that seed is the placeholder virtual machine. The placeholder virtual machine is not visible on the network and is not accessible until you recover it or run a test recovery.

Note During test recovery, Disaster Recovery to Cloud does not create a copy of the recovered virtual machine. When you run a test recovery, the placeholder virtual machine is reconfigured and connected to the selected test network so that you can log in and verify the replication progress.

Run a Test Recovery to Cloud

You run a test recovery to verify that data is replicated correctly from the source virtual machine to the target cloud organization.

Note If the test network is not isolated from the production network and these networks have common routing, a test recovery of a replicated virtual machine might result in duplicate MAC addresses in your virtual data center. If you use the same network for test recoveries and for production, and if you have not disabled the automatic copying of network configurations, see <http://kb.vmware.com/kb/2086292>.

Prerequisites

- Configure at least one replication task.
- Verify that the status of the replication task allows running test recoveries.

Test recoveries are allowed for the following replication statuses: OK, OK (RPO Violation), Error, Error (RPO Violation), Full Sync, Full Sync (RPO Violation), Not Active, Not Active (RPO Violation), Paused, Sync, and Sync (RPO Violation).

- If you have run test recoveries for the replication that you want to test, verify that you have cleared the test results.

Note You cannot run a test recovery before you clean up your previous test results for a replication.

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab and click **Forward replications**.
- 5 Select the replication for which you want to run a test recovery and click the **Test recovery** icon.

The **Test Recovery** wizard opens. If the user session to the target cloud organization is expired, the wizard prompts you to enter user credentials.

- 6 On the **Recovery options** page, select a data synchronization option.

Option	Description
Synchronize recent changes	vSphere Replication runs a synchronization task before it configures the placeholder virtual machine on the cloud site.
Points in time recovery	vSphere Replication configures the placeholder virtual machine and uses the data that is copied on the cloud site at the point in time that you select from the list .

- 7 (Optional) To power on the test virtual machine on the target site after test configuration completes, select the **Power on the virtual machine after recovery** check box.
- 8 Click **Next**.
- 9 Verify that the test configuration settings are correct and click **Finish**.

The test status of the replication changes.

Note You cannot stop a replication while a test recovery for the replication is in progress.

What to do next

After you verify that data appears as expected in the test virtual machine, clean up the test results. See, [Clean up a Test Recovery](#).

Clean up a Test Recovery

You can run a test recovery or a planned migration for a replication only after the results of its previous test recovery are cleaned up.

You can clean up test recovery results for replication tasks that appear in the list of replications on the **Replications** tab.

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab and click **Forward replications**.
- 5 Select the replication with test recovery results that you want to clean up and click the **Cleanup** icon.

Planned Migration to Cloud

Planned migration is an action that is available for replications to cloud. Planned migrations allow you to move your workloads from vCenter Server to your cloud organization.

When you run a planned migration operation, the replication source virtual machine is powered off. The placeholder virtual machine that is created in the cloud during replication is configured to run as a fully functional virtual machine. When the recovered virtual machine is powered on in the target cloud site, the replication task on the source is no longer active.

Migrate a Virtual Machine to Cloud

You can run a planned migration to move your workload from the vCenter Server to your cloud organization.

If you plan maintenance on the source site, you might want to migrate replicated virtual machines to cloud .

Prerequisites

- Verify that the local site and the cloud site are online.
- Verify that you have the privileges to initiate migrations to cloud.
- If you have run test recoveries for the replication that you want to migrate, verify that you cleaned up the test results. For more information, see [Clean up a Test Recovery](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab and click **Forward replications**.

- 5 Select the replication that you want to migrate and click the **Planned Migration** icon.

The **Planned Migration** wizard opens. If the user session to the target cloud organization is expired, the wizard prompts you to enter user credentials.

- 6 On the **Recovery options** page, select a data synchronization option.

Option	Description
Synchronize recent changes	vSphere Replication runs a synchronization task before it configures the placeholder virtual machine on the cloud site.
Points in time recovery	vSphere Replication configures the placeholder virtual machine and uses the data that is copied on the cloud site at the point in time that you select from the list .

- 7 (Optional) To power on the test virtual machine on the target site after test configuration completes, select the **Power on the virtual machine after recovery** check box.

- 8 Click **Next**.

- 9 On the **Source VM shutdown** page, select how to stop the source virtual machine and click **Next**.

Option	Description
Guest shutdown	Shuts down the operating system of the virtual machine within the timeout period that you set in the time spinners. This option uses VMware Tools. Select the Guest shutdown option only if VMware Tools is installed in the guest operating system.
Power off	Immediately shuts down the guest operating system or powers off the virtual machine. The guest operating system might not shut down properly. Select the Power off option only if VMware Tools is not installed on the guest operating system.

- 10 Review your settings and click **Finish**.

The replication status changes to Recovered and the source virtual machine is no longer being replicated to the cloud site.

What to do next

To continue replicating the source virtual machine to the target site, stop the replication task that is in Recovered state and configure a new replication.

Configuring Replications from Cloud



If a virtual machine was recovered in the cloud, you can replicate the virtual machine from your cloud environment to a vCenter Server.

You select whether to configure a new replication from cloud or a reverse replication from cloud depending on the condition of your local environment.

Configuring Replications from Cloud

When the local site does not contain data about a forward or reverse cloud replication for the virtual machine that you want to replicate, you can configure a replication from cloud for that machine.

Note If the local site contains outgoing replication data for a virtual machine that was recovered in the cloud virtual data center, you must stop that replication before attempting to configure a replication for the recovered virtual machine from cloud or use the **Reverse** replication action.

In addition to replicating virtual machines from your local site to the virtual data center in the cloud, you can also use replications from the cloud to restore your site by using the data that was previously replicated in the cloud. For example, a partial or complete breakdown has occurred at your local site, and the source virtual machines that were used for replications to cloud are missing. Additionally, the data for forward cloud replications is missing, too. In your cloud organization, you have recovered some of the replicated virtual machines. To restore them back on your local site, you can configure replications from cloud for the recovered virtual machines.

Reversing Replications to Cloud

On the local site, for a forward cloud replication that is in the recovered status, you can reverse that replication to start transferring data from the recovered virtual machine in the cloud to the local virtual machine that served as the replication source before the recovery operation.

You can configure a reverse replication to update a replicated virtual machine on your local site with the changes that occurred on its restored copy in the cloud. For example, you replicated a virtual machine from the local site to the cloud and recovered the virtual machine to the cloud to use it while your local site is being maintained. While the local site was offline, changes occurred in the recovered virtual machine in the cloud. When your local site is back online, you can copy the changes from the cloud to your local environment, or even migrate the virtual machine from the cloud back to the local environment.

When you reverse a replication, you can only use the original replication settings. You cannot change the datastore location, RPO, PIT policy, and so on.

This chapter includes the following topics:

- [Configure a Replication from Cloud](#)
- [Reverse a Replication to Cloud](#)
- [Configure Failback Recovery Settings for Replications from the Cloud](#)

Configure a Replication from Cloud

You can use vSphere Replication to configure a replication from cloud to your local site.

If your local site was recovered from a major breakdown and you must restore it, or you cannot configure a reverse replication, you can configure a new replication from cloud to synchronize data from the cloud site to your local site.

Note You can configure a replication from cloud for only one virtual machine in a vApp.

Prerequisites

- Verify that the cloud site is available and connected to the local site. See [Connect to a Cloud Provider Site](#).
- Verify that the list of incoming replications does not contain a replication for the virtual machine that you want to configure for a replication from cloud. See [Stop a Replication from Cloud](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 On the **Replications** tab, click **Reverse replications**, and click the **Create new replication** icon.
The **Configure Replication** wizard starts.
- 5 Select the cloud provider site where the virtual machine is located and the virtual machines that you want to protect, and click **Next**.
- 6 Accept the automatic assignment of a vSphere Replication server or select a particular server on the local site and click **Next**.

- 7 On the **Target datastore** page, select a datastore on which to replicate files.

When replicating multiple virtual machines, you can configure a different target datastore for each virtual machine.

- 8 (Optional) Select the **Select seeds** check box.

Replication seeds can reduce the network traffic during the initial full synchronization, but unintended use of replication seeds might lead to data loss.

- 9 Click **Next**.

- 10 (Optional) On the **Select seed** page, review the suggested replication seeds and change them if necessary.

- 11 Select the **The selected seeds are correct** check box and click **Next**.

- 12 On the **Replication settings** page, use the RPO slider 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 point in time instances** and adjust the number of instances to keep.

Note You can keep up to 24 instances for a virtual machine. For example, if you configure vSphere Replication to keep 6 replication instances per day, the maximum number of days you can set is 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 verify 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 must not exceed 4 hours, so that vSphere Replication can create 6 instances in 24 hours.

- 14 (Optional) Enable quiescing for the guest operating system of the source virtual machine.

Note Quiescing options are available only for virtual machines that support quiescing. vSphere Replication does not support VSS quiescing on Virtual Volumes.

- 15 (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.

- 16 Click **Next**.

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

A virtual machine configuration task appears in the Recent Tasks list. A progress bar indicates that the source virtual machine is being configured for replication.

If the configuration operation completes successfully, the replication task appears in the list of reverse replications on the **Replications** tab.

Note If a replication source virtual machine is powered off, the replication starts after you power on the virtual machine.

What to do next

On the **Replications** tab, under **Forward replications** and **Reverse replications**, you can view the status of each replication. For more information on the replication status, see [Monitoring the Status of Replications](#).

Note You can pause, resume, sync, test, recover, and stop replications from cloud, but you cannot reconfigure or move these replications between vSphere Replication servers.

Reverse a Replication to Cloud

You can use vSphere Replication to reverse a recovered forward replication and start copying data from the cloud to your local site.

You can replicate a virtual machine from the local site to the cloud and recover the virtual machine at the cloud site to use it while your local site is being maintained. When your local site is back online, you can synchronize the changes from the cloud to your local environment, or migrate the virtual machine from the cloud back to the local environment.

When you reverse a replication, you can only use the original replication settings. You cannot change the datastore location, RPO, PIT policy, and so on.

Note When you reverse a replication, the source virtual machine on the local site is unregistered from the inventory and its disks are overridden by the disks that are replicated from the cloud. When the source virtual machine is unregistered, you can no longer use it unless you recover the replication.

Prerequisites

- Verify that the cloud site is available and connected to the local site. See [Connect to a Cloud Provider Site](#).
- In the list of forward replications, verify that the status of the replication that you want to reverse is Recovered. See [Migrate a Virtual Machine to Cloud](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.

- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab and click **Forward replications**.
- 5 Select the replication that you want to reverse and click **Reverse**.

Note The replication status must be Recovered.

vSphere Replication validates the source and target virtual machine, and the Reverse Replication dialog box opens.

- 6 Review the settings for the reverse replication and click **OK**.

Caution The source virtual machine on the local site is unregistered from the inventory and becomes inaccessible until you recover the replication.

vSphere Replication starts synchronizing data from the cloud to your local environment.

The reversed replication is removed from the list of forward replications and appears in the list of reverse replications.

What to do next

You can recover the replication to migrate your virtual machine from cloud to your local environment.

Note You can pause, resume, sync, test, recover, and stop replications from cloud, but you cannot reconfigure or move these replications between vSphere Replication servers.

If the reverse replication cannot be configured, try configuring a new replication from cloud. See [Configure a Replication from Cloud](#).

Configure Failback Recovery Settings for Replications from the Cloud

You can configure failback recovery settings for each replication from the cloud.

Procedure

- ◆ This feature is currently not available.

Recovering Virtual Machines from Cloud



You can check if virtual machines are properly replicated in the local site, and migrate replicated virtual machines to your local environment.

This chapter includes the following topics:

- [Test Recovering Virtual Machines from Cloud](#)
- [Recover a Virtual Machine from Cloud](#)

Test Recovering Virtual Machines from Cloud

You can use test recoveries to verify that source data is replicated correctly on the local site.

- vSphere Replication prepares for the recovery operation.
 - If you perform a synchronization of the latest changes, vSphere Replication checks that the cloud site is available before recovering the virtual machine on the target site. Then vSphere Replication synchronizes the changes from the cloud to the local site.
 - If you skip the synchronization and recover with the latest data available, for example, if the cloud site is not available, vSphere Replication uses the latest available data at the local 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 local site.
- vSphere Replication connects the virtual machine to the local vCenter Server network if the test recovery network mapping is configured.

Run a Test Recovery from Cloud

You run a test recovery to verify that data is replicated correctly from the cloud provider site to the local site.

Note If the test network is not isolated from the production network and these networks have common routing, a test recovery of a replicated virtual machine might result in duplicate MAC addresses in your virtual data center. If you use the same network for test recoveries and for production, and if you have not disabled the automatic copying of network configurations, see <http://kb.vmware.com/kb/2086292>.

Prerequisites

- Configure at least one replication task from the cloud provider site to your local site.
- Verify that the status of the replication task allows running test recoveries.

Test recoveries are allowed for the following replication statuses: OK, OK (RPO Violation), Error, Error (RPO Violation), Full Sync, Full Sync (RPO Violation), Not Active, Not Active (RPO Violation), Paused, Sync, and Sync (RPO Violation).

- If you have run test recoveries for the replication that you want to test, verify that you have cleared the test results.

Note You cannot run a test recovery before you clean up your previous test results for a replication.

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab and click **Reverse replications**.
- 5 Select the replication for which you want to run a test recovery and click the **Test recovery** icon.
The **Test Recovery** wizard opens.
- 6 On the **Recovery options** page, select a data synchronization option.

Option	Description
Synchronize recent changes	vSphere Replication runs a synchronization task before it configures the placeholder virtual machine on the local site. This option requires you to log in to the cloud provider site. A dialog box appears for the login.
Use latest available data	vSphere Replication configures the placeholder virtual machine and uses the data that is copied on the local site. If MPIT is enabled, retained instances are converted to virtual machine snapshots.

- 7 (Optional) To power on the test virtual machine on the target site after test configuration completes, select the **Power on the virtual machine after recovery** check box.
- 8 Click **Next**.
- 9 Select a folder for the virtual machine on the local site.
- 10 Select a resource for the virtual machine on the local site.
- 11 Verify that the test configuration settings are correct and click **Finish**.

The test status of the replication changes.

Note You cannot stop a replication while a test recovery for the replication is in progress.

What to do next

After you verify that data appears as expected in the test virtual machine, clean up the test results. See, [Clean up a Test Recovery from Cloud](#).

Clean up a Test Recovery from Cloud

You can run a test recovery of a replication only after you clean up the results of its previous test recovery.

You can clean up test recovery results for replication tasks that appear in the list of replications on the **Replications** tab.

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab and click **Reverse replications**.
- 5 Select the replication with test recovery results that you want to clean up and click the **Cleanup** icon.

Recover a Virtual Machine from Cloud

You can recover a virtual machine from the cloud provider site and move your workload from the cloud organization to your local site.

Prerequisites

- Configure at least one replication task from the cloud provider site to your local site.
- Verify that the status of the replication task allows running recoveries.

Recoveries are allowed for the following replication statuses: OK, OK (RPO Violation), Error, Error (RPO Violation), Full Sync, Full Sync (RPO Violation), Not Active, Not Active (RPO Violation), Paused, Sync, and Sync (RPO Violation).
- If you have run test recoveries for the replication that you want to recover, verify that you have cleared up any previous test results. For more information, see [Clean up a Test Recovery from Cloud](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab and click **Reverse replications**.

- 5 Select the replication that you want to recover and click the **Recover** icon.

The **Recover virtual machine** wizard opens.

- 6 On the **Recovery options** page, select a data synchronization option.

Option	Description
Synchronize recent changes	vSphere Replication runs a synchronization task before it configures the placeholder virtual machine on the local site. This option requires you to log in to the cloud provider site. A dialog box appears for the login.
Use latest available data	vSphere Replication configures the placeholder virtual machine and uses the data that is copied on the local site. If MPIT is enabled, retained instances are converted to virtual machine snapshots.

- 7 To power on the virtual machine on the target site after test configuration completes, select the **Power on the virtual machine after recovery** check box.

- 8 Click **Next**.

- 9 (Optional) If you selected the **Synchronize recent changes** option, on the **Source VM shutdown** page, select how to stop the source virtual machine and click **Next**.

Option	Description
Guest shutdown	Shuts down the operating system of the virtual machine within the timeout period that you set in the time spinners. This option uses VMware Tools. Select the Guest shutdown option only if VMware Tools is installed in the guest OS.
Power off	Immediately shuts down the guest operating system or powers off the virtual machine. The guest OS might not shut down properly. Select the Power off option only if VMware Tools is not installed on the guest OS.

- 10 Select a folder for the virtual machine on the local site.
- 11 Select a resource for the virtual machine on the local site.
- 12 Review your settings and click **Finish**.

The replication status changes to **Recovered** and the source virtual machine is no longer being replicated to the local site. If the recovery network mapping is configured, vSphere Replication connects the virtual machine to the local vCenter Server network.

What to do next

To continue replicating the source virtual machine to the local site, stop the replication task that is in **Recovered** state and configure a new replication.

Monitoring and Managing Replications in vSphere Replication

9

You can monitor the state of replications to the cloud, control their running state, or stop them if you no longer need them from the **Replications** tab of Site Recovery.

This chapter includes the following topics:

- [Monitoring the Status of Replications](#)
- [Pause or Resume a Replication](#)
- [Stop a Replication to Cloud](#)
- [Stop a Replication from Cloud](#)

Monitoring the Status of Replications

You can view the status of replication tasks for a vCenter Server. The lists of forward and reverse replications are under the **Replications** tab of Site Recovery.

Table 9-1. Replication Statuses

Status	Description	Remediation
OK	The replication is running.	Not needed.
Not Active	The replication is not running at the moment. <ul style="list-style-type: none">■ The source virtual machine is powered off.■ A communication problem might have occurred between the source ESXi host and the target site.	<ul style="list-style-type: none">■ Power on the source virtual machine.■ If all replications for an ESXi host are in Not Active state, verify that the security rule Replication-to-Cloud Traffic is enabled on the host. This rule opens TCP ports from 10000 to 10010 for outgoing communication.
Paused	The replication is not running at the moment. A vSphere Replication user has paused the replication.	From the list of replications, select the paused replication and click the Resume icon.

Table 9-1. Replication Statuses (Continued)

Status	Description	Remediation
Error	<p>The replication is not running at the moment.</p> <ul style="list-style-type: none"> ■ A configuration error occurred. ■ A replication error occurred. For example, the target site infrastructure is not accessible. 	<ul style="list-style-type: none"> ■ Reconfigure the replication. ■ Verify whether some problem occurred on the virtual machine by clicking the Site Pair tab and clicking Issues.
Status (RPO violation)	<p>For replication status OK, Sync, or Full Sync, the replication is running, but the RPO that is set for the replication is not met and is violated.</p> <p>For replication status Not Active or Error, the replication is not running, and the RPO that is set for the replication is violated.</p> <ul style="list-style-type: none"> ■ The network connection between the source and the target site is dropping intermittently. ■ The bandwidth of the connection between the source and the target site is too low. ■ The replication is not running, so data cannot be replicated on the target site. 	<ul style="list-style-type: none"> ■ Improve the network connection between the source and target site. ■ Increase the RPO period. ■ For replication status Not Active or Error, address the cause for the status and wait for the next sync.

Pause or Resume a Replication

To control the network traffic between the local site and the cloud site, you can pause and resume replications.

Prerequisites

Verify that you have enough privileges to manage replications. See [Roles and Permissions That Disaster Recovery to Cloud Requires](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab, click **Forward replications** or **Reverse replications**, and select the replication you want to pause or resume.

- 5 Click the **Pause** or **Resume** icon.

You can pause and resume multiple replications simultaneously only if they are replicated to the same virtual data center.

- 6 Confirm the action.

Stop a Replication to Cloud

If you no longer want to replicate a virtual machine to the cloud, you can stop the replication permanently.

When you stop a replication, data is removed from both the local site and the cloud site. Therefore, stopping a replication requires that both sites are online and connected.

If the cloud site is offline, you can force stop the replication task from the local site. When you force stop a replication, you remove the replication task only from the local site. The data on the cloud site remains intact. When the cloud site becomes available, you must delete the replication artifacts from the cloud site manually or contact your cloud provider.

Note For stopped replications that use replication seeds, the seed vApps are not deleted from the cloud site.

Prerequisites

Verify that you have enough privileges to manage replications. See [Roles and Permissions That Disaster Recovery to Cloud Requires](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab, click **Forward replications**, and select the replication you want to stop.
- 5 Click the **Remove** icon.

You can stop multiple replication tasks simultaneously only if they are replicated to the same virtual data center.

- 6 (Optional) To delete the replication only from the local site, select **Force stop replication** in the Stop Replication dialog box.

Note All data that was stored to the cloud during the replication remains on the cloud datastore, and the replication remains visible on the cloud site. You must manually delete the replication artifacts from the cloud site or contact your cloud provider to clear them from the cloud site.

- 7 Click **Remove** to confirm.

If both sites are online, Disaster Recovery to Cloud applies the following changes.

- On the local site, removes the replication entry from the list of forward replications, and removes the replication-related configurations from the source virtual machine.
- On the cloud site, removes the task from the list of reverse replications, and deletes the replication data from the storage.

If you perform a force stop operation, the replication task is deleted from the list of forward replications, and replication-related configurations are removed from the source virtual machine.

Stop a Replication from Cloud

If you no longer want to replicate a virtual machine from the cloud, you can stop the replication permanently.

When you stop a replication, data is removed from both the local and the cloud site. Therefore, stopping a replication requires that both the cloud and the local site are online and connected.

If the cloud site is offline, you can force stop the replication task from the local site. When you force stop a replication, you remove the replication task only from the local site. The data on the cloud site remains intact. When the cloud site becomes available, you must delete the replication artifacts from the cloud site manually or contact your cloud provider.

Note For stopped replications that use replication seeds, the seed VMs are not deleted from the local site.

Prerequisites

Verify that you have enough privileges to manage replications. See [Roles and Permissions That Disaster Recovery to Cloud Requires](#).

Procedure

- 1 Log in to the vSphere Client or vSphere Web Client.
- 2 On the home page, click **Site Recovery** and click **Open Site Recovery**.
- 3 On the Site Recovery home page, select the site pair to the cloud provider site and click **View Details**.
- 4 Click the **Replications** tab, click **Reverse replications**, and select the replication you want to stop.
- 5 Click the **Remove** icon.

You can stop multiple replication tasks simultaneously only if they are replicated to the same virtual data center.

- 6 (Optional) To delete the replication only from the local site, select **Force stop replication** in the Stop Replication dialog box.

Note The replication remains active on the cloud site. Contact your provider to clear the replication from the cloud site.

7 Click **Remove** to confirm.

If both sites are online, Disaster Recovery to Cloud applies the following changes.

- On the cloud site, removes the replication entry, and removes the replication-related configurations from the source virtual machine.
- On the local site, removes the task from the list of reverse replications, and deletes the replication data from the storage.

If only the local site is online and you selected to perform a force stop operation, the replication task is deleted from the list of reverse replications, and replication data is deleted from the storage.