VMware vCloud Air - Disaster Recovery User's Guide

vCloud Air

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

EN-001494-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

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

Contents

About this vCloud Air – Disaster Recovery User's Guide 5

1 The Disaster Recovery Service 7
- Overview of the Disaster Recovery Service 8
- Why Use Disaster Recovery in vCloud Air? 9
- About Setting up the Disaster Recovery Service 10
- Workflow for Using the Disaster Recovery Service 11
- System Requirements and Compatibility 12

2 Managing Disaster Recovery in vCloud Air 13
- Assign a User to the Roles for Disaster Recovery 14
- About Networks for the Disaster Recovery Service 15
- About Placeholders in vCloud Air 15
- Lease Times for Tests and Recoveries 17
- About Test Recoveries 17
- Test a Recovery 18
- Clean up a Test Recovery 18
- About Recovery to vCloud Air 19
- Recover a Virtual Machine 20
- Remove a Replication from vCloud Air 21
- About Failback for Virtual Machines to the Source Site 22

Index 23

About this vCloud Air – Disaster Recovery User's Guide

The *vCloud Air – Disaster Recovery User's Guide* provides information about vCloud Air – Disaster Recovery (formerly known as vCloud Hybrid Service – Disaster Recovery) from VMware®.

This guide provides information about using the Disaster Recovery service 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 the Disaster Recovery service and how to configure and manage it by using both the vSphere Web Client and vCloud Air.
- The second part of this guide explains how to perform the Disaster Recovery service 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 vCloud Air. This guide documents the capabilities and tasks that you do in vCloud Air.

Related Documentation

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

- vSphere Replication for Disaster Recovery to Cloud for information about using the vSphere Web Client to manage the Disaster Recovery service from your source site
- vCloud Air User's Guide for general information about managing your virtual machines in the cloud
- vCloud Air Networking Guide for general information about setting up networking for virtual machines in the cloud

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.

The Disaster Recovery Service 1

vCloud Air – Disaster Recovery is a Recovery-as-a-Service (RaaS) offering intended to protect virtual workloads managed by VMware vSphere that are either deployed in a private cloud or data center.

To implement and consume vCloud Air – Disaster Recovery, you require the following VMware products and services:

- vSphere Replication

  vSphere Replication is a feature of the VMware vSphere platform. vSphere Replication copies a virtual machine to another location, within or between clusters, and makes that copy available for recovery through the VMware vSphere Web Client or through the orchestration of a full disaster recovery product such as VMware vCenter Site Recovery Manager.

- vCloud Air

  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.

- vCloud Connector

  vCloud Connector provides support for initial data seeding and failback of workflows to your source site by using vCloud Connector Offline Data Transfer (ODT).

  NOTE If you are using vCloud Air – Disaster Recovery with access to failback capabilities via vSphere Replication, you can do reverse replication from a vCloud Air data center to your on-premises data center using the vSphere Replication Web Client. If not, you will need to copy virtual machines from vCloud Air to your on-premises data center using vCloud Connector ODT.

Although Disaster Recovery is based on the vCloud Air Subscription model, it is delivered on the Virtual Private Cloud OnDemand platform, which allows you to seamlessly scale your protection capacity to meet variable demands.

To be able to use all the features of Disaster Recovery, it is recommended that you upgrade to vSphere version 6.0. If you are running vSphere version 5.5 or earlier in your data center, you can still use Disaster Recovery to provide the failover capability for your virtual machines. However, you may not be able to use the latest Disaster Recovery features.

This user guide addresses configuration, setup, and management aspects of vCloud Air in support of the Disaster Recovery service.

For information about vSphere Replication, see the vSphere Replication 6.0 Disaster Recovery to Cloud documentation.

This chapter includes the following topics:

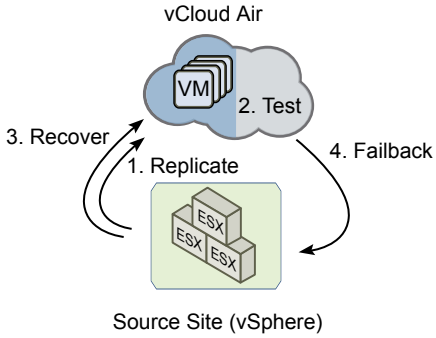
- "Overview of the Disaster Recovery Service," on page 8
- "Why Use Disaster Recovery in vCloud Air?," on page 9
- "About Setting up the Disaster Recovery Service," on page 10
- "Workflow for Using the Disaster Recovery Service," on page 11
- "System Requirements and Compatibility," on page 12

Overview of the Disaster Recovery Service

The Disaster Recovery service enables site administrators to protect their vSphere virtual workloads from a broad range of potential disruptions by asynchronously replicating those workloads from a source site to the cloud for recovery. The Disaster Recovery service uses vSphere Replication (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 the Disaster Recovery service.

Figure 1-1. Interaction Between vSphere Replication and vCloud Air



Features of the Disaster Recovery Service

The following key features provide the benefits of the Disaster Recovery service:

- Simple and secure (enterprise to cloud) asynchronous replication and recovery for virtual machines
- Self-service disaster recovery testing and recovery of workflows per virtual machine
- Guaranteed (warm standby) resource availability on the vCloud Air platform
- On-premises monitoring and management with the vSphere Web Client
- Flexible subscription options for elastic consumption
- Support for initial data seeding by using VMware vCloud Connector Offline Data Transfer (ODT)
- Native failback of workflows to your source site using vSphere Replication

  NOTE You need to use vSphere Replication version 6.0 or later.

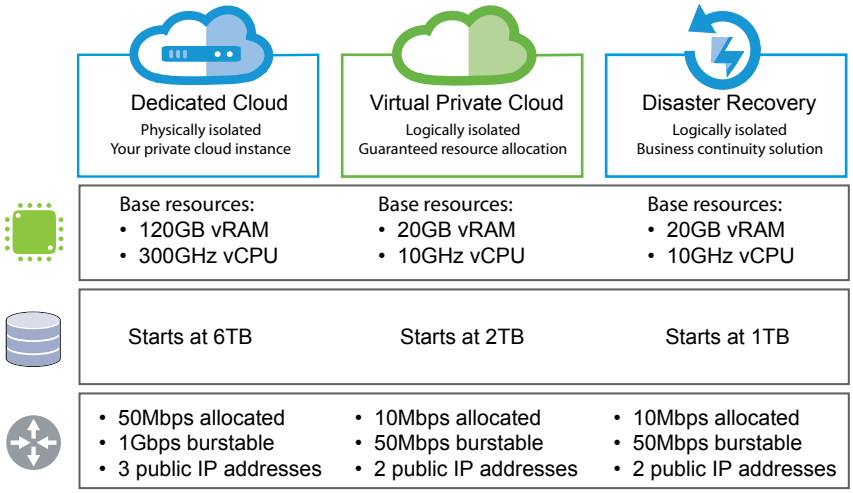
- Self-service RPO settings from 15 minutes to 24 hours per virtual machine

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

- Multiple point in time recovery snapshots
- Unlimited Disaster Recovery tests per year

You may buy the Disaster Recovery service in subscription term-lengths of 1 month, 3 months, 12 months, 24 months, up to 36 months. You can also buy and add resources (20GB vRAM, 10GHz vCPU and 1TB of storage) in bundles. The add-on options offered with the Disaster Recovery service are similar to the options provided with the vCloud Air core services.

Figure 1-2. vCloud Air Subscription Services

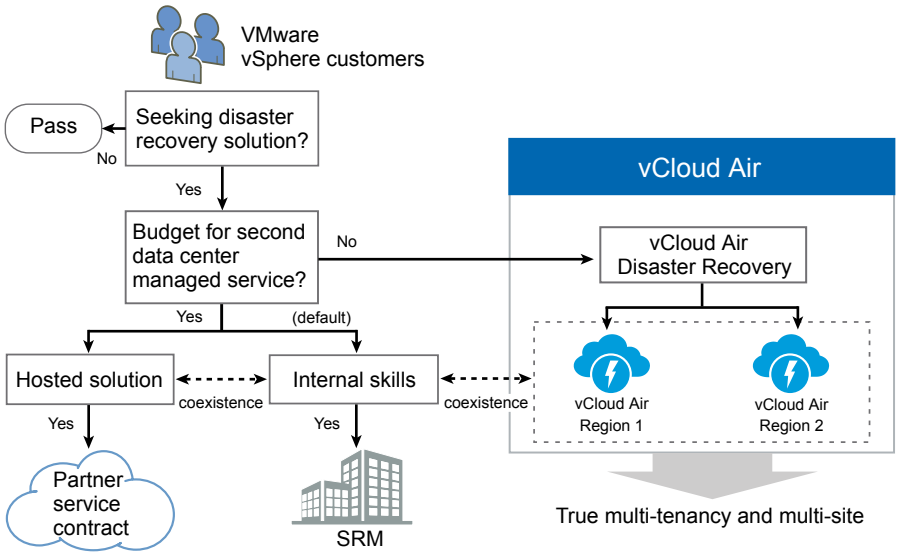


Why Use Disaster Recovery in vCloud Air?

There are 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 vCloud Air – Disaster Recovery is the perfect solution.

Figure 1-3. How do you decide?



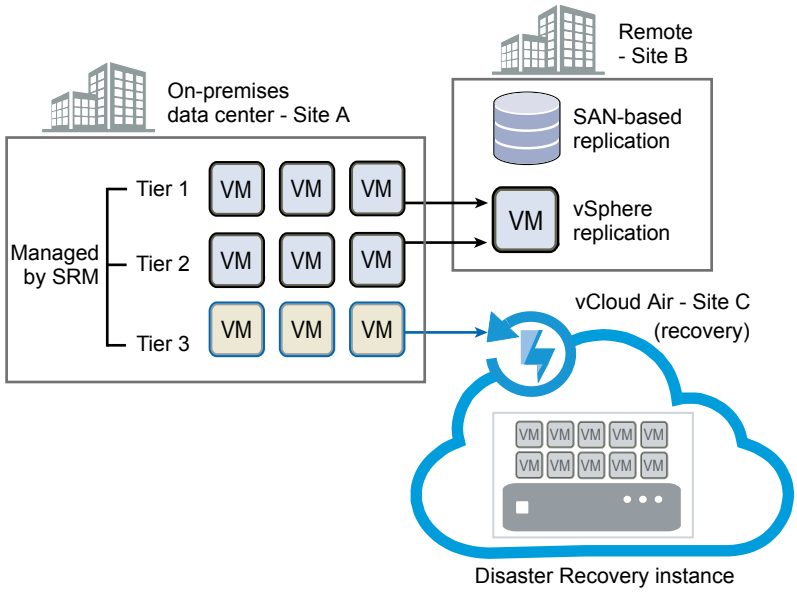
Using the Disaster Recovery service to replicate workloads from a source site to vCloud Air provides the following benefits:

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

- Affords organizations and IT operations groups of various sizes the opportunity to improve business resiliency and compliance standards based on cloud-scale economics.
- Allows for improved recovery point objective (RPO) and recovery time objective (RTO) policy compliance while reducing total cost of ownership (TCO).
- Introduces alternatives for migrating production applications to the cloud with reduced downtime and limited need for offline data transfers (ODT).
- Provides subscription-based Recovery-as-a-Service (RaaS) for vSphere customers and also provides support for different vSphere versions.
- Fully integrated vCenter Web Client
- Simple and easy to use management platform

In addition, the Site Recovery Manager (SRM) platform coexists with the vCloud Air – Disaster Recovery service, which provides the ability to protect Tier 1 or Tier 2 workloads with SAN-based replication. For Tier 3 workloads that do not need as much as critical RPO, you can protect those using vCloud Air, by leveraging the same vSphere Replication appliances, only replicating it out to vCloud Air – Disaster Recovery.

Figure 1-4. vCloud Air Disaster Recovery Co-exists with SRM



About Setting up the Disaster Recovery Service

Subscribing to the Disaster Recovery service is a standard enrollment process whether you already have a separate subscription with vCloud Air.

Prerequisites

Before setting up the Disaster Recovery service, you must meet the following prerequisites:

- You are a licensed vSphere customer running vSphere 5.6 or later (6.0 recommended) on-premises.

  See Disaster Recovery to Cloud System Requirements and Compatibility in *vSphere Replication 6.0 for Disaster Recovery to Cloud* for information.

- You have registered for a My VMware account.

Procedure

1 As a vSphere customer or vSphere and vCloud Air customer, contact your VMware sales representative to purchase a vCloud Air – Disaster Recovery subscription.

NOTE Once a subscription to the vCloud Air – Disaster Recovery service is submitted and approved, management of subscription options, such as feature add-ons, will become available in My VMware.

Similar to the Virtual Private Cloud and Dedicated Cloud services for vCloud Air, the Disaster Recovery service is a core service, which you cannot order directly through My VMware. Follow a standard purchase order process to subscribe to the Disaster Recovery 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 Disaster Recovery service in vCloud Air.

2 Log into My VMware and download the vSphere Replication 6.0 appliance.

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

3 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.

See Installing and Configuring vSphere Replication to Cloud in *vSphere Replication 6.0 for Disaster Recovery to Cloud* for information.

4 Using the vSphere Web Client at your source site, configure your connection to vCloud Air.

See Configuring the Connection to the Cloud in *vSphere Replication 6.0 for Disaster Recovery to Cloud* for information.

5 Log into vCloud Air to create user roles to manage your Disaster Recovery service.

See "Assign a User to the Roles for Disaster Recovery," on page 14 for information.

What to do next

See "Workflow for Using the Disaster Recovery Service," on page 11 for an overview of using vSphere Replication and vCloud Air to manage your Disaster Recovery service.

Workflow for Using the Disaster Recovery Service

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

1 Using vSphere Replication, replicate the virtual machines you plan to protect from your source site to vCloud Air.

NOTE You must initiate replication to the cloud by using vSphere Replication at your source site because replication between your source site and the cloud is not symmetrical, like it is when using VMware Site Recovery Manager. You can initiate replication to the cloud from your source site but, for security reasons, you cannot communicate with the virtual machines at your source site from the cloud.

See Replicating Virtual Machines to Cloud in *vSphere Replication 6.0 for Disaster Recovery to Cloud* for information about configuring and running vSphere Replication Disaster Recovery.

2 After replicating your virtual machines to the cloud, log into vCloud Air to view your virtual data center enabled for disaster recovery and the placeholder virtual machines that you selected for replication.

See "About Placeholders in vCloud Air," on page 15 for information.

3 Using vSphere Replication or vCloud Air, test recovery for a virtual machine and cleanup the test after you run it.

   See "Test a Recovery," on page 18 for information.

4 In the event that your source site becomes unavailable, log into vCloud Air and recover your virtual machines to vCloud Air.

   See "Recover a Virtual Machine," on page 20 for information.

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

System Requirements and Compatibility

To enable replications to vCloud Air - 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.

System Requirements

Replications to vCloud Air - 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. Once you are subscribed to the service, vCloud Air - Disaster Recovery ensures that the environment is configured for replications by providing a disaster recovery-enabled virtual data center (VDC).

Product Compatibility

You must verify that you run a supported version of the products on the source site. Please contact your VMware representative for more details.

VMware recommends the following product versions for this release of vCloud Air - Disaster Recovery:

Table 1-1. Recommended Product Versions

Product	Recommended Version
vSphere Replication appliance	6.0
vCenter Server	6.0
vSphere Web Client	6.0
ESXi host	5.0, 5.1.x, 5.5.x, and 6.0

NOTE You should also ensure that you have Internet connectivity without a proxy or traffic filtering device setup.

Managing Disaster Recovery in vCloud Air

2

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

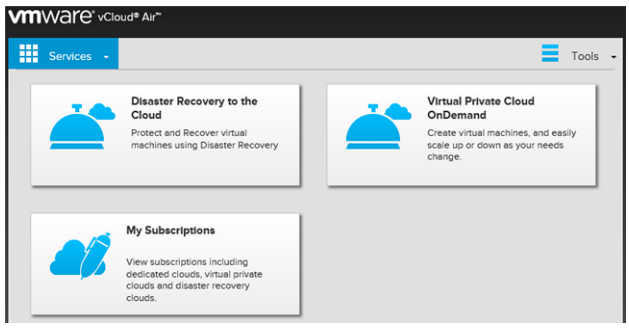
After setting up virtual machines for replication, use vCloud Air to monitor and manage the replication and recovery for those virtual machines; for example, testing recovery or performing a recovery from a placeholder virtual machine in vCloud Air in the event of a disruption at the source site.

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. You can access and operate your virtual machines recovered to the cloud for the following time periods:

- 7 days to access and operate virtual machines when performing tests
- 30 days to access and operate virtual machines when performing recovery

If you are an existing vCloud Air customer when you subscribed to the Disaster Recovery service, you will see the Disaster Recovery tile once you sign in.

Figure 2-1. vCloud Air Services



Clicking on the tile 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.

This chapter includes the following topics:

- "Assign a User to the Roles for Disaster Recovery," on page 14
- "About Networks for the Disaster Recovery Service," on page 15
- "About Placeholders in vCloud Air," on page 15
- "Lease Times for Tests and Recoveries," on page 17
- "About Test Recoveries," on page 17

- "Test a Recovery," on page 18
- "Clean up a Test Recovery," on page 18
- "About Recovery to vCloud Air," on page 19
- "Recover a Virtual Machine," on page 20
- "Remove a Replication from vCloud Air," on page 21
- "About Failback for Virtual Machines to the Source Site," on page 22

Assign a User to the Roles for Disaster Recovery

To use the Web UI for vCloud Air to manage the virtual machines you replicated to the cloud, you must have a user account in vCloud Air and be a member of an administrative role in vCloud Air.

A user in vCloud Air can either be an administrator or an end user. vCloud Air groups administrator privileges in to specific administrator roles. An account administrator can assign a user to one or more of the administrator roles.

Prerequisites

Before assigning a user to an administrative role to access the Disaster Recovery service, you must meet the following prerequisites:

- You have subscribed to the Disaster Recovery service and received the email explaining how to log into vCloud Air for the first time.
- You are assigned to the Account Administrator role in vCloud Air so that you can assign users to roles.
- You have created the user account to which you want to add Disaster Recovery permissions.

  See Add Users in the *vCloud Air User's Guide* for information.

Procedure

1. Click **Tools > Users** in the top right corner of vCloud Air.
2. Select the user for whom you want to grant permissions to the Disaster Recovery service.
3. You can assign any of the following roles to the user's account:

Choose this option:	To grant these permissions:
Account Administrator	Access to all resources, operations and user managementt - add users and reset passwords, and view virtual data centers, virtual machines, and activity logs
Virtual Infrastructure Administrator	Manage assigned virtual data centers, and replications and recovered virtual machines contained within
Network Administrator	Manage networks and gateways of assigned virtual data centers
Read-Only Administrator	View assigned virtual data centers, virtual machines, gateways, networks, activity logs, and users
End User	Manage virtual machines in the assigned virtual data centers

4. You can add a new user by clicking **Add User**, and **View**, **Edit**, or **Reset Password** of existing users.
5. From the **More** drop-down menu, you can **Enable, Disable** or **Delete** a user from the existing list.

About Networks for the Disaster Recovery Service

When you subscribe to the Disaster Recovery service, 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 networkon the inside interface is accessible through the Intranet. You can use these networks for your virtual machines protected by the Disaster Recovery service.

When you configure Disaster Recovery in vSphere Replication by using the **Connect to a cloud provider** wizard, 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 6.0 for Disaster Recovery to Cloud* for information.

You can choose to use the vCloud Air default networks for the 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 the vSphere Web Client, see Select Recovery Networks on the Target Virtual Data Center in *vSphere Replication 6.0 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.

See "Test a Recovery," on page 18 and "Recover a Virtual Machine," on page 20 for information.

About Placeholders in vCloud Air

When you configure replication by using vSphere Replication at your source site, the Disaster Recovery service 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 vCloud Air for a virtual data center enabled for disaster recovery:

- The **Replication** 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 the Disaster Recovery service and to view the status of your replications. The **Cloud provider address** and **Organization Name** required while configuring the vSphere Replication 6.0 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, the Disaster Recovery service replaces the placeholder with a test or production virtual machine respectively.

About the Replication of Placeholders

vCloud Air displays the following information about virtual machine replication.

Figure 2-2. Placeholders in the Replication Tab

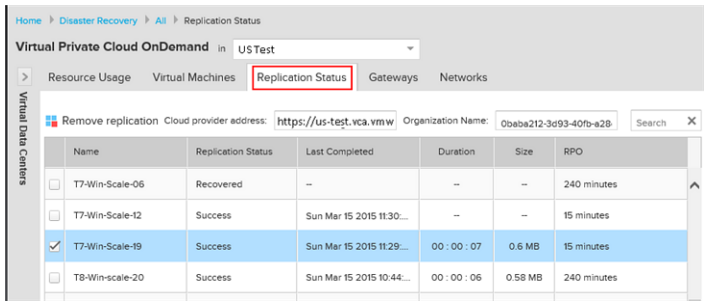


Table 2-1. Replication Information Displayed for Each Placeholder

Column	Description
Name	The name of the placeholder virtual machine
Replication Status	The current status of the replication
Last Completed	Last synchronization completed; displayed using the local time of the browser time zone
Duration	The length of time the last synchronization took
Size	The size of the last data replicated (not the size of the virtual machine)
RPO	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. NOTE Lower RPO times reduce potential data loss but use more bandwidth and system resources. By default, the vSphere Web Client sets 4 hours as the RPO value.

Table 2-2. About the Replication Status Values

Replication Status	Description
Configuring	Virtual machine configuration is in progress.
Full Sync	Full synchronization is in progress.
Initial Full Sync	Initial full synchronization is in progress. This status only appears for the first initial synchronization when the virtual machine is added to the system.
Not Active	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.
OK	The replication is configured correctly—no configuration or replication errors are present. However, the Disaster Recovery service has not sent replication traffic to the cloud.
Paused	The replication is not running because a vSphere Replication user paused the replication. See Pause or Resume a Replication Task in *vSphere Replication 6.0 for Disaster Recovery to Cloud* for information.
Recovered	The Disaster Recovery service recovered the virtual machine to the cloud successfully.
Recovering	The Disaster Recovery service is recovering the virtual machine to the cloud.
Sync	The virtual machine data at the source site is synchronizing with the placeholder virtual machine in vCloud Air.

See Monitoring the Status of Replication Tasks in *vSphere Replication 6.0 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.

Lease Times for Tests and Recoveries

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

To view the lease times for a test or recovered virtual machine in vCloud Air, go to the virtual data center enabled for disaster recovery > **Virtual Machine** tab > **Recovery Time** column.

The **Recovery Time** column shows the time since a test or recovery; displayed using the local time of the browser time zone.

About Test Recoveries

Although you can initiate tests from the vSphere Web Client at your source site or from the vCloud Air Web UI, most often you will initiate tests from the vSphere Web Client at your source site.

However, initiating tests from vCloud Air is necessary when your source site is unavailable and you want to run a final test before executing disaster recovery.

The following conditions apply to testing recoveries:

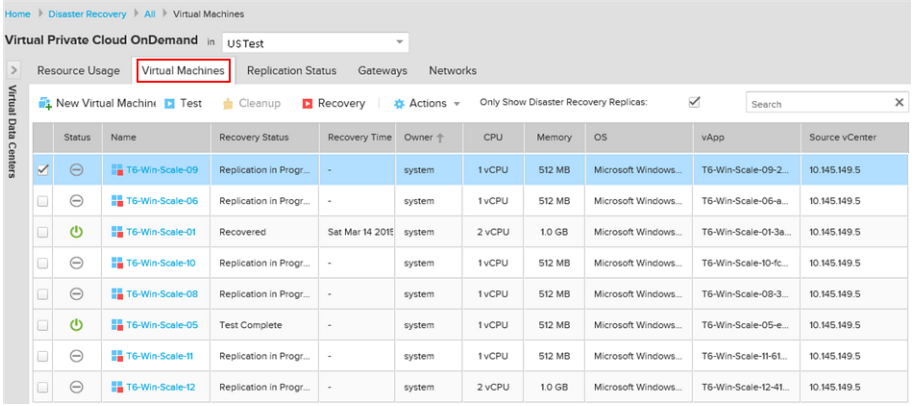
- When you invoke a test from your source site, you have the option to synchronize data between the source site and the cloud before creating the test recovery. This option is not available when initiating a test from vCloud Air.
- Initiating a test from the cloud creates a test recovery using replicated virtual machine data, re-configures 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 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 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," on page 18.

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

Figure 2-3. Virtual Machines Tab in vCloud Air



For information about testing a recovery by using the vSphere Web Client at your source site, see Test Recovery to Cloud in *vSphere Replication 6.0 for Disaster Recovery to Cloud* for information.

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 the Disaster Recovery Service," on page 15 for information.

- You have the correct user permissions to perform the test.

  See "Assign a User to the Roles for Disaster Recovery," on page 14 for information.

Procedure

1. Click the **Virtual Machine** tab.

   The table of virtual machines appears.

2. Select the virtual machine placeholder you want to test.
3. Click **Test**.

   A confirmation dialog box appears.

4. Click **Continue**.

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.

A successful test powers on the virtual machine. In the Virtual Machines table, the Recovery Status changes from Placeholder to Test Complete.

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.

For information about cleaning up a test recovery by using the vSphere Web Client, see Clean Up a Test Recovery in *vSphere Replication 6.0 for Disaster Recovery to Cloud*.

Prerequisites

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

  See "Assign a User to the Roles for Disaster Recovery," on page 14 for information.

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 vCloud Air

Run this workflow to recover your production virtual machines from your 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.

For information about recovering virtual machines to the cloud by using planned migration, see What Happens During a Planned Migration in *vSphere Replication 6.0 for Disaster Recovery to Cloud*.

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.

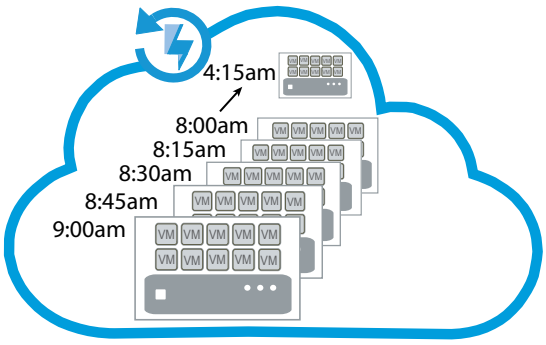
Recovering a virtual machine to vCloud Air stops replication from the source site.

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:

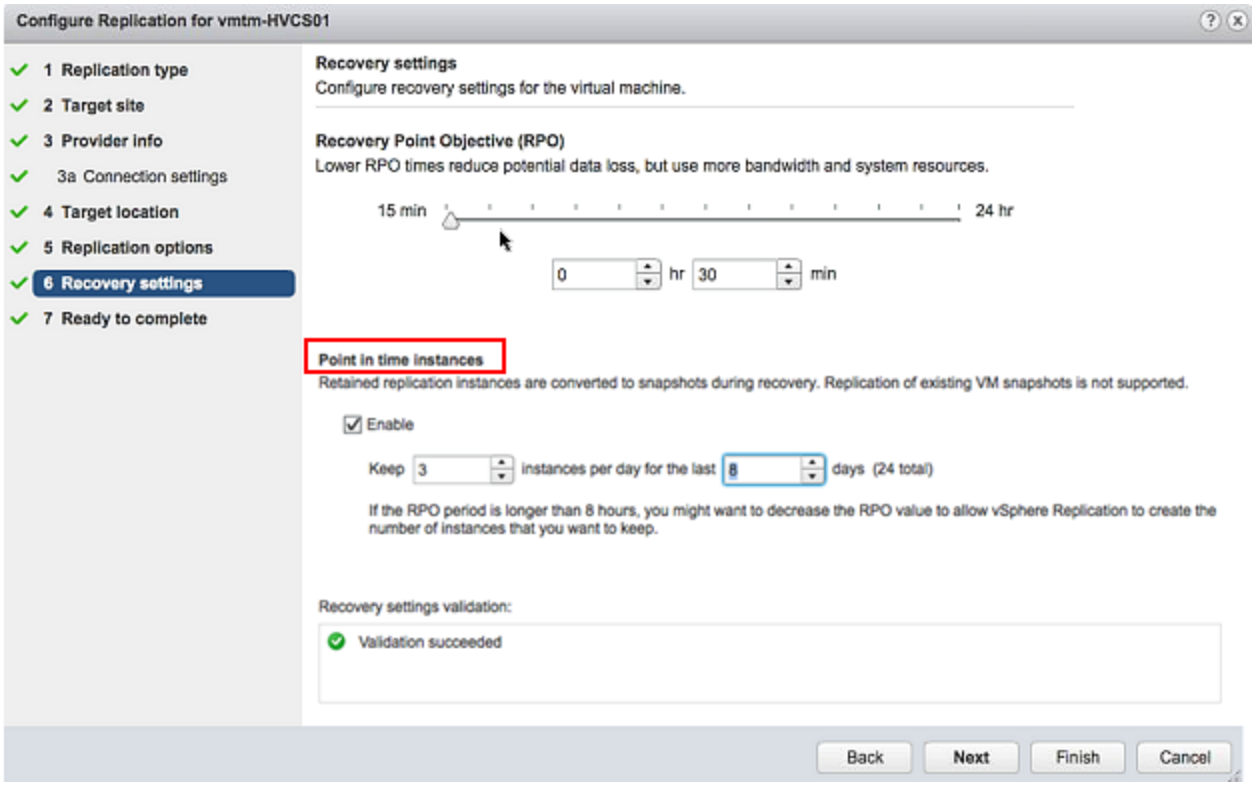
- Set up to 24 previous restore points
- Choose your restore point
- Restore up to 24 days previous replication points (dependent on your RPO setting)

Figure 2-4. 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 a Replication to Cloud for a Single Virtual Machine in *vSphere Replication 6.0 for Disaster Recovery to Cloud* for information about configuring replication to the cloud.

Figure 2-5. Configure Replication - Set MPIT



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 failback 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.

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.

Prerequisites

You have the correct user permissions to recover the virtual machine to the cloud. See "Assign a User to the Roles for Disaster Recovery," on page 14 for information.

If possible, meet these prerequisites:

- Verify that you tested the recovery before recovering the virtual machine to the cloud.
- Verify that you cannot run a planned migration from your source site.

  See Migrate a Virtual Machine to Cloud in *vSphere Replication 6.0 for Disaster Recovery to Cloud* for information about planned migration from your source site.
- Contact VMware Global Support Services and declare a disaster prior to recovering your virtual machines.

Procedure

1 Click the **Virtual Machine** tab.

The table of virtual machines appears.

2 Select the virtual machine that you want to recover.

3 Click **Recovery**.

The confirmation dialog box appears.

4 Click **Continue.**

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 production network.
- 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 "Lease Times for Tests and Recoveries," on page 17.

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 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.

See "Assign a User to the Roles for Disaster Recovery," on page 14 for information.

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.

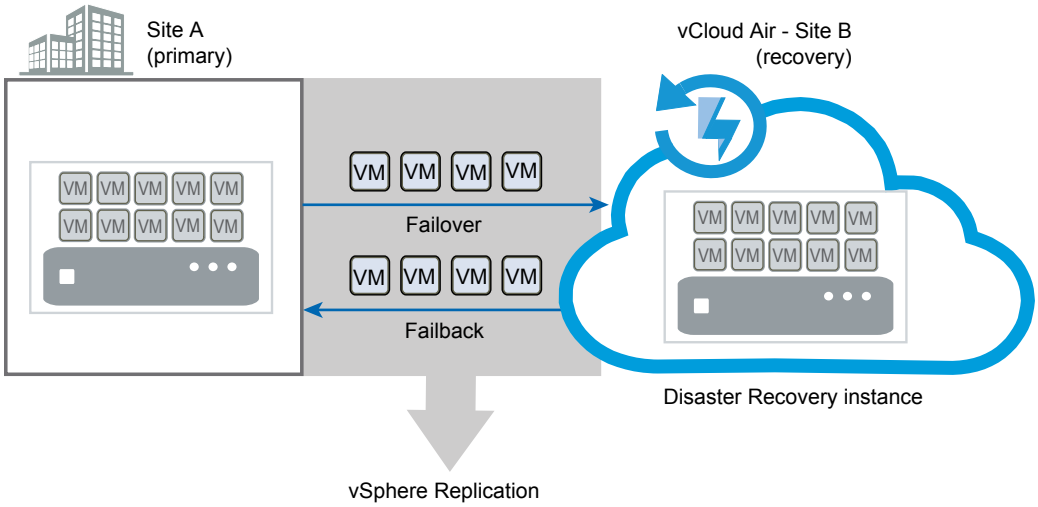
About Failback for Virtual Machines to the Source Site

Native failback of virtual machines that you have previously recovered in vCloud Air is available by using vSphere Replication.

After successfully recovering your replicated virtual machines in vCloud Air, you can failback those virtual machines. In the vSphere Replication, you can configure reverse replication, which repoints the replication of the virtual machines back to your on-premises vSphere environment. In the event of a disaster you would failover all your virtual machines from your on-premises data center to the vCloud Air Disaster Recovery cloud. Once you have restored on-premises data center, native failback provides you with the ability to restore your service from the cloud back to your on-premises data center.

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

Figure 2-6. vCloud Air Disaster Recovery with Native Failback



For information about using vSphere Replication Web Client to configure replication to and from (reverse) the cloud, see Configuring Replication from Cloud in *vSphere Replication 6.0 for Disaster Recovery to Cloud* documentation.

Index

A
access, Disaster Recovery **14**

C
clean up
  results **18**
  test recovery **18**
compatibility **12**

D
data seeding **8**
Disaster Recovery
  default networks **15**
  features **8**
  login credentials **10**
  prerequisites **10, 14**
  related documentation **5**
  required VMware products **8**
  setup **10**
  task workflow **11**
  usage metering **13**
DR-VDC, vCloud Air Dashboard **13**

F
failback, vSphere Replication **22**

G
guest customizations, test recovery **17**

I
intended audience **5**

M
migrate, virtual machine to cloud **20**
My VMware, Disaster Recovery subscription **10**

N
network
  customization **13**
  production **20**
networks, Disaster Recovery **15**

O
offline data transfer, Disaster Recovery
  feature **8**

P
permissions, Disaster Recovery **14**
placeholder
  cleanup test **18**
  integrity test **18**
  overview **15**
  status **15**
  virtual machine settings for **13**
planned migration, source site **20**
prerequisites, Disaster Recovery **14**
product compatibility **12**
production network **15**

R
recovery
  network **15**
  overview **19**
  results **20**
  source site unavailable **20**
  test **18**
  time periods to access **13**
Recovery Time column **17**
replication
  image size **15**
  manage **13**
  remove **21**
  source site **11**
  status values **15**
  tab overview **15**
requirements **12**
RPO
  feature **8**
  times **15**
  violation **15**

S
Site Recovery Manager **11**
source site
  clean up test **18**
  connectivity loss **15**
  failback virtual machine **22**
  planned migration **20**
  unaccessible **19**
stop replication **21**
system requirements **12**

T

test
- network **15**
- overview **17**
- recovery **18**
- reset virtual machine after **18**
- schedule **17**
- successful **17**

U

usage metering **13**

V

vCloud Connector, tasks **7**
vCloud Director, guest customization **17**
virtual machine
- data after recovery **19**
- Disaster Recovery leases **17**
- failback to source site **22**
- power on **17, 20**
- recover **20**

VMware Global Support Services **17**
vSphere
- Connect to a cloud provider wizard **15**
- OVF Deployment wizard **10**
- test recovery **17**
- Web Client **10**

vSphere Replication
- documentation **7**
- download appliance **10**
- tasks **7, 11**