User Guide

23 NOV 2021

VMware Cloud Director Availability 4.3

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

Contents

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

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://`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, extend your session to that site by accepting an authentication token or by providing credentials for the local VMware Cloud Director. Any replication operation to remote cloud sites and specific replication operations from remote cloud sites require an extended session.

Extending Session Authentication from Cloud to Cloud

VMware Cloud Director user logins create a session and receive a bearer JSON Web Token (JWT) used for authenticating future requests.

The Cloud Service manages its own session that is not directly tied to the VMware Cloud Director session. Create a local Cloud Service session by using either of the following two authentication methods:

- Provide a local VMware Cloud Director user and password for authentication for creating the Cloud Service session. Internally, the Cloud Service uses those credentials for creating a brand new VMware Cloud Director session that results in a brand new JWT.
- Alternatively, use an existing JWT without providing credentials for the Cloud Service which uses the existing VMware Cloud Director session for performing the necessary operations. The VMware Cloud Director Availability plug-in in the local VMware Cloud Director automatically uses that existing JWT for authentication.

Locally for your cloud site, by creating a Cloud Service session, you can use the local site replications, tasks, and others. As your current Cloud Service session associated a JWT for the local VMware Cloud Director, you can also browse the local VMware Cloud Director. While the JWT has not expired, you can perform replication operations that require accessing the local VMware Cloud Director.

To perform replication operations on remote cloud sites, you must extend your local Cloud Service session to the remote cloud site by using either of the following two authentication methods:

- When the remote VMware Cloud Director organization uses local users, provide the user credentials.

- When the local and the remote VMware Cloud Director and their organizations are associated, click **Use Multisite**. As one organization can be associated with multiple remote organizations, select the organization for authentication.
- For VMware Cloud Director Availability 4.3, when multiple cloud sites use a single VMware Cloud Director instance click **Use Multisite**. The drop-down menu for selecting an organization contains only the current organization.

Extending your Cloud Service session from the local to the remote VMware Cloud Director without providing local user credentials for the remote VMware Cloud Director uses the JWT for authenticating the extended session to the remote site.

After authenticating to the remote site, the Cloud Service keeps the newly created extended session and for the replication operations in the remote site uses the extended session without requiring credentials.

On-Premises Authentication to the Cloud

For versions of VMware Cloud Director Availability earlier than 4.3 or earlier than vCenter Server 7.0, the on-premises tenants have the following two options for performing disaster recovery operations that require authentication to the cloud site.

- When the VMware Cloud Director Availability vSphere Client Plug-In prompts for credentials, provide a local VMware Cloud Director user credentials for authentication. This option allows restricting the access to the on-premises infrastructure but does not allow using a dedicated identity management solution for authentication.
- Alternatively, use the VMware Cloud Director Availability plug-in in VMware Cloud Director for replication management operations. This option allows using a dedicated identity management solution for authentication but does not allow restricting access to the local on-premises infrastructure as during pairing requires selecting **Allow Access from Cloud**.

With vCenter Server 7.0 or later, VMware Cloud Director Availability 4.3 provides one new authentication mechanism for the on-premises tenants for performing disaster recovery operations in the VMware Cloud Director Availability vSphere Client Plug-In that require authentication to the cloud site, for example, configuring a new replication or falling over.

- When the VMware Cloud Director organization uses an external identity provider, for example, SAML, the on-premises tenants can now use that method for authentication.

1. When performing a replication operation requiring authentication, the VMware Cloud Director Availability vSphere Client Plug-In prompts for providing the remote site credentials. In that prompt, clicking **Use API token authentication** generates and displays a temporary token for authentication that requires acceptance in the VMware Cloud Director Availability plug-in in VMware Cloud Director.

2 Clicking **Login** opens a new browser window with the VMware Cloud Director Availability plug-in in VMware Cloud Director.

   a The tenant can select their typical authentication method for authenticating to VMware Cloud Director, such as single-sign-on or multi-factor authentication.

   b After they authenticate in VMware Cloud Director, a prompt requests verifying and accepting that the temporary token matches the one displayed in the VMware Cloud Director Availability vSphere Client Plug-In.

3 Accepting the temporary token associates it with the existing JWT of the VMware Cloud Director session. This association grants the VMware Cloud Director Availability vSphere Client Plug-In access to the cloud site for the duration of the session and the tenant can resume the disaster recovery workflow that requested credentials.

Note

- The token acceptance interval is 5 minutes. After this timeframe expires, VMware Cloud Director Availability requires generating a new token.
- A single token allows accepting or rejecting only once.
- Accepting the token creates a regular session that is active for up to 24 hours, or 30 minutes of inactivity.
- Logging out from vSphere invalidates the accepted token. After re-authenticating, when performing a replication operation requiring authentication you must generate a new token and then accept it.
- The tenant must ensure logging into the correct VMware Cloud Director organization for the on-premises site, or they cannot accept the token.
- On-premises authentication with a token requires vCenter Server 7.0 or later in the on-premises site and in each site VMware Cloud Director Availability 4.3 or later and is available only by using the VMware Cloud Director Availability vSphere Client Plug-In.

Session Expiration

- The local Cloud Service session has a soft time limit 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 you cannot prolong without re-authenticating. By default, the hard session lifespan expires after 24 hours. During this time, you can perform all operations, until you log out of the management interface, or in the **Peer Sites** page you select the site and you click **Logout**. In the *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 to a remote cloud site expires when the remote JWT becomes invalid, due to expiry or due to manual logout. By default, the lifespan of VMware Cloud Director JWT also expires in 24 hours. When modifying the lifespan of the JWT, for example, reducing to one hour, the extended session expires after one hour. When extending the lifespan of JWT 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 Extended Session Authentication

Extend the session to the remote site for the following replication operations, depending on where the replications reside.

Incoming Replications from Cloud

To manage the replications on the remote site you can perform some replication operations without authenticating and providing the remote site credentials, while you must authenticate and provide the remote site credentials for performing the remaining replication operations.

Replication Operations Not Requiring Authentication: No Credentials Needed	Replication Operations Requiring Authentication: 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	

Outgoing Replications to Cloud

To manage the replications on the remote cloud site for all replication operations you must authenticate and provide the remote site credentials.

Replication Operations Requiring Authentication: Provide Credentials for the Remote Site
Migrate
Failover
Test failover
New protection
New migration

Replication Operations Requiring Authentication: Provide Credentials for the Remote Site
Replication settings
Network settings
Disk settings
Change storage policy
Sync
Pause
Resume
Delete replication

Tenant Organization Impersonation

For information about impersonating as a tenant, see Log In by Using the VMware Cloud Director™ Provider Admin Portal.

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 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 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.

Replicating Workloads

4

Protect or migrate workloads by replicating vApps or virtual machines. VMware Cloud Director Availability protects or migrates vApps and virtual machines by replicating the workload from the source site to the destination site.

The replications are incoming from source sites, or outgoing to destination sites.

Replication Types

Protection

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

Migration

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

In VMware Cloud Director Availability 4.1 and later, the **service provider** controls protections and migrations separately by using replication policies, either only incoming, or only outgoing, or both, or neither.

By default, for a newly deployed VMware Cloud Director Availability:

- Protections are inactive in the default replication policy, both incoming and outgoing. To allow protections to or from the site, the **service provider** must modify the default policy. Alternatively, keep disaster recovery only for subscribers by assigning a custom policy to the organizations. For more information, see Configuring Replication Policies.
- Migrations are active in the default replication policy, both incoming and outgoing, to allow migrating workloads for everyone.

In VMware Cloud Director Availability 4.3 and later, for replication using **Data engine Classic**, on start virtual machine replication when VMware Cloud Director Availability encounters a virtual machine that is already configured for replication, possibly by another replication solution, it is unconfigured first and then it is configured for replication.

Replications Use Cases

Replications support the following sources and destinations:

SDDC	Solution	Description
On-premises	vCenter Server	An on-premises SDDC, managed by VMware Cloud Director Availability On-Premises Appliance.
	VMware Cloud Director	A private cloud site in an on-premises SDDC, managed by Cloud Replication Management Appliance.
VMware Cloud on AWS	VMC vCenter Server	An SDDC in VMware Cloud on AWS, managed by VMware Cloud Director Availability On-Premises Appliance
	VMware Cloud Director service	A VMware Cloud Director instance in VMware Cloud on AWS, managed by Cloud Replication Management Appliance.

For information about VMware Cloud Director Availability in VMware Cloud on AWS, see Migration to VMware Cloud Director service in the *Migration to VMware Cloud Director service Guide*.

In the following table:

- According to the replication type and the selected data engine:
- ✖ represents a non-operational use case.
- ⚠ represents a disabled or inactive use case that might be operational in a future version.
- ✔ represents an operational use case.
- * Note limitations.

Destination	Replication Type	Selected Data Engine:	Source			
			VMware Cloud Director	vCenter Server	VMC vCenter Server	VMware Cloud Director service*
VMware Cloud Director	Protection	Classic	✔	✔	✔**	✔**
		VMC	✖	✖	✖	✖
	Migration	Classic	✔	✔	✔	✔
		VMC	✖	✖	✖	✔
vCenter Server	Protection	Classic	✔	✖	✖	✔**
		VMC	✖	✖	✖	✖
	Migration	Classic	✔	✖	✖	✔**
		VMC	⚠	✖	✖	⚠

Destination	Replication Type	Selected Data Engine:	Source			
			VMware Cloud Director	vCenter Server	VMC vCenter Server	VMware Cloud Director service*
VMC vCenter Server	Protection	Classic	✗	✗	✗	✗
		VMC	✗	✗	✗	✗
	Migration	Classic	✗	✗	✗	✗
		VMC	⚠	✗	✗	⚠
VMware Cloud Director service*	Protection	Classic	✗	✗	✗	✗
		VMC	✗	✗	✗	✗
	Migration	Classic	✗	✗	✗	✗
		VMC	✓	✓	✓	✓

Note * For VMware Cloud Director service you could use either the **Classic** data engine or the **VMC** data engine but not both.

** The protection is in a single direction. The reverse workflow is not operational.

Depending on the selected data engine in VMware Cloud Director Availability, some use cases might not be operational. For example, when the **VMC** data engine is selected and the **Classic** data engine is not selected, VMware Cloud Director Availability cannot replicate between on-premises SDDCs.

For information about selecting the data engines, see Pair VMware Cloud Director Cloud Sites in the *Migration to VMware Cloud Director service Guide*.

Recovery Point Objective - RPO

Shorter RPO lowers the data loss during recovery, at the expense of consuming more network bandwidth for keeping the destination site replica updated and increasing the volume of event data in the vCenter Server database.

Shorter RPO requires all operations in the background to complete in shorter time periods. Reducing the RPO increases the stress for all infrastructure components and increases the demands for both the source and for the destination sites and for the connectivity between them. For information about monitoring the environment to discover possible bottlenecks and implementing infrastructure changes for optimizing the flow of the replication data traffic, see the Replication Flow document.

Target RPO of Protections

RPO is the longest tolerable time period of data loss from a protected workload.

For example, protected virtual machine with one hour RPO means that the recovered virtual machine in the destination site can incur no more than one hour of data being lost when the source site fails. In VMware Cloud Director Availability 4.3 and later, for protections the RPO selection ranges from one minute to 24 hours. With shorter RPO, an I/O intensive protected workload can cause RPO violations.

Note Migrations RPO is 24 hours.

When each replication reaches its target RPO, in addition to updating the destination site replica the Replicator Service writes about 3800 bytes in the vCenter Server events database. For reducing the volume of event data, configure a longer RPO or limit the number of days that vCenter Server retains event data.

Quiescing

To achieve a consistent state, by quiescing the Replicator Service guarantees a failure consistency among all disks in a virtual machine.

Activate Quiesce

Activating quiescing might obtain a higher level of failure consistency among the disks belonging to a virtual machine.

The operating system of a virtual machine determines the available types of quiesce. Quiescing is available only for virtual machine operating systems that support quiescing.

Owner

The user that starts a replication becomes its owner.

After starting the replication, the **system administrator** can change the owner of a selected replication. Any replication started by the **system administrator** is not visible to the respective organization and its tenants unless the **system administrator** explicitly changes the replication ownership to the organization. To manage such a replication by a tenant, change the replication owner to the organization of the tenant.

As a **system administrator**, to change a replication owner, select the replication and click **All Actions > Change Owner**. In the **Change Replication Owner** window, select a new owner organization for the selected replications and click **Apply**.

- **System organization** - assigns the system administrator as a replication owner. Tenants do not see replications owned by the system organization.
- **Tenant organization** - assigns the organization in the destination* site as a replication owner, allowing the tenants from the destination organization to see and interact with the replication. Destination organization ownership applies both for replications from cloud sites to cloud sites and from on-premises sites to cloud sites.

* If the destination of the selected replication is an on-premises site, assigns the organization in the source site as a replication owner, allowing the tenants from the source organization to see and interact with the replication. Source organization ownership applies only for replications from cloud sites to on-premises sites.

Replication tasks initiated by the **system administrator** are not visible to the tenants, even after providing the organization with ownership.

Compute Policy

VMware Cloud Director Availability 4.3 allows the service providers and their tenants to select a placement compute policy for a specific cluster or host for the recovered virtual machine (VM).

Select the policy when configuring new replications or in the replication settings of an existing replication.

VDC VM Placement Policy

> The placement policies represent organization VDC compute policies that define the VM-host affinity rules controlling the placement of tenant workloads on a host, group of hosts, or one or more clusters. Selecting a placement policy adds the recovery VM to a VM group in vCenter Server, where the VM groups represent the host group to which they have positive affinities. A positive affinity rule places a VM group on a specific host.

For information about creating placement policies in a provider VDC and about adding them to an organization VDC, select the VMware Cloud Director version in the following *VMware Cloud Director* documentation.

- See Create a VM Placement Policy within a Provider VDC.
- See Add a VM Placement Policy to an Organization VDC.

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

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)

- RDM in virtual compatibility mode can be protected.
- RDM in physical compatibility mode is skipped from replication.

Multi-writer Disks

VMware Cloud Director Availability does not support disks in multi-wire 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

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

The **service provider** 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 to allow configuring custom SLA settings in the replications or to only use preset SLA profiles. For information about the SLA profiles, see Configuring SLA Profiles.
- Whether for protections to allow advanced retention rules to enable retention policy configuration for the number of rotated instances and their time distance spread apart. For more information, see *Advanced Retention Rules* in Using Instances.
- The maximum number of rotated instances per protection, automatically managed and subjected to an automatic retention. For information about the instances, see Using Instances.
- The maximum number of stored instances per protection, manually managed and not subjected to an automatic retention. For information about the instances, see Using Instances.
- The protections Recovery Point Objective (RPO) for an organization. For information about the RPO, see Chapter 4 Replicating Workloads.

Events and Notifications

- Activating settings changes allows tenants to manage their event notifications. For information about the tenant events and notifications, see Events and Notifications and Configure Tenants Events in the *Administration Guide*.

General limits

- The maximum number of incoming replications, including both replications and protections that can be created for an organization. Deselecting this limit allows unlimited number of incoming replications.

- The maximum throughput allowed per each VMware Cloud Director Availability On-Premises Appliance. For information about the throttle, see Bandwith Throttling in the *Administration Guide*.

Default Policy

The default replication policy applies to all organizations that are not associated with a custom replication policy.

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.

To enable protections when only using the default policy, without creating custom policies, you must modify the default policy attributes and allow incoming and or outgoing protections.

Table 4-3. Default Policy Attributes

Setting	Default Value
Policy name	Default Policy
Incoming migrations	Selected. In both directions, the migrations are allowed, by default.
Outgoing migrations	
Incoming protections	Deselected. By default, in both directions, the protections are disallowed.
Outgoing protections	
Custom SLA settings	Unavailable when incoming protections are deselected, by default. To allow selecting and configuring custom SLA settings, advanced retention rules, maximum number of rotated or stored instances, or minimum allowed RPO, first select the incoming protections.
Allow advanced retention rules	
Max rotated instances per protection	
Max stored instances per protection	
Minimum allowed RPO	
Settings changes	Selected
Limit the number of configured replications	Deselected (unlimited). To select and configure the limit for the number of configured replications, the incoming migrations, or incoming protections, or both must be selected.
Bandwidth throttling	Deselected (unlimited)

New Replication Validation

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

- 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 the assigned replication policy to the destination organization allows setting custom SLA settings in the replication or requires using the preset SLA profiles.
- Whether the assigned replication policy to the destination organization allows advanced retention rules for protections.
- 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.
- Whether the total number of allowed incoming virtual machine replications, both migrations and protections, incoming from on-premises sites and from cloud sites, does not exceed the limit that is assigned to the destination organization.
- Whether the network throughput per each VMware Cloud Director Availability On-Premises Appliance does not exceed the maximum throughput of the policy that is assigned to the destination organization.

When any of these replication attributes is violated, the new 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 create replication policies.

Prerequisites

- Verify that VMware Cloud Director Availability 4.3 or later is deployed in the cloud site for allowing advanced retention rules.
- 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**.

Option	Description
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.
Allow advanced retention rules	If incoming protections are selected, select to enable advanced retention rules for protections for configuring the number of rotated instances and their time distance spread apart.
Max rotated instances per protection	If incoming protections are selected, enter the maximum number of rotated instances per protection, up to 24.
Max stored instances per protection	If incoming protections are selected, enter the maximum number of stored instances per protection, up to 24.
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 from as short as one minute to the maximum of 24 hours. **Note** For shorter RPO, follow the recommendations for lowering the occurrence of RPO violations for the protection, by using all-flash storage and see Chapter 4 Replicating Workloads. With short RPO, even when meeting these recommendations, an I/O intensive protected workload can still cause RPO violations.
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 created the replication policy and you see the new policy 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 the replication policies assigned to VMware Cloud Director organizations, as a **service provider** you can edit any existing replication policy.

Prerequisites

- Verify that VMware Cloud Director Availability 4.3 or later is deployed in the cloud site for allowing advanced retention rules.
- 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**.

Option	Description
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.
Allow advanced retention rules	If incoming protections are selected, select to enable advanced retention rules for protections for configuring the number of rotated instances and their time distance spread apart.
Max rotated instances per protection	If incoming protections are selected, enter the maximum number of rotated instances per protection.
Max stored instances per protection	If incoming protections are selected, enter the maximum number of stored instances per protection.
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. **Note** For shorter RPO, follow the recommendations for lowering the occurrence of RPO violations for the protection, by using all-flash storage and see Chapter 4 Replicating Workloads. With short RPO, even when meeting these recommendations, an I/O intensive protected workload can still cause RPO violations.
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. After you modify the value, the new value takes effect after 30 minutes.

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 for protections, the service providers can define and control the following SLA settings: Recovery Point Objective (RPO), advanced retention policies for the rotated instances, quiescing, compression, and initial synchronization time.

SLA Settings Enforced by SLA Profiles

As a **service provider**, you can assign one or more SLA profiles to multiple VMware Cloud Director organizations to control the following SLA settings of the protections.

- The target recovery point objective (RPO). For information about the RPO, see Chapter 4 Replicating Workloads.
- For protections, allow advanced retention rules and add rule, up to five rules, to enable retention policy configuration for the number of rotated instances and their time distance spread apart. For more information, see *Advanced Retention Rules* in Using Instances.
- Whether quiesce is activated to ensure application level consistency before creating an instance.
- Whether the replication traffic compression is activated to reduce network traffic at the expense of CPU.

- Timeslot that allows to set a delay start that is convenient for the first synchronization.

After you assign one or more SLA profiles to an organization, the assigned SLA profiles can be selected in the replication settings.

Note Migrations do not use SLA profiles.

Predefined SLA Profiles

By default, VMware Cloud Director Availability provides the following predefined SLA profiles that are not assigned to any organization. The predefined SLA profiles set the following SLA settings.

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	4 hours
Enable retention policy	Selected		Deselected
Preserve retained instances	14	7	Keep latest instance only.
Retained instances over the last	1 day		
Enable quiesce	No		
Compress replication traffic	Selected		
Delay start synchronization	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 protection is available after enabling the **Allowed custom SLA settings** option in the replication policy. For more information, see Configuring Replication Policies.

Create an SLA Profile

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

Prerequisites

- Verify that VMware Cloud Director Availability 4.3 or later is deployed in the cloud site for adding advanced retention rules.

- 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).

      Note For shorter RPO, follow the recommendations for lowering the occurrence of RPO violations for the protection, by using all-flash storage and see Chapter 4 Replicating Workloads.

      With short RPO, even when meeting these recommendations, an I/O intensive protected workload can still cause RPO violations.

   c. Select whether for protections to allow advanced retention rules and click **Add rule**, up to five rules, to enable retention policy configuration for the number of rotated instances and their time distance spread apart.

   d. Select whether to activate quiesce.

   e. Select whether to enable compression of the replication traffic.

   f. Select whether to delay the first synchronization and select a timeslot.

Results

You created the SLA profile and on the **SLA Profiles** page you can see the new SLA profile listed.

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 4.3 or later is deployed in the cloud site for adding advanced retention rules.

- 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.

    > **Note** For shorter RPO, follow the recommendations for lowering the occurrence of RPO violations for the protection, by using all-flash storage and see Chapter 4 Replicating Workloads.
    >
    > With short RPO, even when meeting these recommendations, an I/O intensive protected workload can still cause RPO violations.

    c. Select whether for protections to allow advanced retention rules and click **Add rule**, up to five rules, to enable retention policy configuration for the number of rotated instances and their time distance spread apart.

    d. Select whether to activate quiesce.

    e. Select whether to enable compression of the replication traffic.

    f. Select whether to delay the first synchronization and select a timeslot.

Results

You have modified the SLA profile and on the **SLA Profiles** page 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 s**ervice 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 protected 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 the following two types of instances to which any protected workload can be recovered.

Rotated instances

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

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.

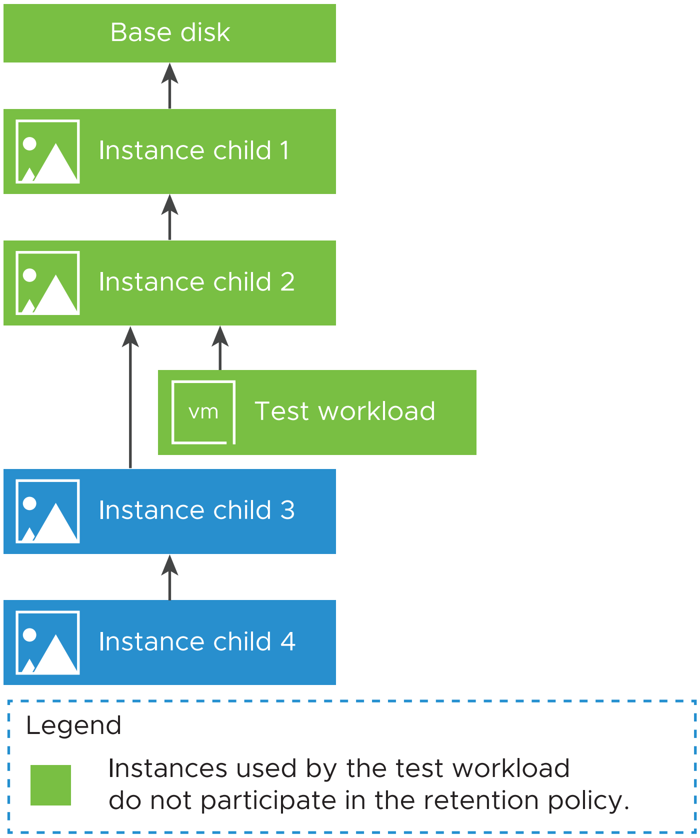
After manually storing an instance, the stored instance remains unchanged and if the protection is still active, the workload can be recovered to that stored instance.

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

Note Migrations do not use instances.

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 allows deleting.

Note After a test failover, the protection can have more stored instances than the replication 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 rule. After a test failover, the automatically created rotated instances continue to participate in the retention rule. After performing a test cleanup, the instances stored by the test failover are no longer stored and again start participating in the retention rule.



In the destination datastore, VMware Cloud Director Availability stores the instances in a hierarchy based on a redo-log. The retention rules for the rotated instances and the number of stored instances both determine the hierarchy depth. Every read of the recovered virtual machine that does not hit the child disks goes up the hierarchy to the parent disks.

As a result, the read performance of the recovered virtual machine depends on both the hierarchy depth and the instance sizes. The recovered virtual machine achieves better read performance when the instance is closer to the base disk.

- After performing failover or migration, the recovered virtual machine reaches optimal read performance once the instances consolidation completes. The period to consolidate instances depends on the number of parent instances and their size. This consolidation can run for both powered on and powered off virtual machines.
- After performing a test failover, the recovered virtual machine read performance might not be optimal, as instances consolidation does not run. To improve the read performance of the recovered virtual machine when performing a test failover, select an older instance since it is closer to the base disk.

Advanced Retention Rules

VMware Cloud Director Availability 4.3 and later allow configuring multiple retention rules for the rotated instances of the protections.

- In the replication policy assigned to the organization, to allow configuring more than one and up to five retention rules for protections, select **Allow advanced retention rules**.

  When this option is deselected, you can configure only a single retention rule for protections, unless you select an SLA profile assigned to the organization that is configured with multiple retention rules. When using an SLA profile, the maximum number of instances for the replication policy is not taken into account and the instances are restricted according to the SLA profile.
- In the SLA profile assigned to the organization, you can configure up to five retention rules.

  When the assigned replication policy does not allow advanced retention rules, in the replication settings of a protection you can select an assigned to the organization SLA profile that is configured with multiple retention rules.
- In the replication settings for a new or an existing protection, you can configure a single retention rule, or if the assigned replication policy allows, you can configure multiple retention rules.

  When the assigned replication policy does not allow advanced retention rules, you can select an assigned to the organization SLA profile that is configured with multiple retention rules.

In the SLA profile, or in the replication settings, under **Retention policy for point in time instances** select **Enable retention policy**, click **Add rule**, and create up to five rules, to enable retention rules configuration for the number of rotated instances and their time distance spread apart.

Each retention rule allows selecting the following retention settings.

Instances

Select how many rotated instances participate in the current retention rule.

Distance

Select the time distance that the rotated instances spread apart in the current retention rule.

Unit

Select the time unit for spreading the rotated instances in the current retention rule. Select one from:

- Minutes
- Hours
- Days
- Weeks
- Months
- Years

Selecting the number of instances, and the time distance and unit calculates and shows the overall retention period in the current retention rule for the selected retention settings. For example, the calculated retention period is:

- 10 instances, over distance 10 minutes unit - Retention period: 100 minutes.
- 10 instances, over distance 1 hours unit - Retention period: 10 hours.
- 2 instances, over distance 3 days unit - Retention period: 6 days.
- 2 instances, over distance 2 months unit - Retention period: 4 months.

The total number of instances in this example matches the maximum of 24 rotated instances.

VMware Cloud Director Availability evaluates multiple retention rules from top to bottom and first retains the instances that match the upper-level rules, then proceeds down the chain of retention rules.

Note When selecting any of the retention settings, consider the following.

- The target recovery point objective (RPO) must always be lower than or equal to the configured retention period distance, or you see a `Retention distance should be greater than RPO` message.
- Each advanced retention rule can have variable time distance between the rotated instances. From the first to the last rule, the distance for each next rule must increase, or you see a `Retention rules should have increasing distance` message.
- When reconfiguring a replication from using an SLA profile with multiple retention rules to manually-configured SLA settings with **Allow advanced retention rules** deselected in the replication policy, shows a `Policy doesn not allow multiple rules` message, until you remove the additional rules, leaving only one retention rule.

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 Virtual Machine Replications 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.
- VMware Cloud Director Availability 4.3 and later supports adding of other virtual machines to an existing vApp replication.

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 to a Single 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 4.3 or later 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. For on-premises to cloud replications click **Incoming Replications** or **Outgoing Replications**, depending on the context where you are currently logged in.
2. Click **New Protection** or **New Migration**.

3 Complete the **New Replication** wizard.

   a On the **vCenter VMs** page, select one or more virtual machines to replicate as a single vApp replication.

   b 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 replication.
   - Excluding virtual machines from the vApp replication.
   - Adding of virtual machines to the vApp replication for VMware Cloud Director Availability 4.3 and later.

   c On the **vApp Settings** page, configure the following settings and click **Next**.

   - Enter a name for the resulting vApp replication.

     To add the selected virtual machines to any existing vApp replication for VMware Cloud Director Availability 4.3 and later, enter the name of the existing vApp replication.

   - Optionally, change the order of boot of the virtual machines in the vApp replication 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 replication.

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, exclude or include replicated virtual machines in an existing vApp.

Prerequisites

- Verify that VMware Cloud Director Availability 4.3 or later 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 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 excluded virtual machine replication to a new vApp replication. Alternatively, you can later add this virtual machine to an existing vApp replication for VMware Cloud Director Availability 4.3 and later, as in the next step.

   b In the **Delete** window, to confirm click **Delete**.

7 To add replicated virtual machines to any existing on-premises to cloud vApp replication, create a replication.

   a To create an on-premises to cloud replication, click **New Protection** or **New Migration**.

   b On the **vCenter VMs** page, select one or more virtual machines for adding in an existing vApp replication.

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

   d On the **vApp Settings** page, to add the selected virtual machines to an existing vApp replication, in the **vApp name** text box enter the existing vApp name and click **Next**.

   After entering an existing vApp name, under **vApp name** a `vApp group '`*`name`*`' has` *`number`* `VM(s) already` message shows the count of virtual machines in the vApp.

Results

VMware Cloud Director Availability replicates the virtual machines from the source on-premises site as a 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@VCLOUD_DIRECTOR_IP:443?
org=ORG_NAME&vdc=VDC_NAME&vapp=VAPP_NAME' VAPP_NAME.ova
```

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

Importing a Virtual Machine from a Removable Media

You can import a virtual machine from a removable media directly in VMware 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 `.vmx` 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.
Retention policy for point in time instances	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. The number of preserved replication instances depends on the configured retention policy and requires that the RPO period is short enough for the replication instances to be created. For example, if you select to preserve four replication instances per day, the RPO period must not exceed six hours, to allow for the retention of four replication instances in 24 hours.
Enable quiesce	Select the quiescing method for the guest OS of the source virtual machine. **Note** Quiescing is available only for virtual machines that support quiescing. For more information, see Guest OS Quiescing Support.
Compress replication traffic	Select to compress the replication data that is transferred through the network and to reduce the network traffic. However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore.

8. On the **Scheduling** page, select when to start the replication and click **Next**.
   - Start the replication when the wizard finishes by leaving **Immediately** selected.

- Schedule the start of the replication by selecting **At a specific time**.

9 On the **Ready to Complete** page, verify that the configuration settings are correct and click **Finish**.

Results

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

What to do next

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

Create a Protection

Configuring a protection allows protecting a vApp or a virtual machine from one organization to another, while keeping the workload running in the source site. 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 4.3 or later is deployed in both the source and in the destination sites for selecting a placement compute 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 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 If you are configuring an on-premises to cloud replication, on the **Destination VDC and Storage policy** page, select the virtual data center for the replication destination and the storage policy for placing the recovered virtual machines, and click **Next**.

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

   For VDCs that do not have replications to them, the Quota column shows `Currently unavailable`, refreshing every 10 minutes.

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

Option	Description
Use SLA profile	To set the SLA settings of the replication, select any of the preconfigured SLA profiles. To manually configure the SLA settings, select **Configure settings manually**.
Target recovery point objective (RPO)	If you selected **Configure settings manually**, set the acceptable period for which data can be lost if there is a site failure by using the slider or by clicking the time intervals. The available RPO range for a protection is from one minute to 24 hours. **Note** For the lowest RPO of one minute, follow the recommendations for lowering the occurrence of RPO violations for the protection, by using all-flash storage and see Chapter 4 Replicating Workloads. With one minute RPO, even when meeting these recommendations, an I/O intensive protected workload can still cause RPO violations.
Retention policy for point in time instances	If you selected **Configure settings manually**, to preserve multiple rotated distinct instances to which the virtual machines can be recovered, select this option, select the number of replication instances to keep, and select the retention time distance and unit. The retention distance unit must be greater than RPO.
Compress replication traffic	If you selected **Configure settings manually**, to apply compression on the replication data traffic for reducing the network data traffic at the expense of CPU, select this option.
Delay start synchronization	If you selected **Configure settings manually**, choose the following option. ■ 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.
VDC VM placement policy	Select an organization VDC placement compute policy for the recovered virtual machines.
Exclude disks	To select specific hard disks of the virtual machines for replicating to the destination site for reducing the replication data network traffic, select this option.
Configure Seed VMs	To select a previous copy of the virtual machines in the destination site for reducing the replication data network traffic, 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 replication settings of the protection 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 fail over, or test, or migrate the protected workload to the destination site. When failing over, the source workload might not be operational. For more information, see Perform a Failover Task, or Test Failover, or Perform a Migrate Task.

Create a Migration

Configuring a migration allows later migrating a vApp or a virtual machine to a remote organization and running the workload in the destination site.

Prerequisites

- Verify that VMware Cloud Director Availability 4.3 or later is deployed in both the source and in the destination sites for selecting a placement compute 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 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 If you are configuring an on-premises to cloud replication, on the **Destination VDC and Storage policy** page, select the virtual data center for the replication destination 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 apply compression on the replication data traffic for reducing the network data traffic at the expense of CPU, leave **Compress replication traffic** selected.
   - To start the replication when the wizard finishes, leave **Delay start synchronization** deselected. Alternatively, to schedule the start of the replication, select it and enter the local date and time for starting the replication.
   - From the **VDC VM placement policy** drop-down menu, select an organization VDC placement compute policy for the recovered virtual machines.
   - To select specific hard disks of the virtual machines for replicating to the destination site for reducing the replication data network traffic, select **Exclude disks**.
   - To select a previous copy of the virtual machines in the destination site for reducing the replication data network traffic, select **Configure Seed VMs**.

   c If you selected **Configure Seed VMs**, on the **Seed VM** page select a vApp or a virtual machine to use as seed and click **Next**.

   d If you selected **Exclude disks**, on the **Replicated Disks** page select the virtual machine disks for replicating and click **Next**.

   e On the **Ready to complete** page, verify that the replication settings of the migration 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.

Note The target recovery point objective (RPO) for a migration is 24 hours. For information about the RPO, see Chapter 4 Replicating Workloads.

What to do next

You can migrate, or test, or fail over the workload to the destination site. During migration, if the source workload is powered on, then it is powered off and a manual synchronization runs. Then the vApp or virtual machines are recovered on the destination site. After a successful recovery, all source virtual machines are lastly synchronized while powered off. For more information, see Perform a Migrate Task or Test Failover or 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.

Using Disaster Recovery and Migration Plans

In cloud sites, orchestrate complex failover or migration by using disaster recovery or migration plans. The plans attach existing replications to ordered steps with optional delay or prompt attributes. Prioritize which workloads failover or migrate first and power on, followed by workloads pending specific conditions before recovering or migrating and powering on.

VMware Cloud Director Availability 4.3 introduces disaster recovery and migration plans. The plans orchestrate failing over or migrating already created vApp and virtual machine incoming replications to the disaster recovery site. Sequence and organize each workload disaster recovery or migration by priority, with available delays and prompts.

Plans

Each plan consists of sequential actions, called steps. The plans can contain an unlimited number of ordered steps.

- Disaster recovery plans contain steps performing test failover or failover of the protected workloads.
- Migration plans allow scheduling of the initial synchronization and contain steps performing migrations.

Steps

Each step in the plan can perform multiple existing replication tasks such as a test failover, a failover, or a migration of the workload with optional attributes after the step completes, like a delay or a prompt.

Delay

This step attribute allows configuring a waiting time before executing the next step. The delay applies after completing all replication tasks in the current step.

Prompt

This step attribute allows configuring a user prompt message, suspending the current step execution before the next step occurs, until approval of the prompt in the current step.

Scheduling Migrations Synchronization

Scheduling migration initial synchronization

You can schedule the initial synchronization time when creating any migration.

Then the initial synchronization waits for the scheduled time, while the replication remains paused.

Scheduling migration plans synchronization

You can schedule a synchronization when creating or editing a migration plan.

Then all the plan migrations synchronize at the scheduled time, regardless of their previous synchronizations.

Delayed synchronization

At the migration plan scheduled time, if the migrations are started paused, meaning the virtual machine is not running or migration initial synchronization time is scheduled in the future, the migration performs its initial synchronization.

Synchronize before migrate

At the migration plan scheduled time, if the migrations are already synchronized, meaning the virtual machine is running and no migration initial synchronization time is scheduled at all or it has been scheduled but the synchronization already passed, the migration performs a subsequent synchronization, for reducing the Recovery Time Objective (RTO) near the actual migration.

Note Configuring the scheduled synchronization in a migration plan overwrites the initial synchronization of its migrations.

Step and Plan Execution

Execution of the plan repeats for each step the following fixed execution sequence, according to the configured attributes.

1 Execute and complete the step of the plan. In parallel, for each vApp or virtual machine in the step:

   a First, perform the replication task like test failover or failover by using the latest available instance for the replication. Migrate tasks perform at least one synchronization before falling over.

   b After the replication task completes, power on the workload.

2 Skip, unless a delay is configured.

   a Else, the step waits for the configured seconds or minutes.

   b After the delay, the plan resumes executing #3.

3 Skip, unless a prompt is configured.

   a Else, suspend the plan after completing the current step, until approving the prompt.

   b Prompt the user. Approving the prompt resumes executing #4.

4 Repeat this sequence with the next step in the plan, if any more, executing from #1.

- After the last step, the plan completes with a `Completed Failover` or a `Completed Migrate` state, regardless of whether certain replication operations completed with a warning.
- Alternatively, the plan suspends with a `Suspended` state on a prompt, or when clicking **Suspend**, or at any step where the replication operation fails with an error message. For example, a plan suspends at a migration step that requires authentication with the remote site.

Plan States

The allowed operations on a plan depend on the current state of the plan and on the last operation.

Not started plans

Not started state persists before executing any plan operation, or after executing test cleanup operation. The plans allow all operations, like test failover, failover or migrate, editing and modifying the steps, and attaching and detaching replications.

Running plans

While running, plans only allow clicking **Suspend**, suspending the plan after the current step executes. Running plans do not allow any other replication operation, nor modifying the steps, nor their order, nor attaching and detaching replications.

Suspended plans

- Suspended on prompt plans resume after approving the prompt. Alternatively, they resume with failover or migrate.
- Suspended plans after test or cleanup step allow resuming with test failover or test cleanup, failover or migrate,
- Suspended plans after a failover or a migrate step, allow resuming with failover or migrate.
- All suspended plans allow editing and modifying the steps and attaching and detaching replications. For example, detaching replications that cause suspending the plan, allows resuming the plan execution.
- Modifying the steps order then resuming uses the previous step order before the modification. New steps execute according to their order, for example, adding a step and moving it before the currently suspended step resumes execution with the new step first.

Completed plans

- Completed failover and completed migrate plans only allow deleting or cloning in a new plan. Such plans do not allow editing nor modifying their steps, nor attaching and detaching replications.
- Completed test failover plans, allow test cleanup, failover, migrate, and editing but do not allow attaching and detaching replications.

- Migration plans migrate their workloads and complete. Similarly, failover plans perform failover and complete.
- Empty steps execute and complete, performing no operations and continue with the next step.
- Empty plans without steps or with empty steps execute without performing any tasks and have a `Completed` state.

Replications Implications

- Steps can only use existing replications and do not create new replications.

- The plan steps treat the replicated workload similarly, regardless of whether it is a vApp replication or a virtual machine replication.
- One replication task can be part of multiple plans but not in multiple steps in the same plan.

  When using the same replication task in more than one plan and several plans using this task start simultaneously, the plan that first starts the replication task completes its steps. The remaining plans steps also complete while skipping this reused replication task as already performed when the step completed. If the step is in progress, remaining plans can fail.

  For example, running two plans that contain steps with replication tasks for the same workload. The first plan executes a step performing a failover task then the second plan executes a step performing a test failover task. As a result, the plan executing the test failover task fails, at the step containing the already failed over replication.
- Deleting a replication while used in a plan, detaches the replication from the step where attached, without the plan failing.
- To change advanced replication settings, like network settings or disk settings, directly modify the replication settings. After the modifications, all plans using the modified replication execute by using the updated replication settings.

Plans Operations

The plans are available only from the cloud site. After logging in the cloud site, in the left pane, under the **Replications** section click **Recovery Plans**.

Note The plans are not available from on-premises sites. On-premises workloads can be part of the plans and are managed from cloud site.

New recovery plan

Allows entering a name and optional description then creates a blank disaster recovery plan for adding steps that perform protections.

New migration plan

Allows entering a name, optional description, optional synchronization schedule of the migrations then creates a blank migration plan for adding steps that perform migrations. Scheduling the migration in the plan overrides the usual scheduled migration.

Selecting an existing plan that is in a `Not started` or in a `Suspended` state allows the following actions.

New step

Adds a step in the selected plan. For information about the actions of the steps, see the next section.

Edit

Editing allows modifying the selected plan name and description and for migration plans modifying the automatic synchronization schedule. Editing is available for plans in a `Not started`, or `Completed Test`, or `Suspended` state.

Delete

Prompts a confirmation for removing the selected plan. Deleting is available for suspended, completed, and not started plans. Deleting is not available only for plans in a `Running` state.

Suspend

Requests pause of the execution of the selected plan after completing the currently running replication task in the current step. Suspending is available for any plan in a `Running` state. While suspended, the plan allows attaching and detaching replications, re-ordering the steps, and adding or removing steps. Modifying the steps or their order causes resuming the plan execution at the first step and skipping completed steps, where an already approved prompt means a completed step. When a prompt suspends the step, after reordering the steps and then approving the prompt resumes with the original next step as before reordering and the plan completes.

Test

Performs a test failover task for all workloads in the selected plan. Testing is inactive after a test or after a failover or a migrate task completes.

Test Cleanup

Performs a cleanup of the test failover tasks for all workloads in the selected plan. Cleanup is inactive, until completing a test.

Failover

Performs a failover task for all workloads in the selected plan. Failover is inactive after a failover or a migrate task completes. Failover is available for plans in a `Not started`, or `Completed Test`, or `Suspended` state.

Migrate

Performs a migration task for all workloads in the selected plan. Migrate suspends unless authenticated with the remote site. Migrate is inactive after a failover or a migrate task completes. Similar to failover, migrate is available for plans in a `Not started`, or `Completed Test`, or `Suspended` state.

Monitor tasks

Opens **Replication Tasks**, filtered to only display the tasks of the selected plan.

Other actions

- Change owner - allows selecting a new owner organization for the selected plan. The ownership and the visibility of a plan belong to the user who initially created it. For example, plans created by the service provider are not visible to a tenant user, until the changing the owner. Change owner is inactive after failover or migrate complete.
- Clone - prompts for a name of the duplicate plan and copies the steps of the selected plan in the duplicate plan. Optionally, cloning allows detaching all replications from the steps of the duplicate plan, while preserving the steps. Cloning a disaster recovery plan creates a disaster recovery plan duplicate, similarly cloning a migration plan, creates a migration plan duplicate. Both completed and suspended plans allow cloning. The cloned plan is in a `Not started` state with `Not started` steps, regardless of whether any steps completed in the source plan.

Steps Actions

Selecting an existing plan that is in a `Not started` or in a `Suspended` state allows adding steps in the plan.

New step

- For disaster recovery plans, completing the **New Recovery Step** wizard allows attaching multiple vApp or virtual machine protections for recovery in the step and creates a recovery step.
- For migration plans, completing the **New Migration Step** wizard allows attaching multiple vApp or virtual machine migrations for recovery in the step and creates a migration step.

Completing each of the **New Step** wizards allows selecting an optional delay and an optional prompt that suspends that step unless approved.

Selecting an existing and not executed step from an existing plan that is in a `Not started` or in a `Suspended` state allows the following actions for the step.

Edit

Allows modifying the name, the optional delay, and the optional prompt of the selected step.

Delete

Prompts a confirmation for removing the selected step from the current plan. Deleting is available for completed steps but not while a step is running.

Attach

The **Attach replications** window allows selecting vApp or virtual machine replications for attaching in the selected step.

- When attaching a vApp replication, changing the number of replicated virtual machines in that vApp replication, affects the plan. Adding virtual machine replications for that vApp attaches the new virtual machine replications to the step with the attached the vApp. Similarly, removing virtual machine replications from the vApp detaches them from the step.
- Alternatively, attaching all the virtual machine replications of a vApp replication in the step permanently fixes those virtual machine replications as part of the step. Adding or removing virtual machine replications to the same vApp replication does not affect the step or the plan.

Selecting an already attached replication in a step allows the following actions for the replication.

Detach

Prompts a confirmation for removing the selected replication from the current step.

Move to step

Prompts for selecting a destination step for the selected replication. Moving is inactive when the plan contains only one step.

Note The order of the steps in a plan allows re-arranging by dragging and dropping each step for re-ordering.

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: - **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 *network name*. 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.
IP mode	- **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.

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

Option	Description
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 *vmname-001*. 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	Select how to connect the virtual machine to a network in the target cloud site: ■ **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 *network name*. As a result, the vApp is bridged and has a direct connection to the target OrgVDC network.
Connected	Select to enable the connection for the NICs in the virtual machine to the target site network.
Primary NIC	Select the primary NIC for the virtual machine.
MAC address	See the MAC address for each NIC in each virtual machine in the selected replication.
Reset MAC	Select to reset the MAC address of the highlighted NIC in the target site.
IP mode	■ **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**.

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

Option	Description
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 *vmname-001*. 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	Select the discovered network that the vApp connects to in the target site after a migration, failover, or test failover: ■ ***Network name*** select to replicate the source vApp network in the target site and connect the target vApp to the selected orgVDC *Network name* 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	■ **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.

Table 4-8. Virtual Machine Network Settings Configuration for Replications from Cloud to Cloud (continued)

Option	Description
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	■ **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.

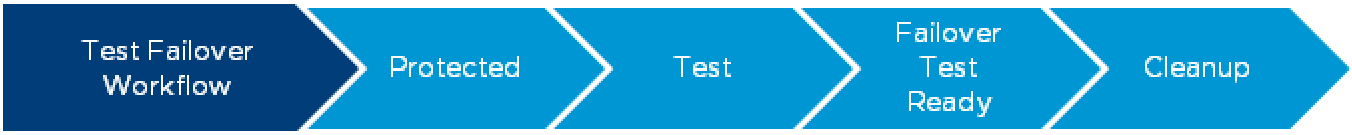
Using Test Failover, Failover, Reverse, or Migrate

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 *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	■ 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 *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	■ 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 Reverse a Replication.
- 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**.

Reverse a Replication

After performing a fail over or a migrate, return the workload from the destination site back to the original source site by reversing the replication.

After performing fail over or migrate, the workload runs in the destination site. Performing a subsequent reverse task replicates the failed-over or migrated workload data to the source workload.

Optimized reverse:

VMware Cloud Director Availability skips performing a full synchronization back to the original source workload when performing a reverse task by replicating only the deltas.

Optimized reverse works only if the original source workload is not powered-on since the initial migrate and when no blocks changed in the original source and the original source disks are not modified in any way.

Optimized reverse is available for limited time after performing migrate, by default, for a week. Under **Details** of the failed-over replication, see the `Optimized reverse` expiration time. After this time expires, or if the source workload is powered-on, reversing the replication skips optimized reverse and performs a full synchronization.

Note

- When reversing a replication from a Cloud Director site back to an on-premises site, VMware Cloud Director Availability uses the original datastore for the placing the virtual machines, regardless of the current on-premises local placement setting.

Prerequisites

- Verify that in the destination datastore, at least double the allocated storage of the virtual machine is available for a successful reverse operation.
- Verify that VMware Cloud Director Availability 4.3 or later is deployed in both the source and destination sites for optimized reverse.
- Verify that you can access VMware Cloud Director Availability as a **tenant** or as a **provider**. For more information, see Chapter 2 Accessing VMware Cloud Director Availability.
- Verify that the replication is in a `Failed-Over` recovery state before you can start a reverse task. For optimized reverse, ensure that the replication is migrated. For more information, see Perform a Failover Task or Perform a Migrate 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 an exiting replication that is failed-over and click **All actions > Reverse**.

Optimized reverse requires already migrated replications. Alternatively, when the source workload is powered-on, reverse performs full synchronization.

3 In the **Reverse** window, to confirm the reversal of the replication, click **Reverse**.

Reversing the replication enables the replication traffic and recovers the workload back to the original source site.

The Last changed column shows the reverse task progress in percentages. After reversing a replication, the direction of this replication reverses. To see the reversed replication:

- After reversing an incoming replication, in the left pane, click **Outgoing Replications**.
- After reversing an outgoing replication, in the left pane, click **Incoming Replications**.

4 (Optional) In the bottom, to monitor the task progress click the **Tasks** tab.

Results

After the reverse task completes, the Recovery state column of this replication shows `Reversed` and the reversed replication overwrites the original source workload. The reversed workload runs in the destination site, while protected in the original source site.

What to do next

- You can test, fail over, or migrate the reversed workload back in the original source site. For more information, see Test Failover, Perform a Failover Task, or Perform a Migrate Task.

  When any of those tasks completes, the Recovery state column of this replication shows a green `Failed-Back` state. Then, after failing-back a reversed replication you can only perform a reverse task.

- You can pause the reversed replication and edit the replication configuration. You can permanently stop the traffic of this replication and remove it with all retained replication instances by clicking **All actions > Delete replication**.

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	■ 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 Reverse a Replication.
- 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.
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.

Monitoring 5

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

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 *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	■ 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 exists. The values shown for the that time are NaN, which evaluates to 0.

What to do next

You can select another organization and see its traffic information. You can also monitor the traffic for each replication. For more information, see Monitor the Traffic 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.