

VMware Cloud Director Availability User Guide

26 NOV 2020

VMware Cloud Director Availability 4.1

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

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

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

Copyright © 2018-2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 User Guide** 5
- 2 Accessing VMware Cloud Director Availability** 6
 - Accessing the VMware Cloud Director Availability Tenant Portal 6
 - Log In to the VMware Cloud Director Availability Tenant Portal 6
 - Log In by Using the VMware Cloud Director™ Tenant Portal 7
 - Accessing the VMware Cloud Director Availability Provider Portal 7
 - Log In to VMware Cloud Director Availability as a Provider 7
 - Log In by Using the VMware Cloud Director™ Provider Admin Portal 8
 - Access the VMware Cloud Director Availability vSphere Client Plug-In 9
- 3 Authenticating to Remote Sites** 11
 - Authenticate to Remote Sites as a Tenant 13
 - Authenticate to Remote Sites as a Provider 14
 - Multisite Authentication 14
- 4 Using Replications** 17
 - Configuring Replication Policies 21
 - Create a Replication Policy 23
 - Edit a Replication Policy 24
 - Delete a Replication Policy 25
 - Assign a Replication Policy to Organizations 26
 - Review the Replication Policies Assignments 26
 - Replication Policy Conflicts 27
 - Synchronize With VMware Cloud Director 28
 - Configuring SLA Profiles 28
 - Create an SLA Profile 29
 - Edit an SLA Profile 30
 - Delete an SLA Profile 31
 - Assign an SLA Profile to Organizations 32
 - Using Instances 32
 - Store an Instance 33
 - Delete an Instance 34
 - Grouping VMs in a vApp Replication to the Cloud 35
 - Group VMs in a vApp Replication to the Cloud 36
 - Modify the Settings of vApp Replications to the Cloud 37
 - Using Replication Seeds 38
 - Export a Virtual Machine or a vApp to a Removable Media 40

- Importing a Virtual Machine from a Removable Media 40
- Configure a Replication by Using a Replication Seed 41
- Create a Migration 43
- Create a Protection 45
- Create a Replication for Encrypted Virtual Machines 47
- Selecting Replicated Disks 49
 - Select Replicated Disks 50
- Configuring Network Settings of Replications to the Cloud 51
 - Configure the Network Settings of On-Premises to Cloud Replications 52
 - Modify the Network Settings of Cloud to Cloud Replications 54
- Select a Storage Policy 56
- Using Test Failover, Failover, Reverse, or Migrate 57
 - Test Failover 57
 - Perform a Failover Task 59
 - Perform a Reverse Task 60
 - Perform a Migrate Task 62
- Replication States 63

5 Monitoring 65

- Forward Tenant Event Notifications 65
- Monitoring the Traffic Usage 67
 - Monitor the Traffic Usage as a Tenant 67
 - Monitor and Export Organization Traffic Usage as a Service Provider 68
 - Monitor the Traffic Usage of a Virtual Machine Replication 69
- Monitoring the Disk Usage 70
 - Monitor the Disk Usage as a Tenant 70
 - Monitor and Export Organization Disk Usage as a Service Provider 71
 - Monitor the Disk Usage of a Virtual Machine Replication 72
- Monitoring the Resource Requirements 73
 - Monitor the Resource Requirements as a Tenant 74
 - Monitor the Resource Requirements as a Service Provider 74

6 Bandwidth Throttling 76

- Configure the Global Bandwidth Throttling for the Cloud Site 77
- Configure the On-Premises Outbound Bandwidth Throttling 77

User Guide

1

VMware Cloud Director Availability™ offers simple and secure onboarding, migration, and disaster recovery services. Migrate and protect vSphere workloads: between on-premises sites and a multi-tenant cloud site, or between cloud sites.

- After onboarding a tenant with a provider, the on-premises appliance pairs 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 workloads can be migrated or protected between the cloud sites.
- When VMware Cloud Director Availability is paired with another site, tenants and service providers can:
 - Replicate 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 workloads.
- Tenants and providers can manage replications and perform workflows by accessing the VMware Cloud Director Availability portal or in VMware Cloud Director.
- On-premises tenants can access the VMware Cloud Director 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 VMware Cloud Director Availability

2

Access the VMware Cloud Director Availability portal dedicated to providers or to tenants. Alternatively, in VMware Cloud Director you can access the provider admin portal or the tenant portal. For replications between on-premises and cloud sites, access the VMware Cloud Director Availability vSphere Client Plug-In.

This chapter includes the following topics:

- [Accessing the VMware Cloud Director Availability Tenant Portal](#)
- [Accessing the VMware Cloud Director Availability Provider Portal](#)
- [Access the VMware Cloud Director Availability vSphere Client Plug-In](#)

Accessing the VMware Cloud Director Availability Tenant Portal

Tenant users can log in to the VMware Cloud Director Availability Tenant Portal by using the user interface of the Replication Management Appliance, or by using the VMware Cloud Director tenant portal.

Log In to the VMware Cloud Director Availability Tenant Portal

Tenants log in to the VMware Cloud Director Availability Tenant Portal to operate workloads enabled for replications.

Prerequisites

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

Procedure

- 1 In a Web Browser, go to the VMware Cloud Director Availability Tenant Portal at **https://VMware Cloud Director Availability Service 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 Cloud Director™ Tenant Portal

During the initial configuration, VMware Cloud Director Availability registers as a plug-in in VMware Cloud Director™ and provides access for the tenants directly from the VMware Cloud Director™ tenant portal.

When you access the VMware Cloud Director Availability Tenant Portal from the VMware Cloud 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 VMware Cloud Director Availability environment is running VMware Cloud Director™ 9.1 or later.
- Verify that your VMware Cloud Director tenant user profile has **Organization Administrator** privileges.

Procedure

- 1 In a Web browser, go to your organization tenant portal URL, for example `https://cloud.example.com/tenant/Organization-Name`.
- 2 Log in with a VMware Cloud Director **Organization Administrator** user.
- 3 Open the VMware Cloud Director Availability Tenant Portal, by selecting **Availability** from the main menu.

Accessing the VMware Cloud Director Availability Provider Portal

As a **provider**, log in to the VMware Cloud Director Availability Provider Portal by using the management interface of the Replication Management Appliance, or by using the VMware Cloud Director provider admin portal.

Log In to VMware Cloud Director Availability as a Provider

As a **provider**, log in to the VMware Cloud Director Availability Provider Portal to view and manage replication workloads, monitor services health status, and administer VMware Cloud Director Availability.

Prerequisites

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

Procedure

- 1 In a Web browser, go to the VMware Cloud Director Availability Provider Portal at `https://Replication-Management-Appliance-IP-address/ui/admin`.

- 2 Select the type of the login user, enter the user credentials, and click **Login**.
 - Select **Appliance login** and enter the **root** user password.
 - Alternatively, select **SSO login**, enter the **System Administrator** user name as *providerusername@system*, and enter the password.

Log In by Using the VMware Cloud Director™ Provider Admin Portal

During the initial VMware Cloud Director Availability configuration, VMware Cloud Director Availability registers as a VMware Cloud Director™ plug-in and provides access to the VMware Cloud Director Availability Tenant Portal directly from the VMware Cloud Director provider admin portal.

When you access the VMware Cloud Director Availability Tenant Portal from the VMware Cloud Director provider admin portal, you can manage cloud and disaster recovery environments from a single user interface. The first time you access the VMware Cloud Director Availability Tenant Portal from the VMware Cloud Director provider admin portal, you must trust the SSL certificate of the Cloud Service appliance as described in [Step 5](#).

Prerequisites

- Verify that your VMware Cloud Director Availability environment is running VMware Cloud 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://cloud.example.com/provider/login**.
- 2 Log in with a VMware Cloud Director **System Administrator** user.
- 3 From the main menu, select **Cloud Director Availability**.
- 4 If logging in for the first time, click the `https://Cloud-Replication-Management-Appliance-IP-Address:8443` link.
- 5 In the newly opened browser tab, verify the thumbprint and trust the SSL certificate of the Cloud Replication Management Appliance by clicking **Accept**.

You must trust the SSL certificate of the Cloud Replication Management Appliance only when you access the VMware Cloud Director Availability Tenant Portal for the first time. After you trust the certificate, by selecting **Availability** from the VMware Cloud Director provider admin portal main menu opens the VMware Cloud Director Availability Tenant Portal.

Access the VMware Cloud Director Availability vSphere Client Plug-In

By using the VMware Cloud Director Availability vSphere Client Plug-In, you can create and manage on-premises to cloud and cloud to on-premises replications. Also, you can perform system monitoring, configuration, and maintenance of the on-premises appliance.

The VMware Cloud Director Availability vSphere Client Plug-In is registered during the initial configuration of the on-premises appliance. Use the VMware Cloud Director 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 VMware Cloud Director Availability Tenant Portal](#).

Procedure

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

Option	Description
Getting Started	Choose a cloud provider, download the OVA template, and register the VMware Cloud Director 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 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.

Option	Description
System Monitoring	See the health status of the services, the manager, and the cloud site. You can restart the services or restart the 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 VMware Cloud Director Availability version and build details and access the online documentation.

Authenticating to Remote Sites

3

To manage replications on remote cloud sites, you must first extend your session to the remote site by providing credentials for the remote VMware Cloud Director. Extending the session is required before performing specific replication operations from remote cloud sites and before performing any replication operations to remote cloud sites.

Extended Session Authentication

In VMware Cloud Director, when users log in they create a session and they receive a bearer JSON Web Token (JWT) that is used to authenticate future requests.

The Cloud Service manages its own session and it is not directly tied to the VMware Cloud Director session. You create a Cloud Service session by providing credentials, which in turn the Cloud Service uses to create a brand new VMware Cloud Director session.

Locally for your site, after you have a valid Cloud Service session, you can browse and monitor the local inventory of replications, tasks, and others. As your current Cloud Service session associates with a JWT token for the local VMware Cloud Director, you can also browse the local VMware Cloud Director inventory. As long as the JWT is valid, you can perform replication operations that require accessing the local VMware Cloud Director.

To perform replication operations on remote sites, you must extend your local session to the remote site. Extending your session means that you must reauthenticate and provide local user credentials for the remote VMware Cloud Director. After authenticating to the remote site, the local Cloud Service keeps the newly created extended session and for the replication operations in the remote site is using the extended session.

Note You cannot extend the session to remote sites by using Lightweight Directory Access Protocol (LDAP) nor Security Assertion Markup Language (SAML).

Session Expiration

- The local Cloud Service session has a soft time limit that is reached due to inactivity. By default, the soft session lifespan expires after your session is idle for over 30 minutes and you are not viewing a dynamically refreshing management interface page.

- The local Cloud Service session also has a hard time limit that cannot be prolonged without reauthentication. By default, the hard session lifespan expires after 24 hours. During this time, you can perform all operations, unless you navigate to **Sites** and click **Logout**, or log out of the management interface. In the *VMware Cloud Director Availability Security Guide* document, for more information about the two types of lifespans of the session, see [Security Configuration Properties](#), and for more information about the user sessions, see [Users and Sessions](#).
- The extended Cloud Service session expires when the remote JWT becomes invalid, due to expiration or manual logout. By default, the lifespan of VMware Cloud Director JWT also expires in 24 hours. If the lifespan of JWT is modified, and for example, reduced to 1 hour, the extended session expires after 1 hour. If the lifespan of JWT is expanded over 24 hours, the extended session expires according to either of the Cloud Service session lifespans, meaning after 24 hours or after 30 minutes of inactivity.

Replication Operations Requiring an Extended Session

Extend the session to remote sites for the following replication operations, depending on where the replications reside:

- Under **Incoming Replications > from Cloud**, to manage the replications on the remote site you can perform some operations without providing the remote site credentials, and you must provide the remote site credentials to perform the remaining replication operations.

No Credentials Needed	Provide Credentials for the Remote Site
Migrate	New protection
Failover	New migration
Test failover	Network settings
Replication settings	Disk settings
Change owner	
Change storage policy	
Sync	
Pause	
Resume	
Delete replication	

- Under **Outgoing Replications > to Cloud**, to manage the replications on the remote site for all replication operations you must provide the remote site credentials.

Provide Credentials for the Remote Site
Migrate
Failover
Test failover

Provide Credentials for the Remote Site
New protection
New migration
Replication settings
Network settings
Disk settings
Change storage policy
Sync
Pause
Resume
Delete replication

This chapter includes the following topics:

- [Authenticate to Remote Sites as a Tenant](#)
- [Authenticate to Remote Sites as a Provider](#)
- [Multisite Authentication](#)

Authenticate to Remote Sites as a Tenant

From the local site you can manage VMware Cloud Director Availability objects in remote sites, after in the local site you extend the session 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 a list of replication operations that require authentication to remote sites, see [Chapter 3 Authenticating to Remote Sites](#).

Prerequisites

- Verify that the remote site is paired. For information about pairing sites, see the VMware Cloud Director Availability Administration Guide document.
- Verify that you can access VMware Cloud Director Availability as a tenant. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).
- 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**.

Results

The session is extended to the remote site and you can manage the remote site replications. For more information about the duration of the extended session, see [Chapter 3 Authenticating to Remote Sites](#).

Authenticate to Remote Sites as a Provider

From the local site you can manage VMware Cloud Director Availability objects in remote sites, after in the local site you extend the session 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 a list of replication operations that require authentication to remote sites, see [Chapter 3 Authenticating to Remote Sites](#).

Prerequisites

- Verify that the remote site is paired. For information about pairing sites, see the VMware Cloud Director Availability Administration Guide document.
- Verify that you can access VMware Cloud Director Availability as a provider. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#). For information about tenant impersonation, see [Log In by Using the VMware Cloud Director™ Provider Admin Portal](#).
- 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**.

Results

The session is extended to the remote site and you can manage the remote site replications. For more information about the duration of the extended session, see [Chapter 3 Authenticating to Remote Sites](#).

Multisite Authentication

VMware Cloud Director Availability 4.1 supports the VMware Cloud Director Multisite feature and you can use your external identity provider to authenticate to the remote site and manage geographically distributed installations as single entities.

Prerequisites

- Both sites must be running VMware Cloud Director Availability 4.1 and must be paired.
 - Both VMware Cloud Director instances must be associated.
 - The source and destination organizations, for example *source@VCD1* and *destination@VCD2*, must have an active association member status. That means, they must have successfully established bidirectional association and the communication between the two organizations must also be successful.
-
- **Important** Both organizations must have the same users imported. For example, if you use LDAP or SAML authentication, configure both organizations to use the same Identity Provider, and import the same user in each site. The same user that you use to log in to the local site must also exist in the remote site.
-

Procedure

- 1 Log in to the tenant portal of the source VMware Cloud Director instance.
 - a In a Web browser, navigate to the tenant portal URL of your organization.
For example, `https://VCD1/tenant/source_org`.
 - b Enter tenant user credentials.
 - c Click **Log In**.
- 2 In the source VMware Cloud Director instance, create a replication.
 - a From the main menu, select the **Availability** plug-in.
 - b Click **Outgoing Replications**.
In the top-right corner, verify that the destination site is the remote site.
 - c Click **New Replication**.
- 3 Configure the multisite authentication.
 - a In the credentials prompt, click the **Use multisite authentication** link.
 - b From the **Organization** drop-down menu, select the destination organization.
For example, select the remote *destination* organization.
 - c Click **Log in**.

Your session is now extended to the remote site and you now have the same privileges as in a session extended by using local users credentials. For more information on the extended session, see [Chapter 3 Authenticating to Remote Sites](#).

What to do next

- You can browse the remote inventory, such as virtual machines, vApps, VDCs, and others.

- You can perform management operations, such as starting a new replication, failover, and others.

Using Replications

4

In the VMware Cloud Director Availability Tenant Portal or in the VMware Cloud Director 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 the workload from one site to another. The replications can be incoming to the site, or outgoing from the site.

Replication Types

Migration

Migrating a vApp or a virtual machine to a remote organization runs the workload in the destination site.

Protection

Protecting a vApp or a virtual machine from one organization to another keeps the workload running in the source site.

From VMware Cloud Director Availability 4.1 and later, the **service provider** separately enables migrations and protections in the replication policies either only incoming or only outgoing, or both, or neither. In previous versions, the **service provider** controls both replication types together, as incoming replications or outgoing replications.

In a newly deployed VMware Cloud Director Availability 4.1 or later, by default:

- Migrations are allowed, both incoming and outgoing, in the default replication policy to get more workloads with migration available for everyone.
- Protections are disabled, both incoming and outgoing, in the default replication policy. To enable the site for protections, the **service provider** must modify the default policy. Alternatively, keep DR only for subscribers by assigning a custom policy to the organizations. For more information, see [Configuring Replication Policies](#).

After upgrading from a previous version, replication policies with enabled incoming replications now have enabled incoming migrations and enabled incoming protections. Policies before the upgrade with disabled incoming replications now have disabled incoming migrations and disabled incoming protections. Similarly, the previous outgoing replications now control the outgoing migrations and outgoing protections.

VMware Cloud Director Availability 4.1 and later sites interpret previous versions of paired sites with enabled replications as enabled both migrations and protections. For information about pairing sites with mismatching versions, select the latest VMware Cloud Director Availability site version in [Managing Connections Between Cloud Sites](#) in the *VMware Cloud Director Availability Administration Guide*.

Recovery Point Objective - RPO

The RPO is the longest tolerable time frame 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.

When each virtual machine reaches its RPO target, the Replicator Service 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 longer RPO value to reduce the volume of event data.

Note Migrations RPO, by default is 24 hours.

Quiescing

The Replicator Service guarantees a failure consistency among all disks in a virtual machine. Enabling quiescing might obtain a higher level of failure 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

VMware Cloud Director Availability preserves and periodically synchronizes the VMware Cloud Director settings that accompany the vApps or the virtual machines in a replication. After a successful protection or migration, VMware Cloud Director 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 Version 3.0	Replicated in Version 3.5 or Later
vApp Name	Yes	Yes
Description	Yes	Yes
Leases	-	-
Starting and Stopping VMs Configuration	-	-

Table 4-1. Replicated vApp Settings (continued)

vApp Settings	Replicated in Version 3.0	Replicated in Version 3.5 or Later
Metadata	Yes	Yes
vApp Networks	-	Yes

Table 4-2. Replicated VM Settings

VM Settings	Replicated in Version 3.0	Replicated in Version 3.5 or Later
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

Attention Before performing a failover or a test failover, by default the active option in VMware Cloud Director - **VM discovery** must be deactivated. For information about deactivating virtual machine discovery, select the VMware Cloud Director version in [Discovering and Adopting vApps](#) in the *VMware Cloud Director* documentation.

Modifying the Hardware of a Source Virtual Machine While Protected by VMware Cloud Director Availability

- Adding another virtual disk to a replicated virtual machine at the source site pauses the replication.
- VMDK resizing with vSphere 7.0 in the source site automatically resizes the protected virtual machine disk in the destination site, retaining the replication instances.
- Modifying the vCPU count or the RAM size of the source virtual machine replicates on RPO or on manual synchronization in the destination site.

Replicating Thin or Thick Provisioning Virtual Disks

The replicated disks provision format depends whether using replication seeding. For information about seeds, see [Using Replication Seeds](#).

- If not using replication seed, the replica disks are always thin provisioned.

- If using replication seed, the replica disks depend on the seed.
 - If the replication seed is thick-provisioned, the replica disks are provisioned as thick.
 - If the replication seed is thin-provisioned, the replica disks are provisioned as thin.

Replicating Other Storage

Storage DRS (SDRS)

- At the protected site, storage DRS is supported.
- At the recovery site, storage DRS does not move replication files between datastores. Datastore maintenance mode, storage balancing, and IO balancing all ignore replication files. The only supported way to move the replication files between datastores is to change the storage policy.

Raw Device Mapping (RDM)

- RDMs in virtual compatibility mode can be protected.
- RDMs in physical compatibility mode are skipped from replication.

Multi-Writer Disks

VMware Cloud Director Availability does not support disks in multiwriter mode.

Independent Disks

VMware Cloud Director Availability does not migrate independent disks.

Change Block Tracking (CBT)

VMware Cloud Director Availability instances are not compatible with CBT. For information about the instances, see [Using Instances](#).

This chapter includes the following topics:

- [Configuring Replication Policies](#)
- [Configuring SLA Profiles](#)
- [Using Instances](#)
- [Grouping VMs in a vApp Replication to the Cloud](#)
- [Using Replication Seeds](#)
- [Create a Migration](#)
- [Create a Protection](#)
- [Create a Replication for Encrypted Virtual Machines](#)
- [Selecting Replicated Disks](#)
- [Configuring Network Settings of Replications to the Cloud](#)

- [Select a Storage Policy](#)
- [Using Test Failover, Failover, Reverse, or Migrate](#)
- [Replication States](#)

Configuring Replication Policies

The replication policies are sets of rules controlled by the **service provider** that define and control the replication attributes on a VMware Cloud Director organization level.

Replication Attributes Enforced by Replication Policies

As a **service provider** you can assign a single replication policy to multiple VMware Cloud Director organizations to control the following replication attributes:

- Migration
 - Whether an organization can be used as a replication destination for incoming migrations.
 - Whether an organization can be used as a replication source for outgoing migrations.
- Protection
 - Whether an organization can be used as a replication destination for incoming protections.
 - Whether an organization can be used as a replication source for outgoing protections.
- Whether custom SLA settings are allowed in the replications or to use set SLA profiles. For more information, see [Configuring SLA Profiles](#).
- The maximum number of rotated instances, automatically managed and subjected to an automatic retention, per single replication. For more information, see [Using Instances](#).
- The maximum number of stored instances, manually managed and not subjected to an automatic retention, per single replication. For more information, see [Using Instances](#).
- The minimum allowed Recovery Point Objective (RPO) for an organization. For more information, see [Chapter 4 Using Replications](#).
- General limits
 - The maximum number of replications that can be created for an organization.
 - The maximum throughput allowed per each VMware Cloud Director Availability On-Premises Appliance. For more information, see [Chapter 6 Bandwidth Throttling](#).

Default Policy

The default replication policy applies to all organizations that are not associated with a custom replication policy. If only using the default policy, without creating custom policies, to enable the replications, you must modify the default policy attributes to allow incoming and or outgoing migrations and or protections.

Table 4-3. Default Policy Attributes

Setting	Default Value
Policy name	Default Policy
Incoming migrations	Enabled
Outgoing migrations	Enabled
Incoming protections	Disabled
Outgoing protections	Disabled
Custom SLA settings	Enabled
Max rotated instances per protection	Not available *
Max stored instances per protection	Not available *
Minimum allowed RPO	Not available *
Limit the number of configured replications	Disabled
Bandwidth throttling	Disabled

* To select and configure the maximum number of rotated or stored instances or RPO, you must first select the incoming protections.

Note By default, the Default Policy does not allow any protections. Neither incoming nor outgoing protections are allowed, unless you modify the Default Policy, for all organizations not assigned with a custom policy.

New Replication Validation

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

- Whether the assigned replication policy to the destination organization allows custom SLA settings to be set in the replication or to use the set SLA profiles.
- Whether the destination organization allows incoming migrations.
- Whether the source organization allows outgoing migrations.
- Whether the destination organization allows incoming protections.
- Whether the source organization allows outgoing protections.
- Whether on the destination organization the total number of allowed virtual machine replications is not exceeding, including both incoming from on-premises and cloud replications.
- Whether the number of rotated instances per replication of the new replication complies with the policy that is assigned to the destination organization.

- Whether the number of stored 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 these replication attributes is violated, the replication cannot be created.

Create a Replication Policy

To control the replication settings allowed for replications on a VMware Cloud Director organization level, as a **service provider** you can create replication policies.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 In the left pane under **Configuration**, click **Policies**.
- 2 In the **Policies** page, click **New**.
- 3 In the **New Policy** window, configure the replication attributes, and click **Create**.

Setting	Value
Policy name	Enter a unique, case-sensitive name for the new policy.
Incoming migrations	Select to allow incoming migrations.
Outgoing migrations	Select to allow outgoing migrations.
Incoming protections	Select to allow incoming protections.
Outgoing protections	Select to allow outgoing protections.
Custom SLA settings	Select to allow custom SLA settings per replication. Deselect to allow only the SLA profiles to set the SLA settings.
Max rotated instances per protection	If incoming protections are selected, enter the maximum number of rotated instances per replication.
Max stored instances per protection	If incoming protections are selected, enter the maximum number of stored instances per replication.
Minimum allowed RPO	If incoming protections are selected, set the minimum allowed RPO by using the Recovery Point Objective (RPO) slider or by clicking the time ranges.
Events and Notifications	Select to allow users control of the event notifications.

Setting	Value
Limit the number of configured replications	If incoming migrations or incoming protections or both are selected, enter the maximum number of replications.
Bandwidth throttling	Select whether to allow bandwidth throttling and if selected enter the maximum throughput per each VMware Cloud Director Availability On-Premises Appliance.

Results

You created the replication policy and you see it listed on the **Policies** page.

What to do next

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

Edit a Replication Policy

To modify the replication settings of VMware Cloud Director organizations, as a **service provider** you can edit any existing replication policy.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 In the left pane under **Configuration**, click **Policies**.
- 2 In the **Policies** page, select a replication policy and click **Edit**.
- 3 In the **Edit Policy** window, modify the following replication policy settings and click **Apply**.

Setting	Value
Policy name	Enter a unique, case-sensitive name for the new policy.
Incoming migrations	Select to allow incoming migrations.
Outgoing migrations	Select to allow outgoing migrations.
Incoming protections	Select to allow incoming protections.
Outgoing protections	Select to allow outgoing protections.
Custom SLA settings	Select to allow custom SLA settings per replication. Deselect to allow only the SLA profiles to set the SLA settings.
Max rotated instances per protection	If incoming protections are selected, enter the maximum number of rotated instances per replication.

Setting	Value
Max stored instances per protection	If incoming protections are selected, enter the maximum number of stored instances per replication.
Minimum allowed RPO	If incoming protections are selected, set the minimum allowed RPO by using the Recovery Point Objective (RPO) slider or by clicking the time ranges.
Events and Notifications	Select to allow users control of the event notifications.
Limit the number of configured replications	If incoming migrations or incoming protections or both are selected, enter the maximum number of replications.
Bandwidth throttling	Select whether to allow bandwidth throttling and if selected enter the maximum throughput per each VMware Cloud Director Availability On-Premises Appliance.

Results

You reconfigured the replication policy and all new replications that belong to organizations assigned with this policy must comply with the new replication policy settings.

What to do next

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 a replication policy is no longer needed, as a **service provider** 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.
- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 In the left pane under **Configuration**, click **Policies**.
- 2 In the **Policies** page, select the replication policy and click **Delete**.
- 3 In the **Delete Policy** dialog box, to confirm the deletion click **Delete**.

Results

You removed the replication policy.

Assign a Replication Policy to Organizations

To control the replication settings of VMware Cloud Director organizations, as a **service provider** you can assign replication policies to the organizations.

The default replication policy is assigned to an organization unless a custom policy is assigned to the organization.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 In the left pane under **Configuration**, click **Policies**.
- 2 In the **Policies** page, select a replication policy and click **Assign**.
- 3 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 VMware Cloud Director organizations.

What to do next

- 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](#).
- You can see all organizations and their assigned policies by clicking Organizations. For more information, see [Review the Replication Policies Assignments](#).

Review the Replication Policies Assignments

As a **service provider** you can see the assigned replication policies to all VMware Cloud Director organizations.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 In the left pane under **Configuration**, click **Policies**.
- 2 In the **Policies** page, click **Organizations**.

Results

In the **Organizations** page, a list of all VMware Cloud Director organizations and their assigned replication policy shows.

What to do next

In the **Organizations** page, you can assign a replication policy to an organization by selecting it and clicking **Assign**. For more information, see [Assign a Replication Policy to Organizations](#).

Replication Policy Conflicts

Assigning a replication policy to an organization or modifying an existing replication policy assigned to an organization, can result in conflicts such as exceeding quotas, minimum RPO conflicts, and instances conflicts.

When the service providers 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. For more information, see [Check for Replication Policies Conflicts](#).

Resolving Replication Policy Conflicts

The service providers 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. The service providers can also, stop, pause, migrate, or failover the conflicting replications.

Check for Replication Policies Conflicts

As a **service provider** you can validate the compliance status of each replication policy to see the exceeding quotas, minimum RPO conflicts, and instances conflicts.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 In the left pane under **Configuration**, click **Policies**.
- 2 In the **Policies** page, select a replication policy.

Results

In the bottom pane, 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 With VMware Cloud Director

By default, VMware Cloud Director Availability automatically synchronizes the VMware Cloud Director organizations information every hour. As a **service provider**, to reflect recent organization modifications you can initiate a manual synchronization between VMware Cloud Director Availability and VMware Cloud Director.

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 In the left pane under **Configuration**, click **Policies**.
- 2 (Optional) To synchronize VMware Cloud Director Availability with VMware Cloud Director now, click **Sync with Cloud**.

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

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

Note If you recently created an organization and automatic synchronization did not yet occur, the new organization is not assigned automatically to the default replication policy. If you configure a replication for the newly created organization, VMware Cloud Director Availability treats the organization as if the default replication policy is assigned.

Configuring SLA Profiles

By using Service Level Agreement (SLA) profiles, the service providers can define and control the following SLA replications settings: Recovery Point Objective (RPO), retention policy for the point in time instances, quiescing, compression, and initial synchronization time.

SLA Settings Enforced by SLA Profiles

As a **service provider**, you can assign a single SLA profile to multiple VMware Cloud Director organizations to control the following SLA settings of the replications:

- The target recovery point objective (RPO).
- The retention policy for the point-in-time instances.
- Whether the quiescing is enabled.
- Whether the compression is enabled.
- Timeslot to delay the initial synchronization.

After you assign SLA profiles to an organization, the organization can use the SLA profile in replications. Migrations do not use SLA profiles.

Predefined SLA Profiles

By default, VMware Cloud Director Availability provides the Gold, Silver, and Bronze predefined SLA profiles that are not assigned to any organization. The predefined SLA profiles set the following default SLA settings for replications:

Table 4-4. Predefined SLA Profile Settings

SLA Setting	Gold	Silver	Bronze
SLA profile name	Gold	Silver	Bronze
Target recovery point objective (RPO)	30 minutes	2 hours	6 hours
Preserve retained instances	14	7	Disabled
Retained instances spread evenly over the last	2 weeks	1 week	
Enable quiesce	No	No	No
Compress replication traffic	Disabled	Disabled	Disabled
Delay start synchronization	No delay	No delay	No delay

As a **service provider**, you can modify the SLA settings of the predefined SLA profiles, delete them, or create additional SLA profiles.

Using Custom SLA Settings

Using custom SLA settings instead of selecting an SLA profile in a replication is available after you enable the **Allowed custom SLA settings** option in the replication policy. For more information, see [Configuring Replication Policies](#).

Create an SLA Profile

To control the Service Level Agreement (SLA) settings allowed for all replications in a VMware Cloud Director organization, as a **service provider**, you can create additional SLA profiles.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, click **SLA Profiles**.
- 2 In the **SLA Profiles** page, click **New**.
- 3 In the **New SLA profile** window, set up the SLA settings and click **Create**.
 - a Enter a unique, case-sensitive name for the SLA profile.
 - b Set the minimum allowed Recovery Point Objective (RPO).
 - c Set the retention policy for the point-in-time instances.
 - d Select whether to allow quiesce.
 - e Select whether to allow compression of the replication traffic.
 - f Select whether to delay the initial synchronization and select a timeslot.

Results

You created the SLA profile and you can see it listed in the **SLA Profiles** page.

What to do next

You can assign the new SLA profile to one or more VMware Cloud Director organizations. For more information, see [Assign an SLA Profile to Organizations](#).

Edit an SLA Profile

To control the Service Level Agreement (SLA) settings allowed for all replications in a VMware Cloud Director organization, as a **service provider**, you can modify the SLA profiles.

You can modify the predefined SLA profiles. You cannot modify an SLA profile that is already assigned to an organization and if any active replications are configured with that SLA profile.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, click **SLA Profiles**.
- 2 Select an SLA profile and click **Edit**.

- 3 In the **Edit SLA profile** window, modify the following SLA settings and click **Apply**.
 - a Enter a unique, case-sensitive name for the SLA profile.
 - b Set the minimum allowed RPO by using the **Recovery Point Objective (RPO)** slider or by clicking the time ranges.
 - c Set the retention policy for the point-in-time instances.
 - d Select whether to allow quiesce.
 - e Select whether to allow compression of the replication traffic.
 - f Select whether to delay the initial synchronization and select a timeslot.

Results

You have modified the SLA profile and you can see the modified SLA settings.

What to do next

You can assign the modified SLA profile to one or more VMware Cloud Director organizations. For more information, see [Assign an SLA Profile to Organizations](#).

Delete an SLA Profile

If you no longer need an SLA profile, as a **service provider** you can delete it.

You can delete the predefined SLA profiles. You cannot delete an SLA profile that is already assigned to an organization and any active replications are configured with that SLA profile.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, click **SLA Profiles**.
- 2 Select an SLA profile and click **Delete**.
- 3 In the **Delete SLA profile** window, click **Delete**.

Results

You removed the SLA profile. For VMware Cloud Director organizations to which the deleted SLA profile was assigned to continue using the remaining assigned profiles.

What to do next

You can create new or edit the remaining SLA profiles. For more information, see [Create an SLA Profile](#) and [Edit an SLA Profile](#).

Assign an SLA Profile to Organizations

To control the Service Level Agreement (SLA) settings allowed for all replications in a VMware Cloud Director organization, as a **service provider**, you can assign one or more SLA profiles to the organization.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, click **SLA Profiles**.
- 2 Select an SLA profile and click **Assign**.
- 3 In the **Assign SLA profile** window, select the organizations to which you want to assign the profile, and click **Assign**.

Results

You assigned the selected SLA profile to the selected organizations.

What to do next

You can repeat this procedure and select another SLA profile so that you assign multiple SLA profiles to each organization. You can also modify an already assigned SLA profile. For more information, see [Edit an SLA Profile](#).

Using Instances

To recover a workload to a previous state, you can use rotated or stored instances. To avoid the automatic retention of rotated instances, you can store particular rotated instances. The stored instances do not change and you can use them to recover the workload to the stored instance, regardless of the overall retention period of the rotated instances.

VMware Cloud Director Availability supports two types of instances to which any workload can be recovered:

Rotated instances:

The rotated instances are automatically retained and rotated during the lifespan of the replication.

VMware Cloud Director Availability automatically retains a configurable number of the last rotated instances and allows the workload to be recovered to any one of them.

Stored instances:

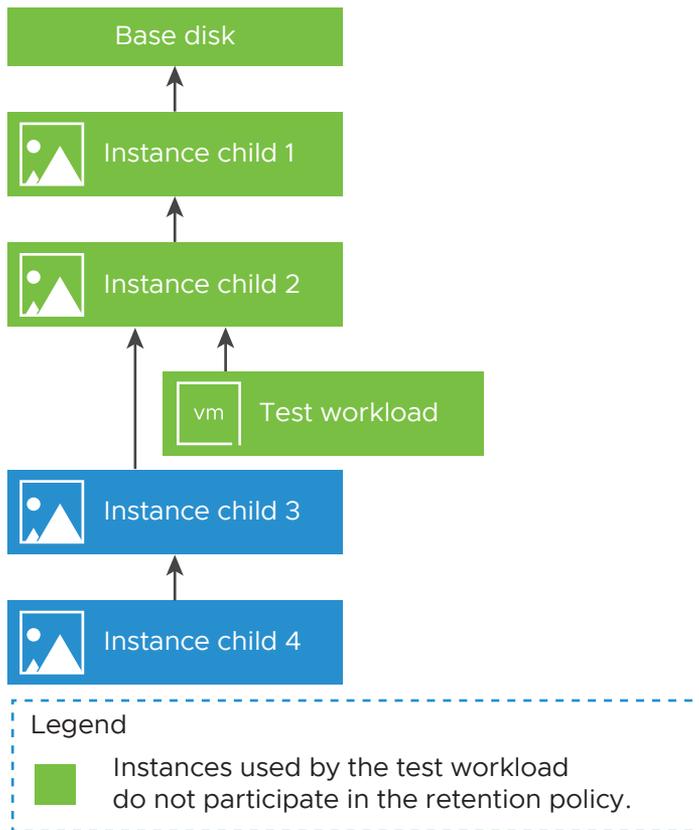
The automatic retention does not affect the stored instances.

After manually storing an instance, the stored instance remains unchanged and if the replication is still active, the workload can be recovered to that stored instance.

Any replication can have both stored instances and rotated instances, depending on the number of allowed stored and rotated instances by the policy.

The automatic retention of a rotated instance can be bypassed by storing it. VMware Cloud Director Availability retains the stored instance until it is no longer marked as stored or until it is manually deleted. Any stored instance, without the latest one can be deleted.

Note After a test failover, the replication can have more stored instances than the policy allows for. Performing a test failover stores the current instance and stores all its parent instances, up to the base disk. Those stored instances no longer participate in the retention policy. After a test failover, the automatically created rotated instances continue to participate in the retention policy. After performing a test cleanup, the instances stored by the test failover are no longer stored and again start participating in the retention policy.



Store an Instance

To retain rotated instances permanently, you store an instance. VMware Cloud Director Availability retains the stored instance until no longer marked as stored or until you manually delete it.

VMware Cloud Director Availability rotates the rotated instances to preserve the configured maximum number of rotated instances per replication. You can retain a configurable number of stored instances permanently.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 or later is deployed in the site.
- Verify that you can access VMware Cloud Director Availability as a **tenant user** or as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).
- Verify that before storing instances, Changed Block Tracking (CBT) is not enabled for the virtual machine.

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 Choose whether to store an instance for a virtual machine or for a vApp replication.
 - To store an instance for a virtual machine replication, in the top-right corner of the page click the **VM** button.
 - To store an instance for a vApp replication, in the top-right corner of the page click the **vApp** button.
- 3 In the bottom pane, click the **Instances** tab.
- 4 To store a rotated instance, select it and click **Store**.

You can subject the stored instance back to automatic retention by clicking **Don't Store**.

Results

You stored the selected instances and they remain available to restore to until the replication is active. The remaining rotated instances continue to be rotated and created to preserve the configured maximum number of rotated instances per replication.

What to do next

You can delete the stored instances to maintain the configured maximum number of stored instances per replication. For more information, see [Delete an Instance](#).

Delete an Instance

To remove a stored instance or a rotated instance, you can delete it. You can delete any stored or rotated instance, without the latest one.

VMware Cloud Director Availability does not modify the stored instances. To maintain the configured maximum number of stored instances per replication, you can delete a stored instance permanently. Optionally, you can also manually delete rotated instances but VMware Cloud Director Availability rotates them and this procedure is not necessary.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 or later is deployed in the site.
- Verify that you can access VMware Cloud Director Availability as a **tenant user** or as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 Choose whether to store an instance for a virtual machine or for a vApp replication.
 - To store an instance for a virtual machine replication, in the top-right corner of the page click the **VM** button.
 - To store an instance for a vApp replication, in the top-right corner of the page click the **vApp** button.
- 3 In the bottom pane, click the **Instances** tab.
- 4 To delete instances, select them and click **Delete**.

You can select both rotated and stored instances to delete, without the latest one. VMware Cloud Director Availability rotates the rotated instances and it is not necessary to delete them manually.

Results

You deleted the selected instances. The remaining rotated instances continue to be rotated and created to preserve the configured maximum number of rotated instances per replication.

What to do next

You can store more instances. For more information, see [Store an Instance](#).

Grouping VMs in a vApp Replication to the Cloud

For on-premises to cloud replications, you can create a collection of virtual machines in a single vApp, 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.

Group multiple virtual machines in a vApp replication, with the following virtual machines relations:

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

Once created, the vApp replication supports the following actions.

- Modifying the vApp replication settings, the vApp settings like delay and boot order, and the remaining settings of the replication.

- Removing virtual machines from the vApp replication.
- No adding of other virtual machines to the vApp replication for versions earlier than VMware Cloud Director Availability 4.3.

Partial Failover

VMware Cloud Director Availability supports performing replication operations for the entire vApp or for one or more virtual machines from the vApp.

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

Group VMs in a vApp Replication to the Cloud

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 VMware Cloud Director Availability is deployed in both the source on-premises site and in the destination cloud site.
- Verify you can access VMware Cloud Director Availability as a **tenant** or as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director 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 the on-premises site and click **Next**.
 - b On the **vCenter VMs** page, select multiple virtual machines to replicate in a vApp.

- c Select **Group VMs to a single vApp** and click **Next**.

Note Once created, the vApp replication supports the following virtual machine operations at a later state.

- Partial failover of some of the virtual machines from the vApp.
 - Excluding virtual machines from the vApp.
 - No adding of virtual machines to the vApp for versions earlier than VMware Cloud Director Availability 4.3.
-

- d On the **vApp Settings** page, configure 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 and dropping them.
 - Optionally, enter a start wait time for configuring the boot delay interval of the replicated virtual machines in the vApp.

Results

In the destination cloud site, a single vApp replication represents the grouped multiple virtual machines.

Modify the Settings of vApp Replications to the Cloud

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 their boot delay. Also, you can modify the vApp replication settings or exclude replicated virtual machines.

Prerequisites

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

Procedure

- 1 Select a vApp, replicated from an on-premises site to a cloud site.
- 2 To modify the vApp settings, click **All actions > vApp Settings**.
- 3 In the **Edit vApp Settings** window, configure the vApp settings and click **Apply**.
 - a In the **vApp name**, modify the name of the vApp.
 - b To change the order of boot of the virtual machines in the vApp, drag and drop them.
 - c To set a boot delay for each virtual machine, under **Start wait** enter a number and select seconds or minutes.

- 4 To modify the replication settings of the vApp replication, click **All actions > Settings**.
- 5 In the **Edit Replication Settings** window, configure the settings of the vApp replication and click **Apply**.
 - a To change the target recovery point objective (RPO), click the timeline or the preset times.
 - b To enable the retention policy, select it and configure the number of instances and a duration for spreading them.
 - c To activate the quiesce, select the toggle.
 - d To compress the replication traffic, select the toggle.
- 6 To exclude replicated virtual machines from vApp replications, on the top of the page under **Grouping**, click **VM**.
 - a To exclude a virtual machine replication from the vApp, select the replication to exclude and click **Delete**.

You can later add this virtual machine replication to a new vApp replication, but not to an existing vApp replication for earlier versions than VMware Cloud Director Availability 4.3.
 - b In the **Delete** window, to confirm click **Delete**.

Results

VMware Cloud Director Availability replicates the vApp in the destination cloud site with the modified settings.

Using Replication Seeds

New replications perform a complete initial synchronization, copying the entire source data from the vApp or virtual machine (VM) to a datastore in the destination site. Using a replication seed lowers the network data traffic and the required time for the initial synchronization while briefly consuming double space.

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 destination site. Use removable media, failover of a previous replication, or other means of data transfer. Then, in the destination site, configure a replication using the vApp or the VM copy as a replication seed.

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

Note VMware Cloud Director Availability stores the replication data in the destination site without creating copies of the seed vApp or VM. You can use a seed vApp or VM for configuring only one replication.

Destination datastore space consumption

To be able to create the independent disk for the replication, when starting a replication with or without seed requires at least as much space as the source VM capacity in a single compliant destination datastore.

To start a replication using a seed VM requires twice the same storage space. The double space requirement lasts for a short period of time between the independent disk creation and the removal of the seed VM.

Using a seed VM lowers the network traffic, not the datastore usage, and requires as much free space, as for replicating from scratch, even though the space is only briefly reserved and might not even get fully utilized.

After VMware Cloud Director Availability collects the storage consumption and updates the independent disk, the disk usage with the respective quota reservation might shrink. Shrinking is due to reporting the actual usage, instead of the total disk capacity.

Use a VM as a replication seed

To use a VM as a seed, in the destination 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 destination 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 Cloud 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 for creating a seed vApp or VM in the destination 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 destination site. VMware Cloud Director 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 destination site and continue using the on-premises workload. At a later point, you protect it in the destination 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 destination site by using other means than VMware Cloud Director 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 VMware Cloud 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 Cloud Director™. Alternatively, you can import a virtual machine in vCenter Server and then import the virtual machine in VMware Cloud Director™ by using the vSphere Client.

Import a Virtual Machine Directly in VMware Cloud Director™

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

Import a Virtual Machine in VMware Cloud Director Through vCenter Server

Import a virtual machine in VMware Cloud 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 VMware Cloud 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 VMware Cloud Director Availability.

Configure a Replication by Using a Replication Seed

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

Prerequisites

- Verify that the free space in the destination datastore is at least double that of the source vApp or virtual machine. For information about the double space requirement, see [Destination datastore space consumption](#).
- Verify that the seed vApps or virtual machines exist in the target site.
- Before starting a replication using a seed, in the target site you must power off the seed virtual machines, because they are unregistered from the target VMware Cloud Director and vCenter Server inventories. If the new replication fails, the virtual machine files and disks remain on the datastore. For the virtual machine to appear in the inventories, locate the `.vmtx` file of the virtual machine, manually import the virtual machine in the vCenter Server inventory, and import it to the VMware Cloud 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 **VMware Cloud Director 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 virtual machine, 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 virtual machines and for the replicated data before the recovery. For seed virtual machines, Replicator Service uses the storage policy of the seed virtual machine.

Option	Description
Retention policy for point in time instances	<p>Select to preserve multiple distinct replication instances (snapshots) to which virtual machines can be recovered. Also 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	<p>Select the quiescing method for the guest OS of the source virtual machine.</p> <p>Note Quiescing is available only for virtual machines that support quiescing. For more information, see Guest OS Quiescing Support.</p>
Compress replication traffic	<p>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.</p>

- 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 VMware Cloud Director Availability is deployed in both the source and in the destination sites.
- Verify that you can access VMware Cloud Director Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).
- Verify that your session is extended to the site in which the vApps or virtual machines you are about to migrate reside. For more information, see [Chapter 3 Authenticating to Remote Sites](#).

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 Click **All Actions > New migration**.
- 3 Follow the prompts of the **New Replication** wizard.

- a On the **Target VDC and Storage policy** page, select the destination virtual data center for the replication and the storage policy for placing the recovered virtual machines, and click **Next**.

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

For VDCs that do not have replications to them, the **Quota** column shows **Currently unavailable**, and is refreshed once every 10 minutes.

- b On the **Settings** page, configure the following replication settings and click **Next**.
 - To start the replication when the wizard finishes, leave **Delay start synchronization** deselected.
 - To schedule the start of the replication, select **Delay start synchronization** and enter the local date and time to start the replication.
 - To exclude some hard disks of the virtual machines from replicating to the destination site, select **Exclude disks**.
 - To use a previous copy of the virtual machines in the destination site, select **Configure Seed VMs**.
- c If you selected **Configure Seed VMs**, on the **Seed VM** page you must select a vApp or a virtual machine to use as seed and click **Next**.
- d If you selected **Exclude disks**, on the **Disks** page you must select the hard disks to replicate and click **Next**.
- e On the **Ready to Complete** page, verify that the replication 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.

What to do next

You can migrate to the destination site. To migrate, the source workload must be operational. For more information, see [Perform a Migrate Task](#).

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 VMware Cloud Director Availability is deployed in both the source and in the destination sites.
- Verify that you can access VMware Cloud Director Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).
- Verify that your session is extended to the site in which the vApps or virtual machines you are about to protect reside. For more information, see [Chapter 3 Authenticating to Remote Sites](#).

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 Click **All Actions** > **New Protection**.

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

- a On the **Target VDC and Storage policy** page, select the destination virtual data center for the replication and the storage policy for placing the recovered virtual machines, and click **Next**.

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

For VDCs that do not have replications to them, the **Quota** column shows **Currently unavailable**, and is refreshed once every 10 minutes.

- b On the **Settings** page, configure the following replication settings and click **Next**.

Option	Description
SLA profile	To set the SLA settings of the replication, select any of the preconfigured SLA profiles. To view the SLA profile settings, click Show details . To modify the SLA settings and use custom SLA settings, deselect this option.
Target recovery point objective (RPO)	If you deselected SLA profile , to set the acceptable period for which data can be lost if there is a site failure use the slider or click the time intervals. The available RPO range is from 5 minutes to 24 hours.
Retention policy for point in time instances	If you deselected SLA profile , to preserve multiple distinct replication instances to which the virtual machines can be recovered, select this 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.
Delay start synchronization	<ul style="list-style-type: none"> ■ To schedule the start of the replication, select this option and enter the local date and time to start the replication. ■ To start the replication when the wizard finishes, leave this option deselected.
Exclude disks	To exclude some hard disks of the virtual machines from replicating to the destination site, select this option.
Configure Seed VMs	To use a previous copy of the virtual machines in the destination site, select this option.

- c If you selected **Configure Seed VMs**, on the **Seed VM** page you must select a vApp or a virtual machine to use as seed and click **Next**.
- d If you selected **Exclude disks**, on the **Disks** page you must select the hard disks to replicate and click **Next**.
- e 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.

What to do next

You can test or fail over the workload to the destination site. To fail over, the source workload might not be operational. For more information, see [Test Failover](#) and [Perform a Failover Task](#).

Create a Replication for Encrypted Virtual Machines

The storage policy drives the encryption for virtual machines in vCenter Server and VMware Cloud Director. Enable encryption in the storage policy and assign it to the virtual machine configuration files and its disks. The replication follows the encryption status. First encrypt the virtual machines before adding them in the replication.

Starting with VMware Cloud Director Availability 4.1, you can improve the security of your data by replicating encrypted virtual machines from one cloud site to another cloud site.

Important Cannot replicate a vApp containing both encrypted and non-encrypted virtual machines.

If the replicated virtual machine changes from encrypted to unencrypted, reestablish the replication by stopping and then starting it.

Prerequisites

- To replicate encrypted virtual machines, verify that later or the following versions are installed in both the source and in the destination cloud sites.
 - VMware Cloud Director Availability 4.1 or later
 - VMware Cloud Director 10.1 or later
 - vCenter Server 6.7 U3 or later
- Prerequisites for the ESXi hosts.
 - Install the HBR agent VIB in all the ESXi hosts in both the source and the destination sites. After installing the HBR agent, it encrypts the traffic originating from the source ESXi host, providing end-to-end encryption. For more information about VIBs and how to install them, see [VIBs, Image Profiles, and Software Depots](#) in the *VMware ESXi Upgrade*. You can download the HBR agent VIB file directly from the Cloud Replicator Appliance:
 - Either from the appliance filesystem, download the `/opt/vmware/hbr/vib/vmware-hbr-agent-build_number.i386.vib` file.
 - Alternatively, from the following URL download the `https://Replicator_Address/hbr-agent.vib` file.

- Prerequisites for the vCenter Server instances.
 - For virtual machine encryption to work in vCenter Server, configure a Key Management Server (KMS). Use the same KMS for both the source and the destination vCenter Server instances. Make sure that the KMS cluster names also match. For information about setting up a Key Management Server cluster, see [Set up the Key Management Server Cluster](#) in the *vSphere Security Guide*.
 - In vCenter Server, you must also have an encryption storage policy. For more information, see [Create an Encryption Storage Policy](#) in the *vSphere Security Guide* and for more information about the virtual machine encryption, see [Virtual Machine Encryption](#) in the *vSphere Security Guide*.
- Prerequisites for VMware Cloud Director.
 - Verify that the **Organization Administrator** role has the **vApp: View VM and VM's Disks Encryption Status** right. For more information, see [Rights in Predefined Global Tenant Roles](#) in the *VMware Cloud Director Tenant Portal Guide*.
 - Add the encryption-enabled storage policy to a provider VDC. For more information, see [Add a VM Storage Policy to a Provider Virtual Data Center](#) in the *VMware Cloud Director Service Provider Admin Portal Guide*.
 - Add the encryption-enabled storage policy to an organization VDC. For more information, see [Add a VM Storage Policy to an Organization Virtual Data Center](#) in the *VMware Cloud Director Service Provider Admin Portal Guide*.
 - Create an encrypted virtual machine by applying the encryption-enabled storage policy. Replications for encrypted virtual machines can only include virtual machines with an encryption-enabled storage policy.
- Verify that you can access VMware Cloud Director Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).
- Verify that your session is extended to the site in which the vApps or virtual machines you are about to replicate reside. For more information, see [Chapter 3 Authenticating to Remote Sites](#).

Procedure

- 1 In the left pane, choose a replication direction.
For a replication with encrypted virtual machines, choose an incoming replication from a cloud site, or an outgoing replication to a cloud site.
- 2 To create a replication for encrypted virtual machines, select either new protection or new migration.
 - Click **All Actions > New Protection**.
 - Click **All Actions > New Migration**.

3 Complete the **New Replication** wizard.

- a In the **Cloud vApps and VMs** page, select only virtual machines that show status `Yes` in the Encrypted column, and click **Next**.

The Encrypted column shows status `N/A` when the currently logged user does not have the **View Encryption Status of VMs and VM's disks** right in VMware Cloud Director or the version of VMware Cloud Director does not support the encryption of virtual machines.

Note In a replication for encrypted virtual machines, select only encrypted virtual machines.

- b In the **Destination VDC and Storage policy** page under **Storage policy**, select a storage policy that shows `Encrypted` in the Encryption capability column and click **Next**.

After selecting an encrypted virtual machine, you can only select an encrypted storage policy.

- c In the **Settings** page, configure the replication settings and click **Next**.
- d If in the **Settings** page you selected **Configure Seed VMs**, in the **Seed VM** page select the seed and click **Next**.
- e In the **Ready to Complete** page, verify that the replication settings are correct and click **Finish**.

The initial synchronization of a replication containing an encrypted virtual machine takes longer to complete than a replication with the same settings that contains a non-encrypted virtual machine with the same hardware.

Results

The new replication containing encrypted virtual machines uses encryption for the data communication.

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 VMware Cloud Director 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, VMware Cloud Director 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 VMware Cloud Director Availability, for example in vCenter Server or in VMware Cloud Director.

- After adding a disk to the source virtual machine hardware, VMware Cloud Director Availability selects it for replication and pauses the replication.
- After removing a disk from the source virtual machine hardware, VMware Cloud Director 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 select the hard disks that are replicated.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in both the source and in the destination sites.

- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).
- Verify that you are using vCenter Server version 6.7 or later to select replicated disks from the VMware Cloud Director Availability vSphere Client Plug-In. If you use vCenter Server version 6.5, select replicated disks after you log in to the VMware Cloud Director Availability Tenant Portal.

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 Select a replication with a **Green** overall health.
- 3 Click **All Actions > Disk settings**.
- 4 In the **Disks** window, select the virtual machine in the replication and on the right side select the hard disks to replicate.
- 5 After you modify the selection, click **Select**.

Results

The selected disks are replicated in the destination site.

Configuring Network Settings of Replications to the Cloud

For on-premises to cloud, or cloud to cloud replications, you can set the destination network settings of a vApp or virtual machine. After a migration, failover, or a test failover, VMware Cloud Director Availability applies these network settings in the destination cloud site.

- For the cloud to cloud replications, VMware Cloud Director Availability replicates all the types of source vApp networks in the destination cloud site: isolated, bridged, also called direct, and fenced (NAT-routed) networks. VMware Cloud Director Availability replicates the source networks settings like: IP pools, NAT routes, firewall rules, and DNS settings, in the destination site.

If replicating from NSX-V to NSX-T backed destination VDC, the following networking features cannot be replicated:

If the NAT-routed vApp networks are attached to an organization VDC network, the NAT-routed networks are converted to bridged, also called direct networks.

The isolated vApp networks do not support the DHCP service.

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

If not explicitly selected, the destination organization VDC networks are automatically resolved. The mapping is based on the default network gateways and applies on failover, on migrate, and to the test 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, VMware Cloud Director 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 VMware Cloud Director Availability is deployed in both the on-premises site and in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director 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 **All actions > Network settings**.
- 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 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 4-5. 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. To commit the IP address changes to the virtual machine guest OS, select Guest customization. ■ 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 enter a static IP address to the highlighted NIC. To commit the IP address changes to the virtual machine guest OS, select Guest customization.
IP address	Set the IP address of each virtual machine or NIC under the vApp.
Computer name	Enter a computer name for each virtual machine. If you skip entering a computer name, VMware Cloud Director automatically generates one, for example <i>vmname-001</i> . To commit the computer name to the guest OS, select Guest customization .
Guest customization	Select to commit the IP address changes and Computer name to the guest OS of the virtual machine.

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 4-6. 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	<p>Select how to connect the virtual machine to a network in the target cloud site:</p> <ul style="list-style-type: none"> ■ Mixed is 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.

Table 4-6. Virtual Machine Network Settings Configuration for Replications from On-Premises to Cloud (continued)

Option	Description
IP mode	<ul style="list-style-type: none"> ■ None is selected by default, no IP addressing mode is specified. ■ Mixed is 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. To commit the IP address changes to the virtual machine guest OS, select Guest customization. ■ 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 enter a static IP address to the highlighted NIC. To commit the IP address changes to the virtual machine guest OS, select Guest customization.
IP address	Select Static - Manual from the IP Mode drop-down menu and enter a static IPv4 address for the highlighted NIC. To commit the IP address changes to the guest OS, select Guest customization .
Guest customization	Select to commit the IP address changes and Computer name to the guest OS of the virtual machine.
Computer name	Enter a computer name for the virtual machine. If you skip entering a computer name, VMware Cloud Director automatically generates one, for example <i>vmname-001</i> . To commit the computer name to the guest OS, select Guest customization .

- 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, VMware Cloud Director Availability replicates the workload to the target cloud site. Then VMware Cloud Director 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, VMware Cloud Director 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 VMware Cloud Director Availability is successfully deployed in both cloud sites.
- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director 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 **All actions > Network settings**.
- 3 In the **Network Settings** window, configure the target network settings of the selected replications.

Table 4-7. 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.
IP mode	<ul style="list-style-type: none"> ■ None is selected by default, no IP addressing mode is specified. ■ Mixed is 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 from the target network DHCP server. ■ Static - Manual select to enter 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 4-8. 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 is selected by default, no IP addressing mode is specified. ■ Mixed is selected when multiple NICs have different network configurations. ■ Static - IP Pool select to obtain an IP address from an IP pool in the target network. To commit the IP address changes to the guest OS, select Guest customization. ■ DHCP select to obtain an IP address from the target network DHCP server. ■ Static - Manual select to enter a static IP address. To commit the IP address changes to the guest OS, select Guest customization.
IP address	When Static - Manual from the IP Mode drop-down menu is selected, enter a static IPv4 address to the highlighted NIC. To commit the IP address changes to the guest OS, select Guest customization .
Guest customization	Select to commit the IP address changes to the guest OS.

- 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, VMware Cloud Director Availability replicates the workload to the target cloud site. Then VMware Cloud Director Availability attaches the selected network settings to the target vApp or virtual machine.

Select a Storage Policy

You can select a new storage policy for the placement of newly recovered virtual machines or vApps. By modifying the selected storage policy, you can move the destination replica files from one datastore to another.

Prerequisites

- Verify that you can access VMware Cloud Director Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 To select a new storage policy for a virtual machine replication, in the top right of the page click the **VM** button, or to select a new storage policy for a vApp replication, click the **vApp** button.
- 3 Select a replication with a **Green** overall health.
- 4 Click **All Actions > Change storage policy**.
- 5 In the **Edit storage policy** window, select the new storage policy.
- 6 Optionally, you can select **Reset current storage policy**.

If the datastore that the replication resides on no longer belongs to the current storage policy, VMware Cloud Director Availability moves the replication to a datastore that belongs to the current storage policy. If there is a datastore with sufficient free space in the storage policy, the replication can move to that datastore, otherwise, the replication does not move.

- 7 After you modify the selection, click **OK**.

Results

In the **Tasks history** pane, the **Change storage profile** task runs for the selected storage policy.

Using Test Failover, Failover, Reverse, or Migrate

Test the failover, fail over, or migrate workloads by replicating vApps or virtual machines in the VMware Cloud Director Availability Tenant Portal. From on-premises or from a cloud site, you can test a failover, fail over, reverse failover, or migrate workloads.

Test Failover

By performing a test failover you can validate that the data from the source site replicates correctly in the destination site.

Perform a test failover for a replication then delete the test data.



Prerequisites

Before testing failover:

Important

- Verify that in the destination datastore, at least double the allocated storage of the virtual machine is available. For information about the storage requirements and examples, see [Deployment Requirements](#) in the *VMware Cloud Director Availability Installation, Configuration, and Upgrade Guide in the Cloud* then select your VMware Cloud Director Availability version.
 - Verify that in VMware Cloud Director, the **VM discovery** option is not activated. For information about deactivating virtual machine discovery, see [Discovering and Adopting vApps](#) in the *VMware Cloud Director documentation*.
-
- Verify that the vApp or the virtual machine is already protected in the destination site. For more information, see [Create a Protection](#).
 - Verify that you can access VMware Cloud Director Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 Select the protected vApp or virtual machine to test the failover and click **All actions > Test Failover**.
- 3 In the **Test Failover** wizard, configure the 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 in 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. After the test finishes, for the vApp and its virtual machines in the **Recovery state** column you see a `Test image ready` state.

- 4 To delete the test failover results, select the replication to clean.
 - a Click **All actions > Test Cleanup**.
 - b In the **Test Cleanup** window, click **Cleanup**.

The cleanup deletes all recovered vApps and virtual machines.

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 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

Important Before performing failover:

- Verify that in the destination datastore for sites running versions earlier than VMware Cloud Director Availability 4.2, at least double the allocated storage of the virtual machine including RAM size, is available. For information about the storage requirements and examples, see [Deployment Requirements](#) in the *VMware Cloud Director Availability Installation, Configuration, and Upgrade Guide in the Cloud* then select your VMware Cloud Director Availability version.
 - Verify that in VMware Cloud Director, the **VM discovery** option is not activated. For information about deactivating virtual machine discovery, see [Discovering and Adopting vApps](#) in the *VMware Cloud Director documentation*.
-
- Verify that the vApp or the virtual machine is protected in the destination site. For more information, see [Create a Protection](#).
 - Verify that VMware Cloud Director Availability is deployed in both the source and in the destination sites.
 - Verify that you can access VMware Cloud Director Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 Select the protected vApp or virtual machine to fail over and click **All actions > Failover**.
- 3 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	Select this option 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 this option 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**.
- 4 In the bottom pane, to monitor the progress of the task, click the **Tasks** tab.

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, remove the replication from the vApp and virtual machine list, and remove all retained replication instances, by clicking **Delete**.

Perform a Reverse Task

After a failover, return the workload data from the destination site back to the source site by reversing the replication.

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, VMware Cloud Director Availability uses the original datastore for the placement of the workload, regardless of the current on-premises local placement setting.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in both the source and in the destination sites.
- Verify that you can access VMware Cloud Director Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).
- Verify that the vApp or the virtual machine is failed over, before you can start a reverse task. For more information, see [Perform a Failover Task](#).
- Verify that 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 by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 Select the vApp or the virtual machine that are failed over and click **All actions > Reverse**.
- 3 In the **Reverse** window, click **Reverse**.

Reversing the replication enables the replication traffic and allows the replication to be recovered back to the source.

- 4 In the bottom pane, to monitor the progress of the **Reverse** task click the **Tasks** tab.

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.

Perform a Migrate Task

By migrating an existing replication to a remote organization, the workload runs in the destination site and the source workload is powered off.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in both the source and in the destination sites.
- Verify that you can access VMware Cloud Director Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).
- Verify that the vApp or the virtual machine is protected in the destination site, before you start a migrate task. For more information, see [Create a Migration](#).

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 Select the protected vApp or virtual machine to migrate over and click **All actions > Migrate**.
- 3 In the **Migrate** wizard, configure your selected workload for the migration.
 - a On the **Migrate 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 **Ready To Complete** page, review the task details and click **Finish**.

After a successful recovery, all source virtual machines are synchronized and then powered off. The migration completes when in the **Recovery state** column of the replication you see **Failed-Over**.

- 4 In the bottom pane, to monitor the progress of the task, click the **Tasks** tab.

Results

A manual (offline) sync runs. If the source workload is powered on, then it is powered off and a manual sync runs. Then the vApp or virtual machines are recovered on the destination site.

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, remove the replication from the vApp and virtual machine list, and remove all retained replication instances, by clicking **All actions > Delete**.

Replication States

The replication state depends on the state of the virtual machines that the vApp replication contains. Depending on the state of the replication, you can perform specific actions.

Replication Overall Health States

The **Overall Health** shows a color-coded overall replication health state.

Overall Health	Description
Green	There are no problems with the replication.
Yellow	There is a potential problem with the replication.
Red	The replication is not healthy. You must manually troubleshoot the problem.

Data Connection States

When a replication is configured, the data connection state shows the state of the replication.

Data Connection State	Description
Healthy	A green color-coded state, showing that the source can send data and the destination is receiving the data successfully. A successfully recovered replication is healthy.
Error	A red color-coded state, showing that there is a problem in the destination site. For example, the target datastore is full. You must manually troubleshoot the destination site.
Paused	A yellow color-coded state, showing that the replication is paused. No data is transferred. Recovery Point Objective (RPO) violations are expected.
Powered Off	The source virtual machine is powered off. Data transfer starts after you turn on the source virtual machine or you manually synchronize the replication.
Initial Synchronizing	The initial synchronization between the source and the destination sites is in progress.
Synchronizing	Synchronization between the source and the destination sites is in progress.
Pruning	Destination instances are being pruned.

Data Connection State	Description
Unknown	The source and destination states are unknown. There is a problem in both sites that you must manually troubleshoot.
Finished	The replication has been recovered and is no longer ongoing.

Recovery States

After performing a recovery operation, monitor the recovery state of the replication.

Recovery State	Description
Not started	Recovery operation is not started for the replication.
Complete	Recovery operation is complete. All instances are destroyed.
Test Image Ready	A test failover has completed successfully.
Recovering	Recovery operation is in progress.
Reversed	The replication has been reversed.
Unknown	The recovery status is unknown.

You can enable event notifications as a **tenant** user. Also, you can monitor data traffic usage and disk usage of replications and organizations, and required compute resources like CPU, memory, and storage of the replicated workloads that are provisioned on failover.

This chapter includes the following topics:

- [Forward Tenant Event Notifications](#)
- [Monitoring the Traffic Usage](#)
- [Monitoring the Disk Usage](#)
- [Monitoring the Resource Requirements](#)

Forward Tenant Event Notifications

As a **tenant** user, you can forward the VMware Cloud Director Availability event notifications to VMware Cloud Director, or by using email delivery. Both delivery channels carry the same event information.

For more information about the event notifications and their delivery channels, see [Event Notifications](#) in the *VMware Cloud Director Availability Administration Guide*.

Prerequisites

- Verify that VMware Cloud Director Availability 4.1 or later is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a tenant or as a service provider. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 Log in to the management interface of the Cloud Replication Management Appliance.
 - a In a Web browser, go to **`https://Appliance-IP-Address`**.
 - b Enter **tenant** user credentials.
 - c Click **Login**.
- 2 In the left pane, click **Event and Notifications**.

- 3 To configure email notifications in the VMware Cloud Director Tenant Portal, next to **Cloud Director Email** click **Configure in VCD** .

VMware Cloud Director Availability reads the following email settings from VMware Cloud Director:

- The SMTP server configuration.
 - The sender email address.
 - The recipients of the email, either explicit email address or the email addresses of organization administrators.
 - The default subject prefix.
- 4 To configure the notification delivery channels for replication management operations, next to **Replication Management Events** click **Edit**.
 - a To receive the events in VMware Cloud Director, select **Cloud Director events** as the notifications delivery channel.
 - b To save the selected delivery channel for replication management event notifications, in the **Replication Management Events** window click **Apply**.
 - 5 To configure the notification delivery channels and settings for replication monitoring, next to **Replication Monitoring Events** click **Edit**.

Option	Description
Replication Monitoring Channels	<ul style="list-style-type: none"> ■ To receive the events in VMware Cloud Director, select Cloud Director events as the notifications delivery channel. ■ If configured in VMware Cloud Director, to receive the events over email by using the VMware Cloud Director email configuration, select Cloud Director email as the notifications delivery channel.
RPO violation threshold time	Only forward events for replications with RPO violation time above this threshold. Use 0 to forward events for any RPO violation. The default value is 0 minutes.
RPO violation threshold count	Only forward events for replications with RPO violations count above this threshold. Use 0 to forward events for any number of replications with an RPO violation. The default value is 0.

- 6 To save the selected delivery channels for replication monitoring event notifications, in the **Replication Monitoring Events** window click **Apply**.

Results

VMware Cloud Director Availability starts forwarding tenant event notifications by using the selected delivery channels.

What to do next

You can monitor VMware Cloud Director Availability tenant events by using VMware Cloud Director, or your email client.

Monitoring the Traffic Usage

VMware Cloud Director 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.

VMware Cloud Director 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 Manager Service collects the traffic information for all replications to and from cloud sites and to and from on premises sites. The Manager Service aggregates the traffic information by organization.
- The cloud Replicator Service 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 Replicator Service counts the compressed bytes.
- Every 300 seconds, the Manager Service records to its persistent storage the historical traffic information from all connected Replicator Service instances. In an event of a Replicator Service 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.
- VMware Cloud Director 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

Monitor the Traffic Usage as a Tenant

As a **tenant**, on the **Dashboard** page 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 only available for virtual machines and is not available for vApps.

Prerequisites

- Verify that VMware Cloud Director Availability is successfully deployed in the site.

- Verify that you can access VMware Cloud Director Availability as a **tenant**. For more information, see [Accessing the VMware Cloud Director Availability Tenant Portal](#).

Procedure

- 1 On the **Dashboard** page, in the traffic data chart for the local site, enter the beginning and the end of the traffic reporting period.
- 2 To change the traffic data chart reporting interval, in the traffic 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.

In the bottom of the traffic 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 Usage 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 VMware Cloud Director Availability is successfully deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

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 exist. The values shown for 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 Usage of a Virtual Machine Replication](#).

Monitor the Traffic Usage of a Virtual Machine Replication

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

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

Prerequisites

- Verify that VMware Cloud Director Availability is successfully deployed in the site.
- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 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 bottom pane, the **Traffic** data chart shows the amount of traffic transferred by the selected replication in the past three minutes.

- 5 To switch the data chart from a live traffic view to historical data, click **Recorded**.
- 6 To change the data 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 set 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 the Traffic Usage as a Tenant](#) or see [Monitor and Export Organization Traffic Usage as a Service Provider](#).

Monitoring the Disk Usage

VMware Cloud Director Availability counts the disk space used by each virtual machine replication and aggregates the disk usage information per organization. You can monitor the disk usage for every replication in all directions. You can also monitor the disk usage for every organization.

VMware Cloud Director Availability shows the replication disk usage that an on-premises site or a cloud site uses for a certain period. The disk usage data charts show the disk space used by the replica files in the site.

You can access the historical disk usage information for any virtual machine replication and per organization.

Disk Usage Monitoring Retention

- When querying the historical disk usage information, you can set the beginning and the end of the information period.
- VMware Cloud Director Availability stores the historical disk usage 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.

Monitor the Disk Usage as a Tenant

As a **tenant user**, on the **Dashboard** page you can see the disk usage data chart for your organization. The chart shows the disk space that is used for the last five hours, up to two months.

The disk usage information is only available for virtual machines and is not available for vApps.

Prerequisites

- Verify that VMware Cloud Director Availability is successfully deployed in the site.
- Verify that you can access VMware Cloud Director Availability as a **tenant**. For more information, see [Accessing the VMware Cloud Director Availability Tenant Portal](#).

Procedure

- 1 On the **Dashboard** page, in the disk usage chart for the local site, enter the beginning and the end of the disk usage reporting period.
- 2 To change the disk usage data chart reporting interval, in the disk usage chart for the local site, select an interval of reporting.
 - To see the last five hours of disk usage, select the **5 minutes** interval.
 - To see the last two weeks of disk usage, select the **1 hour** interval.
 - To see the last two months of disk usage, select the **1 day** interval.

In the bottom of the disk usage chart, you can see the average disk usage for the selected interval.

Results

You see the disk usage information for your organization.

What to do next

You can monitor the historical disk usage for each replication. For more information, see [Monitor the Disk Usage of a Virtual Machine Replication](#).

Monitor and Export Organization Disk Usage as a Service Provider

As a **service provider**, you can see the volume of stored data for each organization. You can also export the daily storage data for a given period to a file.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

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

At the bottom of the disk usage data chart, you can see the average disk usage for the selected interval.

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

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

What to do next

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

Monitor the Disk Usage of a Virtual Machine Replication

In VMware Cloud Director Availability, you can see the historical disc usage for each virtual machine replication.

The disk usage information is only available for virtual machines and is not available for vApps.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 is deployed in the site.
- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **service provider**. For more information, see [Chapter 2 Accessing VMware Cloud Director Availability](#).

Procedure

- 1 In the left pane, choose a replication direction by clicking **Incoming Replications** or **Outgoing Replications**.
- 2 To show the virtual machine replications, click **VM**.
- 3 Select the virtual machine replication for which you want to see the disk usage information.
- 4 In the bottom pane, click the **Disk usage** tab.

In the bottom pane, the **Disk usage** data chart shows the disk space used by the selected replication.

- 5 To change the data chart reporting interval, enter the beginning and the end of the disk usage reporting period and select an interval of reporting.
 - To see the last five hours of disk usage, select the **5 minutes** interval.
 - To see the last two weeks of disk usage, select the **1 hour** interval.
 - To see the last two months of disk usage, select the **1 day** interval.

At the bottom of the disk usage data chart, you can see the average disk usage for the selected interval.

Results

You see the disk usage information for the selected replication. You can set 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 disk usage information. You can also monitor the disk usage as a tenant on the dashboard, or you can monitor and export the disk usage information for each organization. For more information, see [Monitor the Disk Usage as a Tenant](#) or [Monitor and Export Organization Disk Usage as a Service Provider](#).

Monitoring the Resource Requirements

VMware Cloud Director Availability shows the compute resource requirements of the replications that are provisioned on a failover. This information provides the required destination capacity and resources to fail over the protected workload to the destination site successfully.

The resource requirements contain the following information:

- The source virtual machine number of vCPUs.
- The virtual machine memory size.
- The sum of the capacity of the replicated disks.

The resource requirements are available for each virtual machine replication that does not have a test failover and is not failed over.

Aggregated information about the resource requirements is available on the following levels:

- On a vApp replication level as a sum of the resource requirements for each virtual machine replication in the vApp.
- On a destination OrgVDC level as a sum of the resource requirements for each virtual machine replication to the OrgVDC.
- On a destination organization level as a sum of the resource requirements for each OrgVDC in the organization.
- On a provider VDC level as a sum of the resource requirements for each OrgVDC in the provider VDC.

The resource requirements can help both the tenant users and the service providers with estimates about their OrgVDC:

- Tenants can see the required resources to fail over and power on the protected virtual machines in the destination cloud site. The resource requirements help the tenants estimate their OrgVDC capacity and help with provisioning planning.
- Service providers can see the required resources to fail over and power on the protected virtual machines:
 - Per tenant to provide extra capacity in their OrgVDC.

- By all tenants to calculate the level of over-provisioning for their disaster recovery service.

Monitor the Resource Requirements as a Tenant

As a **tenant**, in VMware Cloud Director Availability, you can see the required compute resources to fail over and power on the protected virtual machines in the destination cloud site. With this information, you can estimate your OrgVDC capacity and it helps you with provisioning planning.

VMware Cloud Director Availability presents the resource requirements as the combined CPU, memory, and storage resources that are provisioned on a failover for all virtual machine replications.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 or later is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **tenant**. For more information, see [Accessing the VMware Cloud Director Availability Tenant Portal](#).

Procedure

- 1 At the bottom of the **Dashboard** page, see the **Required resources** dashboard.

In this dashboard, you can see the combined resource requirements from all the OrgVDCs in your organization.

- 2 To see the resources required by an OrgVDC, in the left pane, click **Resources > by Organization VDCs**.

In the table that shows, you can see the required resources for each OrgVDC in your organization. In the top-right corner of the page, you can see the combined required resources from all the OrgVDCs in your organization.

- 3 To see the resources required by each replicated workload, navigate to the list of replications.

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

- b To see the resources required by virtual machine replications, click the **VM** button and click the **Resources** button.

For all virtual machine replications listed in the table, in the columns for CPUs, Memory, and Disk capacity you can see the resource requirements for each virtual machine replication.

- c To see the resources required by vApp replications, click the **vApp** button and click the **Resources** button.

For all vApp replication listed in the table, in the columns for CPUs, Memory, and Disk capacity you can see the resource requirements for each vApp replication.

Monitor the Resource Requirements as a Service Provider

As a **service provider**, in VMware Cloud Director Availability, you can see the required compute resources per tenant and by all tenants to fail over and power on the protected virtual machines in

the destination cloud site. With this information, you can calculate the level of over-provisioning in the disaster recovery infrastructure and provide the extra capacity to tenants.

VMware Cloud Director Availability presents the resource requirements as the combined CPU, memory, and storage resources that are provisioned on a failover for all virtual machine replications.

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 or later is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 At the bottom of the **Dashboard** page, see the **Required resources** dashboard.

In this dashboard, you can see the resource requirements by organization and a summary of the top five organizations and their proportional required resources.

- 2 To see the resources required by an organization, in the left pane click **Required Resources > by Organization**.

In the table that appears, you can see the resources required for each organization. If you expand an organization, you can also see the required resources for all VDCs in that organization.

- 3 To see the resources required by a provider VDC, in the left pane click **Required Resources > by Provider VDC**.

In the table that appears, you can see the resources required for each provider VDC. At the top of the page, you can see the combined resource requirements from all provider VDCs.

- 4 To see the resources required by each replicated workload, navigate to the replications view.

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

- b To see the resources required by the virtual machine replications, under *Show details* click **Resources**, while under *Grouping* **VM** is selected.

For all virtual machine replication listed in the table, in the columns for CPUs, Memory, and Disk capacity you can see the resource requirements for each virtual machine replication.

- c To see the resources required by vApp replications, under *Grouping* click **vApp**, while under *Show details* **Resources** is selected.

For all vApp machine replication listed in the table, in the columns for CPUs, Memory, and Disk capacity you can see the resource requirements for each vApp replication.

Bandwidth Throttling

6

In VMware Cloud Director Availability, as a **service provider**, you can set a global limit for the total incoming replication traffic from all remote cloud or on-premises sites. You can also configure a limit for the replication data traffic from the on-premises to cloud sites. Throttling the network bandwidth avoids the network saturation and prevents the overloading of the management connections with the replication data traffic that shares the network infrastructure.

Global Bandwidth Throttling for the Cloud Site

The global bandwidth throttling limits the transfer rate of the combined incoming replication data traffic to all local Cloud Replicator Appliance instances from all remote cloud or on-premises sites. 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 Cloud Replicator Appliance instances. The number of data connections or the activity within the connections has no effect on the bandwidth throttling.

On-Premises Outbound Bandwidth Throttling

The on-premises outbound bandwidth throttling applies per an individual VMware Cloud Director Availability On-Premises Appliance.

Configuring the organization replication policies with an outbound bandwidth throttling limit for the traffic from on-premises appliances to the cloud site is in megabits per second. This limit applies only to the replication data traffic from a VMware Cloud Director Availability On-Premises Appliance to a cloud site. This limit does not affect the management traffic and the replication data traffic from a cloud site to a cloud site and from a cloud site to a VMware Cloud Director Availability On-Premises Appliance.

Configuring a replication policy with a bandwidth throttling limit affects all VMware Cloud Director Availability On-Premises Appliance instances, on all on-premises sites that target the respective organization. Each VMware Cloud Director Availability On-Premises Appliance 4.0 receives and enforces the limit. Older versions of the appliance do not receive the limit.

This chapter includes the following topics:

- [Configure the Global Bandwidth Throttling for the Cloud Site](#)

- [Configure the On-Premises Outbound Bandwidth Throttling](#)

Configure the Global Bandwidth Throttling for the Cloud Site

In VMware Cloud Director Availability, as a **service provider**, you can configure the bandwidth throttling to set a limit for the incoming replication traffic from all remote cloud or on-premises sites.

Prerequisites

- Verify that VMware Cloud Director Availability is deployed in the cloud site.
- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 In the left pane under **Configuration**, click **Settings**.
- 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 From the **Tunnel nic** menu, select the Cloud Tunnel Appliance network adapter that is connected to the local site components.
 - d To save the settings, click **Apply**.

What to do next

You can also configure a limit for the replication data traffic from the on-premises sites to the cloud site. For more information, see [Configure the On-Premises Outbound Bandwidth Throttling](#).

Configure the On-Premises Outbound Bandwidth Throttling

In VMware Cloud Director Availability 4.0, as a **service provider**, you can configure the replication policies to set a limit for the replication data traffic from the on-premises sites to the cloud site.

Configuring the bandwidth throttling limit in the replication policy affects all VMware Cloud Director Availability On-Premises Appliance instances, on all on-premises sites that target the organization to which this replication policy applies.

For more information about the replication policies, see [Configuring Replication Policies](#).

Prerequisites

- Verify that VMware Cloud Director Availability 4.0 is deployed in the cloud site.

- Verify that you can access VMware Cloud Director Availability as a **service provider**. For more information, see [Accessing the VMware Cloud Director Availability Provider Portal](#).

Procedure

- 1 In the left pane, click **Policies**.
- 2 Select an existing replication policy.
- 3 Click **Edit**.
- 4 In the **Edit Policy** window, select **Enable bandwidth throttling**.
- 5 In **Max throughput per On-Premises Replicator Appliance**, enter the limit in mbit/s.
- 6 To save the bandwidth throttling limit, click **Apply**.
Without re-pairing the on-premises sites, the bandwidth limit applies in 30 minutes.
- 7 In the list of policies, in the Maximum throughput column you can see the bandwidth throttling limits for each policy.

Results

All instances of the VMware Cloud Director Availability On-Premises Appliance in the organization to which the replication policy applies receive and enforce the configured bandwidth throttling limit.

What to do next

You can also configure a global limit for the total incoming replication traffic from all cloud sites. For more information, see [Configure the Global Bandwidth Throttling for the Cloud Site](#).