vCloud Air - Dedicated Disaster Recovery User's Guide

vCloud Air Disaster Recovery

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.
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
Contents

About this Guide 5

1 About Dedicated Disaster Recovery 7
   Why Use Dedicated Disaster Recovery 8
   Service Architecture 9
   Setting up this Service 10
   Workflow for Using this Service 11
   System Requirements and Compatibility 12

2 Deploying Hybridity Services 15
   Configure vSphere Replication Appliance 15

3 Managing Dedicated Disaster Recovery in vCloud Air 17
   About Networks for Dedicated Disaster Recovery 18
   About Placeholders in Dedicated Disaster Recovery 18

4 Configure a Target Site 21

5 Configure Virtual Machine Replication to Cloud 27
   Monitor Replication in vCloud Air 31

6 About Test Recoveries 33
   Test a Recovery 33
   Clean up a Test Recovery 34

7 About Recovery to Cloud 37
   Recover a Virtual Machine 38
   Monitoring the Status of Replication Tasks 39
   Stop Replicating a Virtual Machine 40
   Remove a Replication from vCloud Air 40

8 About Reverse Replication 43
   Reverse Replicate Virtual Machines 43

9 Configure vSphere Replication
   Alarms 45

10 Best Practices 47

11 Troubleshooting 49
Index  51
About this Guide


This guide explains how to use the single-tenant Dedicated Disaster Recovery to manage virtual machines replicated from your source site to the cloud as well as from the cloud back to your source site. This guide provides information in two parts:

- The first part of this guide provides an overview of Dedicated Disaster Recovery and how to configure and manage it by using the Hybrid Cloud Manager (HCM), the vSphere Web Client, and the vCloud Air User Interface (UI).
- The second part of this guide explains how to perform the Dedicated Disaster Recovery tasks in vCloud Air.

Intended Audience

This guide documents the tasks for disaster recovery administrators who are responsible for configuring and managing disaster recovery from their source sites to Dedicated Disaster Recovery. This guide documents the capabilities and tasks that you do using the vCloud Air UI.

Related Documentation

In addition to reading this guide, see the following documentation for complete information about using Dedicated Disaster Recovery:

- vCloud Air – Dedicated Disaster Recovery Release Notes for new features and known issues related to Dedicated Disaster Recovery.
- vCloud Air Advanced Networking Services Guide, including Direct Connect for vCloud Air for general information about configuring networking for virtual machines in the cloud.
- vCloud Air Hybrid Cloud Manager Guide for information on installing the HCM, including Proximity Routing and Stretching a Layer 2 Network to vCloud Air.
- vSphere Replication for Disaster Recovery to Cloud for information about using the vSphere Web Client to manage Dedicated Disaster Recovery from your source site.
VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.
Dedicated Disaster Recovery is a single-tenant, cloud-based disaster recovery service intended to protect virtual workloads managed by VMware vSphere that are either deployed in a private cloud or a data center. It provides a continuously available recovery site for VMware virtualized data centers. It is simple to set-up, manage, and costs less than the traditional disaster recovery solutions.

Dedicated Disaster Recovery is an expansion of the current vCloud Air Disaster Recovery service (that was available from January 2016). It is now based on the vCloud Air Dedicated cloud platform.

To implement and use Dedicated Disaster Recovery, you require the following products and services:

- **vCloud Air – Dedicated Cloud account**
  vCloud Air is a secure Infrastructure-as-a-Service (IaaS) cloud owned and operated by VMware, built on the trusted foundation of vSphere. The service supports existing workloads and new application development, giving IT administrators and architects a common platform for seamlessly extending existing data centers to the cloud by leveraging the same tools and processes they use today. You need a Dedicated Cloud subscription on vCloud Air and based on your needs you can create local accounts or integrate with your existing ADFS and SAML v2.

- **vSphere Replication Appliance**
  vSphere Replication Appliance is a feature of the VMware vSphere platform. vSphere Replication Appliance copies a virtual machine to another location, within or between clusters, and makes that copy available for recovery through the VMware vSphere Web Client.

- **vCloud® Air Hybrid Cloud Manager™ (HCM)**
  HCM seamlessly integrates vSphere® vCenter™ networks into vCloud Air. Hybrid networking extends your on-premises vSphere® vCenter™ networks into vCloud Air, supporting bidirectional virtual machine mobility while using Dedicated Disaster Recovery.

- **vCenter Administrator login and Internet connectivity.**

Using vSphere Replication and HCM on-premises, Dedicated Disaster Recovery can accommodate the most demanding business critical applications and allows you to scale your protection capacity to meet variable demands. This user guide addresses configuration, setup, and management aspects of vCloud Air in support of Dedicated Disaster Recovery.

This chapter includes the following topics:

- “Why Use Dedicated Disaster Recovery?,” on page 8
- “Service Architecture,” on page 9
- “Setting up this Service,” on page 10
- “Workflow for Using this Service,” on page 11
Why Use Dedicated Disaster Recovery?

There are a few key factors to consider before you decide what type of a Disaster Recovery solution is right for you. Are you looking to build and maintain your disaster recovery data center on your own, have a large budget, and are looking at hosted solutions? Typically, this is not the case.

You may have the budget but not enough skills or vice versa, in which case Dedicated Disaster Recovery is the perfect solution.

- Business continuity and disaster recovery are some of the key factors for ensuring your business critical environment, data, and online presence are available with minimal downtime. The availability services offered on vCloud Air help ensure that your data is protected, recoverable, and accessible by you and your customers.

- If you are looking for a cost-efficient and agile solution to implement or to replace dated, complex, and costly disaster recovery plans, VMware's vCloud Air – Dedicated Disaster Recovery, provides a cloud-based failover environment for dependable recovery when faced with an operational disruption.

- Dedicated Disaster Recovery enables site administrators to protect their vSphere onsite business-critical workloads from a broad range of potential disruptions by asynchronously replicating those workloads from a source site to the cloud for recovery and it uses vSphere Replication Appliance (host-based replication) to replicate virtual machines to vCloud Air.

- Administrators can perform a variety of disaster recovery operations for their virtual machines, including testing, planned migrations, and recovery by using Dedicated Disaster Recovery.

Benefits of this Service

Dedicated Disaster Recovery provides the following benefits:

- Simple and easy to use management platform that allows secure (enterprise to cloud) asynchronous replication and recovery of virtual machines.

- Introduces major efficiency gains over traditional business continuity and disaster recovery (BC/DR) practices.

- Allows for improved recovery point objective (RPO) and recovery time objective (RTO) policy compliance while reducing total cost of ownership (TCO).

  **Note**  
  RPO is the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds your BC/DR maximum allowable threshold. Whereas, RTO is the duration of time and a service level within which data must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

- Reverse failover of workflows to your source site.

  **Note**  
  You need to use vSphere Replication version 6.1.

- Self-service RPO settings from 15 minutes to 24 hours per virtual machine, perform unlimited 7 days run time tests, and run failed-over virtual machines for up to 30 days.

  **Note**  
  RPO policy compliance is dependent on available bandwidth from the source site to vCloud Air.

- Multiple point in time recovery snapshots that allows you to recover back up to 24 previous replication point in time.

- Introduces alternatives for migrating production applications to the cloud with reduced downtime and limited need for offline data transfers (ODT).
On-premises monitoring and management with the fully integrated vSphere Web Client.

Networking features include firewall, load balancer, virtual private networks, and DHCP+NAT.


Access to VMware’s production-level support.

Service Architecture

This section provides an overview of the Dedicated Disaster Recovery architecture and its key components.

Overview

Below is a high-level diagram of the service.

Figure 1-1. Dedicated Disaster Recovery Architecture

The left-hand side block contains your on-premises components:

- Hybrid Cloud Manager (HCM), which orchestrates Cloud Gateway (CGW) and WAN Opt to provide better performance
- HCM CGW, which provides the data plane connectivity
- vCenter, and
- vSphere Replication Appliance.

The right-hand side block contains your cloud components:

- Hybrid DMZ, consisting of the different services provided over the Org Edge Gateways, such as Firewall, Load Balancer, VPNs
- vCloud Air Dedicated Cloud
vCloud Air provides L2 stretching from your on-premises site to the cloud and the networks that are available on-premises are also available on the cloud. Virtual machines on your on-premises data center can be seamlessly replicated with the help of Dedicated Disaster Recovery and there is no need to re-IP or make any changes when disaster strikes. You can recover your virtual machines to vCloud Air Dedicated Disaster Recovery and use the Backup Routes (BGP) to inform about the workloads that are now available on the cloud.

**Proximity Routing**

Proximity Routing is a networking feature you can enable when you configure the CGW in HCM. It ensures that replications between virtual machines connected to stretched and routed networks, both on-premises and in the cloud, is symmetrical. IP-renumbering is not required after recovery and you can retain the MAC address while configuring replication. By default, "Retain MAC" is enabled if the source virtual machine is in a stretched network, and disabled when the network is not stretched.

Virtual machine stretched-network recovery (triggered on start of replication) runs on HCM. If a stretched network is pre-configured then virtual machines that are connected to the stretched networks will recover on the stretched network.

**Figure 1-2. Proximity Routing for Dedicated Disaster Recovery**

For more information, see MAC Address Retention and Proximity Routing.

**Setting up this Service**

Dedicated Disaster Recovery is a core service. You can order it directly through the My VMware portal by selecting a Dedicated subscription and adding HCM Advanced or Enterprise to the subscription.

You also need to add-on two additional public IP addresses for HCM to use. See the Hybrid Cloud Manager Installation and Administration Guide for Installing HCM.

You may also need ANS Standard or ANS Premium if you are using the Hybrid DMZ design or features such as, Direct Connect:

- See vCloud Air Advanced Networking Services for information about the ANS editors.
- See Hybrid DMZ Reference Designs for information about the Hybrid DMZ reference designs for vCloud Air.

See Workflow for Using this Service for an overview of using HCM, vSphere Replication and vCloud Air UI to manage Dedicated Disaster Recovery.
Workflow for Using this Service

As part of the enrollment process, VMware sets up your virtual data center enabled for disaster recovery that serves as your replication target and recovery site. VMware emails your login credentials for the Dedicated Disaster Recovery service in vCloud Air.

To configure and recover virtual machines protected by Dedicated Disaster Recovery, perform the following tasks in vSphere Replication and vCloud Air:

Prerequisites

Before you can use this service, you must meet the following prerequisites:

- You are a licensed vSphere customer running vSphere 6.1 (recommended) on-premises.
  
  See Disaster Recovery to Cloud System Requirements and Compatibility in vSphere Replication 6.1 for Disaster Recovery to Cloud for information.

- You have registered for a My VMware account.

- VMware has provided login access to the Dedicated Disaster Recovery service.

- vSphere Replication and HCM are enabled.

Procedure

1. Log into My VMware and download the vSphere Replication 6.1 appliance.

   vSphere Replication appliance is distributed as an OVF virtual appliance. You can deploy the appliance by using the standard vSphere OVF Deployment wizard. Download the vSphere Replication OVF package to a local directory or obtain its online URL.

2. Log into the vSphere Web Client at your source site to install the vSphere Replication appliance. Select the vCenter hosts and clusters where you will deploy the OVF template for the vSphere Replication appliance.

   Ensure vSphere Replication appliance is installed into vCenter and plug-in available via vSphere web client.

   See Installing and Configuring vSphere Replication to Cloud in vSphere Replication 6.1 for Disaster Recovery to Cloud for information.

3. Log into vCloud Air UI to create user roles to manage your Dedicated Disaster Recovery.

4. Ensure HCM has been installed and registered with Dedicated Disaster Recovery (target site). The VMware executed custom script is automatically run on vCenter to complete the vSphere Replication with HCM configuration.

   See Deploying Hybridity Service for information.

5. Using the vSphere Web Client at your source site, configure your connection to Dedicated Disaster Recovery.

   See Configure a Target Site for information.

6. Using vSphere Replication, replicate the virtual machines you plan to protect from your source site to Dedicated Disaster Recovery.

   See Configure Replication to Cloud for information.

7. After replicating your virtual machines to the cloud, log into Dedicated Disaster Recovery to view your virtual data center enabled for disaster recovery and the placeholder virtual machines that you selected for replication.

   See About Placeholders in Dedicated Disaster Recovery for information.
8 Using vSphere Replication or vCloud Air, test recovery for a virtual machine and cleanup the test after you run it.

See About Test Recoveries for information.

9 In the event that your source site becomes unavailable, log into the vCloud Air UI and recover your virtual machines to Dedicated Disaster Recovery.

See About Recovery to Cloud for information.

10 Once your source site is available, reverse replicate your virtual machines from the vCloud Air UI.

See Reverse Replicate Virtual Machines for information.

System Requirements and Compatibility

Once you are subscribed to the service, VMware ensures that the environment is configured for replications by providing a disaster recovery-enabled virtual data center (VDC). To enable replications to Dedicated Disaster Recovery, your on-premises environment must meet certain requirements in terms of additional configuration and specific versions of the VMware products that you use.

Product Compatibility

Replications to Dedicated Disaster Recovery and access to new features require that you run certain versions of VMware products on the source site and on the target site. You must verify that you run a supported version of the products. Please contact your VMware representative for more details.

VMware recommends the following product versions for this release of Dedicated Disaster Recovery:

<table>
<thead>
<tr>
<th>Table 1-1. Recommended Cloud Component Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
</tr>
<tr>
<td>vCloud Director</td>
</tr>
<tr>
<td>vCenter</td>
</tr>
<tr>
<td>ESX</td>
</tr>
<tr>
<td>NSX</td>
</tr>
</tbody>
</table>

**Note** Ensure that virtual machine or vApp limits adhere to the vCloud Director resource standards and constraints.

<table>
<thead>
<tr>
<th>Table 1-2. Recommended On-premises Component Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
</tr>
<tr>
<td>vSphere Replication Appliance</td>
</tr>
<tr>
<td>vCenter Server</td>
</tr>
<tr>
<td>vSphere Web Client</td>
</tr>
<tr>
<td>ESXi host</td>
</tr>
<tr>
<td>HCM (1 per vCenter)</td>
</tr>
<tr>
<td>Virtual machine hardware</td>
</tr>
</tbody>
</table>

Supported Browsers

The following browsers are recommended while working with the vCloud Air and vSphere UIs.
**Table 1-3. Recommended Browsers**

<table>
<thead>
<tr>
<th>Browser</th>
<th>Recommended Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>54</td>
</tr>
<tr>
<td>Firefox</td>
<td>49</td>
</tr>
<tr>
<td>Safari</td>
<td>10</td>
</tr>
</tbody>
</table>

**Note** Ensure that you have Internet connectivity without a proxy or traffic filtering device setup.

**Performance Metrics**

The maximum limits for Dedicated Disaster Recovery are as follows:

**Table 1-4. Maximum Limits**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total virtual machines configured for replication per tenant</td>
<td>1000</td>
</tr>
<tr>
<td>Concurrent configured replications</td>
<td>30</td>
</tr>
<tr>
<td>Concurrent recovery operations</td>
<td>100</td>
</tr>
</tbody>
</table>

**Resource Allocation**

Dedicated Disaster Recovery offers flexible term-based subscription options and convenient feature add-ons.

After you subscribe to Dedicated Disaster Recovery, you are provisioned with a disaster recovery-enabled VDC that includes the following resources:

**Table 1-5. Resources Allocated with Subscription**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Dedicated Disaster Recovery Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>35GHz vCPU and 240GB vRAM</td>
</tr>
<tr>
<td>Storage</td>
<td>6TB SSD-Accelerated Storage</td>
</tr>
<tr>
<td>Storage</td>
<td>6TB Basic Storage</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>50Mbps</td>
</tr>
<tr>
<td>Public IP Addresses</td>
<td>3 included</td>
</tr>
<tr>
<td>Memory Upgrade</td>
<td>240GB to 480GB RAM</td>
</tr>
<tr>
<td>All-SSD Standard Block Storage</td>
<td>2TB</td>
</tr>
<tr>
<td>All-SSD Premium Block Storage</td>
<td>2TB</td>
</tr>
<tr>
<td>Data Protection</td>
<td>1TB</td>
</tr>
<tr>
<td>Direct Connect - Cross Connect</td>
<td>1Gbps</td>
</tr>
<tr>
<td>Direct Connect - Cross Connect</td>
<td>10Gbps</td>
</tr>
<tr>
<td>Direct Connect - Network Exchange</td>
<td>1Gbps</td>
</tr>
<tr>
<td>Direct Connect - Network Exchange</td>
<td>10Gbps</td>
</tr>
<tr>
<td>Advanced Networking</td>
<td>Standard</td>
</tr>
<tr>
<td>Advanced Networking</td>
<td>Premium</td>
</tr>
<tr>
<td>Hybrid Cloud Manager</td>
<td>Advanced</td>
</tr>
<tr>
<td>Hybrid Cloud Manager</td>
<td>Enterprise</td>
</tr>
</tbody>
</table>
Table 1-5. Resources Allocated with Subscription (Continued)

<table>
<thead>
<tr>
<th>Resource</th>
<th>Dedicated Disaster Recovery Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline Data Transfer</td>
<td>11TB one-time Data Transfer</td>
</tr>
<tr>
<td>Failover Tests</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Support</td>
<td>Production-level</td>
</tr>
</tbody>
</table>


Connectivity and Firewall Considerations

Dedicated Disaster Recovery uses the IPsec tunnel established between Cloud Gateways as the data path for replications.

For proper communication ensure that the below listed source and targets are capable of communicating with the corresponding port requirements.

Table 1-6. Port Access Requirements

<table>
<thead>
<tr>
<th>Network Port</th>
<th>Protocol</th>
<th>Source Site</th>
<th>Target Site</th>
<th>Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>ESXi host</td>
<td>vCenter Server</td>
<td>vCenter Server reverse proxy forwards vSphere Installation Bundle (VIB) download request to vSphere Replication appliance.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>vSphere Replication appliance</td>
<td>vCloud Air</td>
<td>vSphere Replication appliance connects to this port to send replication data to a cloud organization.</td>
</tr>
<tr>
<td>10000-10010</td>
<td>TCP</td>
<td>ESXi host</td>
<td>vSphere Replication appliance</td>
<td>vCloud Tunneling Agent (vCTA) opens one of these ports on the vSphere Replication appliance. ESXi hosts connect to that port to send replication data to a cloud organization.</td>
</tr>
</tbody>
</table>

See Configure Network Connectivity for HCM port access requirements.
Deploying Hybridity Services

HCM provides the data plane to build the tunnel between your on-premises workloads to the cloud with the help of Cloud Gateway (CGW). You must install HCM on your vCenter and configure it to work with the vSphere Replication appliance so that all the replication traffic, regardless of the target site, will go through the HCM CGW and WAN optimization appliances.

Download HCM 2.0 U1 OVA file and then refer to the Hybrid Cloud Manager Installation and Administration Guide to complete the following tasks:

- Deploy HCM
- Register HCM with vCenter
- Register HCM with vCloud Air
- Configure Hybrid Cloud Gateway
- Stretch a Layer 2 Network to vCloud Air

Configure vSphere Replication Appliance

You must configure and patch the vSphere Replication Appliance to communicate with HCM.

- After configuring vSphere Replication Appliance, download the Python script.

Prerequisites

- Deploy the vSphere Replication Appliance and refer to Installing and Configuring vSphere Replication to Cloud to install and configure it.

Procedure

1. Copy the Hms_Jar_Edit.py script to the vSphere Replication Appliance.
2. Use the python Hms_Jar_Edit.py <HCM IP> syntax to execute the binary.

The vSphere Replication Appliance can now communicate with HCM.
Managing Dedicated Disaster Recovery in vCloud Air

When you subscribe to Dedicated Disaster Recovery, you use the vCloud Air UI to monitor and manage the virtual machines you are replicating to the cloud.

After setting up virtual machines for replication, use the vCloud Air UI to monitor and manage the replication and recovery for those virtual machines; for example, testing a recovery or performing a recovery to a placeholder virtual machine in the event of a disruption at the source site.

After replication from the source site begins, you can modify the network and customization settings configured for the placeholder virtual machine. Other settings for a placeholder virtual machine are not available before you recover the virtual machine to the cloud. After you recover a virtual machine to the cloud, it has the same capability that the virtual machine had at the source site.

When a virtual machine powers on as a result of a test or recovery, its operation in vCloud Air is subject to the following runtime leases:

- Virtual machines powered on during a disaster recovery test—7 business day lease
- Virtual machines powered on after being recovered to the cloud—30 day lease

Clicking on Disaster Recovery displays your new disaster recovery-enabled VDC, where you can replicate your on-premises virtual machines in to this VDC, perform test and recovery failovers, as well as reverse replications. To view the lease times for a test or recovered virtual machine in vCloud Air, go to the Disaster Recovery > Virtual Machines tab > Test/Recovery Time column. The Test/Recovery Time column shows the time since a test or recovery, displayed using the local time of the browser time zone.

Figure 3-1. Dedicated Disaster Recovery Service

This chapter includes the following topics:

- “About Networks for Dedicated Disaster Recovery,” on page 18
- “About Placeholders in Dedicated Disaster Recovery,” on page 18
About Networks for Dedicated Disaster Recovery

When you subscribe to Dedicated Disaster Recovery, VMware creates two default networks for the service—an isolated network and an external routed network. The gateway for the routed network has a public IP address on its outside interface so that the routed network on the inside interface is accessible through the Intranet. You can use these networks for your virtual machines protected by Dedicated Disaster Recovery.

When you configure Dedicated Disaster Recovery in vSphere Replication, you specify which networks to use for the Test network and the Recovery network. The network choices that appear in the wizard are the networks configured for vCloud Air.

See Connect to a Cloud Provider Site in vSphere Replication 6.1 for Disaster Recovery to Cloud for information. You can choose to use the vCloud Air default networks for the Dedicated Disaster Recovery service; for example, specify the default isolated network as your test network and the default routed network as your recovery network. If you decide to create networks for test and recovery in vCloud Air, you must update the target networks in the vSphere Web Client.

For information about updating your target networks in the vSphere Web Client, see Select Recovery Networks on the Target Virtual Data Center in vSphere Replication 6.1 for Disaster Recovery to Cloud. For information about adding networks in vCloud Air, see Add a Network to a Virtual Data Center in the vCloud Air Networking Guide. When you test a recovery or recover a virtual machine to the cloud, vCloud Air attaches the virtual machine to the test or recovery networks respectively.

About Placeholders in Dedicated Disaster Recovery

When you configure replication by using vSphere Replication at your source site, Dedicated Disaster Recovery creates placeholder virtual machines in vCloud Air which represent the virtual machines at your source site.

Placeholder virtual machines are accessible in two areas of the vCloud Air UI for a virtual data center enabled for disaster recovery:

- The Replications tab—contains placeholders for the virtual machines replicated from your source site.
  
  Use the Replication tab to verify that your virtual machines are protected by Dedicated Disaster Recovery and to view the status of your replications. The Cloud provider address and Organization Name required while configuring the vSphere Replication 6.1 Web Client for replication to the cloud are also listed here.

- The Virtual Machines tab—contains placeholders, virtual machines for which you are testing recovery, and virtual machines recovered to the cloud. A placeholder virtual machine appears in the Virtual Machines tab after the initial full synchronization of replication data from the source site successfully completes.
  
  Use the Virtual Machines tab to test recovery and recover the virtual machines to the cloud in the event your source site is unavailable.
  
  The status of each placeholder determines what actions are available for that virtual machine represented. After you test a recovery or recover a virtual machine to the cloud, Dedicated Disaster Recovery service replaces the placeholder with a test or production virtual machine respectively.

About the Replication of Placeholders

vCloud Air UI displays the following information about virtual machine replication.
Table 3-1. Replication Information Displayed for Each Placeholder

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the placeholder virtual machine.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the replication.</td>
</tr>
<tr>
<td>Last Completed</td>
<td>Last synchronization completed; displayed using the local time of the browser time zone.</td>
</tr>
<tr>
<td>Sync Duration</td>
<td>The length of time the last synchronization took.</td>
</tr>
<tr>
<td>Sync Size</td>
<td>The size of the last data replicated (not the size of the virtual machine).</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery point objective (RPO), which is the replication time interval that you specify, 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 in the cloud. Replication occurs at the RPO interval that you set in the vSphere Web client. <strong>Note</strong> Lower RPO times reduce potential data loss but use more bandwidth and system resources.</td>
</tr>
</tbody>
</table>

Table 3-2. About the Replication Status Values

<table>
<thead>
<tr>
<th>Replication Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring</td>
<td>Virtual machine configuration is in progress.</td>
</tr>
<tr>
<td>Full Sync</td>
<td>Full synchronization is in progress.</td>
</tr>
<tr>
<td>Initial Full Sync</td>
<td>Initial full synchronization is in progress. This status only appears for the first initial synchronization when the virtual machine is added to the system.</td>
</tr>
<tr>
<td>Not Active</td>
<td>The virtual machine replication is configured properly and vCloud Air did not encounter a replication error. However, vCloud Air is not receiving replication traffic for the placeholder or does not have an open connection for the placeholder.</td>
</tr>
<tr>
<td>OK</td>
<td>The replication is configured correctly—no configuration or replication errors are present. However, Dedicated Disaster Recovery has not sent replication traffic to the cloud.</td>
</tr>
<tr>
<td>Paused</td>
<td>The replication is not running because a vSphere Replication user paused the replication. See Pause or Resume a Replication Task in vSphere Replication 6.1 for Disaster Recovery to Cloud for information.</td>
</tr>
<tr>
<td>Recovered</td>
<td>Dedicated Disaster Recovery recovered the virtual machine to the cloud successfully.</td>
</tr>
<tr>
<td>Recovering</td>
<td>Dedicated Disaster Recovery service is recovering the virtual machine to the cloud.</td>
</tr>
<tr>
<td>Sync</td>
<td>The virtual machine data at the source site is synchronizing with the placeholder virtual machine in vCloud Air.</td>
</tr>
</tbody>
</table>
See Monitoring the Status of Replication Tasks in vSphere Replication 6.1 for Disaster Recovery to Cloud for information.

**NOTE** If an RPO violation occurs when vCloud Air (the replication target) loses connectivity to the source site, it is displayed in the Web console.
Configure a Target Site

Before you configure replication tasks to the cloud, you must configure the connections between your vSphere environment and virtual data centers that belong to the Dedicated Disaster Recovery service.

To configure a Target Site:

**Prerequisites**

- Ensure you can login to vSphere Replication through the vSphere Replication Appliance and vSphere Web Client.
- Ensure you have login credentials to the vCloud Air - Dedicated Disaster Recovery service.

**Procedure**

1. In a web browser, open your unique vCloud Air - Dedicated Disaster Recovery service URL.
   
   **Note** This URL is specific to your organization and is provided by VMware on successful subscription to the service.

2. Enter your username and password and click Login.

3. Click Disaster Recovery.

   Ensure that your virtual data center has disaster recovery resources available.

4. Click the Replications tab.

   Note down the Cloud provider address (Cloud endpoint URL) and the Organization Name.

5. Now, login to your vSphere Web Client.

6. Click vSphere Replication > Home > Manage.
7 Under the vSphere Replication tab, click **Target Sites** and then click the **Connect to a Cloud Provider** icon.

8 On the **Connection settings** page of the **Connect to a Cloud Provider** wizard, enter the **Cloud provider address** and **Organization Name** you had noted down in Step 4 along with your vCloud Air **User name** and **Password**.

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

9 Click **Next**.

The Connect to a Cloud Provider 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.
10 From the list of virtual data centers, select a target for the connection and click **Next**.

11 Review your connection settings and click **Finish**.

12 The connection to your cloud organization appears under **Target Sites** and the Status is displayed as **Missing network settings**, because you have not selected the networks to use for recovery and test recovery operations on the target site.

13 Right-click on the virtual data center name and select **Configure target networks**.
14 On the **Network Settings** page, select the Recovery network and Test network from the drop-down menu and click **Next**. The drop-down menus displays only the networks that are configured for vCloud Air.

If stretched network is pre-configured, then virtual machines which are connected to the stretched network will recover on the stretched network. If a stretched network is not found, the virtual machines will automatically recover on the recovery network. Virtual machines which are not associated with a stretched network will recover on the default network.

15 On the **Local recovery networks** page, select the cloud networks from the left pane and select the local recovery networks from the right pane. Click **Add Mappings** and click **Next**.
16 On the **Local 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**.

17 Under **Ready to complete**, review your settings and click **Finish**.
What to do next

You can now configure virtual machines to replicate to Dedicated Disaster Recovery.

When you test a replication or perform a recovery operation, vCloud Air automatically attaches the virtual machine to the test or recovery (or stretched) network respectively.
Configure Virtual Machine Replication to Cloud

After configuring a target site, you can configure your virtual machines to replicate to Dedicated Disaster Recovery.

Prerequisites

Ensure that a target site is configured correctly.

Procedure

1. On the vSphere Web Client Home page, click VMs and Templates.
2. In the Navigator menu, navigate down to the virtual machine level.
   A list of your virtual machines will be displayed.
3 Right-click the virtual machine that you want to replicate and select **All vSphere Replication Actions > Configure Replication.**
4 A Configure Replication wizard opens. Select Replicate to a cloud provider and click Next.

5 Select the Target site to which you want to replicate the virtual machine and click Next.

   The target cloud provider you had configured in the previous topic is displayed under VDC Name.

6 On the Target location page, select where to store replication data. From the drop-down, select the Standard storage policy for replication placement and click Next.

7 (Optional) On the Replication options page, select the quiescing method for the Guest Operating System (OS) of the source virtual machine.

   **NOTE** Quiescing is a process of bringing the on-disk data of a virtual machine into a state suitable for backups. Quiescing options are available only for virtual machines that support quiescing.

8 (Optional) Select Enable network compression for VR data and click Next.

   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 site.
9 On the **Recovery settings** page, use the RPO slider to set an acceptable data loss period in case of a site failure.

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

10 (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.

11 Click **Next**.

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

You can check the state of each replication. Under **Monitor > vSphere Replication**, you will see that the virtual machine is in the process of configuring against the target site.

**What to do next**

Click the **Refresh** icon to refresh the Monitor page. The Replication status of the virtual machine is now in the **Not Active** state. Continue to refresh the Monitor page until you see that the **Initial Full Sync** from this virtual machine to vCloud Air has begun.
You can see the progress of the Initial Full Sync on the Replication Details tab at the bottom of the Monitor tab page. After the Initial Full Sync is complete the status changes to OK.

**Monitor Replication in vCloud Air**

Along with monitoring the virtual machine replication progress from the on-premises vCenter, you can also monitor it from the vCloud Air – Dedicated Disaster Recovery UI.

**Prerequisites**

Ensure that you are logged in to your Dedicated Disaster Recovery site.

**Procedure**

1. Click Disaster Recovery.
2. Click the Replications tab.
   
   The virtual machine in the list is in the Configuring state and after it is configured the Replication Status changes to Initial Full Sync.
3. After the Initial Full Sync is complete, the Replication Status changes to Replication OK (Incoming).
4. After the sync is complete, the Replication Status under the Replications tab changes to Success.

**What to do next**

Do not manually power ON the replicated virtual machines in the cloud, because you may need to use the Test Recovery option for testing or the Recovery option in case of a disaster, which is explained in the next section.
You can initiate tests from the vSphere Web Client at your on-premises data center (source site) or from the vCloud Air UI.

Test recoveries allow you to verify that source data is replicated correctly on the target site. When you initiate a replication task to the cloud, a placeholder virtual machine is created on the target virtual data center. Initiating tests from the vCloud Air UI is necessary when your source site is unavailable and you may want to run a final test recovery.

The following conditions apply to testing recoveries:

- When you invoke a test from your source site, you have the option to synchronize data between the source site and the cloud before creating the test recovery. This option is not available when initiating a test from vCloud Air.
- Initiating a test from the cloud creates a test recovery using replicated virtual machine data, reconfigures the virtual machine to connect to the test network, and applies guest customization.
- Testing a recovery does not affect services at the source site.
- While a test recovery runs, the Dedicated Disaster Recovery service continues to replicate data from the virtual machines at your source site configured for protection to vCloud Air.

**Note** Your subscription for the Dedicated Disaster Recovery service requires your coordination with VMware Global Support Services when testing recoveries for virtual machines in vCloud Air. Contact your Global Support Services representative for information.

For information about testing a recovery, see Test a Recovery. A successful test recovery powers on the virtual machine. When you perform a test, the Recovery Status changes from Placeholder to Test Complete.

This chapter includes the following topics:

- “Test a Recovery,” on page 33
- “Clean up a Test Recovery,” on page 34

### Test a Recovery

To guarantee a recovery in the event of disruption at your source site, you should test a placeholder virtual machine to ensure its integrity is intact.

**Prerequisites**

- Verify that a test network was configured.
  
  See About Networks for Dedicated Disaster Recovery for information.
- You have the correct user permissions to perform the test.
**Procedure**

1. Click the **Virtual Machines** tab.
   
   The table of virtual machines appears.

2. Select the virtual machine placeholder you want to test and click **Test** or **Actions > Test**.

3. A confirmation dialog box appears.

4. Click **Yes** to continue.

5. Follow the prompts to failover the virtual machine(s) with a point-in-time date/time.

   vSphere Replication configures the placeholder virtual machine for testing and uses the data that is copied on the target site at the point-in-time that you select from the list.

During test recovery, the Dedicated Disaster Recovery service does not create a copy of the recovered virtual machine. Testing a placeholder creates a test virtual machine using replicated data, reconfigures the test virtual machine to connect to the test network, and applies guest customization to the virtual machine so that you can log in and verify the replication progress.

**Clean up a Test Recovery**

After you test a recovery for a placeholder virtual machine, return the virtual machine to the ready state by running a cleanup. Cleaning up a test recovery releases resources consumed by the test and prepares for the next test, planned migration, or disaster recovery.

You can run a cleanup from the vSphere Web Client at your source site or from vCloud Air regardless of where you initiated the preceding test.
Prerequisites

- Verify that you tested the placeholder virtual machine.
- You have the correct user permissions to clean up the test.

Procedure

1. Click the Virtual Machines tab.
   - The table of virtual machines appears.
2. Select the tested recovery you want to clean up.
3. Click Cleanup.
   - A confirmation dialog box appears.
4. Click Continue.

Running a clean up after a test resets the test recovery for the virtual machine by performing these tasks:

- Powers off the test virtual machine.
- Replaces the test virtual machine with a placeholder, preserving the virtual machine identity and configuration information.
- Cleans up replicated storage snapshots that the virtual machine used during testing.
- Resets the Recovery Status from Test to Placeholder.
About Recovery to Cloud

Run this workflow to recover your production virtual machines from your on-premises data center (source site) to vCloud Air. When possible, VMware recommends you test the recovery before running the recovery.

You can recover a virtual machine by using vCloud Air when your source site is no longer accessible. You might be able to begin a recovery from your source site by using your local vSphere Web Client; for example, you have sufficient warning of an outage and still have access to your local vSphere Web Client so that you can run a planned migration.

When you recover a virtual machine from your source site to vCloud Air, the production state of the virtual machine represents a point in time before the outage. Data accumulated after the last replication to vCloud Air and before the recovery is not available in the cloud.

Recovering a virtual machine to vCloud Air stops replication from the source site.

Multiple Point in Time Recovery

By enabling the multiple point in time (MPIT) setting, you can leverage previous replication points for better control on failover. It allows you to:

- Set up to 24 previous restore points
- Choose your restore point
- Restore up to 24 days previous replication points (dependent on your RPO setting)

**Figure 7-1. Choose from up to 24 Recovery Snapshots**

You can choose the MPIT settings in the Recovery settings step while configuring a virtual machine for replication in the vSphere Web Client. See Configure Virtual Machine Replication to Cloud.
Assume you have set a 15 minutes (minimum) recovery point objective (RPO) and you start the replication at 9:00 a.m., which means data changes for that particular virtual machine are replicated every 15 minutes. Now in the event of a failover, you can pick a specific time to recover from. For example, if the on-premises data center has an issue and you need to failover at 11 a.m. However, at that time you find that the data may not be suitable. If you have enabled MPIT, you can recover the data copied over at say, 10:30 a.m.

If you were to set your RPO 24 hours (maximum), then you would have the ability to restore up to 24 days previous replication points. This allows you to reverse failover up to 24 days. With the MPIT recovery you can pick the specific point in time that you want to have data recovered, allowing you to successfully recover in the event of data corruption.

This chapter includes the following topics:

- “Recover a Virtual Machine,” on page 38
- “Monitoring the Status of Replication Tasks,” on page 39
- “Stop Replicating a Virtual Machine,” on page 40
- “Remove a Replication from vCloud Air,” on page 40

**Recover a Virtual Machine**

Recovering a virtual machine shuts down the virtual machine at your source site (if possible) and recovers it in the cloud. During recovery, all replication activity is stopped. If a stretched network was pre-configured and if you initiate recovery from the cloud, virtual machines which are connected to the stretched network automatically recover on the stretched network, else they recover on the recovery network.

**Prerequisites**

You have the correct user permissions to recover the virtual machine to the cloud.

If possible, meet these prerequisites:

- Verify that you tested the recovery before recovering the virtual machine to the cloud.
- Contact VMware Global Support Services and declare the disaster prior to recovering your virtual machines.
- If you have run test recoveries for the replication that you want to migrate, verify that you cleaned up the test results.

**Procedure**

1. Click the **Virtual Machine** tab.
   
   The table of virtual machines appears.

2. Select the virtual machine(s) that you want to recover.

3. Click **Recovery** or **Actions > Recovery**.
   
   The confirmation dialog box appears.

4. Click **Yes** to continue.
5 Select the Point-in-Time instance to which you want to recover the virtual machine and click OK.

Multiple point-in-time option is only available if the virtual machine was configured to save multiple replication instances while configuring replication.

**Figure 7-2. Set MPIT**

![Point-in-Time Recovery Selection](image)

6 Report any issues that occur during failover.

7 During the recovery process the status of the virtual machine in vCloud Air will be **Recovery in Progress**.

8 Once the recovery is complete the Recovery Status changes to **Recovered**, the virtual machine in vCloud Air is powered ON and connected to the Recovery network (or Stretched network).

Recovering the virtual machine has the following result:

- In the Virtual Machine tab, the Recovery Status changes from Placeholder or Test Complete to Recovered.
- Connects the virtual machine to the recovery network that was configured earlier.
- Powers on the virtual machine in the cloud.

After you recover a virtual machine to the cloud, it has the same capabilities that the virtual machine had at the source site. You can access and operate your virtual machine recovered to the cloud for the time periods listed in Managing Dedicated Disaster Recovery in vCloud Air.

### Monitoring the Status of Replication Tasks

In the vSphere Web Client, you can check the status of replication tasks for a vCenter Server. The list of outgoing replications is located under **vSphere Replication > Monitor**.

**Table 7-1. Replication Status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Not Active | Replication is not currently running. | ■ Source virtual machine is powered off.  
 ■ Communication breakdown between ESXi host and target site. |                                              |
| Paused     | Replication is paused.       | vSphere Replication user has paused the replication.                 |                                              |
| Error      | Configuration error occurred. |                                                                      |                                              |
| Recovered  | Recovery complete.           |                                                                      |                                              |
Stop Replicating a Virtual Machine

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

**Prerequisites**

To stop a replication, both your on-premises data center (source site) and Dedicated Disaster Recovery should be online and connected.

**Procedure**

1. On the vSphere Replication home page, click the **Monitor** tab and then click **Outgoing Replications**.
2. Right-click a replication and select **Stop**.
   - You can stop multiple replication tasks simultaneously only if they are replicated to the same virtual data center.
3. When you stop a replication, the virtual machine gets unconfigured for replication and vApp and virtual machine disks are deleted from Dedicated Disaster Recovery.
4. When you force stop replication, you remove the replication task only from the source site. All data that was stored on Dedicated Disaster Recovery during the replication remains on the target datastore, and the replication remains visible on the target site. You must manually delete the replication artifacts from Dedicated Disaster Recovery.
5. Click **OK** to confirm.

If force stop operation is performed on a virtual machine on source site, the replication status of the virtual machine in Dedicated Disaster Recovery will be in error state and you will have to remove the replication from the vCloud Air UI.

**What to do next**

See Remove a Replication from vCloud Air.

Remove a Replication from vCloud Air

When disaster recovery is no longer required for a virtual machine, you can stop the virtual machine replication to vCloud Air.

Stop the replication by using the vSphere Web Client at the source site. See Stop a Replication Task in vSphere Replication 6.0 for Disaster Recovery to Cloud for information.

Stopping a replication from the source site, removes the replication data from the source site and the cloud when both sites are connected.

If the cloud is offline when you stop a replication from the source site, the Dedicated Disaster Recovery service does not remove the replication data from vCloud Air. You must manually remove the replication from vCloud Air.

**Note** Use caution when removing a placeholder virtual machine from vCloud Air because placeholders are not protected in vCloud Air from accidental deletion.

**Prerequisites**

You have the correct user permissions to remove the replication.
Procedure

1. Click the Replication Status tab. The list of virtual machines along with their replication status appears.

2. Select the checkbox next to the virtual machine that you want to remove.

3. Click Remove replication. A confirmation dialog box appears.

4. Click Continue. The placeholder virtual machine is deleted from the list in the Replication Status tab and all replication data is deleted from the cloud storage.
Reverse replication of virtual machines that you have previously recovered is available by using vSphere Replication.

Once you have restored your on-premises data center, after a maintenance procedure or a disaster, you can reverse replicate the virtual machines which were recovered on vCloud Air. In vSphere Replication, you can configure reverse replication that will repoint the replication of the virtual machines running on vCloud Air back to your on-premises vSphere environment. Reverse replication provides you with the ability to restore your services from the cloud back to your on-premises data center.

**NOTE** To use reverse replication you must power-off the virtual machine before you copy it. You can start multiple copies simultaneously and run them in parallel.

**Figure 8-1. vCloud Air - Dedicated Disaster Recovery with Reverse Failover**

Reverse Replicate Virtual Machines

Using vSphere Replication you can reverse replicate (failover) a recovered outgoing replication and start copying data from the cloud to your on-premises data center (source site).

If you replicated virtual machines from your on-premises data center to the cloud and recovered those virtual machines in the cloud for use while your on-premises data center was being maintained (or in the event of a disaster), once your on-premises data center is back online, you can synchronize the changes from the cloud to on-premises, or migrate the virtual machine from the cloud back to your on-premises data center.
Prerequisites

- Verify that Dedicated Disaster Recovery is available and connected to your on-premises data center.
- Verify the status of the replication you want to reverse is Recovered.
- vSphere version is 6.1

Procedure

1. Login to vSphere Web Client.
2. Under vSphere Replication tab, click Monitor > Outgoing Replications.
3. In the list of outgoing replications, select the replication that you want to reverse, and click the Reverse replication icon.
   The replication status must be Recovered.
4. If the connection between your cloud and on-premises is lost, you will be prompted to enter the cloud provider address, organization name, and login credentials.
5. Review the settings and click OK.
   The source virtual machine on the source site is unregistered from the inventory and becomes inaccessible until you recover the replication. vSphere Replication starts synchronizing data from the cloud to your on-premises environment.
6. The reversed replication is removed from the list of outgoing replications and appears in the list of incoming replications.
   If the virtual machine in cloud is powered Off the replication status will be shown as Not Active until the virtual machine is powered On. After the Initial Full Sync is complete the replication status changes to OK.
7. After reverse replication is complete, the recovery Status of the virtual machine in the Dedicated Disaster Recovery UI will be Reverse Replication in Progress and the replication Status will be shown as Success.
Configure vSphere Replication Alarms

You can configure and edit alarms to alert you when a specific vSphere Replication events occur. For example, you may configure an alarm to trigger if the replication status of a virtual machine changes after you configure that virtual machine for replication.

Using the steps listed below, you can configure an alarm for the virtual machines in your vCenter if their Replication Status changes to RPO Violation.

Procedure

1. Select the vSphere Replication Appliance.
2. Click Manage > Alarm Definitions.

Depending on the inventory object selected different alarm definitions are displayed.
3 Click the green + sign to create alarms based on triggered events.
   The New Alarm Definition wizard opens.
4 Enter an **Alarm name**, **Description**, and select **Virtual Machines** from the 'Monitor' drop-down.
5 Click **Next**.
6 Select **specific event occurring on this object...** from the **Monitor for options**.
7 Select **Enable this alarm** checkbox.
8 Click on the Add (+) and select **RPO violated** from the **Event** drop-down list and set the status to **Alert**.
9 Add second event **RPO restored** to clear the alarm when Replication become OK and set the Status to **Normal**.
10 Choose the Action method and click **Finish**. In this example, an email is sent as a notification when the alarm is triggered.

The new alarm is created and is triggered when an RPO violation occurs on any of the virtual machines in the selected vCenter.

**Note** Reports are available via the vSphere Web Client to show transferred bytes, RPO violations and relocated virtual machine count.
VMware recommends a few best practices to be followed while using the service.

- Replication datapath requires CGW to be deployed via HCM. Ensure that the firewall requirements for CGW are met.
- CGW tunnel should be up and active while configuring virtual machines replications.
- Virtual machines recovery should be enforced via the Dedicated Disaster Recovery UI.
- Use allocation pool as allocation model for Dedicated Disaster Recovery-enabled VDCs, which will allow you to scale up more virtual machines.
- You need to associate a virtual machine with a stretched network before initiating replication if you want to later recover it over a stretched network.
Troubleshooting

This section lists some of the issues and their causes that may occur in Dedicated Disaster Recovery.

- **Second vCloud Director endpoint on the on-premises HCM cloud collection table causes virtual machine replications to go in to the 'Not Active' state**

  Initially you register HCM and vSphere Replication Management Server (VRMS) to one cloud endpoint and then you register both HCM and VRMS to another cloud endpoint and later remove the second registration. However, the second cloud registration still exists in the database and the Dedicated Disaster Recovery transport service receives two cloud registrations from HMS, which causes messages or events to be sent to the second (stale) cloud registration. This is not visible from the UI.

  To resolve this issue, contact vCloud Air support and they will delete the second cloud registration from the database.

- **Cannot configure replication on virtual machines that you created in an ESXi host**

  If you have created a virtual machine in ESXi and not in vCenter, when you configure it for replication, that virtual machine does not Power ON after recovery, because the replicated virtual machine has a MAC address that is not recognized by vCenter.

  After test recovery is complete, you can resolve this issue by resetting the MAC address and powering on the virtual machine manually.

- **User authentication failure**

  User authentication failure should not occur as OrgAdmin is directly authenticated against vCloud Director. However, if it does occur, it may be due to the role associated with the user account. Verify that the user role has the required privileges.

- **Cloud registration fails**

  It may be due to any of the following reasons:

  - The role associated with the user account may not have the correct privileges.
  - vCloud Director is not reachable from on-premises datacenter.
  - HCM does not retry if login credentials are incorrect. The credentials must be authenticated before HCM attempts to log in and start the cloud registration.

- **Virtual machine replication errors or virtual machine in ‘Not Active’ state**

  - A replication error is displayed when the tunnel does not get created due to the HCM transport service breakdown. Review the on-premises HCM log files.
- A virtual machine may be shown as 'Not Active' state due to the CGW. Ensure that the CGW status is active in the on-premises HCM UI.

- **Virtual machine not displayed in the Dedicated Disaster Recovery UI**

Some virtual machines may not be displayed in the UI due to a lag in vCloud Director inventory updates. Also, the virtual machines created in vCloud Director or the ones that are not associated with replication groups will not be displayed in the Dedicated Disaster Recovery UI. You can view these virtual machines in the vCloud Director UI.

- **Cannot ping after test/recovery**

If you cannot ping a virtual machine after test and recovery, verify if the pings are coming from the same subnet. In the case of recovery over a stretched network, the IP address should be preserved on the cloud side after successful recovery. You can test if the ping works in the same L2 segment before proceeding to a different segment.

For Technical Support, file a request through standard VMware process available at [My VMware](https://my.vmware.com).
Index

C
  clean up
    results 34
  test recovery 34
  compatibility 12
  connectivity 14

D
  Dedicated Disaster Recovery
    required VMware products 8
  task workflow 11
  Disaster Recovery
    default networks 18
    features 8
    login credentials 10
    prerequisites 10
    related documentation 5
    setup 10
    usage metering 17
  DR-VDC, vCloud Air Dashboard 17

F
  failback, vSphere Replication 43

G
  guest customizations, test recovery 33

I
  intended audience 5

M
  migrate, virtual machine to cloud 38
  My VMware, Disaster Recovery subscription 10

N
  network
    customization 17
    production 38
  networks, Disaster Recovery 18

O
  offline data transfer, Disaster Recovery feature 8

P
  placeholder
    cleanup test 34
    integrity test 33
    overview 18

R
  recovery
    network 18
    overview 37
  results 38
  source site unavailable 38
  test 33
  time periods to access 17
  Recovery Time column 17
  replication
    image size 18
    manage 17
    remove 40
  source site 11
  status values 18
  tab overview 18
  requirements 12
  resources 13
  RPO
    feature 8
    times 18
    violation 18

S
  source site
    clean up test 34
    connectivity loss 18
    failback virtual machine 43
    planned migration 38
    unaccessible 37
  stop replication 40
  system requirements 12

T
  test
    network 18
    overview 33
    recovery 33
    reset virtual machine after 34
schedule 33
successful 33

U
usage metering 17

V
vCloud Connector, tasks 7
vCloud Director, guest customization 33
virtual machine
data after recovery 37
Disaster Recovery leases 17
failback to source site 43
power on 17, 33, 38
recover 38
VMware Global Support Services 33
vSphere
Connect to a cloud provider wizard 18
test recovery 33
Web Client 10
vSphere Replication
documentation 7
download appliance 10
tasks 7, 11