

Using vCloud Availability

VMware vCloud Availability 3.5



vmware®

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

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

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

docfeedback@vmware.com

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

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

Contents

1	Using VMware vCloud Availability	5
2	Accessing vCloud Availability	6
	Accessing the vCloud Availability Portal as a Tenant	6
	Log In to the vCloud Availability Portal as a Tenant	6
	Log In by Using the VMware vCloud Director Tenant Portal	6
	Accessing the vCloud Availability Portal as a Service Provider	7
	Log In to the vCloud Availability Portal as a Service Provider	7
	Log In by Using the VMware vCloud Director Service Provider Admin Portal	7
	Access the vCloud Availability vSphere Client Plug-In	8
3	Configuring Replication Policies	10
	Create a Replication Policy	11
	Assign a Replication Policy to Organizations	12
	Edit a Replication Policy	12
	Delete a Replication Policy	13
	Replication Policy Conflicts	13
	Check for Replication Policy Conflicts	14
	Synchronize vCloud Availability With vCloud Director	14
	Review Replication Policy Assignments	15
4	Using Replications	16
	Grouping VMs in a vApp Replication	18
	Group VMs in a vApp Replication	18
	Modify the Settings of Grouped VMs	19
	Selecting Replicated Disks	20
	Select Replicated Disks	21
	Using Replication Seeds	22
	Export a Virtual Machine or a vApp to a Removable Media	23
	Importing a Virtual Machine from a Removable Media	23
	Configure a Replication by Using a Replication Seed	24
	Create a Migration	26
	Create a Protection	27
	Configuring Network Settings of Replications to the Cloud	28
	Configure the Network Settings of On-Premises to Cloud Replications	29
	Modify the Network Settings of Cloud to Cloud Replications	31
5	Performing vCloud Availability Workflows	33

[Authenticating to Remote Sites](#) 34

[Authenticate to Remote Sites as a Tenant](#) 34

[Authenticate to Remote Sites as a Service Provider](#) 34

[Test Failover](#) 35

[Perform a Failover Task](#) 36

[Perform a Reverse Task](#) 37

6 Monitoring the Traffic Usage 39

[Monitor Tenant Traffic](#) 40

[Monitor and Export Organization Traffic Usage as a Service Provider](#) 40

[Monitor the Traffic of a Virtual Machine Replication](#) 41

7 Bandwidth Throttling 43

[Configure Bandwidth Throttling](#) 43

Using VMware vCloud Availability

1

vCloud Availability offers simple and secure onboarding, migration, and disaster recovery services. Migrate and protect vSphere workloads: from on-premises sites to a multi-tenant cloud site and the reverse, and between cloud sites.

- After a tenant onboards with a cloud provider, the vCloud Availability On-Premises Appliance is paired with the cloud site. vSphere workloads like vApps and virtual machines can be migrated or protected to and from that cloud site.
- After pairing a cloud site with another cloud site, the vSphere workloads can be migrated or protected between the cloud sites.
- When vCloud Availability is paired with another site, tenants and service providers can:
 - Replicate vSphere workloads to that site. After replicating the workload, when using a protection - the workload in the source site keeps staying active. When using a migration - the workload in the destination site becomes active.
 - Perform disaster recovery workflows like test failover, failover, and reverse tasks on the replicated vSphere workloads.
- Tenants and service providers can manage replications and perform workflows in the vCloud Availability Portal or in vCloud Director. Tenants can also use the vCloud Availability vSphere Client Plug-In.
- Replication policies can be set per-tenant or per-organization. The replication policies disallow or allow the incoming or the outgoing replications. The policies also control the maximum number of virtual machines, the maximum number of retained instances per replication and the minimum Recovery Point Objective (RPO).

Accessing vCloud Availability

2

Access the vCloud Availability Portal dedicated to service providers or to tenants. Alternatively, in vCloud Director you can access the Service Provider Admin Portal or the tenant portal. For on-premises to cloud replications and the reverse, use the vCloud Availability vSphere Client Plug-In.

This chapter includes the following topics:

- [Accessing the vCloud Availability Portal as a Tenant](#)
- [Accessing the vCloud Availability Portal as a Service Provider](#)
- [Access the vCloud Availability vSphere Client Plug-In](#)

Accessing the vCloud Availability Portal as a Tenant

Tenant users can log in to the vCloud Availability Portal by using the user interface in the vCloud Availability vApp Replication Manager appliance, or by using the vCloud Director tenant portal.

Log In to the vCloud Availability Portal as a Tenant

Tenants can log in to the vCloud Availability Portal to operate workloads enabled for replications from VMware vCloud Director sites.

Prerequisites

Verify that your vCloud Director tenant user profile has **Organization Administrator** privileges.

Procedure

- 1 In a Web Browser, go to the vCloud Availability Portal at **`https://Public-API-Endpoint/ui/login`**.
- 2 Enter your **Organization Administrator** user name as **`username@Org-Name`**, enter the password, and click **Login**.

Log In by Using the VMware vCloud Director Tenant Portal

During the initial vCloud Availability configuration, vCloud Availability registers as a VMware vCloud Director plug-in and provides access to the vCloud Availability Portal directly from the vCloud Director tenant portal.

When you access the vCloud Availability Portal from the vCloud Director tenant portal, you can manage cloud and disaster recovery environments from a single user interface which simplifies the management operations.

Prerequisites

- Verify that your vCloud Availability environment is running VMware vCloud Director 9.1 or later.
- Verify that your vCloud Director tenant user profile has **Organization Administrator** privileges.

Procedure

- 1 In a Web browser, go to your organization tenant portal URL at <https://vcloud.example.com/tenant/Organization-Name>.
- 2 Log in with a vCloud Director **Organization Administrator** user.
- 3 Open the vCloud Availability Portal, by selecting **Availability** from the main menu.

Accessing the vCloud Availability Portal as a Service Provider

Service providers can log in to the vCloud Availability Portal by using the user interface in the vCloud Availability vApp Replication Manager appliance, or by using the vCloud Director Service Provider Admin Portal.

Log In to the vCloud Availability Portal as a Service Provider

Service providers can log in to the vCloud Availability Portal to view and manage the information on DR workloads from the vCloud Director sites, monitor services health status, and administer vCloud Availability.

Prerequisites

Verify that the user profile has **System Administrator** privileges.

Procedure

- 1 In a Web browser, go to the vCloud Availability Portal at <https://vApp-Replication-Manager-IP-address/ui/login>.
- 2 Enter the **System Administrator** user name as *providerusername@system*, enter the password, and click **Login**.

Log In by Using the VMware vCloud Director Service Provider Admin Portal

During the initial vCloud Availability configuration, vCloud Availability registers as a VMware vCloud Director plug-in and provides access to the vCloud Availability Portal directly from the vCloud Director Service Provider Admin Portal.

When you access the vCloud Availability Portal from the vCloud Director Service Provider Admin Portal, you can manage cloud and disaster recovery environments from a single user interface. The first time you access the vCloud Availability Portal from the vCloud Director Service Provider Admin Portal, you must trust the SSL certificate of the vCloud Availability vApp Replication Manager appliance as described in [Step Step 5](#).

Prerequisites

- Verify that your vCloud Availability environment is running vCloud Director 9.1 or later.
- Verify that the user profile has **System Administrator** privileges.

Procedure

- 1 In a Web browser, go to the organization service provider portal URL at **`https://vcloud.example.com/provider/login`**.
- 2 Log in with a vCloud Director **System Administrator** user.
- 3 From the main menu, select **Availability**.

You see the The service at `https://vApp-Replication-Manager-IP-Address:8443` is currently unavailable. Try again later and if the problem persists, contact your cloud provider. message.

- 4 Click the `https://vApp-Replication-Manager-IP-Address:8443` link.

A new tab opens in your Web browser.

- 5 Trust the SSL certificate of the vCloud Availability vApp Replication Manager appliance, by clicking **Accept**.

You must trust the SSL certificate of the vCloud Availability vApp Replication Manager appliance only when you use vCloud Director Service Provider Admin Portal to access the vCloud Availability Portal for the first time. After you trust the certificate, by selecting **Availability** from the vCloud Director Service Provider Admin Portal main menu opens the vCloud Availability Portal.

Access the vCloud Availability vSphere Client Plug-In

Create and manage on-premises to cloud and cloud to on-premises replications in the vCloud Availability vSphere Client Plug-In. Also, you can configure, perform system monitoring, and maintenance of the vCloud Availability On-Premises Appliance.

The vCloud Availability vSphere Client Plug-In is registered during the initial configuration of the vCloud Availability On-Premises Appliance. Use the vCloud Availability vSphere Client Plug-In to monitor and operate with incoming and outgoing replications and perform appliance management tasks.

Prerequisites

Verify that the vCenter Server version is 6.5 Update 3 or later. For vCenter Server 6.5 Update 2 or older, see [Accessing the vCloud Availability Portal as a Tenant](#).

Procedure

- 1 Log in to the vSphere Client as a vCenter Server **Administrator**.
- 2 You can access the vCloud Availability vSphere Client Plug-In:
 - In the top header, click **Menu > vCloud Availability**.
 - In the **Navigator** pane, click **vCloud Availability**.
- 3 On the **vCloud Availability** page, click the following tabs.

Option	Description
Getting Started	Choose a cloud provider, download the OVA template, and register the vCloud Availability On-Premises Appliance with vSphere.
Dashboard	See the status of the incoming and outgoing replications, recent tasks, and a traffic report chart.
Outgoing Replications	Operate with the vApps and virtual machines that are replicated from the on premises site to the cloud site. See the replication type: protection or migration, the RPO, the destination data center. See the replication state, the recovery state, the replication health, and the last modification timestamp.
Incoming Replications	Operate with the vApps and virtual machines that are replicated from the cloud site to the on-premises site. See the replication type: protection or migration, the RPO, the source data center. See the replication state, the recovery state, the replication health, and the last modification timestamp.
Replication Tasks	See the replication task name, target, start, and end time or progress. Filter the tasks by running, succeeded, or failed status in the on-premises site.
Configuration	See and modify the on-premises site details, the cloud site pairing, the VM placement, the vCenter Server Lookup service address. You can modify the settings of the vCloud Availability On-Premises Appliance: root password, network, certificate, time, logging level, and SSH access. See the version, check for upgrades and modify the repository for upgrades.
System Monitoring	See the health status of the services, the manager, and the cloud site. You can restart the services or the vCloud Availability On-Premises Appliance.
System Tasks	See the system task name, target, start, and end time or progress. Filter the tasks by running, succeeded, or failed status in the on-premises site.
Support	See, generate, download, and delete support bundle archive packages.
About	See the vCloud Availability version and build details and access the online documentation.

Configuring Replication Policies

3

Replication policies are sets of rules that define and control the replication attributes on a vCloud Director organization level.

Replication Attributes Enforced by Replication Policies

You can assign a single replication policy to multiple vCloud Director organizations to control the following attributes of a replication:

- Whether an organization can be used as a replication source.
- Whether an organization can be used as a replication destination.
- The minimum Recovery Point Objective (RPO) for an organization.
- The maximum number of retained snapshots per single virtual machine replication for an organization.
- The maximum number of virtual machine replications that can be created for an organization.

Default Replication Policy

The default replication policy applies to organizations that you did not associate with a custom replication policy. You might use only the default replication policy and to enable replication, edit the default replication policy attributes.

Table 3-1. Default Replication Policy Attributes

Setting	Default Value
Outgoing replications	Not allowed
Incoming replications	Not allowed
Maximum number of virtual machine replications	0
Maximum retained instances per replication	24
Minimum allowed RPO	15 min

New Replication Validation

When you create a protection or a migration, the **New Replication** wizard validates the replication attributes of the policy that is assigned to the organization.

- Whether the source organization allows outgoing replications.
- Whether the destination organization allows incoming replications.
- Whether on the destination organization you are not exceeding the total number of allowed virtual machine replications, that includes both incoming from on-premises and cloud replications.
- Whether the number of retained instances per replication of the new replication complies with the policy that is assigned to the destination organization.
- Whether the RPO of the new replication is higher than or equal to the minimum RPO of the policy that is assigned to the destination organization.

If any of the replication attributes is violated, you cannot create the replication.

This chapter includes the following topics:

- [Create a Replication Policy](#)
- [Assign a Replication Policy to Organizations](#)
- [Edit a Replication Policy](#)
- [Delete a Replication Policy](#)
- [Replication Policy Conflicts](#)
- [Synchronize vCloud Availability With vCloud Director](#)
- [Review Replication Policy Assignments](#)

Create a Replication Policy

To control the replication settings allowed for replications on a VMware vCloud Director organization level, you create a replication policy.

Procedure

- 1 Log in to the vCloud Availability Portal by using **System administrator** credentials.
- 2 In the left pane, click **Policies**.
- 3 On the **Policies** page, click **New**.
- 4 In the **New Policy** window, configure the replication attributes, and click **Create**.
 - a Enter a unique, case-sensitive name for the replication policy.
 - b Select whether to allow incoming and outgoing replications.
 - c Enter the maximum number of virtual machines replications.

- d Enter the maximum number of retained instances per replication.
- e Set minimum allowed RPO by using the **Recovery Point Objective (RPO)** slider or by clicking the time ranges.

Results

You created the replication policy and it shows on the **Policies** page.

What to do next

You can assign the new policy to a VMware vCloud Director organization. For more information, see [Assign a Replication Policy to Organizations](#).

Assign a Replication Policy to Organizations

To control the replication settings of vCloud Director organizations, you assign a replication policy to the organizations.

If you do not assign a custom policy to an organization, the default replication policy is assigned to the organization.

Procedure

- 1 Log in to the vCloud Availability Portal by using **System administrator** credentials.
- 2 In the left pane, click **Policies**.
- 3 On the **Policies** page, select a replication policy and click **Assign**.
- 4 In the **Assign Policy** window, to assign the policy to one or more organizations select them, and click **Assign**.

Results

You assigned the policy to the selected vCloud Director organizations.

If there are conflicts between the assigned replication policy and the existing replications, you must first resolve the conflicts. For more information, see [Replication Policy Conflicts](#).

Edit a Replication Policy

You can edit an existing replication policy to change the replication settings of VMware vCloud Director organizations.

Procedure

- 1 Log in to the vCloud Availability Portal by using **System administrator** credentials.
- 2 In the left pane, click **Policies**.
- 3 On the Policies page, select a replication policy and click **Edit**.

- 4 In the **Edit Policy** window, edit the replication policy settings and click **Apply**.
 - a Enter a unique, case-sensitive name for the replication policy.
 - b Select whether to allow incoming and outgoing replications.
 - c Enter the maximum number of virtual machines replications.
 - d Enter the maximum number of retained instances per replication.
 - e Set minimum allowed RPO by using the **Recovery Point Objective (RPO)** slider or by clicking the time ranges.

Results

You reconfigured the replication policy and all new replications belonging to organizations to which the policy is assigned must comply with the new replication policy settings.

If there are conflicts between the edited replication policy and the existing replications, you must resolve the conflicts. For more information, see [Replication Policy Conflicts](#).

Delete a Replication Policy

If you do not need a replication policy, you can delete it.

Prerequisites

Ensure that the replication policy you are removing is not assigned to any organization. You cannot delete a replication policy that is associated with an organization.

Procedure

- 1 Log in to the vCloud Availability Portal by using **System administrator** credentials.
- 2 In the left pane, click **Policies**.
- 3 On the **Policies** page, select the replication policy and click **Delete**.
- 4 In the **Delete Policy** dialog box, to confirm the deletion click **Delete**.

Results

You removed the replication policy.

Replication Policy Conflicts

Assigning a replication policy to an organization or modifying an existing replication policy assigned to an organization, can result in conflicts.

When you assign a replication policy to an organization or modify an existing replication policy that is already assigned, all new replications in the organization must adhere to the new replication policy attributes. The replication policy modification does not affect existing replications in the organization and can cause replication policy conflicts. See [Check for Replication Policy Conflicts](#).

Resolving Replication Policy Conflicts

You can manually resolve replication conflicts that a replication policy shows, by modifying the replication policy or by modifying all replications that conflict the replication policy.

- Reconfigure the replication policy attributes that the replications are violating.
- Reconfigure the replication settings of all replications that violate the policy. You can also, stop, pause, migrate, or failover the conflicting replications.

Check for Replication Policy Conflicts

Discover replication policy conflicts by using the vCloud Availability Portal.

Procedure

- 1 Log in to the vCloud Availability Portal by using **System administrator** credentials.
- 2 In the left pane, click **Policies**.
- 3 On the **Policies** page, select a replication policy.

Results

On the **Policies** page, the **Compliance status** table shows with a list of all organizations to which the selected policy is assigned and the number of configured replications for each organization.

In the last three columns in the **Compliance status** table, you can see the number of replication policy conflicts, listed as:

- Number of incoming replications exceeding the selected policy quota
- Number of incoming replications violating the minimum allowed RPO
- Number of incoming replications retaining more instances than the policy limit

Synchronize vCloud Availability With vCloud Director

By default, vCloud Availability automatically synchronizes VMware vCloud Director organizations information every hour. You can initiate a manual synchronization between vCloud Availability and VMware vCloud Director, and reflect recent vCloud Director organization modifications.

Procedure

- 1 Log in to the vCloud Availability Portal by using **System administrator** credentials.
- 2 In the left pane, click **Policies**.

3 (Optional) Manually synchronize vCloud Availability with vCloud Director, by clicking **Sync with Cloud**.

The manual synchronization between vCloud Availability and vCloud Director performs the following actions.

- The default replication policy automatically assigns to newly created vCloud Director organizations.
- vCloud Availability cleans up leftover mappings for recently deleted vCloud Director organizations.

If you recently created a vCloud Director organization and auto synchronization did not occur, the new organization is not assigned automatically to the default replication policy. If you configure an incoming or an outgoing replication for a vApp in the newly created organization, vCloud Availability treats the organization as if the default replication policy is assigned.

Review Replication Policy Assignments

To review the assigned replication policies to all VMware vCloud Director organizations, you use the Organizations tab in the vCloud Availability Portal.

Procedure

- 1** Log in to the vCloud Availability Portal by using **System administrator** credentials.
- 2** In the left pane, click **Policies**.
- 3** On the **Policies** page, click the **Organizations** tab.

Results

A list of all VMware vCloud Director organizations and their assigned replication policy shows.

Using Replications

4

In the vCloud Availability Portal or in the vCloud Availability vSphere Client Plug-In, you can protect or migrate workloads by replicating vApps or virtual machines.

Protect or migrate vApps and virtual machines by replicating them from one site to another.

Replication Types

- Protecting a vApp or a virtual machine from one organization to another keeps the workload running in the source site.
- Migrating a vApp or a virtual machine to a remote organization runs the workload in the destination site.

Recovery Point Objective - RPO

The RPO is the longest tolerable timeframe of data loss. For example, with one hour RPO the recovered virtual machine can have no more than one hour of data lost. Shorter RPO intervals, ensure less data loss during recovery, at the expense of consuming more network bandwidth to keep the replica up to date. For more information on the RPO setting, see [How the Recovery Point Objective Affects Replication Scheduling](#) in the *VMware vSphere Replication Administration* documentation.

When each virtual machine reaches its RPO target, the vCloud Availability Replicator writes about 3800 bytes in the vCenter Server events database. Low RPO values, increase the volume of event data in the database. You can limit the number of days that vCenter Server retains event data, or set a higher RPO value to reduce the volume of event data.

Note For a migration, the RPO is 24 hours by default.

Quiescing

vCloud Availability Replicator guarantees a crash consistency among all disks in a virtual machine. If you use quiescing, you might obtain a higher level of crash consistency among the disks that belong to a virtual machine. The operating system of a virtual machine determines the available quiescing types. Quiescing is available only for virtual machine operating systems that support quiescing. For more information, see [Guest OS Quiescing Support](#) in the vSphere Replication documentation.

Replicated Workload Settings

vCloud Availability preserves and periodically synchronizes the vCloud Director settings that accompany the vApps or the virtual machines in a replication. After a successful protection or migration, vCloud Availability reads these settings from the source site and applies them to the destination site, at the end of the replication workflow.

Table 4-1. Replicated vApp Settings

vApp Settings	Replicated in vCloud Availability 3.0	Replicated in vCloud Availability 3.5
vApp Name	Yes	Yes
Description	Yes	Yes
Leases	-	-
Starting and Stopping VMs Configuration	-	-
Metadata	Yes	Yes
vApp Networks	-	Yes

Table 4-2. Replicated VM Settings

VM Settings	Replicated in vCloud Availability 3.0	Replicated in vCloud Availability 3.5
VM Name	Yes	Yes
Computer name	Yes	Yes
Description	Yes	Yes
Hot add settings	-	-
Guest OS Customization	-	Yes
Guest properties	-	Yes
Resource allocation	-	-
Metadata	Yes	Yes

This chapter includes the following topics:

- [Grouping VMs in a vApp Replication](#)
- [Selecting Replicated Disks](#)
- [Using Replication Seeds](#)
- [Create a Migration](#)

- [Create a Protection](#)
- [Configuring Network Settings of Replications to the Cloud](#)

Grouping VMs in a vApp Replication

For on-premises to cloud replications, you can create a collection of virtual machines in a single container, managed and replicated as a single unit. You can specify the virtual machines boot order, boot delays, and protect or migrate them as a single vApp replication in the destination cloud site.

In the destination cloud site, the grouped multiple virtual machines are represented as a vApp replication. In this vApp, the virtual machines relations are:

- The boot order works from top to bottom.
- By default, there is no set boot delay. The start wait is measured as the time that passed after the boot of the previous virtual machine.

After creating the vApp replication:

- You can edit the replication settings.
- You can remove virtual machines from the replication.
- You cannot add other virtual machines to the replication.

Partial Failover

You can perform replication operations on the vApp or on a single virtual machine from the vApp.

Failing over one of the virtual machines from a vApp replication, in the destination site results in two vApp replications with the same name. One replication contains the failed over virtual machine and the other replication contains the remaining virtual machines that are not failed over.

Group VMs in a vApp Replication

When creating a replication from an on premises site to a cloud site, you can group multiple virtual machines in a single vApp replication. For the vApp replication, set the order of boot and, optionally, set boot delays for the grouped virtual machines.

Prerequisites

- Verify that vCloud Availability 3.5 is deployed in both the on-premises site and in the destination cloud site.
- Verify you can access vCloud Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing vCloud Availability](#).

Procedure

- 1 Click **Incoming Replications > from On-Prem**.
- 2 Click **New Protection** or **New Migration**.

3 Complete the **New Replication** wizard.

- a On the **Source Site** page, select your on-premises site and click **Next**.
- b On the **vCenter VMs** page, select multiple virtual machines to replicate in a vApp.
- c Enable **Group VMs to a single vApp**, and click **Next**.

After the vApp replication is created, you can exclude but cannot add replicated virtual machines.

- d On the **vApp Settings** page, set the following settings and click **Next**.
 - Enter a name for the resulting vApp.
 - Optionally, change the order of boot of the virtual machines in the vApp by dragging the rows.
 - Optionally, enter a start wait time to select the boot delay interval of the replicated virtual machines in the vApp.

Results

In the destination cloud site, the grouped multiple virtual machines are represented in a vApp replication.

Modify the Settings of Grouped VMs

After grouping virtual machines in an on premises to cloud replication, you can modify the resulting vApp name and the grouped virtual machines order of boot and boot delay. Also, you can modify the vApp replication settings or exclude replicated virtual machines.

Prerequisites

- Verify that vCloud Availability 3.5 is deployed in both the on-premises site and in the destination cloud site.
- Verify you can access vCloud Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing vCloud Availability](#).

Procedure

- 1 Under **Incoming Replications**, click **from On-Prem** and select a vApp.
- 2 To modify the vApp settings, click the **vApp Settings** button.
- 3 In the **Edit vApp Settings** window, modify the vApp settings.
 - a In the **vApp name**, modify the name of the vApp.
 - b To change the order of boot of the virtual machines, drag the rows.
 - c To set a boot delay for each virtual machine, under **Start wait** enter a number and select seconds or minutes.
 - d To accept the changes, click **Apply**.
- 4 To modify the settings of the vApp replication, click the **Settings** button.

- 5 In the **Edit Protection Settings** window, modify the replication settings.
 - a To change the target recovery point objective (RPO) between 5 minutes and 24 hours, click the timeline or the preset times.
 - b To modify the retention policy, select the number of instances and a duration to spread them.
 - c To enable the quiesce, enable the toggle.
 - d To compress the replication traffic, enable the toggle.
 - e To accept the changes, click **Apply**.
- 6 To exclude replicated virtual machines from vApp replications, on the top of the page, click **VM**.
 - a To exclude a VM replication, select it and click **Delete**.
 You can later add this VM replication to a new vApp replication but not to an existing vApp replication.
 - b In the **Delete** window, to confirm the exclusion click **Delete**.

Results

vCloud Availability replicates the vApp in the destination cloud site with the modified settings.

Selecting Replicated Disks

In the replicated virtual machines, some hard drives contain information that does not need to be transferred to the destination site. For example, you can exclude from replicating a hard disk that only holds a swap partition.

With vCloud Availability, you can select which source disks in a virtual machine to replicate when creating the replication. Also, you can modify this selection after creating the replication. By default, all disks in a virtual machine are selected for replication. Also, you can deselect all disks. Without any disks selected, vCloud Availability replicates only the vApp or virtual machine settings.

The same storage policy applies to all the selected disks in a virtual machine.

Replication Direction

You can modify the selected disks in all incoming and outgoing replications:

- From an on-premises site to a cloud site
- From a cloud site to an on-premises site
- From a cloud site to another cloud site

Disk Properties

- **Disk Key** is the virtual device key of the disks and is unique for a virtual machine. The disk key is calculated and depends on the controller type and socket the disk is attached to.
- **Label** shows the virtual hard drive label.

- Capacity shows the hard drive space.

Modifying the Virtual Machine Hardware

After creating a replication, you can also edit the source virtual machine hardware and modify the disk count externally to vCloud Availability, for example in vCenter Server or in vCloud Director.

- After adding a disk to the source virtual machine hardware, vCloud Availability selects it for replication and pauses the replication.
- After removing a disk from the source virtual machine hardware, vCloud Availability removes it from the replication configuration without pausing the replication. Previously replicated instances keep their disk count as of the time of their creation.

Disk Mismatch

- When using a seed virtual machine, the disk count in the virtual machine at the destination must match the number of selected disks in the source virtual machine.
- For a successful reverse replication, you must address any differences in the selected disks between the source and the recovered workload. Attempting a reverse replication with mismatching disks shows an error message and the source vApp or virtual machine is powered off, without completing the reverse replication.

Select Replicated Disks

From either the source site or the destination site, for existing replications you can modify the selected disks for replication.

Prerequisites

- Verify that vCloud Availability 3.5 is deployed in both the source and in the destination sites.
- Verify that you can access vCloud Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing vCloud Availability](#).
- Verify that you are using vCenter Server version 6.7 or later to select replicated disks from the vCloud Availability vSphere Client Plug-In. If you use vCenter Server version 6.5, select replicated disks after you log in to the vCloud Availability Portal.

Procedure

- 1 In the left pane, choose a replication direction..
- 2 To modify the disks of a virtual machine, in the top of the page click the **VM** button, or to modify the disks of a vApp, click the **vApp** button.
- 3 Select a replication with a **Green** overall health.
- 4 Click the **Disks** button.
- 5 In the **Disks** window, select the virtual machine in the replication and on the right side select disks for replication.

6 After you modify the selection, click **Select**.

Results

The selected disks are replicated in the destination site.

Using Replication Seeds

For each new replication, vCloud Availability performs a full initial synchronization copying the entire source data from the vApp or VM to a datastore in the target site. Use a replication seed to reduce the network traffic and the required time for the replication initial synchronization.

Due to the size of the vApp or VM or to the network bandwidth, an initial full synchronization might take a long time. To reduce the initial synchronization time, you transfer the source vApp or VM to the target site. Use removable media, failover of a previous replication, or other means of data transfer. Then, in the target site, configure a replication that uses the vApp or VM copy as a replication seed.

When a replication uses a seed vApp or VM, vCloud Availability does not copy the whole source vApp or VM data to the target site. Instead, vCloud Availability copies only the different data blocks between the source vApp or VM and the seed and reuses the seed data in the target site as a basis for replication.

Note vCloud Availability stores the replication data in the target site without creating copies of the seed vApp or VM. You can use a seed vApp or VM to configure only one replication.

Use a VM as a Replication Seed

To use a VM as a seed, in the target site, select a VM that has an identical disk configuration with the seed VM. The size and number of disks, and their assignment to disk controllers and bus nodes must match the replication source and the seed VM.

For example, if a replication source VM has two 4 GB disks, one of them assigned to SCSI controller 0 at bus number 0, the second one to SCSI controller 1 at bus number 2. Your seed VM must have the same hardware configuration - two 4 GB disks, at SCSI 0:0 and at SCSI 1:2.

The disks in the source virtual machine must match the disks in the seed VM. Else the reverse replication fails with a Disks of provided seed VM don't match the disks of the source VM message.

For more information, see [Selecting Replicated Disks](#).

Use a vApp as a Replication Seed

To use a vApp as a seed, in the target site, select a vApp that has an identical VM set with the seed vApp. The VMs in the seed vApp must have a matching name to the VMs in the source site vApp. Each VM in the seed vApp, must meet the prerequisites to be a seed VM of the VM with the same name in the source site.

After you start a replication, in the VMware vCloud Director inventory, the seed vApp is empty and you can manually copy the vApp settings and metadata that are not replicated from the source site. The seed vApp remains available as an empty copy and you can remove it at your discretion.

Create a Replication Seed

Use one of the following methods to create a seed vApp or VM in the target site.

- Offline data transfer: Export the VM as an OVF package and a Cloud service administrator imports the package to your cloud organization.
- Clone a VM: Create a seed vApp or VM by cloning the vApp or VM from the target site. vCloud Availability calculates the checksum and exchanges the different blocks from the replication source to the seed vApp or VM.
- Failover data from a previous replication: Set up a replication, fail over to the target site and continue using the on-premises workload. At a later point, you protect it in the target site by using the VM that you failed over earlier as a seed.
- Copy over the network: Copy a source VM to the cloud organization and transfer the source data to the target site by using other means than vCloud Availability.

Export a Virtual Machine or a vApp to a Removable Media

To use a replication seed for configuring a replication, you must export a virtual machine to removable media and provide it to your service provider.

Prerequisites

- Verify that you have sufficient user privileges in the vSphere Client to power off a virtual machine.
- Verify that you have the VMware OVF Tool installed and configured.

Procedure

- 1 Power off the virtual machine on the protected side by using the vSphere Client.
- 2 Export a virtual machine from vCenter Server to a removable media.

```
ovftool 'vi://root@VC_IP/Datacenter_Name/vm/VM_FQDN' VM_FQDN.ova
```

After the process finishes, you can power on the virtual machine.

- 3 (Optional) Export a vApp from vCloud Director to a removable media.

```
ovftool 'vcloud://ORG_ADMIN@VCLLOUD_DIRECTOR_IP:443?org=ORG_NAME&vdc=VDC_NAME&vapp=VAPP_NAME'
VAPP_NAME.ova
```

- 4 Provide the removable media containing the exported files to your service provider.

Importing a Virtual Machine from a Removable Media

You can import a virtual machine from a removable media directly in VMware vCloud Director.

Alternatively, you can import a virtual machine in vCenter Server and then import the virtual machine in VMware vCloud Director by using the vSphere Client.

Import a Virtual Machine Directly in VMware vCloud Director

To configure a replication by using seed, you first import the virtual machine in VMware vCloud Director.

Prerequisites

Verify that you have a removable media containing exported virtual machine files.

Procedure

- ◆ Import the virtual machine from the removable media in VMware vCloud Director.

```
ovftool PATH_TO_DISK/VM_FQDN/VM_FQDN.ovf 'vcloud://VCD_USER@VCD_IP:443?
org=org1&vapp=VM_FQDNvApp&vdc=vdc_org_name'
```

You must extract an OVA file exported from vCenter Server by using `tar -x` and use the resulting `.ovf` file to import in VMware vCloud Director.

Note Do not power on the imported virtual machine.

What to do next

You can now configure a replication by using the created seed vApp in vCloud Availability.

Import a Virtual Machine in vCloud Director Through vCenter Server

Import a virtual machine in VMware vCloud Director to configure replication by using vCenter Server.

Prerequisites

Verify that you have a removable media containing exported virtual machine files.

Procedure

- 1 Deploy the VM from the removable media to vCenter Server.

```
ovftool -ds=DATASTORE_NAME VM_FQDN.ova "vi://root@VC_IP/?ip=HOST_IP"
```

Note Do not power on the imported VM.

- 2 In the vSphere Client, drag the VM to the tenant resource pool.
- 3 Import a vApp from vCenter Server in vCloud Director. For more information, see [Import a Virtual Machine to a vApp from vSphere](#).

What to do next

You can now configure a replication by using the created seed vApp in vCloud Availability.

Configure a Replication by Using a Replication Seed

When creating a new incoming or outgoing replication, you can use a vApp or VM as a seed to avoid transferring large amounts of data over the network during the initial full synchronization.

Prerequisites

Verify that the seed vApps or VMs exist in the target site.

Before starting a replication, in the target site you must power off the seed VMs, because they are unregistered from the target VMware vCloud Director and vCenter Server inventories. If the new replication fails, the VM files and disks remain on the datastore. For the VM to appear in the inventories, locate the .vmx file of the VM, manually import the VM in the vCenter Server inventory, and import it to the VMware vCloud Director inventory.

Procedure

- 1 In a Web browser, navigate to the vSphere Client and log in as an administrator.
- 2 From the vSphere Client **Menu**, select **VMs and Templates**.
- 3 In the **Navigator** pane, right-click the virtual machine and select **vCloud Availability > Configure Protection**.

The **New Outgoing Replication** wizard opens.

- 4 On the **vCenter VMs** page, select the virtual machines that you want to protect and click **Next**.
- 5 On the **Target VDC** page, select the target virtual data center to which you want to replicate the virtual machines, and click **Next**.
- 6 On the **Seed VM** page, select the vApp or VM, under **Seed** select the seed you want to use, and click **Next**.

Note If you remove a disk from a replication source virtual machine, the seed disk is not deleted from the datastore in the target site.

- 7 On the **Protection Settings** page, select the settings for the replication, and click **Next**.

Option	Description
Target recovery point objective (RPO)	Use the slider or click the time intervals to set the acceptable period for which data can be lost in the case of a site failure. The available RPO range is from 5 minutes to 24 hours.
Storage policy	From the Storage policy drop-down menu, select the storage policy for placing the recovered VMs and for the replicated data before the recovery. For seed VMs, vCloud Availability Replicator uses the storage policy of the seed VM.
Retention policy for point in time instances	<p>To preserve multiple distinct replication instances (snapshots) to which VMs can be recovered, select the option, select the number of replication instances to keep, and select the preservation period.</p> <p>The number of preserved replication instances depends on the configured retention policy and requires that the RPO period is short enough for the replication instances to be created. For example, if you select to preserve four replication instances per day, the RPO period must not exceed six hours, to allow for the retention of four replication instances in 24 hours.</p>

Option	Description
Enable quiesce	Select the quiescing method for the guest OS of the source VM. Note Quiescing is available only for VMs that support quiescing. For more information, see Guest OS Quiescing Support .
Compress replication traffic	Select to compress the replication data that is transferred through the network and to reduce the network traffic. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

- 8 On the **Scheduling** page, select when to start the replication and click **Next**.
 - Start the replication when the wizard finishes by leaving **Immediately** selected.
 - Schedule the start of the replication by selecting **At a specific time**.
- 9 On the **Ready to Complete** page, verify that the configuration settings are correct and click **Finish**.

Results

In the **Recent Tasks** pane, an **Enable replication of virtual machine** task appears and displays the status of the new replication.

What to do next

You can monitor the replication task progress by clicking the **Replication Tasks** tab.

Create a Migration

Migrate a vApp or a virtual machine to a remote organization, and run the workload in the destination site, by configuring a migration. After a successful replication in the destination site, you can power on the source virtual machine in the destination site.

Prerequisites

- Verify that vCloud Availability is deployed in both the source and in the destination sites.
- If configuring an incoming replication, verify that you are log in to the site in which the vApps or virtual machines you are about to migrate reside.

Procedure

- 1 In the left pane, choose a replication direction.
- 2 To migrate a virtual machine, in the top of the page click the **VM** button, or to migrate a vApp, click the **vApp** button.
- 3 Click **New Migration**.

4 Follow the prompts of the **New Replication** wizard.

- a On the **Seed VM** page, optionally select a vApp or a virtual machine to use as seed and click **Next**.
- b If you did not select a seed, on the **Migration Settings** page, select a storage policy for placing the recovered virtual machines, and click **Next**.

For seed vApps and virtual machines, vCloud Availability Replicator uses the storage policy of the seed.

- c On the **Scheduling** page, select when to start the replication and click **Next**.
 - Start the replication when the wizard finishes by leaving **Immediately** selected.
 - Schedule the start of the replication by selecting **At a specific time**.
- d On the **Ready to Complete** page, verify that the configuration settings are correct and click **Finish**.

Results

After the replication finishes, for the vApp and its virtual machines in the **Replication type** column, you see a Migration state and in the **Replication state** column you see a Healthy state.

Create a Protection

Protect a vApp or a virtual machine from one organization to another, and keep the workload running in the source site, by configuring a protection. If the source site is unavailable, after a successful replication you can fail over and power on the source virtual machine in the destination site.

Prerequisites

- Verify that vCloud Availability is deployed in both the source and in the destination sites.
- If configuring an incoming replication, verify that you are logged in to the site in which the vApp or virtual machine you are about to protect reside.

Procedure

- 1 In the left pane, choose a replication direction.
- 2 To protect a virtual machine, in the top of the page click the **VM** button, or to protect a vApp, click the **vApp** button.
- 3 Click **New Protection**.

4 Follow the prompts of the **New Replication** wizard.

- a On the **Seed VM** page, optionally select a vApp or a virtual machine to use as seed and click **Next**.
- b On the **Protection Settings** page, select the settings for the replication, and click **Next**.

Option	Description
Target recovery point objective (RPO)	Use the slider or click the time intervals to set the acceptable period for which data can be lost if there is a site failure. The available RPO range is from 5 minutes to 24 hours.
Storage policy	From the Storage policy drop-down menu, select the storage policy for placing the recovered virtual machines and for the replicated data before the recovery. For seed vApps and virtual machines, vCloud Availability Replicator uses the storage policy of the seed.
Retention policy for point in time instances	<p>To preserve multiple distinct replication instances (snapshots) to which VMs can be recovered, select the option, select the number of replication instances to keep, and select the preservation period.</p> <p>The number of preserved replication instances depends on the configured retention policy and requires that the RPO period is short enough for the replication instances to be created. For example, if you select to preserve four replication instances per day, the RPO period must not exceed six hours, to allow for the retention of four replication instances in 24 hours.</p>
Enable quiesce	Select the quiescing method for the guest operating system of the source virtual machine.
Compress replication traffic	Select to compress the replication data that is transferred through the network and to reduce the network traffic. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

- c On the **Scheduling** page, select when to start the replication and click **Next**.
 - Start the replication when the wizard finishes by leaving **Immediately** selected.
 - Schedule the start of the replication by selecting **At a specific time**.
- d On the **Ready to Complete** page, verify that the configuration settings are correct and click **Finish**.

Results

After the replication finishes, for the vApp and its virtual machines in the **Replication type** column, you see a Protection state and in the **Replication state** column you see a Healthy state.

Configuring Network Settings of Replications to the Cloud

For on-premises to cloud, or cloud to cloud replications, you can set the target network settings of a vApp or virtual machine. vCloud Availability applies these network settings in the target cloud site, after a migration, failover, or a test failover.

- For the cloud to cloud replications, vCloud Availability replicates all the types of source vApp networks in the target cloud site: Isolated, bridged (direct) and fenced (NAT-routed) networks. vCloud Availability replicates the source networks settings like: IP pools, NAT routes, firewall rules, and DNS settings, in the target site.

- For the on-premises to cloud replications, vCloud Availability creates a new bridged vApp network in the target cloud site and you can configure the vApp network settings.

Configure the Network Settings of On-Premises to Cloud Replications

For the on-premises to cloud replications, you can set target network settings of the vApp or virtual machine. After a migration, failover, or a test failover, vCloud Availability attaches the selected network settings in the target cloud site.

For the on-premises to cloud replications, the network settings are provided as vApp > VM > NIC and you set the network settings at the NIC level.

Prerequisites

- Verify that vCloud Availability is deployed in both the on-premises site and in the cloud site.
- Verify that you can access vCloud Availability as a **tenant** or as a **service provider**. For more information, see [Chapter 2 Accessing vCloud Availability](#).

Procedure

- 1 Under **Incoming Replications > from On-Prem**, click **vApp** or **VM**.
- 2 Select the on-premises to cloud replications to configure the target network settings and click the **Networks** button.
- 3 In the **Network Settings** window, configure the target network settings of the selected replications.

Table 4-3. vApp Network Settings Configuration for Replications from On-Premises to Cloud

Option	Description
vApp / VM	See the name of the vApps, their virtual machines, and their network interface cards (NICs).
Connect to target orgVDC network	Select how to connect the vApps to a network in the target cloud site: <ul style="list-style-type: none"> ■ Mixed selected when multiple NICs are connected to different networks. ■ None select not to connect the highlighted virtual machine NIC to any network. ■ Network name select to connect the highlighted virtual machine NIC to the target OrgVDC <i>network name</i>. As a result, the vApp is bridged and has a direct connection to the target OrgVDC network.
Connected	Select to enable the connection for the selected NICs in each virtual machine to the target OrgVDC network.
Primary NIC	Select the primary NIC for each virtual machine in the vApp.
MAC address	See the MAC address for each NIC in the virtual machines in the vApp.
Reset MAC	Select to reset the MAC address of the highlighted NIC in the target site.

Table 4-3. vApp Network Settings Configuration for Replications from On-Premises to Cloud (continued)

Option	Description
IP mode	<ul style="list-style-type: none"> ■ None selected by default, no IP addressing mode is specified. ■ Mixed selected when multiple NICs have different network configurations. ■ Static - IP Pool select to obtain an IP address for the highlighted NIC from an IP pool in the target network. ■ DHCP select to obtain an IP address for the highlighted NIC when the connected target network is configured with a DHCP server. ■ Static - Manual select to assign a static IP address to the highlighted NIC.
IP address	Set the IP address of each virtual machine or NIC under the vApp.

Tip When in **Connect to target orgVDC network** you select **None**, even when you select **Connected**, the target vApp is replicated without any networks.

Table 4-4. Virtual Machine Network Settings Configuration for Replications from On-Premises to Cloud

Option	Description
VMs	See the name of virtual machines and their network interface cards (NICs).
Connect to target orgVDC network	Select how to connect the virtual machine to a network in the target cloud site: <ul style="list-style-type: none"> ■ Mixed selected when multiple NICs are connected to different networks. ■ None select not to connect the highlighted virtual machine NIC to any network. ■ Network name select to connect the highlighted virtual machine NIC to the target OrgVDC <i>network name</i>. As a result, the vApp is bridged and has a direct connection to the target OrgVDC network.
Connected	Select to enable the connection for the NICs in the virtual machine to the target site network.
Primary NIC	Select the primary NIC for the virtual machine.
MAC address	See the MAC address for each NIC in each virtual machine in the selected replication.
Reset MAC	Select to reset the MAC address of the highlighted NIC in the target site.
IP mode	<ul style="list-style-type: none"> ■ None selected by default, no IP addressing mode is specified. ■ Mixed selected when multiple NICs have different network configurations. ■ Static - IP Pool select to obtain an IP address for the highlighted NIC from an IP pool in the target network. ■ DHCP select to obtain an IP address for the highlighted NIC when the connected target network is configured with a DHCP server. ■ Static - Manual select to assign a static IP address to the highlighted NIC.
IP address	Select Static - Manual from the IP Mode drop-down menu and assign a static IPv4 address to the highlighted NIC.

4 For the selected on-premises to cloud replications, to confirm the target network settings, click **Apply**.

Results

After a successful on-premises to cloud migration, failover, or a test failover, vCloud Availability replicates the workload to the target cloud site. Then vCloud Availability attaches the selected network settings to the target vApp or virtual machine.

Modify the Network Settings of Cloud to Cloud Replications

For the cloud to cloud replications, you can modify the automatically discovered network settings of the vApp or virtual machine. After a migration, failover, or a test failover, vCloud Availability attaches the selected network settings in the target cloud site.

For the cloud to cloud replications, the network settings are provided as vApp > Network > NIC and you modify the network settings at the network level.

Prerequisites

- Verify that vCloud Availability 3.5 is deployed in both cloud sites.
- Verify that you can access vCloud Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing vCloud Availability](#).

Procedure

- 1 Under **Incoming Replications > from Cloud**, click **vApp** or **VM**
- 2 Select the cloud to cloud replications for which you want to view the discovered network settings and click the **Networks** button.
- 3 In the **Network Settings** window, configure the target network settings of the selected replications.

Table 4-5. vApp Network Settings Configuration for Replications from Cloud to Cloud

Option	Description
Source vApp networks	See the name of the vApps, their networks, and the virtual machine network interface cards (NIC).
Connect to target orgVDC network	<p>Select the discovered network that the vApp connects to in the target site after a migration, failover, or test failover:</p> <ul style="list-style-type: none"> ■ Network name select to replicate the source vApp network in the target site and connect the target vApp to the selected orgVDC <i>Network name</i> in the target site. ■ None select to replicate the source vApp networks without connecting the target vApp to any network in the target site. ■ Mixed selected when multiple vApps, virtual machines, or NICs are connected to different networks.
Connected	Select to connect the selected NICs to the vApp network.
Primary NIC	See the discovered primary NIC for each virtual machine in the vApp.
MAC address	See the MAC address for each NIC in the virtual machines in the vApp.
Reset MAC	Select to reset the MAC address of the highlighted NIC in the target site.

Table 4-5. vApp Network Settings Configuration for Replications from Cloud to Cloud (continued)

Option	Description
IP mode	<ul style="list-style-type: none"> ■ None selected by default, no IP addressing mode is specified. ■ Mixed selected when multiple NICs have different network configurations. ■ Static - IP Pool selected obtains an IP address for the highlighted NIC from an IP pool in the target network. ■ DHCP selected obtains an IP address for the highlighted NIC from the target network DHCP server. ■ Static - Manual selected assigns a static IP address to the highlighted NIC.
IP address	Set the IP address of each virtual machine or NIC under the vApp.

Tip When in **Connect to target orgVDC network** you select **None**, and you select **Connected**, the virtual machine NICs are enabled for communication in the target vApp network. The target vApp network is kept isolated and is not connected to the OrgVDC network in the target site.

Table 4-6. Virtual Machine Network Settings Configuration for Replications from Cloud to Cloud

Option	Description
VMs	See the name of the virtual machines and their network interface cards (NIC).
Source vApp networks	See the name of the vApp network that the virtual machine connects to in the source site.
Connected	Select to connect the selected NICs in the virtual machine to the target cloud site network.
Primary NIC	See the discovered primary NIC for the virtual machine.
MAC Address	See the MAC address for each NIC in each virtual machine in the selected replication.
Reset MAC	Select to reset the MAC address of the highlighted NIC of the virtual machine in the target site.
IP mode	<ul style="list-style-type: none"> ■ None selected by default, no IP addressing mode is specified. ■ Mixed selected when multiple NICs have different network configurations. ■ Static - IP Pool selected obtains an IP address from an IP pool in the target network. ■ DHCP selected obtains an IP address from the target network DHCP server. ■ Static - Manual selected assigns a static IP address.
IP address	When Static - Manual from the IP Mode drop-down menu is selected, assign a static IPv4 address to the highlighted NIC.

- 4 For the selected cloud to cloud replications, to confirm the target network settings, click **Apply**.

Results

After a successful cloud to cloud migration, failover, or a test failover, vCloud Availability replicates the workload to the target cloud site. Then vCloud Availability attaches the selected network settings to the target vApp or virtual machine.

Performing vCloud Availability Workflows

5

Protect or migrate workloads by replicating vApps or virtual machines in the vCloud Availability Portal. From or to on-premises sites you can test a failover, fail over, and reverse failover workloads to or from cloud sites.

Recovery Point Objective - RPO

The RPO is the longest tolerable timeframe of data loss. For example, with one hour RPO the recovered virtual machine can have no more than one hour of data lost. Shorter RPO intervals, ensure less data loss during recovery, at the expense of consuming more network bandwidth to keep the replica up-to-date. For more information on the RPO setting, see [How the Recovery Point Objective Affects Replication Scheduling](#) in the *vSphere Replication Administration* document.

When each virtual machine reaches its RPO target, vCloud Availability Replicator writes about 3800 bytes in the vCenter Server events database. Low RPO values, increase the volume of event data in the database. You can limit the number of days that vCenter Server retains event data, or set a higher RPO value to reduce the volume of event data.

Note For a migration, the RPO is 24 hours by default.

Quiescing

vCloud Availability Replicator guarantees a crash consistency among all disks in a virtual machine. If you use quiescing, you might obtain a higher level of crash consistency among the disks that belong to a virtual machine. The operating system of a virtual machine determines the available quiescing types. Quiescing is available only for virtual machine operating systems that support quiescing. For more information, see [Guest OS Quiescing Support](#).

This chapter includes the following topics:

- [Authenticating to Remote Sites](#)
- [Test Failover](#)
- [Perform a Failover Task](#)
- [Perform a Reverse Task](#)

Authenticating to Remote Sites

To perform vCloud Availability workflows, establish a connection between the local and the remote organizations by authenticating from the local site to the remote sites.

Authenticate to Remote Sites as a Tenant

From the local site you can manage vCloud Availability objects in remote sites, after in the local site you establish a connection to the remote sites by authenticating as a **Organization Administrator**.

You can defer this authentication procedure until you need access to the remote site. For information about disaster recovery operations that require you to authenticate to remote sites, see [Chapter 5 Performing vCloud Availability Workflows](#).

Prerequisites

- Verify that the remote site is paired. For information about pairing sites, see the Administering vCloud Availability document.
- Verify that you can access vCloud Availability as a tenant. For more information, see [Accessing the vCloud Availability Portal as a Tenant](#).
- Verify that in both the local and the remote organizations, the tenant user has **Organization Administrator** privileges assigned, to perform replication operations on the remote site.

Procedure

- 1 In the left pane, click **Sites**.
- 2 On the **Cloud sites** page, select the remote site you want to authenticate to and click **Login**.
- 3 In the **Log In** window, enter the remote site **Organization Administrator** credentials, and click **Login**.

Authenticate to Remote Sites as a Service Provider

From the local site you can manage vCloud Availability objects in a remote site, after in the local site you establish a connection to the remote sites by authenticating as a **Organization Administrator** or as a **System Administrator**.

You can defer this authentication procedure until you need access to the remote site. For information about disaster recovery operations that require you to authenticate to remote sites, see [Chapter 5 Performing vCloud Availability Workflows](#).

Prerequisites

- Verify that the remote site is paired. For information about pairing sites, see the Administering vCloud Availability document.
- Verify that you can access vCloud Availability as a service provider. For more information, see [Accessing the vCloud Availability Portal as a Tenant](#).

- Verify that you have credentials for both the local and the remote organizations, to perform replication operations on the remote site.

Procedure

- 1 In the left pane, click **Sites**.
- 2 On the **Cloud sites** page, select the remote site you want to authenticate to and click **Login**.
- 3 In the **Log In** window, enter the remote site **Organization Administrator** or **System Administrator** credentials, and click **Login**.

Test Failover

Validate the data from the source site replicates correctly in the destination site by performing a test failover.

You perform a test failover for a replication and then delete the test data.



Prerequisites

- Verify that vCloud Availability is deployed in both the source and in the destination sites.
- Verify that the vApp or the virtual machine is protected in the destination site, before you test the failover.

Procedure

- 1 In the left pane, choose a replication direction.
- 2 To test failover of a virtual machine, in the top of the page click the **VM** button, or to test failover a vApp, click the **vApp** button.
- 3 Select the protected vApp or virtual machine to fail over and click **Test Failover**.

4 In the **Test Failover** wizard, configure your selected workload for the failover test.

- a On the **Recovery Settings** page, configure the recovered workload and click **Next**.

Option	Description
Power on recovered vApps	Select to power on the virtual machines on the destination site after the task completes.
Network settings	<ul style="list-style-type: none"> ■ Select Apply preconfigured network settings on failover, to assign the network configured during the virtual machine replication. ■ Select Connect all VMs to network and from the drop-down menu select a network to connect the replicated virtual machines to.

- b On the **Recovery Instance** page, configure the recovery point in time and click **Next**.

Option	Description
Synchronize all VMs to their current state	Creates an instance of the powered on workload with its latest changes and uses that instance for the test failover.
Manually select existing instance	Select an instance without synchronizing the data for the recovered workload.

- c On the **Ready To Complete** page, review the test details and click **Finish**.

In the **Last changed** column, you can monitor the progress of the test.

Results

After the test finishes, for the vApp and its virtual machines in the **Recovery state** column you see a Test image ready state.

What to do next

- You can fail over the workload to the destination site. For more information, see [Perform a Failover Task](#).

You can perform a failover, test cleanup, or edit the replication settings. If you no longer have to protect the workload, you can delete the replication to remove it from the vApp and virtual machine list.

Perform a Failover Task

If the protected source site is unavailable, in the destination site perform a workload disaster recovery operation.

Prerequisites

- Verify that vCloud Availability is deployed in both the source and in the destination sites.
- Verify that the vApp or the virtual machine is protected in the destination site, before you start a failover task.

Procedure

- 1 In the left pane, choose a replication direction.

- 2 To fail over of a virtual machine, in the top of the page click the **VM** button, or to fail over a vApp, click the **vApp** button.
- 3 Select the protected vApp or virtual machine to fail over and click **Failover**.
- 4 In the **Failover** wizard, configure your selected workload for the failover.
 - a On the **Recovery Settings** page, configure the recovered workload and click **Next**.

Option	Description
Consolidate VM disks	Enable for a better performance of the recovered virtual machines at the expense of the failover task taking longer to complete.
Power on recovered vApps	Select to power on the virtual machines on the destination site after the task completes.
Network settings	<ul style="list-style-type: none"> ■ Select Apply preconfigured network settings on failover, to assign the network configured during the virtual machine replication. ■ Select Connect all VMs to network and from the drop-down menu select a network to connect the replicated virtual machines to.

- b On the **Recovery Instance** page, configure the recovery point in time and click **Next**.

Option	Description
Synchronize all VMs to their current state	Creates an instance of the powered on workload with its latest changes and uses that instance for the failover task.
Manually select existing instance	Select an instance without synchronizing the data for the recovered workload.

- c On the **Ready To Complete** page, review the task details and click **Finish**.
- 5 In the left pane, to monitor the progress of the task, click **Replication Tasks**.

Results

After the failover task finishes, the failed over workload is running in the destination site and the workload is no longer protected upon the task completion. For the vApp and its virtual machines, in the **Recovery state** column you see a Failed-Over state.

What to do next

- You can reverse and reprotect the workload back to the source site. For more information, see [Perform a Reverse Task](#).
- You can permanently stop the replication traffic and remove all retained workload instances, by clicking **Delete** to remove the replication from the vApp and virtual machine list.

Perform a Reverse Task

After a failover, return the workload data from the destination site back to the source site by performing a reverse task.

After a failover from the source site to the destination site, the migrated workload runs on the destination site. A subsequent reverse task replicates the recovered workload data back to the source protected vApp or virtual machine.

Note When reversing a replication from a cloud site back to an on-premises site, vCloud Availability uses the original datastore for placement of the workload, regardless of the current on-premises local placement setting.

Prerequisites

- Verify that vCloud Availability is deployed in both the source and in the destination sites.
- Verify that you can access vCloud Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing vCloud Availability](#).
- Verify that the vApp or the virtual machine is failed over, before you can start a reverse task.
- Verify that, for vCloud Availability 3.5 the number of disks in the seed virtual machine matches that of the source virtual machine. Performing a reverse task with mismatching configuration of disks fails with the Disks of provided seed VM don't match the disks of the source VM message. For more information, see [Selecting Replicated Disks](#).

Procedure

- 1 In the left pane, choose a replication direction..
- 2 To reverse a failover of a virtual machine, in the top of the page click the **VM** button, or to reverse failover a vApp, click the **vApp** button.
- 3 Select the vApp or the virtual machine that are failed over and click **Reverse**.
- 4 In the **Reverse** window, click **Reverse**.
- 5 In the left pane monitor the progress of the **Reverse** task, by clicking **Replication Tasks**.

Results

After the reverse task finishes, the reversed replication overwrites the source vApp or virtual machine. The reversed workload runs in the primary destination site with a workload protection in the primary source site. For the vApp and its virtual machines, in the **Recovery state** column you see a Reversed state.

What to do next

- You can test or fail over the workload back in the original source site. For more information, see [Test Failover](#) and [Perform a Failover Task](#).
- You can pause the reversed replication, edit the replication configuration, or migrate the workload.

Monitoring the Traffic Usage

6

vCloud Availability counts the traffic data transferred by each virtual machine replication and aggregates the traffic volume information per organization. In a cloud site, you can monitor the traffic for every replication in all directions and you can also monitor the traffic for every organization.

vCloud Availability shows the replication traffic volume that an on premises or a cloud site generates for a given period.

Traffic Usage Monitoring Collection Mechanism

- The vCloud Availability Replication Manager collects the traffic information for all replications to and from cloud sites and to and from on premises sites. The vCloud Availability Replication Manager aggregates the traffic information by organization.
- The cloud vCloud Availability Replicator instance always collects the replication data traffic, for any replication direction. The traffic count includes the replication protocol overhead and TLS overhead and excludes TCP/IP/Ethernet/VPN overhead. If the stream is compressed, the vCloud Availability Replicator counts the compressed bytes.
- Every 300 seconds, the vCloud Availability Replication Manager records to its persistent storage the historical traffic information from all connected vCloud Availability Replicator instances. In an event of a vCloud Availability Replicator instance failure, up to five minutes of historical traffic information might be lost.

Traffic Usage Monitoring Retention

- You can access both live and historical traffic information for virtual machine replications, or historical traffic information per organization.
- When querying the historical traffic information, you can set the beginning and the end of the information period.
- vCloud Availability stores the historical traffic information for the following intervals:
 - 5 minutes intervals, available for the last 5 hours.
 - Hourly intervals, available for the last 14 days

- Daily intervals, available for the last 60 days

This chapter includes the following topics:

- [Monitor Tenant Traffic](#)
- [Monitor and Export Organization Traffic Usage as a Service Provider](#)
- [Monitor the Traffic of a Virtual Machine Replication](#)

Monitor Tenant Traffic

As a tenant, you can see a traffic data chart for your organization. The chart shows the bytes of transferred data for the last five hours, up to two months.

The traffic information is available for virtual machines and is not available for vApps.

Procedure

- 1 Log in to the vSphere Client as a vCenter Server **Administrator**.
- 2 Access the vCloud Availability vSphere Client Plug-In, by clicking **Menu > vCloud Availability**.
- 3 On the **Dashboard** page, in the traffic data chart for the local site, enter the beginning and the end of the traffic reporting period.
- 4 To change the traffic data chart reporting interval, in the traffic data chart for the local site, select an interval of reporting.
 - To see the last five hours of traffic, select the **5 minutes** interval.
 - To see the last two weeks of traffic, select the **1 hour** interval.
 - To see the last two months of traffic, select the **1 day** interval.

On the bottom of the traffic data chart, you can see the amount of traffic transferred for the selected interval.

Results

You see the historical traffic information for your organization.

What to do next

You can also monitor the live and historical traffic for each replication. For more information, see [Monitor the Traffic of a Virtual Machine Replication](#).

Monitor and Export Organization Traffic Usage as a Service Provider

As a service provider, you can see the volume of transferred data for each organization. You can also export data samples for a given period to a file that contains daily usage or traffic data.

Prerequisites

- Verify that vCloud Availability 3.5 or newer is deployed in the cloud site.
- Verify that you can access vCloud Availability as a service provider. For more information, see [Accessing the vCloud Availability Portal as a Service Provider](#).

Procedure

- 1 In the left pane, click **Reports**.
- 2 In the **Organization** pane, select an organization for which you want to filter the displayed traffic information.
- 3 In the organization traffic data chart, enter the beginning and the end of the traffic reporting period, and select the interval of reporting.
 - To see the last five hours of traffic, select the **5 minutes** interval.
 - To see the last two weeks of traffic, select the **1 hour** interval.
 - To see the last two months of traffic, select the **1 day** interval.

On the bottom of the traffic data chart, you can see the amount of traffic transferred for the selected interval.

- 4 To export daily usage and traffic data for all organizations in a .tsv file, enter the beginning and the end of the reporting period and click **Export daily usage data** or **Export daily traffic data**.

The timestamps in the report are in UTC. The exported data includes records for the time the replications did not exists. The values shown for the that time are NaN, which evaluates to 0.

What to do next

You can select another organization and see its traffic information. You can also monitor the traffic for each replication. For more information, see [Monitor the Traffic of a Virtual Machine Replication](#).

Monitor the Traffic of a Virtual Machine Replication

See the live or the recorded volume of transferred data for each virtual machine replication.

The traffic information is available for virtual machines and is not available for vApps.

Prerequisites

- Verify that vCloud Availability is deployed in both the source and in the destination sites.
- Verify that you can access vCloud Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing vCloud Availability](#).

Procedure

- 1 In the left pane, choose a replication direction..
- 2 To show the virtual machine replications, click **VM**.

3 Select a virtual machine replication for which you want to see the traffic information.

4 In the bottom pane, click the **Traffic** tab.

In the traffic data chart bottom, see the amount of traffic transferred by the selected replication in the past three minutes.

5 To switch the chart from a live traffic view to historical data, click **Recorded**.

6 To change the chart reporting interval, enter the beginning and the end of the traffic reporting period and select an interval of reporting.

- To see the last five hours of traffic, select the **5 minutes** interval.
- To see the last two weeks of traffic, select the **1 hour** interval.
- To see the last two months of traffic, select the **1 day** interval.

On the bottom of the traffic data chart, you can see the amount of traffic transferred for the selected interval.

Results

You see the traffic information for the selected replication and you can specify the information data interval and the beginning and the end of the information period.

What to do next

You can select another replication and see its traffic information. You can also monitor the traffic as a single tenant, or you can monitor the traffic for each organization. For more information, see [Monitor Tenant Traffic](#) or see [Monitor and Export Organization Traffic Usage as a Service Provider](#).

Bandwidth Throttling

7

Starting with vCloud Availability 3.5.1, you can set a global limit for the total incoming replication traffic from all sites. Throttling the network bandwidth used by vCloud Availability avoids the network saturation and prevents the overloading of the management connections with the replication data traffic that shares the network infrastructure.

Bandwidth throttling limits the transfer rate of the combined incoming replication data traffic to all local vCloud Availability Cloud Replicator Appliance nodes. This transfer rate is measured in megabits per second.

Throttling the global network bandwidth only applies to the inbound replication data traffic without affecting other types of network traffic like data and management. The global traffic limit operates with any number of vCloud Availability Cloud Replicator Appliance nodes. The number of data connections or the activity within the connections has no effect on the bandwidth throttling.

This chapter includes the following topics:

- [Configure Bandwidth Throttling](#)

Configure Bandwidth Throttling

In vCloud Availability, the service provider can configure the bandwidth throttling to set a limit for the incoming replication traffic from all cloud sites.

Prerequisites

- Verify that vCloud Availability 3.5.1 or newer is deployed in the cloud site.
- Verify that you can access vCloud Availability as a service provider. For more information, see [Accessing the vCloud Availability Portal as a Service Provider](#).

Procedure

- 1 In the left pane, click **Configuration**.
- 2 Under **Traffic settings** next to **Bandwidth throttling**, click **Edit**.

- 3 In the **Bandwidth throttling** window, configure the traffic settings.
 - a To enable bandwidth throttling, select the **Limit all incoming traffic** radio button.
 - b In the **Maximum mbit/s** text box, enter a numerical value for the replication traffic limit in megabits per second.
 - c To save the settings, click **Apply**.