vCloud Availability User's Guide

11 APR 2019

VMware vCloud Availability 3.0

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

Contents

About vCloud Availability User's Guide

1

The *vCloud Availability User's Guide* document provides information on how to manage and monitor the VMware vCloud® Availability solution from the tenant, and from the service provider sides by using the vCloud Availability Portal.

Intended Audience

This information is intended for VMware Cloud Provider Program service providers and experienced system administrators who are familiar with virtual machine technology and data center operations including but not limited to the following areas:

- VMware vSphere®
- VMware vCloud Director®
- VMware vCloud® Availability

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.

Accessing the vCloud Availability Portal as a Tenant

2

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.

This chapter includes the following topics:

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

3

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.

This chapter includes the following topics:

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.

Authenticating to Remote Sites 4

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.

This chapter includes the following topics:

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 8 Performing vCloud Availability Workflows.

Prerequisites

- Verify that the remote site is paired. For information about pairing sites, see the vCloud Availability Administration Guide document.
- Verify that you can access vCloud Availability as a tenant. For more information, see Chapter 2 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 8 Performing vCloud Availability Workflows.

Prerequisites

- Verify that the remote site is paired. For information about pairing sites, see the vCloud Availability Administration Guide document.
- Verify that you can access vCloud Availability as a service provider. For more information, see Chapter 2 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**.

Using the vCloud Availability vSphere Client Plug-In

5

In vSphere, you can create new and manage existing virtual machine replications by using the vCloud Availability vSphere Client Plug-In.

This chapter includes the following topics:

Access the vCloud Availability vSphere Client Plug-In

During the configuration of the on-premises vCloud Availability appliance, it registers as a vSphere Client plug-in. You use the vCloud Availability vSphere Client Plug-In to view and configure incoming and outgoing replications and perform system health monitoring and maintenance.

By using the vCloud Availability vSphere Client Plug-In, on the **vCloud Availability** dashboard, you can monitor the configured replications and the replication tasks.

Prerequisites

- Verify that your vCenter Server version is 6.5 Update 2 or later. In vCenter Server 6.5 Update 1 or older you can use the service from the vCloud Director user interface.
- Verify that you authenticate as a user that is a member of the vCenter Server **Administrators** group.

Procedure

1. In a Web browser, navigate to the vSphere Client and log in as an administrator.
2. To access the vCloud Availability vSphere Client Plug-In, click **Menu > vCloud Availability**.
3. Optionally, to access the vCloud Availability vSphere Client Plug-In, in the **Navigator** pane click **vCloud Availability**.
4. On the **vCloud Availability** page, you can click the following tabs.

Option	Description
Dashboard	Shows you an overview of the network topology, the protected vCenter Server instances, the cloud replication status, and the recently performed tasks.
Outgoing Replications	Shows you the VMs/vApps that are replicated from this site to the cloud, their RPO, the destination organization, the destination data center, the replication state, the recovery state, the replication type: protection or migration, the overall health, and a timestamp of the last change.

Option	Description
Incoming Replications	Shows you the VMs/vApps that are replicated from the cloud to this site, their RPO, the source organization, the source data center, the replication state, the recovery state, the replication type: protection or migration, the overall health, and a timestamp of the last change.
Replication Tasks	Shows you the replication tasks for a site.
System Monitoring	Shows you the environment health status and allows you to restart the appliance or its services.
About	Shows you the product version and the build details.

Configuring Replication Policies

6

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 6-1. 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

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 Replication Seeds

7

For each new replication that you configure, an initial full synchronization operation is performed. During this operation, vCloud Availability copies the whole data from the source vApp or VM to a datastore in the target site. Use replication seeds to reduce the network traffic and the time that is required for the initial full synchronization of a replication.

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 copy the source vApp or VM to the target site by using 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.

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.

This chapter includes the following topics:

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@VCLOUD_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	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. 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.
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.

Performing vCloud Availability Workflows

8

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:

- Configure the Network Settings of a Replication

Creating Replications

In the vCloud Availability Portal, you can protect or migrate workloads by replicating vApps or virtual machines.

Replication Types: Protection and Migration

- To protect a vApp or a virtual machine from one organization to another, and keep the workload running in the source site, you configure a protection.
- To migrate a vApp or a virtual machine to a remote organization, and run the workload in the destination site, you configure a migration.

Replicated Workload Settings

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

Table 8-1. 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 8-2. 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

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	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. 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.
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.

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	■ 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	■ 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.

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 failed over, before you can start a reverse task.

Procedure

1. In the left pane, choose a replication direction.
2. Select the vApp or the virtual machine to that are failed over, and click **Reverse**.
3. In the **Reverse** window, click **Reverse**.
4. 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.

Configure the Network Settings of a Replication

To apply network settings to the target vApp or virtual machine after a migration, failover, or a test failover, for on-premises to cloud replications, or for cloud to cloud replications you configure the network settings.

Prerequisites

- Verify that vCloud Availability is deployed in the source and in the destination sites.

Procedure

1. Log in to the vCloud Availability Portal as a Tenant or as a Service Provider in the site where the replicated vApp or virtual machine resides.
2. Under **Incoming Replications** or **Outgoing Replications**, select a replication for which you want to configure the network settings.
3. Click **Networks**.

   The **Network Settings** window opens.

4 For the selected replication, configure the following network settings.

Table 8-3. Network Settings Configuration

Option	Description
VMs	Shows you the name of the virtual machines in the selected replication.
MAC Address	Shows you the MAC address for each network card (NIC) in each virtual machine in the selected replication.
Reset MAC	Allows you to reset the selected MAC address for each NIC in each vApp and in each virtual machine in the target site.
Connected	Allows you to control whether each NIC in each vApp and in each virtual machine is connected to the target site network.
Connect to network	Select a network in the target site to which to connect the vApp or virtual machine.
Primary NIC	If the source virtual machine is configured with multiple NICs, you must specify the primary NIC.

IP Mode	■ **Mixed** - If the virtual machine is configured with multiple NICs, and their network configuration is different, the selected replication shows you this state.
	■ **Static - IP Pool** - If the connected network is configured with an **IP Pool**, the selected replication obtains the IP address from the IP pool.
	■ **DHCP** - If the connected network is configured with a DHCP server, the selected replication obtains the IP address from that DHCP server.
	■ **Static - Manual** - Allows you to assign a static IP address to the selected replication.
	■ **Keep** - Depends on the virtual machine presence in the target site.
	  ■ If for the selected replication in the target site there is no existing virtual machine, after migrate, failover, or test failover, the target virtual machine is created without network settings configuration.
	  ■ If for the selected replication in the target site there is an existing virtual machine (a seed virtual machine), after migration, failover, or test failover, in the target virtual machine for that NIC the network settings do not change.

IP Address	If from the **IP Mode** drop-down menu you select **Static - Manual**, you can assign a static IPv4 address to the corresponding NIC.

5 For the selected replication, apply the network settings by clicking **Apply**.

Results

After a successful migration, failover, or a test failover, in the target site the vApp or virtual machine is created with the configured network settings.

Migrate from vCloud Availability for vCloud Director 2.x to vCloud Availability 3.0.x

9

As a service provider or as a tenant, transfer the existing replications from vCloud Availability for vCloud Director version 2.0 to vCloud Availability version 3.0.x by using a failover task.

You can perform the migration of a protected virtual machine as a tenant or as a service provider. First log in to the tenant vCloud Availability Portal 2.0 in the cloud site, locate the protected virtual machine, and perform a failover for that virtual machine. After the failover, log in to the new on-premises appliance and migrate the virtual machine replication.

Prerequisites

- Verify that the vCloud Availability for vCloud Director 2.0 holds an organization with at least one virtual machine replication protected from the tenant side.
- Verify that the vCloud Availability for vCloud Director 2.0 and vCloud Availability 3.0 are deployed in the same environment configured with vCloud Director and vCenter Server. The on-premises vCloud Availability appliance and the vSphere Replication appliance are deployed on a vCenter Server 6.5 or 6.7 instance.

Procedure

1. Log in to the vCloud Availability Portal 2.0 by using **Organization Administrator** credentials.
2. Under **Workspaces**, click the **Workloads** tab and locate the virtual machine that you want to migrate.

   The virtual machine is protected on the tenant side.
3. Call the **Actions** pane by clicking the virtual machine.
4. Select the task by clicking **Failover**.
5. Select to power off the failed over virtual machine.

   The vApp that results in the cloud site is powered off and you can use it for seeding.
6. In the **Actions** pane, run the failover task by clicking **Start**.

   In the **Actions** pane, you can monitor the progress of the task.

   On the **Workloads** tab, the virtual machine shows a `Failed over` status.
7. (Optional) Log in to your organization in the vCloud Director (cloud) environment to verify that the virtual machine is failed over.

8 Log in to the vSphere Client at the on-premises data center as an administrator.

9 Select **VMs and Templates** and locate the source virtual machine that you failed over to the cloud.

10 To configure the virtual machine for a replication in vCloud Availability 3.0, right-click the virtual machine and select **vCloud Availability > Configure Protection**.

11 Enter your cloud **Organization Administrator** credentials.

   This organization is the existing cloud organization to which the virtual machine replication belongs.

12 In the **New Outgoing Replication** wizard, configure the virtual machine for replication.

   a On the **vCenter VMs** page, verify that the source virtual machine you right-clicked is selected and click **Next**.

   b On the **Target VDC** page, select the virtual data center to use as a destination for the replication.

   c From the list with existing virtual machines in the destination virtual data center, select the virtual machine failed over to the cloud to use as a seed, and click **Next**.

   d Set the recovery point objective (RPO) and click **Next**.

   e On the **Scheduling** page, select to allow the virtual machine to be configured for replication immediately, and click **Next**.

   f Close the wizard by clicking **Finish**.

      To monitor the migration progress, navigate to **Menu > vCloud Availability > Protected vCenter Server > vCloud Availability > Tasks**.

Results

- In the on-premises vSphere Client, to view the newly replicated source virtual machine navigate to **Menu > vCloud Availability > Protected vCenter Server > vCloud Availability > Outgoing Replications**.
- In the cloud site with the new vCloud Availability 3.0 appliance, to view the newly replicated source virtual machine navigate to **Incoming Replications > from On-Prem**.

What to do next

If you see a failed over replication, clean up the vCloud Availability for vCloud Director 2.0 environment by detaching and forcing remove of the replication.